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，并管理跨多租户基础架构的存储活动。

Element 是SolidFire集群的核心存储操作系统。 Element 软件在集群中的所有节点上独立运行，使集群中的节点能够组合资源，并作为单一存储系统呈现给外部客户端。 Element 软件负责整个系统的集群协调、扩展和管理。

该软件接口基于 Element API 构建。

- "访问 Element 软件用户界面"
- "部署后配置SolidFire系统选项"
- "升级存储系统组件"
- "使用 Element 软件用户界面中的基本选项。"
- "管理账户"
- "管理您的系统"
- "管理卷和虚拟卷"
- "保护您的数据"
- "排查系统故障"

查找更多信息

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

您必须确保浏览器中的弹出窗口拦截器和 NoScript 设置已禁用。

您可以使用 IPv4 或 IPv6 地址访问 UI，具体取决于集群创建期间的配置。

1. 选择下列选项之一：
   - IPv6：输入 https://[IPv6 MVIP 地址] 例如：

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

   - IPv4：输入 https://[IPv4 MVIP 地址] 例如：

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

2. 对于 DNS，请输入主机名。
3. 点击忽略所有身份验证证书消息。

查找更多信息

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

部署后配置SolidFire系统选项

部署后配置SolidFire系统选项

设置好SolidFire系统后，您可能需要执行一些可选任务。

如果您更改了系统中的凭据，您可能需要了解这对其他组件的影响。

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。您还应该在必要时更新密码。

查找更多信息

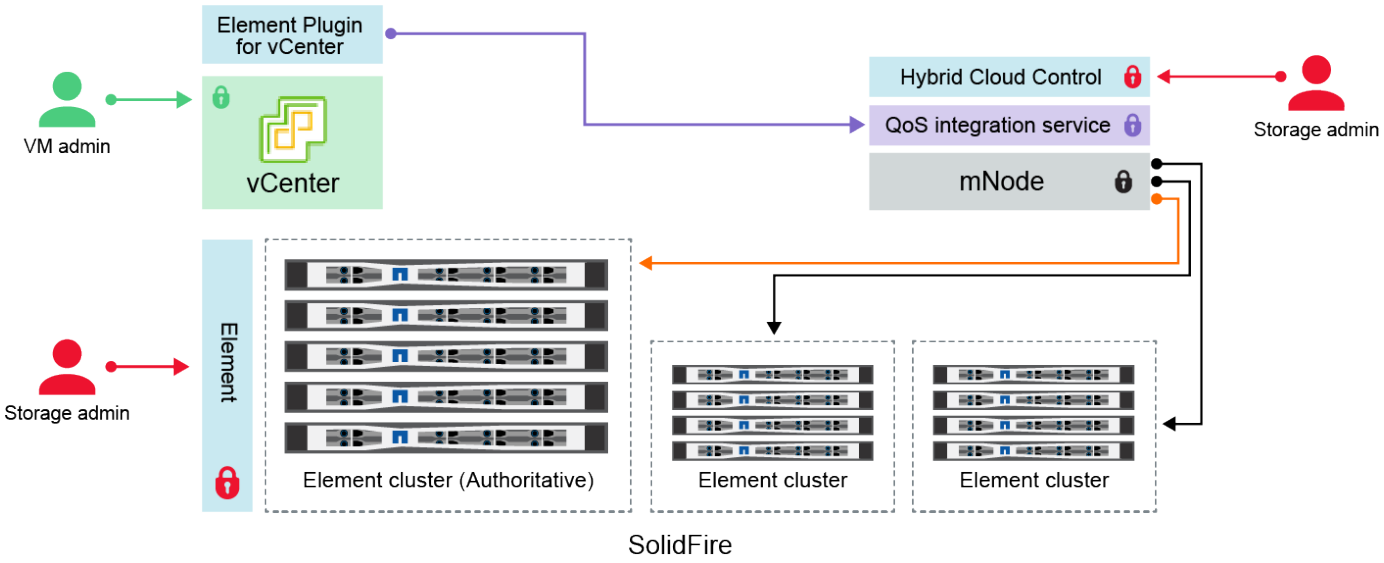
- "更改NetApp HCI和NetApp SolidFire中的凭据"
- "更改 Element 软件的默认 SSL 证书"
- "更改节点的 IPMI 密码"
- "启用多重身份验证"
- "开始使用外部密钥管理"
- "创建支持 FIPS 驱动器的集群"

更改NetApp HCI和NetApp SolidFire中的凭据

根据部署NetApp HCI或NetApp SolidFire 的组织的安全策略，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，您应该了解此举对部署中其他软件组件的影响。

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

NetApp SolidFire组件交互
：



凭证类型和图标	管理员使用情况	请参阅这些说明
元素凭证	适用范围： NetApp HCI和SolidFire 管理员使用以下凭据登录： • 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，它只接受存储集群的管理员凭据，即最初设置 mnode 的_权威集群_。对于之后添加到混合云控制的存储集群，mnode 安全地存储管理员凭据。如果后续添加的存储集群的凭证发生更改，则还必须使用 mnode API 在 mnode 中更新凭证。	• "更新存储集群管理员密码。" • 使用以下命令更新 mnode 中的存储集群管理员凭据："修改集群管理员 API" 。
vSphere 单点登录凭据	适用范围：仅限NetApp HCI 管理员使用这些凭据登录 VMware vSphere Client。当 vCenter 作为NetApp HCI安装的一部分时，凭据在NetApp部署引擎中配置如下： • 使用指定的密码，以 username@vsphere.local 用户名登录，并 • administrator@vsphere.local 使用指定的密码。当使用现有的 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"。

凭证类型和图标	管理员使用情况	请参阅这些说明
基板管理控制器 (BMC) 凭证 	适用范围：仅限NetApp HCI 管理员使用这些凭据登录到NetApp HCI部署中NetApp计算节点的BMC 。 BMC提供基本的硬件监控和虚拟控制台功能。 在NetApp HCI部署中，每个NetApp计算节点的BMC （有时称为 *IPMI*）凭据安全地存储在 mnode 上。 NetApp Hybrid Cloud Control 使用BMC凭证作为服务帐户，在计算节点固件升级期间与计算节点中的BMC进行通信。 当BMC凭证更改时，mnode 上相应计算节点的凭证也必须更新，以保留所有混合云控制功能。	• "在NetApp HCI上为每个节点配置 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" 。 • "在管理节点上更改BMC凭据"。
ESXi凭证 	适用范围：仅限NetApp HCI 管理员可以使用 SSH 或本地 DCUI 和本地 root 帐户登录到 ESXi 主机。在NetApp HCI部署中，用户名是“root”，密码是在NetApp部署引擎中首次安装该计算节点时指定的。 在NetApp HCI部署中，每个NetApp计算节点的 ESXi 根凭据都安全地存储在 mnode 上。 NetApp Hybrid Cloud Control 使用服务帐户的凭据，在计算节点固件升级和运行状况检查期间直接与 ESXi 主机通信。 当 VMware 管理员更改 ESXi 根凭据时，必须在 mnode 上更新相应计算节点的凭据，以保留混合云控制功能。	"更新 vCenter 和 ESXi 主机的凭据"。
QoS集成密码 	适用范围： NetApp HCI和SolidFire中的可选组件 不用于管理员交互式登录。 VMware vSphere 和 Element Software 之间的 QoS 集成通过以下方式实现： • 适用于 vCenter Server 的 Element 插件，以及 • 在 mnode 上提供 QoS 服务。 为了进行身份验证，QoS 服务使用一个仅用于此上下文的密码。QoS 密码是在 vCenter Server 的 Element 插件初始安装期间指定的，或者是在NetApp HCI部署期间自动生成的。 对其他部件无影响。	"更新NetApp Element vCenter Server 插件中的 QoSSIOC 凭据"。 NetApp Element Plug-in for vCenter Server SIOC 密码也称为 *QoSSIOC* 密码。 请查看https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Plug-in_for_vCenter_server/mNode_Status_shows_as_'Network_Down'_or_'Down'_in_the_mNode_Settings_tab_of_the_Element_Plugin_for_vCenter_(VCP)[vCenter Server Element插件知识库文章^]。

凭证类型和图标	管理员使用情况	请参阅这些说明
vCenter Service Appliance 凭据 	适用范围：仅限通过NetApp部署引擎设置的NetApp HCI 。 管理员可以登录到 vCenter Server 设备虚拟机。在NetApp HCI部署中，用户名是“root”，密码是在NetApp部署引擎中首次安装该计算节点时指定的。根据部署的 VMware vSphere 版本，vSphere 单点登录域中的某些管理员也可以登录到该设备。 对其他部件无影响。	无需更改。
NetApp管理节点管理员凭据 	适用范围： NetApp HCI和SolidFire中的可选组件 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，默认情况下未启用通过 SSH 登录。 在NetApp HCI部署中，用户名和密码是由用户在NetApp部署引擎中首次安装该计算节点时指定的。 对其他部件无影响。	无需更改。

查找更多信息

- "更改 Element 软件的默认 SSL 证书"
- "更改节点的 IPMI 密码"
- "启用多重身份验证"
- "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 证书和私钥。

创建NetApp Element软件集群时，该集群会创建一个唯一的自签名安全套接字层 (SSL) 证书和私钥，用于通过 Element UI、每个节点的 UI 或 API 进行的所有 HTTPS 通信。 Element 软件支持自签名证书以及由受信任的证书颁发机构 (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 证书的更多信息并进行更改。

- 获取**SSL**证书

  你可以使用"GetSSLCertificate 方法"检索有关当前已安装的 SSL 证书的信息，包括所有证书详细信息。

- 设置**SSL**证书

  你可以使用"SetSSLCertificate 方法"将集群和每个节点的 SSL 证书设置为您提供的证书和私钥。系统会对证书和私钥进行验证，以防止应用无效证书。

- 移除**SSL**证书

  这"RemoveSSLCertificate 方法"移除当前已安装的 SSL 证书和私钥。然后，集群会生成一个新的自签名证书和私钥。

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

查找更多信息

- "更改管理节点默认 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"
- "NetApp Element vCenter Server 插件"

更改节点的默认 **IPMI** 密码

只要您拥有对节点的远程 IPMI 访问权限，即可更改默认的智能平台管理接口 (IPMI) 管理员密码。如果安装有任何更新，您可能需要执行此操作。

有关配置节点 IPM 访问权限的详细信息，请参阅"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，应立即更改每个存储节点上 IPMI 管理员帐户的默认密码。

你需要什么

您应该为每个存储节点配置 IPMI IP 地址。

步骤

1. 在能够访问 IPMI 网络的计算机上打开网页浏览器，并浏览到节点的 IPMI IP 地址。
2. 请输入用户名 `ADMIN`和密码 `ADMIN`在登录提示符中。
3. 登录后，点击“配置”选项卡。
4. 点击“用户”。
5. 选择 `ADMIN`用户并点击*修改用户*。
6. 选中“更改密码”复选框。
7. 请在“密码”和“确认密码”字段中输入新密码。
8. 点击“修改”，然后点击“确定”。

9. 对其他所有使用默认 IPMI 密码的 H410S 节点重复此过程。

更改 **H610S** 节点的默认 **IPMI** 密码

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

你需要什么

您应该为每个存储节点配置 IPMI IP 地址。

步骤

1. 在能够访问 IPMI 网络的计算机上打开网页浏览器，并浏览到节点的 IPMI IP 地址。
2. 请输入用户名 `root`和密码 `calvin`在登录提示符中。
3. 登录后，点击页面左上角的菜单导航图标，打开侧边栏抽屉。
4. 点击“设置”。
5. 点击“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. 请在“密码”和“确认密码”字段中输入新的、强密码。
9. 点击页面底部的“保存”。
10. 对其他所有使用默认 IPMI 密码的 H610S 节点重复此过程。

查找更多信息

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

使用 **Element** 软件用户界面中的基本选项。

使用 **Element** 软件用户界面中的基本选项。

NetApp Element软件 Web 用户界面 (Element UI) 使您能够监控SolidFire系统并执行常见任务。

基本功能包括查看由用户界面活动激活的 API 命令并提供反馈。

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

了解更多信息

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

API活动

查看 **API** 活动

Element 系统以NetApp Element API 为基础，实现了其特性和功能。 Element UI 使您能够在使用该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 API 活动和后台系统 API 活动，以及您当前正在查看的页面上发出的 API 调用。

您可以使用 API 日志来确定特定任务使用了哪些 API 方法，并了解如何使用 API 方法和对象来构建自定义应用程序。

有关每种方法的详细信息，请参见 "Element Software API 参考"。

1. 在 Element UI 导航栏中，单击“API 日志”。
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”以显示 API 响应流量。
   c. 请选择以下选项之一来筛选 API 流量类型：
      - 用户发起：指您在此 Web UI 会话期间的活动所产生的 API 流量。
      - 后台轮询：由后台系统活动产生的 API 流量。
      - 当前页面：您当前正在查看的页面上的任务所产生的 API 流量。

查找更多信息

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

集群负载会影响接口刷新率。

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

当您在浏览器中重新加载页面时，刷新间隔将重置为默认值。点击页面右上角的集群名称，即可查看当前的刷新间隔。请注意，间隔控制的是 API 请求的频率，而不是服务器返回数据的速度。

当集群负载过重时，它可能会将来自 Element UI 的 API 请求排队。在极少数情况下，当系统响应严重延迟时（例如网络连接缓慢且集群繁忙），如果系统未能及时响应排队的 API 请求，您可能会被从 Element UI 中注销。如果您被重定向到注销屏幕，您可以在忽略任何初始浏览器身份验证提示后再次登录。返回概览页面时，如果您的浏览器未保存集群凭据，系统可能会提示您输入集群凭据。

Element界面中的图标

NetApp Element软件界面会显示图标来表示您可以对系统资源执行的操作。

下表提供了一个快速参考：

图标	描述
	操作
	备份
	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

您可以通过在用户界面中提供的反馈表单来帮助改进 Element 软件的 Web 用户界面并解决任何用户界面问题。

1. 在 Element UI 的任何页面上，单击“反馈”按钮。
2. 请在“摘要”和“描述”字段中输入相关信息。
3. 请附上任何有用的屏幕截图。

4. 请输入姓名和电子邮件地址。
5. 选中此复选框以包含有关您当前环境的数据。
6. 单击“提交”。

查找更多信息

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

管理账户

管理账户

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，会将其分配给特定帐户。您还可以管理SolidFire存储系统的集群管理员帐户。

- "使用 CHAP 处理账户"
- "管理集群管理员用户帐户"

了解更多信息

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

使用 **CHAP** 处理账户

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 (CHAP) 身份验证。创建卷时，会将其分配给特定帐户。

一个账户最多可以分配两千卷，但一卷只能属于一个账户。

CHAP算法

从 Element 12.7 开始，支持符合 FIPS 标准的 CHAP 安全算法 SHA1、SHA-256 和 SHA3-256。当主机 iSCSI 发起程序与 Element iSCSI 目标创建 iSCSI 会话时，它会请求要使用的 CHAP 算法列表。 Element iSCSI 目标从主机 iSCSI 发起程序请求的列表中选择它支持的第一个算法。要确认 Element iSCSI 目标选择最安全的算法，必须配置主机 iSCSI 发起程序发送算法列表，该列表按安全性从高到低排序，例如 SHA3-256 或 SHA1 或 MD5。当主机 iSCSI 发起程序未请求 SHA 算法时，Element iSCSI 目标选择 MD5，假设主机提出的算法列表中包含 MD5。您可能需要更新主机 iSCSI 发起程序配置，以启用对安全算法的支持。

在 Element 12.7 或更高版本升级期间，如果您已将主机 iSCSI 发起程序配置更新为发送包含 SHA 算法列表的会话请求，则在存储节点重启时，新的安全算法将被激活，并且新的或重新连接的 iSCSI 会话将使用最安全的协议建立。升级过程中，所有现有的 iSCSI 会话都将从 MD5 转换为 SHA。如果您不更新主机 iSCSI 发起程序配置以请求 SHA，则现有的 iSCSI 会话将继续使用 MD5。稍后，在您更新主机 iSCSI 发起程序 CHAP 算法之后，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 发起程序具有以下特性：`node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5`该设置被注释掉，导致 iSCSI 发起程序仅使用 MD5。取消主机上此设置的注释并重新启动 iSCSI 发起程序，即可触发该主机上的 iSCSI 会话开始使用 SHA3-256。

如果需要，您可以使用 "列出 ISCSI 会话"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。

系统中的每个账户名称都必须是唯一的。

1. 选择“管理”>“帐户”。
2. 点击“创建账户”。
3. 请输入*用户名*。
4. 在“CHAP 设置”部分，输入以下信息：

   将凭据字段留空，即可自动生成任一密码。

   - CHAP节点会话认证的*发起方密钥*。
   - CHAP节点会话认证的目标密钥。
5. 点击“创建账户”。

查看账户详情

您可以以图形格式查看各个账户的业绩活动。

图表信息提供帐户的 I/O 和吞吐量信息。平均活动水平和峰值活动水平以 10 秒的报告周期为增量显示。这些统计数据包括分配给该帐户的所有交易量的活动。

1. 选择“管理”>“帐户”。
2. 点击帐户的“操作”图标。
3. 单击“查看详细信息”。

以下是一些细节：

- 状态：账户的状态。可能值：
  - 活跃账户：一个活跃的账户。
  - 已锁定：一个已锁定的帐户。
  - 已删除：已被删除并清除的帐户。
- 活动卷数：分配给帐户的活动卷数。
- 压缩率：分配给该帐户的卷的压缩效率得分。
- 重复数据删除：分配给该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评分。
- 整体效率：分配给该账户的业务量的整体效率得分。

编辑帐户

您可以编辑帐户以更改状态、更改 CHAP 密钥或修改帐户名称。

修改帐户中的 CHAP 设置或从访问组中删除发起程序或卷可能会导致发起程序意外失去对卷的访问权限。为验证卷访问不会意外丢失，请务必注销受帐户或访问组更改影响的 iSCSI 会话，并在完成对启动器设置和集群设置的任何更改后，验证启动器是否可以重新连接到卷。

与管理服务关联的持久卷会被分配给在安装或升级期间创建的新帐户。如果您使用的是持久卷，请勿修改或删除其关联的帐户。

1. 选择“管理”>“帐户”。
2. 点击帐户的“操作”图标。
3. 在出现的菜单中，选择“编辑”。
4. 可选： 编辑 用户名。
5. *可选：*单击“状态”下拉列表，然后选择其他状态。

将状态更改为 已锁定 将终止与该帐户的所有 iSCSI 连接，并且该帐户将无法再访问。与该帐户关联的卷已维护；但是，这些卷无法通过 iSCSI 发现。

6. 可选：*在 **CHAP** 设置 下，编辑用于节点会话身份验证的 发起方密钥 和 目标密钥 凭据。

如果您不更改 **CHAP** 设置 凭据，则它们将保持不变。如果将凭据字段留空，系统将生成新密码。

7. 点击“保存更改”。

删除帐户

不再需要账户时，您可以将其删除。

在删除帐户之前，请删除并清除与该帐户关联的所有卷。

与管理服务关联的持久卷会被分配给在安装或升级期间创建的新帐户。如果您使用的是持久卷，请勿修改或删除其关联的帐户。

1. 选择“管理”>“帐户”。
2. 点击要删除的帐户旁边的“操作”图标。
3. 在出现的菜单中，选择“删除”。
4. 确认此操作。

查找更多信息

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

管理集群管理员用户帐户

您可以管理SolidFire存储系统的集群管理员帐户，方法是创建、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 设置以管理系统用户访问权限。

存储集群管理员帐户类型

在运行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。该帐户是集群中具有最高访问权限的主要管理帐户。该账户类似于 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

  您可以授予集群管理员帐户有限的管理权限，使其能够在集群内执行特定任务。分配给每个集群管理员帐户的凭据用于验证存储系统中的 API 和 Element UI 请求。

> 要通过每个节点的 UI 访问集群中的活动节点，需要本地（非 LDAP）集群管理员帐户。访问尚未加入集群的节点不需要账户凭证。

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. 点击“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顺序编号。
   - 用户名：创建集群管理员帐户时赋予该帐户的名称。
   - 访问权限：分配给用户帐户的用户权限。可能值：
     - read
     - reporting
     - 节点
     - 驱动
     - 卷
     - 账户
     - 集群管理员

- administrator
- 支持管理员

> 所有权限均对管理员访问类型可用。
>
> 通过 API 可以访问 Element UI 中没有的某些访问类型。

+

- 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

您可以创建新的集群管理员帐户，并授予其权限以允许或限制对存储系统特定区域的访问。设置集群管理员帐户权限时，系统会授予您未分配给集群管理员的任何权限的只读权限。

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"

之后您可以更改集群管理员帐户的报表、节点、驱动器、卷、帐户和集群级访问权限。启用权限后，系统会为该级别分配写入权限。系统会授予管理员用户只读权限，仅对您未选择的级别有效。

之后您还可以删除系统管理员创建的任何集群管理员用户帐户。您无法删除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. 点击“用户”>“集群管理员”。
   b. 点击“创建集群管理员”。
   c. 选择“集群”用户类型。
   d. 输入账号和密码，并确认密码。
   e. 选择要应用于帐户的用户权限。
   f. 选中此复选框即表示您同意最终用户许可协议。
   g. 点击“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. 点击“集群”>“LDAP”。
   b. 请确保已启用 LDAP 身份验证。
   c. 点击“测试用户身份验证”，复制显示的用户或用户所属组之一的专有名称，以便稍后粘贴。

d. 点击“用户”>“集群管理员”。
e. 点击“创建集群管理员”。
f. 选择 LDAP 用户类型。
g. 在“专有名称”字段中，按照文本框中的示例输入用户或组的完整专有名称。或者，从你之前复制的专有名称中粘贴。

   如果专有名称属于某个组，则 LDAP 服务器上该组的任何成员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，用户名的通用格式为“`LDAP:<完整可分辨名称>`”。

a. 选择要应用于帐户的用户权限。
b. 选中此复选框即表示您同意最终用户许可协议。
c. 点击“创建集群管理员”。

编辑集群管理员权限

您可以更改集群管理员帐户的报表、节点、驱动器、卷、帐户和集群级访问权限。启用权限后，系统会为该级别分配写入权限。系统会授予管理员用户只读权限，仅对您未选择的级别有效。

1. 点击“用户”>“集群管理员”。
2. 单击要编辑的集群管理员旁边的“操作”图标。
3. 单击“编辑”。
4. 选择要应用于帐户的用户权限。
5. 点击“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. 点击“用户”>“集群管理员”。
2. 单击要编辑的集群管理员旁边的“操作”图标。
3. 单击“编辑”。
4. 在“更改密码”字段中，输入新密码并确认。
5. 点击“保存更改”。

相关信息

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

管理 LDAP

您可以设置轻量级目录访问协议 (LDAP)，以启用对SolidFire存储的安全、基于目录的登录功能。您可以在集群级别配置 LDAP，并授权 LDAP 用户和组。

管理 LDAP 包括使用现有的 Microsoft Active Directory 环境为SolidFire集群设置 LDAP 身份验证，并测试配置。

你可以同时使用 IPv4 地址和 IPv6 地址。

启用 LDAP 涉及以下几个主要步骤，详细描述如下：

1. 完成 **LDAP** 支持的预配置步骤。请确认您已具备配置 LDAP 身份验证所需的所有详细信息。
2. 启用**LDAP**身份验证。可以使用 Element UI 或 Element API。
3. 验证 **LDAP** 配置。 （可选）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）。可以通过运行 `TestLdapAuthentication API` 方法或使用 `Element UI` 来测试 `LDAP` 配置是否正确。对于本次初始测试，请使用用户名“`sAMAccountName”。 `readonly`用户。这将验证您的集群是否已正确配置 LDAP 身份验证，并验证…… `readonly`凭证和访问权限均正确。如果此步骤失败，请重复步骤 1 至 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步骤 4。复制 `distinguished`名称（DN）或用户（或组）。此 DN 将在步骤 6 中使用。
6. 添加 **LDAP** 集群管理员（从“测试 LDAP 身份验证”步骤复制并粘贴 DN）。使用 Element UI 或 AddLdapClusterAdmin API 方法，创建一个具有适当访问级别的新集群管理员用户。用户名部分，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集群。如果您添加了 LDAP 组，则可以以该组中的任何用户身份登录。

完成 **LDAP** 支持所需的所有预配置步骤

在 Element 中启用 LDAP 支持之前，您应该设置 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. 创建用户和用户组。
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。这使得 LDAP 管理员能够集中管理用户对存储系统的访问权限。

您可以使用 Element 用户界面或 Element API 配置 LDAP。本流程介绍如何使用 Element UI 配置 LDAP。

本示例展示了如何在SolidFire上配置 LDAP 身份验证，它使用 `SearchAndBind`作为身份验证类型。该示例使用单个 Windows Server 2012 R2 Active Directory 服务器。

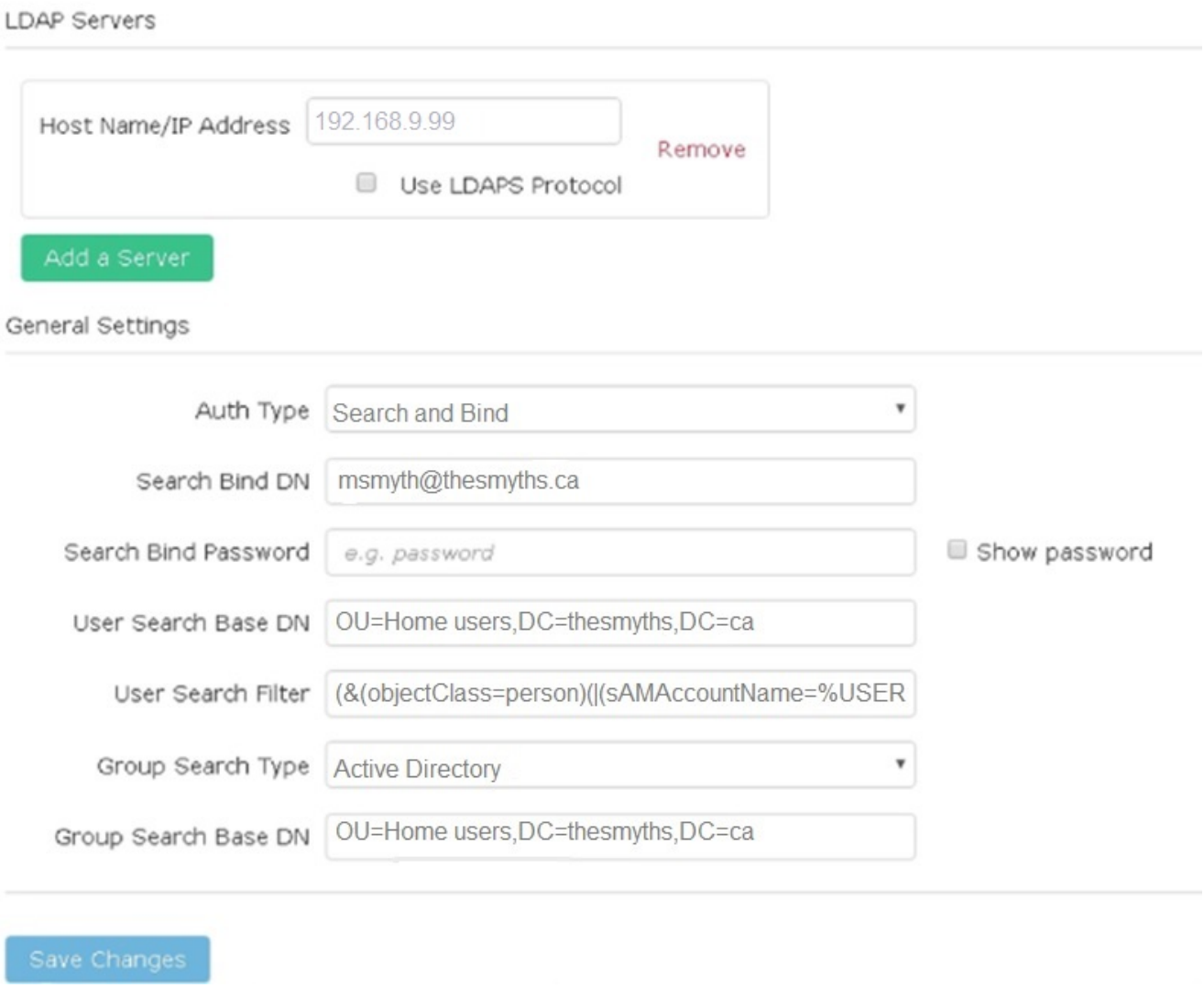
步骤

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

   也可以选择输入自定义端口号。

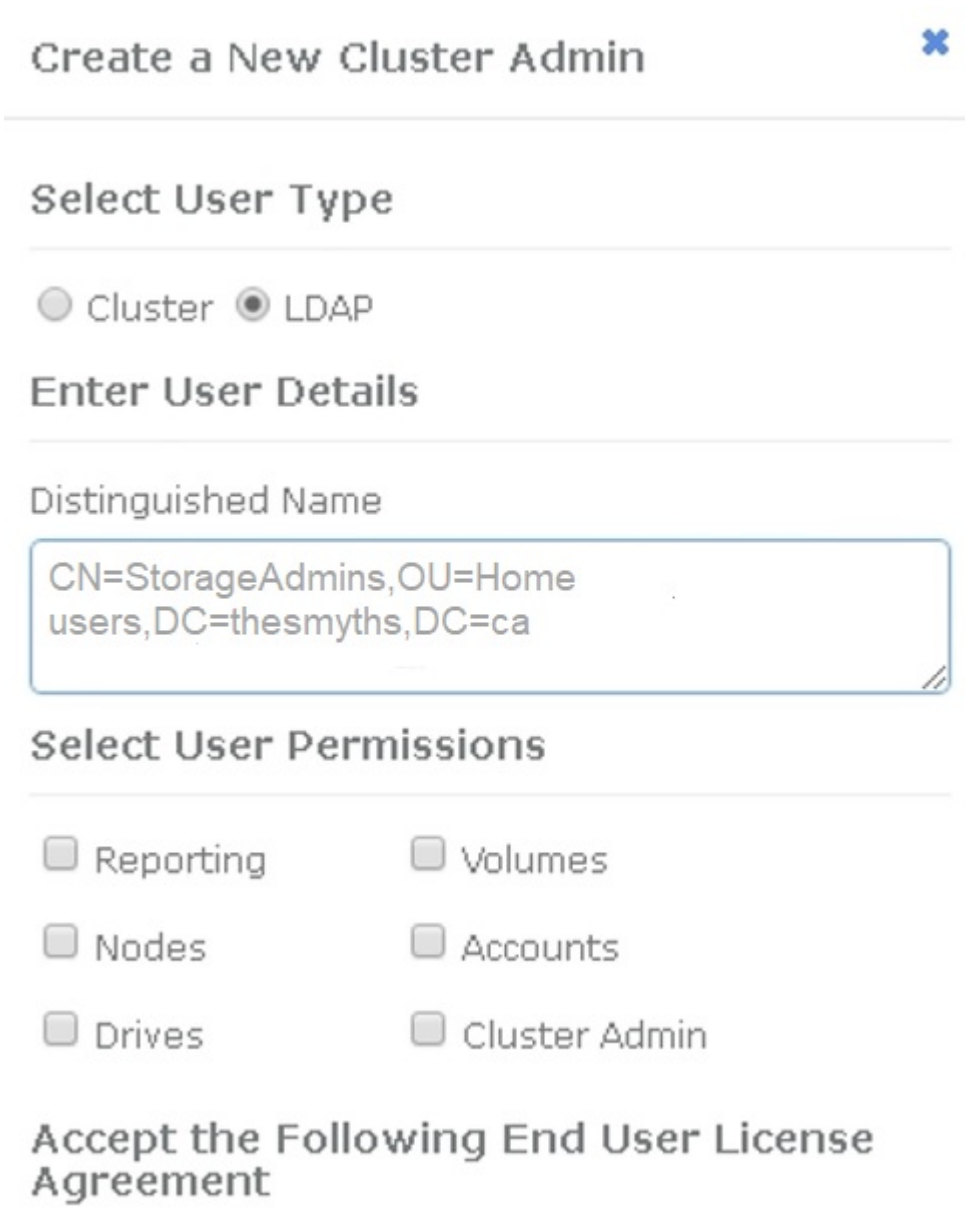
   例如，要添加自定义端口号，请输入<主机名或 IP 地址>:<端口号>

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



7. 点击“启用 LDAP”。
8. 如果要测试用户的服务器访问权限，请点击“测试用户身份验证”。
9. 复制显示的专有名称和用户组信息，以便稍后在创建集群管理员时使用。

10. 点击“保存更改”以保存所有新设置。
11. 要在此组中创建用户以便任何人都可以登录，请完成以下步骤：
    a. 点击“用户”>“查看”。



    b. 对于新用户，请在“用户类型”中选择“**LDAP**”，并将复制的组粘贴到“专有名称”字段中。
    c. 选择权限，通常是所有权限。
    d. 向下滚动至最终用户许可协议，然后点击“我接受”。
    e. 点击“创建集群管理员”。

    现在您拥有一个具有 Active Directory 组值的用户。

为了测试这一点，请从 Element UI 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。这使得 LDAP 管理员能够集中管理用户对存储系统的访问权限。

您可以使用 Element 用户界面或 Element API 配置 LDAP。本流程描述了如何使用 Element API 配置 LDAP。

要在SolidFire集群上使用 LDAP 身份验证，首先需要使用以下命令在集群上启用 LDAP 身份验证：`EnableLdapAuthentication` API 方法。

步骤

1. 首先在集群上启用 LDAP 身份验证，使用以下命令： `EnableLdapAuthentication` API 方法。
2. 请输入所需信息。

```
{
     "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	描述
authType: SearchAndBind	指示集群将使用只读服务帐户首先搜索正在接受身份验证的用户，如果找到并已通过身份验证，则绑定该用户。
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	指定在 LDAP 树中开始搜索组的位置。在这个例子中，我们使用了树的根节点。如果您的 LDAP 树非常大，您可能需要将其设置为更细粒度的子树，以减少搜索时间。

使用的参数	描述
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	指定在 LDAP 树中开始搜索用户的位置。在这个例子中，我们使用了树的根节点。如果您的 LDAP 树非常大，您可能需要将其设置为更细粒度的子树，以减少搜索时间。
groupSearchType: Active Directory	使用 Windows Active Directory 服务器作为 LDAP 服务器。

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
要使用用户主体名称（登录邮箱地址），您可以将用户搜索筛选器更改为：
 	
`"(&(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%)))" ----

使用 sAMAccountName 作为登录SolidFire集群的用户名。这些设置告诉 LDAP 在 sAMAccountName 属性中搜索登录期间指定的用户名，并将搜索范围限制为 objectClass 属性值为“person”的条目。	搜索绑定DN
这是用于搜索 LDAP 目录的只读用户的专有名称。对于活动目录，通常最简单的方法是使用用户主体名称（电子邮件地址格式）。	搜索绑定密码

为了测试这一点，请从 Element UI 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“集群”选项卡的 LDAP 页面上查看 LDAP 信息。

您必须启用 LDAP 才能查看这些 LDAP 配置设置。

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
  - 搜索和绑定
- 搜索绑定 **DN**：用于登录以执行 LDAP 用户搜索的完整 DN（需要对 LDAP 目录具有绑定级访问权限）。
- 搜索绑定密码：用于验证对 LDAP 服务器访问权限的密码。
- 用户搜索基准 **DN**：用于启动用户搜索的树的基准 DN。系统从指定位置开始搜索子树。
- 用户搜索筛选条件：请使用您的域名输入以下内容：

```
(&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
```

- 群组搜索类型：控制使用的默认群组搜索筛选器的搜索类型。可能值：
  - Active Directory：用户所有 LDAP 组的嵌套成员关系。
  - 无群组：不提供群组支持。
  - 成员 DN：成员 DN 风格的组（单级）。
- 组搜索基本 **DN**：用于启动组搜索的树的基本 DN。系统从指定位置开始搜索子树。
- 测试用户身份验证：LDAP 配置完成后，使用此功能测试 LDAP 服务器的用户名和密码身份验证。输入一个已存在的帐户进行测试。此处会显示专有名称和用户组信息，您可以复制这些信息以备日后创建集群管理员时使用。

测试 **LDAP** 配置

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

步骤

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

错误消息	描述
`xLDAPUserNotFound`	• 在已配置的数据库中找不到被测试用户。 `userSearchBaseDN`子树。 • 这 `userSearchFilter`配置错误。
`xLDAPBindFailed (Error: Invalid credentials)`	• 被测试的用户名是有效的 LDAP 用户，但提供的密码不正确。 • 被测试的用户名是有效的 LDAP 用户，但该帐户当前已被禁用。

错误消息	描述
`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错误。
`xLDAPSearchFailed (Error: No such object)`	这 `userSearchBaseDN`在 LDAP 树中不是有效位置。
`xLDAPSearchFailed (Error: Referral)`	• 这 `userSearchBaseDN`在 LDAP 树中不是有效位置。 • 这 `userSearchBaseDN`和 `groupSearchBaseDN`位于嵌套的组织单元中。这可能会导致权限问题。解决方法是将组织单元 (OU) 包含在用户和组的基本 DN 条目中（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，则结果包括指定用户的专有名称和用户所属的组列表。

```
{
"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，您应该记下所有配置设置，因为禁用 LDAP 会清除所有设置。

步骤

1. 点击“集群”>“LDAP”。
2. 点击“否”。
3. 点击“禁用 LDAP”。

查找更多信息

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

管理您的系统

管理您的系统

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

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

了解更多信息

- "SolidFire和 Element 软件文档"

- "NetApp Element vCenter Server 插件"

启用多重身份验证

设置多重身份验证

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

您可以使用 Element API 的以下基本步骤来设置集群以使用多因素身份验证。

每个 API 方法的详细信息可以在以下位置找到： "元素 API 参考"。

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

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

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

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

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

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

   - email=bob@company.com — 其中 IdP 配置为在 SAML 属性中发布电子邮件地址。
   - group=cluster-administrator - 其中 IdP 配置为释放一个组属性，所有用户都应该有权访问该组属性。请注意，出于安全考虑，SAML 属性名称/值对区分大小写。
5. 通过调用以下 API 方法为集群启用 MFA： `EnableIdpAuthentication`

查找更多信息

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

多因素身份验证的补充信息

关于多因素身份验证，您应该注意以下注意事项。

- 要刷新不再有效的身份提供商 (IdP) 证书，您需要使用非身份提供商管理员用户调用以下 API 方法：

`UpdateIdpConfiguration`

- MFA 与长度小于 2048 位的证书不兼容。默认情况下，集群上会创建一个 2048 位 SSL 证书。调用 API 方法时，应避免设置较小的证书： `SetSSLCertificate`

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

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

查找更多信息

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

配置集群设置

启用和禁用集群的静态数据加密

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

您可以使用 Element UI 或 API 启用静态硬件加密。启用静态数据硬件加密功能不会影响集群的性能或效率。您只能使用 Element API 启用静态软件加密。

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

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

你需要什么

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

检查静态加密状态

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

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

选项

- [启用基于硬件的静态数据加密]

- [启用静态数据软件加密]
- [禁用静态数据的硬件加密]

启用基于硬件的静态数据加密

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

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

启用静态数据软件加密

软件静态加密在集群上启用后无法禁用。

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

禁用静态数据的硬件加密

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

查找更多信息

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

设置集群满阈值

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

你需要什么

您必须拥有集群管理员权限。

步骤

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

查找更多信息

"元素的块空间阈值是如何计算的"

启用和禁用卷负载均衡

从 Element 12.8 开始，您可以使用卷负载均衡，根据每个卷的实际 IOPS 而不是 QoS 策略中配置的最小 IOPS，在节点之间平衡卷。您可以使用 Element UI 或 API 启用和禁用卷负载均衡（默认情况下处于禁用状态）。

步骤

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

   启用卷负载均衡

   选择“启用基于实际 IOPS 的负载均衡”，并确认您的选择。

   禁用卷负载均衡：

   选择“禁用基于实际 IOPS 的负载均衡”，并确认您的选择。

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

查找更多信息

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

启用和禁用支持访问

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

您必须拥有集群管理员权限才能更改支持访问权限。

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

管理使用条款横幅

您可以启用、编辑或配置包含用户消息的横幅。

选项

[启用“使用条款”横幅] [编辑使用条款横幅] [禁用“使用条款”横幅]

启用“使用条款”横幅

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

您必须拥有集群管理员权限才能启用使用条款功能。

1. 点击“用户”>“使用条款”。
2. 在“使用条款”表单中，输入要在“使用条款”对话框中显示的文本。

   请勿超过 4096 个字符。

3. 单击“启用”。

编辑使用条款横幅

您可以编辑用户选择“使用条款”登录横幅时看到的文本。

你需要什么

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

步骤

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

   请勿超过 4096 个字符。

3. 点击“保存更改”。

禁用“使用条款”横幅

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

你需要什么

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

步骤

1. 点击“用户”>“使用条款”。
2. 单击“禁用”。

设置网络时间协议

配置集群要查询的网络时间协议服务器

您可以指示集群中的每个节点向网络时间协议 (NTP) 服务器查询更新。集群仅联系已配置

的服务器，并向这些服务器请求 NTP 信息。

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

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

使用 FQDN 取决于各个存储节点的 DNS 设置是否已就位并正常运行。为此，请在每个存储节点上配置 DNS 服务器，并通过查看“网络端口要求”页面确保端口已打开。

您最多可以输入五个不同的 NTP 服务器。

你可以同时使用 IPv4 地址和 IPv6 地址。

你需要什么

您必须拥有集群管理员权限才能配置此设置。

步骤

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

查找更多信息

- "配置集群监听 NTP 广播。"
- "SolidFire和 Element 软件文档"
- "NetApp Element vCenter Server 插件"

配置集群监听 **NTP** 广播。

通过使用广播模式，您可以指示集群中的每个节点在网络上监听来自特定服务器的网络时间协议 (NTP) 广播消息。

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

你需要什么

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

步骤

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

4. 要设置广播客户端，请在“服务器”字段中输入您在广播模式下配置的 NTP 服务器。
5. 点击“保存更改”。

查找更多信息

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

管理 SNMP

了解 SNMP

您可以在集群中配置简单网络管理协议 (SNMP)。

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

ⓘ 你可以同时使用 IPv4 地址和 IPv6 地址。

SNMP 详细信息

在集群选项卡的 SNMP 页面上，您可以查看以下信息。

- **SNMP MIB**

  您可以查看或下载的 MIB 文件。

- 常规**SNMP**设置

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

- **SNMP**陷阱设置

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

配置 SNMP 请求器

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

1. 点击菜单：集群[SNMP]。
2. 在“常规 SNMP 设置”下，单击“是”以启用 SNMP。
3. 从“版本”列表中选择“版本 2”。
4. 在“请求者”部分，输入“社区字符串”和“网络”信息。

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

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

查找更多信息

- 配置SNMP陷阱
- 使用管理信息库文件查看托管对象数据

配置 **SNMP USM** 用户

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

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

配置**SNMP**陷阱

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

启用 SNMP 陷阱后， SolidFire集群会生成与事件日志条目和系统警报关联的陷阱。要接收 SNMP 通知，您需要选择要生成的陷阱并确定陷阱信息的接收者。默认情况下，不会生成任何陷阱。

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

使用管理信息库文件查看托管对象数据

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

MIB中提供的统计数据显示了以下系统活动：

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

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

步骤

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

管理驱动器

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

驱动细节

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

首次初始化集群时，活动驱动器列表为空。创建新的SolidFire集群后，您可以添加未分配给集群且列在“可用”选项卡中的驱动器。

活动驱动器列表中包含以下元素。

- 驱动器 **ID**

  分配给硬盘的顺序编号。

- 节点 **ID**

  节点添加到集群时分配的节点编号。

- 节点名称

  存放驱动器的节点的名称。

- 投币口

  硬盘实际所在的插槽编号。

- 容量

  硬盘容量，单位为 GB。

- 序列号

  硬盘的序列号。

- 剩余磨损量

  磨损程度指示器。

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

- 类型

  驱动类型。类型可以是块或元数据。

了解更多信息

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

管理节点

管理节点

您可以从集群选项卡的“节点”页面管理SolidFire存储和光纤通道节点。

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

查找更多信息

向集群添加节点

向集群添加节点

当需要更多存储空间时，或者在创建集群之后，您可以向集群添加节点。节点首次上电时需要进行初始配置。节点配置完成后，它将出现在待处理节点列表中，您可以将其添加到集群中。

集群中每个节点上的软件版本必须兼容。向集群添加节点时，集群会根据需要在新节点上安装集群版本的NetApp Element软件。

您可以向现有集群添加容量较小或较大的节点。您可以向集群添加更大容量的节点，以满足容量增长的需求。向包含较小节点的集群中添加较大节点时，必须成对添加。这样就为 Double Helix 留出了足够的空间，以便在较大的节点之一发生故障时能够转移数据。您可以向较大的节点集群中添加较小的节点容量，以提高性能。

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

"NetApp视频：按需扩展：扩展SolidFire集群"

您可以向NetApp HCI设备添加节点。

步骤

1. 选择“集群”>“节点”。
2. 点击“待处理”查看待处理节点列表。

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

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

3. 执行以下操作之一：
   - 要添加单个节点，请单击要添加的节点旁边的“操作”图标。
   - 要添加多个节点，请选中要添加的节点的复选框，然后选择“批量操作”。 *注意：*如果您添加的节点的 Element 软件版本与集群上运行的版本不同，则集群会异步地将该节点更新为集群主节点上运行的 Element 软件版本。节点更新后，会自动添加到集群中。在此异步过程中，节点将处于 pendingActive 状态。
4. 单击“添加”。

   该节点出现在活动节点列表中。

查找更多信息

Node 版本控制和兼容性

Node 版本控制和兼容性

节点兼容性取决于节点上安装的 Element 软件版本。如果节点和集群的版本不兼容，Element 软件存储集群会自动将节点镜像到集群上的 Element 软件版本。

以下列表描述了构成 Element 软件版本号的软件版本重要性级别：

- 主要的

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

- 次要的

  第二个数字表示添加到主要版本中的较小软件功能或对现有软件功能的增强。该组件在主版本组件内递增，

表示此增量版本与任何其他具有不同次组件的 Element 软件增量版本都不兼容。例如，11.0 与 11.1 不兼容，11.1 与 11.2 也不兼容。

- 微

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

主版本号和次版本号必须匹配才能兼容。微型计算机的编号不必完全匹配即可兼容。

混合节点环境下的集群容量

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

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

最好不要将未加密节点和加密节点混用。在混合节点集群中，任何节点的容量都不能超过集群总容量的 33%。例如，在一个包含四个 SF 系列 4805 节点的集群中，可以单独添加的最大节点是 SF 系列 9605。集群容量阈值是根据此情况下最大节点可能发生的损失来计算的。

根据您的 Element 软件版本，以下 SF 系列存储节点不受支持：

从.....开始	不支持存储节点...
元素 12.8	• SF4805 • SF9605 • SF19210 • SF38410
元素 12.7	• SF2405 • SF9608
元素 12.0	• SF3010 • SF6010 • SF9010

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

查看节点详情

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

步骤

1. 点击“集群”>“节点”。
2. 要查看特定节点的详细信息，请单击节点的“操作”图标。
3. 单击“查看详细信息”。
4. 查看节点详细信息：
   - 节点 **ID**：系统生成的节点 ID。
   - 节点名称：节点的主机名。
   - 节点角色：节点在集群中所扮演的角色。可能值：
     - 集群主节点：执行集群范围管理任务的节点，包含 MVIP 和 SVIP。
     - 集成节点：参与集群的节点。根据集群大小，集成节点的数量为 3 个或 5 个。
     - 光纤通道：集群中的一个节点。
   - 节点类型：节点的模型类型。
   - 活动硬盘：节点中活动硬盘的数量。
   - 节点利用率：基于节点热度的节点利用率百分比。显示的值是 recentPrimaryTotalHeat 的百分比。从 Element 12.8 版本开始可用。
   - 管理 **IP**：分配给节点的用于 1GbE 或 10GbE 网络管理任务的管理 IP (MIP) 地址。
   - 集群 **IP**：分配给节点的集群 IP (CIP) 地址，用于同一集群中节点之间的通信。
   - 存储 **IP**：分配给节点的存储 IP (SIP) 地址，用于 iSCSI 网络发现和所有数据网络流量。
   - 管理 **VLAN ID**：管理局域网的虚拟 ID。
   - 存储 **VLAN ID**：存储局域网的虚拟 ID。
   - 版本：每个节点上运行的软件版本。
   - 复制端口：节点上用于远程复制的端口。
   - 服务标签：分配给节点的唯一服务标签编号。
   - 自定义保护域：分配给节点的自定义保护域。

查看光纤通道端口详情

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

查看连接到集群的光纤通道端口的相关信息。

步骤

1. 点击“集群”>“FC端口”。
2. 要筛选此页面上的信息，请点击“筛选”。
3. 请查看详细信息：
   - 节点 **ID**：承载连接会话的节点。
   - 节点名称：系统生成的节点名称。
   - 插槽：光纤通道端口所在的插槽编号。

- **HBA** 端口：光纤通道主机总线适配器 (HBA) 上的物理端口。
- **WWNN**：全球节点名称。
- **WWPN**：目标全球端口名称。
- 交换机 **WWN**：光纤通道交换机的全球通用名称。
- 端口状态：端口的当前状态。
- **nPort ID**：光纤通道架构上的节点端口 ID。
- 速度：协商的光纤通道速度。可能的值如下：
  - 4Gbps
  - 8Gbps
  - 16Gbps

查找更多信息

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

管理虚拟网络

管理虚拟网络

SolidFire存储中的虚拟网络允许将位于不同逻辑网络上的多个客户端之间的流量连接到一个集群。使用 VLAN 标记可以在网络堆栈中隔离与集群的连接。

查找更多信息

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

添加虚拟网络

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

你需要什么

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

对于此配置，您必须考虑以下标准：

- 未启用 VRF 的 VLAN 要求发起方与 SVIP 位于同一子网中。

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

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

步骤

1. 点击“集群”>“网络”。
2. 点击“创建VLAN”。
3. 在“创建新 VLAN”对话框中，在以下字段中输入值：
    - **VLAN**名称
    - **VLAN**标签
    - **SVIP**
    - **Netmask**
    - （可选）描述
4. 输入 **IP** 地址块 中 IP 地址范围的 起始 **IP** 地址。
5. 输入 IP 地址范围的*大小*，即要包含在地址块中的 IP 地址数量。
6. 点击“添加块”为该 VLAN 添加一个非连续的 IP 地址块。
7. 点击“创建VLAN”。

查看虚拟网络详情

步骤

1. 点击“集群”>“网络”。
2. 查看详细信息。
    - **ID**：VLAN 网络的唯一 ID，由系统分配。
    - 名称：VLAN 网络的唯一用户指定名称。
    - **VLAN** 标签：创建虚拟网络时分配的 VLAN 标签。
    - **SVIP**：分配给虚拟网络的存储虚拟 IP 地址。
    - 子网掩码：此虚拟网络的子网掩码。
    - 网关：虚拟网络网关的唯一IP地址。必须启用 VRF。
    - **VRF** 已启用：指示虚拟路由和转发是否已启用。
    - 使用的**IP**地址：用于虚拟网络的虚拟网络IP地址范围。

启用虚拟路由和转发

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

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

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

查找更多信息

添加虚拟网络

编辑虚拟网络

您可以更改 VLAN 属性，例如 VLAN 名称、子网掩码和 IP 地址块大小。 VLAN 的 VLAN 标签和 SVIP 不能修改。对于非 VRF VLAN，网关属性不是有效参数。

如果存在任何 iSCSI、远程复制或其他网络会话，则修改可能会失败。

管理 VLAN IP 地址范围大小时，应注意以下限制：

- 您只能从创建 VLAN 时分配的初始 IP 地址范围内删除 IP 地址。
- 您可以删除在初始 IP 地址范围之后添加的 IP 地址块，但不能通过删除 IP 地址来调整 IP 地址块的大小。
- 当您尝试从初始 IP 地址范围或 IP 地址块中删除集群中节点正在使用的 IP 地址时，操作可能会失败。
- 您无法将特定正在使用的 IP 地址重新分配给集群中的其他节点。

您可以使用以下步骤添加 IP 地址块：

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

故障排除知识库文章链接

链接到知识库文章，以获取有关管理 VLAN IP 地址范围的故障排除帮助。

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

编辑 **VRF VLAN**

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

1. 点击“集群”>“网络”。
2. 单击要编辑的 VLAN 的“操作”图标。
3. 单击“编辑”。
4. 在“编辑 VLAN”对话框中输入 VRF VLAN 的新属性。
5. 点击“保存更改”。

删除虚拟网络

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

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

查找更多信息

编辑虚拟网络

创建支持 **FIPS** 驱动器的集群

为 **FIPS** 驱动器功能准备元素集群

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

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

集群被视为符合 FIPS 标准的驱动器，需满足以下条件：

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

启用静态数据加密

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

驱动器，必须启用静态加密。

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

查找更多信息

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

确定节点是否已准备好使用 **FIPS** 驱动器功能

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

生成的报告显示以下状态之一：

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

步骤

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

   ```
   GetFipsReport
   ```

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

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

查找更多信息

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

启用 **FIPS** 驱动器功能

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

集群上必须启用静态数据加密，并且所有节点和驱动器都必须具备 FIPS 功能，当 GetFipsReport 对所有节点显

示“就绪”状态时，即可表明这一点。

步骤

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

```
EnableFeature params: FipsDrives
```

查找更多信息

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

检查 **FIPS** 驱动器状态

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

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

```
GetFeatureStatus
```

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

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

查找更多信息

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

排查 **FIPS** 驱动器功能故障

使用NetApp Element软件用户界面，您可以查看与 FIPS 驱动器功能相关的系统集群故障或错误信息的警报。

1. 使用 Element UI，选择“报告”>“警报”。
2. 查找集群故障，包括：
   - FIPS驱动程序不匹配
   - FIPS 导致不合规
3. 有关解决方法建议，请参阅集群故障代码信息。

查找更多信息

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

建立安全通信

在您的集群上启用 **HTTPS** 的 **FIPS 140-2** 标准

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

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

> ⓘ 启用 FIPS 140-2 模式后，无法禁用。启用 FIPS 140-2 模式后，集群中的每个节点都会重新启动并运行自检，以确保 NCSM 已正确启用并在 FIPS 140-2 认证模式下运行。这会导致集群上的管理连接和存储连接中断。您应该仔细规划，只有当您的环境需要它提供的加密机制时才启用此模式。

更多信息请参阅 Element API 信息。

以下是启用 FIPS 的 API 请求示例：

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

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

查找更多信息

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

SSL密码

SSL 密码是主机用来建立安全通信的加密算法。 Element 软件支持标准密码，启用 FIPS

140-2 模式时还支持非标准密码。

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

- **FIPS 140-2** 已禁用

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（dh 2048）-A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（dh 2048）-A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

  TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

  TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C

  TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

- 符合**FIPS 140-2**标准

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（dh 2048）-A

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（dh 2048）-A

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (sect571r1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (sect571r1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

查找更多信息

在您的集群上启用 HTTPS 的 FIPS 140-2 标准

开始使用外部密钥管理

开始使用外部密钥管理

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

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

查找更多信息

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

设置外部密钥管理

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

你需要什么

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

步骤

1. 与外部密钥服务器（EKS）建立信任关系。
   a. 为 Element 集群创建公钥/私钥对，通过调用以下 API 方法与密钥服务器建立信任关系："创建公钥/私钥对"
   b. 获取证书颁发机构需要签署的证书签名请求（CSR）。 CSR 使密钥服务器能够验证将要访问密钥的 Element 集群是否已通过 Element 集群的身份验证。调用以下 API 方法："获取客户端证书签名请求"
   c. 使用 EKS/证书颁发机构对检索到的 CSR 进行签名。更多信息请参阅第三方文档。
2. 在集群上创建服务器和提供程序，以便与 EKS 通信。密钥提供者定义密钥的获取地点，服务器定义要与之通信的 EKS 的具体属性。
   a. 通过调用以下 API 方法创建密钥提供程序，密钥服务器详细信息将存放于此："创建密钥提供程序Kmip"
   b. 通过调用以下 API 方法，创建提供证书颁发机构的签名证书和公钥证书的密钥服务器："创建密钥服务器Kmip" "测试密钥服务器Kmip"

      如果测试失败，请检查服务器连接和配置。然后重复测试。

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

      如果测试失败，请检查服务器连接和配置。然后重复测试。

3. 接下来，请执行以下操作之一，以实现静态数据加密：
   a. （用于静态数据硬件加密）启用"静态硬件加密"通过调用以下方法提供包含用于存储密钥的密钥服务器的密钥提供程序的 ID："启用静态加密" API 方法。

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

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

查找更多信息

- "启用和禁用集群加密"

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

重新密钥软件加密静态主密钥

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

您可能需要在以下某个过程中重新输入密码：

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

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

你需要什么

- 您已启用静态软件加密。"CreateCluster"在不包含卷且没有 I/O 的新集群上执行此方法。使用链接：../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`确认该州是 `enabled`在继续之前。
- 你有"建立了信任关系"SolidFire集群与外部密钥服务器 (EKS) 之间。运行"测试密钥提供程序Kmip"验证与密钥提供程序的连接是否已建立的方法。

步骤

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

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

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

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. 运行 `GetSoftwareEncryptionatRestInfo`命令确认新的关键细节，包括 `keyProviderID`已更新。

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

查找更多信息

- "使用 Element API 管理存储"

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

恢复无法访问或无效的身份验证密钥

偶尔会出现需要用户干预的错误。如果发生错误，将会生成集群故障（称为集群故障代码）。这里描述了两种最可能的情况。

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

当集群首次启动且密钥服务器无法访问或所需密钥不可用时，可能会发生这种情况。

1. 请按照集群故障代码（如有）中的恢复步骤进行操作。

可能会设置 **sliceServiceUnhealthy** 故障，因为元数据驱动器已被标记为故障并置于“可用”状态。

清除步骤：

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

看"集群故障代码"了解更多信息。

外部密钥管理 **API** 命令

EKM管理和配置可用API列表。

用于在集群和外部客户拥有的服务器之间建立信任关系：

- 创建公钥/私钥对
- 获取客户端证书签名请求

用于定义外部客户自有服务器的具体细节：

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

用于创建和维护管理外部密钥服务器的密钥提供程序：

- 创建密钥提供程序Kmip
- 删除密钥提供程序Kmip
- AddKeyServerToProviderKmip

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

有关 API 方法的信息，请参阅 "API 参考信息"。

管理卷和虚拟卷

了解如何管理卷和虚拟卷

您可以通过 Element UI 中的“管理”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、发起程序和服务质量 (QoS) 策略。

使用卷

SolidFire系统使用卷来配置存储。卷是可通过网络由 iSCSI 或光纤通道客户端访问的块设备。在“管理”选项卡的“卷”页面上，您可以创建、修改、克隆和删除节点上的卷。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的存储容器、协议端点、绑定和主机的信息并执行相关任务。

NetApp Element软件存储系统出厂时默认禁用虚拟卷 (VVols) 功能。您必须通过 Element UI 手动启用 vSphere VVol 功能，此操作为一次性任务。

启用 VVol 功能后，用户界面中会出现一个 VVols 选项卡，提供与 VVols 相关的监控和有限的管理选项。此外，一个名为 VASA Provider 的存储端软件组件充当 vSphere 的存储感知服务。大多数 VVols 命令（例如 VVol 创建、克隆和编辑）由 vCenter Server 或 ESXi 主机发起，并由 VASA Provider 转换为 Element 软件存储系统的 Element API。可以使用 Element UI 发起创建、删除和管理存储容器以及删除虚拟卷的命令。

使用 Element 软件存储系统的虚拟卷功能所需的大部分配置都在 vSphere 中完成。请参阅《VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide》以在 vCenter 中注册 VASA Provider、创建和管理 VVol 数据存储以及根据策略管理存储。

对于 Element 12.5 及更早版本，请勿向单个 vCenter 实例注册多个NetApp Element VASA 提供程序。如果添加了第二个NetApp Element VASA 提供程序，则所有 VVOL 数据存储都将无法访问。

如果您已将 VASA 提供商注册到 vCenter，则可通过升级补丁获得对多个 vCenter 的 VASA 支持。要安装，请从以下位置下载 VASA39 .tar.gz 文件： "NetApp软件下载"前往现场并按照清单上的说明进行操作。 NetApp Element VASA 提供程序使用NetApp证书。通过此补丁，vCenter 可以直接使用未经修改的证书，以支持多个 vCenter 用于 VASA 和 VVols。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"

与批量访问组和发起者合作

您可以使用 iSCSI 发起程序或光纤通道发起程序来访问卷访问组中定义的卷。

您可以通过映射卷集合中的 iSCSI 发起程序 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认证方法有两种类型：

- 账户级 CHAP 认证：您可以为账户分配 CHAP 认证。
- 发起方级 CHAP 身份验证：您可以为特定发起方分配唯一的 CHAP 目标和密钥，而无需在单个帐户中绑定到单个 CHAP。这种发起方级别的 CHAP 身份验证取代了帐户级别的凭据。

（可选）使用每个发起方的 CHAP，您可以强制执行发起方授权和每个发起方的 CHAP 身份验证。这些选项可以根据每个发起者进行定义，一个访问组可以包含具有不同选项的多个发起者。

将每个 WWPN 添加到访问组即可启用对访问组中卷的光纤通道网络访问。

卷访问组具有以下限制：

- 一个访问组中最多允许有 64 个 IQN 或 WWPN。
- 一个访问组最多可以包含 2000 卷。
- 一个 IQN 或 WWPN 只能属于一个访问组。
- 一个卷册最多可以属于四个访问组。

"了解如何与批量访问组和发起者合作"

了解更多信息

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

使用卷

管理服务质量政策

服务质量 (QoS) 策略允许您创建和保存可应用于多个卷的标准化服务质量设置。您可以在“管理”选项卡的“QoS 策略”页面中创建、编辑和删除 QoS 策略。

如果您正在使用 QoS 策略，请不要在卷上使用自定义 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"

看"服务性能和质量"。

- 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，并在创建卷时应用这些策略。

1. 选择“管理”>“QoS策略”。
2. 点击“创建QoS策略”。
3. 请输入*保单名称*。
4. 输入最小 **IOPS**、最大 **IOPS** 和 突发 **IOPS** 值。
5. 点击“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 策略会影响与该策略关联的所有卷。

1. 选择“管理”>“QoS策略”。
2. 单击要编辑的 QoS 策略的“操作”图标。
3. 在出现的菜单中，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：
    - 策略名称
    - 最小 IOPS
    - 最大 IOPS
    - 突发 IOPS
5. 点击“保存更改”。

删除 **QoS** 策略

如果不再需要 QoS 策略，您可以将其删除。删除 QoS 策略时，与该策略关联的所有卷将保留 QoS 设置，但会与该策略解除关联。

如果您要尝试将卷与 QoS 策略解除关联，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 策略旁边的“操作”图标。
3. 在出现的菜单中，选择“删除”。
4. 确认此操作。

查找更多信息

- "移除卷的 QoS 策略关联"

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

管理卷

SolidFire系统使用卷来配置存储。卷是可通过网络由 iSCSI 或光纤通道客户端访问的块设备。

在“管理”选项卡的“卷”页面上，您可以创建、修改、克隆和删除节点上的卷。

创建卷

您可以创建卷并将该卷与指定的帐户关联。每卷书籍都必须与一个账户关联。通过此关联，该帐户可以使用 CHAP 凭据通过 iSCSI 发起程序访问卷。

创建卷时可以指定 QoS 设置。

1. 选择“管理”>“卷”。
2. 点击“创建卷”。
3. 在“创建新卷”对话框中，输入“卷名称”。
4. 请输入体积总大小。

   默认卷大小选择单位为 GB。您可以创建以 GB 或 GiB 为单位大小的卷：

   - 1GB = 10亿字节
   - 1GiB = 1,073,741,824 字节
5. 选择体积的*块大小*。
6. 点击“帐户”下拉列表，然后选择应该有权访问该卷的帐户。

   如果账户不存在，请点击“创建账户”链接，输入新账户名称，然后点击“创建”。账户已创建并与新卷关联。

   如果账户数量超过 50 个，则列表不会显示。开始输入后，自动完成功能会显示可供选择的值。

7. 要设置*服务质量*，请执行以下操作之一：
   a. 在“策略”下，您可以选择现有的 QoS 策略（如有）。
   b. 在“自定义设置”下，设置 IOPS 的自定义最小值、最大值和突发值，或使用默认的 QoS 值。

      最大 IOPS 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达到此 IOPS 水平。
8. 点击“创建卷”。

查看成交量详情

1. 选择“管理”>“卷”。

2. 查看详细信息。
   - **ID**：系统生成的卷 ID。
   - 名称：创建卷时赋予该卷的名称。
   - 帐户：分配给该卷的帐户名称。
   - 访问组：卷所属的卷访问组的名称。
   - 访问权限：创建卷时分配给该卷的访问类型。可能值：
     - 读/写：所有读写操作均被接受。
     - 只读：允许所有读取操作；不允许写入操作。
     - 已锁定：仅允许管理员访问。
     - ReplicationTarget：指定为复制卷对中的目标卷。
   - 已用空间：体积中已使用的空间百分比。
   - 大小：卷的总大小（以 GB 为单位）。
   - 主节点 **ID**：此卷的主节点。
   - 辅助节点 **ID**：此卷的辅助节点列表。在过渡状态下（例如次级节点发生变化时），可能存在多个值，但通常只有一个值。
   - **QoS** 节流：识别卷是否因主存储节点负载过高而受到节流。
   - **QoS**策略：用户定义的QoS策略的名称和链接。
   - 最小 **IOPS**：保证该卷的最小 IOPS 数。
   - 最大 **IOPS**：卷允许的最大 IOPS 数。
   - 突发**IOPS**：在短时间内允许达到的最大IOPS数量。默认值 = 15,000。
   - 快照数：为该卷创建的快照数量。
   - 属性：通过 API 方法以键/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
     - 否
   - 创建于：卷的创建日期和时间。

查看单笔交易详情

您可以查看各个卷的性能统计信息。

1. 选择“报告”>“销量表现”。
2. 在音量列表中，单击音量对应的“操作”图标。
3. 单击“查看详细信息”。

   页面底部出现一个托盘，其中包含有关该卷的一般信息。

4. 要查看有关销量的更多详细信息，请点击*查看更多详情*。

该系统会显示详细信息以及音量性能图表。

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的计量单位。您还可以修改用于复制的帐户访问权限或限制对卷的访问。

当集群上有足够的空间且满足以下条件时，您可以调整卷的大小：

- 正常运行条件。
- 报告称出现容量错误或故障。
- 该卷正在被克隆。
- 音量正在重新同步。

步骤

1. 选择“管理”>“卷”。
2. 在“活动”窗口中，单击要编辑的卷的“操作”图标。
3. 单击“编辑”。
4. *可选：*更改卷的总大小。
   - 你可以增加体积，但不能减少体积。在一次调整大小的操作中，您只能调整一个卷的大小。垃圾回收操作和软件升级不会中断调整大小操作。
   - 如果要调整复制卷的大小，应首先增加指定为复制目标的卷的大小。然后您可以调整源卷的大小。目标体积可以大于或等于源体积，但不能小于源体积。

     默认卷大小选择单位为 GB。您可以创建以 GB 或 GiB 为单位大小的卷：

   - 1GB = 10亿字节
   - 1GiB = 1,073,741,824 字节
5. *可选：*请选择以下不同的帐户访问级别：
   - 只读
   - 读写
   - 已锁定
   - 复制目标
6. 可选： 选择应该有权访问该卷的帐户。

   如果账户不存在，请点击“创建账户”链接，输入新的账户名称，然后点击“创建”。账户已创建并与卷关联。

   > 如果账户数量超过 50 个，则列表不会显示。开始输入后，自动完成功能会显示可供选择的值。

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，您可以选择现有的 QoS 策略（如有）。

b. 在“自定义设置”下，设置 IOPS 的自定义最小值、最大值和突发值，或使用默认的 QoS 值。

如果您在卷上使用 QoS 策略，您可以设置自定义 QoS 以移除 QoS 策略与该卷的关联。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。输入值必须为有效的整数。

配置卷，使其突发值极高。这样一来，系统就能更快地处理偶尔出现的大块顺序工作负载，同时还能限制卷的持续 IOPS。

8. 点击“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；该卷在大约 8 小时内保持可用。如果在系统清除卷之前还原它，该卷将恢复联机并还原 iSCSI 连接。

如果用于创建快照的卷被删除，则其关联的快照将变为非活动状态。当删除源卷时，关联的非活动快照也会从系统中删除。

在安装或升级过程中，会创建与管理服务关联的持久卷并将其分配给新帐户。如果您使用的是持久卷，请勿修改或删除卷或其关联的帐户。

步骤

1. 选择“管理”>“卷”。
2. 要删除单个卷，请执行以下步骤：
   a. 点击要删除的卷对应的“操作”图标。
   b. 在出现的菜单中，单击“删除”。
   c. 确认此操作。

   系统会将卷移至“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，选中要删除的卷旁边的复选框。
   b. 点击“批量操作”。
   c. 在出现的菜单中，单击“删除”。
   d. 确认此操作。

      系统会将卷移至“卷”页面上的“已删除”区域。

恢复已删除的卷

如果系统中的某个卷已被删除但尚未被清除，则可以将其恢复。系统会在删除卷后大约八小时自动清除该卷。如

果系统已清除该卷，则无法恢复。

1. 选择“管理”>“卷”。
2. 点击“已删除”选项卡查看已删除卷的列表。
3. 单击要恢复的卷对应的“操作”图标。
4. 在出现的菜单中，单击“恢复”。
5. 确认此操作。

   该卷被放入*活动*卷列表中，并且与该卷的 iSCSI 连接已恢复。

清除卷

当一个卷被清除时，它会从系统中永久删除。该卷中的所有数据都丢失了。

系统会在删除卷八小时后自动清除这些卷。但是，如果您想在预定时间之前清除卷，您可以这样做。

1. 选择“管理”>“卷”。
2. 点击“已删除”按钮。
3. 执行以下步骤以清除单个卷或多个卷。

选项	步骤
清除单个卷	a. 单击要清除的卷的“操作”图标。 b. 点击“清除”。 c. 确认此操作。
清除多个卷	a. 选择要清除的卷。 b. 点击“批量操作”。 c. 在出现的菜单中，选择“清除”。 d. 确认此操作。

克隆卷

您可以创建单个卷或多个卷的克隆，以创建数据在特定时间点的副本。克隆卷时，系统会创建卷的快照，然后创建快照引用的数据的副本。这是一个异步过程，该过程所需的时间取决于您要克隆的卷的大小和当前的集群负载。

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。超出这些限制的请求将被排队，稍后处理。

不同的操作系统对克隆卷的处理方式各不相同。 VMware ESXi 会将克隆卷视为卷副本或快照卷。该卷将是一个可用于创建新数据存储的设备。有关挂载克隆卷和处理快照 LUN 的更多信息，请参阅 VMware 文档。 "挂载 VMFS 数据存储副本"和 "管理重复的 VMFS 数据存储"。

在通过克隆到较小大小来截断克隆卷之前，请确保已准备好分区，以便它们能够适应较小的卷。

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”页面的卷列表中，单击要克隆的卷的“操作”图标。
   b. 在出现的菜单中，单击“克隆”。
   c. 在“克隆卷”窗口中，输入新克隆卷的卷名。
   d. 使用“容量大小”微调框和列表选择容量的大小和测量单位。

      默认卷大小选择单位为 GB。您可以创建以 GB 或 GiB 为单位大小的卷：

      - 1GB = 10亿字节
      - 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卷关联的帐户。

      您可以在此步骤中创建帐户，方法是单击“创建帐户”链接，输入帐户名称，然后单击“创建”。创建账户后，系统会自动将其添加到“账户”列表中。

3. 要克隆多个卷，请执行以下步骤：
   a. 在“活动”页面的卷列表中，选中要克隆的任何卷旁边的复选框。
   b. 点击“批量操作”。
   c. 在出现的菜单中，选择“克隆”。
   d. 在“克隆多个卷”对话框中，在“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. 点击“开始克隆”。

   增加克隆的体积大小，会在新体积的末尾产生额外的可用空间。根据您对卷的使用方式，您可能需要扩展分区或在可用空间中创建新分区才能充分利用它。

了解更多信息

- "SolidFire和 Element 软件文档"
- "NetApp Element vCenter Server 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。创建卷访问组时，也可以进行光纤通道卷

LUN 分配。

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，主机可能不会自动发现新的 LUN ID，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. 点击要编辑的访问组的“操作”图标。
3. 在出现的菜单中，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. 对于列表中要分配 LUN 的每个卷，请在相应的 **LUN** 字段中输入新值。
6. 点击“保存更改”。

对卷应用**QoS**策略

您可以将现有的 QoS 策略批量应用于一个或多个卷。

您要批量应用的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复选框。
3. 点击“批量操作”。
4. 在出现的菜单中，单击“应用 QoS 策略”。
5. 从下拉列表中选择 QoS 策略。
6. 单击“应用”。

查找更多信息

服务质量政策

移除卷的 **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。

您要修改的卷应该与 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“操作”图标。
3. 单击“编辑”。
4. 在出现的“服务质量”菜单下，点击“自定义设置”。
5. 修改 最小 **IOPS**、最大 **IOPS** 和 突发 **IOPS**，或保持默认设置。
6. 点击“保存更改”。

查找更多信息

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 (VVols) 功能。 Element 软件系统默认禁用 VVols 功能，并且在新安装或升级过程中不会自动启用该功能。启用 VVols 功能只需进行一次配置。

你需要什么

- 集群必须运行 Element 9.0 或更高版本。
- 集群必须连接到与 VVols 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 Virtual Volumes 功能会永久更改 Element 软件配置。只有当您的集群连接到 VMware ESXi VVols 兼容环境时，才应启用 VVols 功能。只有将集群恢复到出厂映像才能禁用 VVols 功能并恢复默认设置，但这会删除系统上的所有数据。

步骤

1. 选择“集群”>“设置”。
2. 查找虚拟卷的集群特定设置。
3. 点击“启用虚拟卷”。
4. 单击“是”确认虚拟卷配置更改。

   VVols 选项卡出现在 Element 用户界面中。

   > 启用 VVols 功能后， SolidFire集群会启动 VASA 提供程序，打开 8444 端口以进行 VASA 流量传输，并创建 vCenter 和所有 ESXi 主机可以发现的协议端点。

5. 从“集群”>“设置”中的“虚拟卷 (VVols)”设置中复制 VASA 提供程序 URL。您将使用此 URL 在 vCenter 中注册 VASA 提供程序。
6. 在 **VVols** > 存储容器 中创建存储容器。

   > 您必须创建至少一个存储容器，以便将虚拟机配置到 VVol 数据存储中。

7. 选择 **VVols** > 协议端点。
8. 确认集群中每个节点都已创建协议端点。

> vSphere 中还需要进行其他配置任务。请参阅《VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide》以在 vCenter 中注册 VASA Provider、创建和管理 VVol 数据存储以及根据策略管理存储。

查找更多信息

"VMware vSphere Virtual Volumes for SolidFire存储配置指南"

查看虚拟卷详情

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。

你需要什么

- 您应该在集群的 Element UI 中启用 VVols 功能。
- 你应该创建一个关联的存储容器。
- 您应该将 vSphere 集群配置为使用 Element 软件的 VVols 功能。
- 你应该至少在 vSphere 中创建一台虚拟机。

步骤

1. 点击“虚拟卷”>“虚拟卷”。

   显示所有活动虚拟卷的信息。

2. 点击要查看的虚拟卷的“操作”图标。
3. 在出现的菜单中，选择“查看详细信息”。

详细信息

VVols 选项卡的“虚拟卷”页面提供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：基础卷的 ID。
- 快照 **ID**：底层卷快照的 ID。如果虚拟卷不代表SolidFire快照，则该值为 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，与父卷没有链接。
- 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。
- 客户操作系统类型：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。
- 访问权限：分配给虚拟卷的读写权限。
- 大小：虚拟卷的大小，单位为 GB 或 GiB。
- 快照数量：关联的快照数量。点击数字可查看快照详情。
- 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：虚拟卷创建任务完成的时间。

单个虚拟卷详情

在 VVols 选项卡上的“虚拟卷”页面中，选择单个虚拟卷并查看其详细信息时，会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，与父卷没有链接。
- 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：基础卷的 ID。
- 访问权限：分配给虚拟卷的读写权限。
- 账户名称：包含该卷的账户名称。
- 访问组：关联的卷访问组。
- 总卷大小：以字节为单位的总已配置容量。
- 非零块：最后一次垃圾回收操作完成后，包含数据的 4KiB 块的总数。
- 零块：最后一轮垃圾回收操作完成后，没有数据的 4KiB 块的总数。
- 快照数量：关联的快照数量。点击数字可查看快照详情。
- 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**：因为虚拟卷始终使用 512 字节块大小模拟，所以该值始终为“是”。
- 卷册配对：指示卷册是否配对。
- 创建时间：虚拟卷创建任务完成的时间。
- 块大小：体积中块的大小。
- 未对齐写入：对于 512e 卷，指不在 4k 扇区边界上的写入操作次数。大量未对齐的写入操作可能表明分区对齐不正确。
- 未对齐读取：对于 512e 卷，读取操作不在 4k 扇区边界上的数量。大量未比对的读取序列可能表明分区比对不正确。
- **scsiEUIDeviceID**：基于 EUI-64 的 16 字节格式的卷的全局唯一 SCSI 设备标识符。
- **scsiNAADeviceID**：NAA IEEE 注册扩展格式中卷的全局唯一 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

尽管虚拟卷应该始终从 VMware 管理层中删除，但您可以通过 Element UI 启用删除虚拟卷的功能。只有在绝对必要的情况下，例如 vSphere 无法清理SolidFire存储上的虚拟卷时，才应该从 Element UI 中删除虚拟卷。

1. 选择 **VVols** > 虚拟卷。
2. 单击要删除的虚拟卷的“操作”图标。
3. 在出现的菜单中，选择“删除”。

> 您应该从 VMware 管理层删除虚拟卷，以确保在删除之前虚拟卷已正确解除绑定。只有在绝对必要的情况下，例如 vSphere 无法清理SolidFire存储上的虚拟卷时，才应该从 Element UI 中删除虚拟卷。如果从 Element UI 中删除虚拟卷，该卷将立即被清除。

4. 确认此操作。
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*以确认清除操作是否成功。

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 数据存储表示。

创建存储容器并将其与NetApp Element帐户关联。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。存储容器不会在 Element 存储上分配任何空间。它们的作用仅仅是将虚拟卷在逻辑上关联起来。

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

创建一个存储容器

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

开始之前，请在集群的 Element UI 中启用 VVols 功能。

步骤

1. 选择 **VVols** > 存储容器。
2. 点击“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. 请输入存储容器的名称。
   b. 配置 CHAP 的发起方密钥和目标密钥。

      > 将 CHAP 设置字段留空以自动生成密钥。

   c. 点击“创建存储容器”按钮。
4. 确认新存储容器出现在“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。

查看存储容器详情

在 VVols 选项卡的“存储容器”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：
  - 活动状态：存储容器正在使用中。
  - 已锁定：储物容器已锁定。
- **PE** 类型：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。

查看单个存储容器的详细信息

您可以通过在 VVols 选项卡的“存储容器”页面上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：
  - 活动状态：存储容器正在使用中。
  - 已锁定：储物容器已锁定。
- **CHAP**发起者秘密：发起者独有的CHAP秘密。
- **CHAP**目标秘密：针对目标的独特CHAP秘密。
- 存储容器 **ID**：虚拟卷存储容器的 UUID。
- 协议端点类型：指示协议端点类型（SCSI 是唯一可用的协议）。

编辑存储容器

您可以在 Element UI 中修改存储容器的 CHAP 身份验证。

1. 选择 **VVols** > 存储容器。
2. 点击要编辑的存储容器旁边的“操作”图标。
3. 在出现的菜单中，选择“编辑”。
4. 在 CHAP 设置中，编辑用于身份验证的发起方密钥和目标密钥凭据。

   如果您不更改 CHAP 设置凭据，则它们将保持不变。如果将凭据字段留空，系统会自动生成新的密钥。

5. 点击“保存更改”。

删除存储容器

您可以从 Element 用户界面删除存储容器。

你需要什么

确保所有虚拟机都已从 VVol 数据存储中删除。

步骤

1. 选择 **VVols** > 存储容器。
2. 点击要删除的存储容器旁边的“操作”图标。
3. 在出现的菜单中，选择“删除”。
4. 确认此操作。
5. 刷新“存储容器”子选项卡中的存储容器列表，以确认存储容器已被删除。

协议端点

了解协议端点

协议端点是主机用来访问运行NetApp Element软件的集群上的存储的接入点。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有六个协议端点，分别映射到每个 ESXi 主机。协议端点由 Element 软件动态管理，可根据需要创建、移动或删除，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。每个协议端点都会占用一个可用的 SCSI 地址，就像标准的 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，但此存储设备无法格式化或用作存储。

iSCSI 是唯一受支持的协议。不支持光纤通道协议。

协议端点详情

VVols 选项卡上的“协议端点”页面提供协议端点信息。

- 主提供者 **ID**

  主协议端点提供程序的 ID。

- 辅助提供者 **ID**

  辅助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。可能的值如下：

- 已激活：协议端点正在使用中。
- 开始：协议端点正在启动。
- 故障转移：协议端点已发生故障转移。
- 保留：协议端点已保留。

- 提供商类型

  协议端点提供程序的类型。可能的值如下：

  - 主云
  - 二级

- **SCSI NAA** 设备 **ID**

  NAA IEEE 注册扩展格式中协议端点的全球唯一 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集群选择最佳协议端点，创建将 ESXi 主机和虚拟卷与该协议端点关联的绑定，并将该绑定返回给 ESXi 主机。绑定完成后，ESXi 主机可以对绑定的虚拟卷执行 I/O 操作。

装订细节

VVols 选项卡上的“绑定”页面提供有关每个虚拟卷的绑定信息。

显示以下信息：

- 主机 **ID**

  集群已知的托管虚拟卷的 ESXi 主机的 UUID。

- 协议端点 **ID**

  与SolidFire集群中每个节点对应的协议端点 ID。

- 频段 **ID** 中的协议端点

  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** 辅助 **ID**

  虚拟卷的辅助 ID，即 SCSI 二级 LUN ID。

房东详情

VVols 选项卡上的“主机”页面提供有关托管虚拟卷的 VMware ESXi 主机的信息。

显示以下信息：

- 主机 **ID**

  集群已知的托管虚拟卷的 ESXi 主机的 UUID。

- 主机地址

  ESXi主机的IP地址或DNS名称。

- 装订

  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。

- 发起者**IQN**

  虚拟卷主机的启动器 IQN。

- * SolidFire协议端点 ID*

  当前对 ESXi 主机可见的协议端点。

与批量访问组和发起者合作

创建卷访问组

您可以通过将发起程序映射到卷集合来创建卷访问组，从而实现安全访问。然后，您可以使用帐户 CHAP 发起程序密钥和目标密钥授予对组中卷的访问权限。

如果使用基于发起方的 CHAP，则可以为卷访问组中的单个发起方添加 CHAP 凭证，从而提供更高的安全性。这样，您就可以将此选项应用于已存在的卷访问组。

步骤

1. 点击“管理”>“访问组”。

2. 点击“创建访问组”。
3. 在“名称”字段中输入卷访问组的名称。
4. 可以通过以下方式之一将发起程序添加到卷访问组：

选项	描述
添加光纤通道发起程序	a. 在“添加发起程序”下，从“未绑定光纤通道发起程序”列表中选择一个现有的光纤通道发起程序。 b. 点击*添加FC发起者*。 在此步骤中，您可以点击“创建发起者”链接，输入发起者名称，然后点击“创建”，即可创建发起者。创建发起程序后，系统会自动将其添加到发起程序列表中。 格式示例如下： `5f:47:ac:c0:5c:74:d4:02`
添加 iSCSI 发起程序	在“添加发起方”下，从发起方列表中选择一个现有的发起方。 注意： 您可以在此步骤中创建发起者，方法是单击“创建发起者”链接，输入发起者名称，然后单击“创建”。创建发起程序后，系统会自动将其添加到发起程序列表中。 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”来查找每个卷的发起者 IQN。 修改发起程序时，可以将 requiredCHAP 属性切换为 True，这样就可以设置目标发起程序密钥。有关详细信息，请参阅 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器。
6. 在“添加卷”下，从“卷”列表中选择一个卷。

   该卷出现在“已附加卷”列表中。
7. *可选：*根据需要添加更多卷。
8. 点击“创建访问组”。

查找更多信息

[将卷添加到访问组]

查看个人访问组详情

您可以以图形格式查看单个访问组的详细信息，例如附加的卷和启动器。

1. 点击“管理”>“访问组”。
2. 点击访问组的“操作”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。

显示以下信息：

- **ID**：系统生成的访问组 ID。
- 名称：创建访问组时赋予该组的名称。
- 活动卷：访问组中的活动卷数量。
- 压缩：访问组的压缩效率得分。
- 去重：访问组的去重效率得分。
- 精简配置：访问组的精简配置效率得分。
- 总体效率：访问组的总体效率得分。
- 发起者：连接到访问组的发起者数量。

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。

您还可以使用此过程将卷添加到光纤通道卷访问组。

1. 点击“管理”>“访问组”。
2. 单击要添加卷的访问组的“操作”图标。
3. 点击“编辑”按钮。
4. 在“添加卷”下，从“卷”列表中选择一个卷。

   重复此步骤即可增加音量。
5. 点击“保存更改”。

从访问组中移除卷

从访问组中移除卷后，该组将不再拥有对该卷的访问权限。

修改帐户中的 CHAP 设置或从访问组中删除发起程序或卷可能会导致发起程序意外失去对卷的访问权限。为验证卷访问不会意外丢失，请务必注销受帐户或访问组更改影响的 iSCSI 会话，并在完成对启动器设置和集群设置的任何更改后，验证启动器是否可以重新连接到卷。

1. 点击“管理”>“访问组”。
2. 单击要从中删除卷的访问组的“操作”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“已附加卷”列表上的箭头。
5. 从列表中选择要删除的卷，然后单击 **x** 图标将其从列表中删除。

   重复此步骤可以移除更多卷。

6. 点击“保存更改”。

创建发起者

您可以创建 iSCSI 或光纤通道发起程序，并可选择为其分配别名。

您还可以通过 API 调用来分配基于发起方的 CHAP 属性。要为每个发起方添加 CHAP 帐户名称和凭据，您必须使用 `CreateInitiator`调用 API 来移除和添加 CHAP 访问权限和属性。通过指定一个或多个虚拟网络 ID，可以将发起方访问权限限制为一个或多个 VLAN。 `CreateInitiators`和 `ModifyInitiators`API调用。如果没有指定虚拟网络，则发起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. 点击“管理”>“发起者”。
2. 点击“创建发起者”。
3. 执行以下步骤创建单个启动器或多个启动器：

选项	步骤
创建一个单一发起者	a. 点击“创建单个发起者”。 b. 在 **IQN/WWPN** 字段中输入发起人的 IQN 或 WWPN。 c. 在“别名”字段中输入发起者的友好名称。 d. 点击“创建发起者”。

选项	步骤
创建多个启动器	a. 点击“批量创建发起者”。 b. 在文本框中输入 IQN 或 WWPN 列表。 c. 点击“添加发起者”。 d. 从结果列表中选择一个发起者，然后单击“别名”列中相应的“添加”图标，为该发起者添加别名。 e. 点击勾选标记以确认新别名。 f. 点击“创建发起者”。

编辑发起者

您可以更改现有发起程序的别名，或者在别名尚不存在时添加别名。

要为每个发起方添加 CHAP 帐户名称和凭据，您必须使用 `ModifyInitiator`调用 API 来移除和添加 CHAP 访问权限和属性。

看"使用 Element API 管理存储"。

步骤

1. 点击“管理”>“发起者”。
2. 点击要编辑的发起者的“操作”图标。
3. 单击“编辑”。
4. 在“别名”字段中输入发起者的新别名。
5. 点击“保存更改”。

将单个启动器添加到卷访问组

您可以将发起程序添加到现有的卷访问组。

将启动器添加到卷访问组后，该启动器将有权访问该卷访问组中的所有卷。

您可以通过单击“操作”图标，然后在活动卷列表中选择卷的“查看详细信息”来找到每个卷的发起者。

如果使用基于发起方的 CHAP，则可以为卷访问组中的单个发起方添加 CHAP 凭证，从而提供更高的安全性。这样，您就可以将此选项应用于已存在的卷访问组。

步骤

1. 点击“管理”>“访问组”。
2. 点击要编辑的访问组的“操作”图标。
3. 单击“编辑”。
4. 要将光纤通道发起程序添加到卷访问组，请执行以下步骤：

a. 在“添加发起程序”下，从“未绑定光纤通道发起程序”列表中选择一个现有的光纤通道发起程序。

b. 点击*添加FC发起者*。

> 在此步骤中，您可以点击“创建发起者”链接，输入发起者名称，然后点击“创建”，即可创建发起者。创建发起程序后，系统会自动将其添加到 发起程序 列表中。

格式示例如下：

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

5. 要将 iSCSI 发起程序添加到卷访问组，请在“添加发起程序”下，从“发起程序”列表中选择现有发起程序。

> 在此步骤中，您可以点击“创建发起者”链接，输入发起者名称，然后点击“创建”，即可创建发起者。创建发起程序后，系统会自动将其添加到 发起程序 列表中。

发起者 IQN 的可接受格式如下：iqn.yyyy-mm，其中 y 和 m 为数字，后面跟着文本，该文本必须仅包含数字、小写字母字符、句点 (.)、冒号 (:) 或破折号 (-)。

格式示例如下：

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

> 您可以从“管理”>“卷”>“活动卷”页面找到每个卷的发起方 IQN，方法是单击“操作”图标，然后选择卷的“查看详细信息”。

6. 点击“保存更改”。

向卷访问组添加多个启动器

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

将启动器添加到卷访问组后，启动器将有权访问该卷访问组中的所有卷。

> 您可以通过单击“操作”图标，然后在活动卷列表中单击卷的“查看详细信息”，找到每个卷的发起者。

您可以向现有卷访问组添加多个启动器，以启用对卷的访问，并为该卷访问组中的每个启动器分配唯一的 CHAP 凭证。这样，您就可以将此选项应用于已存在的卷访问组。

您可以通过 API 调用分配基于发起方的 CHAP 属性。要为每个发起方添加 CHAP 帐户名称和凭据，必须使用 ModifyInitiator API 调用来删除和添加 CHAP 访问权限和属性。

有关详细信息，请参阅"使用 Element API 管理存储"。

步骤

1. 点击“管理”>“发起者”。
2. 选择要添加到访问组的发起者。
3. 点击“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”。

从访问组中移除发起者

从访问组中移除启动器后，它将无法再访问该卷访问组中的卷。账户对该卷的正常访问未受影响。

修改帐户中的 CHAP 设置或从访问组中删除发起程序或卷可能会导致发起程序意外失去对卷的访问权限。为验证卷访问不会意外丢失，请务必注销受帐户或访问组更改影响的 iSCSI 会话，并在完成对启动器设置和集群设置的任何更改后，验证启动器是否可以重新连接到卷。

步骤

1. 点击“管理”>“访问组”。
2. 点击要移除的访问组的“操作”图标。
3. 在出现的菜单中，选择“编辑”。
4. 在“编辑卷访问组”对话框的“添加启动器”下，单击“启动器”列表上的箭头。
5. 选择要从访问组中移除的每个发起者的 x 图标。
6. 点击“保存更改”。

删除访问组

不再需要访问组时，您可以将其删除。在删除卷访问组之前，无需从该卷访问组中删除启动器 ID 和卷 ID。删除访问组后，该组对卷的访问权限将停止。

1. 点击“管理”>“访问组”。
2. 点击要删除的访问组的“操作”图标。
3. 在出现的菜单中，单击“删除”。
4. 要同时删除与此访问组关联的发起程序，请选中“删除此访问组中的发起程序”复选框。
5. 确认此操作。

删除发起者

不再需要启动器时，您可以将其删除。删除启动器时，系统会将其从所有关联的卷访问组中移除。使用该发起程序建立的任何连接都将保持有效，直到连接被重置为止。

步骤

1. 点击“管理”>“发起者”。

2. 执行以下步骤删除单个或多个启动器：

选项	步骤
删除单个发起者	a. 点击要删除的发起者的“操作”图标。 b. 单击“删除”。 c. 确认此操作。
删除多个发起者	a. 选中要删除的发起者旁边的复选框。 b. 点击“批量操作”按钮。 c. 在出现的菜单中，选择“删除”。 d. 确认此操作。

保护您的数据

保护您的数据

NetApp Element软件能够以多种方式保护您的数据，其功能包括：为单个卷或卷组创建快照、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

  仅快照数据保护会在特定时间点将已更改的数据复制到远程集群。只有在源集群上创建的快照才会被复制。来自源卷的活动写入操作不会发生。

  使用卷快照进行数据保护

- 在 **Element** 上运行的集群和卷之间的远程复制

  您可以同步或异步地从集群对中的任何一个集群复制卷数据，这两个集群都在 Element 上运行，以实现故障转移和故障恢复场景。

  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 拍摄的快照复制到ONTAP ，以用于灾难恢复。在SnapMirror关系中，Element 是一个端点， ONTAP是另一个端点。

  在 Element 和ONTAP集群之间使用SnapMirror复制

- 备份和恢复来自**SolidFire**、**S3** 或 **Swift** 对象存储的卷

  您可以将卷备份和恢复到其他SolidFire存储，以及与 Amazon S3 或 OpenStack Swift 兼容的辅助对象存储。

  将卷备份和恢复到SolidFire、S3 或 Swift 对象存储

了解更多信息

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

使用卷快照进行数据保护

使用卷快照进行数据保护

卷快照是卷在特定时间点的副本。您可以对卷进行快照，并在以后需要将卷回滚到创建快照时的状态时使用该快照。

快照类似于卷克隆。但是，快照只是卷元数据的副本，因此您无法挂载或写入它们。创建卷快照也只需要少量系统资源和空间，因此快照创建速度比克隆更快。

您可以对单个卷或一组卷进行快照。

（可选）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的时间点。或者，您可以从复制的快照创建卷的克隆。

查找更多信息

- 使用单个卷快照进行数据保护
- 使用组快照进行数据保护任务
- 安排快照

使用单个卷快照进行数据保护

使用单个卷快照进行数据保护

卷快照是卷在特定时间点的副本。您可以为快照使用单个卷，而不是一组卷。

查找更多信息

- 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

您可以创建活动卷的快照，以保存卷映像到任何时间点的状态。单个卷最多可以创建 32

个快照。

1. 点击“管理”>“卷”。
2. 单击要用于快照的卷的“操作”图标。
3. 在出现的菜单中，选择“快照”。
4. 在“创建卷快照”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，以确保在配对父卷时，快照被捕获到复制中。
6. 要设置快照的保留期限，请从以下选项中选择：
   - 点击“永久保留”可将快照无限期地保留在系统中。
   - 点击“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
7. 要拍摄一张即时快照，请执行以下步骤：
   a. 点击*立即拍摄快照*。
   b. 点击创建快照。
8. 要安排快照在未来某个时间运行，请执行以下步骤：
   a. 点击“创建快照日程”。
   b. 输入新的课程表名称。
   c. 请从列表中选择*日程类型*。
   d. *可选：*选中“重复计划”复选框，即可定期重复执行计划快照。
   e. 点击“创建日程”。

查找更多信息

安排快照

编辑快照保留

您可以更改快照的保留期限，以控制系统何时或是否删除快照。您指定的保留期限从您输入新的时间间隔时开始计算。设置保留期时，可以选择从当前时间开始的保留期（保留期不是从快照创建时间开始计算的）。您可以以分钟、小时和天为单位指定时间间隔。

步骤

1. 点击“数据保护”>“快照”。
2. 点击要编辑的快照旁边的“操作”图标。
3. 在出现的菜单中，单击“编辑”。
4. *可选：*选中“配对时在复制中包含快照”复选框，以确保在配对父卷时，快照被捕获到复制中。
5. 可选： 选择快照的保留选项：
   - 点击“永久保留”可将快照无限期地保留在系统中。
   - 点击“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
6. 点击“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。如果在删除快照时快照正在同步到目标集群，则同步复制完成，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删除已复制到目标的快照。已删除的快照会保留在目标集群的已删除快照列表中，直到系统检测到您已在源集群上删除该快照为止。当目标系统检测到您已删除源快照时，目标系统将停止快照的复制。

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. 点击“数据保护”>“快照”。
2. 点击要删除的快照旁边的“操作”图标。
3. 在出现的菜单中，选择“删除”。
4. 确认此操作。

从快照克隆卷

您可以从卷的快照创建新卷。执行此操作时，系统会使用快照信息，利用创建快照时卷上包含的数据克隆一个新卷。此过程会将有关该卷其他快照的信息存储在新创建的卷中。

1. 点击“数据保护”>“快照”。
2. 单击要用于卷克隆的快照的“操作”图标。
3. 在出现的菜单中，单击“从快照克隆卷”。
4. 在“从快照克隆卷”对话框中输入“卷名称”。
5. 选择新卷的*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*来关联新卷。
8. 点击“开始克隆”。

将卷回滚到快照

您可以随时将卷回滚到之前的快照。这将撤销自创建快照以来对卷所做的任何更改。

步骤

1. 点击“数据保护”>“快照”。
2. 单击要用于卷回滚的快照的“操作”图标。
3. 在出现的菜单中，选择“将卷回快照”。
4. 可选： 在回滚到快照之前保存卷的当前状态：
   a. 在“回滚到快照”对话框中，选择“将卷的当前状态保存为快照”。
   b. 请输入新快照的名称。

5. 点击“回滚快照”。

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SolidFire集群中的快照备份到外部对象存储，或者备份到另一个SolidFire集群。将快照备份到外部对象存储时，必须与该对象存储建立允许读/写操作的连接。

- "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. 点击数据保护 > 快照。
2. 点击要备份的快照旁边的“操作”图标。
3. 在出现的菜单中，单击“备份到”。
4. 在“集成备份”对话框的“备份到”下，选择“S3”。
5. 在“数据格式”下选择一个选项：
   - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
   - 未压缩：一种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“密钥”字段中输入帐户的密钥。
9. 在“S3 存储桶”字段中输入要存储备份的 S3 存储桶。
10. 可选：在“姓名标签”字段中输入要附加到前缀的姓名标签。
11. 点击“开始阅读”。

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 兼容的辅助对象存储中。

1. 点击“数据保护”>“快照”。
2. 点击要备份的快照旁边的“操作”图标。
3. 在出现的菜单中，单击“备份到”。
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：

- 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
- 未压缩：一种与其他系统兼容的未压缩格式。

6. 输入要用于访问对象存储的*URL*。
7. 请输入账户的*用户名*。
8. 请输入账户的*身份验证密钥*。
9. 请输入用于存储备份的*容器*。
10. 可选：输入*姓名标签*。
11. 点击“开始阅读”。

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配对。

当从一个集群备份或恢复到另一个集群时，系统会生成一个密钥，用于集群之间的身份验证。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程度的安全性。作为备份或恢复过程的一部分，您需要在开始操作之前从目标卷生成批量卷写入密钥。

1. 在目标集群上，单击“管理”>“卷”。
2. 点击目标卷的“操作”图标。
3. 在出现的菜单中，单击“从……恢复”。
4. 在“集成还原”对话框的“还原来源”下，选择“SolidFire”。
5. 在“数据格式”下选择数据格式：
   - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
   - 未压缩：一种与其他系统兼容的未压缩格式。
6. 点击“生成密钥”。
7. 将“批量写入密钥”框中的密钥复制到剪贴板。
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的“操作”图标。
10. 在出现的菜单中，单击“备份到”。
11. 在集成备份对话框的*备份到*下，选择* SolidFire*。
12. 选择与您之前在“数据格式”字段中选择的数据格式相同的数据格式。
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，粘贴您之前在目标集群上生成的密钥。
17. 点击“开始阅读”。

使用组快照进行数据保护任务

您可以创建一组相关卷的组快照，以保留每个卷的元数据在特定时间点的副本。将来，您可以将组快照用作备份或回滚，以将卷组的状态恢复到以前的状态。

查找更多信息

- 创建群组快照
- 编辑群组快照
- 编辑群组快照成员
- 删除群组快照
- 将卷回滚到组快照
- 克隆多个卷
- 从组快照克隆多个卷

群组快照详情

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**

  系统生成的群组快照 ID。

- **UUID**

  群组快照的唯一 ID。

- 姓名

  用户自定义的组快照名称。

- 创造时间

  创建群组快照的时间。

- 地位

  快照的当前状态。可能值：

  - 准备中：快照正在准备使用，目前还不可写。
  - 完成：此快照已完成准备，现在可以使用了。
  - 活动分支：快照是当前活动分支。

- 卷数

  该组中的卷数。

- 保留至

  快照将被删除的日期和时间。

- 远程复制

  指示快照是否已启用复制到远程SolidFire集群。可能值：

  - 已启用：快照已启用远程复制。
  - 已禁用：快照未启用远程复制。

创建群组快照

您可以创建一组卷的快照，还可以创建组快照计划来自动执行组快照。单个组快照可以同时对最多 32 个卷进行快照。

步骤

1. 点击“管理”>“卷”。
2. 使用复选框选择一组卷册中的多个卷册。
3. 点击“批量操作”。
4. 点击“群组快照”。
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含在复制中”复选框，以确保在父卷配对时，每个快照都会被复制到复制中。
7. 选择群组快照的保留选项：
   - 点击“永久保留”可将快照无限期地保留在系统中。
   - 点击“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
8. 要拍摄一张即时快照，请执行以下步骤：
   a. 点击*立即拍摄群组快照*。
   b. 点击“创建群组快照”。
9. 要安排快照在未来某个时间运行，请执行以下步骤：
   a. 点击“创建群组快照计划”。
   b. 输入新的课程表名称。
   c. 从列表中选择*日程类型*。
   d. *可选：*选中“重复计划”复选框，即可定期重复执行计划快照。
   e. 点击“创建日程”。

编辑群组快照

您可以编辑现有组快照的复制和保留设置。

1. 点击“数据保护”>“群组快照”。

2. 点击要编辑的群组快照旁边的“操作”图标。
3. 在出现的菜单中，选择“编辑”。
4. 可选： 更改组快照的复制设置：
   a. 点击“当前复制”旁边的“编辑”。
   b. 选中“配对时将每个组快照成员包含在复制中”复选框，以确保在父卷配对时，每个快照都会被捕获到复制中。
5. *可选：*要更改组快照的保留设置，请从以下选项中选择：
   a. 点击“当前保留期限”旁边的“编辑”。
   b. 选择群组快照的保留选项：
      - 点击“永久保留”可将快照无限期地保留在系统中。
      - 点击“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
6. 点击“保存更改”。

删除群组快照

您可以从系统中删除群组快照。删除群组快照时，您可以选择是删除与该群组关联的所有快照，还是保留为单独的快照。

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

1. 点击“数据保护”>“群组快照”。
2. 点击要删除的快照旁边的“操作”图标。
3. 在出现的菜单中，单击“删除”。
4. 请在确认对话框中选择以下选项之一：
   - 点击“删除群组快照及所有群组快照成员”以删除群组快照和所有成员快照。
   - 点击“将群组快照成员保留为单独的快照”以删除群组快照，但保留所有成员快照。
5. 确认此操作。

将卷回滚到组快照

您可以随时将一组卷回滚到组快照状态。

回滚一组卷时，组中的所有卷都会恢复到创建组快照时的状态。回滚操作还会将卷大小恢复到原始快照中记录的大小。如果系统已清除某个卷，则该卷的所有快照也会在清除时被删除；系统不会恢复任何已删除的卷快照。

1. 点击“数据保护”>“群组快照”。
2. 单击要用于卷回滚的组快照的“操作”图标。
3. 在出现的菜单中，选择“将卷回滚到组快照”。
4. 可选：在回滚到快照之前保存卷的当前状态：
   a. 在“回滚到快照”对话框中，选择“将卷的当前状态保存为组快照”。
   b. 请输入新快照的名称。

5. 点击“回滚组快照”。

编辑群组快照成员

您可以编辑现有群组快照成员的保留设置。

1. 点击“数据保护”>“快照”。
2. 点击“成员”选项卡。
3. 点击要编辑的群组快照成员旁边的“操作”图标。
4. 在出现的菜单中，选择“编辑”。
5. 要更改快照的复制设置，请从以下选项中选择：
   - 点击“永久保留”可将快照无限期地保留在系统中。
   - 点击“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
6. 点击“保存更改”。

克隆多个卷

您可以在一次操作中创建多个卷克隆，从而创建一组卷上数据的某个时间点的副本。

克隆卷时，系统会创建该卷的快照，然后根据快照中的数据创建一个新卷。您可以挂载并写入新的卷克隆。克隆多个卷是一个异步过程，所需时间取决于被克隆卷的大小和数量。

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. 点击“管理”>“卷”。
2. 点击“活动”选项卡。
3. 使用复选框选择多个卷册，创建一个卷册组。
4. 点击“批量操作”。
5. 在弹出的菜单中点击“克隆”。
6. 在“克隆多个卷”对话框中输入“新卷名称前缀”。

   该前缀应用于该组中的所有卷。

7. 可选： 选择一个不同的帐户，克隆帐户将属于该帐户。

   如果您不选择帐户，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式。

   如果您未选择访问方式，系统将使用当前卷访问方式。

9. 点击“开始克隆”。

从组快照克隆多个卷

您可以从某个时间点的组快照克隆一组卷。此操作要求卷的组快照已存在，因为组快照将用作创建卷的基础。创建卷之后，就可以像使用系统中的任何其他卷一样使用它们。

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. 点击“数据保护”>“群组快照”。
2. 单击要用于卷克隆的组快照的“操作”图标。
3. 在出现的菜单中，选择“从组快照克隆卷”。
4. 在“从组快照克隆卷”对话框中输入“新卷名称前缀”。

   该前缀将应用于从组快照创建的所有卷。

5. 可选： 选择一个不同的帐户，克隆帐户将属于该帐户。

   如果您不选择帐户，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式。

   如果您未选择访问方式，系统将使用当前卷访问方式。

7. 点击“开始克隆”。

安排快照

安排快照

您可以通过安排卷快照按指定时间间隔执行，来保护卷或卷组上的数据。您可以安排单个卷快照或组快照自动运行。

配置快照计划时，您可以选择基于星期几或月份几的时间间隔。您还可以指定下次快照发生的日期、小时和分钟。如果卷正在复制，则可以将生成的快照存储在远程存储系统中。

查找更多信息

- 创建快照计划
- 编辑快照日程
- 删除快照计划
- 复制快照日程

快照日程详情

在“数据保护 > 计划”页面上，您可以在快照计划列表中查看以下信息。

- **ID**

  系统生成的快照 ID。

- 类型

  日程安排类型。目前仅支持快照类型。

- 姓名

  该日程表创建时所起的名称。快照计划名称最多可包含 223 个字符，并且包含 az、0-9 和破折号 (-) 字符。

- 频率

  该日程安排的运行频率。频率可以按小时和分钟、周或月设置。

- 再次发生的

  说明该日程安排是只运行一次还是定期运行。

- 手动暂停

  指示日程是否已被手动暂停。

- 卷 ID

  该调度程序运行时将使用的卷的 ID。

- 最后一次运行

  上次运行该日程表的时间。

- 上次运行状态

  上次计划执行的结果。可能值：

  - 成功
  - 失败

创建快照计划

您可以安排对一个或多个卷进行快照，使其按指定的时间间隔自动执行。

配置快照计划时，您可以选择基于星期几或月份几的时间间隔。您还可以创建重复计划，并指定下次快照发生的日期、小时和分钟。

如果您安排快照运行的时间段不能被 5 分钟整除，则快照将在下一个能被 5 分钟整除的时间段运行。例如，如果您安排快照在 UTC 时间 12:42:00 运行，它将在 UTC 时间 12:45:00 运行。您无法安排快照运行的间隔小于 5 分钟。

从 Element 12.5 开始，您可以从用户界面启用序列创建并选择按先进先出 (FIFO) 原则保留快照。

- *启用序列创建*选项指定一次只复制一个快照。当先前的快照复制仍在进行中时，创建新快照会失败。如果未选中该复选框，则允许在另一个快照复制仍在进行时创建快照。
- **FIFO** 选项增加了保留一致数量的最新快照的功能。选中该复选框后，快照将按先进先出 (FIFO) 的原则保留。当 FIFO 快照队列达到最大深度后，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”>“日程安排”。
2. 选择“创建日程”。
3. 在“卷 ID CSV”字段中，输入单个卷 ID 或以逗号分隔的卷 ID 列表，以包含在快照操作中。
4. 请输入新的课程表名称。
5. 选择日程类型，并从提供的选项中设置日程。
6. *可选：*选择*重复计划*可无限期重复快照计划。
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，系统将使用快照创建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，以确保在配对父卷时，快照被捕获到复制中。
9. *可选：*选中“启用序列创建”复选框，以确保一次只复制一个快照。
10. 要设置快照的保留期限，请从以下选项中选择：
    - *可选：*选中 *FIFO（先进先出）*复选框，以保留一致数量的最新快照。
    - 选择“永久保留”可将快照无限期地保留在系统中。
    - 选择“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
11. 选择“创建日程”。

编辑快照日程

您可以修改现有的快照计划。修改后，下次运行计划时将使用更新后的属性。原始计划创建的任何快照都将保留在存储系统中。

步骤

1. 点击“数据保护”>“日程安排”。
2. 点击要更改的日程表旁边的“操作”图标。
3. 在出现的菜单中，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 或以逗号分隔的卷 ID 列表。
5. 要暂停或恢复日程安排，请从以下选项中选择：
    - 要暂停正在进行的日程安排，请从“手动暂停日程安排”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，可以在“新日程名称”字段中输入不同的日程名称。
7. 要更改运行计划，使其在一周或一个月中的不同日期运行，请选择“计划类型”，然后从提供的选项中更改计划。
8. *可选：*选择*重复计划*可无限期重复快照计划。
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，系统将使用快照创建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，以确保在配对父卷时，快照被捕获到复制中。
11. 要更改保留设置，请从以下选项中选择：
    - 点击“永久保留”可将快照无限期地保留在系统中。
    - 点击“设置保留期限”，然后使用日期微调框选择系统保留快照的时间长度。
12. 点击“保存更改”。

复制快照日程

您可以复制日程表并保留其现有属性。

1. 点击“数据保护”>“日程安排”。
2. 点击要复制的日程表旁边的“操作”图标。
3. 在出现的菜单中，单击“制作副本”。

   此时会弹出“创建日程”对话框，其中填充了日程的当前属性。
4. *可选：*请输入新日程的名称和更新后的属性。
5. 点击“创建日程”。

删除快照计划

您可以删除快照计划。删除计划任务后，将不会运行任何未来的计划快照。计划任务创建的所有快照都会保留在存储系统中。

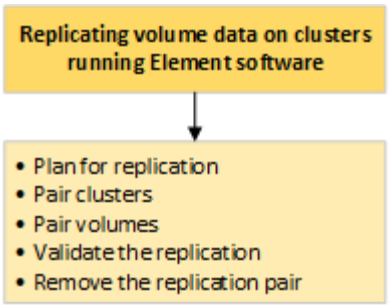
1. 点击“数据保护”>“日程安排”。
2. 点击要删除的日程表旁边的“操作”图标。
3. 在出现的菜单中，单击“删除”。
4. 确认此操作。

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，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。您可以同步或异步地从集群对中的任一集群复制卷数据，以实现故障转移和故障恢复场景。

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"
- "复制的成对集群"
- "对数"
- "验证卷复制"
- "复制完成后删除卷关系"
- "管理交易量关系"

规划集群和卷配对以实现实时复制

实时远程复制要求您将两个运行 Element 软件的存储集群配对，将每个集群上的卷配对，并验证复制。复制完成后，您应该删除卷关系。

你需要什么

- 您必须拥有配对集群中一个或两个集群的集群管理员权限。
- 配对集群的管理网络和存储网络上的所有节点 IP 地址都相互路由。
- 所有配对节点的 MTU 必须相同，并且集群之间必须端到端支持 MTU。
- 两个存储集群都应该具有唯一的集群名称、MVIP、SVIP 和所有节点 IP 地址。
- 集群上 Element 软件版本之间的差异不超过一个主版本。如果差异较大，则必须升级其中一个集群以执行数据复制。

NetApp尚未对 WAN 加速器设备进行认证，使其可用于数据复制。如果将这些设备部署在正在复制数据的两个集群之间，可能会干扰压缩和去重功能。在将任何 WAN 加速器设备部署到生产环境之前，务必充分评估其效果。

查找更多信息

- 复制的成对集群
- 对数
- 为配对卷分配复制源和目标

复制的成对集群

要使用实时复制功能，首先必须将两个集群配对。将两个集群配对连接后，您可以配置一个集群上的活动卷，使其持续复制到第二个集群，从而提供持续数据保护 (CDP)。

你需要什么

- 您必须拥有配对集群中一个或两个集群的集群管理员权限。
- 所有节点的 MIP 和 SIP 都相互路由。
- 集群间往返延迟小于 2000 毫秒。
- 两个存储集群都应该具有唯一的集群名称、MVIP、SVIP 和所有节点 IP 地址。
- 集群上 Element 软件版本之间的差异不超过一个主版本。如果差异较大，则必须升级其中一个集群以执行数据复制。

集群配对需要管理网络上的节点之间完全连通。复制需要存储集群网络上各个节点之间的连接。

您可以将一个集群与最多四个其他集群配对，以复制卷。您还可以将集群组内的不同集群相互配对。

使用 **MVIP** 或配对密钥对集群进行配对

如果两个集群都有集群管理员访问权限，则可以使用目标集群的 MVIP 将源集群和目标集群配对。如果集群管理员访问权限仅在集群对中的一个集群上可用，则可以在目标集群上使用配对密钥来完成集群配对。

1. 选择以下方法之一进行聚类配对：
   - "使用MVIP进行配对聚类"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。
   - "使用配对密钥配对簇"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。

查找更多信息

网络端口要求

使用**MVIP**进行配对聚类

你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。使用此方法需要对两个集群都具有集群管理员权限。在集群配对之前，需要使用集群管理员用户名和密码来验证集群访问权限。

1. 在本地集群上，选择“数据保护”>“集群对”。
2. 点击“配对集群”。
3. 单击“开始配对”，然后单击“是”，以表明您有权访问远程集群。
4. 输入远程集群MVIP地址。
5. 点击“完成远程集群配对”。

   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. 点击“配对集群”。
8. 点击“完成配对”。
9. 点击“完成配对”按钮。

查找更多信息

- 使用配对密钥配对簇
- "使用MVIP（视频）进行集群配对"

使用配对密钥配对簇

如果您拥有本地集群的集群管理员权限，但没有远程集群的集群管理员权限，则可以使用配对密钥将集群配对。在本地集群上生成配对密钥，然后安全地将其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，从而实现实时复制。

1. 在本地集群上，选择“数据保护”>“集群对”。
2. 点击“配对集群”。
3. 单击“开始配对”，然后单击“否”，表示您无权访问远程集群。
4. 点击“生成密钥”。

   此操作会生成用于配对的文本键，并在本地集群上创建一个未配置的集群对。如果您未完成此步骤，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. 使远程集群站点的集群管理员能够访问配对密钥。

   集群配对密钥包含 MVIP 版本、用户名、密码和数据库信息，以允许进行远程复制的卷连接。应妥善保管此密钥，不得以任何可能导致用户名或密码被意外或不安全访问的方式存储。

   请勿修改配对密钥中的任何字符。密钥一旦被修改，就会失效。

7. 在远程集群上，选择“数据保护”>“集群对”。
8. 点击“配对集群”。
9. 点击“完成配对”，然后在“配对密钥”字段中输入配对密钥（建议粘贴）。
10. 点击“完成配对”。

查找更多信息

- 使用MVIP进行配对聚类
- "使用聚类配对键进行聚类配对（视频）"

验证集群对连接

集群配对完成后，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“簇对”窗口中，验证簇对是否已连接。
3. *可选：*返回本地集群和*集群对*窗口，并验证集群对是否已连接。

对数

对数

在集群对中建立集群之间的连接后，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。建立卷配对关系时，必须确定哪个卷是复制目标。

您可以将存储在连接集群对中不同存储集群上的两个卷配对进行实时复制。将两个集群配对后，您可以配置一个集群上的活动卷，使其持续复制到第二个集群，从而提供持续数据保护 (CDP)。您还可以将任一卷指定为复制的源或目标。

销量配对始终是一对一的。卷与另一个集群上的卷配对后，就不能再与其他任何卷配对了。

你需要什么

- 您已在集群对中的集群之间建立了连接。
- 您拥有配对集群中的一个或两个集群的集群管理员权限。

步骤

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

创建具有读取或写入权限的目标卷

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

1. 选择“管理”>“卷”。
2. 点击“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，并选择应该有权访问该卷的帐户。
5. 点击“创建卷”。
6. 在“活动”窗口中，单击音量对应的“操作”图标。
7. 单击“编辑”。
8. 将帐户访问级别更改为“复制目标”。
9. 点击“保存更改”。

使用卷 ID 配对卷

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。

你需要什么

- 确保包含这些卷的集群已配对。
- 在远程集群上创建一个新卷。

> 配对过程完成后，您可以指定复制源和目标。复制源或目标可以是卷对中的任何一个卷。您应该创建一个不包含任何数据的目标卷，该目标卷具有与源卷完全相同的特征，例如大小、卷的块大小设置（512e 或 4k）和 QoS 配置。如果将现有卷指定为复制目标，则该卷上的数据将被覆盖。目标体积可以大于或等于源体积，但不能小于源体积。

- 知道目标卷的ID。

步骤

1. 选择“管理”>“卷”。
2. 点击要配对的音量对应的“操作”图标。
3. 点击“配对”。
4. 在“配对音量”对话框中，选择“开始配对”。
5. 选择“我愿意”表示您有权访问远程集群。
6. 从列表中选择一种*复制模式*：
   - 实时（异步）：写入操作在源集群上提交后，会向客户端发出确认。
   - 实时（同步）：写入操作在源集群和目标集群上都提交后，会向客户端发出确认。
   - 仅限快照：仅在源集群上创建的快照才会被复制。来自源卷的活动写入不会被复制。
7. 从列表中选择一个远程集群。
8. 选择远程卷 ID。
9. 点击“开始配对”。

   系统打开一个网页浏览器标签页，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. 请在“确认音量配对”中确认详细信息。
12. 点击“完成配对”。

    确认配对后，两个集群开始连接卷进行配对的过程。在配对过程中，您可以在“卷对”窗口的“卷状态”列中看到消息。音量对显示 `PausedMisconfigured`直到分配了源和目标卷对。

    配对成功后，建议您刷新卷表，从已配对卷的“操作”列表中删除“配对”选项。如果您不刷新表格，则“配对”选项仍然可供选择。如果您再次选择“配对”选项，则会打开一个新标签页，由于该音量已配对，系统会报告：

`StartVolumePairing Failed: xVolumeAlreadyPaired` Element UI 页面的“交易对数量”窗口中出现错误信息。

查找更多信息

- 音量配对消息
- 音量配对警告
- 为配对卷分配复制源和目标

使用配对密钥配对卷

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。

你需要什么

- 确保包含这些卷的集群已配对。
- 确保远程集群上有可用于配对的卷。

> 配对过程完成后，您可以指定复制源和目标。复制源或目标可以是卷对中的任何一个卷。您应该创建一个不包含任何数据的目标卷，该目标卷具有与源卷完全相同的特征，例如大小、卷的块大小设置（512e 或 4k）和 QoS 配置。如果将现有卷指定为复制目标，则该卷上的数据将被覆盖。目标体积可以大于或等于源体积，但不能小于源体积。

步骤

1. 选择“管理”>“卷”。
2. 点击要配对的音量对应的“操作”图标。
3. 点击“配对”。
4. 在“配对音量”对话框中，选择“开始配对”。
5. 选择“我没有”表示您没有访问远程集群的权限。
6. 从列表中选择一种*复制模式*：
   - 实时（异步）：写入操作在源集群上提交后，会向客户端发出确认。
   - 实时（同步）：写入操作在源集群和目标集群上都提交后，会向客户端发出确认。
   - 仅限快照：仅在源集群上创建的快照才会被复制。来自源卷的活动写入不会被复制。
7. 点击“生成密钥”。

> 此操作会生成用于配对的文本键，并在本地集群上创建一个未配置的卷对。如果您未完成此操作，则需要手动删除卷对。

8. 将配对密钥复制到电脑剪贴板。
9. 使远程集群站点的集群管理员能够访问配对密钥。

> 应妥善保管卷配对密钥，不得以任何可能导致意外或不安全访问的方式使用。

请勿修改配对密钥中的任何字符。密钥一旦被修改，就会失效。

10. 在远程集群 Element UI 中，选择“管理”>“卷”。
11. 点击要配对的音量对应的操作图标。
12. 点击“配对”。
13. 在“配对音量”对话框中，选择“完成配对”。
14. 将另一个集群中的配对密钥粘贴到“配对密钥”框中。
15. 点击“完成配对”。

    确认配对后，两个集群开始连接卷进行配对的过程。在配对过程中，您可以在“卷对”窗口的“卷状态”列中看到消息。音量对显示 `PausedMisconfigured`直到分配了源和目标卷对。

    配对成功后，建议您刷新卷表，从已配对卷的“操作”列表中删除“配对”选项。如果您不刷新表格，则“配对”选项仍然可供选择。如果您再次选择“配对”选项，则会打开一个新标签页，由于该音量已配对，系统会报告：`StartVolumePairing Failed: xVolumeAlreadyPaired` Element UI 页面的“交易对数量”窗口中出现错误信息。

查找更多信息

- 音量配对消息
- 音量配对警告
- 为配对卷分配复制源和目标

为配对卷分配复制源和目标

卷配对完成后，必须指定源卷及其复制目标卷。复制源或目标可以是卷对中的任何一个卷。如果源卷不可用，您还可以使用此过程将发送到源卷的数据重定向到远程目标卷。

你需要什么

您可以访问包含源卷和目标卷的集群。

步骤

1. 准备源卷：

   a. 从包含要指定为源的卷的集群中，选择“管理”>“卷”。
   b. 点击要指定为音源的音量旁边的“操作”图标，然后点击“编辑”。
   c. 在“访问”下拉列表中，选择“读/写”。

   如果要反转源和目标分配，此操作将导致卷对显示以下消息，直到分配新的复制目标为止：`PausedMisconfigured`

   更改访问权限会暂停卷复制，并导致数据传输停止。请务必协调好两个站点上的这些变更。

   a. 点击“保存更改”。

2. 准备目标体积：
    a. 从包含要指定为目标的卷的集群中，选择“管理”>“卷”。
    b. 单击要指定为目标的卷的“操作”图标，然后单击“编辑”。
    c. 在“访问”下拉列表中，选择“复制目标”。

> 如果将现有卷指定为复制目标，则该卷上的数据将被覆盖。您应该使用一个不包含任何数据的新目标卷，该目标卷具有与源卷完全相同的特征，例如大小、512e 设置和 QoS 配置。目标体积可以大于或等于源体积，但不能小于源体积。

    d. 点击“保存更改”。

查找更多信息

- 使用卷 ID 配对卷
- 使用配对密钥配对卷

验证卷复制

卷复制完成后，应确保源卷和目标卷处于活动状态。当处于活动状态时，卷已配对，数据正从源卷发送到目标卷，并且数据保持同步。

1. 在两个集群中，选择“数据保护”>“卷对”。
2. 确认卷状态为“活动”。

查找更多信息

音量配对警告

复制完成后删除卷关系

复制完成后，如果您不再需要卷对关系，则可以删除卷关系。

1. 选择“数据保护”>“卷对”。
2. 点击要删除的卷对旁边的“操作”图标。
3. 单击“删除”。
4. 确认消息。

管理交易量关系

暂停复制

如果需要暂时停止 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，则可以暂停复制。

1. 选择“数据保护”>“卷对”。

2. 点击音量对对应的操作图标。
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。请务必协调好两个站点上的这些变更。

5. 点击“保存更改”。

更改复制模式

您可以编辑卷对属性来更改卷对关系的复制模式。

1. 选择“数据保护”>“卷对”。
2. 点击音量对对应的操作图标。
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）：写入操作在源集群上提交后，会向客户端发出确认。
   - 实时（同步）：写入操作在源集群和目标集群上都提交后，会向客户端发出确认。
   - 仅限快照：仅在源集群上创建的快照才会被复制。来自源卷的活动写入不会被复制。 *注意：*更改复制模式会立即更改模式。请务必协调好两个站点上的这些变更。
5. 点击“保存更改”。

删除卷对

如果要移除两个卷之间的关联关系，可以删除卷对。

1. 选择“数据保护”>“卷对”。
2. 点击要删除的卷对旁边的“操作”图标。
3. 单击“删除”。
4. 确认消息。

删除一个簇对

您可以从元素 UI 中删除该对中的任一簇。

1. 点击“数据保护”>“集群对”。
2. 点击集群对的“操作”图标。
3. 在出现的菜单中，单击“删除”。
4. 确认此操作。
5. 从集群配对中的第二个集群再次执行这些步骤。

簇对详情

数据保护选项卡上的“集群配对”页面提供有关已配对或正在配对的集群的信息。系统会在“状态”列中显示配对和进度消息。

- **ID**

  系统为每个集群对生成一个ID。

- 远程集群名称

  这对簇中另一个簇的名称。

- 远程**MVIP**

  集群对中另一集群的管理虚拟 IP 地址。

- 地位

  远程集群的复制状态

- 正在复制卷

  集群中包含的用于复制的卷的数量。

- **UUID**

  为配对中的每个聚类分配一个唯一的 ID。

体积对

成交量对详情

数据保护选项卡上的“卷对”页面提供有关已配对或正在配对的卷的信息。系统会在“音量状态”列中显示配对和进度消息。

- **ID**

  系统生成的卷 ID。

- 姓名

  该卷创建时所起的名称。卷名最多可包含 223 个字符，并且包含 az、0-9 和破折号 (-)。

- 帐户

  分配给该卷的帐户名称。

- 音量状态

  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。可能的值如下：

  - 异步
  - 仅 Snapshot
  - 同步

- 方向

  成交量数据的方向：

  - 源音量图标（) 表示数据正在写入集群外部的目标。
  - 目标音量图标（) 表示数据正从外部源写入本地卷。

- 异步延迟

  自上次与远程集群同步以来经过的时间。如果该卷未配对，则其值为空。

- 远程集群

  卷所在的远程集群名称。

- 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。

音量配对消息

在初始配对过程中，您可以从“数据保护”选项卡下的“卷对”页面查看卷配对消息。这些消息可以显示在复制卷列表视图中源端和目标端的卷对中。

- 已暂停/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。

- 恢复连接

  远程复制同步现已激活。开始同步过程并等待数据。

- 恢复**RRSync**

  正在向配对集群创建卷元数据的单螺旋副本。

- 恢复本地同步

  正在将卷元数据的双螺旋副本复制到配对的集群中。

- 恢复数据传输

  数据传输已恢复。

- 积极的

  卷已配对，正在将数据从源卷发送到目标卷，且数据处于同步状态。

- 闲置的

  没有发生复制活动。

音量配对警告

在数据保护选项卡上的“卷对”页面中，配对卷后会显示这些消息。除非另有说明，否则这些消息可以显示在复制卷列表视图中的源端和目标端。

- 已暂停集群已满

  由于目标集群已满，源复制和批量数据传输无法进行。该消息仅显示在消息对的源端。

- 暂停超出最大快照计数

  目标卷已达到最大快照数量，无法复制更多快照。

- 暂停手动

  本地音量已手动暂停。必须先取消暂停，复制才能恢复。

- 已暂停手动遥控器

  远程音量处于手动暂停模式。需要手动干预才能暂停远程卷，然后才能恢复复制。

- 已暂停，配置错误

  等待活跃的源和目标。需要人工干预才能恢复复制。

- 暂停**QoS**

  目标QoS无法维持传入的IO。复制自动恢复。该消息仅显示在消息对的源端。

- 已暂停慢链接

  检测到慢速连接，已停止复制。复制自动恢复。该消息仅显示在消息对的源端。

- 暂停音量大小不匹配

  目标体积与源体积大小不同。

- 已暂停**XCopy**

  正在向源卷发出 SCSI XCOPY 命令。该命令必须完成，复制才能恢复。该消息仅显示在消息对的源端。

- 已停止，配置错误

  检测到永久性配置错误。远程音量已被清除或取消配对。无法采取任何纠正措施；必须重新配对。

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 的“数据保护”选项卡创建SnapMirror关系。必须启用SnapMirror功能才能在用户界面中看到此功能。

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SnapMirror功能，可将快照副本复制并恢复到NetApp ONTAP系统。使用此技术的主要原因是实现NetApp HCI到ONTAP的灾难恢复。端点包括ONTAP、 ONTAP Select和Cloud Volumes ONTAP。请参阅 TR-4641 NetApp HCI数据保护。

"NetApp技术报告 4641： NetApp HCI数据保护"

查找更多信息

- "使用NetApp HCI、 ONTAP和融合基础架构构建您的数据架构"
- "NetApp Element软件与ONTAP (ONTAP CLI) 之间的复制"

SnapMirror概述

运行NetApp Element软件的系统支持SnapMirror功能，可复制和恢复NetApp ONTAP系统的快照。

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 还包含管理 Element 软件和ONTAP系统之间SnapMirror关系所需的所有功能。

在特定用例中，您可以将ONTAP生成的卷复制到 Element 卷，但功能有限。有关详细信息，请参阅 "Element 软件与ONTAP (ONTAP CLI) 之间的数据复制"。

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。系统默认禁用SnapMirror功能，并且在新安装或升级时不会自动启用该功能。启用SnapMirror功能只需进行一次配置。

SnapMirror只能在运行 Element 软件的集群上启用，并且该软件必须与NetApp ONTAP系统上的卷一起使用。只有当您的集群连接到NetApp ONTAP卷以使用时，才应启用SnapMirror功能。

你需要什么

存储集群必须运行NetApp Element软件。

步骤

1. 点击“集群”>“设置”。
2. 查找SnapMirror的集群特定设置。
3. 点击“启用SnapMirror”。

> 启用SnapMirror功能会永久更改 Element 软件配置。只有将集群恢复到出厂映像，才能禁用SnapMirror功能并恢复默认设置。

4. 点击“是”确认SnapMirror配置更改。

在卷上启用**SnapMirror**

您必须在 Element UI 中启用卷上的SnapMirror。这样就可以将数据复制到指定的ONTAP卷。这是运行NetApp Element软件的集群管理员授予SnapMirror控制卷的权限。

你需要什么

- 您已在集群的 Element UI 中启用SnapMirror 。
- SnapMirror端点可用。
- 体积必须为 512e 块大小。
- 该卷未参与远程复制。
- 卷访问类型不是复制目标。

> 创建或克隆卷时也可以设置此属性。

步骤

1. 点击“管理”>“卷”。
2. 点击要启用SnapMirror的卷对应的 操作 图标。
3. 在出现的菜单中，选择“编辑”。
4. 在“编辑卷”对话框中，选中“启用SnapMirror”复选框。
5. 点击“保存更改”。

创建 **SnapMirror** 端点

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

SnapMirror端点是一个ONTAP集群，它充当运行 Element 软件的集群的复制目标。在创建SnapMirror关系之前，您需要先创建SnapMirror端点。

在运行 Element 软件的存储集群上，您可以创建和管理最多四个SnapMirror端点。

如果最初使用 API 创建了一个现有端点，但没有保存凭据，则可以在 Element UI 中看到该端点并验证其存在性，但无法使用 Element UI 对其进行管理。该端点只能使用 Element API 进行管理。

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

你需要什么

- 您应该在存储集群的 Element UI 中启用SnapMirror 。
- 您知道该终端的ONTAP凭据。

步骤

1. 点击“数据保护”>“SnapMirror端点”。
2. 点击“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. 输入与该终端关联的ONTAP管理员凭据。
5. 查看更多详情：
   - LIFs：列出用于与 Element 通信的ONTAP集群间逻辑接口。
   - 状态：显示SnapMirror端点的当前状态。可能的值有：已连接、已断开连接和未管理。
6. 点击“创建端点”。

创建 **SnapMirror** 关系

您必须在NetApp Element UI 中创建SnapMirror关系。

当卷尚未启用SnapMirror功能，并且您选择从 Element UI 创建关系时， SnapMirror将自动在该卷上启用。

你需要什么

该卷已启用SnapMirror 。

步骤

1. 点击“管理”>“卷”。
2. 点击要加入此关系的卷的*操作*图标。
3. 点击“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卷还是现有的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*存储虚拟机*。
   b. 从下拉列表中选择“聚合”。
   c. 在“卷名后缀”字段中，输入后缀。

系统检测源卷名称并将其复制到“卷名称”字段。您输入的后缀会附加到名称后面。

d. 单击“创建目标卷”。

7. 要使用现有的ONTAP卷，请单击“使用现有卷”。
   a. 为此关系选择*存储虚拟机*。
   b. 选择作为此新关系目标的卷。
8. 在“关系详情”部分，选择一项保单。如果所选策略有保留规则，则“规则”表会显示这些规则和相关的标签。
9. 可选：选择一个时间安排。

   这决定了该关系创建副本的频率。

10. 可选：在“限制带宽为”字段中，输入与此关系相关的数据传输可以消耗的最大带宽量。
11. 查看更多详情：
    - 状态：目标卷的当前关系状态。可能的值有：
      - 未初始化：目标卷尚未初始化。
      - snapmirrored：目标卷已初始化，可以接收SnapMirror更新。
      - 断开连接：目标卷是读/写卷，并且存在快照。
    - 状态：当前关系状态。可能的值有：空闲、传输、检查、静默、已静默、已排队、准备、完成、中止和中断。
    - 延迟时间：目标系统比源系统滞后的时间（以秒为单位）。滞后时间不得超过传输计划间隔。
    - 带宽限制：与此关系相关的数据传输可以使用的最大带宽量。
    - 上次传输时间：上次传输快照的时间戳。点击查看更多信息。
    - 策略名称：关系的ONTAP SnapMirror策略的名称。
    - 策略类型：为该关系选择的ONTAP SnapMirror策略类型。可能的值有：
      - 异步镜像
      - 镜像库
    - 日程名称： ONTAP系统中为该关系选择的现有日程的名称。
12. 如果此时不进行初始化，请确保未选中“初始化”复选框。

    初始化过程可能很耗时。您可能需要在非高峰时段运行此程序。初始化过程执行基线传输；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，也可以使用计划任务按照计划任务启动初始化过程（以及后续更新）。

13. 点击“创建关系”。
14. 点击“数据保护”> “SnapMirror关系”查看此新的SnapMirror关系。

SnapMirror关系操作

您可以在“数据保护”选项卡的“SnapMirror关系”页面中配置关系。这里介绍“操作”图标中的选项。

- 编辑：编辑关系中使用的策略或时间表。
- 删除：删除SnapMirror关系。此功能不会删除目标卷。
- 初始化：执行首次初始基线数据传输，以建立新的关系。
- 更新：按需更新关系，将自上次更新以来包含的任何新数据和快照副本复制到目标位置。
- 静默：阻止关系的任何进一步更新。
- 恢复：恢复一段已经中断的关系。
- 中断：将目标卷变为读写模式，并停止所有当前和未来的传输。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：以与断开之前相同的方向重新建立断开的关系。
- 反向重新同步：自动执行创建和初始化反向新关系所需的必要步骤。只有当现有关系破裂时，才能这样做。此操作不会删除当前关系。原始源卷恢复到最新的通用快照副本，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的新数据都会发送回原始源卷。
- 中止：取消当前正在进行的转账。如果对已中止的关系发出SnapMirror更新，则该关系将从中止发生之前创建的最后一个重启检查点的最后一次传输继续。

SnapMirror 标签

SnapMirror 标签

SnapMirror标签用作标记，用于根据关系的保留规则传输指定的快照。

给快照添加标签，即可将其标记为SnapMirror复制的目标。该关系的作用是通过选择匹配的标记快照，将其复制到目标卷，并确保保留正确数量的副本，从而在数据传输时强制执行规则。它指的是确定保留数量和保留期限的政策。该策略可以包含任意数量的规则，并且每条规则都有一个唯一的标签。此标签用作快照和保留规则之间的链接。

SnapMirror标签指示对选定的快照、组快照或计划应用了哪条规则。

给快照添加SnapMirror标签

SnapMirror标签指定SnapMirror端点上的快照保留策略。您可以为快照添加标签，也可以对快照进行分组。

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

向群组快照添加标签时，任何已存在于各个快照中的标签都将被覆盖。

你需要什么

- 集群上已启用SnapMirror 。
- 您想要添加的标签已存在于ONTAP中。

步骤

1. 点击“数据保护”>“快照”或“群组快照”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“编辑快照”对话框中，在“SnapMirror标签”字段中输入文本。标签必须与应用于SnapMirror关系的策略中的规则标签相匹配。
4. 点击“保存更改”。

向快照计划添加**SnapMirror**标签

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

你需要什么

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

步骤

1. 点击“数据保护”>“日程安排”。
2. 可以通过以下方式之一将SnapMirror标签添加到日程安排中：

选项	步骤
创建新日程	a. 选择“创建日程”。 b. 请填写所有其他相关信息。 c. 选择“创建日程”。
修改现有日程	a. 点击要添加标签的日程表的“操作”图标，然后选择“编辑”。 b. 在弹出的对话框中，在 * SnapMirror标签 * 字段中输入文本。 c. 选择“保存更改”。

查找更多信息

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功能断开连接并故障转移到目标卷。

如果原始集群完全失效或不存在，请联系NetApp支持部门以获取进一步帮助。

从 **Element** 集群执行故障转移

您可以从 Element 集群执行故障转移，使目标卷可读写，并可供目标端的主机访问。在从 Element 集群执行故障转移之前，必须断开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 CLI 发出断开关系命令。

你需要什么

- SnapMirror关系存在，并且目标卷上至少有一个有效的快照。
- 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. 找到与要故障转移的源卷的关系。
3. 点击“操作”图标。
4. 点击*中断*。
5. 确认此操作。

   目标集群上的卷现在具有读写访问权限，可以挂载到应用程序主机以恢复生产工作负载。此操作将导致所有SnapMirror复制停止。这段关系表明它已经破裂。

执行回退到 **Element** 的操作

了解如何执行故障恢复到 **Element** 模式

当主端的问题得到缓解后，您必须重新同步原始源卷并回退到NetApp Element软件。根据原始源卷是否存在，或者是否需要回退到新创建的卷，您需要执行的步骤会有所不同。

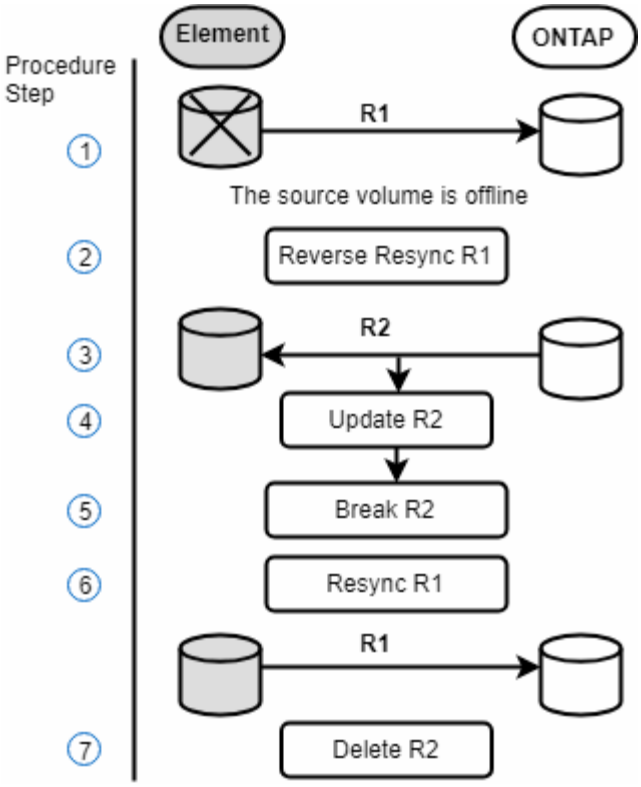
SnapMirror故障恢复场景

SnapMirror灾难恢复功能通过两种故障恢复场景进行说明。这些假设是原有的关系已经破裂（失败）。

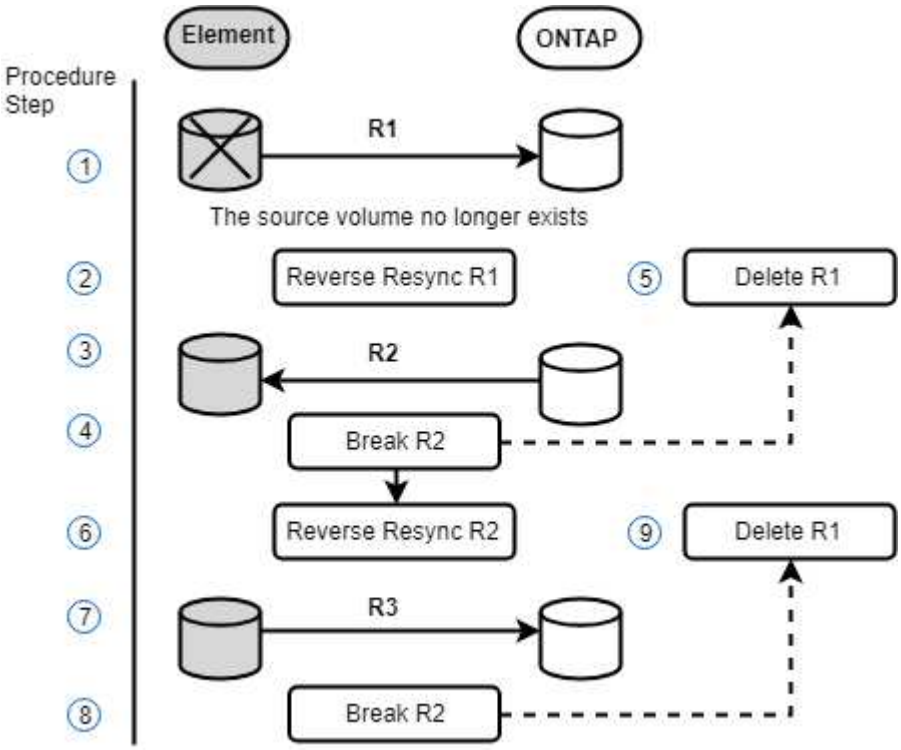
为便于参考，已将相应流程中的步骤列出。

> 在此示例中，R1 = 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 代表通过反向重新同步操作创建的反向关系。

下图显示了源卷仍然存在时的故障恢复场景：



下图显示了源卷不存在时的故障恢复方案：



查找更多信息

- 如果源卷仍然存在，则执行故障恢复。
- 当源卷不存在时，执行故障恢复。

- SnapMirror故障恢复场景

如果源卷仍然存在，则执行故障恢复。

您可以使用NetApp Element UI 重新同步原始源卷并进行故障恢复。此程序适用于原始源卷仍然存在的情况。

1. 在 Element UI 中，找到您为了执行故障转移而断开的关系。
2. 点击操作图标，然后点击*反向重新同步*。
3. 确认此操作。

> 反向同步操作会创建一个新的关系，其中原始源卷和目标卷的角色互换（这将导致两个关系，因为原始关系仍然存在）。作为反向重新同步操作的一部分，来自原始目标卷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的活动卷并向其写入数据，但您需要断开所有主机与源卷的连接，并在重定向回原始主卷之前执行SnapMirror更新。

4. 点击刚刚创建的反向关系的“操作”图标，然后点击“更新”。

   现在您已完成反向同步，并确保目标端的卷上没有活动会话，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. 点击反向关系的“操作”图标，然后点击“断开”。
6. 点击原始关系的操作图标，然后点击“重新同步”。

> 现在可以挂载原始主卷，以恢复原始主卷上的生产工作负载。原始SnapMirror复制将根据为该关系配置的策略和计划恢复。

7. 确认原始关系状态为“已镜像”后，点击反向关系的“操作”图标，然后点击“删除”。

查找更多信息

SnapMirror故障恢复场景

当源卷不存在时，执行故障恢复。

您可以使用NetApp Element UI 重新同步原始源卷并进行故障恢复。本节适用于原始源卷丢失但原始集群仍然完好无损的情况。有关如何恢复到新集群的说明，请参阅NetApp支持网站上的文档。

你需要什么

- Element 卷和ONTAP卷之间的复制关系已断开。
- 《元素》卷已彻底丢失。
- 原始卷名显示为“未找到”。

步骤

1. 在 Element UI 中，找到您为了执行故障转移而断开的关系。

最佳实践： 记下SnapMirror政策和原始破裂关系的日程安排详情。重建关系时需要这些信息。

2. 点击“操作”图标，然后点击“反向重新同步”。
3. 确认此操作。

> 反向重新同步操作会创建一个新的关系，其中原始源卷和目标卷的角色互换（这将导致两个关系，因为原始关系仍然存在）。由于原始卷已不存在，系统将创建一个新的 Element 卷，其卷名称和卷大小与原始源卷相同。新卷被分配了名为 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。

作为反向重新同步操作的一部分，最新快照中的数据传输到新卷。您可以继续访问目标端的活动卷并向其写入数据，但您需要断开所有主机与活动卷的连接，并在稍后的步骤中恢复原始主关系之前执行SnapMirror更新。完成反向同步后，请确保目标端卷上没有活动会话连接，并且最新数据位于原始主卷上，然后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. 单击在反向同步操作期间创建的反向关系的“操作”图标，然后单击“断开”。
5. 单击原始关系的“操作”图标（其中源卷不存在），然后单击“删除”。
6. 点击您在步骤 4 中断开的反向关系的 操作 图标，然后点击 反向重新同步。
7. 这将源和目标互换，从而得到与原始关系具有相同卷源和卷目标的关系。
8. 点击“操作”图标，然后点击“编辑”，即可使用您记下的原始 QoS 策略和计划设置更新此关系。
9. 现在可以安全地删除您在步骤 6 中反向同步的反向关系了。

查找更多信息

SnapMirror故障恢复场景

从**ONTAP**到 **Element** 执行传输或一次性迁移

通常情况下，当您使用SnapMirror从运行NetApp Element软件的SolidFire存储集群向ONTAP软件进行灾难恢复时，Element 是源， ONTAP是目标。然而，在某些情况下，ONTAP存储系统可以作为源，而 Element 作为目标。

- 存在两种情况：
  - 此前不存在灾难恢复合作关系。请按照此流程中的所有步骤操作。
  - 之前确实存在灾难恢复关系，但与用于此次缓解的卷之间不存在这种关系。在这种情况下，只需按照以下步骤 3 和 4 操作即可。

你需要什么

- 元素目标节点必须已对ONTAP开放。
- Element 卷必须已启用SnapMirror复制功能。

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创建与元素集群的关系：

```
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ONTAP snapmirror show 命令验证SnapMirror关系是否已创建。

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

3. 使用 `ElementCreateVolume`使用 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 体积

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

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

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

NetApp Element软件与ONTAP (ONTAP CLI) 之间的复制

NetApp Element软件与ONTAP之间的复制概览（ONTAP CLI）

您可以使用SnapMirror将 Element 卷的快照副本复制到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，然后在服务恢复后重新激活 Element 系统。

从ONTAP 9.4 开始，您可以将ONTAP节点上创建的 LUN 快照副本复制回 Element 系统。您可能在 Element 站点发生故障期间创建了 LUN，或者您可能正在使用 LUN 将数据从ONTAP迁移到 Element 软件。

如果符合以下条件，您应该使用 Element 进行ONTAP备份：

- 你应该采用最佳实践，而不是探索所有可行的方案。
- 您应该使用ONTAP命令行界面 (CLI)，而不是系统管理器或自动脚本工具。
- 您正在使用 iSCSI 向客户端提供数据。

如果您需要更多关于SnapMirror配置或概念方面的信息，请参阅"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 卷的快照副本复制到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，然后在服务恢复后重新激活 Element 源卷。

从ONTAP 9.4 开始，您可以将ONTAP节点上创建的 LUN 快照副本复制回 Element 系统。您可能在 Element 站点发生故障期间创建了 LUN，或者您可能正在使用 LUN 将数据从ONTAP迁移到 Element 软件。

数据保护关系类型

SnapMirror提供两种数据保护关系。对于每种类型， SnapMirror会在初始化或更新关系之前创建 Element 源卷的快照副本：

- 在灾难恢复 (DR) 数据保护关系中，目标卷仅包含SnapMirror创建的快照副本，在主站点发生灾难时，您可以从中继续提供数据。
- 在长期保留数据保护关系中，目标卷包含 Element 软件创建的时间点快照副本，以及SnapMirror创建的快照副本。例如，您可能希望保留 20 年间创建的每月快照副本。

默认策略

首次调用SnapMirror时，它会执行从源卷到目标卷的_基线传输_。 *SnapMirror* 策略 定义了基线的内容以及任何更新。

创建数据保护关系时，您可以使用默认策略或自定义策略。策略类型决定了要包含哪些快照副本以及要保留多少个副本。

下表显示了默认策略。使用 `MirrorLatest`制定建立传统DR关系的政策。使用 `MirrorAndVault`或者 `Unified7year`创建统一复制关系的策略，其中灾难恢复和长期保留配置在同一目标卷上。

策略	策略类型	更新行为
Mirror最新	async-mirror	传输由SnapMirror创建的快照副本。

MirrorAndVault	mirror-vault	传输由SnapMirror创建的快照副本以及自上次更新以来创建的任何较旧的快照副本，前提是它们带有SnapMirror标签“daily”或“weekly”。
Unified7year	mirror-vault	传输由SnapMirror创建的快照副本以及自上次更新以来创建的任何较旧的快照副本，前提是它们带有SnapMirror标签“daily”、“weekly”或“monthly”。

有关SnapMirror策略的完整背景信息，包括使用哪种策略的指南，请参阅"数据保护概述"。

了解**SnapMirror**标签

所有具有“mirror-vault”策略类型的策略都必须有一条规则，指定要复制哪些快照副本。例如，“daily”规则表示只有被赋予SnapMirror标签“daily”的快照副本才应该被复制。配置元素快照副本时，您可以分配SnapMirror标签。

从 **Element** 源集群到**ONTAP**目标集群的复制

您可以使用SnapMirror将 Element 卷的快照副本复制到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，然后在服务恢复后重新激活 Element 源卷。

Element 容量大致相当于ONTAP LUN。当 Element 软件和ONTAP之间建立数据保护关系时， SnapMirror会创建一个与 Element 卷同名的 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：

- 一个ONTAP卷只能包含来自一个 Element 卷的数据。
- 您无法将ONTAP卷中的数据复制到多个 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ONTAP系统上创建的 LUN 快照副本复制回 Element 卷：

- 如果 Element 源和ONTAP目标之间已经存在SnapMirror关系，则在从目标提供数据时创建的 LUN 会在源重新激活时自动复制。
- 否则，您必须在ONTAP源集群和 Element 目标集群之间创建并初始化SnapMirror关系。

复制规则如下：

- 复制关系必须具有“async-mirror”类型的策略。

  不支持类型为“mirror-vault”的策略。

- 仅支持 iSCSI LUN。
- 一次只能将ONTAP卷中的单个 LUN 复制到 Element 卷。
- 您无法将ONTAP卷中的 LUN 复制到多个 Element 卷。

前提条件

在配置 Element 和ONTAP之间的数据保护关系之前，您必须完成以下任务：

- Element 集群必须运行NetApp Element软件版本 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“`mirror-vault`”策略类型，则必须配置SnapMirror标签才能复制 Element 快照副本。

> 你只能在以下情况下执行此任务："Element 软件 Web 用户界面"或使用"API 方法"。

- 您必须确保端口 5010 可用。
- 如果您预见到可能需要移动目标卷，则必须确保源和目标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通信。

支持详情

下表显示了 Element 到ONTAP备份的支持详情。

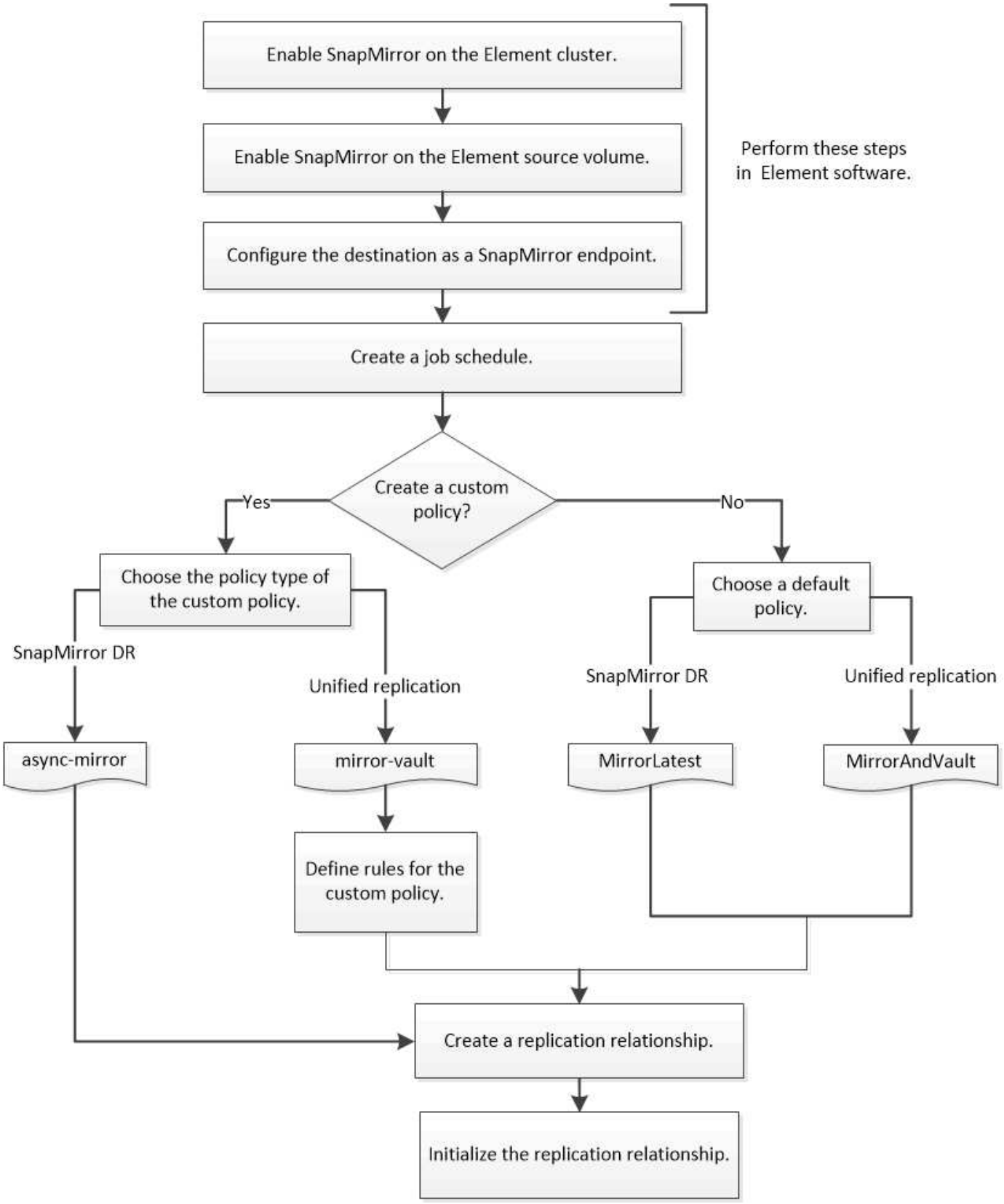
资源或功能	支持详情
SnapMirror	• 不支持SnapMirror恢复功能。 • 这 `MirrorAllSnapshots`和 `XDPDefault`不支持策略。 • 不支持“`vault`”策略类型。 • 系统定义的规则“`all_source_snapshots`”不受支持。 • “`mirror-vault`”策略类型仅支持从Element软件复制到ONTAP。使用“`async-mirror`”将ONTAP复制到 Element 软件。 • 这 `-schedule`和 `-prefix`选项 `snapmirror policy add-rule`不支持。 • 这 `-preserve`和 `-quick-resync`选项 `snapmirror resync`不支持。 • 存储效率无法保持。 • 不支持扇出式和级联式数据保护部署。
ONTAP	• ONTAP Select从ONTAP 9.4 和 Element 10.3 开始受支持。 • 从ONTAP 9.5 和 Element 11.0 开始支持Cloud Volumes ONTAP 。

Element	• 体积大小限制为 8 TiB。 • 卷块大小必须为 512 字节。不支持 4K 字节的块大小。 • 卷大小必须是 1 MiB 的倍数。 • 容量属性未被保留。 • 要复制的快照副本最大数量为 30。
网络	• 每次传输只允许建立一个 TCP 连接。 • 元素节点必须指定为 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。
支持向量机预测	SVM DR 配置中的ONTAP卷不受支持。
MetroCluster	MetroCluster配置中的ONTAP卷不受支持。

Element 和**ONTAP**之间复制的工作流程

无论您是将数据从 Element 复制到ONTAP，还是从ONTAP复制到 Element，您都需要配置作业计划、指定策略，并创建和初始化关系。您可以使用默认策略或自定义策略。

工作流程假定您已完成以下列出的先决任务："前提条件" 。有关SnapMirror策略的完整背景信息，包括使用哪种策略的指南，请参阅"数据保护概述"。



在 **Element** 软件中启用**SnapMirror**

在 **Element** 集群上启用**SnapMirror**

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

软件的 Web 用户界面中或使用以下方式执行此任务： "API 方法"。

开始之前

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

关于此任务

Element 系统默认禁用SnapMirror。 SnapMirror不会在新安装或升级过程中自动启用。

SnapMirror一旦启用，便无法禁用。只有将集群恢复到出厂映像才能禁用SnapMirror功能并恢复默认设置。

步骤

1. 点击“集群”>“设置”。
2. 查找SnapMirror的集群特定设置。
3. 点击“启用SnapMirror”。

在 **Element** 源卷上启用**SnapMirror**

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 软件的 Web 用户界面中或使用以下方式执行此任务："修改音量"和"修改卷"API 方法。

开始之前

- 您必须在 Element 集群上启用SnapMirror 。
- 卷块大小必须为 512 字节。
- 该卷不得参与 Element 远程复制。
- 卷访问类型不能是“复制目标”。

关于此任务

以下步骤假设卷已存在。创建或克隆卷时，也可以启用SnapMirror 。

步骤

1. 选择“管理”>“卷”。
2. 选择音量按钮。
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

您必须在 Element 集群上启用SnapMirror 。

步骤

1. 点击“数据保护”>“SnapMirror端点”。
2. 点击“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. 点击“创建端点”。

配置复制关系

创建复制作业计划

无论您是将数据从 Element 复制到ONTAP，还是从ONTAP复制到 Element，您都需要配置作业计划、指定策略，并创建和初始化关系。您可以使用默认策略或自定义策略。

你可以使用 `job schedule cron create`创建复制作业计划的命令。作业计划确定 SnapMirror 何时自动更新向其分配了计划的数据保护关系。

关于此任务

创建数据保护关系时，您需要指定一个工作计划。如果您不分配工作计划，则必须手动更新关系。

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
   ```

   为了 `-month`， `-dayofweek` ， 和 `-hour`您可以指定 `all`分别按月、按周、按小时运行该作业。

   从ONTAP 9.10.1 开始，您可以将 Vserver 添加到作业计划中：

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

   以下示例创建一个名为“ `my_weekly`每周六凌晨 3 点运行：

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

自定义复制策略

创建自定义复制策略

创建复制关系时，可以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_规则_，以确定在初始化和更新期间传输哪些快照副本。

如果关系的默认策略不合适，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尝试传输快照副本的次数。

关于此任务

复制策略的_策略类型_决定了它支持的关系类型。下表列出了可用的保单类型。

策略类型	关系类型
async-mirror	SnapMirror DR
mirror-vault	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，您可以使用以下方式指定为SnapMirror同步关系创建通用快照复制计划的计划： `-common-snapshot-schedule`范围。默认情况下， SnapMirror同步关系的常用快照复制计划为一小时。您可以为SnapMirror同步关系的快照复制计划指定 30 分钟到 2 小时之间的值。

   以下示例为SnapMirror DR 创建自定义复制策略，该策略启用数据传输的网络压缩：

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

   以下示例创建统一复制的自定义复制策略：

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

完成后

对于"mirror-vault"策略类型，您必须定义规则来确定在初始化和更新期间传输哪些快照副本。

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

为策略定义规则

对于"mirror-vault"策略类型的自定义策略，您必须至少定义一条规则来确定在初始化和更新期间传输哪些快照副本。您还可以使用"mirror-vault"策略类型定义默认策略的

规则。

关于此任务

所有具有“mirror-vault”策略类型的策略都必须有一条规则，指定要复制哪些快照副本。例如，“bi-monthly”规则表示只有分配了SnapMirror标签“bi-monthly”的快照副本才应该被复制。配置元素快照副本时，您可以分配SnapMirror标签。

每种策略类型都与一条或多条系统定义的规则相关联。当您指定策略类型时，这些规则会自动分配给该策略。下表显示了系统定义的规则。

系统定义的规则	用于政策类型	结果
sm_created	异步镜像，镜像库	SnapMirror创建的快照副本会在初始化和更新时传输。
每日	mirror-vault	初始化和更新时，源上带有SnapMirror标签“daily”的新快照副本将被传输。
weekly	mirror-vault	初始化和更新时，源上带有SnapMirror标签“weekly”的新快照副本将被传输。
月度	mirror-vault	初始化和更新时，源上带有SnapMirror标签“monthly` 的新快照副本将被传输。

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：

- 默认情况下 MirrorAndVault`策略方面，您可以创建一个名为“``bi-monthly”的规则，将源上的快照副本与带有“bi-monthly” SnapMirror标签的副本进行匹配。
- 对于具有“mirror-vault”策略类型的自定义策略，您可以创建一个名为“bi-weekly”的规则，以匹配源上带有“bi-weekly” SnapMirror标签的快照副本。

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。

   以下示例添加了一条带有SnapMirror标签的规则 `bi-monthly`恢复默认设置 `MirrorAndVault`政策：

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

以下示例添加了一条带有SnapMirror标签的规则 `bi-weekly`按照习俗 `my_snapvault`政策：

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

以下示例添加了一条带有SnapMirror标签的规则 `app_consistent`按照习俗 `Sync`政策：

```
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标签匹配的快照副本：

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

创建复制关系

创建从元素源到**ONTAP**目标的关联

主存储器中的源卷与辅助存储器中的目标卷之间的关系称为_数据保护关系_。你可以使用 `snapmirror create`用于创建从 Element 源到ONTAP目标，或从ONTAP源到 Element 目标的数据保护关系的命令。

您可以使用SnapMirror将 Element 卷的快照副本复制到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，然后在服务恢复后重新激活 Element 源卷。

开始之前

- 包含要复制的卷的 Element 节点必须已对ONTAP开放。
- Element 卷必须已启用SnapMirror复制功能。
- 如果您使用的是“`mirror-vault`”策略类型，则必须配置SnapMirror标签才能复制 Element 快照副本。

> 你只能在以下情况下执行此任务："Element 软件 Web 用户界面"或使用"API 方法"。

关于此任务

您必须在表单中指定元素源路径。 `<hostip:>/lun/<name>`其中“`lun`”是实际的字符串“`lun`”， `name`是元素卷的名称。

Element 容量大致相当于ONTAP LUN。当 Element 软件和ONTAP之间建立数据保护关系时， SnapMirror会创建一个与 Element 卷同名的 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的 LUN。

复制规则如下：

- 一个ONTAP卷只能包含来自一个 Element 卷的数据。
- 您无法将ONTAP卷中的数据复制到多个 Element 卷。

在ONTAP 9.3 及更早版本中，一个目标卷最多可以包含 251 个快照副本。在ONTAP 9.4 及更高版本中，目标卷最多可以包含 1019 个快照副本。

步骤

1. 从目标集群，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。

   以下示例使用默认值创建SnapMirror灾难恢复关系。 `MirrorLatest`政策：

   ```
   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
   ```

   以下示例使用默认值创建统一复制关系。 `MirrorAndVault`政策：

   ```
   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
   ```

   以下示例使用以下方式创建统一复制关系： `Unified7year`政策：

   ```
   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
   ```

   以下示例使用自定义创建统一复制关系。 `my_unified`政策：

   ```
   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`命令用于验证SnapMirror关系是否已创建。有关完整的命令语法，请参见手册页。

创建从**ONTAP**源到 **Element** 目标的关联

从ONTAP 9.4 开始，您可以使用SnapMirror将ONTAP源上创建的 LUN 快照副本复制回 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

- 元素目标节点必须已对ONTAP开放。
- Element 卷必须已启用SnapMirror复制功能。

关于此任务

您必须在表单中指定元素目标路径。 `<hostip:>/lun/<name>`其中"`lun`"是实际的字符串"`lun`"， `name`是元素卷的名称。

复制规则如下：

- 复制关系必须具有"`async-mirror`"类型的策略。

  您可以使用默认策略或自定义策略。

- 仅支持 iSCSI LUN。
- 一次只能将ONTAP卷中的单个 LUN 复制到 Element 卷。
- 您无法将ONTAP卷中的 LUN 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。

   以下示例使用默认值创建SnapMirror灾难恢复关系。 `MirrorLatest`政策：

   ```
   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
   ```

   以下示例使用自定义方式创建SnapMirror DR 关系。 `my_mirror`政策：

   ```
   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`命令用于验证SnapMirror关系是否已创建。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_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。

开始之前

- 包含要复制的卷的 Element 节点必须已对ONTAP开放。
- Element 卷必须已启用SnapMirror复制功能。
- 如果您使用的是“`mirror-vault`”策略类型，则必须配置SnapMirror标签才能复制 Element 快照副本。

> 你只能在以下情况下执行此任务："Element 软件 Web 用户界面"或使用"API 方法"。

关于此任务

您必须在表单中指定元素源路径。 `<hostip:>/lun/<name>`其中“`lun`”是实际的字符串“`lun`”， `*name*`是元素卷的名称。

初始化过程可能很耗时。您可能需要在非高峰时段运行基线传输。

> 如果由于任何原因导致从ONTAP源到 Element 目标的关系初始化失败，即使您已纠正了问题（例如，无效的 LUN 名称），它仍将继续失败。解决方法如下：
>
> 1. 删除这段关系。
> 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。

   以下示例初始化源卷之间的关系 `0005`IP 地址为 `10.0.0.11`，目标卷为 `volA_dst`在 `svm_backup`：

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

从SnapMirror DR 目标卷提供数据

使目标卷可写。

当灾难导致SnapMirror DR 关系的主站点无法工作时，您可以从目标卷提供数据，从而最大限度地减少中断。当主站点的服务恢复后，您可以重新激活源卷。

在能够将数据从卷提供给客户端之前，需要将目标卷设置为可写。你可以使用 `snapmirror quiesce`停止向目的地发送预定传输的命令 `snapmirror abort`下令停止正在进行的转账，以及 `snapmirror break`使目标位置可写的命令。

关于此任务

您必须在表单中指定元素源路径。 `<hostip:>/lun/<name>`其中"`lun`"是实际的字符串"`lun`"， `name`是元素卷的名称。

步骤

1. 停止前往目的地的预定接送服务：

   ```
   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。

   以下示例停止源卷之间的计划传输 `0005`IP地址为`10.0.0.11`，目标卷为 `volA_dst`在`svm_backup`：

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

2. 停止向目的地的持续转账：

   ```
   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。

   以下示例停止源卷之间的正在进行的传输 `0005`IP地址为`10.0.0.11`，目标卷为 `volA_dst`在`svm_backup`：

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

3. 终止与SnapMirror DR 的合作关系：

   ```
   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。

以下示例打破了源卷之间的关系 0005`IP 地址为 10.0.0.11，目标卷为 `volA_dst`在 `svm_backup`以及目的地数量 `volA_dst`在 `svm_backup：

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

配置数据访问的目标卷

将目标卷设置为可写后，必须配置该卷以进行数据访问。在源卷重新激活之前，SAN 主机可以访问目标卷中的数据。

1. 将元素 LUN 映射到相应的启动器组。
2. 从 SAN 主机发起程序创建到 SAN LIF 的 iSCSI 会话。
3. 在 SAN 客户端上，执行存储重新扫描以检测连接的 LUN。

重新激活原始源音量

当您不再需要从目标位置提供数据时，您可以重新建立源卷和目标卷之间的原始数据保护关系。

关于此任务

以下步骤假设原始源体积中的基线完好无损。如果基线不完整，则必须先创建并初始化从中提供数据的卷与原始源卷之间的关系，然后再执行该过程。

您必须在表单中指定元素源路径。 <hostip:>/lun/<name>`其中"`lun"是实际的字符串"lun"， `name`是元素卷的名称。

从ONTAP 9.4 开始，当您从ONTAP目标提供数据时创建的 LUN 快照副本会在 Element 源重新激活时自动复制。

复制规则如下：

- 仅支持 iSCSI LUN。
- 一次只能将ONTAP卷中的单个 LUN 复制到 Element 卷。
- 您无法将ONTAP卷中的 LUN 复制到多个 Element 卷。

步骤

1. 删除原数据保护关系：

   ```
   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。

   以下示例删除了原始源卷之间的关系， 0005 IP 地址为 10.0.0.11，以及您正在从中提供数据的卷，volA_dst`在 `svm_backup：

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

2. 颠覆原有的数据保护关系：

   ```
   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，但可能会很耗时。您可能需要在非高峰时段运行重新同步操作。

   以下示例颠倒了原始源卷之间的关系， `0005` IP 地址为 10.0.0.11，以及您正在从中提供数据的卷，`volA_dst`在 `svm_backup`：

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

3. 更新反向关系：

   ```
   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快照副本，则该命令会失败。使用 `snapmirror initialize`重新初始化关系。

   以下示例更新了您正在从中提供数据的卷之间的关系： `volA_dst`在 `svm_backup`以及原始资料卷，`0005` IP地址为10.0.0.11：

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

4. 停止反向关系的预定转账：

   ```
   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。

   以下示例会停止您正在从中提供数据的卷之间的计划传输： `volA_dst`在 `svm_backup`以及原始资料卷， `0005` IP地址为10.0.0.11：

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

5. 停止反向转账：

   ```
   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。

   以下示例停止您正在从中提供数据的卷之间的正在进行的传输： `volA_dst`在 `svm_backup`以及原始资料卷， `0005` IP地址为10.0.0.11：

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

6. 打破这种反向关系：

   ```
   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。

   以下示例打破了您正在提供数据的卷之间的关系， `volA_dst`在 `svm_backup`以及原始资料卷， `0005` IP地址为10.0.0.11：

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

7. 删除反向数据保护关系：

   ```
   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。

   以下示例删除了原始源卷之间的反向关系， `0005` IP 地址为 10.0.0.11，以及您正在从中提供数据的卷， `volA_dst`在 `svm_backup`：

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

8. 重建原有的数据保护关系：

   ```
   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。

以下示例重新建立了原始源卷之间的关系， 0005 IP 地址为 10.0.0.11，原始目标卷为： volA_dst`在 `svm_backup：

```
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`命令用于验证SnapMirror关系是否已创建。有关完整的命令语法，请参见手册页。

手动更新复制关系

如果由于网络错误导致更新失败，您可能需要手动更新复制关系。

关于此任务

您必须在表单中指定元素源路径。 <hostip:>/lun/<name>`其中"`lun"是实际的字符串"lun"， `name`是元素卷的名称。

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快照副本，则该命令会失败。使用 `snapmirror initialize`重新初始化关系。

   以下示例更新了源卷之间的关系 0005`IP地址为10.0.0.11，目标卷为 `volA_dst`在 `svm_backup：

   ```
   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

在将目标卷设置为可写之后、由于源卷和目标卷上不存在公共快照副本而导致更新失败之后，或者如果要更改关系的复制策略，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，但可能会很耗时。您可能需要在非高峰时段运行重新同步操作。

您必须在表单中指定元素源路径。 `<hostip:>/lun/<name>`其中"`lun`"是实际的字符串"lun"， `name`是元素卷的名称。

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。

   以下示例重新同步源卷之间的关系 `0005`IP地址为`10.0.0.11`，目标卷为 `volA_dst`在`svm_backup`：

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

备份和恢复卷

备份和恢复卷

您可以将卷备份和恢复到其他SolidFire存储，以及与 Amazon S3 或 OpenStack Swift 兼容的辅助对象存储。

从 OpenStack Swift 或 Amazon S3 恢复卷时，需要原始备份过程中的清单信息。如果您要恢复备份在SolidFire存储系统上的卷，则不需要清单信息。

查找更多信息

- 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 对象存储的备份恢复卷
- 从备份恢复 OpenStack Swift 对象存储中的卷
- 从SolidFire存储集群上的备份恢复卷

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. 点击"管理">"卷"。
2. 单击要备份的卷的"操作"图标。
3. 在出现的菜单中，单击"备份到"。
4. 在"集成备份"对话框的"备份到"下，选择"S3"。

5. 在“数据格式”下选择一个选项：
   - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
   - 未压缩：一种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“密钥”字段中输入帐户的密钥。
9. 在“S3 存储桶”字段中输入要存储备份的 S3 存储桶。
10. 在“姓名标签”字段中输入要附加到前缀的姓名标签。
11. 点击“开始阅读”。

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. 点击“管理”>“卷”。
2. 单击要备份的卷的“操作”图标。
3. 在出现的菜单中，单击“备份到”。
4. 在“集成备份”对话框的“备份到”下，选择“Swift”。
5. 在“数据格式”下选择数据格式：
   - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
   - 未压缩：一种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. 请在“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”字段中输入要存储备份的容器。
10. 可选：在 **Nametag** 字段中输入要附加到前缀的名称标签。
11. 点击“开始阅读”。

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配对。

看"复制的成对集群"。

当从一个集群备份或恢复到另一个集群时，系统会生成一个密钥，用于集群之间的身份验证。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程度的安全性。作为备份或恢复过程的一部分，您需要在开始操作之前从目标卷生成批量卷写入密钥。

1. 在目标集群上，管理 > 卷。

2. 单击目标卷的“操作”图标。
3. 在出现的菜单中，单击“从……恢复”。
4. 在“集成还原”对话框的“还原自”下，选择“SolidFire”。
5. 在“数据格式”下选择一个选项：
    - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
    - 未压缩：一种与其他系统兼容的未压缩格式。
6. 点击“生成密钥”。
7. 将“批量写入密钥”框中的密钥复制到剪贴板。
8. 在源集群上，转到“管理”>“卷”。
9. 单击要备份的卷的“操作”图标。
10. 在出现的菜单中，单击“备份到”。
11. 在“集成备份”对话框的“备份到”下，选择“SolidFire”。
12. 在“数据格式”字段中选择与之前相同的选项。
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. 在“批量卷写入密钥”字段中，粘贴您之前在目标集群上生成的密钥。
17. 点击“开始阅读”。

从 **Amazon S3** 对象存储的备份恢复卷

您可以从 Amazon S3 对象存储中的备份恢复卷。

1. 点击“报告”>“事件日志”。
2. 找到创建所需恢复备份的备份事件。
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. 点击“管理”>“卷”。
6. 单击要恢复的卷对应的“操作”图标。
7. 在出现的菜单中，单击“从……恢复”。
8. 在“集成还原”对话框的“还原来源”下，选择“S3”。
9. 在“数据格式”下选择与备份文件匹配的选项：
    - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
    - 未压缩：一种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“密钥”字段中输入帐户的密钥。
13. 在“S3 存储桶”字段中输入要存储备份的 S3 存储桶。
14. 将清单信息粘贴到“清单”字段中。
15. 点击“开始写作”。

从备份恢复 **OpenStack Swift** 对象存储中的卷

您可以从 OpenStack Swift 对象存储的备份中恢复卷。

1. 点击“报告”>“事件日志”。
2. 找到创建所需恢复备份的备份事件。
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. 点击“管理”>“卷”。
6. 单击要恢复的卷对应的“操作”图标。
7. 在出现的菜单中，单击“从……恢复”。
8. 在“集成还原”对话框的“还原来源”下，选择“Swift”。
9. 在“数据格式”下选择与备份文件匹配的选项：
   - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
   - 未压缩：一种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. 请在“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”字段中输入存储备份的容器名称。
14. 将清单信息粘贴到“清单”字段中。
15. 点击“开始写作”。

从**SolidFire**存储集群上的备份恢复卷

您可以从SolidFire存储集群上的备份恢复卷。

当从一个集群备份或恢复到另一个集群时，系统会生成一个密钥，用于集群之间的身份验证。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程度的安全性。作为备份或恢复过程的一部分，您需要在开始操作之前从目标卷生成批量卷写入密钥。

1. 在目标集群上，单击“管理”>“卷”。
2. 单击要恢复的卷对应的“操作”图标。
3. 在出现的菜单中，单击“从……恢复”。
4. 在“集成还原”对话框的“还原自”下，选择“SolidFire”。

5. 在“数据格式”下选择与备份文件匹配的选项：
   - 原生格式：一种仅能被SolidFire存储系统读取的压缩格式。
   - 未压缩：一种与其他系统兼容的未压缩格式。
6. 点击“生成密钥”。
7. 将*批量写入密钥*信息复制到剪贴板。
8. 在源集群上，单击“管理”>“卷”。
9. 单击要用于恢复的卷的“操作”图标。
10. 在出现的菜单中，单击“备份到”。
11. 在“集成备份”对话框中，选择“备份到”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. 将剪贴板中的密钥粘贴到“批量写入密钥”字段中。
17. 点击“开始阅读”。

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一个域。

分配保护域时，节点间会开始数据同步，在数据同步完成之前，某些集群操作将不可用。为集群配置自定义保护域后，添加新的存储节点时，必须先为该节点分配保护域并允许数据同步完成，才能为新节点添加驱动器。参观"保护域文档"了解更多关于保护域的信息。

要使自定义保护域方案对集群有用，每个机箱内的所有存储节点都必须分配到同一个自定义保护域。要实现这一点，您需要创建足够多的自定义保护域（最小的自定义保护域方案是三个域）。最佳实践是，为每个域配置相同数量的节点，并尽量确保分配给特定域的每个节点都是同一类型。

步骤

1. 点击“集群”>“节点”。
2. 点击“配置保护域”。

   在“配置自定义保护域”窗口中，您可以查看当前已配置的保护域（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”。

   对您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，请确保您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。如果您应用了保护域方案，并且需要立即进行更改，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. 点击“配置保护域”。

结果

根据集群规模的大小，域之间的数据同步可能需要一些时间。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 仪表板会在“自定义保护域运行状况”窗格中显示集群的保护状态。

可能出现的错误

以下是应用自定义保护域配置后可能会出现的一些错误：

错误	描述	解决方法
设置保护域布局失败：保护域布局会导致节点 ID {9} 无法使用。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。
设置保护域布局失败：保护域类型“custom”拆分了保护域类型“chassis”。	多节点机箱中的每个节点都被分配一个与其他节点不同的保护域。	确保机箱内的所有节点都分配到相同的保护域。

查找更多信息

- "自定义保护域"
- "使用 Element API 管理存储"

排查系统故障

系统事件

查看系统事件信息

您可以查看系统中检测到的各种事件的相关信息。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：

物品	描述
ID	每个事件都关联一个唯一的ID。
事件类型	记录的事件类型，例如 API 事件或克隆事件。
消息	与该事件相关的消息。

详细信息	有助于确定事件发生原因的信息。
Service ID	报告该事件的服务（如适用）。
节点	报告事件的节点（如果适用）。
驱动器 ID	报告该事件的驱动器（如果适用）。
Event Time	事件发生的时间。

查找更多信息

事件类型

事件类型

该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、正常的事件，也可以是需要管理员关注的事件。事件日志页面上的“事件类型”列指示事件发生在系统的哪个部分。

系统不会在事件日志中记录只读 API 命令。

以下列表描述了事件日志中出现的事件类型：

- **apiEvent**

  用户通过 API 或 Web UI 发起的、修改设置的事件。

- **binAssignmentsEvent**

  与数据箱分配相关的事件。箱子本质上是保存数据的容器，它们在集群中相互映射。

- **binSyncEvent**

  与数据在块服务之间重新分配相关的系统事件。

- **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。

- 批量操作事件

  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。

- 克隆事件

  与卷克隆相关的事件。

- 集群主事件

  集群初始化时或集群配置更改时（例如添加或删除节点）出现的事件。

- **cSumEvent**

  与端到端校验和验证过程中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将自动停止，并且在生成此事件后不会重新启动。

- 数据事件

  与数据读写相关的事件。

- **dbEvent**

  与集群中集成节点维护的全局数据库相关的事件。

- **driveEvent**

  与驱动操作相关的事件。

- **encryptionAtRestEvent**

  与集群加密过程相关的事件。

- 合奏活动

  与集合中节点数量增加或减少相关的事件。

- 光纤通道事件

  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，以回收块驱动器上的存储空间。这个过程也称为垃圾回收。

- **ieEvent**

  内部系统错误。

- 安装事件

  自动软件安装事件。软件正在自动安装到待处理的节点上。

- **iSCSI**事件

  与系统中的 iSCSI 问题相关的事件。

- **limitEvent**

  与账户或集群中的卷或虚拟卷数量接近允许的最大值相关的事件。

- 维护模式事件

  与节点维护模式相关的事件，例如禁用节点。

- **networkEvent**

  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。

  当 10 分钟监控间隔内，任何接口的错误计数超过默认阈值 1000 时，就会触发这些事件。这些事件适用于网络错误，例如接收丢失、循环冗余校验 (CRC) 错误、长度错误、溢出错误和帧错误。

- 平台硬件事件

  与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。

- 调度器事件

  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。

- 切片事件

  与 Slice 服务器相关的事件，例如删除元数据驱动器或卷。

  切片重新分配事件有三种类型，其中包含有关卷分配到的服务的信息：

  - 翻转：将主要服务更改为新的主要服务

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - 迁移：将辅助服务更改为新的辅助服务

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

  - 修剪：从一组服务中移除一个卷

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

- **snmpTrapEvent**

  与 SNMP 陷阱相关的事件。

- **statEvent**

  与系统统计相关的事件。

- **tsEvent**

  与系统传输服务相关的事件。

- 意外异常

  与意外系统异常相关的事件。

- **ureEvent**

  与从存储设备读取数据时发生的不可恢复的读取错误相关的事件。

- **vasaProviderEvent**

  与 VASA（vSphere APIs for Storage Awareness）提供程序相关的事件。

查看正在运行的任务的状态

您可以通过 Web UI 查看 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“报告”选项卡访问“正在运行的任务”页面。

如果任务数量很多，系统可能会将它们排队，然后分批运行。 “正在运行的任务”页面显示当前正在同步的服务。当一个任务完成后，它将被下一个排队的同步任务替换。同步任务可能会持续显示在“正在运行的任务”页面上，直到没有更多任务需要完成为止。

您可以在包含目标卷的集群的“正在运行的任务”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

您可以查看有关集群故障或系统错误的警报信息。警报可以是信息、警告或错误，是衡量集群运行状况的良好指标。大多数错误会自动解决。

您可以使用 ListClusterFaults API 方法自动执行警报监控。这样您就可以收到所有警报的通知。

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：

物品	描述
ID	与集群警报关联的唯一ID。
严重性	警报的重要性程度。可能值： • 警告：一个小问题，可能很快需要处理。系统升级仍然允许。 • 错误：可能导致性能下降或失去高可用性 (HA) 的故障。一般而言，这些错误不应影响服务的其他方面。 • 严重故障：影响服务的严重故障。系统无法处理 API 或客户端 I/O 请求。在这种状态下运行可能会导致数据丢失。 • 最佳实践：未使用推荐的系统配置最佳实践。
类型	受故障影响的部件。可以是节点、驱动器、集群、服务或卷。
节点	此故障所指节点的节点 ID。包含节点和驱动器故障，否则设置为 -（短横线）。
驱动器 ID	此故障所指的驱动器的驱动器 ID。包含驱动器故障，否则设置为 -（短横线）。
Error Code	用于描述故障原因的描述性代码。
详细信息	对故障的描述及更多细节。
日期	故障记录的日期和时间。

2. 点击“显示详情”查看单个警报的相关信息。
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，有关该警报的所有信息（包括解决日期）都会移至“已解决”区域。

查找更多信息

- 集群故障代码
- "使用 Element API 管理存储"

集群故障代码

系统通过生成故障代码来报告错误或可能感兴趣的状态，该故障代码列在“警报”页面上。这些代码可以帮助您确定系统的哪个组件收到了警报以及警报生成的原因。

以下列表概述了不同类型的代码：

- **authenticationServiceFault**

  一个或多个集群节点上的身份验证服务未按预期运行。

  联系 NetApp 支持部门获得帮助。

- 可用虚拟网络**IP**地址少

  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中添加更多 IP 地址。

- **blockClusterFull**

  没有足够的可用块存储空间可用于承受单节点丢失。有关集群填充程度的详细信息，请参阅 GetClusterFullThreshold API 方法。此集群故障表明存在以下情况之一：

  - stage3Low（警告）：已超过用户定义的阈值。调整集群已满设置或添加更多节点。
  - stage4Critical（错误）：没有足够的空间从 1 个节点故障中恢复。不允许创建卷、快照和克隆。
  - stage5完全消耗（严重）1；不允许写入或建立新的iSCSI连接。现有 iSCSI 连接将保持不变。在集群增加更多容量之前，写入操作将会失败。

  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。

- **blocksDegraded**

  由于故障，数据块不再完全复制。

严重性	描述
警告	只有两份完整的数据块副本可供访问。
错误	只能访问到数据块的完整副本。
批判的	无法获取完整的数据块副本。

  *注意：*此警告状态只会在三螺旋系统中出现。

  要解决此故障，请恢复任何离线节点或阻止服务，或联系NetApp支持寻求帮助。

- **blockServiceTooFull**

  一个块服务占用了过多的空间。

  要解决此故障，请增加已配置容量。

- 阻止服务不健康

  检测到某个阻塞服务运行状况不佳：

- 严重程度 = 警告：不采取任何措施。此警告期将在 cTimeUntilBSIsKilledMSec=330000 毫秒后到期。
- 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正常驱动器。
- 严重性 = 严重：多个节点上的块服务出现故障，故障数量大于或等于复制计数（双螺旋为 2）。数据不可用，箱体同步将无法完成。

  检查网络连接问题和硬件错误。如果特定硬件组件发生故障，则会出现其他故障。当阻塞服务恢复正常或服务停用后，故障将会清除。

- **BmcSelfTest**失败

  基板管理控制器（BMC）自检失败。

  请联系NetApp支持部门寻求帮助。

  在升级到 Element 12.5 或更高版本期间， `BmcSelfTestFailed`如果节点上的BMC已发生故障，或者节点的BMC在升级过程中发生故障，则不会生成故障。升级过程中自检失败的 BMC 将发出警告 `BmcSelfTestFailed`整个集群升级完成后出现警告故障。

- 时钟偏差超过故障阈值

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

  要解决此故障，请使用网络内部的 NTP 服务器，而不是安装默认服务器。如果您使用的是内部 NTP 服务器，请联系NetApp支持部门寻求帮助。

- 集群无法同步

  空间不足，离线块存储驱动器上的数据无法同步到仍在活动的驱动器。

  要解决此故障，请增加存储空间。

- 集群已满

  存储集群中已无可用存储空间。

  要解决此故障，请增加存储空间。

- 集群**IOPS**配置过高

  集群IOPS配置过高。所有最小 QoS IOPS 之和大于集群的预期 IOPS。无法同时为所有卷维持最低服务质量要求。

  要解决此问题，请降低卷的最小 QoS IOPS 设置。

- **CPU**热事件阈值

  一个或多个 CPU 上的 CPU 热事件数量超过了设定的阈值。

  如果在十分钟内未检测到新的 CPU 过热事件，则警告将自动解除。

- 禁用驱动器安全失败

集群未配置为启用驱动器安全（静态加密），但至少有一个驱动器启用了驱动器安全，这意味着禁用这些驱动器上的驱动器安全失败了。该故障被记录为“警告”级别。

要解决此故障，请检查故障详细信息，找出无法禁用驱动器安全功能的原因。可能的原因有：

- 无法获取加密密钥，请调查密钥访问或外部密钥服务器方面的问题。
- 驱动器上的禁用操作失败，请确定是否可能获取了错误的密钥。

  如果以上两种情况都不是故障原因，则可能需要更换硬盘。

即使提供了正确的身份验证密钥，如果驱动器无法成功禁用安全功能，您也可以尝试恢复该驱动器。要执行此操作，请将驱动器移至“可用”位置，从系统中移除驱动器，对驱动器执行安全擦除，然后将其移回“活动”位置。

- 已断开连接的集群对

  集群对已断开连接或配置错误。

  检查集群之间的网络连接。

- 已断开连接的远程节点

  远程节点已断开连接或配置错误。

  检查节点间的网络连接情况。

- 已断开连接的**SnapMirror**端点

  远程SnapMirror端点已断开连接或配置错误。

  检查集群与远程 SnapMirrorEndpoint 之间的网络连接。

- 可驾车

  集群中有一个或多个驱动器可用。一般来说，所有集群都应该添加所有驱动器，并且没有驱动器处于可用状态。如果此故障意外出现，请联系NetApp支持。

  要解决此故障，请将所有可用驱动器添加到存储集群。

- 驱动器故障

  当一个或多个驱动器发生故障时，集群会返回此故障，表明存在以下情况之一：

  - 驱动器管理器无法访问该驱动器。
  - 切片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造成的，无法重新启动。
  - 硬盘丢失。
  - 节点的主服务无法访问（节点中的所有驱动器均被视为丢失/故障）。
  - 硬盘已被锁定，无法获取硬盘的身份验证密钥。
  - 驱动器已锁定，解锁操作失败。

要解决此问题：

- 检查节点的网络连接情况。
- 更换硬盘。
- 请确保身份验证密钥可用。

- 驱动器健康故障

硬盘未通过 SMART 健康检查，因此，硬盘的功能有所降低。该故障的严重程度等级为“严重”：

- 序列号为 <序列号> 的驱动器，位于插槽：<节点插槽><驱动器插槽>，SMART 整体健康检查未通过。

要解决此故障，请更换驱动器。

- 驱动磨损故障

硬盘剩余寿命已低于阈值，但仍可正常工作。此故障有两种严重程度级别：严重和警告。

- 序列号为<序列号>的驱动器位于插槽：<节点插槽><驱动器插槽>，磨损程度严重。
- 序列号为<序列号>的驱动器位于插槽：<节点插槽><驱动器插槽>，磨损储备较低。

要解决此故障，请尽快更换硬盘。

- 重复集群主候选对象

检测到多个存储集群主节点候选者。

联系 NetApp 支持部门获得帮助。

- 启用驱动器安全失败

集群配置为需要驱动器安全（静态加密），但至少有一个驱动器无法启用驱动器安全。该故障被记录为“警告”级别。

要解决此故障，请检查故障详细信息，找出无法启用驱动器安全功能的原因。可能的原因有：

- 无法获取加密密钥，请调查密钥访问或外部密钥服务器方面的问题。
- 驱动器启用操作失败，请确定是否可能获取了错误的密钥。如果以上两种情况都不是故障原因，则可能需要更换硬盘。

即使提供了正确的身份验证密钥，如果驱动器无法成功启用安全功能，您也可以尝试恢复该驱动器。要执行此操作，请将驱动器移至“可用”位置，从系统中移除驱动器，对驱动器执行安全擦除，然后将其移回“活动”位置。

- 合奏退化

一个或多个集合节点已断开网络连接或已断电。

要解决此故障，请恢复网络连接或电源。

- 例外

报告的故障并非例行故障。这些故障不会自动从故障队列中清除。

联系 NetApp 支持部门获得帮助。

- 空间已满

  阻塞服务不响应数据写入请求。这会导致切片服务没有足够的空间来存储失败的写入操作。

  要解决此故障，请恢复块服务功能，以允许写入正常继续，并将故障空间从切片服务中刷新出来。

- 风扇传感器

  风扇传感器故障或缺失。

  要解决此故障，请更换任何故障硬件。

- 光纤通道接入降级

  一段时间内，光纤通道节点无法通过其存储 IP 响应存储集群中的其他节点。在这种状态下，节点将被视为无响应，并产生集群故障。

  检查网络连接。

- 光纤通道接入不可用

  所有光纤通道节点均无响应。显示节点 ID。

  检查网络连接。

- 光纤通道主动式**IxL**

  IxL Nexus 的数量已接近每个光纤通道节点 8000 个活动会话的支持上限。

  - 最佳实践限制为 5500。
  - 警告限值为 7500。
  - 最大限制（不强制执行）为 8192。

  要解决此故障，请将 IxL Nexus 数量减少到 5500 以下的最佳实践限制。

- 光纤通道配置

  此集群故障表明存在以下情况之一：

  - PCI 插槽上意外地出现了一个光纤通道端口。
  - 出现了一款意想不到的光纤通道 HBA 型号。
  - 光纤通道 HBA 的固件存在问题。
  - 光纤通道端口未上线。
  - 配置光纤通道直通功能时一直存在问题。

  联系 NetApp 支持部门获得帮助。

- 光纤通道**IOPS**

集群中光纤通道节点的总 IOPS 计数已接近 IOPS 限制。限制条件是：

- FC0025：每个光纤通道节点在 4K 块大小下 IOPS 限制为 450K。
- FCN001：每个光纤通道节点在 4K 块大小下，OPS 限制为 625K。

要解决此故障，请在所有可用的光纤通道节点上平衡负载。

- **fibreChannelStaticIxL**

  IxL Nexus 的数量已接近每个光纤通道节点支持的静态会话数上限 16000。

  - 最佳实践限制为 11000。
  - 警告限值为 15000。
  - 最大限制（强制执行）为 16384。

  要解决此故障，请将 IxL Nexus 数量减少到 11000 以下的最佳实践限制。

- **fileSystemCapacityLow**

  其中一个文件系统空间不足。

  要解决此故障，请增加文件系统的容量。

- **fileSystemIsReadOnly**

  文件系统已进入只读模式。

  联系 NetApp 支持部门获得帮助。

- **fips**驱动器不匹配

  将非 FIPS 驱动器物理插入到支持 FIPS 的存储节点中，或者将 FIPS 驱动器物理插入到非 FIPS 存储节点中。每个节点生成一个故障报告，列出所有受影响的驱动器。

  要解决此故障，请移除或更换有问题的不匹配的硬盘驱动器。

- **fipsDrivesOutOfCompliance**

  系统检测到启用 FIPS 驱动器功能后，静态数据加密功能被禁用。当启用 FIPS 驱动器功能并且存储集群中存在非 FIPS 驱动器或节点时，也会产生此故障。

  要解决此故障，请启用静态数据加密或从存储集群中移除非 FIPS 硬件。

- **fips**自检失败

  FIPS 子系统在自检过程中检测到故障。

  联系 NetApp 支持部门获得帮助。

- 硬件配置不匹配

  此集群故障表明存在以下情况之一：

- 配置与节点定义不匹配。
- 此类型的节点使用了不正确的驱动器容量。
- 检测到不支持的驱动器。一个可能的原因是已安装的 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。

联系 NetApp 支持部门获得帮助。

- **idPCertificateExpiration**

  集群的服务提供商 SSL 证书（用于第三方身份提供商 (IdP)）即将到期或已经到期。该故障根据紧急程度采用以下严重级别：

严重性	描述
警告	证书有效期为30天。
错误	证书有效期为7天。
批判的	证书将在3天内过期或已经过期。

  要解决此故障，请在 SSL 证书过期前更新它。使用 UpdateIdpConfiguration API 方法 `refreshCertificateExpirationTime=true`提供更新后的SSL证书。

- 不一致的键合模式

  VLAN 设备上的绑定模式缺失。此故障将显示预期的键合模式和当前使用的键合模式。

- 不一致的**Mtus**

  此集群故障表明存在以下情况之一：

  - Bond1G 不匹配：在 Bond1G 接口上检测到不一致的 MTU。
  - Bond10G 不匹配：在 Bond10G 接口上检测到不一致的 MTU。

  此故障会显示相关节点以及关联的 MTU 值。

- 路由规则不一致

  此接口的路由规则不一致。

- 子网掩码不一致

  VLAN 设备上的网络掩码与内部记录的 VLAN 网络掩码不匹配。此故障会显示预期的网络掩码和当前使用的网络掩码。

- 错误的**BondPortCount**

绑定端口的数量不正确。

- 无效的已配置光纤通道节点计数

  两个预期的光纤通道节点连接中，有一个连接性能下降。当仅连接一个光纤通道节点时，就会出现此故障。

  要解决此故障，请检查集群网络连接和网络布线，并检查是否存在故障服务。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**

  尝试平衡中断时发生异常。

  联系 NetApp 支持部门获得帮助。

- **kmip**证书故障
  - 根证书颁发机构（CA）证书即将到期。

    要解决此故障，请从根 CA 获取一个有效期至少还有 30 天的新证书，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，对其进行签名，确保新的到期日期至少还有 30 天，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 获取一个有效期至少还有 30 天的新证书，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，对其进行签名，确保新的到期日期至少还有 30 天，然后使用 ModifyKeyServerKmip 将过期的 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，请检查是否提供了正确的证书，如有必要，请从根 CA 重新获取证书。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，请检查是否已安装正确的 KMIP 客户端证书。客户端证书的根 CA 应该安装在 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正常运行且可通过网络访问。使用 TestKeyServerKimp 和 TestKeyProviderKmip 测试您的连接。

- 身份验证失败

  要解决此故障，请检查是否使用了正确的根 CA 和 KMIP 客户端证书，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，请检查错误详情。根据返回的错误信息，可能需要对外部密钥服务器进行故障排除。

- 内存**Ecc**阈值

检测到大量可纠正或不可纠正的ECC错误。该故障根据紧急程度采用以下严重级别：

事件	严重性	描述
单个 DIMM cErrorCount 达到 cDimmCorrectableErrWarnThreshold。	警告	DIMM 内存插槽上超过阈值的可纠正 ECC 内存错误：<处理器> <DIMM 插槽>
单个 DIMM 的 cErrorCount 会一直高于 cDimmCorrectableErrWarnThreshold，直到 DIMM 的 cErrorFaultTimer 超时为止。	错误	DIMM 内存条上超过阈值的可纠正 ECC 内存错误：<处理器> <DIMM>
内存控制器报告 cErrorCount 高于 cMemCtlrCorrectableErrWarnThreshold，并且指定了 cMemCtlrCorrectableErrWarnDuration。	警告	内存控制器上超过阈值的可纠正ECC内存错误：<处理器> <内存控制器>
内存控制器报告的 cErrorCount 超过 cMemCtlrCorrectableErrWarnThreshold，直到内存控制器的 cErrorFaultTimer 超时为止。	错误	DIMM 内存条上超过阈值的可纠正 ECC 内存错误：<处理器> <DIMM>
单个 DIMM 报告的 uErrorCount 大于零，但小于 cDimmUncorrectableErrFaultThreshold。	警告	DIMM 内存条上检测到不可纠正的 ECC 内存错误：<处理器> <DIMM 插槽>
单个 DIMM 报告的 uErrorCount 至少为 cDimmUncorrectableErrFaultThreshold。	错误	DIMM 内存条上检测到不可纠正的 ECC 内存错误：<处理器> <DIMM 插槽>

内存控制器报告的 uErrorCount 大于零，但小于 cMemCtlrUncorrectableErrFaultThreshold。	警告	内存控制器上检测到不可纠正的 ECC 内存错误：<处理器> <内存控制器>
内存控制器报告的 uErrorCount 至少为 cMemCtlrUncorrectableErrFaultThreshold。	错误	内存控制器上检测到不可纠正的 ECC 内存错误：<处理器> <内存控制器>

要解决此故障，请联系NetApp支持部门寻求帮助。

- 内存使用阈值

  内存使用量高于正常水平。该故障根据紧急程度采用以下严重级别：

  有关故障类型的更多详细信息，请参阅错误故障中的“详细信息”标题。

严重性	描述
警告	系统内存不足。
错误	系统内存严重不足。
批判的	系统内存已完全耗尽。

要解决此故障，请联系NetApp支持部门寻求帮助。

- **metadataClusterFull**

  可用的元数据存储空间不足以应对单个节点的丢失。有关集群填充程度的详细信息，请参阅 GetClusterFullThreshold API 方法。此集群故障表明存在以下情况之一：

  - stage3Low（警告）：已超过用户定义的阈值。调整集群已满设置或添加更多节点。
  - stage4Critical（错误）：没有足够的空间从 1 个节点故障中恢复。不允许创建卷、快照和克隆。
  - stage5完全消耗（严重）1；不允许写入或建立新的iSCSI连接。现有 iSCSI 连接将保持不变。在集群增加更多容量之前，写入操作将会失败。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**

  网络设备的 MTU 大小配置不正确。

  要解决此故障，请确保所有网络接口和交换机端口都配置为巨型帧（MTU 最大可达 9000 字节）。

- 网络配置

此集群故障表明存在以下情况之一：

- 未找到预期的接口。
- 存在重复接口。
- 已配置的接口已关闭。
- 需要重启网络。

联系 NetApp 支持部门获得帮助。

- 无可用虚拟网络**IP**地址

  该IP地址块中没有可用的虚拟网络地址。

  - virtualNetworkID # TAG(###) 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中添加更多 IP 地址。

- **nodeHardwareFault**（网络接口**<**名称**>**已关闭或网线已拔出）

  网络接口出现故障或网线被拔出。

  要解决此故障，请检查节点或多个节点的网络连接。

- **nodeHardwareFault**（驱动器加密功能状态与节点中插槽 **<**节点插槽**><**驱动器插槽**>** 内的驱动器的加密功能状态不匹配）

  硬盘的加密功能与其安装的存储节点不匹配。

- **nodeHardwareFault**（此节点类型的**<**驱动器类型**>**驱动器容量**<**实际容量**>**不正确 **-** 预期容量**>**）

  存储节点中包含一个容量与该节点不匹配的驱动器。

- **nodeHardwareFault**（在插槽**<**节点插槽**><**驱动器插槽**>**中检测到不支持的驱动器；驱动器统计信息和健康信息将不可用）

  存储节点中包含它不支持的驱动器。

- **nodeHardwareFault**（插槽 **<node slot><drive slot>** 中的驱动器应使用固件版本 **<expected version>**，但当前使用的是不支持的版本 **<actual version>**）

  存储节点中包含一个运行不受支持的固件版本的驱动器。

- 节点维护模式

  一个节点已置于维护模式。该故障根据紧急程度采用以下严重级别：

严重性	描述
警告	表示该节点仍处于维护模式。

错误	表示维护模式未能禁用，很可能是由于备用电源故障或处于活动状态所致。

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支持部门寻求帮助。

- **nodeOffline**

  Element软件无法与指定节点通信。检查网络连接。

- 未使用**LACP**债券模式

  LACP 绑定模式未配置。

  要解决此故障，请在部署存储节点时使用 LACP 绑定；如果未启用或正确配置 LACP，客户端可能会遇到性能问题。

- **ntp**服务器不可达

  存储集群无法与指定的 NTP 服务器通信。

  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的 NTP 服务器时间相差过大。存储集群无法自动纠正这种差异。

  要解决此故障，请使用网络内部的 NTP 服务器，而不是安装默认服务器。如果您使用的是内部 NTP 服务器且问题仍然存在，请联系NetApp支持部门寻求帮助。

- **nvramDeviceStatus**

  NVRAM设备出现错误、正在发生故障或已经发生故障。该故障的严重程度如下：

严重性	描述
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 • 能源来源生命周期状态 • 能源来源温度状态 • 警告阈值已超出

错误	硬件检测到错误或严重状态。集群主控尝试将切片驱动器从运行中移除（这将生成一个驱动器移除事件）。如果辅助分区服务不可用，则不会移除驱动器。除了警告级别的错误之外，还返回了以下错误： • NVRAM设备挂载点不存在。 • NVRAM设备分区不存在。 • NVRAM设备分区存在，但未挂载。
批判的	硬件检测到错误或严重状态。集群主控尝试将切片驱动器从运行中移除（这将生成一个驱动器移除事件）。如果辅助分区服务不可用，则不会移除驱动器。 • 持久性丢失 • armStatusSaveNArmed • csaveStatusError

更换节点中任何故障的硬件。如果此方法无法解决问题，请联系NetApp支持部门寻求帮助。

- 电源错误

  此集群故障表明存在以下情况之一：

  - 电源缺失。
  - 电源故障。
  - 电源输入缺失或超出范围。

  要解决此故障，请确认所有节点均已提供冗余电源。联系 NetApp 支持部门获得帮助。

- 预留空间已满

  集群的整体配置容量已满。

  要解决此故障，请添加更多已配置空间，或删除并清除卷。

- 远程复制异步延迟超过限制

  配置的异步复制延迟已超过设定值。检查集群间的网络连接。

- 远程副本集群已满

  由于目标存储集群已满，卷已暂停远程复制。

  要解决此故障，请释放目标存储集群上的一些空间。

- **remoteRepSnapshotClusterFull**

  由于目标存储集群已满，卷已暂停快照的远程复制。

要解决此故障，请释放目标存储集群上的一些空间。

- 远程副本快照超出限制

  由于目标存储集群卷已超出其快照限制，因此卷已暂停远程快照复制。

  要解决此故障，请增加目标存储集群上的快照限制。

- **scheduleActionError**

  一项或多项预定活动已运行，但失败了。

  如果计划的活动再次运行并成功，或者计划的活动被删除，或者活动被暂停并恢复，则故障将被清除。

- 传感器读取失败

  传感器无法与基板管理控制器（BMC）通信。

  联系 NetApp 支持部门获得帮助。

- 服务未运行

  所需服务未运行。

  联系 NetApp 支持部门获得帮助。

- **sliceServiceTooFull**

  切片服务的预置容量过少。

  要解决此故障，请增加已配置容量。

- **sliceServiceUnhealthy**

  系统检测到某个切片服务运行状况不佳，正在自动将其停用。

  - 严重程度 = 警告：不采取任何措施。此警告期将在 6 分钟后结束。
  - 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正常驱动器。

  检查网络连接问题和硬件错误。如果特定硬件组件发生故障，则会出现其他故障。当切片服务可访问或服务已停用时，故障将清除。

- 已启用 **SSH**

  SSH 服务已在存储集群中的一个或多个节点上启用。

  要解决此故障，请禁用相应节点上的 SSH 服务，或联系NetApp支持寻求帮助。

- **ssl**证书过期时间

  与此节点关联的 SSL 证书即将过期或已过期。该故障根据紧急程度采用以下严重级别：

严重性	描述

警告	证书有效期为30天。
错误	证书有效期为7天。
批判的	证书将在3天内过期或已经过期。

要解决此故障，请更新 SSL 证书。如有需要，请联系NetApp支持部门寻求帮助。

- 搁浅容量

  单个节点占用了存储集群一半以上的容量。

  为了保持数据冗余，系统会降低最大节点的容量，使其部分数据块容量闲置（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。

- 温度传感器

  温度传感器显示温度高于正常值。此故障可能与电源错误或风扇传感器故障同时触发。

  要解决此故障，请检查存储集群附近是否存在气流阻塞。如有需要，请联系NetApp支持部门寻求帮助。

- 升级

  升级工作已持续超过24小时。

  要解决此故障，请恢复升级或联系NetApp支持寻求帮助。

- 无响应服务

  服务已停止响应。

  联系 NetApp 支持部门获得帮助。

- 虚拟网络配置

  此集群故障表明存在以下情况之一：

  - 接口不存在。
  - 接口中存在错误的命名空间。
  - 子网掩码不正确。
  - IP地址错误。
  - 接口未启动并运行。
  - 节点上存在多余的接口。

  联系 NetApp 支持部门获得帮助。

- 音量降低

辅助卷尚未完成复制和同步。同步完成后，该消息将被清除。

- 卷离线

  存储集群中的一个或多个卷处于脱机状态。同时还会出现 **volumeDegraded** 故障。

  联系 NetApp 支持部门获得帮助。

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。该信息提供节点上每个驱动器的 CPU 和每秒读/写 I/O 操作数 (IOPS) 的实时统计信息。利用率图表每五秒更新一次，驱动器统计信息图表每十秒更新一次。

1. 点击“集群”>“节点”。
2. 点击要查看的节点的“操作”按钮。
3. 单击“查看详细信息”。

将光标悬停在折线图或柱状图上，即可查看折线图和柱状图上的特定时间点。

销量表现

查看音量表现

您可以查看集群中所有卷的详细性能信息。您可以按卷 ID 或任何性能列排序信息。您还可以按特定条件筛选信息。

您可以通过单击“刷新间隔”列表并选择不同的值来更改系统刷新页面上性能信息的频率。如果集群的卷少于 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”，则禁用自动页面刷新。

您可以点击“开启自动刷新”重新启用自动刷新功能。

1. 在 Element UI 中，选择“报告”>“音量性能”。
2. 在音量列表中，单击音量对应的“操作”图标。
3. 单击“查看详细信息”。

   页面底部会显示一个托盘，其中包含有关该卷的一般信息。

4. 要查看有关销量的更多详细信息，请点击*查看更多详情*。

   该系统会显示详细信息以及音量性能图表。

查找更多信息

销量表现详情

您可以在 Element UI 的“报告”选项卡的“卷性能”页面中查看卷的性能统计信息。

以下列表列出了您可以获取的详细信息：

- **ID**

  系统生成的卷 ID。

- 姓名

  该卷创建时所起的名称。

- 帐户

  分配给该卷的帐户名称。

- 访问组

  卷所属的卷访问组的名称。

- 容量利用率

  表示客户使用容量大小的百分比值。

  可能值：

  - 0 = 客户端未使用卷
  - 100 = 客户端正在使用最大值
  - >100 = 客户端正在使用突发模式

- 总**IOPS**

  当前正在对卷执行的 IOPS（读取和写入）总数。

- 读取**IOPS**

  当前正在对该卷执行的读取 IOPS 总数。

- 写入**IOPS**

  当前正在对该卷执行的写入 IOPS 总数。

- 总吞吐量

  当前正在对卷执行的总吞吐量（读取和写入）。

- 读取吞吐量

  当前正在对该卷执行的总读取吞吐量。

- 写入吞吐量

  当前正在对该卷执行的总写入吞吐量。

- 总延迟

  完成对卷的读取和写入操作的平均时间（以微秒为单位）。

- 读取延迟

  在过去 500 毫秒内完成对卷的读取操作的平均时间（以微秒为单位）。

- 写入延迟

  在过去 500 毫秒内完成对卷的写入操作的平均时间（以微秒为单位）。

- 队列深度

  卷上未完成的读取和写入操作的数量。

- 平均 **I/O** 大小

  最近 500 毫秒内对卷进行的最新 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。您可以筛选信息，只保留所需的会话。

1. 在 Element UI 中，选择“报告”>“iSCSI 会话”。
2. 要查看筛选条件字段，请点击“筛选”。

查找更多信息

iSCSI 会话详情

iSCSI 会话详情

您可以查看有关连接到集群的 iSCSI 会话的信息。

以下列表描述了您可以找到的有关 iSCSI 会话的信息：

- 节点

  托管该卷主元数据分区的节点。

- 帐户

  拥有该卷的账户名称。如果值为空，则显示短横线（-）。

- 体积

  节点上标识的卷名称。

- 卷号

  与目标 IQN 关联的卷的 ID。

- 发起方 **ID**

  系统生成的发起者 ID。

- 发起者别名

  发起者的一个可选名称，以便在长列表中更容易找到发起者。

- 发起方**IP**

  发起会话的端点的 IP 地址。

- 发起人 **IQN**

  发起会话的端点的 IQN。

- 目标**IP**地址

  卷所在的节点的 IP 地址。

- 目标**IQN**

  该体积的IQN。

- **CHAP**

  iSCSI 会话的 CHAP 算法。如果未使用 CHAP 算法，则会显示短横线 (-)。从 Element 12.8 版本开始可用。

- 创建于*

  会议成立日期。

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。您可以筛选信息，仅显示您希望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，请点击“筛选”。

查找更多信息

光纤通道会话详情

光纤通道会话详情

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。

以下列表描述了您可以找到的有关连接到集群的 FC 会话的信息：

- 节点 **ID**

  承载连接会话的节点。

- 节点名称

  系统生成的节点名称。

- 发起方 **ID**

  系统生成的发起者 ID。

- 发起人 **WWPN**

  起始全球港口名称。

- 发起者别名

  发起者的一个可选名称，以便在长列表中更容易找到发起者。

- 目标 **WWPN**

  目标全球端口名称。

- 卷访问组

  会话所属的卷访问组的名称。

- 卷访问组 ID

  系统生成的访问组 ID。

排除驱动器故障

排除驱动器故障

您可以将故障的固态硬盘 (SSD) 更换为新的硬盘。 SolidFire存储节点的 SSD 支持热插拔。如果您怀疑 SSD 出现故障，请联系NetApp支持部门以验证故障并指导您完成正确的故障排除步骤。 NetApp支持团队还会根据您的服务级别协议，协助您获得替换硬盘。

在这种情况下，“可更换”意味着您可以从活动节点中移除故障驱动器，并用NetApp的新 SSD 驱动器替换它。不

建议在活动集群中移除未发生故障的驱动器。

您应该按照NetApp支持部门的建议，在现场备有备用硬盘，以便在硬盘发生故障时立即进行更换。

> 为了进行测试，如果您要通过从节点中拔出驱动器来模拟驱动器故障，则必须等待 30 秒后才能将驱动器插入驱动器插槽。

如果某个硬盘发生故障，Double Helix 会将硬盘上的数据重新分配到集群中剩余的节点上。同一节点上的多个硬盘发生故障不是问题，因为 Element 软件可以防止同一节点上存在两份数据副本。硬盘故障会导致以下情况：

- 数据已从硬盘迁移出去。
- 集群总容量会因硬盘容量而减少。
- 双螺旋数据保护确保数据有两个有效副本。

> 如果移除驱动器会导致存储空间不足以迁移数据， SolidFire存储系统不支持移除驱动器。

了解更多信息

- 从集群中移除故障驱动器。
- MDSS驱动器基本故障排除
- 移除 MDSS 驱动器
- "更换SolidFire存储节点的硬盘"
- "更换 H600S 系列存储节点的硬盘"
- "H410S 和 H610S 硬件信息"
- "SF系列硬件信息"

从集群中移除故障驱动器。

如果硬盘的自诊断功能告诉节点硬盘发生故障，或者与硬盘的通信停止了五分半钟或更长时间， SolidFire系统会将硬盘置于故障状态。系统会显示故障硬盘列表。您必须从NetApp Element软件的故障驱动器列表中删除故障驱动器。

当节点离线时，警报 列表中的驱动器会显示为 **blockServiceUnhealthy**。重启节点时，如果节点及其驱动器在五分半钟内恢复联机，则驱动器会自动更新并继续作为集群中的活动驱动器。

1. 在 Element UI 中，选择“集群”>“驱动器”。
2. 点击“失败”查看失败的驱动器列表。
3. 记下故障硬盘的插槽编号。

   您需要这些信息来定位机箱中出现故障的硬盘。

4. 请使用以下方法之一移除故障硬盘：

选项	步骤

移除单个驱动器	a. 点击要删除的驱动器旁边的“操作”。 b. 单击“删除”。
移除多个驱动器	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”。

MDSS驱动器基本故障排除

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（或切片）驱动器重新添加到集群来恢复它们。如果节点上已启用 MDSS 功能，则可以在NetApp Element 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，切片服务将关闭，并且来自两个驱动器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出现的故障情况，并提供了纠正问题的基本建议：

系统切片驱动器故障

- 在这种情况下，槽位 2 经过验证后恢复为可用状态。
- 必须先重新安装系统切片驱动器，才能恢复切片服务。
- 当系统分区驱动器可用时，您应该更换系统分区驱动器，同时添加该驱动器和插槽 2 驱动器。

> 你不能单独将硬盘添加到插槽 2 中作为元数据硬盘。必须同时将两个硬盘添加到节点中。

插槽 **2** 故障

- 在这种情况下，系统切片驱动器经过验证后恢复到可用状态。
- 当插槽 2 可用时，应将插槽 2 更换为备用硬盘，同时添加系统切片硬盘和插槽 2 硬盘。

系统切片驱动器和插槽 **2** 故障

- 您应该将系统分区驱动器和插槽 2 都更换为备用驱动器。当两个硬盘都可用时，同时添加系统切片硬盘和插槽 2 硬盘。

操作顺序

- 用备用硬盘替换故障的硬件硬盘（如果两个硬盘都发生故障，则两个硬盘都需更换）。
- 当驱动器重新加载完毕且处于可用状态时，将其重新添加到集群中。

验证操作

- 确认插槽 0（或内部）和插槽 2 中的驱动器在“活动驱动器”列表中被识别为元数据驱动器。
- 确认所有切片平衡已完成（至少 30 分钟内事件日志中没有进一步移动切片的消息）。

了解更多信息

添加 MDSS 驱动器

添加 **MDSS** 驱动器

您可以通过将插槽 2 中的块驱动器转换为切片驱动器，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切片服务 (MDSS) 功能实现的。要启用此功能，您必须联系NetApp支持。

要使切片驱动器恢复可用状态，可能需要用新的或备用的驱动器替换故障驱动器。必须同时添加系统切片驱动器和插槽 2 的驱动器。如果尝试单独添加插槽 2 切片驱动器，或者在添加系统切片驱动器之前添加，系统将产生错误。

1. 点击“集群”>“驱动器”。
2. 点击“可用”查看可用驱动器列表。
3. 选择要添加的切片驱动器。
4. 点击“批量操作”。
5. 单击“添加”。
6. 在“活动驱动器”选项卡中确认驱动器已添加。

移除 **MDSS** 驱动器

您可以移除多驱动器切片服务 (MDSS) 驱动器。此步骤仅适用于节点具有多个切片驱动器的情况。

> 如果系统切片驱动器和插槽 2 驱动器发生故障，系统将关闭切片服务并移除驱动器。如果没有发生故障，要移除硬盘，则必须同时移除两个硬盘。

1. 点击“集群”>“驱动器”。
2. 在“可用驱动器”选项卡中，单击要移除的切片驱动器的复选框。
3. 点击“批量操作”。
4. 单击“删除”。
5. 确认此操作。

排查节点故障

从集群中移除节点

您可以从集群中移除节点以进行维护或更换。在将节点脱机之前，应使用NetApp Element UI 或 API 删除节点。

移除存储节点的步骤概述如下：

- 确保集群中有足够的容量来创建节点上的数据副本。

- 使用 UI 或 RemoveDrives API 方法从集群中移除驱动器。

  这样一来，系统就会将数据从节点的驱动器迁移到集群中的其他驱动器。这个过程所需的时间取决于需要迁移的数据量。

- 从集群中删除节点。

在关闭或启动节点之前，请注意以下事项：

- 如果操作不当，关闭节点和集群会带来风险。

  关闭节点电源的操作应在NetApp支持人员的指导下进行。

- 如果节点在任何类型的关机情况下停机超过 5.5 分钟，Double Helix 数据保护就会开始将单个复制块写入另一个节点以复制数据。在这种情况下，请联系NetApp支持部门，以获取有关分析故障节点的帮助。
- 要安全地重启或关闭节点，可以使用 Shutdown API 命令。
- 如果节点处于宕机或关闭状态，您必须先联系NetApp支持，然后才能将其重新联机。
- 节点恢复上线后，必须根据其停止服务的时间长短，将驱动器重新添加到集群中。

了解更多信息

"更换故障的SolidFire机箱"

"更换故障的 H600S 系列节点"

关闭集群电源

执行以下步骤关闭整个集群的电源。

步骤

1. （可选）联系NetApp支持以获取完成初步步骤的帮助。
2. 确认所有 I/O 操作均已停止。
3. 断开所有 iSCSI 会话：
   a. 导航到集群上的管理虚拟 IP (MVIP) 地址以打开 Element UI。
   b. 请注意节点列表中列出的节点。
   c. 对集群中的每个节点 ID 运行带有 halt 选项的 Shutdown API 方法。

> 重启集群时，必须按照以下步骤验证所有节点是否都已上线：
>
> 1. 验证所有严重级别和 `volumesOffline`集群故障已解决。
> 2. 等待 10 到 15 分钟，让集群稳定下来。
> 3. 开始启动主机以访问数据。
>
> 如果您希望在维护后启动节点并验证其健康状况时留出更多时间，请联系技术支持以获取延迟数据同步的帮助，以防止不必要的 bin 同步。

查找更多信息

"如何优雅地关闭和启动NetApp Solidfire/HCI 存储集群"

使用每个节点的存储节点实用程序

使用每个节点的存储节点实用程序

如果NetApp Element软件 UI 中的标准监控工具无法提供足够的故障排除信息，您可以使用每个节点的实用程序来排查网络问题。每个节点的实用程序提供特定的信息和工具，可以帮助您排查节点之间或与管理节点之间的网络问题。

查找更多信息

- 使用节点级用户界面访问每个节点的设置。
- 从每个节点的用户界面查看网络设置详情。
- 从每个节点的用户界面查看集群设置详情
- 使用节点级用户界面运行系统测试。
- 使用节点级用户界面运行系统实用程序

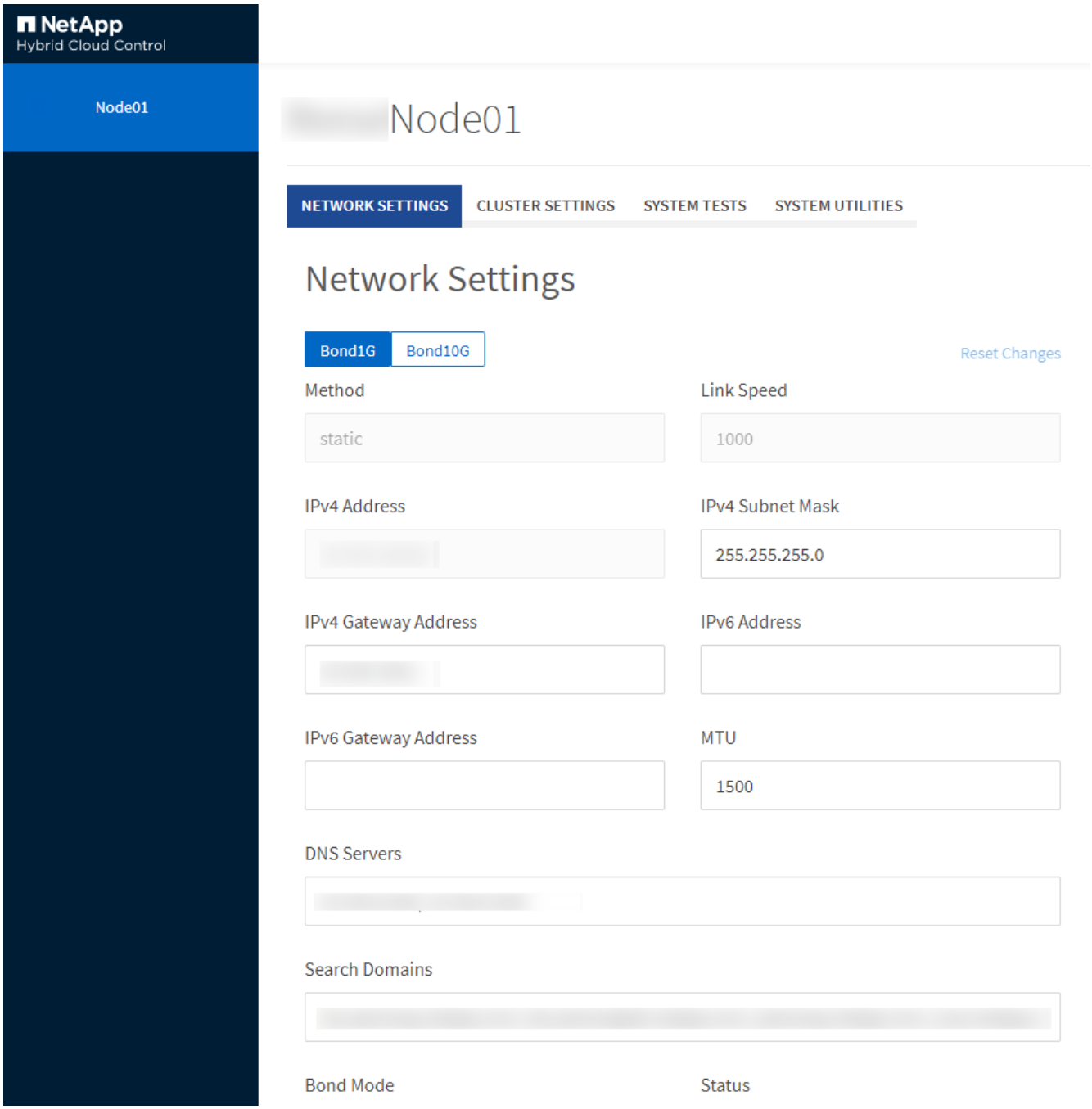
使用节点级用户界面访问每个节点的设置。

输入管理节点 IP 并进行身份验证后，即可在每个节点的用户界面中访问网络设置、集群设置、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，则必须以集群管理员用户身份登录。

您应该一次只配置或修改一个节点。在对其他节点进行修改之前，应确保指定的网络设置能够达到预期效果，并且网络稳定且运行良好。

1. 使用以下方法之一打开每个节点的用户界面：
   - 在浏览器窗口中输入管理 IP 地址，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。



从每个节点的用户界面查看网络设置详情。

您可以更改存储节点网络设置，为节点赋予一组新的网络属性。

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 回环接口。

- 手动：用于定义默认情况下不进行任何配置的接口。
- dhcp：用于通过 DHCP 获取 IP 地址。
- 静态：用于定义具有静态分配的 IPv4 地址的以太网接口。

- 链路速度

  虚拟网卡协商的速度。

- IPv4地址

  eth0 网络的 IPv4 地址。

- IPv4子网掩码

  IPv4 网络的地址细分。

- IPv4网关地址

  路由器网络地址，用于将数据包发送到本地网络之外。

- IPv6地址

  eth0 网络的 IPv6 地址。

- IPv6网关地址

  路由器网络地址，用于将数据包发送到本地网络之外。

- **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网卡，则该值应为 9000。

- DNS服务器

  用于集群通信的网络接口。

- 搜索域

  搜索系统中可用的其他 MAC 地址。

- 键合模式

  可以是以下几种模式之一：

  - 主动/被动（默认）
  - 艾尔布
  - LACP

- 地位

  可能值：

- 运行中
- 已关闭
- 已启动

- 虚拟网络标签

  虚拟网络创建时分配的标签。

- 路线

  通过配置使用的关联接口，指向特定主机或网络的静态路由。

从每个节点的用户界面查看集群设置详情

集群配置完成后，您可以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

  节点在集群中扮演的角色。可能值：

  - 存储：存储节点或光纤通道节点。
  - 管理：节点是管理节点。

- 主机名

  节点名称。

- 簇

  集群名称。

- 集群成员资格

  节点状态。可能值：

  - 可用：该节点没有关联的集群名称，并且尚未成为集群的一部分。
  - 待处理：节点已配置完毕，可以添加到指定的集群中。访问该节点无需身份验证。
  - 待激活：系统正在节点上安装兼容软件。完成后，节点将变为活动状态。
  - 活动状态：该节点正在参与集群。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。

- 合奏

  数据库集合中的节点。

- 节点 **ID**

  向集群添加节点时分配的 ID。

- 集群接口

  用于集群通信的网络接口。

- 管理界面

  管理网络接口。默认值为 Bond1G，但也可以使用 Bond10G。

- 存储接口

  使用 Bond10G 的存储网络接口。

- 具备加密功能

  指示节点是否支持驱动器加密。

使用节点级用户界面运行系统测试。

将网络设置更改提交到网络配置后，即可对其进行测试。您可以运行测试以确保存储节点稳定，并且可以毫无问题地上线。

您已登录到存储节点的单节点用户界面。

1. 点击“系统测试”。
2. 单击要运行的测试旁边的“运行测试”或选择“运行所有测试”。

   运行所有测试操作可能很耗时，并且只能在NetApp支持人员的指导下进行。

   - 测试连接集成

     测试并验证与数据库集合的连接性。默认情况下，测试使用节点所属集群的集成模型。或者，您可以提供不同的组件来测试连接性。

   - 测试连接**Mvip**

     ping 指定的管理虚拟 IP (MVIP) 地址，然后向 MVIP 执行简单的 API 调用以验证连接性。默认情况下，测试使用节点所属集群的 MVIP。

   - 测试连接**Svip**

     使用与网络适配器上设置的最大传输单元 (MTU) 大小相匹配的 Internet 控制消息协议 (ICMP) 数据包来 ping 指定的存储虚拟 IP (SVIP) 地址。然后它作为 iSCSI 发起程序连接到 SVIP。默认情况下，测试使用节点所属集群的 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。这与工

厂测试相同。

此测试会占用大量资源，仅应在NetApp支持部门要求时运行。

- 测试本地连接

  通过 ping 集群 IP (CIP) 来测试与集群中所有其他节点的连接性。只有当节点属于活动集群时，此测试才会显示在该节点上。

- 测试定位集群

  验证节点是否可以找到集群配置中指定的集群。

- 测试网络配置

  验证配置的网络设置与系统上使用的网络设置是否匹配。本测试并非旨在检测节点在集群中积极参与运行时发生的硬件故障。

- 测试 **Ping**

  对指定的主机列表进行 ping 操作；如果没有指定主机，则动态构建集群中所有已注册节点的列表，并对每个节点进行 ping 操作以实现简单的连接。

- 测试远程连接

  通过 ping 集群 IP (CIP) 来测试与远程配对集群中所有节点的连接性。只有当节点属于活动集群时，此测试才会显示在该节点上。

使用节点级用户界面运行系统实用程序

您可以使用存储节点的单节点 UI 来创建或删除支持包、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单节点用户界面。

1. 点击“系统实用工具”。
2. 单击要运行的系统实用程序对应的按钮。
   - 控制功率

     重启、断电或关闭节点。

     此操作会导致网络连接暂时中断。

     请指定以下参数：

     - 操作：选项包括重启和停止（关机）。
     - 唤醒延迟：节点重新上线前的任何额外时间。
   - 收集节点日志

在节点的 /tmp/bundles 目录下创建一个支持包。

请指定以下参数：

- 捆绑包名称：每个创建的支持捆绑包的唯一名称。如果没有提供名称，则使用“supportbundle”和节点名称作为文件名。
- 额外参数：此参数将传递给 sf_make_support_bundle 脚本。此参数仅应在NetApp支持部门要求时使用。
- 超时秒数：指定等待每个 ping 响应的秒数。

◦ 删除节点日志

删除节点上所有使用 创建集群支持包 或 CreateSupportBundle API 方法创建的当前支持包。

◦ 重置驱动器

初始化驱动器并删除驱动器上当前存储的所有数据。您可以将该驱动器重新用于现有节点或升级后的节点。

请指定以下参数：

- 驱动器：要重置的设备名称列表（不是驱动器 ID）。

◦ 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。在此操作过程中，所有数据将被删除，但节点的网络设置将被保留。只有当节点未分配给集群且处于可用状态时，才能重置节点。

使用此选项时，节点上的所有数据、软件包（软件升级）、配置和日志文件都将被删除。

◦ 重启网络连接

重启节点上的所有网络服务。

此操作可能会导致网络连接暂时中断。

◦ 重启服务

重启节点上的 Element 软件服务。

此操作可能会导致节点服务暂时中断。此操作应仅在NetApp支持人员的指导下执行。

请指定以下参数：

- 服务：要重启的服务名称。
- 操作：要对服务执行的操作。选项包括启动、停止和重启。

您可以使用管理节点 (mNode) 来升级系统服务、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支持访问权限以进行故障排除。

> 最佳实践是，只将一个管理节点与一个 VMware vCenter 实例关联，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。

看"管理节点文档"了解更多信息。

了解集群填充程度

运行 Element 软件的集群会在集群容量不足时生成集群故障，以警告存储管理员。集群填充程度分为三个级别，所有这些级别都会显示在NetApp Element UI 中：警告、错误和严重。

系统使用 BlockClusterFull 错误代码来警告集群块存储已满。您可以在 Element UI 的“警报”选项卡中查看集群满负荷严重级别。

以下列表包含有关 BlockClusterFull 严重级别的信息：

- 警告

  这是一个客户可配置的警告，当集群的块容量接近错误严重级别时，该警告会显示。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。您必须尽快增加容量或释放容量。

- 错误

  当集群处于这种状态时，如果一个节点丢失，集群中将没有足够的容量来重建双螺旋数据保护。如果集群处于此状态，则不允许创建新卷、执行克隆和生成快照。任何集群都不应处于这种安全或推荐的状态。您必须增加容量或立即释放容量。

- 批判的

  出现此严重错误是因为集群资源已 100% 使用。它处于只读状态，无法与集群建立新的 iSCSI 连接。达到这个阶段后，您必须立即释放或增加更多容量。

系统使用 MetadataClusterFull 错误代码来警告集群元数据存储空间已满。您可以在 Element UI 的“报告”选项卡的“概览”页面上的“集群容量”部分查看集群元数据存储已满情况。

以下列表包含有关 MetadataClusterFull 严重级别的信息：

- 警告

  这是一个客户可配置的警告，当集群的元数据容量接近错误严重级别时，该警告会显示。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。您必须尽快增加容量或释放容量。

- 错误

  当集群处于这种状态时，如果一个节点丢失，集群中将没有足够的容量来重建双螺旋数据保护。如果集群处于此状态，则不允许创建新卷、执行克隆和生成快照。任何集群都不应处于这种安全或推荐的状态。您必须

增加容量或立即释放容量。

- 批判的

  出现此严重错误是因为集群资源已 100% 使用。它处于只读状态，无法与集群建立新的 iSCSI 连接。达到这个阶段后，您必须立即释放或增加更多容量。

以下内容适用于双节点集群阈值：

- 元数据完整性错误率比临界值低 20%。
- 块容量不足错误是指比临界容量少 1 个块驱动器（包括闲置容量）；这意味着比临界容量少了 2 个块驱动器的容量。