



# 使用 **SANtricity** 解决方案 E-Series storage systems

NetApp  
March 12, 2026

# 目录

使用 SANtricity 解决方案	1
Web 服务代理	1
了解SANtricity Web服务代理	1
了解 Web 服务	1
安装和配置	8
在SANtricity Web服务代理中管理用户访问	18
在SANtricity Web服务代理中管理安全性和证书	21
使用SANtricity Web服务代理管理存储系统	24
管理SANtricity Web服务代理统计信息的自动轮询	28
使用SANtricity万维网服务代理管理AutoSupport	30
远程卷镜像	32
了解SANtricity远程存储卷	32
使用SANtricity远程存储卷的要求和限制	33
为SANtricity远程存储卷配置硬件	35
为SANtricity远程存储卷导入远程存储	37
管理SANtricity远程存储卷的导入进度	38
修改SANtricity远程存储卷的远程存储连接设置	39
删除SANtricity远程存储卷的远程存储对象	39
适用于 vCenter 的存储插件	40
了解适用于vCenter的SANtricity存储插件	40
入门	42
管理证书	55
管理阵列	61
导入设置	66
管理阵列组	72
升级操作系统软件	74
配置存储	79
配置主机	98
配置池和卷组	105
删除适用于vCenter的SANtricity存储插件	129
SANtricity Storage Plugin for vCenter 的常见问题解答	130
传统解决方案	143
云连接器	143

# 使用 SANtricity 解决方案

## Web 服务代理

### 了解SANtricity Web服务代理

SANtricity Web 服务代理是一种 RESTful API 服务器，单独安装在主机系统上，用于管理数百个新旧的 NetApp E 系列存储系统。此代理包含 SANtricity Unified Manager ，它是一个基于 Web 的界面，可提供类似的功能。

### 安装概述

安装和配置 Web 服务代理涉及以下步骤：

1. ["查看安装和升级要求"](#)。
2. ["下载并安装 Web 服务代理文件"](#)。
3. ["登录到 API 和 Unified Manager"](#)。
4. ["配置 Web 服务代理"](#)。

### 了解更多信息

- Unified Manager —此代理安装包括 SANtricity Unified Manager 。 Unified Manager 是一个基于 Web 的界面，可用于对较新的 E 系列和 EF 系列存储系统进行配置访问。有关详细信息，请参见 Unified Manager 联机帮助，该帮助可从其用户界面或获得 ["SANtricity 软件文档站点"](#)。
- 表述性状态传输（ Representational state transfer ， REST ） — Web 服务是一种 RESTful API ，可用于访问几乎所有 SANtricity 管理功能，因此您应熟悉 REST 概念。有关详细信息，请参见 ["架构模式和基于网络的软件架构设计"](#)。
- JavaScript 对象表示法（ JSON ） —由于 Web 服务中的数据是通过 JSON 进行编码的，因此您应熟悉 JSON 编程概念。有关详细信息，请参见 ["JSON 简介"](#)。

## 了解 Web 服务

### 了解SANtricity Web服务和Unified Manager

在安装和配置 Web 服务代理之前，请阅读 Web 服务和 SANtricity 统一管理器概述。

### Web 服务

Web 服务是一种应用程序编程接口（ Application Programming Interface ， API ），可用于配置，管理和监控 NetApp E 系列和 EF 系列存储系统。通过发出 API 请求，您可以完成 E 系列存储系统的配置，配置和性能监控等工作流。

使用 Web 服务 API 管理存储系统时，您应熟悉以下内容：

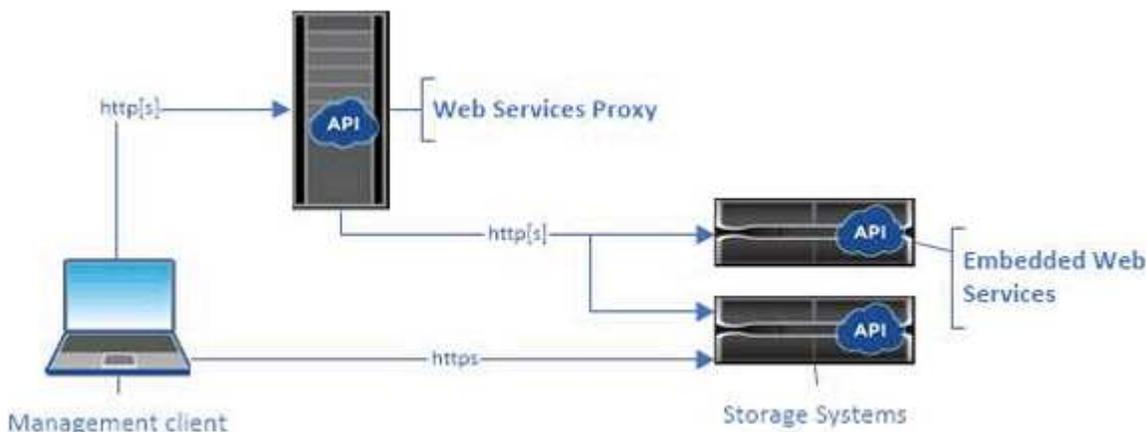
- JavaScript 对象表示法（ JSON ） —由于 Web 服务中的数据是通过 JSON 进行编码的，因此您应熟悉 JSON 编程概念。有关详细信息，请参见 ["JSON 简介"](#)。

- 表述性状态传输（Representational state transfer，REST）— Web 服务是一种 RESTful API，可用于访问几乎所有 SANtricity 管理功能，因此您应熟悉 REST 概念。有关详细信息，请参见 ["架构模式和基于网络的软件架构设计"](#)。
- 编程语言概念— Java 和 Python 是 Web 服务 API 中最常用的编程语言，但任何可发出 HTTP 请求的编程语言都足以进行 API 交互。

Web 服务有两种实施方式：

- 嵌入式—运行 NetApp SANtricity 11.30 或更高版本的 E2800/EF280 存储系统、运行 SANtricity 11.40 或更高版本的 E5700/EF570、运行 SANtricity 11.60 或更高版本的 EF300 或 EF600 以及运行 SANtricity 11.90 或更高版本的 E4000 的每个控制器上均嵌入了一个 RESTful API 服务器。无需安装。
- \* 代理 \* — SANtricity Web 服务代理是一种 RESTful API 服务器，单独安装在 Windows 或 Linux 服务器上。这款基于主机的应用程序可以管理数百个新旧 NetApp E 系列存储系统。通常，对于具有 10 个以上存储系统的网络，应使用代理。与嵌入式 API 相比，代理可以更高效地处理大量请求。

API 的核心可用于这两种实施方式。



下表对代理和嵌入式版本进行了比较。

注意事项	代理	嵌入式
安装	需要主机系统（Linux 或 Windows）。此代理可从下载 <a href="#">"NetApp 支持站点"</a> 或 <a href="#">"DockerHub"</a> 。	无需安装或启用。
安全性	默认情况下，最低安全设置。  安全设置较低，因此开发人员可以快速轻松地开始使用 API。如果需要，您可以为代理配置与嵌入式版本相同的安全配置文件。	默认情况下为高安全性设置。  安全设置较高，因为 API 直接在控制器上运行。例如，它不允许 HTTP 访问，并对 HTTPS 禁用所有 SSL 和较早的 TLS 加密协议。
集中管理	从一台服务器管理所有存储系统。	仅管理嵌入该控制器的控制器。

### Unified Manager

此代理安装包包含 Unified Manager，它是一个基于 Web 的界面，可用于对 E2800，E5700，EF300 和

EF600 等较新的 E 系列和 EF 系列存储系统进行配置访问。

在 Unified Manager 中，您可以执行以下批处理操作：

- 从中央视图查看多个存储系统的状态
- 发现网络中的多个存储系统
- 将设置从一个存储系统导入到多个系统
- 升级多个存储系统的固件

### SANtricity Web 服务代理的兼容性和限制

以下兼容性和限制适用于使用 Web 服务代理。

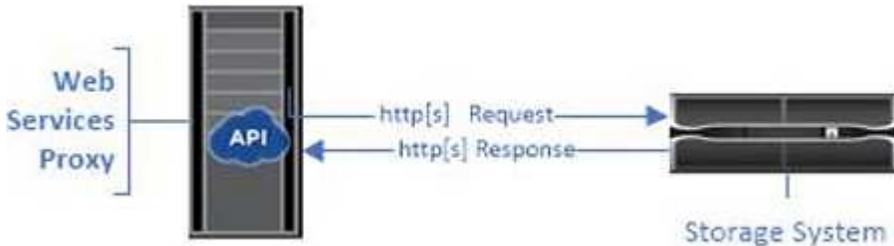
注意事项	兼容性或限制
HTTP 支持	Web 服务代理允许使用 HTTP 或 HTTPS。（出于安全原因，嵌入式版本的 Web 服务需要 HTTPS。）
存储系统和固件	Web 服务代理可以管理所有 E 系列存储系统，包括混合使用旧系统和最新的 E2800，EF280，E5700，EF570，EF300，和 EF600 系列系统。
IP 支持	Web 服务代理支持 IPv4 协议或 IPv6 协议。   当 Web 服务代理尝试从控制器配置自动发现管理地址时，IPv6 协议可能会失败。失败的可能原因包括在存储系统上启用 IP 地址转发或 IPv6 期间出现问题，但服务器上未启用 IPv6。
NVSRAM 文件名限制	Web 服务代理使用 NVSRAM 文件名来准确标识版本信息。因此，在将 NVSRAM 文件名与 Web 服务代理结合使用时，您无法更改这些文件名。Web 服务代理可能无法将重命名的 NVSRAM 文件识别为有效的固件文件。
符号 Web	符号 Web 是 REST API 中的 URL。它可以访问几乎所有符号调用。SYMBOL 函数属于以下 URL：  `+http://host:port/devmgr/storage-system/storage 数组 ID/ 符号 / 符号函数 +`   通过 Web 服务代理支持已禁用符号的存储系统。

## 了解SANtricity Web服务代理API基础知识

在 Web 服务 API 中， HTTP 通信涉及请求响应周期。

请求中的 URL 元素

无论使用何种编程语言或工具，每次对 Web 服务 API 的调用都具有类似的结构，其中包含 URL ， HTTP 动词和接受标头。



如以下示例所示，所有请求都包含一个 URL ， 并包含表中所述的元素。

` + <https://webservices.name.com:8443/devmgr/v2/storage-systems> + `

区域	Description
HTTP 传输  https : //	Web 服务代理支持使用 HTTP 或 HTTPS 。  出于安全原因，嵌入式 Web 服务需要 HTTPS 。
基本 URL 和端口  webservices.name.com:8443	每个请求都必须正确路由到 Web 服务的活动实例。需要提供实例的 FQDN （完全限定域名）或 IP 地址以及侦听端口。默认情况下， Web 服务通过端口 8080 （用于 HTTP ）和端口 8443 （用于 HTTPS ）进行通信。  对于 Web 服务代理，可以在代理安装期间或在 wsconfig.xml 文件中更改这两个端口。端口争用在运行各种管理应用程序的数据中心主机上很常见。  对于嵌入式 Web 服务，无法更改控制器上的端口；为了确保安全连接，默认为端口 8443 。

区域	Description
API 路径  devmgr/v2/storage-systems	<p>向 Web 服务 API 中的特定 REST 资源或端点发出请求。大多数端点采用以下形式：</p> <p>devmgr/v2/&lt; 资源 &gt;/[id]</p> <p>API 路径包含三部分：</p> <ul style="list-style-type: none"> <li>• devmgr （ Device Manager ） 是 Web 服务 API 的命名空间。</li> <li>• v2 表示要访问的 API 版本。您也可以使用 utils 访问登录端点。</li> <li>• s 存储系统 是文档中的一个类别。</li> </ul>

支持的 HTTP 动词

支持的 HTTP 动词包括 GET ， POST 和 DELETE ：

- 获取请求用于只读请求。
- POST 请求用于创建和更新对象，也用于可能涉及安全问题的读取请求。
- 删除请求通常用于从管理中删除对象，彻底删除对象或重置对象的状态。



目前， Web 服务 API 不支持 PUT 或修补程序。而是可以使用 POST 为这些动词提供典型功能。

接受标题

返回请求正文时， Web 服务将以 JSON 格式返回数据（除非另有说明）。某些客户端默认请求 "text/html" 或类似内容。在这些情况下， API 会以 HTTP 代码 406 进行响应，表示它无法提供此格式的数据。作为最佳实践，对于任何预期 JSON 为响应类型的情况，您应将 accept 标头定义为 "application/json"。在其他未返回响应正文的情况下（例如， delete ），如果接受标头不会发生原因任何意外影响，则会返回相应正文。

## Responses

向 API 发出请求时，响应将返回两个关键信息：

- HTTP 状态代码—指示请求是否成功。
- 可选响应正文—通常提供一个 JSON 正文来表示资源的状态，或者提供一个正文来提供有关故障性质的更多详细信息。

您必须检查状态代码和内容类型标题，以确定生成的响应正文。对于 HTTP 状态代码 200-203 和 422 ， Web Services 将返回一个 JSON 正文并返回响应。对于其他 HTTP 状态代码， Web 服务通常不会返回额外的 JSON 正文，因为规范不允许返回（ 204 ），或者因为状态不言自明。下表列出了常见的 HTTP 状态代码和定义。它还指示是否在 JSON 正文中返回与每个 HTTP 代码关联的信息。

HTTP 状态代码	Description	JSON 正文
200 正常	表示响应成功。	是的。

HTTP 状态代码	Description	JSON 正文
已创建 201	指示已创建对象。在极少数情况下会使用此代码，而不是 200 状态。	是的。
202 已接受	表示已接受此请求并将其作为异步请求进行处理，但您必须随后发出请求才能获得实际结果。	是的。
203 非权威信息	与 200 响应类似，但 Web 服务无法保证数据是最新的（例如，此时只能使用缓存的数据）。	是的。
204 无内容	表示操作成功，但没有响应正文。	否
400 个错误请求	指示请求中提供的 JSON 正文无效。	否
401 未授权	指示发生身份验证失败。未提供凭据，或者用户名或密码无效。	否
403 已禁用	授权失败，表示经过身份验证的用户无权访问请求的端点。	否
未找到 404	指示找不到请求的资源。此代码适用于标识符请求的不存在 API 或不存在的资源。	否
422 不可处理实体	表示请求格式通常良好，但输入参数无效或存储系统的状态不允许 Web 服务满足请求。	是的。
424 依赖关系失败	用于在 Web 服务代理中指示请求的存储系统当前不可访问。因此，Web 服务无法满足此请求。	否
429 个请求太多	表示已超过请求限制，应稍后重试。	否

了解SANtricity Web服务代理术语

以下术语适用于 Web 服务代理。

期限	定义
API	应用程序编程接口（Application Programming Interface，API）是一组协议和方法，可使开发人员与设备进行通信。Web 服务 API 用于与 E 系列存储系统进行通信。
ASUP	AutoSupport（ASUP）功能可收集客户支持包中的数据，并自动将消息文件发送给技术支持以进行远程故障排除和问题分析。
端点	端点是可通过 API 使用的功能。端点包括 HTTP 动词和 URI 路径。在 Web 服务中，端点可以执行发现存储系统和创建卷等任务。
HTTP 动词	HTTP 动词是端点对应的操作，例如检索和创建数据。在 Web 服务中，HTTP 动词包括 POST，GET 和 DELETE。
JSON	JavaScript 对象表示法（JavaScript Object Notation，JSON）是一种结构化数据格式，与 XML 非常相似，它使用的是最低可读格式。Web 服务中的数据通过 JSON 进行编码。
REST / RESTful	<p>表述性状态传输（Representational state transfer，REST）是一种宽松的规范，用于定义 API 的架构模式。由于大多数 REST API 不完全符合规范，因此它们被描述为 reSTful 或 reST 类。通常，“reSTful”API 与编程语言无关，并且具有以下特征：</p> <ul style="list-style-type: none"> <li>• 基于 HTTP，遵循协议的一般语义</li> <li>• 结构化数据（JSON，XML 等）的生产者和使用者</li> <li>• 面向对象（而不是面向操作）</li> </ul> <p>Web 服务是一种 RESTful API，可用于访问几乎所有 SANtricity 管理功能。</p>
存储系统	存储系统是 E 系列阵列，其中包括磁盘架，控制器，驱动器，软件，和固件。
符号 API	SYMBOL 是一种用于管理 E 系列存储系统的传统 API。Web 服务 API 的底层实施使用 SYMBOL。

期限	定义
Web 服务	Web 服务是 NetApp 为开发人员设计的一种 API，用于管理 E 系列存储系统。Web 服务有两种实施方式：嵌入在控制器上，一个单独的代理可以安装在 Linux 或 Windows 上。

## 安装和配置

查看**SANtricity Web**服务代理的安装和升级要求

在安装 Web 服务代理之前，请查看安装要求和升级注意事项。

### 安装要求

您可以在 Windows 或 Linux 主机系统上安装和配置 Web 服务代理。

代理安装包括以下要求。

要求	Description
主机名限制	请确保计划安装 Web 服务代理的服务器的服务器的主机名仅包含 ASCII 字母，数字和连字符（-）。此要求是由于 Java keytool 的限制所致，该工具用于为服务器生成自签名证书。如果服务器的主机名包含任何其他字符，例如下划线（_），则 Webserver 将无法在安装后启动。
操作系统	您可以在以下操作系统上安装代理： <ul style="list-style-type: none"> <li>• Linux</li> <li>• Windows</li> </ul> 有关操作系统和固件兼容性的完整列表，请参见 " <a href="#">NetApp 互操作性表工具</a> "。
Linux：其他注意事项	要使 Web 服务器正常运行，需要使用 Linux 标准基础库（init-function）。您必须为操作系统安装 lsb/inserv 软件包。有关详细信息，请参阅自述文件的 "所需的其他软件包" 部分。
多个实例	一个服务器上只能安装一个 Web 服务代理实例；但是，您可以在网络中的多个服务器上安装该代理。

要求	Description
容量规划	<p>Web 服务代理需要足够的空间来进行日志记录。确保您的系统满足以下可用磁盘空间要求：</p> <ul style="list-style-type: none"> <li>• 所需安装空间— 275 MB</li> <li>• 最小日志记录空间— 200 MB</li> <li>• 系统内存— 2 GB ； 堆空间默认为 1 GB</li> </ul> <p>您可以使用磁盘空间监控工具验证可用于永久性存储和日志记录的磁盘驱动器空间。</p>
许可证	<p>Web 服务代理是一款免费的独立产品，不需要许可证密钥。但是，适用的版权和服务条款仍适用。如果要在图形或控制台模式下安装代理，则必须接受最终用户许可协议（EULA）。</p>

#### 升级注意事项

如果要从先前版本升级，请注意，某些项目会保留或删除。

- 对于 Web 服务代理，将保留先前的配置设置。这些设置包括用户密码，所有已发现的存储系统，服务器证书，可信证书和服务器运行时配置。
- 对于 Unified Manager ， 先前加载在存储库中的所有 SANtricity OS 文件都会在升级期间删除。

#### 安装或升级SANtricity Web Services Proxy 和SANtricity Unified Manager 文件

安装涉及下载文件，然后在 Linux 或 Windows 服务器上安装代理软件包。您也可以按照以下说明升级代理。

#### 下载 Web 服务代理文件

您可以从 NetApp 支持站点的软件下载页面下载安装文件和自述文件。

下载包包括 Web 服务代理和 Unified Manager 界面。

#### 步骤

1. 转至 "[NetApp 支持—下载](#)"。
2. 选择 \* E 系列 SANtricity Web 服务代理 \* 。
3. 按照说明下载文件。请确保为您的服务器选择正确的下载包（例如，适用于 Windows 的 exe ； 适用于 Linux 的 BIN 或 RPM ） 。
4. 将安装文件下载到要安装代理和 Unified Manager 的服务器。

#### 在 Windows 或 Linux 服务器上安装

您可以使用以下三种模式之一（图形，控制台或静默）或 RPM 文件（仅限 Linux ）安装 Web 服务代理和 Unified Manager 。

## 开始之前

- ["查看安装要求"](#)。
- 确保已将正确的安装文件（适用于 Windows 的 exe ； 适用于 Linux 的 BIN ）下载到要安装代理和 Unified Manager 的服务器。

## 图形模式安装

您可以在图形模式下为 Windows 或 Linux 运行安装。在图形模式下，系统会在 Windows 模式界面中显示提示。

### 步骤

1. 访问下载安装文件的文件夹。
2. 启动 Windows 或 Linux 安装，如下所示：

- Windows —双击安装文件：

```
santricity_webservice-windows_x64-nn.nnn.nnnn.exe
```

- Linux —运行以下命令：`santricity_webservice-linux_x64-nn.nnn.nn.nnn.bin`

在上述文件名中，`nn.nn.nn.nnnn` 表示版本号。

安装过程将启动，此时将显示 NetApp SANtricity Web 服务代理 + Unified Manager 启动屏幕。

3. 按照屏幕上的提示进行操作。

在安装期间，系统会提示您启用多项功能并输入一些配置参数。如有必要，您可以稍后在配置文件中更改其中任何一个选项。



在升级期间、系统不会提示您输入配置参数。

4. 出现 Webserver started 消息时，单击 \* 确定 \* 完成安装。

此时将显示安装完成对话框。

5. 如果要启动 Unified Manager 或交互式 API 文档，请单击复选框，然后单击 \* 完成 \* 。

## 控制台模式安装

您可以在控制台模式下为 Windows 或 Linux 运行安装。在控制台模式下，终端窗口中会显示提示。

### 步骤

1. 运行以下命令：``<install filename> -i console``

在上述命令中，``<install filename>`` 表示您下载的代理安装文件的名称（例如：`santricity_webservice-windows_x64-n.nn.nn.nnnnn.exe`）。



要在安装过程中随时取消安装，请在命令提示符处键入 `quit`。

安装过程将开始，并显示启动安装程序 - 简介消息。

2. 按照屏幕上的提示进行操作。

在安装期间，系统会提示您启用多项功能并输入一些配置参数。如有必要，您可以稍后在配置文件中更改其中任何一个选项。



在升级期间、系统不会提示您输入配置参数。

3. 安装完成后，按 \* 输入 \* 退出安装程序。

### 静默模式安装

您可以在静默模式下为 Windows 或 Linux 运行安装。在静默模式下，终端窗口中不会显示任何返回消息或脚本。

#### 步骤

1. 运行以下命令：`<install filename> -i silent`

在上述命令中，`<install filename>` 表示您下载的代理安装文件的名称（例如：santricity\_webservice-windows\_x64-n.nn.nn.nnnnn.exe）。

2. 按 \* 输入 \*。

安装过程可能需要几分钟才能完成。成功安装后，终端窗口将显示命令提示符。

### rpm 命令安装（仅限 Linux）

对于与 RPM 软件包管理系统兼容的 Linux 系统，您可以使用可选的 RPM 文件安装 Web 服务代理。

#### 步骤

1. 将 RPM 文件下载到要安装代理和 Unified Manager 的服务器。
2. 打开终端窗口。
3. 输入以下命令：

```
rpm -U santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
```



在上述命令中，nn.nn.nn.nnnn 表示版本号。

安装过程可能需要几分钟才能完成。成功安装后，终端窗口将显示命令提示符。

### 登录到SANtricity Web服务代理API和Unified Manager

Web 服务包括 API 文档，您可以通过这些文档直接与 REST API 进行交互。它还包括 Unified Manager，这是一个基于浏览器的界面，用于管理多个 E 系列存储系统。

## 登录到 Web 服务 API

安装 Web 服务代理后，您可以在浏览器中访问交互式 API 文档。

API 文档随每个 Web 服务实例一起运行，也可以从 NetApp 支持站点获得静态 PDF 格式的文档。要访问交互式版本，请打开浏览器并输入指向 Web 服务所在位置的 URL（嵌入式版本的控制器或代理的服务器）。



Web 服务 API 实施 OpenAPI 规范（最初称为 Swagger 规范）。

首次登录时，请使用 "admin" 凭据。"admin" 被视为超级管理员，可以访问所有功能和角色。

### 步骤

1. 打开浏览器。
2. 输入嵌入式或代理实施的 URL：
  - 嵌入式：`https://<controller>:<port>/devmgr/docs/`
  - 代理：`+ http://<服务器>:<端口>/devmgr/docs/+`

在此 URL 中，`<控制器>` 是控制器的 IP 地址或 FQDN，`<端口>` 是控制器的管理端口号（默认为 8443）。

在此 URL 中，`<server>` 是安装了代理的服务器的 IP 地址或 FQDN，`<port>` 是侦听端口号（对于 HTTP，默认为 8080，对于 HTTPS，默认为 8443）。



如果侦听端口已在使用中，则代理会检测到冲突并提示您选择其他侦听端口。

此时将在浏览器中打开 API 文档。

3. 交互式 API 文档打开后，转到页面右上角的下拉菜单并选择 \* 实用程序 \*。
4. 单击 \* 登录 \* 类别以查看可用端点。
5. 单击 \* 发布：/login\* 端点，然后单击 \* 试用 \*。
6. 对于首次登录，输入 admin 作为用户名和密码。
7. 单击 \* 执行 \*。
8. 要访问端点以进行存储管理，请转到右上角的下拉菜单并选择 \* v2\*。

此时将显示端点的高级类别。您可以按照表中所述导航 API 文档。

区域	Description
下拉菜单	<p>页面右上角的下拉菜单提供了在 API 文档（V2）版本 2，符号界面（SYMBOL V2）和用于登录的 API 实用程序（utils）之间切换的选项。</p> <p> 由于 API 文档的版本 1 是预发布版本，并且不普遍提供，因此下拉菜单中不会包含 V1。</p>

区域	<b>Description</b>
类别	API 文档按高级类别（例如：管理，配置）进行组织。单击某个类别可查看相关端点。
端点	选择一个端点以查看其 URL 路径，所需参数，响应正文以及 URL 可能返回的状态代码。
试用	<p>单击 * 试用 * 直接与端点交互。此按钮在端点的每个展开视图中提供。</p> <p>单击按钮时，将显示用于输入参数的字段（如果适用）。然后，您可以输入值并单击 * 执行 *。</p> <p>交互式文档使用 JavaScript 直接向 API 发出请求，而不是测试请求。</p>

### 登录到 Unified Manager

安装 Web 服务代理后，您可以访问 Unified Manager 以在基于 Web 的界面中管理多个存储系统。

要访问 Unified Manager，请打开浏览器并输入指向安装代理的 URL。支持以下浏览器和版本。

浏览器	最低版本
Google Chrome	79.
Microsoft Internet Explorer	11.
Microsoft Edge	79.
Mozilla Firefox	70
Safari	12

### 步骤

1. 打开浏览器并输入以下 URL：

` + http : //< 服务器 > : < 端口 >/um+`

在此 URL 中，`< 服务器 >` 表示安装了 Web 服务代理的服务器的 IP 地址或 FQDN，`< 端口 >` 表示侦听端口号（对于 HTTP，默认为 8080，对于 HTTPS，默认为 8443）。

此时将打开 Unified Manager 登录页面。

2. 对于首次登录，请输入 admin 作为用户名，然后设置并确认管理员用户的密码。

此密码最多可包含 30 个字符。有关用户和密码的详细信息，请参见 Unified Manager 联机帮助的访问管理

部分。

## 配置SANtricity Web服务代理

您可以修改 Web 服务代理设置，以满足环境的独特操作和性能要求。

### 停止或重新启动 Web 服务器

Web 服务器服务会在安装期间启动并在后台运行。在某些配置任务期间，您可能需要停止或重新启动 Web 服务器服务。

### 步骤

1. 执行以下操作之一：

- 对于 Windows，请转到 \* 开始 \* 菜单，选择菜单：管理工具 [ 服务 ]，找到 \* NetApp SANtricity Web Services\*，然后选择 \* 停止 \* 或 \* 重新启动 \*。
- 对于 Linux，选择停止和重新启动适用于您的操作系统版本的 Web 服务器的方法。在安装期间，弹出对话框会指示启动的守护进程。例如：

```
web_services_proxy webserver 已安装并启动。您可以使用 systemctl  
start|stop|restart|status web_services_proxy.service 与其进行交互
```

与此服务交互的最常见方法是使用 systemctl 命令。

### 解决端口冲突

如果 Web 服务代理正在运行，而另一个应用程序在定义的地址或端口上可用，则可以在 wsconfig.xml 文件中解决端口冲突。

### 步骤

1. 打开 wsconfig.xml 文件，该文件位于：

- ( Windows ) — C : \Program Files\NetApp\SANtricity Web 服务代理
- ( Linux ) — /opt/netapp/SANtricity web\_services\_proxy

2. 将以下行添加到 wsconfig.xml 文件中，其中 *n* 是端口号：

```
<sslport clientauth="request">*n*</sslport>  
<port>n</port>
```

下表显示了控制 HTTP 端口和 HTTPS 端口的属性。

Name	Description	父节点	属性	Required
配置	配置的根节点	空	version —配置模式的当前版本为 1.0。 ◦	是的。

Name	Description	父节点	属性	Required
sslport	用于侦听 SSL 请求的 TCP 端口。默认为 8443。	配置	客户端身份验证	否
port	用于侦听 HTTP 请求的 TCP 端口默认为 8080。	配置	-	否

3. 保存并关闭文件。
4. 重新启动 Web 服务器服务，以使更改生效。

#### 配置负载均衡和 / 或高可用性

要在高可用性（HA）配置中使用 Web 服务代理，您可以配置负载均衡。在 HA 配置中，通常一个节点接收所有请求，而另一个节点处于备用状态，或者在所有节点之间对请求进行负载均衡。

Web 服务代理可以位于高可用性（HA）环境中，无论请求的接收方是谁，大多数 API 都可以正常运行。元数据标记和文件夹是两个例外，因为标记和文件夹存储在本地数据库中，不会在 Web 服务代理实例之间共享。

但是，在少数请求中会出现一些已知的时间问题。具体而言，对于小型窗口，一个代理实例的数据更新速度可以比另一个实例更快。Web 服务代理包含一个特殊配置，用于删除此计时问题描述。默认情况下，此选项不会启用，因为它会增加处理请求所需的时间（以确保数据一致性）。要启用此选项，必须向 .ini 文件（适用于 Windows）或 .SH 文件（适用于 Linux）添加属性。

#### 步骤

1. 执行以下操作之一：
  - Windows：打开 appserver64.ini 文件，然后添加 `Dload-balance.enables=true` 属性。  
例如：`vmarg.7=-dload-balance.enabled=true`
  - Linux：打开 webserver.sh 文件，然后添加 `Dload-balance.enables=true` 属性。  
例如：`debug_start_options="-dload-balance.enabled=true"`
2. 保存所做的更改。
3. 重新启动 Web 服务器服务，以使更改生效。

#### 禁用符号 HTTPS

您可以禁用符号命令（默认设置）并通过远程操作步骤调用（RPC）发送命令。可以在 wsconfig.xml 文件中更改此设置。

默认情况下，对于运行 SANtricity OS 08.40 或更高版本的所有 E2800 系列和 E5700 系列存储系统，Web 服务代理都会通过 HTTPS 发送符号命令。通过 HTTPS 发送的符号命令将通过身份验证发送到存储系统。如果需要，您可以禁用 HTTPS 符号支持并通过 RPC 发送命令。只要配置了基于 RPC 的符号，存储系统的所有被动命令都将在不进行身份验证的情况下启用。



使用基于 RPC 的符号时，Web 服务代理无法连接到禁用了符号管理端口的系统。

#### 步骤

1. 打开 wsconfig.xml 文件，该文件位于：
  - ( Windows ) — C : \Program Files\NetApp\SANtricity Web 服务代理
  - ( Linux ) — /opt/netapp/SANtricity web\_services\_proxy
2. 在 devicemgt.symbolclientstrategy 条目中，将 https Preferred 值替换为 rpcOnly。

例如：

```
<env key="devicemgt.symbolclientstrategy">rpcOnly"
```

3. 保存文件。

#### 配置跨源资源共享

您可以配置跨源资源共享（CORS），这种机制使用额外的 HTTP 标头为一个源运行的 Web 应用程序提供从另一个源服务器访问选定资源的权限。

CORS 由工作目录中的 cors.cfg 文件处理。默认情况下，CORS 配置处于打开状态，因此跨域访问不受限制。

如果不存在任何配置文件，则 CORS 处于打开状态。但是，如果存在 cors.cfg 文件，则会使用它。如果 cors.cfg 文件为空，则无法发出 CORS 请求。

#### 步骤

1. 打开位于工作目录中的 cors.cfg 文件。
2. 将所需行添加到文件中。

CORS 配置文件中的每一行都是要匹配的正则表达式模式。原始标题必须与 cors.cfg 文件中的一行匹配。如果任何线模式与原始标题匹配，则允许请求。将比较完整的原始服务器，而不仅仅是主机元素。

3. 保存文件。

请求会在主机上根据协议进行匹配，如以下协议：

- 将 localhost 与任何协议匹配 - ` \\* localhost`
- 仅将 localhost 与 HTTPS 匹配 - ` https://localhost`

#### 卸载 SANtricity Web 服务代理

要删除 Web 服务代理和 Unified Manager，您可以使用任何模式（图形，控制台，静默或 RPM 文件），而不管使用哪种方法安装代理。

#### 图形模式卸载

您可以在图形模式下对 Windows 或 Linux 运行卸载。在图形模式下，系统会在 Windows 模式界面中显示提示。

## 步骤

1. 对 Windows 或 Linux 启动卸载，如下所示：

- Windows —转到包含 `uninstall_web_services_proxy` 卸载文件的目录。默认目录位于以下位置： `C:\Program Files/NetApp/SANtricity Web 服务代理/`。双击 `uninstall_web_services_proxy.exe`。



或者，您也可以转到菜单：控制面板 [ 程序 > 卸载程序 ]，然后选择 "NetApp SANtricity Web 服务代理"。

- Linux —转到包含 Web 服务代理卸载文件的目录。默认目录位于以下位置： `+`/opt/netapp/SANtricity web_services_proxy/uninstall_web_services_proxy``

2. 运行以下命令：

```
uninstall_web_services_proxy -i 图形用户界面
```

此时将显示 SANtricity Web 服务代理启动屏幕。

3. 在卸载对话框中，单击 \* 卸载 \*。

此时将显示卸载程序进度条并显示进度。

4. 出现 "卸 载完成 " 消息时，单击 \* 完成 \*。

## 控制台模式卸载

您可以在控制台模式下对 Windows 或 Linux 运行卸载。在控制台模式下，终端窗口中会显示提示。

## 步骤

1. 转到 `uninstall_web_services_proxy` 目录。

2. 运行以下命令：

```
uninstall_web_services_proxy -i console
```

卸载过程将开始。

3. 卸载完成后，按 \* 输入 \* 退出安装程序。

## 静默模式卸载

您可以在静默模式下对 Windows 或 Linux 运行卸载。在静默模式下，终端窗口中不会显示任何返回消息或脚本。

## 步骤

1. 转到 `uninstall_web_services_proxy` 目录。

2. 运行以下命令：

```
uninstall_web_services_proxy -i silent
```

卸载过程将运行，但终端窗口中不会显示任何返回消息或脚本。成功卸载 Web 服务代理后，终端窗口将显

示命令提示符。

### rpm 命令卸载（仅限 Linux）

您可以使用 RPM 命令从 Linux 系统卸载 Web 服务代理。

#### 步骤

1. 打开终端窗口。
2. 输入以下命令行：

```
rpm -e SANtricity Web 服务
```



卸载过程可能会留下不属于原始安装的文件。手动删除这些文件以完全删除 Web 服务代理。

## 在SANtricity Web服务代理中管理用户访问

出于安全考虑，您可以管理用户对 Web 服务 API 和 Unified Manager 的访问。

### 访问管理概述

访问管理包括基于角色的登录，密码加密，基本身份验证和 LDAP 集成。

### 基于角色的访问

基于角色的访问控制（Role-Based Access Control，RBAC）可将预定义用户与角色关联起来。每个角色都会为特定级别的功能授予权限。

下表介绍了每个角色。

Role	Description
security.admin	SSL 和证书管理。
storage.admin	对存储系统配置的完全读 / 写访问权限。
storage.monitor	用于查看存储系统数据的只读访问权限。
support.admin	访问存储系统上的所有硬件资源以及 AutoSupport（ASUP）检索等支持操作。

默认用户帐户在 users.properties 文件中定义。您可以通过直接修改 users.properties 文件或使用 Unified Manager 中的访问管理功能来更改用户帐户。

下表列出了可用于 Web 服务代理的用户登录。

预定义的用户登录	Description
管理员	超级管理员，有权访问所有功能并包括所有角色。对于 Unified Manager，您必须在首次登录时设置密码。
storage	负责所有存储配置的管理员。此用户包括以下角色： storage.admin， support.admin 和 storage.monitor。在设置密码之前，此帐户将被禁用。
安全性	负责安全配置的用户。此用户包括以下角色： security.admin 和 storage.monitor。在设置密码之前，此帐户将被禁用。
支持	负责硬件资源，故障数据和固件升级的用户。此用户包括以下角色： support.admin 和 storage.monitor。在设置密码之前，此帐户将被禁用。
监控	对系统具有只读访问权限的用户。此用户仅包含 storage.monitor 角色。在设置密码之前，此帐户将被禁用。
rw (旧阵列的旧阵列)	RW（读 / 写）用户包括以下角色： storage.admin， support.admin 和 storage.monitor。在设置密码之前，此帐户将被禁用。
RO (旧阵列的原有)	ro（只读）用户仅包含 storage.monitor 角色。在设置密码之前，此帐户将被禁用。

## 密码加密

对于每个密码，您可以使用现有 SHA256 密码编码应用一个额外的加密过程。此附加加密过程会对每个 SHA256 哈希加密的每个密码（Salt）随机应用一组字节。所有新创建的密码均采用 Salted SHA256 加密。



在 Web 服务代理 3.0 版之前，密码仅通过 SHA256 哈希进行加密。任何现有的 SHA256 仅哈希加密密码都会保留此编码，并且在 users.properties 文件下仍然有效。但是，SHA256 仅哈希加密密码不如采用 Salted SHA256 加密的密码安全。

## 基本身份验证

默认情况下，基本身份验证处于启用状态，这意味着服务器返回基本身份验证质询。可以在 wsconfig.xml 文件中更改此设置。

## LDAP

为 Web 服务代理启用了轻型目录访问协议（Lightweight Directory Access Protocol，LDAP），这是一种用于访问和维护分布式目录信息服务的应用程序协议。LDAP 集成支持用户身份验证以及将角色映射到组。

有关配置 LDAP 功能的信息，请参阅 Unified Manager 界面或交互式 API 文档的 LDAP 部分中的配置选项。

## 配置用户访问

您可以通过对密码应用额外加密，设置基本身份验证以及定义基于角色的访问来管理用户访问。

## 对密码应用额外加密

为了获得最高的安全性，您可以使用现有 SHA256 密码编码对密码应用额外的加密。

此附加加密过程会对每个 SHA256 哈希加密的每个密码（Salt）随机应用一组字节。所有新创建的密码均采用 Salted SHA256 加密。

### 步骤

1. 打开 users.properties 文件，该文件位于：
  - （Windows）— C : \Program Files\NetApp\SANtricity Web Services Proxy\data\config
  - （Linux）— /opt/netapp/SANtricity web\_services\_proxy/data/config
2. 以纯文本格式重新输入加密密码。
3. 运行 securepasswds 命令行实用程序重新加密密码，或者只需重新启动 Web 服务代理即可。此实用程序安装在 Web 服务代理的根目录安装目录中。



或者，每当通过 Unified Manager 编辑密码时，您都可以对本地用户密码进行盐和哈希处理。

## 配置基本身份验证

默认情况下，基本身份验证处于启用状态，这意味着服务器返回基本身份验证质询。如果需要，您可以在 wsconfig.xml 文件中更改此设置。

1. 打开 wsconfig.xml 文件，该文件位于：
  - （Windows）— C : \Program Files\NetApp\SANtricity Web 服务代理
  - （Linux）— /opt/netapp/SANtricity web\_services\_proxy
2. 通过指定 false（未启用）或 true（已启用）修改文件中的以下行。

例如：`<env key="enable-basic-auth">true</env>`

3. 保存文件。
4. 重新启动 Web 服务器服务，以使更改生效。

## 配置基于角色的访问

要限制用户对特定功能的访问，您可以修改为每个用户帐户指定的角色。

Web 服务代理包括基于角色的访问控制（Role-Based Access Control，RBAC），其中的角色与预定义的用户相关联。每个角色都会为特定级别的功能授予权限。您可以通过直接修改 users.properties 文件来更改分配给用户帐户的角色。



您也可以使用 Unified Manager 中的访问管理来更改用户帐户。有关详细信息，请参见 Unified Manager 提供的联机帮助。

### 步骤

1. 打开 users.properties 文件，该文件位于：
  - （Windows）— C : \Program Files\NetApp\SANtricity Web Services Proxy\data\config

- ( Linux ) — /opt/netapp/SANtricity web\_services\_proxy/data/config

2. 找到要修改的用户帐户所在的行（存储，安全性，监控，支持， RW ， 或 ro ）。



请勿修改管理员用户。这是一个超级用户，可以访问所有功能。

3. 根据需要添加或删除指定的角色。

角色包括：

- security.admin — SSL 和证书管理。
- storage.admin —对存储系统配置的完全读 / 写访问权限。
- storage.monitor —用于查看存储系统数据的只读访问权限。
- support.admin —访问存储系统上的所有硬件资源以及 AutoSupport （ ASUP ） 检索等支持操作。



包括管理员在内的所有用户都需要 storage.monitor 角色。

4. 保存文件。

## 在SANtricity Web服务代理中管理安全性和证书

为了确保 Web 服务代理中的安全性，您可以指定 SSL 端口名称并管理证书。证书用于标识客户端和服务器之间安全连接的网站所有者。

### 启用 SSL

Web 服务代理使用安全套接字层（SSL）来实现安全性，此功能在安装期间启用。您可以在 wsconfig.xml 文件中更改 SSL 端口指定。

#### 步骤

1. 打开 wsconfig.xml 文件，该文件位于：
  - ( Windows ) — C : \Program Files\NetApp\SANtricity Web 服务代理
  - ( Linux ) — /opt/netapp/SANtricity web\_services\_proxy
2. 添加或更改 SSL 端口号，类似于以下示例：

```
<sslport clientauth="request">8443</sslport>
```

#### 结果

在配置了 SSL 的情况下启动服务器时，服务器将查找密钥库和信任存储库文件。

- 如果服务器未找到密钥库，则服务器将使用检测到的第一个非环回 IPv4 地址的 IP 地址生成密钥库，然后向密钥库添加自签名证书。
- 如果服务器未找到信任存储库，或者未指定信任存储库，则服务器将使用密钥库作为信任存储库。

## 绕过证书验证

为了支持安全连接，Web 服务代理会根据自己的可信证书验证存储系统的`证书。如果需要，您可以指定代理在连接到存储系统之前绕过此验证。

### 开始之前

- 所有存储系统连接都必须安全。

### 步骤

1. 打开 wsconfig.xml 文件，该文件位于：
  - ( Windows ) — C : \Program Files\NetApp\SANtricity Web 服务代理
  - ( Linux ) — /opt/netapp/SANtricity web\_services\_proxy
2. 在 trust.all.arrays 条目中输入 true ，如示例所示：

```
<env key="trust.all.arrays">true</env>
```

3. 保存文件。

## 生成并导入主机管理证书

证书用于标识客户端和服务器之间安全连接的网站所有者。要为安装了 Web 服务代理的主机系统生成和导入证书颁发机构（CA）证书，您可以使用 API 端点。

要管理主机系统的证书，请使用 API 执行以下任务：

- 为主机系统创建证书签名请求（CSR）。
- 将 CSR 文件发送到 CA ，然后等待它们向您发送证书文件。
- 将签名证书导入到主机系统。



您还可以在 Unified Manager 界面中管理证书。有关详细信息，请参见 Unified Manager 中提供的联机帮助。

### 步骤

1. 登录到 ["交互式 API 文档"](#)。
2. 转到右上角的下拉菜单，然后选择 \* 。 v2\* 。
3. 展开 \* 管理 \* 链接并向下滚动到 \* /certificates \* 端点。
4. 生成 CSR 文件：
  - a. 选择 \* 发布： /certificates \* ，然后选择 \* 试用 \* 。

Web 服务器将重新生成自签名证书。然后，您可以在字段中输入信息，以定义通用名称，组织，组织单位，备用 ID 以及用于生成 CSR 的其他信息。

- b. 在 \* 示例值 \* 窗格中添加所需信息以生成有效的 CA 证书，然后执行命令。



请勿再次调用 \* POST : /certificates \* 或 \* POST : /certifices/reset\* , 否则必须重新生成 CSR 。调用 \* POST : /certificates\* 或 \* POST : /certificates/reset\* 时, 将使用新的私钥生成新的自签名证书。如果您发送的 CSR 是在服务器上上次重置私钥之前生成的, 则新的安全证书将不起作用。您必须生成新的 CSR 并请求新的 CA 证书。

- c. 执行 \* 获取: /certificates /server\* 端点, 确认当前证书状态为自签名证书, 并使用从 \* post : /certificates \* 命令添加的信息。

此时, 服务器证书 (以别名 jetty 表示) 仍为自签名证书。

- d. 展开 \* 发布: /certifices/export\* 端点, 选择 \* 试用 \* , 输入 CSR 文件的文件名, 然后单击 \* 执行 \* 。
5. 将 fileUrl 复制并粘贴到新的浏览器选项卡中以下载 CSR 文件, 然后将 CSR 文件发送到有效的 CA 以请求新的 Web 服务器证书链。
6. 当 CA 发出新的证书链时, 请使用证书管理器工具拆分根证书, 中间证书和 Web 服务器证书, 然后将其导入到 Web 服务代理服务器:
  - a. 展开 \* POST : /sslconfig/server\* 端点并选择 \* 试用 \* 。
  - b. 在 \* 别名 \* 字段中输入 CA 根证书的名称。
  - c. 在 \* replaceMainServerCertificer\* 字段中选择 \* false \* 。
  - d. 浏览并选择新的 CA 根证书。
  - e. 单击 \* 执行 \* 。
  - f. 确认证书上传成功。
  - g. 对 CA 中间证书重复 CA 证书上传操作步骤。
  - h. 对新的 Web 服务器安全证书文件重复证书上传操作步骤, 但在此步骤中, 请在 \* 更换主服务器证书 \* 下拉列表中选择 \* 真 \* 。
  - i. 确认 Web 服务器安全证书导入成功。
  - j. 要确认新的根证书, 中间证书和 Web 服务器证书在密钥库中可用, 请运行 \* 获取: /certificates/server\* 。
7. 选择并展开 \* 发布: /certifices/reload \* 端点, 然后选择 \* 试用 \* 。出现提示时, 无论是否要重新启动这两个控制器, 请选择 \* 错误 \* 。 ("True" 仅适用于双阵列控制器。) 单击 \* 执行 \* 。

/certifices/reload \* 端点通常会返回成功的 http 202 响应。但是, 重新加载 Web 服务器信任存储库和密钥库证书确实会在 API 进程和 Web 服务器证书重新加载进程之间造成争用情况。在极少数情况下, Web 服务器证书重新加载可能会击败 API 处理。在这种情况下, 即使重新加载成功完成, 它也似乎失败。如果发生这种情况, 请继续执行下一步。如果重新加载实际失败, 下一步也会失败。

8. 关闭与 Web 服务代理的当前浏览器会话, 打开一个新的浏览器会话, 然后确认可以与 Web 服务代理建立新的安全浏览器连接。

通过使用匿名或非公开浏览会话, 您可以打开与服务器的连接, 而无需使用先前浏览会话中保存的任何数据。

## 登录锁定功能

只能通过REST API进行配置、您可以限制嵌入式Web服务和代理Web服务的登录尝试次数。根据您的设置、一旦超过Web服务的登录尝试次数、锁定功能将启用。

## 步骤

1. 登录到 ["交互式 API 文档"](#)。
2. 转到右上角的下拉菜单，然后选择 \*。v2\*。
3. 单击\*get:/settings /lockout\*端点以检索锁定设置。
4. 单击\*POST: /SETTINGS/LOCD\*端点，然后单击\*TURE IT OUT \*以配置锁定设置。

## 使用SANtricity Web服务代理管理存储系统

要管理网络中的存储系统，您必须先发现它们，然后将其添加到管理列表中。

### 发现存储系统

您可以设置自动发现或手动发现存储系统。

#### 自动发现存储系统

您可以通过修改 wsconfig.xml 文件中的设置来指定在网络中自动发现存储系统。默认情况下，IPv6 自动发现处于禁用状态，IPv4 处于启用状态。

要添加存储系统，只需提供一个管理 IP 或 DNS 地址即可。如果未配置路径或路径已配置且可轮换，则服务器会自动发现所有管理路径。



如果在建立初始连接后尝试使用 IPv6 协议自动从控制器配置发现存储系统，则此过程可能会失败。失败的可能原因包括：在存储系统上启用 IP 地址转发或 IPv6 期间出现问题，但服务器上未启用 IPv6。

### 开始之前

在启用 IPv6 发现设置之前，请确认您的基础架构支持与存储系统的 IPv6 连接，以缓解任何连接问题。

## 步骤

1. 打开 wsconfig.xml 文件，该文件位于：
  - ( Windows ) — C : \Program Files\NetApp\SANtricity Web 服务代理
  - ( Linux ) — /opt/netapp/SANtricity web\_services\_proxy
2. 在自动发现字符串中，根据需要将设置从 true 更改为 false。请参见以下示例。

```
<env key="autodiscover.ipv6.enable">true</env>
```



如果配置了路径，但未对路径进行配置，使服务器能够路由到地址，则会发生间歇性连接错误。如果您无法将 IP 地址设置为可从主机路由，请关闭自动发现（将设置更改为 false）。

3. 保存文件。

您可以使用 API 端点发现存储系统并将其添加到受管列表中。此操作步骤会在存储系统和 API 之间创建管理连接。



此任务介绍如何使用 REST API 发现和添加存储系统，以便您可以在交互式 API 文档中管理这些系统。但是，您可能需要改用 Unified Manager 来管理存储系统，它提供了一个易于使用的界面。有关详细信息，请参见 Unified Manager 提供的联机帮助。

### 开始之前

对于 SANtricity 版本为 11.30 及更高版本的存储系统，必须在 SANtricity System Manager 界面中为 SYMBOL 启用原有管理界面。否则，发现端点将失败。要查找此设置，请打开 System Manager ，然后转到菜单：设置 [ 系统 > 其他设置 > 更改管理界面 ]。

### 步骤

1. 登录到 "交互式 API 文档"。
2. 发现存储系统，如下所示：
  - a. 在 API 文档中，确保在下拉列表选择了 \* V2 \* ，然后展开 \* 存储系统 \* 类别。
  - b. 单击 \* 发布： /discover\* 端点，然后单击 \* 试用 \* 。
  - c. 按照表中所述输入参数。

startIP
endIP
将字符串替换为网络中一个或多个存储系统的起始和结束 IP 地址范围。
使用代理
将此值设置为： <ul style="list-style-type: none"><li>• true = 使用带内代理进行网络扫描。</li><li>• false = 不要在网络扫描中使用带内代理。</li></ul>
连接超时
输入在连接超时之前允许扫描的秒数。
maxPortsToUse.
输入用于网络扫描的最大端口数。

- d. 单击 \* 执行 \* 。



API 操作在不提示用户的情况下执行。

发现过程在后台运行。

- a. 确保此代码返回 202 。
- b. 在 \* 响应正文 \* 下，找到为 requestId 返回的值。您需要此请求 ID 才能在下一步中查看结果。

3. 查看发现结果，如下所示：

- a. 单击 \* 获取： /discover 星 \* 端点，然后单击 \* 试用 \* 。
- b. 输入上一步中的请求 ID 。如果将 \* 请求 ID \* 留空，则端点默认为上次执行的请求 ID 。
- c. 单击 \* 执行 \* 。
- d. 确保此代码返回 200 。
- e. 在响应正文中，找到您的请求 ID 以及 storageSystems 的字符串。这些字符串类似于以下示例：

```
"storageSystems": [  
  {  
    "serialNumber": "123456789",  
    "wwn": "000A011000AF0000000000001A0C000E",  
    "label": "EF570_Array",  
    "firmware": "08.41.10.01",  
    "nvsram": "N5700-841834-001",  
    "ipAddresses": [  
      "10.xxx.xx.213",  
      "10.xxx.xx.214"  
    ],  
  },  
]
```

- f. 记下 WWN ， 标签和 IP 地址的值。您需要这些信息才能执行下一步。

4. 添加存储系统，如下所示：

- a. 单击 \* 发布： /storage-system \* 端点，然后单击 \* 试用 \* 。
- b. 按照表中所述输入参数。

id

为此存储系统输入一个唯一名称。您可以输入标签（显示在 GET： /discovery 的响应中），但名称可以是您选择的任何字符串。如果不为此字段提供值， Web 服务将自动分配唯一标识符。

控制器插件

输入 GET： /discovery 响应中显示的 IP 地址。对于双控制器，请使用逗号分隔 IP 地址。例如：

`"IP 地址 1" , "IP 地址 2" `

验证
输入 <code>true</code> ，以便您可以收到 Web 服务可以连接到存储系统的确认消息。
password
输入存储系统的管理密码。
WWN
输入存储系统的 WWN（显示在对 <code>GET: /discovery</code> 的响应中）。

- c. 删除 `"enableTrace": true` 后的所有字符串，使整个字符串集与以下示例类似：

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP", "Controller-B-Mgmt_IP"
  ],
  "validate": true,
  "password": "array-admin-password",
  "wwn": "000A011000AF000000000001A0C000E",
  "enableTrace": true
}
```

- d. 单击 \* 执行 \*。  
e. 确保代码响应为 201，表示端点已成功执行。

已将 \* 发布: `/storage-systems`\* 端点排队。您可以在下一步中使用 \* 获取: `/storage-systems`\* 端点查看结果。

5. 确认添加列表，如下所示：

- a. 单击 \* 获取: `/storage-system`\* 端点。

不需要任何参数。

- b. 单击 \* 执行 \*。

- c. 确保代码响应为 200，表示端点已成功执行。

- d. 在响应正文中，查找存储系统详细信息。返回的值表示已成功将其添加到受管阵列列表中，类似于以下示例：

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
    ]
  }
]
```

## 纵向扩展受管存储系统的数量

默认情况下，API 最多可以管理 100 个存储系统。如果您需要管理更多，则必须满足服务器的内存要求。

服务器设置为使用 512 MB 的内存。对于网络中每增加 100 个存储系统，请在该数量中增加 250 MB。请勿添加比物理内存更多的内存。为您的操作系统和其他应用程序留出足够的额外空间。



默认缓存大小为 8,192 个事件。对于每 8,192 个事件，MEL 事件缓存的大致数据使用量为 1 MB。因此，通过保留默认值，存储系统的缓存使用量应大约为 1 MB。



除了内存之外，代理还会对每个存储系统使用网络端口。Linux 和 Windows 将网络端口视为文件句柄。作为一项安全措施，大多数操作系统都会限制进程或用户一次可以打开的打开文件句柄的数量。尤其是在 Linux 环境中，如果将开放式 TCP 连接视为文件句柄，则 Web 服务代理很容易超过此限制。由于此修复程序取决于系统，因此您应参考操作系统的文档，了解如何提高此值。

## 步骤

1. 执行以下操作之一：
  - 在 Windows 上，转到 appserver64.init 文件。找到行 `vmarg.3=-Xmx512M`
  - 在 Linux 上，转到 webserver.sh 文件。找到行 `java_options="-Xmx512M"`
2. 要增加内存，请将 512 更换为所需的内存（以 MB 为单位）。
3. 保存文件。

## 管理 SANtricity Web 服务代理统计信息的自动轮询

您可以为已发现的存储系统上的所有磁盘和卷统计信息配置自动轮询。

## 统计信息概述

统计信息提供了有关存储系统的数据收集速率和性能的信息。

通过 Web 服务代理可以访问以下类型的统计信息：

- raw statistics —收集数据时数据点的总计数器。原始统计信息可用于总读取操作或总写入操作。
- "分析的统计信息" —为间隔计算的信息。分析的统计信息示例为每秒读取输入 / 输出操作（IOPS）或写入吞吐量。

原始统计信息是线性的，通常需要至少两个收集的数据点才能从中获得可用数据。分析的统计信息是原始统计信息的派生，这些统计信息提供了重要的指标。为了方便起见，可以从原始统计信息派生的许多值会在分析的统计信息中以可用的时间点格式显示。

无论是否启用了自动轮询，您都可以检索原始统计信息。您可以将 `usecache=true` 查询字符串添加到 URL 末尾，以从上次轮询中检索缓存的统计信息。使用缓存的结果会显著提高统计信息检索的性能。但是，如果多个调用的速率等于或小于配置的轮询间隔缓存，则会检索相同的数据。

## 统计信息功能

Web 服务代理可通过 API 端点从支持的硬件型号和软件版本检索原始的和分析的控制器和接口统计信息。

### 原始统计信息 API

- `` /storage-systems/ { system-id } /controller-statistics``
- `` +/storage-systems/ { system-id } /drive-statistics/ { optional list of disk IDs} +``
- `` +/storage-systems/ { system-id } /interface-statistics/ { optional list of interface IDs} +``
- `` +/storage-systems/ { system-id } /volume-statistics/ { optional list of volume IDs} +``

### 已分析统计信息 API

- `` /storage-systems/ { id } /analysed-controller-statistics/``
- `` +/storage-systems/ { id } /analysed-drive-statistics/ { optional list of disk IDs} +``
- `` +/storage-systems/ { id } /analysed-interface-statistics/ { optional list of interface IDs} +``
- `` +/storage-systems/ { id } /analysed-volume-statistics/ { optional list of volume IDs} +``

这些 URL 将从上次轮询中检索分析的统计信息，只有在启用轮询时才可用。这些 URL 包含以下输入输出数据：

- 每秒操作数
- 吞吐量（以 MB/ 秒为单位）
- 响应时间（以毫秒为单位）

计算基于统计轮询迭代之间的差异，这些迭代是最常见的存储性能衡量指标。这些统计信息比未分析的统计信息更好。



系统启动时，以前不会收集任何统计信息来计算各种指标，因此，分析的统计信息在启动后至少需要一个轮询周期才能返回数据。此外，如果重置累积计数器，则下一轮询周期的数据数将不可预测。

## 配置轮询间隔

要配置轮询间隔，请修改 `wsconfig.xml` 文件以指定轮询间隔（以秒为单位）。



由于统计信息会缓存在内存中，因此每个存储系统的内存使用量可能会增加大约 1.5 MB。

## 开始之前

- 存储系统必须由代理发现。

## 步骤

1. 打开 `wsconfig.xml` 文件，该文件位于：
  - （Windows）— `C:\Program Files\NetApp\SANtricity Web 服务代理`
  - （Linux）— `/opt/netapp/SANtricity web_services_proxy`
2. 在 `<env-entries>` 标记中添加以下行，其中 `n` 是轮询请求之间间隔的秒数：

```
<env key="stats.poll.interval">n</env>
```

例如，如果输入 60，则轮询将以 60 秒为间隔开始。也就是说，系统会在上一轮询期完成后 60 秒开始轮询（无论上一轮询期的持续时间如何）。所有统计信息都带有检索时间戳。系统使用时间戳或时间差来计算 60 秒。

3. 保存文件。

## 使用SANtricity万维网服务代理管理AutoSupport

您可以配置 AutoSupport（ASUP），该功能会收集数据，然后自动将数据发送给技术支持以进行远程故障排除和问题分析。

### AutoSupport 概述（ASUP）

AutoSupport（ASUP）功能会根据手动和基于计划的标准自动向 NetApp 传输消息。

每个 AutoSupport 消息都是一组日志文件，配置数据，状态数据和性能指标。默认情况下，AutoSupport 每周向 NetApp 支持团队传输一次下表中列出的文件。

文件名	Description
<code>x-headers-data.txt</code>	一个 .txt 文件，其中包含 X-header 信息。
<code>Manifest.xml</code>	一个 .xml 文件，详细说明了消息的内容。

文件名	Description
arraydata.xml	一个 .xml 文件，其中包含客户端持久数据的列表。
appserver-config.txt	一个 .txt 文件，其中包含应用程序服务器配置数据。
wsconfig.txt	一个 .txt 文件，其中包含 Web 服务配置数据。
host-info.txt	一个 .txt 文件，其中包含有关主机环境的信息。
Server-logs.7z	包含每个可用 Web 服务器日志文件的 .7z 文件。
client-info.txt	一个 .txt 文件，其中包含用于应用程序特定计数器的任意键 / 值对，例如方法和网页访问。
WebServices-profile.json	<p>这些文件包含 Webservices 配置文件数据和 Jersey 监控统计数据。默认情况下，Jersey 监控统计信息处于启用状态。您可以在 wsconfig.xml 文件中启用和禁用它们，如下所示：</p> <ul style="list-style-type: none"> <li>• 启用：`&lt;env key="enable.jersey.statistics"&gt;true&lt;/env&gt;`</li> <li>• disable：`&lt;env key="enable.jersey.statistics"&gt;false&lt;/env&gt;`</li> </ul>

## 配置 AutoSupport

默认情况下，AutoSupport 在安装时处于启用状态；但是，您可以更改此设置或修改交付类型。

### 启用或禁用 AutoSupport

在首次安装 Web 服务代理期间，AutoSupport 功能处于启用或禁用状态，但您可以在 ASUPConfig 文件中更改此设置。

您可以通过 ASUPConfig.xml 文件启用或禁用 AutoSupport，如以下步骤所述。或者，您也可以使用 \* 配置 \* 和 \* 后 / 上 \* 通过 API 启用或禁用此功能，然后输入 "true" 或 "false"。

1. 打开工作目录中的 ASUPConfig.xml 文件。
2. 找到 <asupdata enable="Boolean\_value" timestamp="timestamp"> 对应的行
3. 输入 true (enable) 或 false (disable)。例如：

```
<asupdata enabled="false" timestamp="0">
```



时间戳条目是多余的。

4. 保存文件。

## 配置 AutoSupport 交付方法

您可以将AutoSupport功能配置为使用HTTPS或SMTP传输方法。HTTPS 是默认传送方法。

1. 访问工作目录中的 ASUPConfig.xml 文件。
2. 在字符串 `<delivery type="n">` 中，按表中所述输入 1， 2 或 3：

价值	Description
1.	<ul style="list-style-type: none"><li>• HTTPS * (默认)</li></ul> <pre>&lt;delivery type="1"&gt;</pre>
2.	<ul style="list-style-type: none"><li>• SMTP * —要将 AutoSupport 传送类型正确配置为 SMTP，必须包括 SMTP 邮件服务器地址以及发件人和收件人用户电子邮件，如下例所示：</li></ul> <pre>&lt;delivery type="3"&gt; &lt;smtp&gt; &lt;mailserver&gt;smtp.example.com&lt;/mailserver&gt; &lt;sender&gt;user@example.com&lt;/sender&gt; &lt;replyto&gt;user@example.com&lt;/replyto&gt; &lt;/smtp&gt; &lt;/delivery&gt;</pre>

## 远程卷镜像

### 了解SANtricity远程存储卷

使用 SANtricity® 远程存储卷功能将数据从远程存储设备直接导入到本地 E 系列卷。此功能有助于简化设备升级过程，并提供数据迁移功能，以便将数据从非 E 系列设备移动到 E 系列系统。

#### 配置概述

SANtricity 系统管理器可对选定子型号 ID 使用远程存储卷功能。要使用此功能，您必须配置远程存储系统和 E 系列存储系统，以便彼此进行通信。

使用以下工作流：

1. ["查看要求和限制"](#)。
2. ["配置硬件"](#)。
3. ["导入远程存储"](#)。



SANtricity远程存储卷目前在E4000系统上不受支持。

了解更多信息

- 联机帮助，可从 System Manager 用户界面或中获取 "[SANtricity 软件文档站点](#)"。
- 有关远程存储卷功能的其他技术信息，请参见 "[远程存储卷技术报告](#)"。

## 使用SANtricity远程存储卷的要求和限制

在配置远程存储卷功能之前，请查看以下要求和限制。

### 硬件要求

#### 支持的协议

对于初始版本的远程存储卷功能，仅支持 iSCSI 和 IPv4 协议。

请参见 "[NetApp 互操作性表工具](#)" 有关主机与用于远程存储卷功能的 E 系列（目标）阵列之间的最新支持和配置信息。

### 存储系统要求

E 系列存储系统必须包括：

- 两个控制器（双工模式）
- 两个 E 系列控制器的 iSCSI 连接，用于通过一个或多个 iSCSI 连接与远程存储系统进行通信
- SANtricity OS 11.71 或更高版本
- 在子型号 ID（SMID）中启用远程存储功能

远程系统可以是 E 系列存储系统，也可以是其他供应商提供的系统。它必须包含支持 iSCSI 的接口。

### 卷要求：

用于导入的卷必须满足大小，状态和其他条件的要求。

### 远程存储卷

导入的源卷称为 " 远程存储卷 "。此卷必须满足以下条件：

- 不能属于其他导入
- 必须处于联机状态

导入开始后，控制器固件将在后台创建远程存储卷。由于此后台进程，远程存储卷在 System Manager 中无法管理，只能用于导入操作。

创建远程存储卷后，该卷将与 E 系列系统上的任何其他标准卷一样进行处理，但以下情况除外：

- 可用作远程存储设备的代理。
- 不能用作其他卷副本或快照的候选项。
- 无法在导入过程中更改数据保证设置。

- 无法映射到任何主机，因为这些主机是严格为导入操作预留的。

每个远程存储卷仅与一个远程存储对象关联；但是，一个远程存储对象可以与多个远程存储卷关联。远程存储卷通过以下方式的组合进行唯一标识：

- 远程存储对象标识符
- 远程存储设备 LUN 编号

#### 目标卷候选项

目标卷是本地 E 系列系统上的目标卷。

目标卷必须满足以下条件：

- 必须是 RAID/DDP 卷。
- 容量必须等于或大于远程存储卷。
- 块大小必须与远程存储卷相同。
- 必须具有有效状态（最佳）。
- 不能具有以下任何关系：卷副本， Snapshot 副本， 异步或同步镜像。
- 不能进行任何重新配置操作：动态卷扩展，动态容量扩展，动态块大小，动态 RAID 迁移，动态容量缩减，或碎片整理。
- 导入开始前无法映射到主机(但是、可以在导入开始后映射)。
- 无法启用 Flash Read Cached （ FRC ）。

System Manager 会在导入远程存储向导中自动检查这些要求。在选择目标卷时，仅会显示满足所有要求的卷。

#### 限制

远程存储功能具有以下限制：

- 必须禁用镜像。
- E 系列系统上的目标卷不能具有快照。
- 在启动导入之前，不得将 E 系列系统上的目标卷映射到任何主机。
- E 系列系统上的目标卷必须已禁用资源配置。
- 不支持将远程存储卷直接映射到一个或多个主机。
- 不支持 Web 服务代理。
- 不支持 iSCSI CHAP 密码。
- 不支持 SMcli 。
- 不支持 VMware 数据存储库。
- 如果存在导入对，则一次只能升级关系 / 导入对中的一个存储系统。

## 准备生产导入

您应在生产导入之前执行测试或 " 试运行 " 导入，以验证存储和网络结构配置是否正确。

许多变量可能会影响导入操作和完成时间。为了确保生产导入成功并获得持续时间估计值，您可以使用这些测试导入来确保所有连接均按预期工作，并且导入操作在适当的时间内完成。然后，您可以在启动生产导入之前进行调整，以获得所需的结果。

## 为SANtricity远程存储卷配置硬件

必须将 E 系列存储系统配置为通过支持的 iSCSI 协议与远程存储系统进行通信。

### 配置远程存储设备和 E 系列阵列

在继续使用 SANtricity 系统管理器配置远程存储卷功能之前，请执行以下操作：

1. 手动在 E 系列系统和远程存储系统之间建立缆线连接，以便可以将这两个系统配置为通过 iSCSI 进行通信。
2. 配置 iSCSI 端口，使 E 系列系统和远程存储系统能够成功地彼此通信。
3. 获取 E 系列系统的 IQN 。
4. 使 E 系列系统对远程存储系统可见。如果远程存储系统是 E 系列系统，请使用目标 E 系列系统的 IQN 作为主机端口的连接信息来创建主机。
5. 如果远程存储设备正在由主机 / 应用程序使用：
  - 停止远程存储设备的 I/O 。
  - 取消映射 / 卸载远程存储设备。
6. 将远程存储设备映射到为 E 系列存储系统定义的主机。
7. 获取用于映射的设备的 LUN 编号。



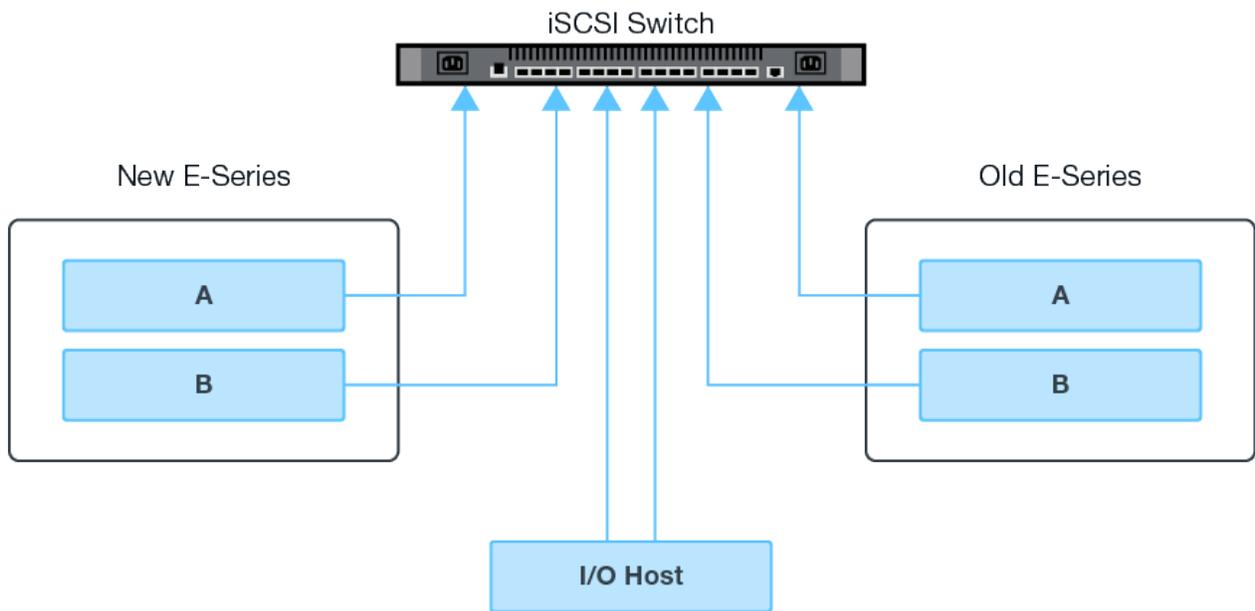
建议：在启动导入过程之前备份远程源卷。

### 为存储阵列布线

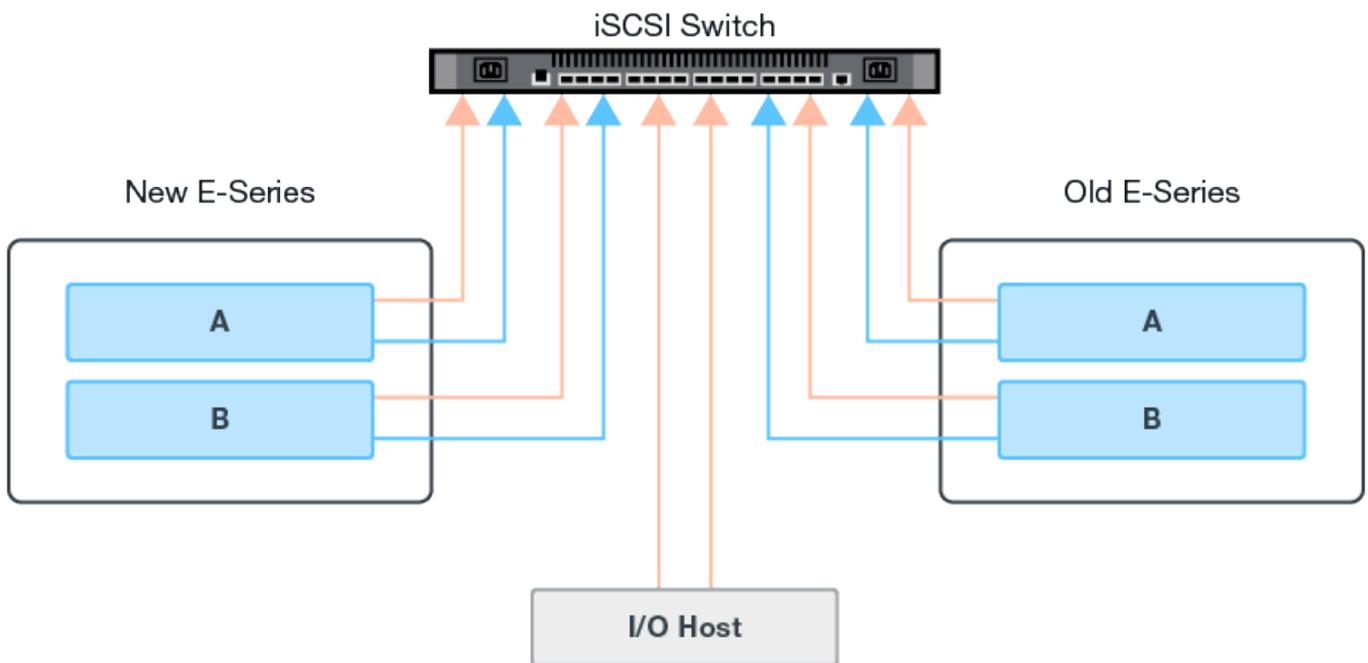
在设置过程中，存储阵列和 I/O 主机必须连接到与 iSCSI 兼容的接口。

下图举例说明了如何为系统布线，以便它们通过 iSCSI 连接执行远程存储卷操作。

## Fabric Connection - Use Case 1



## Fabric Connection - Use Case 2



### 配置 iSCSI 端口

您必须配置 iSCSI 端口，以确保目标（本地 E 系列存储阵列）与源（远程存储阵列）之间的通信。

根据您的子网，可以通过多种方式配置 iSCSI 端口。以下是有关如何配置 iSCSI 端口以用于远程存储卷功能的几个示例。

源 A	源 B	目标 A	目标 B
10.10.1.100/22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

源 A	源 B	目标 A	目标 B
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

## 为SANtricity远程存储卷导入远程存储

要启动从远程系统到本地 E 系列存储系统的存储导入，请使用 SANtricity 系统管理器用户界面中的导入远程存储向导。

您需要什么

- 必须将 E 系列存储系统配置为与远程存储系统进行通信。请参见 ["配置硬件"](#)。
- 对于远程存储系统，请收集以下信息：
  - iSCSI IQN
  - iSCSI IP 地址
  - 远程存储设备（源卷）的 LUN 编号
- 对于本地 E 系列存储系统，请创建或选择要用于数据导入的卷。目标卷必须满足以下要求：
  - 与远程存储设备（源卷）的块大小匹配。
  - 容量等于或大于远程存储设备。
  - 状态为最佳且可用。有关完整的要求列表，请参见 ["要求和限制"](#)。
- 建议：在开始导入过程之前，备份远程存储系统上的卷。

关于此任务

在此任务中，您将在远程存储设备与本地 E 系列存储系统上的卷之间创建映射。完成配置后，导入将开始。



由于许多变量可能会影响导入操作及其完成时间，因此应先执行较小的 "测试" 导入。使用这些测试可确保所有连接均按预期工作，并且导入操作会在适当的时间内完成。

步骤

1. 在 SANtricity 系统管理器中，单击 \* 存储 > 远程存储 \*。
2. 单击 \* 导入远程存储 \*。

此时将显示一个用于导入远程存储的向导。

3. 在配置源面板的步骤 1a 中，输入连接信息。
  - a. 在 \* 名称 \* 字段下，输入远程存储设备的名称。
  - b. 在 \* iSCSI 连接属性 \* 下，为远程存储设备输入以下内容：IQN，IP 地址和端口号（默认值为 3260）。

如果要添加另一个 iSCSI 连接，请单击 \* + 添加另一个 IP 地址 \* 以添加远程存储的其他 IP 地址。完成后，单击 \* 下一步 \*。

单击下一步后，将显示配置源面板的步骤 1b。

4. 在 \* LUN \* 字段下，为远程存储设备选择所需的源 LUN，然后单击 \* 下一步 \*。

此时将打开配置目标面板，并显示要用作导入目标的卷候选对象。由于块大小，容量或卷可用性，某些卷不会显示在候选卷列表中。

5. 从表中，选择 E 系列存储系统上的目标卷。如果需要，请使用滑块更改导入优先级。单击 \* 下一步 \*。在下一个对话框中键入 `continue`，然后单击 \* 继续 \*，确认操作。

如果目标卷的容量大于源卷，则不会向连接到 E 系列系统的主机报告此额外容量。要使用新容量，必须在导入操作完成并断开连接后在主机上执行文件系统扩展操作。

在对话框中确认配置后，将显示 Review 面板。

6. 在 Review 屏幕中，验证指定的远程存储设备，目标和导入设置是否准确。单击 \* 完成 \* 以完成远程存储的创建。

此时将打开另一个对话框，询问您是否要启动另一个导入。

7. 如果需要，请单击 \* 是 \* 以创建另一个远程存储导入。单击是返回到配置源面板的步骤 1a，您可以在其中选择现有配置或添加新配置。如果不想创建另一个导入，请单击 \* 否 \* 退出对话框。

导入过程开始后，整个目标卷将被复制的数据覆盖。如果在此过程中主机向目标卷写入任何新数据，则新数据将传播回远程设备（源卷）。

8. 在远程存储面板下的查看操作对话框中查看操作进度。

完成导入操作所需的时间取决于远程存储系统的大小，导入的优先级设置以及两个存储系统及其关联卷上的 I/O 负载量。导入完成后，本地卷将与远程存储设备重复。

9. 准备好中断两个卷之间的关系后，从操作进行中视图中选择导入对象上的 \* 断开连接 \*。断开关系后，本地卷的性能将恢复正常，不再受远程连接的影响。

## 管理SANtricity远程存储卷的导入进度

导入过程开始后，您可以查看其进度并对其执行操作。

对于每个导入操作，"正在执行的操作"页面将显示完成百分比和估计剩余时间。操作包括更改导入优先级，停止和恢复操作以及断开操作连接。



您还可以从主页页面查看正在进行的操作（\* 主页 > 显示正在进行的操作 \*）。

### 步骤

1. 在 SANtricity 系统管理器中，转到远程存储页面并选择 \* 查看操作 \*。

此时将显示操作进行中对话框。

2. 如果需要，可使用操作列中的链接停止并恢复，更改优先级或断开操作连接。

- \* 更改优先级 \* —选择 \* 更改优先级 \* 可更改正在进行或待处理的操作的优先级。对操作应用优先级，然后单击 \* 确定 \*。
- \* 停止 \* —选择 \* 停止 \* 可暂停从远程存储设备复制数据。导入对之间的关系仍保持不变，您可以在准备好继续导入操作时选择 \* 恢复 \*。
- \* 恢复 \* —选择 \* 恢复 \* 以从停止位置开始已停止或失败的进程。接下来，将优先级应用于恢复操作，然后单击 \* 确定 \*。

恢复操作不会 \* 不 \* 从头开始重新启动导入。如果要从头开始重新启动此过程，必须选择 \* 断开连接 \*，然后通过导入远程存储向导重新创建导入。

- \* 断开连接 \* —选择 \* 断开连接 \* 可中断已停止，已完成或失败的导入操作的源卷和目标卷之间的关系。

## 修改SANtricity远程存储卷的远程存储连接设置

您可以通过查看 / 编辑设置选项编辑，添加或删除任何远程存储配置的连接设置。

更改连接属性将影响正在进行的导入。为避免中断，请仅在导入未运行时更改连接属性。

### 步骤

1. 从 SANtricity 系统管理器的远程存储屏幕中，在结果列表部分下选择所需的远程存储对象。
2. 单击 \* 查看 / 编辑设置 \*。

此时将显示远程存储设置屏幕。

3. 单击 \* 连接属性 \* 选项卡。

此时将显示为远程存储导入配置的 IP 地址和端口设置。

4. 执行以下操作之一：

- \* 编辑 \* —单击远程存储对象对应行项目旁边的 \* 编辑 \*。在字段中输入修改后的 IP 地址和 / 或端口信息。
- \* 添加 \* —单击 \* 添加 \*，然后在提供的字段中输入新的 IP 地址和端口信息。单击 \* 添加 \* 进行确认，然后新连接将显示在远程存储对象列表中。
- \* 删除 \* —从列表中选择所需的连接，然后单击 \* 删除 \*。在提供的字段中键入 delete 确认操作，然后单击 \* 删除 \*。此连接将从远程存储对象列表中删除。

5. 单击 \* 保存 \*。

修改后的连接设置将应用于远程存储对象。

## 删除SANtricity远程存储卷的远程存储对象

导入完成后，如果您不再需要在本地设备和远程设备之间复制数据，则可以删除远程存储对象。

### 步骤

1. 确保没有与要删除的远程存储对象关联的导入。
2. 从 SANtricity 系统管理器的远程存储屏幕中，在结果列表部分下选择所需的远程存储对象。
3. 单击 \* 删除 \*。

此时将显示确认删除远程存储连接对话框。

4. 键入 `remove` 然后单击 \* 删除 \*，确认操作。

此时将删除选定的远程存储对象。

## 适用于 vCenter 的存储插件

### 了解适用于vCenter的SANtricity存储插件

适用于 vCenter 的 SANtricity 存储插件可在 VMware vSphere 客户端会话中对 E 系列存储阵列进行集成管理。

#### 可用任务

您可以使用插件执行以下任务：

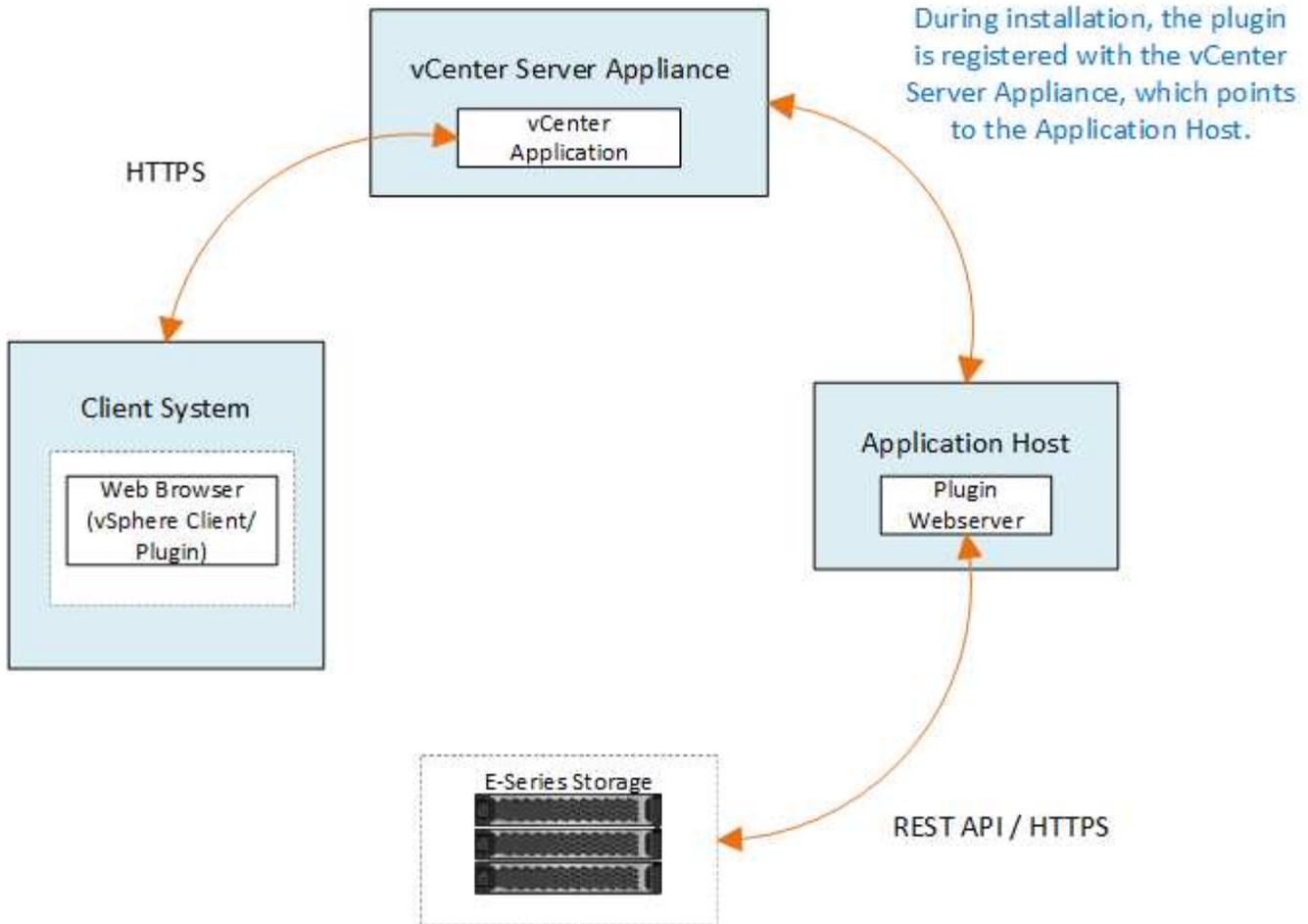
- 查看和管理网络中发现的存储阵列。
- 对包含多个存储阵列的组执行批处理操作。
- 在软件操作系统上执行升级。
- 将设置从一个存储阵列导入到另一个存储阵列。
- 配置卷，SSD 缓存，主机，主机集群，池，和卷组。
- 启动 System Manager 界面以在阵列上执行其他管理任务。



此插件不能直接替代System Manager界面、而是嵌入在存储阵列的每个控制器上。System Manager提供了其他管理功能；如果需要、您可以通过在插件的主视图中选择存储阵列、然后单击\*启动\*来打开System Manager。

要安装和运行插件 Web 服务器，插件需要在 VMware 环境中部署一个 VMware vCenter Server 设备以及一个应用程序主机。

有关 vCenter 环境中通信的详细信息，请参见下图。



## 接口概述

登录到插件后、主页将打开\*管理-全部\*。在此页面中、您可以查看和管理网络中发现的所有存储阵列。

## 导航边栏

导航边栏显示以下内容：

- 管理—发现网络中的存储阵列、启动阵列的System Manager、将设置从一个阵列导入到多个阵列、管理阵列组、升级SANtricity 操作系统以及配置存储。
- 证书管理—管理用于在浏览器和客户端之间进行身份验证的证书。
- 操作-查看批处理操作的进度、例如将设置从一个阵列导入到另一个阵列。



当存储阵列处于非最佳状态时、某些操作不可用。

- 支持—查看技术支持选项、资源和联系人。

## 支持的浏览器

适用于vCenter的存储插件可通过多种类型的浏览器进行访问。支持以下浏览器和版本。

- Google Chrome 89或更高版本

- Mozilla Firefox 80或更高版本
- Microsoft Edge 90或更高版本

#### 用户角色和权限

要访问适用于vCenter的存储插件中的任务、用户必须具有读写权限。默认情况下、所有已定义的VMware vCenter用户ID均无权在此插件中执行任务。

#### 配置概述

配置包括以下步骤：

1. ["安装并注册插件"](#)。
2. ["配置插件访问权限"](#)。
3. ["登录到插件界面"](#)。
4. ["发现存储阵列"](#)。
5. ["配置存储"](#)。

#### 了解更多信息

有关在 vSphere Client 中管理数据存储库的详细信息，请参见 ["VMware vSphere 文档"](#)。

## 入门

### 适用于vCenter的SANtricity存储插件的安装和升级要求

在安装或升级适用于vCenter的SANtricity 存储插件之前、请查看安装要求和升级注意事项。

#### 安装要求

您可以在Windows主机系统上安装和配置适用于vCenter的存储插件。插件安装包括以下要求。

要求	Description
支持的版本	<ul style="list-style-type: none"> <li>• VMware vCenter Server Appliance支持的版本：6.7U3J、7.0U1、7.0U2、7.0U3和8.0。</li> <li>• NetApp SANtricity OS 版本： 11.60.2 或更高版本</li> <li>• 支持的应用程序主机版本： Windows 2016、Windows 2019、Windows 2022。</li> </ul> <p>有关兼容性的详细信息、请参见 <a href="#">"NetApp 互操作性表工具"</a>。</p>
多个实例	您只能在Windows主机上安装一个适用于vCenter的Storage Plugin实例、并且只能将其注册到一个vCSA。

要求	Description
容量规划	适用于vCenter的存储插件需要足够的空间来执行和日志记录。确保您的系统满足以下可用磁盘空间要求： <ul style="list-style-type: none"> <li>• 所需安装空间—275 MB</li> <li>• 存储空间—275 MB + 200 MB (日志记录)</li> <li>• 系统内存—1.5 GB</li> </ul>
许可证	适用于vCenter的存储插件是一款免费的独立产品、不需要许可证密钥。但是，适用的版权和服务条款仍适用。

#### 升级注意事项

如果要从先前版本升级、请注意、必须在升级之前从vCSA中取消注册此插件。

- 升级期间、插件先前的大多数配置设置都会保留下来。这些设置包括用户密码，所有已发现的存储系统，服务器证书，可信证书和服务器运行时配置。
- 升级过程不会保留\*。vcenter.properties\*文件、因此您必须在升级之前取消注册此插件。升级成功后、您可以将此插件重新注册到vCSA。
- 先前加载在存储库中的所有SANtricity OS文件都会在升级期间被删除。

#### 安装或升级适用于vCenter的SANtricity存储插件

按照以下步骤安装适用于vCenter的存储插件并验证插件注册。您也可以按照以下说明升级此插件。

查看安装前提条件

请确保您的系统满足中的要求 "[查看安装和升级要求](#)"。



升级过程不会保留\*。vcenter.properties\*文件。如果要升级、则必须在升级之前取消注册此插件。升级成功后、您可以将此插件重新注册到vCSA。

#### 安装插件软件

要安装插件软件，请执行以下操作：

1. 将安装程序文件复制到要用作应用程序服务器的主机，然后访问下载安装程序的文件夹。
2. 双击安装文件：

```
santricity_storage_vcenterplugin-windows_x64- nn.nn.nnnn.exe
```

在上述文件名中， nn.nn.nn.nnnn 表示版本号。

3. 安装开始后、按照屏幕上的提示启用多项功能并输入一些配置参数。如有必要，您可以稍后在配置文件中更改其中任何一个选项。



在升级期间、系统不会提示您输入配置参数。



在安装期间、系统会提示您进行证书验证。如果要在插件和存储阵列之间强制执行证书验证、请保持选中状态。通过此强制实施，系统会检查存储阵列证书，使其受插件的信任。如果证书不可信，则不允许将其添加到插件中。如果要覆盖证书验证，请取消选中此复选框，以便可以使用自签名证书将所有存储阵列添加到插件中。要了解有关证书的详细信息，请参阅插件界面中提供的联机帮助。

4. 出现Webserver started消息时、单击\*确定\*完成安装、然后单击\*完成\*。
5. 运行 \* 服务 .msc\* 命令验证是否已成功安装应用程序服务器。
6. 验证是否已安装应用程序服务器（ VCP ）服务 \* 适用于 vCenter 的 NetApp SANtricity 存储插件 \* ，并且此服务已启动。



如有必要，您可以在安装后更改证书验证和 Web 服务端口设置。从安装目录中，打开 wsconfig.xml 文件。要删除存储阵列上的证书验证，请将 env key ， trust.all.arrays 更改为 true 。要更改 Web 服务端口，请将 sslport 值修改为 0-65535 范围内的所需端口值。确保使用的端口号未绑定到其他进程。完成后，保存所做的更改并重新启动插件 Web 服务器。如果在将插件注册到 vCSA 后插件 Web 服务器的端口值发生更改，则必须取消注册并重新注册插件，以便 vCSA 能够通过更改后的端口与插件 Web 服务器进行通信。

将此插件注册到 **vCenter Server** 设备

安装插件软件后，请向 vCSA 注册此插件。



此插件一次只能注册到一个 vCSA 。要注册到其他vCSA、您必须从当前vCSA中取消注册此插件、然后从应用程序主机中卸载它。然后、您可以重新安装此插件并将其注册到另一个vCSA。

1. 通过命令行打开提示符并导航到以下目录：

```
` <install directory>\vCenter-register\bin`
```

2. 执行 \* vCenter-register.bat\* 文件： `vcenter-register.bat ^ -action registerPlugin ^ -vcenterHostname <vCenter FQDN> ^ -username <Administrator username> ^`
3. 验证脚本是否成功。

这些日志将保存到 ` %install\_dir%/log/vc-registration.log` 中。

验证插件注册

安装插件并执行注册脚本后，验证此插件是否已成功注册到 vCenter Server 设备。

1. 打开 vCenter Server 设备的 vSphere Client 。
2. 在菜单栏上，选择菜单：管理员 [ 客户端插件 ] 。
3. 确保适用于vCenter的存储插件列为\*已启用\*。

如果插件列为 Disabled ，并显示一条错误消息，指出它无法与应用程序服务器通信，请验证为应用程序服务器定义的端口号是否已启用，以便通过可能正在使用的任何防火墙。默认应用程序服务器传输控制协议（ TCP ）端口号为 8445 。

## 配置SANtricity存储插件的vCenter访问权限

您可以为适用于 vCenter 的存储插件配置访问权限，其中包括用户，角色和权限。

查看所需的 vSphere 特权

要在 vSphere Client 中访问此插件，必须将您分配给具有适当 vSphere 权限的角色。具有 " 配置数据存储库 " vSphere 权限的用户可以对插件进行读写访问，而具有 " 浏览数据存储库 " 权限的用户可以进行只读访问。如果用户不具有上述权限，插件将显示 " 权限不足 " 消息。

插件访问类型	需要 vSphere 权限
读写 (配置)	数据存储库。配置
只读 (查看)	数据存储库。浏览

### 配置存储管理员角色

要为插件用户提供读 / 写权限，您可以创建，克隆或编辑角色。有关在 vSphere Client 中配置角色的详细信息，请参见 VMware 文档中心中的以下主题：

- ["创建自定义角色"](#)

### 访问角色操作

1. 从 vSphere Client 的主页中，从访问控制区域中选择 \* 管理员 \*。
2. 单击访问控制区域中的 \* 角色 \*。
3. 执行以下操作之一：
  - \* 创建新角色 \*：单击 \* 创建角色 \* 操作图标。
  - \* 克隆角色 \*：选择一个现有角色，然后单击 \* 克隆角色 \* 操作图标。
  - \* 编辑现有角色 \*：选择一个现有角色，然后单击 \* 编辑角色 \* 操作图标。



管理员角色不可编辑。

此时将显示相应的向导，具体取决于上述选择。

### 创建新角色

1. 在权限列表中，选择要分配给此角色的访问权限。

要允许对插件进行只读访问，请选择菜单： Datastore[Browse datastore]。要允许读写访问，请选择菜单： Datastore[Configure datastore]。

2. 如果需要，为列表分配其他权限，然后单击 \* 下一步 \*。
3. 为角色命名并提供问题描述。
4. 单击 \* 完成 \*。

## 克隆角色

1. 为角色命名并提供问题描述。
2. 单击 \* 确定 \* 完成向导。
3. 从列表中选择克隆的角色，然后单击 \* 编辑角色 \*。
4. 在权限列表中，选择要分配给此角色的访问权限。

要允许对插件进行只读访问，请选择菜单： Datastore[Browse datastore]。要允许读写访问，请选择菜单： Datastore[Configure datastore]。

5. 单击 \* 下一步 \*。
6. 如果需要，更新名称和问题描述。
7. 单击 \* 完成 \*。

## 编辑现有角色

1. 在权限列表中，选择要分配给此角色的访问权限。

要允许对插件进行只读访问，请选择菜单： Datastore[Browse datastore]。要允许读写访问，请选择菜单： Datastore[Configure datastore]。

2. 单击 \* 下一步 \*。
3. 如果需要，请更新名称或问题描述。
4. 单击 \* 完成 \*。

## 设置 vCenter Server 设备的权限

为角色设置权限后，您必须向 vCenter Server 设备添加权限。此权限允许给定的用户或组访问此插件。

1. 从菜单下拉列表中，选择 \* 主机和集群 \*。
2. 从访问控制区域中选择 \* vCenter Server Appliance\*。
3. 单击 \* 权限 \* 选项卡。
4. 单击 \* 添加权限 \* 操作图标。
5. 选择相应的域和用户 / 组。
6. 选择创建的允许读 / 写插件权限的角色。
7. 如果需要，启用 \* 传播到子系统 \* 选项。
8. 单击 \* 确定 \*。



您可以选择现有权限并对其进行修改，以使用创建的角色。\* 但是，请注意，角色必须具有与读取 / 写入插件权限相同的特权，以避免权限重写。 \*

要访问此插件，您必须使用对该插件具有读 / 写权限的用户帐户登录到 vSphere Client。

有关管理权限的详细信息，请参见 VMware 文档中心中的以下主题：

- "管理 vCenter 组件的权限"
- "角色和权限的最佳实践"

登录并导航适用于vCenter的SANtricity存储插件

您可以登录到适用于 vCenter 的存储插件以导航用户界面。

1. 登录到插件之前，请确保使用的是以下浏览器之一：
  - Google Chrome 89或更高版本
  - Mozilla Firefox 80或更高版本
  - Microsoft Edge 90或更高版本
2. 使用对插件具有读 / 写权限的用户帐户登录到 vSphere Client 。
3. 在 vSphere Client 主页页面中，单击 \* 适用于 vCenter 的 SANtricity 存储插件 \* 。

此插件将在 vSphere Client 窗口中打开。此时，插件的主页将打开至 \* 管理 - 全部 \* 。

4. 从左侧导航边栏访问存储管理任务：
  - \* 管理 \* —发现网络中的存储阵列，打开阵列的 System Manager ，将设置从一个阵列导入到多个阵列，管理阵列组，升级操作系统软件以及配置存储。
  - \* 证书管理 \* —管理用于在浏览器和客户端之间进行身份验证的证书。
  - \* 操作 \* —查看批处理操作的进度，例如将设置从一个阵列导入到另一个阵列。
  - \* 支持 \* —查看技术支持选项，资源和联系人。



当存储阵列处于非最佳状态时、某些操作不可用。

在适用于vCenter的SANtricity存储插件中发现存储阵列

要显示和管理存储资源，您必须使用适用于 vCenter 的存储插件界面发现网络中阵列的 IP 地址。

开始之前

- 您必须知道阵列控制器的网络 IP 地址（或地址范围）。
- 必须正确设置和配置存储阵列，并且您必须知道存储阵列登录凭据（用户名和密码）。

第 1 步：输入要发现的网络地址

步骤

1. 在 Manage 页面中，选择 \* 添加 / 发现 \* 。

此时将显示输入网络地址范围对话框。

2. 执行以下操作之一：
  - 要发现一个阵列，请选择 \* 发现单个存储阵列 \* 单选按钮，然后输入存储阵列中某个控制器的 IP 地址。

- 要发现多个存储阵列，请选择 \* 发现网络范围内的所有存储阵列 \* 单选按钮，然后输入起始网络地址和结束网络地址，以便在本地子网络中搜索。

3. 单击 \* 启动发现 \* 。

发现过程开始时，对话框会在发现存储阵列时显示这些阵列。完成发现过程可能需要几分钟时间。

如果未发现任何可管理的阵列，请验证这些存储阵列是否已正确连接到您的网络，以及其分配的地址是否在范围内。单击 \* 新发现参数 \* 以返回到 " 添加 / 发现 " 页面。

4. 选中要添加到管理域的任何存储阵列旁边的复选框。

系统会对要添加到管理域的每个阵列执行凭据检查。在继续操作之前，您可能需要解决不可信证书的任何问题。

5. 单击 \* 下一步 \* 继续执行向导中的下一步。

如果存储阵列具有有效证书，请转至 [第 3 步：提供密码](#)。

如果任何存储阵列没有有效证书，则会显示解析自签名证书对话框。转至 [第 2 步：在发现期间解析不可信的证书](#)。

如果要导入 CA 签名的证书，请退出发现向导并单击左侧面板中的 \* 证书管理 \* 。有关详细说明，请参见联机帮助。

#### 第 2 步：在发现期间解析不可信的证书

在继续执行发现过程之前，您必须解决任何证书问题。

1. 如果 " 解析自签名证书 " 对话框打开，请查看为不可信证书显示的信息。有关详细信息，您还可以单击表末尾的省略号，然后从弹出菜单中选择 \* 查看 \* 。
2. 执行以下操作之一：
  - 如果您信任与发现的存储阵列的连接，请单击 \* 下一步 \* ，然后单击 \* 是 \* 确认并继续到向导中的下一个对话框。自签名证书将标记为可信证书，存储阵列将添加到插件中。
  - 如果您不相信与存储阵列的连接，请选择 \* 取消 \* 并在添加任何存储阵列之前验证每个存储阵列的安全证书策略。
3. 单击 \* 下一步 \* 继续执行向导中的下一步。

#### 第 3 步：提供密码

作为发现的最后一步，您必须输入要添加到管理域的存储阵列的密码。

1. 对于每个已发现的阵列，请在字段中输入其管理员密码。
2. 单击 \* 完成 \* 。

系统可能需要几分钟才能连接到指定的存储阵列。完成此过程后，存储阵列将添加到管理域中并与选定组（如果指定）关联。

在适用于vCenter的SANtricity存储插件中配置存储

要配置存储，请创建卷，将卷分配给主机，然后将卷分配给数据存储库。

#### 第1步：创建卷

卷是一种数据容器，用于管理和组织存储阵列上的存储空间。您可以使用存储阵列上的可用存储容量创建卷，这有助于组织系统的资源。"卷"的概念类似于在计算机上使用文件夹 / 目录来组织文件以实现快速访问。

卷是主机唯一可见的数据层。在 SAN 环境中，卷会映射到逻辑单元号（LUN）。这些 LUN 用于保存可使用存储阵列支持的一个或多个主机访问协议访问的用户数据。

#### 步骤

1. 从管理页面中，选择存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择菜单：创建 [ 卷 ]。

此时将显示选择主机对话框。

4. 从下拉列表中，选择要将卷分配到的特定主机或主机集群，或者选择稍后再分配主机或主机集群。
5. 要继续为选定主机或主机集群创建卷，请单击 \* 下一步 \*。

此时将显示选择工作负载对话框。工作负载包含具有类似特征的卷，这些卷根据工作负载支持的应用程序类型进行了优化。您可以定义工作负载，也可以选择现有工作负载。

6. 执行以下操作之一：
  - 选择 \* 为现有工作负载创建卷 \* 选项，然后从下拉列表中选择工作负载。
  - 选择 \* 创建新工作负载 \* 选项为支持的应用程序或 " 其他 " 应用程序定义新的工作负载，然后执行以下步骤：
    - i. 从下拉列表中，选择要为其创建新工作负载的应用程序的名称。如果未列出要在此存储阵列上使用的应用程序，请选择 " 其他 " 条目之一。
    - ii. 输入要创建的工作负载的名称。
7. 单击 \* 下一步 \*。如果您的工作负载与支持的应用程序类型关联，请输入所请求的信息；否则，请转到下一步。

此时将显示添加 / 编辑卷对话框。在此对话框中，您可以从符合条件的池或卷组创建卷。对于每个符合条件的池和卷组，将显示可用驱动器数和总可用容量。对于某些特定于应用程序的工作负载，每个符合条件的池或卷组都会根据建议的卷配置显示建议的容量，并以 GiB 显示剩余可用容量。对于其他工作负载，在将卷添加到池或卷组并指定报告的容量时，将显示建议的容量。

8. 开始添加卷之前，请阅读下表中的准则。

字段	Description
可用容量	由于卷是从池或卷组创建的，因此您选择的池或卷组必须具有足够的可用容量。

字段	Description
数据保证 (DA)	<p>要创建启用了 DA 的卷，您计划使用的主机连接必须支持 DA。</p> <ul style="list-style-type: none"> <li>• 如果要创建启用了 DA 的卷、请选择一个支持 DA 的池或卷组(在 Pool and volume group candidates 表中的 "DA" 旁边查找 * 是 *)。</li> <li>• DA 功能在池和卷组级别提供。DA 保护功能可检查并更正数据通过控制器向下传输到驱动器时可能发生的错误。为新卷选择支持 DA 的池或卷组可确保检测到并更正任何错误。</li> <li>• 如果存储阵列中控制器上的任何主机连接不支持 DA，则关联的主机将无法访问已启用 DA 的卷上的数据。</li> </ul>
驱动器安全性	<p>要创建启用了安全保护的卷，必须为存储阵列创建安全密钥。</p> <ul style="list-style-type: none"> <li>• 如果要创建启用了安全保护的卷、请选择一个支持安全的池或卷组(在池和卷组候选项表中、查找 "Secure-Capable" 旁边的 * 是 *)。</li> <li>• 驱动器安全功能在池和卷组级别提供。支持安全的驱动器可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。启用了安全保护的驱动器会在写入期间对数据进行加密，并在读取期间使用唯一的加密密钥对数据进行解密。</li> <li>• 池或卷组可以同时包含支持安全和不支持安全的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。</li> </ul>
资源配置	<p>要创建资源配置的卷，所有驱动器都必须是具有已取消分配或未写入逻辑块错误 (DULBE) 选项的 NVMe 驱动器。</p>

9. 根据您在上一步中选择的是 "其他" 工作负载还是应用程序专用工作负载、选择以下操作之一：

- \* 其他 \* —单击要用于创建一个或多个卷的每个池或卷组中的 \* 添加新卷 \*。
- \* 应用程序专用工作负载 \* —单击 \* 下一步 \* 接受系统为选定工作负载建议的卷和特征，或者单击 \* 编辑卷 \* 更改，添加或删除系统为选定工作负载建议的卷和特征。

此时将显示以下字段。

字段	Description
卷名称	<p>在卷创建序列期间，系统会为卷分配默认名称。您可以接受默认名称，也可以提供一个更具描述性的名称来指示卷中存储的数据类型。</p>
已报告容量	<p>定义新卷的容量以及要使用的容量单位 (MiB, GiB 或 TiB)。对于厚卷，最小容量为 1 MiB，最大容量由池或卷组中驱动器的数量和容量决定。池中的容量以 4 GiB 为增量进行分配。分配的容量不是 4 GiB 的倍数，但不可用。要确保整个容量可用，请以 4 GiB 为增量指定容量。如果存在不可用的容量，则要重新获得该容量，唯一的方法是增加卷的容量。</p>
卷类型	<p>如果选择 "应用程序专用工作负载"、则会显示卷类型字段。这表示为特定于应用程序的工作负载创建的卷类型。</p>

字段	Description
卷块大小（仅限 EF300 和 EF600）	<p>显示了可为卷创建的块大小：</p> <ul style="list-style-type: none"> <li>• 512 – 512 字节</li> <li>• 4 k – 4 , 096 字节</li> </ul>
区块大小	<p>显示了分段大小调整设置，此设置仅适用于卷组中的卷。您可以更改区块大小以优化性能。</p> <ul style="list-style-type: none"> <li>• 允许的分段大小转换 * —系统将确定允许的分段大小转换。与当前区块大小的过渡不适当的区块大小在下拉列表中不可用。允许的过渡通常是当前区块大小的两倍或一半。例如，如果当前卷分段大小为 32 KiB，则允许使用新的卷分段大小 16 KiB 或 64 KiB。</li> <li>• 已启用 SSD 缓存的卷 * —您可以为已启用 SSD 缓存的卷指定 4-KiB 分段大小。确保仅为支持 SSD 缓存且处理小块 I/O 操作的卷（例如，16 KiB I/O 块大小或更小）选择 4-KiB 区块大小。如果为处理大型块顺序操作且已启用 SSD 缓存的卷选择 4 KiB 作为分段大小，则性能可能会受到影响。</li> <li>• 更改区块大小所需的时间 * —更改卷区块大小所需的时间取决于以下变量： <ul style="list-style-type: none"> <li>◦ 主机的 I/O 负载</li> <li>◦ 卷的修改优先级</li> <li>◦ 卷组中的驱动器数量</li> <li>◦ 驱动器通道的数量</li> <li>◦ 存储阵列控制器的处理能力</li> </ul> </li> </ul> <p>更改卷的区块大小时，I/O 性能会受到影响，但数据仍可用。</p>
支持安全保护	<p>只有当池或卷组中的驱动器支持加密时，"支持安全"旁边才会显示 * 是 *。驱动器安全性可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。只有在启用了驱动器安全功能且为存储阵列设置了安全密钥时，此选项才可用。池或卷组可以同时包含支持安全和不支持安全的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。</p>
da.	<p>只有当池或卷组中的驱动器支持数据保证（Data Assurance，DA）时，"DA"旁边才会显示 * 是 *。DA 可提高整个存储系统的数据完整性。通过 DA，存储阵列可以检查在数据通过控制器向下传输到驱动器时可能发生的错误。对新卷使用 DA 可确保检测到任何错误。</p>

10. 要继续对选定应用程序执行卷创建序列，请单击 \* 下一步 \*。

11. 在最后一步中，查看要创建的卷的摘要，并进行任何必要的更改。要进行更改，请单击 \* 返回 \*。对卷配置感到满意后，单击 \* 完成 \*。

第2步：创建主机访问权限并分配卷

可以手动创建主机：

- \* 手动 \* —在手动创建主机期间，您可以通过从列表中选择主机端口标识符或手动输入这些标识符来关联主

机端口标识符。创建主机后，如果您计划共享对卷的访问，则可以为其分配卷或将其添加到主机集群。

## 手动创建主机

### 开始之前

请阅读以下准则：

- 您必须已在环境中添加或发现存储阵列。
- 您必须定义与主机关联的主机标识符端口。
- 请确保提供与主机分配的系统名称相同的名称。
- 如果您选择的名称已在使用中，则此操作不会成功。
- 名称长度不能超过 30 个字符。

### 步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 单击菜单：创建 [ 主机 ]。

此时将显示创建主机对话框。

4. 根据需要选择主机设置。

字段	Description
Name	键入新主机的名称。
主机操作系统类型	从下拉列表中选择新主机上运行的操作系统。
主机接口类型	(可选) 如果存储阵列支持多种类型的主机接口，请选择要使用的主机接口类型。

字段	Description
主机端口	<p>执行以下操作之一：</p> <ul style="list-style-type: none"> <li>• 选择I/O接口-通常、主机端口应已登录并可从下拉列表中使用。您可以从列表中选择主机端口标识符。</li> <li>• 手动添加-如果列表中未显示主机端口标识符、则表示主机端口尚未登录。可以使用 HBA 实用程序或 iSCSI 启动程序实用程序来查找主机端口标识符并将其与主机关联。</li> </ul> <p>您可以手动输入主机端口标识符，也可以将它们从实用程序（一次一个）复制 / 粘贴到主机端口字段中。</p> <p>您必须一次选择一个主机端口标识符才能将其与主机关联，但您可以继续选择与主机关联的任意数量的标识符。每个标识符都会显示在主机端口字段中。如有必要，您还可以通过选择标识符旁边的 * X * 来删除该标识符。</p>
设置 CHAP 启动程序密钥	<p>(可选)如果您选择或手动输入具有iSCSI IQN的主机端口、并且希望要求尝试访问存储阵列的主机使用质询握手身份验证协议(CHAP)进行身份验证、请选中*设置CHAP启动程序密钥*复选框。对于您选择或手动输入的每个 iSCSI 主机端口，请执行以下操作：</p> <ul style="list-style-type: none"> <li>• 输入在每个 iSCSI 主机启动程序上为 CHAP 身份验证设置的相同 CHAP 密钥。如果您使用相互 CHAP 身份验证（双向身份验证，可使主机向存储阵列验证自身，并使存储阵列向主机验证自身），则还必须在初始设置或通过更改设置为存储阵列设置 CHAP 密钥。</li> <li>• 如果不需要主机身份验证，请将此字段留空。</li> </ul> <p>目前，唯一使用的 iSCSI 身份验证方法是 CHAP 。</p>

5. 单击 \* 创建 \* 。

6. 如果需要更新主机信息，请从表中选择主机，然后单击 \* 查看 / 编辑设置 \* 。

成功创建主机后，系统会为为为为主机配置的每个主机端口创建一个默认名称（用户标签）。默认别名为 ` < 主机名端口号 > `。例如，为主机 IPT 创建的第一个端口的默认别名为 ipt\_1 。

7. 接下来，您必须将卷分配给主机或主机集群，以便用于 I/O 操作。选择菜单：配置 [ 配置主机 ] 。

此时将打开配置主机页面。

8. 选择要将卷分配到的主机或主机集群，然后单击 \* 分配卷 \* 。

此时将显示一个对话框，其中列出了可分配的所有卷。您可以对任意列进行排序，也可以在筛选器框中键入某些内容，以便于查找特定卷。

9. 选中要分配的每个卷旁边的复选框，或者选中表标题中的复选框以选择所有卷。

10. 单击 \* 分配 \* 以完成此操作。

系统将执行以下操作：

- 分配的卷将收到下一个可用的 LUN 编号。主机使用此 LUN 编号来访问此卷。
- 用户提供的卷名称将显示在与主机关联的卷列表中。如果适用，出厂配置的访问卷也会显示在与主机关联的卷列表中。

第3步：在vSphere Client中创建数据存储库

要在vSphere Client中创建数据存储库、请参见 ["在 vSphere Client 中创建 VMFS 数据存储库"](#) 主题。

通过增加卷容量来增加现有数据存储库的容量

您可以使用池或卷组中的可用容量来增加卷的报告容量（向主机报告的容量）。

开始之前

请确保：

- 卷的关联池或卷组具有足够的可用容量。
- 卷处于最佳状态，不处于任何修改状态。
- 卷中未使用任何热备用驱动器。（仅适用于卷组中的卷。）



只有某些操作系统才支持增加卷的容量。如果在不支持 LUN 扩展的主机操作系统上增加卷容量，则扩展的容量将不可用，并且无法还原原始卷容量。

步骤

1. 导航到 vSphere Client 中的插件。
2. 在插件中，选择所需的存储阵列。
3. 单击 \* 配置 \* 并选择 \* 管理卷 \*。
4. 选择要增加容量的卷，然后选择 \* 增加容量 \*。

此时将显示确认增加容量对话框。

5. 选择 \* 是 \* 继续。

此时将显示增加报告的容量对话框。

此对话框显示卷当前报告的容量以及卷关联的池或卷组中可用的容量。

6. 使用 \* 通过添加增加报告容量 ... \* 框向当前可用报告容量添加容量。您可以将容量值更改为以兆字节（MiB），吉字节（GiB）或太字节（TiB）为单位显示。
7. 单击 \* 增加 \*。
8. 查看近期任务窗格，了解当前正在对选定卷运行的增加容量操作的进度。此操作可能会很长，并且可能会影响系统性能。
9. 卷容量完成后、您必须手动增加VMFS大小、以便与中所述的匹配 ["增加 vSphere Client 中的 VMFS 数据存储库容量"](#) 主题。

通过添加卷来增加现有数据存储库的容量

1. 您可以通过添加卷来增加数据存储库的容量。按照中的步骤进行操作 [\[第1步：创建卷\]](#)。
2. 接下来，将卷分配给所需主机以增加数据存储库的容量。

请参见 ["增加 vSphere Client 中的 VMFS 数据存储库容量"](#) 主题、了解更多信息。

在适用于vCenter的SANtricity存储插件中查看存储系统状态

您可以从适用于vCenter的存储插件或vSphere Client查看系统状态。

1. 从vSphere Client中打开此插件。
2. 从以下面板查看状态：
  - 存储阵列状态—转到\*管理-全部\*面板。对于每个已发现的阵列、该行提供了一个状态列。
  - 正在执行的操作—单击侧面板上的\*操作\*可查看所有长时间运行的任务、例如导入设置。您还可以从配置下拉列表中查看长时间运行的操作。对于"正在执行的操作"对话框中列出的每个操作、将显示完成操作的百分比以及完成该操作所需的预计剩余时间。在某些情况下、您可以停止某个操作或将其置于较高或较低的优先级。如果需要、可使用操作列中的链接停止或更改操作的优先级。



阅读对话框中提供的所有注意事项文本、尤其是在停止操作时。

下表列出了可能为插件显示的操作。其他操作可能也会显示在System Manager界面中。

操作	操作的可能状态	可以执行的操作
卷创建(仅限大于64 TiB的厚池卷)	正在进行中	无
卷删除(仅限大于64 TiB的厚池卷)	正在进行中	无
向池或卷组添加容量	正在进行中	无
更改卷的RAID级别	正在进行中	无
减少池的容量	正在进行中	无
检查池卷在即时可用性格式(IAF)操作上的剩余时间	正在进行中	无
检查卷组的数据冗余	正在进行中	无
初始化卷	正在进行中	无
增加卷的容量	正在进行中	无
更改卷的区块大小	正在进行中	无

## 管理证书

了解如何在适用于vCenter的SANtricity存储插件中管理证书

通过适用于vCenter的存储插件中的证书管理、您可以创建证书签名请求(Certificate Signing Requests、CSR)、导入证书以及管理现有证书。

## 什么是证书?

证书是数字文件、用于标识网站和服务器等在线实体、以实现Internet上的安全通信。它们可确保Web通信仅在指定服务器和客户端之间以加密格式单独传输、不会被更改。使用适用于vCenter的存储插件、您可以管理主机管理系统上的浏览器以及发现的存储阵列中的控制器的证书。

证书可以由可信的颁发机构签名、也可以是自签名证书。"签名"只是指有人验证了所有者的身份并确定其设备可以受信任。

存储阵列会在每个控制器上随附一个自动生成的自签名证书。您可以继续使用自签名证书、也可以获取CA签名证书、以便在控制器和主机系统之间建立更安全的连接。



虽然CA签名证书可提供更好的安全保护(例如、防止中间人攻击)、但如果您的网络较大、则还需要支付昂贵的费用。相比之下、自签名证书的安全性较低、但它们是免费的。因此、自签名证书最常用于内部测试环境、而不是生产环境。

## 签名证书

签名证书由可信的第三方组织证书颁发机构(CA)进行验证。签名证书包括有关实体(通常是服务器或网站)所有者的详细信息、证书问题描述 和到期日期、实体的有效域以及由字母和数字组成的数字签名。

当您打开浏览器并输入Web地址时、系统会在后台执行证书检查过程、以确定您是否要连接到包含有效的CA签名证书的网站。通常、使用签名证书进行安全保护的站点会在地址中包含挂锁图标和https标志。如果您尝试连接到不包含CA签名证书的网站、浏览器将显示一条警告、指出此站点不安全。

CA会在应用程序过程中执行一些步骤来验证您的身份。他们可能会向您的注册业务发送电子邮件、验证您的业务地址以及执行HTTP或DNS验证。应用程序过程完成后、CA会向您发送数字文件、以便在主机管理系统上加载。通常、这些文件包括以下信任链:

- 根-层次结构顶部是根证书、其中包含用于对其他证书进行签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
- 中间证书—从根分层是中间证书。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。
- 服务器—链的底部是服务器证书、用于标识您的特定实体、例如网站或其他设备。存储阵列中的每个控制器都需要一个单独的服务器证书。

## 自签名证书

存储阵列中的每个控制器都包含一个预安装的自签名证书。自签名证书与CA签名证书类似、只是它由实体所有者而非第三方进行验证。与CA签名证书一样、自签名证书也包含自己的专用密钥、并确保数据经过加密并通过HTTPS连接在服务器和客户端之间发送。

自签名证书不受浏览器的"信任"。每次尝试连接到仅包含自签名证书的网站时、浏览器都会显示一条警告消息。您必须单击警告消息中允许您继续访问网站的链接;这样、您实际上就是在接受自签名证书。

## 管理证书

打开插件时、浏览器会尝试通过检查数字证书来验证管理主机是否为可信源。如果浏览器找不到CA签名的证书、则会打开一条警告消息。从该站点、您可以继续访问该网站以接受该会话的自签名证书。您还可以从CA获取签名的数字证书、以便不再显示警告消息。

## 可信证书

在插件会话期间、当您尝试访问没有CA签名证书的控制器的时、可能会看到其他安全消息。在这种情况下、您可以永久信任自签名证书、也可以为控制器导入CA签名证书、以便插件可以对来自这些控制器的传入客户端请求进行身份验证。

在适用于vCenter的SANtricity存储插件中使用CA签名的证书

您可以获取并导入CA签名的证书、以安全访问托管适用于vCenter的存储插件的管理系统。

使用CA签名证书分为三步操作步骤：

- [第1步：完成CSR文件。](#)
- [第2步：提交CSR文件。](#)
- [\[第3步：导入管理证书\]。](#)

### 第1步：完成CSR文件

您必须先生成证书签名请求(CSR)文件、用于标识您的组织以及运行插件的主机系统。或者、您也可以使用OpenSSL等工具生成CSR文件、然后跳至 [第2步：提交CSR文件。](#)

### 步骤

1. 选择\*证书管理\*。
2. 从\*管理\*选项卡中、选择\*完成CSR\*。
3. 输入以下信息、然后单击\*下一步\*：
  - 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
  - 组织单位(可选)—组织中负责处理证书的部门。
  - 城市/位置-主机系统或业务所在的城市。
  - 省/自治区/直辖市(可选)—主机系统或业务所在的省/自治区/直辖市。
  - 国家/地区ISO代码—您所在国家/地区的两位数ISO (国际标准化组织)代码、例如美国。
4. 输入有关运行此插件的主机系统的以下信息：
  - 公用名—运行插件的主机系统的IP地址或DNS名称。请确保此地址正确无误；它必须与您在浏览器中输入的地址完全匹配才能访问此插件。请勿包含http://或https://。DNS名称不能以通配符开头。
  - 备用IP地址-如果公用名称为IP地址、则可以选择为主机系统输入任何其他IP地址或别名。对于多个条目、请使用逗号分隔格式。
  - 备用DNS名称-如果公用名称为DNS名称、请输入主机系统的任何其他DNS名称。对于多个条目、请使用逗号分隔格式。如果没有备用DNS名称、但您在第一个字段中输入了DNS名称、请将此名称复制到此处。DNS名称不能以通配符开头。
5. 确保主机信息正确无误。否则、从CA返回的证书将在您尝试导入时失败。
6. 单击 \* 完成 \*。

## 第2步：提交CSR文件

创建证书签名请求(CSR)文件后、您可以将生成的CSR文件发送到CA、以接收托管此插件的系统的已签名管理证书。

E系列系统要求对签名证书使用PEM格式(Base64 ASCII编码)、其中包括以下文件类型：.pem、.crt、.cer或.key。

### 步骤

1. 找到已下载的CSR文件。

下载内容的文件夹位置取决于您的浏览器。

2. 将CSR文件提交到CA (例如VeriSign或DigiCert)、并请求PEM格式的签名证书。



将CSR文件提交到CA后、请勿重新生成其他CSR文件。

每当生成CSR时、系统都会创建一个专用密钥对和公有 密钥对。公有 密钥是CSR的一部分、而私钥则保留在系统的密钥库中。当您收到签名证书并将其导入时、系统会确保私钥和公有 密钥都是原始对。如果密钥不匹配、则签名证书将不起作用、您必须从CA请求新证书。

## 第3步：导入管理证书

从证书颁发机构(CA)收到签名证书后、请将这些证书导入到安装此插件的主机系统中。

### 开始之前

- 您必须拥有来自CA的签名证书。这些文件包括根证书、一个或多个中间证书以及服务器证书。
- 如果CA提供了一个链式证书文件(例如.p7b文件)、则必须将链式文件解压缩到各个文件中：根证书、一个或多个中间证书以及服务器证书。您可以使用Windows certmgr实用程序解压缩文件(右键单击并选择菜单：所有任务[导出])。建议使用64位编码。导出完成后、系统将为链中的每个证书文件显示一个CER"文件。
- 您必须将证书文件复制到运行插件的主机系统。

### 步骤

1. 选择\*证书管理\*。
2. 从\*管理\*选项卡中、选择\*导入\*。

此时将打开一个对话框、用于导入证书文件。

3. 单击\*浏览\*以首先选择根证书和中间证书文件、然后选择服务器证书。如果从外部工具生成CSR、则还必须导入随CSR一起创建的私钥文件。

文件名将显示在对话框中。

4. 单击 \* 导入 \*。

### 结果

这些文件将上传并进行验证。证书信息将显示在证书管理页面上。

在适用于vCenter的SANtricity存储插件中重置管理证书

对于托管适用于vCenter的存储插件的管理系统、您可以将管理证书还原到原始出厂自签名状态。

关于此任务

此任务将从运行适用于vCenter的存储插件的主机系统中删除当前管理证书。重置证书后、主机系统将恢复为使用自签名证书。

步骤

1. 选择\*证书管理\*。
2. 从\*管理\*选项卡中、选择\*重置\*。

此时将打开确认重置管理证书对话框。

3. 在字段中键入reset、然后单击\*重置\*。

浏览器刷新后、浏览器可能会阻止对目标站点的访问并报告此站点正在使用HTTP严格传输安全性。切换回自签名证书时会出现此情况。要清除阻止访问目标的条件、您必须从浏览器中清除浏览数据。

结果

系统将恢复为使用服务器中的自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

在适用于vCenter的SANtricity存储插件中导入阵列证书

如有必要、您可以导入存储阵列的证书、以便这些阵列可以在托管适用于vCenter的Storage Plugin的系统上进行身份验证。证书可以由证书颁发机构(CA)签名、也可以是自签名证书。

开始之前

如果要导入可信证书、则必须使用System Manager为存储阵列控制器导入这些证书。

步骤

1. 选择\*证书管理\*。
2. 选择\*可信\*选项卡。

此页面显示为存储阵列报告的所有证书。

3. 选择菜单：Import[证书]以导入CA证书、选择菜单：Import[自签名存储阵列证书]以导入自签名证书。
4. 要限制此视图、您可以使用\*显示证书...\*筛选字段、也可以单击列标题之一对证书行进行排序。
5. 在对话框中、选择证书、然后单击\*导入\*。

已上传并验证此证书。

在适用于vCenter的SANtricity存储插件中查看证书

您可以查看证书的摘要信息、其中包括使用证书的组织、颁发证书的机构、有效期以及指

纹(唯一标识符)。

步骤

1. 选择\*证书管理\*。
2. 选择以下选项卡之一：
  - 管理-显示托管插件的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问插件。
  - 可信-显示插件可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。
3. 要查看有关证书的详细信息、请选择其行、选择行末尾的省略号、然后单击\*查看\*或\*导出\*。

在适用于vCenter的SANtricity存储插件中导出证书

您可以导出证书以查看其完整详细信息。

开始之前

要打开导出的文件、您必须具有证书查看器应用程序。

步骤

1. 选择\*证书管理\*。
2. 选择以下选项卡之一：
  - 管理-显示托管插件的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问插件。
  - 可信-显示插件可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。
3. 从页面中选择一个证书、然后单击行末尾的省略号。
4. 单击\*导出\*、然后保存证书文件。
5. 在证书查看器应用程序中打开文件。

在适用于vCenter的SANtricity存储插件中删除可信证书

您可以删除一个或多个不再需要的证书、例如已过期的证书。

开始之前

请先导入新证书、然后再删除旧证书。



请注意、删除根证书或中间证书可能会影响多个存储阵列、因为这些阵列可以共享相同的证书文件。

步骤

1. 选择\*证书管理\*。
2. 选择\*可信\*选项卡。
3. 在表中选择一个或多个证书、然后单击\*删除\*。



对于预安装的证书、删除功能不可用。

此时将打开确认删除可信证书对话框。

4. 确认删除、然后单击\*删除\*。

此证书将从表中删除。

在适用于vCenter的SANtricity存储插件中解析不可信证书

在证书页面中、您可以通过从存储阵列导入自签名证书或导入可信第三方颁发的证书颁发机构(CA)证书来解析不可信的证书。

开始之前

如果您计划导入CA签名的证书、请确保：

- 您已为存储阵列中的每个控制器生成证书签名请求(.csr文件)、并将其发送给CA。
- CA返回了可信证书文件。
- 证书文件可在本地系统上使用。

关于此任务

如果存储阵列尝试与插件建立安全连接、但此连接无法确认为安全连接、则会发生不可信证书。如果满足以下任一条件、您可能需要安装其他受信任的CA证书：

- 您最近添加了一个存储阵列。
- 一个或两个证书已过期或已撤销。
- 一个或两个证书缺少根证书或中间证书。

步骤

1. 选择\*证书管理\*。
2. 选择\*可信\*选项卡。

此页面显示为存储阵列报告的所有证书。

3. 选择菜单：Import[证书]以导入CA证书、选择菜单：Import[自签名存储阵列证书]以导入自签名证书。
4. 要限制此视图、您可以使用\*显示证书...\*筛选字段、也可以单击列标题之一对证书行进行排序。
5. 在对话框中、选择证书、然后单击\*导入\*。

已上传并验证此证书。

## 管理阵列

了解如何在适用于vCenter的SANtricity存储插件中管理存储阵列

使用添加/发现功能在vCenter的存储插件中查找和添加要管理的存储阵列。在管理页面

## 中、您还可以重命名、删除这些已发现阵列并提供新密码。

### 发现阵列的注意事项

要使插件能够显示和管理存储资源、您必须在组织的网络中发现要管理的存储阵列。您可以发现并添加一个或多个阵列。

### 多个存储阵列

如果您选择发现多个阵列、则输入一个网络IP地址范围、然后系统将尝试单独连接到该范围中的每个IP地址。成功访问的任何存储阵列都会显示在此插件中、然后您可以将其添加到管理域中。

### 单个存储阵列

如果您选择发现单个阵列、请为存储阵列中的一个控制器输入单个IP地址、然后将该阵列添加到管理域中。



插件仅会发现并显示分配给控制器的范围内的单个IP地址或IP地址。如果为这些控制器分配的备用控制器或IP地址不在此单个IP地址或IP地址范围内、则插件将不会发现或显示它们。但是、添加存储阵列后、所有关联的IP地址都将被发现并显示在管理视图中。

### 用户凭据

您必须为要添加的每个存储阵列提供管理员密码。

### 证书

在发现过程中、系统会验证发现的存储阵列是否正在使用受信任源的证书。系统对通过浏览器与建立的所有连接使用两种基于证书的身份验证：

- 可信证书—如果证书链中的一个或两个控制器证书已过期、已撤销或缺少证书、则可能需要安装证书颁发机构提供的其他可信证书。
- 自签名证书-阵列也可以使用自签名证书。如果您尝试在未导入签名证书的情况下发现阵列、则此插件还提供了一个步骤、可用于接受自签名证书。存储阵列的自签名证书将标记为可信、存储阵列将添加到插件中。如果您不相信与存储阵列的连接、请选择\*取消\*并验证存储阵列的安全证书策略、然后再将存储阵列添加到插件。

### 存储阵列状态

打开适用于vCenter的存储插件时、将与每个存储阵列建立通信、并显示每个存储阵列的状态。

在\*管理-全部\*页面中、您可以查看存储阵列的状态和存储阵列连接的状态。

Status	表示
最佳	存储阵列处于最佳状态。没有证书问题、密码有效。
密码无效	提供的存储阵列密码无效。
不可信证书	与存储阵列的一个或多个连接不可信、因为HTTPS证书是自签名的、尚未导入、或者证书是CA签名的、并且根和中间CA证书尚未导入。
需要关注	存储阵列存在问题、需要您进行干预才能进行更正。

Status	表示
锁定	存储阵列处于已锁定状态。
未知	从未联系过存储阵列。如果插件正在启动且尚未与存储阵列进行联系、或者存储阵列处于脱机状态且自插件启动以来从未进行过联系、则可能会发生这种情况。
脱机	插件先前已与存储阵列联系、但现在已断开与该存储阵列的所有连接。

#### 插件界面与System Manager的对比

您可以使用适用于vCenter的存储插件执行存储阵列上的基本操作任务；但是、有时可能需要启动System Manager来执行插件中不可用的任务。

System Manager是存储阵列控制器上的嵌入式应用程序、它通过以太网管理端口连接到网络。System Manager包括所有基于阵列的功能。

下表可帮助您确定是否可以使用插件界面或System Manager界面执行特定存储阵列任务。

功能	插件界面	System Manager界面
对包含多个存储阵列的组执行批处理操作	是的。	否操作在一个阵列上执行。
升级SANtricity OS固件	是的。批处理操作中的一个或多个阵列。	是的。仅限单个阵列。
将设置从一个阵列导入到多个阵列	是的。	否
主机和主机集群管理(创建、分配卷、更新和删除)	是的。	是的。
池和卷组管理(创建、更新、启用安全性和删除)	是的。	是的。
卷管理(创建、调整大小、更新和删除)	是的。	是的。
SSD缓存管理(创建、更新和删除)	是的。	是的。
镜像和快照管理	否	是的。
硬件管理(查看控制器状态、配置端口连接、使控制器脱机、启用热备件、擦除驱动器、等)	否	是的。
管理警报(电子邮件、SNMP和系统日志)	否	是的。
安全密钥管理	否	是的。
控制器的证书管理	否	是的。
控制器访问管理(LDAP、SAML等)	否	是的。
AutoSupport 管理	否	是的。

在适用于vCenter的SANtricity存储插件中发现存储阵列

要在适用于vCenter的存储插件中显示和管理存储资源、您必须发现网络中阵列的IP地址。

开始之前

- 您必须知道阵列控制器的网络 IP 地址（或地址范围）。
- 必须正确设置和配置存储阵列。
- 存储阵列密码必须使用System Manager的"访问管理"图块进行设置。

关于此任务

阵列发现是一种多步骤操作步骤：

- [第 1 步：输入要发现的网络地址](#)
- [第 2 步：在发现期间解析不可信的证书](#)
- [第 3 步：提供密码](#)

第 1 步：输入要发现的网络地址

要发现存储阵列、首先需要输入一个IP地址或一个IP地址范围、以便在本地子网络中进行搜索。添加/发现功能将打开一个向导、指导您完成发现过程。

步骤

1. 从\*管理\*页面中、选择\*添加/发现\*。

此时将显示输入网络地址范围对话框。

2. 执行以下操作之一：

- 要发现一个阵列，请选择 \* 发现单个存储阵列 \* 单选按钮，然后输入存储阵列中某个控制器的 IP 地址。
- 要发现多个存储阵列，请选择 \* 发现网络范围内的所有存储阵列 \* 单选按钮，然后输入起始网络地址和结束网络地址，以便在本地子网络中搜索。

3. 单击 \* 启动发现 \* 。

发现过程开始时，对话框会在发现存储阵列时显示这些阵列。完成发现过程可能需要几分钟时间。



如果未发现任何可管理的阵列，请验证这些存储阵列是否已正确连接到您的网络，以及其分配的地址是否在范围内。单击 \* 新发现参数 \* 以返回到 " 添加 / 发现 " 页面。

4. 选中要添加到管理域的任何存储阵列旁边的复选框。

系统会对要添加到管理域的每个阵列执行凭据检查。在继续操作之前，您可能需要解决不可信证书的任何问题。

5. 单击 \* 下一步 \* 继续执行向导中的下一步。

6. 如果存储阵列具有有效证书，请转至 [第 3 步：提供密码](#)。如果任何存储阵列没有有效证书、则会显示解析自签名证书对话框；请转到 [第 2 步：在发现期间解析不可信的证书](#)。如果要导入CA签名的证书、请取消发现对话框并转到 "[导入阵列的证书](#)"。

## 第 2 步：在发现期间解析不可信的证书

如有必要、您必须先解决任何证书问题、然后再继续执行发现过程。

在发现期间、如果任何存储阵列显示"不可信证书"状态、则会显示"解析自签名证书"对话框。您可以在此对话框中解析不可信的证书、也可以导入CA证书(请参见 ["导入阵列的证书"](#))。

### 步骤

1. 如果 " 解析自签名证书 " 对话框打开，请查看为不可信证书显示的信息。有关详细信息，您还可以单击表末尾的省略号，然后从弹出菜单中选择 \* 查看 \*。
2. 执行以下操作之一：
  - 如果您信任与发现的存储阵列的连接、请单击\*下一步\*、然后单击\*是\*确认并继续访问向导中的下一张卡。自签名证书将标记为可信证书、存储阵列将添加到插件中。
  - 如果您不相信与存储阵列的连接、请选择\*取消\*并验证每个存储阵列的安全证书策略、然后再将其中任何一个添加到插件。

## 第 3 步：提供密码

作为发现的最后一步，您必须输入要添加到管理域的存储阵列的密码。

### 步骤

1. 或者、如果您之前已为阵列配置了组、则可以使用下拉列表为已发现的阵列选择一个组。
2. 对于每个已发现的阵列，请在字段中输入其管理员密码。
3. 单击 \* 完成 \*。



系统可能需要几分钟才能连接到指定的存储阵列。

### 结果

存储阵列将添加到管理域中并与选定组(如果指定)关联。



如果要执行管理操作、您可以使用Launch选项为一个或多个存储阵列打开基于浏览器的System Manager。

## 在适用于vCenter的SANtricity存储插件中重命名存储阵列

您可以更改vCenter存储插件的管理页面上显示的存储阵列名称。

### 步骤

1. 在\*管理\*页面中、选中存储阵列名称左侧的复选框。
2. 选择行最右侧的省略号、然后从弹出菜单中选择\*重命名存储阵列\*。
3. 输入新名称并单击\*保存\*。

## 在适用于vCenter的SANtricity存储插件中更改存储阵列密码

您可以在适用于vCenter的存储插件中更新用于查看和访问存储阵列的密码。

## 开始之前

您必须知道在System Manager中设置的存储阵列的当前密码。

## 关于此任务

在此任务中、您可以输入存储阵列的当前密码、以便在插件中访问该密码。如果在System Manager中更改了阵列密码、则可能需要执行此操作。

## 步骤

1. 从\*管理\*页面中、选择一个或多个存储阵列。
2. 选择菜单：不常见任务(提供存储阵列密码)。
3. 输入每个存储阵列的密码、然后单击\*保存\*。

## 在适用于vCenter的SANtricity存储插件中删除存储阵列

如果您不想再从适用于vCenter的存储插件管理一个或多个存储阵列、可以将其删除。

## 关于此任务

您无法访问所删除的任何存储阵列。但是、您可以通过将浏览器直接指向已删除的任何存储阵列的IP地址或主机名来建立与此阵列的连接。

删除存储阵列不会以任何方式影响存储阵列或其数据。如果意外删除了存储阵列、则可以重新添加该存储阵列。

## 步骤

1. 从\*管理\*页面中、选择要删除的一个或多个存储阵列。
2. 选择菜单：不常见任务[删除存储阵列]。

存储阵列将从插件界面的所有视图中删除。

## 从适用于vCenter的SANtricity存储插件启动System Manager

要管理单个阵列、请使用启动选项在新浏览器窗口中打开SANtricity 系统管理器。

System Manager是存储阵列控制器上的嵌入式应用程序、它通过以太网管理端口连接到网络。System Manager包括所有基于阵列的功能。要访问System Manager、您必须使用Web浏览器与网络管理客户端建立带外连接。

## 步骤

1. 从\*管理\*页面中、选择要管理的一个或多个存储阵列。
2. 单击 \* 启动 \*。

系统将在浏览器中打开一个新选项卡、然后显示System Manager登录页面。

3. 输入用户名和密码、然后单击\*登录\*。

## 导入设置

了解适用于vCenter的SANtricity存储插件中的导入设置功能

导入设置功能是一个批处理操作、可用于将单个存储阵列(源)中的设置复制到适用于vCenter的存储插件中的多个阵列(目标)。

可用于导入的设置

可以将以下配置从一个阵列导入到另一个阵列：

- 警报-使用电子邮件、系统日志服务器或SNMP服务器向管理员发送重要事件的警报方法。
- \* AutoSupport \*—一种用于监控存储阵列运行状况并向技术支持发送自动派单的功能。
- 目录服务—一种通过LDAP (轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)管理的用户身份验证方法。
- 系统设置-与以下内容相关的配置：
  - 卷的介质扫描设置
  - SSD设置
  - 自动负载平衡(不包括主机连接报告)
- 存储配置—与以下内容相关的配置：
  - 卷(仅限厚存储库卷和非存储库卷)
  - 卷组和池
  - 热备用驱动器分配

配置 workflow

要导入设置、请按照以下 workflow 进行操作：

1. 在要用作源的存储阵列上、使用System Manager配置设置。
2. 在要用作目标的存储阵列上、使用System Manager备份其配置。
3. 在插件界面中、转到\*管理\*页面并导入设置。
4. 在操作页面中、查看导入设置操作的结果。

复制存储配置的要求

在将存储配置从一个存储阵列导入到另一个存储阵列之前、请查看相关要求和准则。

磁盘架

- 源阵列和目标阵列上控制器所在的磁盘架必须相同。
- 源阵列和目标阵列上的磁盘架ID必须相同。
- 扩展架必须使用相同驱动器类型填充到相同插槽中(如果在配置中使用驱动器、则未使用驱动器的位置无关紧要)。

## 控制器

- 源阵列和目标阵列的控制器类型可以不同、但RVOD机箱类型必须相同。
- 源阵列和目标阵列之间的HIC (包括主机的DA功能)必须相同。
- 不支持从双工导入到单工配置；但是、允许从单工导入到双工。
- FDE设置不包括在导入过程中。

## Status

- 目标阵列必须处于最佳状态。
- 源阵列无需处于最佳状态。

## 存储

- 只要目标阵列上的卷容量大于源阵列、驱动器容量可能会因源阵列和目标阵列而异。(目标阵列可能具有容量更大的较新驱动器、这些驱动器无法通过复制操作完全配置到卷中。)
- 源阵列上64 TB或更大的磁盘池卷将阻止目标上的导入过程。

## 在适用于vCenter的SANtricity存储插件中导入警报设置

您可以将警报配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

### 开始之前

请确保：

- 系统会在System Manager (菜单：设置[警报])中为要用作源的存储阵列配置警报。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。
- 您已在中查看了复制存储配置的要求 "[导入设置概述](#)"。

### 关于此任务

您可以为导入操作选择电子邮件、SNMP或系统日志警报：

- 电子邮件警报-邮件服务器地址和警报收件人的电子邮件地址。
- 系统日志警报—系统日志服务器地址和UDP端口。
- \* SNMP警报\*- SNMP服务器的社区名称和IP地址。

### 步骤

1. 在管理页面中、单击菜单：操作[导入设置]。

此时将打开导入设置向导。

2. 在选择设置对话框中、选择\*电子邮件警报\*、\* SNMP警报\*或\*系统日志警报\*、然后单击\*下一步\*。

此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击\*下一步\*。

4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。



固件低于8.50的存储阵列不可供选择。此外、如果插件无法与该阵列进行通信(例如、阵列脱机或存在证书、密码或网络问题)、则阵列不会显示在此对话框中。

5. 单击 \* 完成 \*。

操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

## 结果

现在、目标存储阵列已配置为通过电子邮件、SNMP或系统日志向管理员发送警报。

## 在适用于vCenter的SANtricity存储插件中导入AutoSupport设置

您可以将AutoSupport 配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

## 开始之前

请确保：

- 已在System Manager (菜单：Support[支持中心])中为要用作源的存储阵列配置AutoSupport。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。
- 您已在其中查看了复制存储配置的要求 "[导入设置概述](#)"。

## 关于此任务

导入的设置包括不同的功能(基本AutoSupport、AutoSupport OnDemand和远程诊断)、维护窗口、交付方法、和派单计划。

## 步骤

1. 在管理页面中、单击菜单：操作[导入设置]。

此时将打开导入设置向导。

2. 在选择设置对话框中、选择\* AutoSupport 、然后单击\*下一步\*。

此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击\*下一步\*。

4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。



固件低于8.50的存储阵列不可供选择。此外、如果插件无法与该阵列进行通信(例如、阵列脱机或存在证书、密码或网络问题)、则阵列不会显示在此对话框中。

5. 单击 \* 完成 \*。

操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

## 结果

现在、目标存储阵列配置了与源阵列相同的AutoSupport 设置。

### 在适用于vCenter的SANtricity存储插件中导入目录服务设置

您可以将目录服务配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

#### 开始之前

请确保：

- 目录服务在System Manager (菜单：设置[访问管理])中为要用作源的存储阵列配置。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。
- 您已在中查看了复制存储配置的要求 "[导入设置概述](#)"。

#### 关于此任务

导入的设置包括LDAP (轻型目录访问协议)服务器的域名和URL、以及LDAP服务器用户组与存储阵列预定义角色的映射。

#### 步骤

1. 在管理页面中、单击菜单：操作[导入设置]。

此时将打开导入设置向导。

2. 在选择设置对话框中、选择\*目录服务\*、然后单击\*下一步\*。

此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击\*下一步\*。

4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。



固件低于8.50的存储阵列不可供选择。此外、如果插件无法与该阵列进行通信(例如、阵列脱机或存在证书、密码或网络问题)、则阵列不会显示在此对话框中。

5. 单击 \* 完成 \* 。

操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

## 结果

现在、目标存储阵列配置了与源阵列相同的目录服务。

### 在适用于vCenter的SANtricity存储插件中导入系统设置

您可以将系统设置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

#### 开始之前

请确保：

- 系统设置在System Manager中为要用作源的存储阵列配置。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。
- 您已在中查看了复制存储配置的要求 "[导入设置概述](#)"。

关于此任务

导入的设置包括卷的介质扫描设置、控制器的SSD设置和自动负载平衡(不包括主机连接报告)。

步骤

1. 在管理页面中、单击菜单：操作[导入设置]。

此时将打开导入设置向导。

2. 在选择设置对话框中、选择\*系统\*、然后单击\*下一步\*。

此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击\*下一步\*。

4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。



固件低于8.50的存储阵列不可供选择。此外、如果插件无法与该阵列进行通信(例如、阵列脱机或存在证书、密码或网络问题)、则阵列不会显示在此对话框中。

5. 单击 \* 完成 \*。

操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

结果

现在、目标存储阵列配置了与源阵列相同的系统设置。

在适用于vCenter的SANtricity存储插件中导入存储配置设置

您可以将存储配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

开始之前

请确保：

- 已在System Manager中为要用作源的存储阵列配置存储。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。
- 您已在中查看了复制存储配置的要求 "[导入设置概述](#)"。
- 源阵列和目标阵列必须满足以下要求：
  - 控制器所在的磁盘架必须相同。
  - 磁盘架ID必须相同。

- 扩展架必须使用相同类型的驱动器填充到相同的插槽中。
  - RVOD机箱类型必须相同。
  - HIC (包括主机的数据保证功能)必须相同。
  - 目标阵列必须处于最佳状态。
  - 目标阵列上的卷容量大于源阵列的容量。
- 您了解以下限制：
    - 不支持从双工导入到单工配置；但是、允许从单工导入到双工。
    - 源阵列上64 TB或更大的磁盘池卷将阻止目标上的导入过程。

#### 关于此任务

导入的设置包括已配置的卷(仅限厚存储库卷和非存储库卷)、卷组、池和热备用驱动器分配。

#### 步骤

1. 在管理页面中、单击菜单：操作[导入设置]。

此时将打开导入设置向导。

2. 在选择设置对话框中、选择\*存储配置\*、然后单击\*下一步\*。

此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击\*下一步\*。

4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。



固件低于8.50的存储阵列不可供选择。此外、如果插件无法与该阵列进行通信(例如、阵列脱机或存在证书、密码或网络问题)、则阵列不会显示在此对话框中。

5. 单击 \* 完成 \*。

操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

#### 结果

现在、目标存储阵列配置了与源阵列相同的存储配置。

## 管理阵列组

了解如何在适用于vCenter的SANtricity存储插件中管理阵列组

您可以通过对一组存储阵列进行分组来在适用于vCenter的存储插件中管理物理和虚拟化基础架构。您可能希望对存储阵列进行分组、以便更轻松地运行监控或报告作业。

存储阵列组的类型：

- 所有组-所有组是默认组、其中包括在您的组织中发现的所有存储阵列。可以从主视图访问所有组。
- 用户创建的组-用户创建的组包含您手动选择添加到该组的存储阵列。可以从主视图访问用户创建的组。

## 在适用于vCenter的SANtricity存储插件中创建存储阵列组

您可以创建存储组、然后将存储阵列添加到这些组中。存储组定义了哪些驱动器提供构成卷的存储。

- 步骤 \*
- 1. 从管理页面中、选择菜单：管理组[创建存储阵列组]。
- 2. 在\*名称\*字段中、键入新组的名称。
- 3. 选择要添加到新组的存储阵列。
- 4. 单击 \* 创建 \*。

## 在适用于vCenter的SANtricity存储插件中将存储阵列添加到组

您可以将一个或多个存储阵列添加到用户创建的组中。

- 步骤 \*
- 1. 在主视图中、选择\*管理\*、然后选择要将存储阵列添加到的组。
- 2. 选择菜单：管理组[将存储阵列添加到组]。
- 3. 选择要添加到组中的存储阵列。
- 4. 单击 \* 添加 \*。

## 在适用于vCenter的SANtricity存储插件中重命名存储阵列组

如果当前名称不再有意义或适用、您可以更改存储阵列组的名称。

关于此任务

请牢记这些准则。

- 名称可以由字母、数字和特殊字符下划线(\_)、连字符(-)和井号(#)组成。如果选择任何其他字符、则会显示一条错误消息。系统将提示您选择其他名称。
- 名称限制为30个字符。名称中的任何前导空格和尾随空格将被删除。
- 请使用一个易于理解和记住的唯一有意义的名称。
- 避免将来会很快失去意义的任意名称或名称。

步骤

1. 在主视图中、选择\*管理\*、然后选择要重命名的存储阵列组。
2. 选择菜单：Manage Groups[重命名存储阵列组]。
3. 在\*组名称\*字段中、键入组的新名称。
4. 单击 \* 重命名 \*。

## 从适用于vCenter的SANtricity存储插件的组中删除存储阵列

如果不再需要从特定存储组管理一个或多个受管存储阵列、则可以从组中删除该存储阵

列。

关于此任务

从组中删除存储阵列不会以任何方式影响存储阵列或其数据。如果您的存储阵列由System Manager管理、则仍可使用浏览器对其进行管理。如果意外从组中删除了存储阵列、则可以重新添加该存储阵列。

步骤

1. 从管理页面中、选择菜单：管理组[从组中删除存储阵列]。
2. 从下拉列表中、选择包含要删除的存储阵列的组、然后单击要从组中删除的每个存储阵列旁边的复选框。
3. 单击 \* 删除 \*。

在适用于vCenter的SANtricity存储插件中删除存储阵列组

您可以删除不再需要的一个或多个存储阵列组。

关于此任务

此操作仅删除存储阵列组。与已删除组关联的存储阵列仍可通过全部管理视图或与其关联的任何其他组进行访问。

步骤

1. 从管理页面中、选择菜单：管理组[删除存储阵列组]。
2. 选择要删除的一个或多个存储阵列组。
3. 单击 \* 删除 \*。

## 升级操作系统软件

了解如何使用适用于vCenter的存储插件管理SANtricity软件升级

在适用于vCenter的存储插件中、您可以为多个相同类型的存储阵列管理SANtricity 软件和NVSRAM升级。

升级工作流

以下步骤提供了执行软件升级的高级工作流：

1. 您可以从支持站点下载最新的SANtricity OS文件(可从支持页面访问链接)。将此文件保存在管理主机系统(在浏览器中访问此插件的主机)上、然后解压缩此文件。
2. 在插件中、您可以将SANtricity OS软件文件和NVSRAM文件加载到存储库(存储文件的服务器区域)。
3. 将文件加载到存储库中后、您可以选择要在升级中使用的文件。从升级SANtricity OS软件页面中、选择操作系统软件文件和NVSRAM文件。选择软件文件后、此页面上将显示兼容存储阵列列表。然后、选择要使用新软件升级的存储阵列。(不能选择不兼容的阵列。)
4. 然后、您可以立即开始软件传输和激活、也可以选择稍后暂存文件以进行激活。在升级过程中、插件将执行以下任务：
  - 对存储阵列执行运行状况检查、以确定是否存在任何可能阻止升级完成的条件。如果任何阵列未通过运行状况检查、您可以跳过该特定阵列并继续对其他阵列进行升级，也可以停止整个过程并对未通过的阵列进行故障排除。

- 将升级文件传输到每个控制器。
- 重新启动控制器并激活新的操作系统软件、一次一个控制器。激活期间、现有操作系统文件将替换为新文件。



您还可以指定稍后激活此软件。

#### 升级注意事项

在升级多个存储阵列之前、请在规划过程中查看主要注意事项。

#### 当前版本

您可以从适用于vCenter的存储插件的"管理"页面查看每个已发现存储阵列的当前SANtricity OS软件版本。此版本显示在SANtricity OS软件列中。单击每行中的操作系统版本时、会在弹出对话框中显示控制器固件和NVSRAM信息。

#### 其他需要升级的组件

在升级过程中、您可能还需要升级主机的多路径/故障转移驱动程序或HBA驱动程序、以便主机可以正确地与控制器进行交互。有关兼容性信息，请参见 ["互操作性表工具"](#)。

#### 双控制器

如果存储阵列包含两个控制器，并且您安装了多路径驱动程序，则在升级期间，存储阵列可以继续处理 I/O。在升级期间，将执行以下过程：

1. 控制器 A 将其所有 LUN 故障转移到控制器 B
2. 升级在控制器 A 上进行
3. 控制器 A 将收回其 LUN 以及控制器 B 的所有 LUN。
4. 升级在控制器 B 上进行

升级完成后，您可能需要在控制器之间手动重新分布卷，以确保卷返回到正确的所属控制器。

#### 在适用于vCenter的SANtricity存储插件中执行升级前运行状况检查

运行状况检查会在升级过程中运行，但您也可以在开始之前单独运行运行运行运行状况检查。运行状况检查会评估存储阵列的组件，以确保升级可以继续。

##### • 步骤 \*

1. 在主视图中，选择 \* 管理 \*，然后选择菜单：升级中心 [ 升级前运行状况检查 ]。

此时将打开升级前运行状况检查对话框，其中列出了所有已发现的存储系统。

2. 如果需要，可对列表中的存储系统进行筛选或排序，以便您可以查看当前未处于最佳状态的所有系统。
3. 选中要通过运行状况检查运行的存储系统对应的复选框。
4. 单击 \* 开始 \*。

执行运行状况检查时，此进度将显示在对话框中。

5. 运行状况检查完成后，您可以单击每行右侧的省略号（...）以查看更多信息并执行其他任务。



如果任何阵列未通过运行状况检查，您可以跳过该特定阵列并继续对其他阵列进行升级，也可以停止整个过程并对未通过的阵列进行故障排除。

## 使用适用于vCenter的存储插件升级SANtricity软件和NVsan

使用最新软件和NVSRAM升级一个或多个存储阵列、以确保您拥有所有最新功能和错误修复。控制器NVSRAM是一个控制器文件、用于指定控制器的默认设置。

开始之前

请确保：

- 运行此插件的主机系统上提供了最新的SANtricity OS文件。
- 您知道是要立即激活软件升级还是稍后激活。您可以选择稍后激活，原因如下：
  - \* 当前时间 \* —激活软件可能需要很长时间，因此您可能需要等待 I/O 负载变轻。控制器会在激活期间进行故障转移，因此，在升级完成之前，性能可能会比平常低。
  - \* 软件包类型 \* —您可能需要先在一个存储阵列上测试新的操作系统软件，然后再升级其他存储阵列上的文件。



\* 数据丢失或存储阵列损坏的风险 \* —升级期间请勿更改存储阵列。为存储阵列供电。

步骤

1. 如果存储阵列仅包含一个控制器或未使用多路径驱动程序，请停止存储阵列的 I/O 活动，以防止出现应用程序错误。如果存储阵列有两个控制器，并且您安装了多路径驱动程序，则无需停止 I/O 活动。
2. 在主视图中、选择\*管理\*、然后选择要升级的一个或多个存储阵列。
3. 选择菜单：Upgrade Center[升级> SANtricity OS >软件]。

此时将显示升级 SANtricity OS 软件页面。

4. 从支持站点将最新的SANtricity OS软件包下载到本地计算机。
  - a. 单击向软件存储库添加新文件
  - b. 单击此链接可查找最新的SANtricity OS下载内容。
  - c. 单击 \* 下载最新版本 \* 链接。
  - d. 按照其余说明将操作系统文件和NVSRAM文件下载到本地计算机。



8.42 及更高版本需要使用数字签名固件。如果您尝试下载未签名的固件，则会显示一个错误，并中止下载。

5. 选择要用于升级控制器的操作系统软件文件和 NVSRAM 文件：
  - a. 从下拉列表中、选择下载到本地计算机的操作系统文件。

如果有多个可用文件，则这些文件将从最新日期到最旧日期进行排序。



此软件存储库将列出与此插件关联的所有软件文件。如果未看到要使用的文件，可以单击链接 \* 将新文件添加到软件存储库 \*，以浏览到要添加的操作系统文件所在的位置。

- a. 从 \* 选择 NVSRAM 文件 \* 下拉列表中，选择要使用的控制器文件。

如果有多个文件，则这些文件将从最新日期到最旧日期进行排序。

6. 在兼容存储阵列表中，查看与选定操作系统软件文件兼容的存储阵列，然后选择要升级的阵列。
  - 默认情况下，您在 " 管理 " 视图中选择的存储阵列以及与选定固件文件兼容的存储阵列将在 " 兼容存储阵列 " 表中选择。
  - 无法使用选定固件文件更新的存储阵列在兼容存储阵列表中不可选择，如状态 \* 不兼容 \* 所示。
7. (可选) 要在不激活软件文件的情况下将其传输到存储阵列，请选中 \* 将操作系统软件传输到存储阵列，将其标记为暂存并稍后激活 \* 复选框。
8. 单击 \* 开始 \*。
9. 根据您选择现在激活还是稍后激活，执行以下操作之一：
  - 键入 `transfer` 确认要在选定升级的阵列上传输建议的操作系统软件版本、然后单击 \* 传输 \*。要激活已传输的软件、请选择菜单：升级中心[激活暂存SANtricity 操作系统软件]。
  - 键入 `upgrade` 确认要在选定升级的阵列上传输和激活建议的操作系统软件版本、然后单击 \* 升级 \*。

系统会将软件文件传输到您选择升级的每个存储阵列，然后通过启动重新启动来激活该文件。

升级操作期间会执行以下操作：

- 升级前运行状况检查会在升级过程中运行。升级前运行状况检查会评估所有存储阵列组件，以确保升级可以继续。
  - 如果存储阵列的任何运行状况检查失败，升级将停止。您可以单击省略号(...) 并选择 \* 保存日志 \* 以查看错误。您还可以选择覆盖运行状况检查错误，然后单击 \* 继续 \* 继续升级。
  - 您可以在升级前运行状况检查后取消升级操作。
10. (可选) 升级完成后、您可以单击省略号(...) 来查看为特定存储阵列升级的内容列表。然后选择 \* 保存日志 \*。

此文件将保存在浏览器的 "Downloads" 文件夹中、名为 `upgrade\_log-`<date>`。JSON`。

在适用于 vCenter 的 SANtricity 存储插件中激活暂存操作系统软件

您可以选择立即激活软件文件，也可以等到更方便的时间再激活。此操作步骤假定您稍后选择激活此软件文件。

关于此任务

您可以传输固件文件、而无需激活这些文件。您可以选择稍后激活，原因如下：

- \* 当前时间 \* —激活软件可能需要很长时间，因此您可能需要等待 I/O 负载变轻。控制器会在激活期间重新启动并进行故障转移，因此在升级完成之前性能可能会比平常低。
- \* 软件包类型 \* —您可能需要先在一個存储阵列上测试新软件和固件，然后再升级其他存储阵列上的文件。



激活过程启动后，您无法停止它。

#### 步骤

1. 在主视图中、选择\*管理\*。如有必要、请单击页面顶部的\*状态\*列对状态为"OS Upgrade (waiting activation)"的所有存储阵列进行排序。
2. 选择要为其激活软件的一个或多个存储阵列、然后选择菜单：升级中心[激活暂存SANtricity 软件]。

升级操作期间会执行以下操作：

- 在激活过程中会运行升级前运行状况检查。升级前运行状况检查会评估所有存储阵列组件，以确保激活可以继续。
- 如果存储阵列的任何运行状况检查失败，则激活将停止。您可以单击省略号(...) 并选择\*保存日志\*以查看错误。您也可以选择覆盖运行状况检查错误，然后单击 \* 继续 \* 继续进行激活。
- 您可以在升级前运行状况检查后取消激活操作。

成功完成升级前运行状况检查后，将激活。激活所需的时间取决于您的存储阵列配置以及要激活的组件。

3. (可选)激活完成后、单击省略号(...)可查看为特定存储阵列激活的内容列表。然后选择\*保存日志\*。

此文件将保存在浏览器的"Downloads"文件夹中、名称为`active\_log-<date>。JSON`。

#### 清除适用于vCenter的SANtricity存储插件中的暂存操作系统软件

您可以删除暂存操作系统软件、以确保稍后不会无意中激活待定版本。删除暂存操作系统软件不会影响存储阵列上运行的当前版本。

#### 步骤

1. 在主视图中、选择\*管理\*、然后选择菜单：升级中心[清除暂存SANtricity 软件]。

此时将打开清除暂存SANtricity 软件对话框、并列出了所有已发现的具有待定软件或NVSRAM的存储系统。

2. 如果需要、可对列表中的存储系统进行筛选或排序、以便您可以查看具有暂存软件的所有系统。
3. 选中要清除的待定软件存储系统对应的复选框。
4. 单击\*清除\*。

此操作的状态将显示在对话框中。

#### 在适用于vCenter的SANtricity存储插件中管理软件存储库

您可以查看和管理软件存储库、其中列出了与适用于vCenter的存储插件关联的所有软件文件。

#### 开始之前

如果使用存储库添加SANtricity OS文件、请确保操作系统文件在本地系统上可用。

#### 关于此任务

您可以使用管理SANtricity 操作系统软件存储库选项将一个或多个操作系统文件导入到运行此插件的主机系统中。您还可以选择删除软件存储库中的一个或多个可用操作系统文件。

## 步骤

1. 在主视图中、选择\*管理\*、然后选择菜单：升级中心[管理SANtricity 软件存储库]。

此时将显示管理SANtricity 操作系统软件存储库对话框。

2. 执行以下操作之一：

- 导入：

- i. 单击 \* 导入 \* 。
- ii. 单击\*浏览\*、然后导航到要添加的操作系统文件所在的位置。操作系统文件的文件名类似于`N2800-830000-000.DLP`。
- iii. 选择要添加的一个或多个操作系统文件、然后单击\*导入\*。

- 删除：

- i. 选择要从软件存储库中删除的一个或多个操作系统文件。
- ii. 单击 \* 删除 \* 。

## 结果

如果选择导入、则会上传并验证文件。如果选择了delete、则这些文件将从软件存储库中删除。

## 配置存储

了解如何在适用于vCenter的SANtricity存储插件中配置存储

在适用于vCenter的存储插件中、您可以创建称为卷的数据容器、以便主机可以访问阵列上的存储。

### 卷类型和特征

卷是一种数据容器，用于管理和组织存储阵列上的存储空间。

您可以使用存储阵列上的可用存储容量创建卷，这有助于组织系统的资源。"卷"的概念类似于在计算机上使用文件夹 / 目录来组织文件以实现快速访问。

卷是主机唯一可见的数据层。在 SAN 环境中，卷会映射到逻辑单元号（LUN）。这些LUN可保存可使用存储阵列支持的一个或多个主机访问协议(包括FC、iSCSI和SAS)访问的用户数据。

池或卷组中的每个卷都可以根据要存储的数据类型具有自己的特征。其中一些特征包括：

- 区块大小—区块是指存储阵列移至条带中下一个驱动器(RAID组)之前存储在驱动器上的数据量(以千字节(KiB)为单位)。区块大小等于或小于卷组的容量。区块大小是固定的、不能为池更改。
- 容量-使用池或卷组中的可用容量创建卷。在创建卷之前、池或卷组必须已存在、并且必须具有足够的可用容量来创建卷。
- 控制器所有权-所有存储阵列均可具有一个或两个控制器。在单控制器阵列上、卷的工作负载由单个控制器管理。在双控制器阵列上、卷将具有一个首选控制器(A或B)、该控制器"拥有"该卷。在双控制器配置中、使用

自动负载平衡功能自动调整卷所有权、以便在工作负载在控制器之间移动时更正任何负载平衡问题。自动负载平衡可实现自动I/O工作负载平衡、并确保在两个控制器之间动态管理和平衡来自主机的传入I/O流量。

- 卷分配—您可以在创建卷时或稍后为主机授予对卷的访问权限。所有主机访问均通过逻辑单元号(LUN)进行管理。主机会检测分配给卷的LUN。如果要将卷分配给多个主机、请使用集群软件确保卷可供所有主机使用。

主机类型可以对主机可以访问的卷数进行特定限制。在创建卷供特定主机使用时、请记住此限制。

- 资源配置—对于EF600或EF300存储阵列、您可以指定在不执行后台初始化过程的情况下立即使用卷。资源配置卷是SSD卷组或池中的厚卷、在创建卷时会分配(分配给卷)驱动器容量、但会取消分配(取消映射)驱动器块。
- 描述性名称—您可以根据需要为卷命名任何名称、但我们建议将此名称设置为描述性名称。

在创建卷期间、系统会为每个卷分配容量、并为其分配名称、区块大小(仅限卷组)、控制器所有权以及卷到主机的分配。卷数据会根据需要在控制器之间自动进行负载平衡。

### 卷的容量

存储阵列中的驱动器可为数据提供物理存储容量。开始存储数据之前、必须先将分配的容量配置到称为池或卷组的逻辑组件中。您可以使用这些存储对象配置、存储、维护和保留存储阵列上的数据。

### 用于创建和扩展卷的容量

您可以从池或卷组中的未分配容量或可用容量创建卷。

- 使用未分配的容量创建卷时、您可以同时创建池或卷组和卷。
- 使用可用容量创建卷时、您正在现有池或卷组上创建一个额外的卷。扩展卷容量后、必须手动增加文件系统大小以匹配。如何执行此操作取决于所使用的文件系统。有关详细信息、请参见主机操作系统文档。



插件界面不提供创建精简卷的选项。

### 报告的卷容量

报告的卷容量等于分配的物理存储容量。必须存在全部物理存储容量。物理分配的空间等于向主机报告的空间。

通常、您会将卷的报告容量设置为您认为卷将增长到的最大容量。卷可为应用程序提供高且可预测的性能、这主要是因为所有用户容量都是在创建时预留和分配的。

### 容量限制

卷的最小容量为1 MiB、最大容量由池或卷组中驱动器的数量和容量决定。

增加卷的报告容量时、请记住以下准则：

- 您最多可以指定三个小数位(例如、55.375 GiB)。
- 容量必须小于(或等于)卷组中的最大可用容量。创建卷时、系统会为动态区块大小(DSS)迁移预先分配一些额外容量。DSS迁移是软件的一项功能、可用于更改卷的区块大小。
- 某些主机操作系统支持大于2 TiB的卷(报告的最大容量由主机操作系统决定)。事实上、某些主机操作系统最多支持128个TiB卷。有关更多详细信息、请参见主机操作系统文档。

## 应用程序特定的工作负载

创建卷时、您可以选择一个工作负载来为特定应用程序自定义存储阵列配置。

工作负载是指支持应用程序的存储对象。您可以为每个应用程序定义一个或多个工作负载或实例。对于某些应用程序、系统会将工作负载配置为包含具有类似底层卷特征的卷。这些卷特征会根据工作负载支持的应用程序类型进行优化。例如、如果您创建了一个支持Microsoft SQL Server应用程序的工作负载、然后为该工作负载创建了卷、则底层卷特征将进行优化以支持Microsoft SQL Server。

在创建卷期间、系统会提示您回答有关工作负载使用情况的问题解答问题。例如、如果要为Microsoft Exchange创建卷、系统会询问您需要多少邮箱、平均邮箱容量要求是多少以及所需数据库副本的数量。系统会使用此信息为您创建最佳卷配置、您可以根据需要对其进行编辑。或者、您也可以根据需要在卷创建序列中跳过此步骤。

## 工作负载类型

您可以创建两种类型的工作负载：特定于应用程序的工作负载和其他工作负载。

- 应用程序专用—当您使用应用程序专用工作负载创建卷时、系统可能会建议优化卷配置、以最大程度地减少应用程序工作负载I/O与应用程序实例中的其他流量之间的争用。对于为以下应用程序类型创建的工作负载、系统会自动建议并优化卷特征、例如I/O类型、区块大小、控制器所有权以及读写缓存。
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - 视频监控应用程序
  - VMware ESXi (适用于要与虚拟机文件系统结合使用的卷)

您可以使用添加/编辑卷对话框查看建议的卷配置以及编辑、添加或删除系统建议的卷和特征。

- 其他(或不支持特定卷创建的应用程序)- 其他工作负载使用的卷配置必须手动指定、以便在创建与特定应用程序无关的工作负载时、或者系统没有为要在存储阵列上使用的应用程序进行内置优化时。您必须使用添加/编辑卷对话框手动指定卷配置。

## 应用程序和工作负载视图

要查看应用程序和工作负载、请启动System Manager。在此界面中、您可以通过多种不同方式查看与应用程序特定工作负载关联的信息：

- 您可以选择卷图块中的应用程序和工作负载选项卡、以查看按工作负载分组的存储阵列卷以及与工作负载关联的应用程序类型。
- 您可以选择"性能"图块中的"应用程序和工作负载"选项卡、以查看逻辑对象的性能指标(延迟、IOPS和MBs)。对象按应用程序和关联工作负载分组。通过定期收集此性能数据、您可以建立基线测量并分析趋势、这有助于您调查与I/O性能相关的问题。

## 在适用于vCenter的SANtricity存储插件中创建存储

在适用于vCenter的存储插件中、您可以先为特定应用程序类型创建工作负载来创建存储。接下来、您可以通过创建具有类似底层卷特征的卷来为工作负载添加存储容量。

### 第1步：创建工作负载

工作负载是指支持应用程序的存储对象。您可以为每个应用程序定义一个或多个工作负载或实例。

## 关于此任务

对于某些应用程序、系统会将工作负载配置为包含具有类似底层卷特征的卷。这些卷特征会根据工作负载支持的应用程序类型进行优化。例如、如果您创建了一个支持Microsoft SQL Server应用程序的工作负载、然后为该工作负载创建了卷、则底层卷特征将进行优化以支持Microsoft SQL Server。

系统建议仅针对以下应用程序类型优化卷配置：

- Microsoft SQL Server
- Microsoft Exchange Server
- 视频监控
- VMware ESXi (适用于要与虚拟机文件系统结合使用的卷)

## 步骤

1. 从管理页面中，选择存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择菜单：创建[工作负载]。

此时将显示创建应用程序工作负载对话框。

4. 使用下拉列表选择要为其创建工作负载的应用程序类型、然后键入工作负载名称。
5. 单击 \* 创建 \*。

## 第2步：创建卷

您可以创建卷来为应用程序特定的工作负载添加存储容量、并使创建的卷对特定主机或主机集群可见。

## 关于此任务

大多数应用程序类型默认为用户定义的卷配置、而其他类型则在创建卷时应用智能配置。例如、如果要为Microsoft Exchange应用程序创建卷、系统会询问您需要多少邮箱、平均邮箱容量要求是多少以及所需数据库副本的数量。系统会使用此信息为您创建最佳卷配置、您可以根据需要对其进行编辑。

您可以从菜单：配置(Manage Volumes > 创建>卷)或菜单：配置(Configure Pools and Volume Groups > Create > Volumes)]创建卷。对于任一选择、操作步骤 都是相同的。

创建卷的过程分为多步操作步骤。

## 步骤2a：为卷选择主机

在第一步中、您可以为卷选择特定的主机或主机集群、也可以选择稍后分配主机。

## 开始之前

请确保：

- 已定义有效的主机或主机集群(转至菜单：配置(Configure Hosts])。
- 已为主机定义主机端口标识符。
- 如果您计划创建启用了DA的卷、则主机连接必须支持数据保证(Data Assurance、DA)。如果存储阵列控制器上的任何主机连接不支持 DA ，则关联的主机将无法访问已启用 DA 的卷上的数据。

## 关于此任务

分配卷时，请记住以下准则：

- 主机的操作系统可以对主机可以访问的卷数设置特定限制。在创建卷供特定主机使用时、请记住此限制。
- 您可以为存储阵列中的每个卷定义一个分配。
- 分配的卷在存储阵列中的控制器之间共享。
- 主机或主机集群不能使用同一逻辑单元号(LUN)两次来访问卷。您必须使用唯一的LUN。
- 如果要加快创建卷的过程、可以跳过主机分配步骤、使新创建的卷脱机初始化。



如果您尝试将卷分配给与主机集群中已建立的主机分配冲突的主机集群、则向主机分配卷将失败。

## 步骤

1. 从管理页面中，选择存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择菜单：创建 [ 卷 ]。

此时将显示选择主机对话框。

4. 从下拉列表中，选择要将卷分配到的特定主机或主机集群，或者选择稍后再分配主机或主机集群。
5. 要继续为选定主机或主机集群创建卷、请单击\*下一步。\*

此时将显示选择工作负载对话框。

## 第2b步：为卷选择工作负载

在第二步中、您可以选择一个工作负载、以便为VMware等特定应用程序自定义存储阵列配置。

## 关于此任务

此任务介绍如何为工作负载创建卷。通常、工作负载包含具有类似特征的卷、这些卷会根据工作负载支持的应用程序类型进行优化。您可以在此步骤中定义工作负载、也可以选择现有工作负载。

请牢记以下准则：

- 在使用特定于应用程序的工作负载时、系统建议使用经过优化的卷配置、以最大程度地减少应用程序工作负载I/O与应用程序实例中的其他流量之间的争用。您可以查看建议的卷配置、然后使用添加/编辑卷对话框(可在下一步中找到)编辑、添加或删除系统建议的卷和特征。
- 使用其他应用程序类型时、您可以使用添加/编辑卷对话框(可在下一步中使用)手动指定卷配置。

## 步骤

1. 执行以下操作之一：
  - 选择 \* 为现有工作负载创建卷 \* 选项，然后从下拉列表中选择工作负载。
  - 选择\*创建新工作负载\*选项为支持的应用程序或"其他"应用程序定义新工作负载、然后执行以下步骤：
    - 从下拉列表中，选择要为其创建新工作负载的应用程序的名称。如果未列出要在此存储阵列上使用的应用程序、请选择"其他"条目之一。

- 输入要创建的工作负载的名称。
2. 单击 \* 下一步 \*。
  3. 如果您的工作负载与支持的应用程序类型关联，请输入所请求的信息；否则，请转到下一步。

## 第2c步：添加或编辑卷

在第三步中、您可以定义卷配置。

### 开始之前

- 池或卷组必须具有足够的可用容量。
- 一个卷组中允许的最大卷数为256。
- 池中允许的最大卷数取决于存储系统型号：
  - 2、048个卷(EF600和E5700系列)
  - 1、024个卷(EF300)
  - 512个卷(E2800系列)
- 要创建启用了数据保证(Data Assurance、DA)的卷、您计划使用的主机连接必须支持DA。
  - 如果要创建启用了DA的卷、请选择一个支持DA的池或卷组(在Pool and volume group candidates表中的"DA"旁边查找\*是\*)。
  - DA 功能在池和卷组级别提供。DA 保护功能可检查并更正数据通过控制器向下传输到驱动器时可能发生的错误。为新卷选择支持 DA 的池或卷组可确保检测到并更正任何错误。
  - 如果存储阵列中控制器上的任何主机连接不支持 DA ，则关联的主机将无法访问已启用 DA 的卷上的数据。
- 要创建启用了安全保护的卷，必须为存储阵列创建安全密钥。
  - 如果要创建启用了安全的卷，请选择一个支持安全的池或卷组（在 Pool and volume group candidates 表中，查找 "Secure-capable" 旁边的是）。
  - 驱动器安全功能在池和卷组级别提供。支持安全的驱动器可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。启用了安全保护的驱动器会在写入期间对数据进行加密，并在读取期间使用唯一的加密密钥对数据进行解密。
  - 池或卷组可以同时包含支持安全和不支持安全的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。
- 要创建资源配置的卷，所有驱动器都必须是具有已取消分配或未写入逻辑块错误（DULBE"）选项的 NVMe 驱动器。

### 关于此任务

您可以从符合条件的池或卷组创建卷、这些池或卷组显示在添加/编辑卷对话框中。对于每个符合条件的池和卷组，将显示可用驱动器数和总可用容量。

对于某些特定于应用程序的工作负载，每个符合条件的池或卷组都会根据建议的卷配置显示建议的容量，并以 GiB 显示剩余可用容量。对于其他工作负载，在将卷添加到池或卷组并指定报告的容量时，将显示建议的容量。

### 步骤

1. 根据您在上一步中选择的是其他工作负载还是应用程序专用工作负载，选择以下操作之一：
  - 其他-单击要用于创建一个或多个卷的每个池或卷组中的\*添加新卷\*。

## 字段详细信息

字段	Description
卷名称	在卷创建序列期间，系统会为卷分配默认名称。您可以接受默认名称，也可以提供一个更具描述性的名称来指示卷中存储的数据类型。
已报告容量	定义新卷的容量以及要使用的容量单位（ MiB ， GiB 或 TiB ）。对于厚卷、最小容量为1 MiB、最大容量由池或卷组中驱动器的数量和容量决定。请注意、复制服务(Snapshot映像、Snapshot卷、卷副本和远程镜像)也需要存储容量；因此、请勿将所有容量分配给标准卷。池中的容量以4 GiB为增量进行分配。分配的容量不是4 GiB的倍数、但不可用。要确保整个容量可用、请以4 GiB为增量指定容量。如果存在不可用的容量，则要重新获得该容量，唯一的方法是增加卷的容量。
卷块大小(仅限EF300和EF600)	显示了可为卷创建的块大小： <ul style="list-style-type: none"> <li>• 512 – 512 字节</li> <li>• 4 k – 4 , 096 字节</li> </ul>
区块大小	显示了分段大小调整设置，此设置仅适用于卷组中的卷。您可以更改区块大小以优化性能。允许的区块大小转换-系统将确定允许的区块大小转换。与当前区块大小的过渡不适当的区块大小在下拉列表中不可用。允许的过渡通常是当前区块大小的两倍或一半。例如，如果当前卷分段大小为 32 KiB ，则允许使用新的卷分段大小 16 KiB 或 64 KiB 。已启用SSD缓存的卷*—您可以为已启用SSD缓存的卷指定4-KiB分段大小。确保仅为支持 SSD 缓存且处理小块 I/O 操作的卷（例如， 16 KiB I/O 块大小或更小）选择 4-KiB 区块大小。如果为处理大型块顺序操作且已启用 SSD 缓存的卷选择 4 KiB 作为分段大小，则性能可能会受到影响。更改区块大小所需的时间-更改卷区块大小所需的时间取决于以下变量： <ul style="list-style-type: none"> <li>• 主机的 I/O 负载</li> <li>• 卷的修改优先级</li> <li>• 卷组中的驱动器数量</li> <li>• 驱动器通道的数量</li> <li>• 存储阵列控制器的处理能力</li> </ul> <p>更改卷的区块大小时， I/O 性能会受到影响，但数据仍可用。</p>
支持安全保护	只有当池或卷组中的驱动器具有安全功能时、“安全功能”旁边才会显示*是*。驱动器安全性可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。只有在启用了驱动器安全功能且为存储阵列设置了安全密钥时，此选项才可用。池或卷组可以同时包含支持安全和不支持安全的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。

字段	Description
da.	只有当池或卷组中的驱动器支持数据保证(Data Assurance、DA)时、"DA"旁边才会显示*是*。DA 可提高整个存储系统的数据完整性。通过 DA ， 存储阵列可以检查在数据通过控制器向下传输到驱动器时可能发生的错误。对新卷使用 DA 可确保检测到任何错误。
已配置资源(仅限EF300和EF600)	只有当驱动器支持此选项时、"已配置资源"旁边才会显示*是*。资源配置是EF300和EF600存储阵列中提供的一项功能、可在不执行后台初始化过程的情况下立即使用卷。

- 应用程序专用工作负载—单击\*下一步\*接受系统为选定工作负载建议的卷和特征、或者单击\*编辑卷\*更改、添加或删除系统为选定工作负载建议的卷和特征。

字段详细信息

字段	Description
卷名称	在卷创建序列期间，系统会为卷分配默认名称。您可以接受默认名称，也可以提供一个更具描述性的名称来指示卷中存储的数据类型。
已报告容量	定义新卷的容量以及要使用的容量单位（ MiB ， GiB 或 TiB ）。对于厚卷、最小容量为1 MiB、最大容量由池或卷组中驱动器的数量和容量决定。请注意、复制服务(Snapshot映像、Snapshot卷、卷副本和远程镜像)也需要存储容量；因此、请勿将所有容量分配给标准卷。池中的容量以 4 GiB 为增量进行分配。分配的容量不是 4 GiB 的倍数，但不可用。要确保整个容量可用，请以 4 GiB 为增量指定容量。如果存在不可用的容量，则要重新获得该容量，唯一的方法是增加卷的容量。
卷类型	卷类型指示为特定于应用程序的工作负载创建的卷类型。
卷块大小(仅限EF300和EF600)	显示了可为卷创建的块大小： <ul style="list-style-type: none"> <li>• 512—512字节</li> <li>• 4 k—4、096字节</li> </ul>
区块大小	显示了分段大小调整设置，此设置仅适用于卷组中的卷。您可以更改区块大小以优化性能。允许的区块大小转换-系统将确定允许的区块大小转换。与当前区块大小的过渡不适当的区块大小在下拉列表中不可用。允许的过渡通常是当前区块大小的两倍或一半。例如，如果当前卷分段大小为 32 KiB ，则允许使用新的卷分段大小 16 KiB 或 64 KiB 。已启用SSD缓存的卷*—您可以为已启用SSD缓存的卷指定4-KiB分段大小。确保仅为支持 SSD 缓存且处理小块 I/O 操作的卷（例如， 16 KiB I/O 块大小或更小）选择 4-KiB 区块大小。如果为处理大型块顺序操作且已启用 SSD 缓存的卷选择 4 KiB 作为分段大小，则性能可能会受到影响。更改区块大小所需的时间-更改卷区块大小所需的时间取决于以下变量： <ul style="list-style-type: none"> <li>• 主机的 I/O 负载</li> <li>• 卷的修改优先级</li> <li>• 卷组中的驱动器数量</li> <li>• 驱动器通道的数量</li> <li>• 存储阵列控制器的处理能力</li> </ul> <p>更改卷的区块大小时， I/O 性能会受到影响，但数据仍可用。</p>
支持安全保护	只有当池或卷组中的驱动器具有安全功能时、“安全功能”旁边才会显示*是*。驱动器安全性可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。只有在已启用驱动器安全功能且为存储阵列设置了安全密钥时、此选项才可用。池或卷组可以同时包含支持安全和不支持安全的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。

字段	Description
da.	只有当池或卷组中的驱动器支持数据保证(Data Assurance、DA)时、"DA"旁边才会显示*是*。DA 可提高整个存储系统的数据完整性。通过 DA ， 存储阵列可以检查在数据通过控制器向下传输到驱动器时可能发生的错误。对新卷使用 DA 可确保检测到任何错误。
已配置资源(仅限EF300和EF600)	只有当驱动器支持此选项时、"已配置资源"旁边才会显示*是*。资源配置是EF300和EF600存储阵列中提供的一项功能、可在不执行后台初始化过程的情况下立即使用卷。

2. 要继续对选定应用程序执行卷创建序列，请单击 \* 下一步 \*。

## 第2D步：查看卷配置

在最后一步中、您将查看要创建的卷的摘要并进行任何必要的更改。

### 步骤

1. 查看要创建的卷。要进行更改，请单击 \* 返回 \*。
2. 对卷配置感到满意后，单击 \* 完成 \*。

### 完成后

- 在vSphere Client中、为卷创建数据存储库。
- 在应用程序主机上执行任何必要的操作系统修改、以便应用程序可以使用卷。
- 运行特定于操作系统的实用程序(可从第三方供应商处获得)、然后运行SMcli命令 `-identifyDevices` 将卷名称与主机存储阵列名称相关联。

SMcli,包括在SANtricity操作系统中,并可通过SANtricity系统管理器下载。有关如何通过SANtricity系统管理器下载SMcli的详细信息、请参阅 ["下载SANtricity系统管理器联机帮助下的命令行界面\(CLI\)主题"](#)。

在适用于vCenter的SANtricity存储插件中增加卷的容量

您可以调整卷大小以增加其报告的容量。

### 开始之前

请确保：

- 卷的关联池或卷组具有足够的可用容量。
- 卷处于最佳状态，不处于任何修改状态。
- 卷中未使用任何热备用驱动器。（仅适用于卷组中的卷。）

### 关于此任务

此任务介绍如何使用池或卷组中可用的容量来增加卷的报告容量(向主机报告的容量)。请务必考虑此池或卷组中的其他卷将来可能具有的任何容量要求。



只有某些操作系统才支持增加卷的容量。如果在不受支持的主机操作系统上增加卷容量、则扩展的容量将不可用、并且无法还原原始卷容量。

#### 步骤

1. 从\*管理\*页面中、选择包含要调整大小的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择要增加容量的卷，然后选择 \* 增加容量 \*。

此时将显示确认增加容量对话框。

4. 选择 \* 是 \* 继续。

此时将显示增加报告的容量对话框。此对话框显示卷当前报告的容量以及卷关联的池或卷组中可用的容量。

5. 使用 \* 通过添加增加报告容量 ... \* 框向当前可用报告容量添加容量。您可以将容量值更改为以兆字节（MiB），吉字节（GiB）或太字节（TiB）为单位显示。
6. 单击 \* 增加 \*。

根据您的选择增加卷的容量。请注意、此操作可能会很长、并且可能会影响系统性能。

#### 完成后

扩展卷容量后、必须手动增加文件系统大小以匹配。如何执行此操作取决于所使用的文件系统。有关详细信息、请参见主机操作系统文档。

#### 在适用于vCenter的SANtricity存储插件中更改卷的设置

您可以更改卷的设置、例如名称、主机分配、区块大小、修改优先级、缓存、等等。

#### 开始之前

确保要更改的卷处于最佳状态。

#### 步骤

1. 从管理页面中、选择包含要更改的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择要更改的卷、然后选择\*查看/编辑设置\*。

此时将显示卷设置对话框。选定卷的配置设置将显示在此对话框中。

4. 选择\*基本\*选项卡以更改卷的名称和主机分配。

## 字段详细信息

正在设置 ...	Description
Name	显示卷的名称。如果当前名称不再有意义或适用、请更改卷的名称。
容量	显示所选卷的已报告容量和已分配容量。
池/卷组	显示池或卷组的名称和RAID级别。指示池或卷组是否支持安全和启用安全。
主机	<p>显示卷分配。您可以将卷分配给主机或主机集群、以便可以对其进行访问以执行I/O操作。此分配授予主机或主机集群对特定卷或存储阵列中的多个卷的访问权限。</p> <ul style="list-style-type: none"> <li>• 已分配给-标识可访问选定卷的主机或主机集群。</li> <li>• * LUN *—逻辑单元号(LUN)是指分配给主机用于访问卷的地址空间的编号。卷以LUN的形式呈现给主机。每个主机都有自己的LUN地址空间。因此、不同的主机可以使用同一个LUN来访问不同的卷。</li> </ul> <p>对于NVMe接口、此列显示命名空间ID。命名空间是指为块访问而格式化的NVMe存储。它类似于SCSI中的逻辑单元、它与存储阵列中的卷相关。命名空间ID是NVMe控制器在命名空间中的唯一标识符、可设置为1到255之间的值。它类似于SCSI中的逻辑单元号(Logical Unit Number、LUN)。</p>
标识符	<p>显示选定卷的标识符。</p> <ul style="list-style-type: none"> <li>• 全球通用标识符(WWID)。卷的唯一十六进制标识符。</li> <li>• 扩展唯一标识符(Extended Unique Identifier、EUI)。卷的EUI-64标识符。</li> <li>• 子系统标识符(SSID)。卷的存储阵列子系统标识符。</li> </ul>

5. 选择\*高级\*选项卡可更改池或卷组中卷的其他配置设置。

正在设置 ...	Description
应用程序和工作负载信息	在创建卷期间、您可以创建应用程序专用的工作负载或其他工作负载。如果适用、将显示选定卷的工作负载名称、应用程序类型和卷类型。如果需要、您可以更改工作负载名称。
服务质量设置	永久禁用数据保证-只有在卷启用了数据保证(Data Assurance、DA)的情况下、才会显示此设置。DA可检查并更正在数据通过控制器向下传输到驱动器时可能发生的错误。使用此选项可在选定卷上永久禁用DA。禁用后、无法在此卷上重新启用DA。启用预读取冗余检查-只有当卷为厚卷时、才会显示此设置。预读取冗余检查可确定卷上的数据是否在执行读取时保持一致。如果控制器固件确定数据不一致、则启用了此功能的卷将返回读取错误。
控制器所有权	定义指定为卷的拥有或主控制器的控制器。控制器所有权非常重要、应仔细规划。对于总I/O、控制器应尽可能保持平衡。
分段规模估算	<p>显示了分段大小调整设置、此设置仅对卷组中的卷显示。您可以更改区块大小以优化性能。允许的区块大小转换-系统将确定允许的区块大小转换。与当前区块大小的过渡不适当的区块大小在下拉列表中不可用。允许的过渡通常是当前区块大小的两倍或一半。例如，如果当前卷分段大小为 32 KiB，则允许使用新的卷分段大小 16 KiB 或 64 KiB。已启用SSD缓存的卷*—您可以为已启用SSD缓存的卷指定4-KiB分段大小。确保仅为支持 SSD 缓存且处理小块 I/O 操作的卷（例如，16 KiB I/O 块大小或更小）选择 4-KiB 区块大小。如果为处理大型块顺序操作且已启用 SSD 缓存的卷选择 4 KiB 作为分段大小，则性能可能会受到影响。*更改区块大小所需的时间。*更改卷区块大小所需的时间取决于以下变量：</p> <ul style="list-style-type: none"> <li>• 主机的 I/O 负载</li> <li>• 卷的修改优先级</li> <li>• 卷组中的驱动器数量</li> <li>• 驱动器通道的数量</li> <li>• 存储阵列控制器的处理能力</li> </ul> <p>更改卷的区块大小时，I/O 性能会受到影响，但数据仍可用。</p>
修改优先级	显示了修改优先级的设置、此设置仅适用于卷组中的卷。修改优先级用于定义为卷修改操作分配的处理时间与系统性能相关。您可以提高卷修改优先级、但这可能会影响系统性能。移动滑块条以选择优先级。修改优先级速率—最低优先级速率有利于系统性能、但修改操作所需时间较长。最高优先级比率有利于修改操作、但系统性能可能会受到影响。
缓存	显示了缓存设置、您可以更改此设置以影响卷的整体I/O性能。

正在设置 ...	Description
SSD 缓存	(此功能在EF600或EF300存储系统上不可用。) 显示了SSD缓存设置、您可以在兼容卷上启用此设置以提高只读性能。如果卷共享相同的驱动器安全和数据保证功能、则这些卷是兼容的。SSD缓存功能使用一个或多个固态硬盘(SSD)来实施读取缓存。由于SSD的读取速度更快、因此应用程序性能得到了提高。由于读取缓存位于存储阵列中、因此使用该存储阵列的所有应用程序将共享缓存。只需选择要缓存的卷、即可自动动态缓存。

6. 单击 \* 保存 \*。

#### 结果

卷设置将根据您的选择进行更改。

在适用于vCenter的SANtricity存储插件中向工作负载添加卷

您可以将未分配的卷添加到现有工作负载或新工作负载。

#### 关于此任务

如果卷是使用命令行界面(CLI)创建的、或者已从其他存储阵列迁移(导入/导出)、则卷不会与工作负载关联。

#### 步骤

1. 从管理页面中、选择包含要添加的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择\*应用程序和工作负载\*选项卡。

此时将显示"Applications & Workloads View"。

4. 选择\*添加到工作负载\*。

此时将显示选择工作负载对话框。

5. 执行以下操作之一：
  - 将卷添加到现有工作负载-选择此选项可将卷添加到现有工作负载。使用下拉列表选择工作负载。此工作负载的关联应用程序类型将分配给您添加到此工作负载的卷。
  - 将卷添加到新工作负载-选择此选项可为应用程序类型定义新工作负载并将卷添加到新工作负载。
6. 选择\*下一步\*继续添加到工作负载序列。

此时将显示选择卷对话框。

7. 选择要添加到工作负载的卷。
8. 查看要添加到选定工作负载的卷。
9. 对工作负载配置感到满意后、单击\*完成\*。

在适用于vCenter的SANtricity存储插件中更改工作负载设置

您可以更改工作负载的名称并查看其关联的应用程序类型。

#### 步骤

1. 从管理页面中、选择包含要更改的工作负载的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择\*应用程序和工作负载\*选项卡。

此时将显示"Applications & Workloads View"。

4. 选择要更改的工作负载、然后选择\*查看/编辑设置\*。

此时将显示应用程序和工作负载设置对话框。

5. (可选)更改用户提供的工作负载名称。
6. 单击 \* 保存 \*。

在适用于vCenter的SANtricity存储插件中初始化卷

首次创建卷时、系统会自动对其进行初始化。但是、Recovery Guru可能会建议您手动初始化卷、以便从某些故障情况中恢复。

请仅在技术支持的指导下使用此选项。您可以选择一个或多个卷进行初始化。

#### 开始之前

- 所有I/O操作均已停止。
- 必须卸载要初始化的卷上的任何设备或文件系统。
- 卷处于最佳状态、并且卷上没有正在进行的修改操作。\*注意：\*操作启动后无法取消。将擦除所有卷数据。除非Recovery Guru建议您尝试执行此操作、否则请勿尝试执行此操作。开始此操作步骤 之前、请联系技术支持。

#### 关于此任务

初始化卷时、卷会保留其WWN、主机分配、已分配容量和预留容量设置。它还会保留相同的数据保证(Data Assurance、DA)设置和安全设置。

无法初始化以下类型的卷：

- 快照卷的基础卷
- 镜像关系中的主卷
- 镜像关系中的二级卷
- 卷副本中的源卷
- 卷副本中的目标卷
- 已在进行初始化的卷

此操作步骤 仅适用于从池或卷组创建的标准卷。

## 步骤

1. 从管理页面中、选择包含要初始化的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择任何卷、然后选择菜单：更多[初始化卷]。

此时将显示初始化卷对话框。存储阵列上的所有卷都会显示在此对话框中。

4. 选择要初始化的一个或多个卷、然后确认要执行此操作。

## 结果

系统将执行以下操作：

- 擦除已初始化的卷中的所有数据。
- 清除块索引、这样会将未写入的块读取为零填充(卷显示为完全空)。

此操作可能会很长，并且可能会影响系统性能。

## 在适用于vCenter的SANtricity存储插件中重新分布卷

重新分配卷以将卷移回其首选控制器所有者。通常、当主机和存储阵列之间的数据路径出现问题时、多路径驱动程序会从其首选控制器所有者移动卷。

## 开始之前

- 您要重新分布的卷未在使用中、或者会发生I/O错误。
- 如果使用要重新分配的卷、则会在所有主机上安装多路径驱动程序、否则会发生I/O错误。如果要重新分布主机上没有多路径驱动程序的卷、则在重新分布操作正在进行期间、必须停止卷的所有I/O活动、以防止出现应用程序错误。

## 关于此任务

大多数主机多路径驱动程序都会尝试通过指向其首选控制器所有者的路径访问每个卷。但是、如果此首选路径不可用、则主机上的多路径驱动程序将故障转移到备用路径。此故障转移可能会通过发生原因 将卷所有权更改为备用控制器。解决导致故障转移的情况后、某些主机可能会自动将卷所有权移回首选控制器所有者、但在某些情况下、您可能需要手动重新分配卷。

## 步骤

1. 从管理页面中、选择包含要重新分布的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择菜单：更多 [ 重新分配卷 ]。

此时将显示重新分配卷对话框。存储阵列上首选控制器所有者与其当前所有者不匹配的所有卷都会显示在此对话框中。

4. 选择要重新分布的一个或多个卷、然后确认要执行此操作。

## 结果

系统会将选定卷移至其首选控制器所有者、或者您可能会看到"重新分配不必要的卷"对话框。

在适用于vCenter的SANtricity存储插件中更改卷的控制器所有权

您可以更改卷的首选控制器所有权、以便通过新路径定向主机应用程序的I/O。

开始之前

如果不使用多路径驱动程序、则必须关闭当前正在使用此卷的任何主机应用程序。此操作可防止在I/O路径发生更改时出现应用程序错误。

关于此任务

您可以更改池或卷组中一个或多个卷的控制器所有权。

步骤

1. 从管理页面中、选择包含要更改其控制器所有权的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择任何卷、然后选择菜单：更多[更改所有权]。

此时将显示更改卷所有权对话框。存储阵列上的所有卷都会显示在此对话框中。

4. 使用\*首选所有者\*下拉列表更改要更改的每个卷的首选控制器、并确认要执行此操作。

结果

- 系统将更改卷的控制器所有权。现在、卷的I/O将通过此I/O路径定向。
- 在多路径驱动程序重新配置以识别新路径之前、卷可能不会使用新的I/O路径。

此操作通常需要不到五分钟的时间。

在适用于vCenter的SANtricity存储插件中更改卷的缓存设置

您可以更改读取缓存和写入缓存设置、以影响卷的整体I/O性能。

关于此任务

更改卷的缓存设置时、请记住以下准则：

- 打开更改缓存设置对话框后、您可能会看到选定缓存属性旁边显示的图标。此图标表示控制器已暂时暂停缓存操作。如果新电池正在充电、已删除控制器或控制器检测到缓存大小不匹配、则可能会发生此操作。清除此条件后、在对话框中选择的缓存属性将变为活动状态。如果选定缓存属性未处于活动状态、请联系技术支持。
- 您可以更改一个卷或一个存储阵列上多个卷的缓存设置。您可以同时更改所有卷的缓存设置。

步骤

1. 从管理页面中、选择包含要更改缓存设置的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择任何卷，然后选择菜单：更多（更改缓存设置）。

此时将显示更改缓存设置对话框。存储阵列上的所有卷都会显示在此对话框中。

4. 选择\*基本\*选项卡可更改读取缓存和写入缓存的设置。

## 字段详细信息

缓存设置	Description
读取缓存	读取缓存是一个缓冲区、用于存储已从驱动器读取的数据。用于读取操作的数据可能已位于上次操作的缓存中、因此无需访问驱动器。数据会一直保留在读取缓存中、直到被刷新为止。
写入缓存	写入缓存是一个缓冲区、用于存储尚未写入驱动器的主机中的数据。数据会一直保留在写入缓存中、直到写入驱动器为止。写入缓存可以提高I/O性能。对卷禁用写入缓存后、缓存会自动刷新。

5. 选择\*高级\*选项卡可更改厚卷的高级设置。高级缓存设置仅适用于厚卷。

## 字段详细信息

正在设置 ...	Description
动态读取缓存预取	动态缓存读取预取允许控制器在从驱动器向缓存读取数据块时将其他顺序数据块复制到缓存中。这种缓存增加了从缓存中填充未来数据请求的可能性。动态缓存读取预取对于使用顺序I/O的多媒体应用程序非常重要预提取到缓存中的数据速率和数据量会根据主机读取的速率和请求大小进行自调整。随机访问不会将发生原因数据预先提取到缓存中。禁用读取缓存时、此功能不适用。
无电池写入缓存	使用无电池写入缓存设置可以继续执行写入缓存、即使电池缺失、出现故障、已完全放电或未充满电也是如此。通常不建议选择不带电池的写入缓存、因为断电后数据可能会丢失。通常、在电池充电或更换故障电池之前、控制器会暂时关闭写入缓存。小心：可能会丢失数据-如果选择此选项并且没有通用电源进行保护、则可能会丢失数据。此外、如果您没有控制器电池、并且启用了无电池写入缓存选项、则可能会丢失数据。
使用镜像进行写入缓存	如果写入到一个控制器的缓存内存中的数据也写入到另一个控制器的缓存中、则会发生具有镜像功能的写入缓存。因此、如果一个控制器发生故障、另一个控制器可以完成所有未完成的写入操作。只有在启用了写入缓存且存在两个控制器的情况下、写入缓存镜像才可用。创建卷时的默认设置是使用镜像进行写入缓存。

6. 单击\*保存\*以更改缓存设置。

## 在适用于vCenter的SANtricity存储插件中更改卷的介质扫描设置

介质扫描是一种后台操作、可扫描卷中的所有数据和冗余信息。使用此选项可以为一个或多个卷启用或禁用介质扫描设置、或者更改扫描持续时间。

### 开始之前

了解以下内容：

- 介质扫描会根据要扫描的容量和扫描持续时间以恒定速率持续运行。后台扫描可能会被较高优先级的后台任务(例如重建)临时暂停、但会以相同的恒定速率恢复。
- 只有在为存储阵列和卷启用了介质扫描选项时、才会扫描此卷。如果还为该卷启用了冗余检查、则会检查该

卷中的冗余信息是否与数据一致、前提是该卷具有冗余。创建每个卷时、默认情况下会为其启用具有冗余检查的介质扫描。

- 如果在扫描期间遇到不可恢复的介质错误、则会使用冗余信息(如果有)修复数据。

例如、最佳RAID 5卷、最佳RAID 6卷或只有一个驱动器发生故障的RAID 6卷均提供冗余信息。如果无法使用冗余信息修复不可恢复的错误、则数据块将添加到不可读扇区日志中。可更正和不可更正的介质错误都会报告到事件日志中。

- 如果冗余检查发现数据与冗余信息不一致、则会向事件日志报告此信息。

#### 关于此任务

介质扫描可检测并修复应用程序不常读取的磁盘块上的介质错误。这样可以防止驱动器发生故障时数据丢失、因为故障驱动器的数据是使用卷组或池中其他驱动器的冗余信息和数据进行重建的。

您可以执行以下操作：

- 为整个存储阵列启用或禁用后台介质扫描
- 更改整个存储阵列的扫描持续时间
- 为一个或多个卷启用或禁用介质扫描
- 为一个或多个卷启用或禁用冗余检查

#### 步骤

1. 从管理页面中、选择包含要更改其介质扫描设置的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 选择任何卷、然后选择菜单：更多(更改介质扫描设置)。

此时将显示更改驱动器介质扫描设置对话框。存储阵列上的所有卷都会显示在此对话框中。

4. 要启用介质扫描、请选中\*在过程中扫描介质...\*复选框。禁用介质扫描复选框会暂停所有介质扫描设置。
5. 指定要运行介质扫描的天数。
6. 选中要对其执行介质扫描的每个卷对应的\*介质扫描\*复选框。系统会为您选择运行介质扫描的每个卷启用冗余检查选项。如果不想对个别卷执行冗余检查、请取消选中\*冗余检查\*复选框。
7. 单击 \* 保存 \*。

#### 结果

系统会根据您的选择对后台介质扫描应用更改。

在适用于vCenter的SANtricity存储插件中删除卷

您可以删除一个或多个卷以增加池或卷组的可用容量。

#### 开始之前

在计划删除的卷上、确保：

- 备份所有数据。
- 所有输入/输出(I/O)均已停止。

- 所有设备和文件系统均已卸载。

#### 关于此任务

通常、如果创建的卷的参数或容量不正确、或者不再满足存储配置需求、则可以删除这些卷。删除卷会增加池或卷组中的可用容量。



删除卷会导致这些卷上的所有数据丢失。

请注意、您\*无法\*删除具有以下条件之一的卷：

- 卷正在初始化。
- 卷正在重建。
- 此卷属于某个卷组、该卷组包含正在执行回写操作的驱动器。
- 卷正在进行修改操作、例如更改区块大小、除非卷现在处于故障状态。
- 卷持有任何类型的永久性预留。
- 此卷是复制卷中的源卷或目标卷、其状态为"Pending"、"In Progress"或"Failed"。



当卷超过给定大小(当前为128 TB)时、将在后台执行删除操作、释放的空间可能不会立即可用。

#### 步骤

1. 从\*管理\*页面中、选择包含要删除的卷的存储阵列。
2. 选择菜单：配置 [ 管理卷 ]。
3. 单击 \* 删除 \*。

此时将显示删除卷对话框。

4. 选择要删除的一个或多个卷、然后确认要执行此操作。
5. 单击 \* 删除 \*。

## 配置主机

了解如何在适用于vCenter的SANtricity存储插件中创建主机

要使用适用于vCenter的存储插件管理存储、您必须发现或定义网络中的每个主机。主机是指向存储阵列上的卷发送I/O的服务器。

#### 手动创建主机

创建主机是向存储阵列告知连接了哪些主机并允许对卷进行I/O访问所需的步骤之一。可以手动创建主机。

- 手动—在手动创建主机期间、您可以通过从列表中选择主机端口标识符或手动输入这些标识符来关联主机端口标识符。创建主机后、如果您计划共享对卷的访问、则可以为其分配卷或将其添加到主机集群。

## 如何分配卷

要使主机向卷发送I/O、您必须为其分配卷。您可以在创建卷时选择主机或主机集群、也可以稍后将卷分配给主机或主机集群。主机集群是一组主机。您可以创建一个主机集群、以便轻松地将相同的卷分配给多个主机。

为主机分配卷非常灵活、可以满足您的特定存储需求。

- 独立主机、不属于主机集群—您可以将卷分配给单个主机。卷只能由一台主机访问。
- 主机集群-您可以将卷分配给主机集群。主机集群中的所有主机均可访问此卷。
- 主机集群中的主机-您可以将卷分配给属于主机集群的单个主机。即使此主机属于主机集群、但此卷只能由单个主机访问、而不能由主机集群中的任何其他主机访问。

创建卷时、系统会自动分配逻辑单元号(LUN)。在I/O操作期间、LUN充当主机和控制器之间的地址。您可以在创建卷后更改LUN。

## 在适用于vCenter的SANtricity存储插件中创建主机访问

要使用适用于vCenter的存储插件管理存储、您必须发现或定义网络中的每个主机。

### 关于此任务

通过创建主机、您可以定义主机参数以提供与存储阵列的连接以及对卷的I/O访问。

创建主机时、请牢记以下准则：

- 您必须定义与主机关联的主机标识符端口。
- 请确保提供与主机分配的系统名称相同的名称。
- 如果您选择的名称已在使用中，则此操作不会成功。
- 名称长度不能超过 30 个字符。

### 步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 单击菜单：创建 [ 主机 ]。

此时将显示创建主机对话框。

4. 根据需要选择主机设置。

## 字段详细信息

正在设置 ...	Description
Name	键入新主机的名称。
主机操作系统类型	从下拉列表中选择新主机上运行的操作系统。
主机接口类型	(可选) 如果存储阵列支持多种类型的主机接口, 请选择要使用的主机接口类型。
主机端口	执行以下操作之一: <ul style="list-style-type: none"><li>• 选择I/O接口-通常、主机端口应已登录并可从下拉列表中使用。您可以从列表中选择主机端口标识符。</li><li>• 手动添加-如果列表中未显示主机端口标识符、则表示主机端口尚未登录。可以使用 HBA 实用程序或 iSCSI 启动程序实用程序来查找主机端口标识符并将其与主机关联。您可以手动输入主机端口标识符, 也可以将它们从实用程序 (一次一个) 复制 / 粘贴到主机端口字段中。您必须一次选择一个主机端口标识符才能将其与主机关联, 但您可以继续选择与主机关联的任意数量的标识符。每个标识符都会显示在主机端口字段中。如有必要, 您还可以通过选择标识符旁边的 * X * 来删除该标识符。</li></ul>
设置 CHAP 启动程序密钥	(可选)如果您选择或手动输入具有iSCSI IQN的主机端口、并且希望要求尝试访问存储阵列的主机使用质询握手身份验证协议(CHAP)进行身份验证、请选中"设置CHAP启动程序密钥"复选框。对于您选择或手动输入的每个iSCSI 主机端口, 请执行以下操作: <ul style="list-style-type: none"><li>• 输入在每个 iSCSI 主机启动程序上为 CHAP 身份验证设置的相同 CHAP 密钥。如果您使用相互 CHAP 身份验证 (双向身份验证, 可使主机向存储阵列验证自身, 并使存储阵列向主机验证自身), 则还必须在初始设置或通过更改设置为存储阵列设置 CHAP 密钥。</li><li>• 如果不需要主机身份验证, 请将此字段留空。目前, 唯一使用的 iSCSI 身份验证方法是 CHAP 。</li></ul>

5. 单击 \* 创建 \* 。

6. 如果需要更新主机信息, 请从表中选择主机, 然后单击 \* 查看 / 编辑设置 \* 。

### 结果

成功创建主机后, 系统会为为主机配置的每个主机端口创建一个默认名称 (用户标签)。默认别名为 ` < 主机名端口号 > `。例如, 为主机 IPT 创建的第一个端口的默认别名为 `ipt_1`。

### 完成后

您必须将卷分配给主机、以便用于I/O操作。转至 ["将卷分配给主机"](#)。

## 在适用于vCenter的SANtricity存储插件中创建主机集群

如果两个或更多主机需要对相同卷进行I/O访问、则可以创建主机集群。

关于此任务

创建主机集群时、请记住以下准则：

- 除非有两个或更多主机可用于创建集群、否则此操作不会启动。
- 主机集群中的主机可以具有不同的操作系统(异构)。
- 主机集群中的NVMe主机不能与非NVMe主机混合使用。
- 要创建启用了数据保证(Data Assurance、DA)的卷、您计划使用的主机连接必须支持DA。

如果存储阵列中控制器上的任何主机连接不支持 DA ，则关联的主机将无法访问已启用 DA 的卷上的数据。

- 如果您选择的名称已在使用中，则此操作不会成功。
- 名称长度不能超过 30 个字符。

步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 选择菜单：创建[主机集群]。

此时将显示创建主机集群对话框。

4. 根据需要选择主机集群的设置。

正在设置 ...	Description
Name	键入新主机集群的名称。
选择要共享卷访问的主机	从下拉列表中选择两个或更多主机。列表中仅显示尚未加入主机集群的主机。

5. 单击 \* 创建 \*。

如果选定主机连接到具有不同数据保证(Data Assurance、DA)功能的接口类型、则会显示一个对话框、其中会显示一条消息、指出DA在主机集群上不可用。此不可用性将阻止将已启用DA的卷添加到主机集群中。选择\*是\*继续、或者选择\*否\*取消。

DA 可提高整个存储系统的数据完整性。通过DA、存储阵列可以检查在主机和驱动器之间移动数据时可能发生的错误。对新卷使用 DA 可确保检测到任何错误。

结果

此时、新主机集群将显示在表中、而分配的主机将显示在下一行中。

完成后

您必须将卷分配给主机集群、以便用于I/O操作。转至 ["将卷分配给主机"](#)。

在适用于vCenter的SANtricity存储插件中为主机分配卷

您必须将卷分配给主机或主机集群、以便用于I/O操作。

开始之前

在将卷分配给主机时、请记住以下准则：

- 一次只能将卷分配给一个主机或主机集群。
- 分配的卷在存储阵列中的控制器之间共享。
- 主机或主机集群不能使用同一逻辑单元号(LUN)两次来访问卷。您必须使用唯一的LUN。
- 对于新卷组、如果在将所有卷分配给主机之前等待所有卷创建和初始化、则卷初始化时间会缩短。请注意、映射与卷组关联的卷后、所有卷都将还原到初始化速度较慢的卷。

关于此任务

卷分配会授予主机或主机集群对存储阵列中该卷的访问权限。

在此任务期间、系统将显示所有未分配的卷、但具有或不具有数据保证(Data Assurance、DA)的主机的功能如下所示：

- 对于支持 DA 的主机，您可以选择已启用 DA 或未启用 DA 的卷。
- 对于不支持 DA 的主机，如果选择的卷已启用 DA ，则会显示一条警告，指出系统必须先自动关闭卷上的 DA ， 然后才能将卷分配给主机。

在以下情况下，分配卷失败：

- 已分配所有卷。
- 此卷已分配给其他主机或主机集群。在以下情况下，无法分配卷：
- 不存在有效的主机或主机集群。
- 尚未为此主机定义主机端口标识符。
- 已定义所有卷分配。

步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 选择要将卷分配到的主机或主机集群，然后单击 \* 分配卷 \*。

此时将显示一个对话框，其中列出了可分配的所有卷。您可以对任意列进行排序，也可以在筛选器框中键入某些内容，以便于查找特定卷。

4. 选中要分配的每个卷旁边的复选框，或者选中表标题中的复选框以选择所有卷。
5. 单击 \* 分配 \* 以完成此操作。

## 结果

将一个或多个卷成功分配给主机或主机集群后，系统将执行以下操作：

- 分配的卷将收到下一个可用的 LUN 编号。主机使用此 LUN 编号来访问此卷。
- 用户提供的卷名称将显示在与主机关联的卷列表中。如果适用，出厂配置的访问卷也会显示在与主机关联的卷列表中。

在适用于vCenter的SANtricity存储插件中取消分配卷

如果您不再需要对卷进行I/O访问、则可以从主机或主机集群中取消分配该卷。

## 关于此任务

取消分配卷时、请记住以下准则：

- 如果要从主机集群中删除最后分配的卷、并且主机集群也包含具有特定分配的卷的主机、请确保在删除主机集群的最后一个分配之前删除或移动这些分配。
- 如果将主机集群、主机或主机端口分配给已注册到操作系统的卷、则必须先清除此注册、然后才能删除这些节点。

## 步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 选择要编辑的主机或主机集群、然后单击\*取消分配卷\*。

此时将显示一个对话框、其中显示了当前分配的所有卷。

4. 选中要取消分配的每个卷旁边的复选框、或者选中表标题中的复选框以选择所有卷。
5. 单击\*取消分配\*。

## 结果

- 已取消分配的卷可用于新分配。
- 在主机上配置更改之前、主机操作系统仍可识别此卷。

在适用于vCenter的SANtricity存储插件中更改主机的设置

您可以更改主机或主机集群的名称、主机操作系统类型以及关联的主机集群。

## 步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 选择要编辑的主机、然后单击\*查看/编辑设置\*。

此时将显示一个对话框，其中显示了当前主机设置。

- 要更改主机属性、请确保已选中\*属性\*选项卡、然后根据需要更改设置。

#### 字段详细信息

正在设置 ...	Description
Name	您可以更改用户提供的主机名称。需要为主机指定名称。
关联的主机集群	您可以选择以下选项之一： <ul style="list-style-type: none"><li>无—此主机仍为独立主机。如果主机已与主机集群关联、则系统会将此主机从集群中删除。</li><li>&lt;Host Cluster&gt;—系统将主机与选定集群关联。</li></ul>
主机操作系统类型	您可以更改在定义的主机上运行的操作系统类型。

- 要更改端口设置、请单击\*主机端口\*选项卡、然后根据需要更改设置。

#### 字段详细信息

正在设置 ...	Description
主机端口	您可以选择以下选项之一： <ul style="list-style-type: none"><li>添加—使用添加将新的主机端口标识符与主机关联。主机端口标识符名称的长度由主机接口技术决定。光纤通道和Infiniband主机端口标识符名称必须包含16个字符。iSCSI 主机端口标识符名称最多包含 223 个字符。此端口必须是唯一的。不允许使用已配置的端口号。</li><li>删除—使用删除删除删除主机端口标识符(取消关联)。删除选项不会物理删除主机端口。此选项将删除主机端口与主机之间的关联。除非您删除主机总线适配器或 iSCSI 启动程序，否则控制器仍可识别主机端口。</li></ul> <p> 如果删除主机端口标识符、它将不再与此主机关联。此外、主机将无法通过此主机端口标识符访问其分配的任何卷。</p>
Label	要更改端口标签名称、请单击*编辑*图标(铅笔)。端口标签名称必须是唯一的。不允许使用已配置的标签名称。
CHAP机密	仅对iSCSI主机显示。您可以为启动程序(iSCSI主机)设置或更改CHAP密钥。系统使用质询握手身份验证协议(Challenge Handshake Authentication Protocol、CHAP)方法、在初始链路期间验证目标和启动程序的身份。身份验证基于一个称为CHAP机密的共享安全密钥。

6. 单击 \* 保存 \*。

在适用于vCenter的SANtricity存储插件中删除主机或主机集群

您可以删除主机或主机集群、以使卷不再与该主机关联。

关于此任务

删除主机或主机集群时、请牢记以下准则：

- 系统将删除任何特定卷分配、并且关联的卷可用于新分配。
- 如果主机属于具有自己特定分配的主机集群、则该主机集群不受影响。但是、如果主机属于没有任何其他分配的主机集群、则主机集群以及任何其他关联的主机或主机端口标识符将继承任何默认分配。
- 与此主机关联的任何主机端口标识符都将变为未定义状态。

步骤

1. 从管理页面中，选择具有主机连接的存储阵列。
2. 选择菜单：配置 [ 配置主机 ]。

此时将打开配置主机页面。

3. 选择要删除的主机或主机集群、然后单击\*删除\*。

此时将显示确认对话框。

4. 确认要执行此操作、然后单击\*删除\*。

结果

如果删除了主机、系统将执行以下操作：

- 删除主机、如果适用、将其从主机集群中删除。
- 删除对任何已分配卷的访问。
- 将关联卷返回到未分配状态。
- 将与主机关联的任何主机端口标识符返回到未关联状态。如果删除了主机集群、系统将执行以下操作：
  - 删除主机集群及其关联主机(如果有)。
  - 删除对任何已分配卷的访问。
  - 将关联卷返回到未分配状态。
  - 将与主机关联的任何主机端口标识符返回到未关联状态。

## 配置池和卷组

在适用于vCenter的SANtricity存储插件中了解存储池和卷组

要在适用于vCenter的存储插件中配置存储、请创建一个池或卷组、其中包含要在存储阵列中使用的硬盘驱动器(HDD)或固态硬盘(SSD)驱动器。

## 配置

物理硬件配置到逻辑组件中、以便对数据进行组织并轻松检索。支持两种类型的分组：

- 池
- 卷组

池和卷组是存储阵列中的顶级存储单元：它们将驱动器的容量划分为可管理的分区。在这些逻辑分区中、是指存储数据的单个卷或LUN。

部署存储系统后、第一步是通过以下方式向各种主机提供可用驱动器容量：

- 创建具有足够容量的池或卷组
- 将满足性能要求所需的驱动器数量添加到池或卷组
- 选择所需的RAID保护级别(如果使用卷组)以满足特定业务要求

您可以在同一存储系统上使用池或卷组、但一个驱动器不能属于多个池或卷组。然后、使用池或卷组上的空间创建提供给主机用于I/O的卷。

## 池

池用于将物理硬盘驱动器聚合到较大的存储空间中、并为其提供增强的RAID保护。池会根据分配给池的驱动器总数创建多个虚拟RAID集、并在所有参与驱动器之间平均分布数据。如果丢失或添加了驱动器、系统会在所有活动驱动器之间动态重新平衡数据。

池可作为另一个RAID级别运行、可对底层RAID架构进行虚拟化、以优化执行重建、驱动器扩展和处理驱动器丢失等任务时的性能和灵活性。在8+2配置中、系统会自动将RAID级别设置为6 (八个数据磁盘加上两个奇偶校验磁盘)。

## 驱动器匹配

您可以选择在池中使用HDD或SSD；但是、与卷组一样、池中的所有驱动器都必须使用相同的技术。控制器会自动选择要包含的驱动器、因此您必须确保具有足够数量的驱动器来支持您选择的技术。

## 管理故障驱动器

池的最小容量为11个驱动器；但是、如果驱动器发生故障、则会为一个驱动器预留一个容量作为备用容量。此备用容量称为“保留容量”。

创建池时、会保留一定的容量以供紧急使用。此容量以多个驱动器表示、但实际实施会分布在整个驱动器池中。保留的默认容量取决于池中的驱动器数量。

创建池后、您可以将保留容量值更改为更多或更少的容量、甚至可以将其设置为无保留容量(0个驱动器值)。可以保留的最大容量(以驱动器数表示)为10、但根据池中的驱动器总数、可用容量可能会更少。

## 卷组

卷组用于定义如何在存储系统中为卷分配容量。磁盘驱动器按RAID组进行组织、卷驻留在RAID组中的驱动器上。因此、卷组配置设置可确定哪些驱动器属于该组、以及使用了哪些RAID级别。

创建卷组时、控制器会自动选择要包含在此组中的驱动器。您必须手动为组选择RAID级别。卷组的容量是所选驱动器总数乘以其容量。

## 驱动器匹配

您必须匹配卷组中的驱动器、以确定其大小和性能。如果卷组中的驱动器较小或较大、则会将所有驱动器识别为最小容量大小。如果卷组中的驱动器速度较慢、速度较快、则会以最慢的速度识别所有驱动器。这些因素会影响存储系统的性能和整体容量。

您不能混用不同的驱动器技术(HDD和SSD驱动器)。RAID 3、5和6最多限制为30个驱动器。RAID 1和RAID 10使用镜像、因此这些卷组的磁盘数量必须为偶数。

## 管理故障驱动器

如果卷组中包含的RAID 1/10、RAID 3、RAID 5或RAID 6卷中的驱动器发生故障、则卷组会使用热备用驱动器作为备用驱动器。热备用驱动器不包含任何数据、并为存储阵列添加了另一个冗余级别。

如果存储阵列中的某个驱动器发生故障、则热备用驱动器会自动替换故障驱动器、而无需物理交换。如果在驱动器发生故障时热备用驱动器可用、则控制器会使用冗余数据将故障驱动器中的数据重建到热备用驱动器。

## 确定是使用池还是卷组

### 选择一个池

- 如果您需要更快的驱动器重建速度和简化的存储管理、以及/或具有高度随机的 workload。
- 如果要将每个卷的数据随机分布在构成池的一组驱动器上。您不能设置或更改池或池中卷的RAID级别。池使用RAID级别6。

### 选择卷组

- 如果您需要最大的系统带宽、调整存储设置的能力以及高度顺序的工作负载、
- 如果要根据RAID级别在驱动器之间分布数据。您可以在创建卷组时指定RAID级别。
- 要在构成卷组的一组驱动器上按顺序写入每个卷的数据。



由于池可以与卷组共存、因此存储阵列可以同时包含池和卷组。

## 自动创建池与手动创建池

根据您的存储配置、您可以允许系统自动创建池、也可以手动自行创建池。池是一组逻辑分组的驱动器。

在创建和管理池之前、请查看以下各节、了解如何自动创建池以及何时可能需要手动创建池。

### 自动创建

如果系统检测到存储阵列中的未分配容量、则会在系统检测到存储阵列中的未分配容量时启动自动创建池。它会自动提示您创建一个或多个池、或者向现有池添加未分配的容量、或者同时创建这两者。

如果满足以下条件之一、则会自动创建池：

- 存储阵列中不存在池、并且有足够的类似驱动器来创建新池。
- 新驱动器将添加到至少具有一个池的存储阵列中。一个池中的每个驱动器必须具有相同的驱动器类型(HDD或SSD)并具有类似的容量。系统将提示您完成以下任务：

- 如果这些类型的驱动器数量充足、请创建一个池。
- 如果未分配的容量包含不同的驱动器类型、请创建多个池。
- 如果已在存储阵列中定义池、请将驱动器添加到现有池、然后将相同驱动器类型的新驱动器添加到该池。
- 将相同驱动器类型的驱动器添加到现有池中、如果新驱动器的驱动器类型不同、请使用其他驱动器类型创建不同的池。

## 手动创建

如果自动创建无法确定最佳配置、您可能需要手动创建池。出现这种情况的原因可能如下：

- 新驱动器可能会添加到多个池中。
- 一个或多个新池候选项可以使用磁盘架丢失保护或抽屉丢失保护。
- 一个或多个当前池候选项无法保持其磁盘架丢失保护或抽屉丢失保护状态。如果存储阵列上有多个应用程序、并且不希望这些应用程序争用相同的驱动器资源、您可能还需要手动创建池。在这种情况下、您可能会考虑手动为一个或多个应用程序创建一个较小的池。您只能分配一个或两个卷、而不能将工作负载分配给一个大型池、该池包含许多卷、可用于分布数据。手动创建专用于特定应用程序工作负载的单独池可以提高存储阵列操作的执行速度、并减少争用。

## 在适用于vCenter的SANtricity存储插件中自动创建池

当系统检测到至少11个未分配的驱动器或检测到一个符合现有池条件的未分配驱动器时、您可以自动创建池。池是一组逻辑分组的驱动器。

### 开始之前

如果满足以下条件之一、则可以启动池自动配置对话框：

- 至少检测到一个未分配的驱动器、可以将其添加到具有类似驱动器类型的现有池中。
- 检测到可用于创建新池的11个或更多未分配驱动器(如果由于驱动器类型不同而无法将其添加到现有池中)。

### 关于此任务

您可以使用自动创建池将存储阵列中所有未分配的驱动器轻松配置到一个池中、并将驱动器添加到现有池中。

请记住以下几点：

- 向存储阵列添加驱动器时、系统会自动检测这些驱动器、并提示您根据驱动器类型和当前配置创建一个或多个池。
- 如果先前已定义池、则系统会自动提示您选择将兼容驱动器添加到现有池。将新驱动器添加到现有池后、系统会自动在新容量中重新分布数据、现在、新容量包含您添加的新驱动器。
- 在配置EF600或EF300存储阵列时、请确保每个控制器可以访问前12个插槽中相同数量的驱动器、以及最后12个插槽中相同数量的驱动器。此配置有助于控制器更有效地使用驱动器端PCIe总线。要创建池、应使用存储阵列中的所有驱动器。

### 步骤

1. 从管理页面中、选择池的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择菜单：更多[启动池自动配置]。

此结果表列出了新池、已添加驱动器的现有池或这两者。默认情况下、新池使用序列号命名。

请注意、系统会执行以下操作：

- 如果有足够数量的驱动器具有相同的驱动器类型(HDD或SSD)并具有类似的容量、则创建一个池。
- 如果未分配的容量包含不同的驱动器类型、则创建多个池。
- 如果已在存储阵列中定义池、则将驱动器添加到现有池、并将相同驱动器类型的新驱动器添加到该池。
- 将相同驱动器类型的驱动器添加到现有池中、如果新驱动器的驱动器类型不同、则使用其他驱动器类型创建不同的池。

4. 要更改新池的名称、请单击\*编辑\*图标(铅笔)。

5. 要查看池的其他特征、请将光标置于或轻触详细信息图标(页面)。

此时将显示有关驱动器类型、安全功能、数据保证(Data Assurance、DA)功能、磁盘架丢失保护和抽盒丢失保护的信息。

对于EF600和EF300存储阵列、还会显示资源配置和卷块大小的设置。

6. 单击 \* 接受 \*。

在适用于vCenter的SANtricity存储插件中手动创建池

如果设置不符合自动池配置的要求、则可以手动创建池。池是一组逻辑分组的驱动器。

开始之前

- 必须至少有11个驱动器具有相同的驱动器类型(HDD或SSD)。
- 磁盘架丢失保护要求构成池的驱动器至少位于六个不同的驱动器架中、并且一个驱动器架中的驱动器不超过两个。
- 抽盒丢失保护功能要求构成池的驱动器至少位于五个不同的抽盒中、并且池中每个抽盒包含同等数量的驱动器架。
- 在配置EF600或EF300存储阵列时、请确保每个控制器可以访问前12个插槽中相同数量的驱动器、以及最后12个插槽中相同数量的驱动器。此配置有助于控制器更有效地使用驱动器端PCIe总线。要创建池、应使用存储阵列中的所有驱动器。

关于此任务

在创建池期间、您可以确定其特征、例如驱动器类型、安全功能、数据保证(Data Assurance、DA)功能、磁盘架丢失保护和抽盒丢失保护。

对于EF600和EF300存储阵列、设置还包括资源配置和卷块大小。

步骤

1. 从管理页面中、选择池的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 单击菜单：创建[池]。

此时将显示创建池对话框。

4. 键入池的名称。
5. (可选)如果存储阵列中有多种类型的驱动器、请选择要使用的驱动器类型。

结果表列出了您可以创建的所有可能池。

6. 根据以下特征选择要使用的候选池、然后单击\*创建\*。

## 字段详细信息

特性	使用 ...
可用容量	以GiB显示候选池的可用容量。选择一个具有满足应用程序存储需求的容量的候选池。保留(备用)容量也会分布在池中、而不是可用容量的一部分。
驱动器总数	显示候选池中的可用驱动器数量。系统会自动预留尽可能多的驱动器以保留容量(对于池中的每六个驱动器、系统会为保留容量预留一个驱动器)。发生驱动器故障时、会使用保留容量来保存重建的数据。
驱动器块大小(仅限EF300和EF600)	显示池中驱动器可以写入的块大小(扇区大小)。值可能包括： <ul style="list-style-type: none"> <li>• 512—512字节扇区大小。</li> <li>• 4k—4、096字节扇区大小。</li> </ul>
支持安全保护	指示候选池是否全部由具有安全功能的驱动器组成、这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。 <ul style="list-style-type: none"> <li>• 您可以使用驱动器安全保护池、但所有驱动器都必须具有安全功能才能使用此功能。</li> <li>• 如果要创建仅FDE池、请在安全功能列中查找*是- FDE*。如果要创建仅FIPS的池、请查找*是- Fips*或*是- FIPS (混合)*。"混合"表示140-2和140-3级驱动器的混合。如果混合使用这些级别、请注意、池将在较低的安全级别(140-2)下运行。</li> <li>• 您可以创建一个由驱动器组成的池、这些驱动器可能支持安全、也可能不支持安全、或者混合了多种安全级别。如果池中的驱动器包含不支持安全的驱动器、则无法确保池的安全。</li> </ul>
是否启用安全性?	提供了使用支持安全的驱动器启用驱动器安全功能的选项。如果池支持安全、并且您已创建安全密钥、则可以选中复选框来启用安全性。 <div style="display: flex; align-items: center; margin-top: 10px;">  <p>启用驱动器安全性后删除驱动器安全性的唯一方法是删除池并擦除驱动器。</p> </div>
支持DA	指示此池候选项是否可使用数据保证(Data Assurance、DA)。DA可检查并更正在数据通过控制器向下传输到驱动器时可能发生的错误。如果要使用DA、请选择一个支持DA的池。只有在启用了DA功能后、此选项才可用。池可以包含支持DA或不支持DA的驱动器、但要使用此功能、所有驱动器都必须支持DA。
支持资源配置(仅限EF300和EF600)	显示资源配置是否可用于此池候选项。资源配置是EF300和EF600存储阵列中提供的一项功能、可在不执行后台初始化过程的情况下立即使用卷。

特性	使用 ...
磁盘架丢失保护	显示磁盘架丢失保护是否可用。磁盘架丢失保护功能可确保在与单个驱动器磁盘架完全失去通信时能够访问池中卷上的数据。
抽盒丢失保护	显示是否提供了抽盒丢失保护、只有在使用包含抽盒的驱动器架时、才会提供此保护。抽盒丢失保护功能可确保在与驱动器架中的单个抽盒完全失去通信时能够访问池中卷上的数据。
支持的卷块大小(仅限EF300和EF600)	显示了可为池中的卷创建的块大小： <ul style="list-style-type: none"> <li>• 512n—512字节原生。</li> <li>• 512e—模拟512字节。</li> <li>• 4 k—4、096字节。</li> </ul>

在适用于vCenter的SANtricity存储插件中创建卷组

您可以为主机可访问的一个或多个卷创建卷组。卷组是指具有RAID级别和容量等共享特征的卷的容器。

开始之前

请查看以下准则：

- 您至少需要一个未分配的驱动器。
- 对于一个卷组中的驱动器容量、存在限制。这些限制因主机类型而异。
- 要启用磁盘架/抽盒丢失保护、您必须创建一个卷组、该卷组使用至少位于三个磁盘架或抽盒中的驱动器、除非您使用的是RAID 1、其中至少包含两个磁盘架/抽盒。
- 在配置EF600或EF300存储阵列时、请确保每个控制器可以访问前12个插槽中相同数量的驱动器、以及最后12个插槽中相同数量的驱动器。此配置有助于控制器更有效地使用驱动器端PCIe总线。当前、系统允许在创建卷组时在"高级"功能下选择驱动器。

查看您选择的RAID级别如何影响卷组的生成容量。

- 如果选择RAID 1、则必须一次添加两个驱动器、以确保选择镜像对。如果选择四个或更多驱动器、则会实现镜像和条带化(称为RAID 10或RAID 1+0)。
- 如果选择RAID 5、则必须至少添加三个驱动器才能创建卷组。
- 如果选择RAID 6、则必须至少添加五个驱动器才能创建卷组。

关于此任务

在创建卷组期间、您可以确定组特征、例如驱动器数量、安全功能、数据保证(Data Assurance、DA)功能、磁盘架丢失保护和抽盒丢失保护。

对于EF600和EF300存储阵列、设置还包括资源配置、驱动器块大小和卷块大小。



借助容量更大的驱动器以及在控制器之间分布卷的功能、可以为每个卷组创建多个卷、从而充分利用存储容量并保护数据。

## 步骤

1. 从管理页面中、选择卷组的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 单击菜单：创建[卷组]。

此时将显示创建卷组对话框。

4. 键入卷组的名称。
5. 选择最符合数据存储和保护要求的RAID级别。此时将显示卷组候选表、并且仅显示支持选定RAID级别的候选卷。
6. (可选)如果存储阵列中有多种类型的驱动器、请选择要使用的驱动器类型。

此时将显示卷组候选表、并且仅显示支持选定驱动器类型和RAID级别的候选卷。

7. (可选)您可以选择自动方法或手动方法来定义要在卷组中使用的驱动器。默认选择为"Automatic"方法。



除非您是了解驱动器冗余和最佳驱动器配置的专家、否则请勿使用手动方法。

要手动选择驱动器、请单击\*手动选择驱动器(高级)链接。单击后、它将更改为\*自动选择驱动器(高级)。

使用手动方法可以选择卷组包含哪些特定驱动器。您可以选择特定的未分配驱动器以获取所需的容量。如果存储阵列包含具有不同介质类型或不同接口类型的驱动器、则只能为单个驱动器类型选择未配置的容量来创建新的卷组。

8. 根据显示的驱动器特征、选择要在卷组中使用的驱动器、然后单击\*创建\*。

显示的驱动器特征取决于您选择的是自动方法还是手动方法。有关详细信息、请参见SANtricity System Manager文档、["创建卷组"](#)。

在适用于vCenter的SANtricity存储插件中向池或卷组添加容量

您可以添加驱动器以扩展现有池或卷组中的可用容量。

## 开始之前

- 驱动器必须处于最佳状态。
- 驱动器必须具有相同的驱动器类型(HDD或SSD)。
- 池或卷组必须处于最佳状态。
- 如果池或卷组包含所有支持安全的驱动器、请仅添加支持安全的驱动器、以继续使用支持安全的驱动器的加密功能。

支持安全的驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。

关于此任务

在此任务中、您可以添加要包含在池或卷组中的可用容量。您可以使用此可用容量创建其他卷。在此操作期间、卷中的数据仍可访问。

对于池、一次最多可以添加60个驱动器。对于卷组、一次最多可以添加两个驱动器。如果需要添加的驱动器数超过最大数量、请重复执行操作步骤。(池中的驱动器数不能超过存储阵列的最大限制。)



添加驱动器后、可能需要增加保留容量。您应考虑在执行扩展操作后增加预留容量。



避免使用能够向不支持DA的池或卷组添加容量的数据保证(Data Assurance、DA)驱动器。池或卷组无法利用支持DA的驱动器的功能。在这种情况下、请考虑使用不支持DA的驱动器。

#### 步骤

1. 从管理页面中、选择具有池或卷组的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择要添加驱动器的池或卷组、然后单击\*添加容量\*。

此时将显示添加容量对话框。仅显示与池或卷组兼容的未分配驱动器。

4. 在\*选择要添加容量的驱动器...\*下、选择要添加到现有池或卷组的一个或多个驱动器。

控制器固件会使用顶部列出的最佳选项来排列未分配的驱动器。添加到池或卷组的总可用容量显示在\*选定总容量\*中的列表下方。

## 字段详细信息

字段	Description
磁盘架	指示驱动器的磁盘架位置。
托架	指示驱动器的托架位置
容量(GiB)	<p>指示驱动器容量。</p> <ul style="list-style-type: none"> <li>• 尽可能选择容量等于池或卷组中当前驱动器容量的驱动器。</li> <li>• 如果您必须添加容量较小的未分配驱动器、请注意、池或卷组中当前每个驱动器的可用容量会减少。因此、池或卷组中的驱动器容量相同。</li> <li>• 如果您必须添加容量更大的未分配驱动器、请注意、您添加的未分配驱动器的可用容量会减少、以便与池或卷组中驱动器的当前容量匹配。</li> </ul>
支持安全保护	<p>指示驱动器是否支持安全保护。</p> <ul style="list-style-type: none"> <li>• 您可以使用驱动器安全功能保护池或卷组、但所有驱动器都必须具有安全功能才能使用此功能。</li> <li>• 可以使用支持安全和不支持安全的驱动器组合创建池或卷组、但无法启用驱动器安全功能。</li> <li>• 包含所有支持安全的驱动器的池或卷组不能接受不支持安全的驱动器来进行备用或扩展、即使未使用加密功能也是如此。</li> <li>• 支持安全的驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。FIPS驱动器可以是级别140-2或140-3、而级别140-3则是更高的安全性级别。如果选择140-2和140-3级别的混合驱动器、则池或卷组将以较低的安全级别(140-2)运行。</li> </ul>
支持DA	<p>指示驱动器是否支持数据保证(Data Assurance、DA)。</p> <ul style="list-style-type: none"> <li>• 建议不要使用数据保证(Data Assurance、DA)无法向支持DA的池或卷组添加容量的驱动器。池或卷组不再具有DA功能、您也无法再对池或卷组中新创建的卷启用DA。</li> <li>• 建议不要使用能够向不支持DA的池或卷组添加容量的数据保证(Data Assurance、DA)驱动器、因为该池或卷组无法利用支持DA的驱动器的功能(驱动器属性不匹配)。在这种情况下、请考虑使用不支持DA的驱动器。</li> </ul>
支持DULBE	<p>指示驱动器是否具有已取消分配或未写入逻辑块错误(DULBE")选项。DULBE"是NVMe驱动器上的一个选项、它允许EF300或EF600存储阵列支持资源配置的卷。</p>

5. 单击 \* 添加 \*。

如果要向池或卷组添加驱动器、则如果选择的驱动器导致池或卷组不再具有以下一个或多个属性、则会显示一个确认对话框：

- 磁盘架丢失保护
- 抽盒丢失保护
- 全磁盘加密功能
- 数据保证功能
- DULBE"功能

6. 要继续、请单击\*是\*；否则请单击\*取消\*。

## 结果

将未分配的驱动器添加到池或卷组后、该池或卷组中每个卷中的数据将重新分配、以包括其他驱动器。

在适用于vCenter的SANtricity存储插件中创建SSD缓存

要动态提高系统性能、您可以使用SSD缓存功能将最常访问的数据("热"数据)缓存到延迟较低的固态驱动器(SSD)上。SSD缓存仅用于主机读取。

## 开始之前

您的存储阵列必须包含一些SSD驱动器。



SSD缓存在EF600或EF300存储系统上不可用。

## 关于此任务

创建SSD缓存时、您可以使用一个或多个驱动器。由于读取缓存位于存储阵列中、因此使用该存储阵列的所有应用程序将共享缓存。选择要缓存的卷、然后自动动态缓存。

创建SSD缓存时、请遵循以下准则。

- 您只能在创建SSD缓存时启用安全性、而不能稍后启用。
- 每个存储阵列仅支持一个SSD缓存。
- 存储阵列上的最大可用SSD缓存容量取决于控制器的主缓存容量。
- Snapshot映像不支持SSD缓存。
- 如果导入或导出启用或禁用了SSD缓存的卷、则不会导入或导出缓存的数据。
- 分配给使用控制器SSD缓存的任何卷均不符合自动负载平衡传输的条件。
- 如果关联卷已启用安全保护、请创建启用安全保护的SSD缓存。

## 步骤

1. 从管理页面中、选择缓存的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 单击菜单：创建SSD缓存。

此时将显示创建SSD缓存对话框。

- 键入SSD缓存的名称。
- 根据以下特征选择要使用的SSD缓存候选项。

#### 字段详细信息

特性	使用 ...
<b>Capacity</b>	显示可用容量(以GiB为单位)。根据应用程序的存储需求选择容量。SSD缓存的最大容量取决于控制器的主缓存容量。如果向SSD缓存分配的容量超过最大值、则任何额外容量都将不可用。SSD缓存容量计入您的总分配容量。
驱动器总数	显示可用于此SSD缓存的驱动器数量。选择包含所需驱动器数量的候选SSD
支持安全保护	指示候选SSD缓存是否全部由具有安全功能的驱动器组成、这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。如果要创建启用了安全保护的SSD缓存、请在支持安全保护列中查找"是-FDE"或"是-FIPS-FIPS-"。
是否启用安全性?	提供了使用支持安全的驱动器启用驱动器安全功能的选项。如果要创建启用了安全保护的SSD缓存、请选中*启用安全性*复选框。注意:启用后、无法禁用安全性。您只能在创建SSD缓存时启用安全性、而不能稍后启用。
支持DA	指示数据保证(Data Assurance、DA)是否可用于此SSD缓存候选项。数据保证(Data Assurance、DA)可检查并更正数据通过控制器向下传输到驱动器时可能发生的错误。如果要使用DA、请选择一个支持DA的SSD缓存候选项。只有在启用了DA功能后、此选项才可用。SSD缓存既可以包含支持DA的驱动器、也可以包含不支持DA的驱动器、但要使用DA、所有驱动器都必须支持DA。

- 将SSD缓存与要实施SSD读取缓存的卷相关联。要立即在兼容卷上启用SSD缓存、请选中\*在映射到主机的现有兼容卷上启用SSD缓存\*复选框。

如果卷共享相同的驱动器安全性和DA功能、则这些卷是兼容的。

- 单击 \* 创建 \*。

在适用于vCenter的SANtricity存储插件中更改池的配置设置

您可以编辑池的设置、包括其名称、容量警报设置、修改优先级和保留容量。

关于此任务

此任务介绍如何更改池的配置设置。



您不能使用插件界面更改池的RAID级别。插件会自动将池配置为RAID 6。

#### 步骤

- 从管理页面中、选择具有池的存储阵列。
- 选择菜单: 配置[配置池和卷组]。
- 选择要编辑的池、然后单击\*查看/编辑设置\*。

此时将显示Pool Settings对话框。

4. 选择\*设置\*选项卡、然后根据需要编辑池设置。

正在设置 ...	Description
Name	您可以更改用户提供的池名称。需要为池指定名称。
容量警报	<p>您可以在池中的可用容量达到或超过指定阈值时发送警报通知。当存储在池中的数据超过指定阈值时、插件会发送一条消息、让您有时间添加更多存储空间或删除不必要的对象。警报显示在信息板上的Notifications区域中、可通过电子邮件和SNMP陷阱消息从服务器发送给管理员。您可以定义以下容量警报：</p> <ul style="list-style-type: none"> <li>• 严重警报-当池中的可用容量达到或超过指定阈值时、此严重警报将向您发出通知。使用spinner控件调整阈值百分比。选中此复选框可禁用此通知。</li> <li>• 早期警报—此早期警报会在池中的可用容量达到指定阈值时向您发出通知。使用spinner控件调整阈值百分比。选中此复选框可禁用此通知。</li> </ul>
修改优先级	<p>您可以指定池中修改操作相对于系统性能的优先级级别。如果池中修改操作的优先级较高、则操作完成速度会更快、但可能会降低主机I/O性能。优先级较低会导致操作所需时间较长、但对主机I/O性能的影响较小。您可以从五个优先级中进行选择：最低、低、中、高和最高。优先级越高、对主机I/O和系统性能的影响就越大。</p> <ul style="list-style-type: none"> <li>• 关键重建优先级—如果多个驱动器故障导致某些数据没有冗余、而另一个驱动器故障可能导致数据丢失、则此滑块条可确定数据重建操作的优先级。</li> <li>• 已降级重建优先级—此滑块用于确定发生驱动器故障时数据重建操作的优先级、但数据仍具有冗余、并且附加驱动器故障不会导致数据丢失。</li> <li>• 后台操作优先级-此滑块条用于确定池处于最佳状态时执行的池后台操作的优先级。这些操作包括动态卷扩展(DVE)、即时可用性格式(IAF)以及将数据迁移到更换或添加的驱动器。</li> </ul>

正在设置 ...	Description
保留容量(EF600或EF300的"优化容量")	<p>保留容量—您可以定义驱动器数量以确定池中为支持潜在驱动器故障而预留的容量。发生驱动器故障时、会使用保留容量来保存重建的数据。在数据重建过程中、池会使用保留容量、而不是在卷组中使用热备用驱动器。使用spinner控件调整驱动器数量。根据驱动器数量、池中的保留容量显示在spinner框旁边。请记住以下有关保留容量的信息。</p> <ul style="list-style-type: none"> <li>• 由于保留容量会从池的总可用容量中减去、因此您预留的容量会影响可用于创建卷的可用容量。如果为保留容量指定0、则池中的所有可用容量将用于创建卷。</li> <li>• 如果减少保留容量、则增加可用于池卷的容量。</li> </ul> <p>额外优化容量(仅限EF600和EF300阵列)—创建池时、系统会生成一个建议的优化容量、以便在可用容量与性能以及驱动器使用寿命之间取得平衡。您可以通过向右移动滑块以提高性能和驱动器使用寿命而降低可用容量的增加来调整这种平衡、也可以将滑块移至左侧以增加可用容量、从而降低性能和驱动器使用寿命。如果未分配一部分容量、SSD驱动器的使用寿命将会延长、并且最大写入性能也会提高。对于与池关联的驱动器、未分配的容量由池的保留容量、可用容量(卷未使用的容量)以及作为额外优化容量而预留的部分可用容量组成。额外的优化容量可通过减少可用容量来确保最低的优化容量级别、因此不可用于创建卷。</p>

5. 单击 \* 保存 \*。

在适用于vCenter的SANtricity存储插件中更改卷组的配置设置

您可以编辑卷组的设置、包括其名称和RAID级别。

开始之前

如果要更改RAID级别以满足访问卷组的应用程序的性能需求、请确保满足以下前提条件：

- 卷组必须处于最佳状态。
- 卷组中必须有足够的容量才能转换为新的RAID级别。

步骤

1. 从管理页面中、选择具有卷组的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择要编辑的卷组、然后单击\*查看/编辑设置\*。

此时将显示卷组设置对话框。

4. 选择\*设置\*选项卡、然后根据需要编辑卷组设置。

正在设置 ...	Description
Name	您可以更改用户提供的卷组名称。需要为卷组指定名称。
RAID级别	<p>从下拉菜单中选择新的RAID级别。</p> <ul style="list-style-type: none"> <li>• * RAID 0条带化*—提供高性能、但不提供任何数据冗余。如果卷组中的一个驱动器发生故障、则所有关联卷都会发生故障、并且所有数据都将丢失。条带化RAID组将两个或更多驱动器组合成一个大逻辑驱动器。</li> <li>• * RAID 1镜像*—提供高性能和最佳数据可用性、适合在企业或个人级别存储敏感数据。通过自动将一个驱动器的内容镜像到镜像对中的第二个驱动器来保护数据。它可以在单个驱动器发生故障时提供保护。</li> <li>• * RAID 10条带化/镜像*—提供RAID 0 (条带化)和RAID 1 (镜像)的组合、可在选择四个或更多驱动器时实现。RAID 10适用于需要高性能和容错能力的高卷事务应用程序、例如数据库。</li> <li>• * RAID 5*—最适合多用户环境(例如数据库或文件系统存储)、其中典型I/O大小较小且读取活动比例较高。</li> <li>• * RAID 6*—最适合需要RAID 5以上冗余保护但不需要高写入性能的环境。使用命令行界面(CLI)只能将RAID 3分配给卷组。更改RAID级别后、此操作将无法在开始后取消。在更改期间、您的数据将保持可用。</li> </ul>
优化容量(仅限EF600阵列)	创建卷组时、系统会生成一个建议的优化容量、以便在可用容量与性能以及驱动器使用寿命之间取得平衡。您可以通过向右移动滑块以提高性能和驱动器使用寿命而降低可用容量的增加来调整这种平衡、也可以将滑块移至左侧以增加可用容量、从而降低性能和驱动器使用寿命。如果未分配一部分容量、SSD驱动器的使用寿命将会延长、并且最大写入性能也会提高。对于与卷组关联的驱动器、未分配的容量由组的可用容量(卷未使用的容量)以及作为额外优化容量而预留的部分可用容量组成。额外的优化容量可通过减少可用容量来确保最低的优化容量级别、因此不可用于创建卷。

5. 单击 \* 保存 \*。

如果因RAID级别更改而导致容量减少、卷冗余丢失或磁盘架/抽屉丢失保护丢失、则会显示一个确认对话框。选择\*是\*继续；否则单击\*否\*。

结果

如果更改卷组的RAID级别、插件将更改组成卷组的每个卷的RAID级别。在此操作期间、性能可能会受到轻微影响。

在适用于vCenter的SANtricity存储插件中更改SSD缓存设置

您可以编辑SSD缓存的名称并查看其状态、最大和当前容量、驱动器安全性和数据保证状态及其关联的卷和驱动器。



EF600或EF300存储系统不支持此功能。

## 步骤

1. 从管理页面中、选择具有SSD缓存的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择要编辑的SSD缓存、然后单击\*查看/编辑设置\*。

此时将显示SSD缓存设置对话框。

4. 根据需要查看或编辑SSD缓存设置。

## 字段详细信息

正在设置 ...	Description
Name	显示SSD缓存的名称、您可以对其进行更改。SSD缓存的名称为必填项。
特性	显示SSD缓存的状态。可能的状态包括： <ul style="list-style-type: none"><li>• 最佳</li><li>• 未知</li><li>• 已降级</li><li>• 失败(失败状态会导致严重的MEL事件。)</li><li>• 已暂停</li></ul>
容量	显示SSD缓存的当前容量和允许的最大容量。SSD缓存允许的最大容量取决于控制器的主缓存大小： <ul style="list-style-type: none"><li>• 最多1 GiB</li><li>• 1 GiB到2 GiB</li><li>• 2 GiB到4 GiB</li><li>• 超过4 GiB</li></ul>
安全性和DA	显示SSD缓存的驱动器安全性和数据保证状态。 <ul style="list-style-type: none"><li>• 支持安全—表示SSD缓存是否全部由支持安全的驱动器组成。支持安全的驱动器是一种自加密驱动器、可以保护其数据免受未经授权的访问。</li><li>• 已启用安全-指示是否已在SSD缓存上启用安全性。</li><li>• *支持DA *-指示SSD缓存是否全部由支持DA的驱动器组成。支持DA的驱动器可以检查并更正在主机和存储阵列之间传输数据时可能发生的错误。</li></ul>
关联对象	显示了与SSD缓存关联的卷和驱动器。

5. 单击 \* 保存 \*。

在适用于vCenter的SANtricity存储插件中查看SSD缓存统计信息

您可以查看SSD缓存的统计信息、例如读取、写入、缓存命中率、缓存分配百分比、和缓存利用率百分比。



EF600或EF300存储系统不支持此功能。

关于此任务

标称统计信息是详细统计信息的一部分、显示在查看SSD缓存统计信息对话框中。只有在将所有SSD统计信息导出到.csv文件时、才能查看SSD缓存的详细统计信息。

在查看和解释统计信息时、请记住、某些解释是通过结合统计信息得出的。

步骤

1. 从管理页面中、选择具有SSD缓存的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择要查看其统计信息的SSD缓存、然后单击菜单：更多(查看SSD缓存)统计信息。

此时将显示查看SSD缓存统计信息对话框、并显示选定SSD缓存的标称统计信息。

字段详细信息

正在设置 ...	Description
读取	显示已启用SSD缓存的卷中的主机读取总数。读取与写入的比率越大、缓存的运行就越好。
写入	主机写入启用了SSD缓存的卷的总数。读取与写入的比率越大、缓存的运行就越好。
缓存命中次数	显示缓存命中数。
缓存命中率%	显示缓存命中百分比。此数字源自缓存命中/(读取+写入)。要实现有效的SSD缓存操作、缓存命中百分比应大于50%。
缓存分配%	显示分配的SSD缓存存储的百分比、以此控制器可用的SSD缓存存储的百分比表示、此百分比是从已分配的字节/可用字节派生的。
缓存利用率%	显示包含已启用卷中的数据的SSD缓存存储的百分比、以分配的SSD缓存存储的百分比表示。此数量表示SSD缓存的利用率或密度。源自已分配的字节/可用字节。
全部导出	将所有SSD缓存统计信息导出为CSV格式。导出的文件包含SSD缓存的所有可用统计信息(标称和详细)。

4. 单击\*取消\*关闭对话框。

在适用于vCenter的SANtricity存储插件中检查卷冗余

在技术支持的指导下或按照Recovery Guru的指示、您可以检查池或卷组中某个卷的冗余情况、以确定该卷上的数据是否一致。

如果池或卷组中的某个驱动器发生故障、则可以使用冗余数据快速重建替代驱动器上的信息。

#### 开始之前

- 池或卷组的状态必须为最佳。
- 池或卷组不能正在进行任何卷修改操作。
- 您可以检查除RAID 0以外的任何RAID级别的冗余、因为RAID 0没有数据冗余。(池仅配置为RAID 6。)



只有在Recovery Guru指示并在技术支持的指导下、才检查卷冗余。

#### 关于此任务

一次只能对一个池或卷组执行此检查。卷冗余检查将执行以下操作：

- 扫描RAID 3卷、RAID 5卷或RAID 6卷中的数据块、并检查每个块的冗余信息。(只能使用命令行界面将RAID 3分配给卷组。)
- 比较RAID 1镜像驱动器上的数据块。
- 如果控制器固件确定数据不一致、则返回冗余错误。



立即对同一个池或卷组运行冗余检查可能会出现发生原因 错误。要避免此问题、请等待一到两分钟、然后再对同一个池或卷组运行另一个冗余检查。

#### 步骤

1. 从管理页面中、选择具有池或卷组的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择菜单：不常见任务(检查卷冗余)。

此时将显示检查冗余对话框。

4. 选择要检查的卷、然后键入check以确认要执行此操作。
5. 单击\*检查\*。

此时将启动检查卷冗余操作。从对话框中的表顶部开始、按顺序扫描池或卷组中的卷。扫描每个卷时会执行以下操作：

- 此时将在卷表中选择此卷。
- 冗余检查的状态显示在状态列中。
- 如果遇到任何介质或奇偶校验错误、则此检查将停止、然后报告此错误。下表提供了有关冗余检查状态的详细信息：

## 字段详细信息

Status	Description
待定	这是第一个要扫描的卷、您尚未单击"开始"启动冗余检查。或者、正在对池或卷组中的其他卷执行冗余检查操作。
正在检查	卷正在进行冗余检查。
已通过	卷已通过冗余检查。在冗余信息中未检测到不一致。
失败	卷未通过冗余检查。在冗余信息中检测到不一致。
介质错误	驱动器介质有缺陷且无法读取。按照Recovery Guru中显示的说明进行操作。
奇偶校验错误	奇偶校验与给定部分数据的奇偶校验不同。奇偶校验错误可能很严重、并且发生原因 可能会导致数据永久丢失。

6. 检查池或卷组中的最后一个卷后、单击\*完成\*。

在适用于vCenter的SANtricity存储插件中删除池或卷组

您可以删除池或卷组以创建更多未分配容量、您可以根据应用程序存储需求对其进行重新配置。

开始之前

- 您必须已备份池或卷组中所有卷上的数据。
- 您必须已停止所有输入/输出(I/O)。
- 您必须卸载卷上的所有文件系统。
- 您必须已删除池或卷组中的任何镜像关系。
- 您必须已停止正在对池或卷组执行的任何卷复制操作。
- 池或卷组不得参与异步镜像操作。
- 卷组中的驱动器不能具有永久性预留。

步骤

1. 从管理页面中、选择具有池或卷组的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 从列表中选择池或卷组。

一次只能选择一个池或卷组。向下滚动列表以查看其他池或卷组。

4. 选择菜单：uncommon Tasks[Delete]并确认。

结果

系统将执行以下操作：

- 删除池或卷组中的所有数据。

- 删除与池或卷组关联的所有驱动器。
- 取消分配关联的驱动器、以便在新的或现有的池或卷组中重复使用这些驱动器。

在适用于vCenter的SANtricity存储插件中整合卷组的可用容量

使用整合可用容量选项整合选定卷组上的现有可用块区。通过执行此操作、您可以使用卷组中的最大可用容量创建更多卷。

开始之前

- 卷组必须至少包含一个可用容量区域。
- 卷组中的所有卷都必须处于联机状态并处于最佳状态。
- 不得正在执行卷修改操作、例如更改卷的区块大小。

关于此任务

操作开始后、您将无法取消。在整合操作期间、您的数据仍可访问。

您可以使用以下任一方法启动整合可用容量对话框：

- 如果至少为卷组检测到一个可用容量区域、则"通知"区域的"主页"页面上将显示"整合可用容量建议"。单击\*整合可用容量\*链接以启动对话框。
- 您还可以从"池和卷组"页面启动"整合可用容量"对话框、如以下任务所述。

有关可用容量区域的更多信息

可用容量区域是指删除卷或在创建卷期间未使用所有可用容量时可能产生的可用容量。在卷组中创建一个或多个可用容量区域的卷时、卷的容量将限制为该卷组中最大的可用容量区域。例如、如果一个卷组的可用容量总计为15 GiB、而最大可用容量区域为10 GiB、则可以创建的最大卷为10 GiB。

您可以整合卷组上的可用容量以提高写入性能。随着主机写入、修改和删除文件、卷组的可用容量将逐渐变得碎片化。最终、可用容量不会位于一个连续块中、而是分散在卷组中的小片段中。这会导致文件进一步碎片化、因为主机必须将新文件作为碎片写入、才能将其放入可用集群范围内。

通过将选定卷组上的可用容量整合在一起、您会发现、每当主机写入新文件时、文件系统性能都会提高。整合过程还有助于防止新文件在将来被碎片化。

步骤

1. 从管理页面中、选择具有卷组的存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择具有要整合的可用容量的卷组、然后选择菜单：不常见任务(整合卷组可用容量)。

此时将显示整合可用容量对话框。

4. 键入`consolidate`确认要执行此操作。
5. 单击\*整合\*。

结果

系统将开始将卷组的可用容量区域整合(碎片整理)为一个连续容量、以便执行后续的存储配置任务。

完成后

从导航边栏中、选择\*操作\*以查看整合可用容量操作的进度。此操作可能会很长，并且可能会影响系统性能。

在适用于vCenter的SANtricity存储插件中打开驱动器上的LED指示灯

您可以找到驱动器、以物理方式识别构成选定池、卷组或SSD缓存的所有驱动器。选定池、卷组或SSD缓存中的每个驱动器上都会亮起一个LED指示灯。

步骤

1. 从管理页面中，选择存储阵列。
2. 选择菜单：配置[配置池和卷组]。
3. 选择要查找的池、卷组或SSD缓存、然后单击菜单：更多(打开定位灯)。

此时将显示一个对话框、指示包含选定池、卷组或SSD缓存的驱动器上的指示灯已打开。

4. 成功找到驱动器后、单击\*关闭\*。

减少适用于vCenter的SANtricity存储插件中现有池或SSD缓存的容量

您可以删除驱动器以减少现有池或SSD缓存的容量。

删除驱动器后、池或SSD缓存中每个卷中的数据将重新分配给其余驱动器。删除的驱动器将变为未分配、其容量将成为存储阵列总可用容量的一部分。

关于此任务

删除容量时、请遵循以下准则：

- 要删除SSD缓存中的最后一个驱动器、必须先删除SSD缓存。
- 不能将池中的驱动器数量减少到少于11个驱动器。
- 一次最多可以删除12个驱动器。如果需要删除12个以上的驱动器、请重复执行操作步骤。
- 如果池或SSD缓存中没有足够的可用容量来容纳数据、则在将这些数据重新分配到池或SSD缓存中的其余驱动器时、您无法删除这些驱动器。

以下是潜在的性能影响：

- 从池或SSD缓存中删除驱动器可能会降低卷性能。
- 从池或SSD缓存中删除容量时、不会占用保留容量。但是、根据池或SSD缓存中剩余的驱动器数量、保留容量可能会减少。

以下是对支持安全的驱动器的影响：

- 如果删除最后一个不支持安全的驱动器、则池中保留所有支持安全的驱动器。在这种情况下、您可以选择为池启用安全性。
- 如果删除最后一个不支持数据保证(Data Assurance、DA)的驱动器、则池将保留所有支持DA的驱动器。
- 在池中创建的任何新卷都将支持DA。如果您希望现有卷支持DA、则需要先删除此卷、然后再重新创建此

卷。

#### 步骤

1. 从管理页面中，选择存储阵列。

选择菜单：配置[配置池和卷组]。

2. 选择池或SSD缓存、然后单击菜单：更多[删除容量]。

此时将显示删除容量对话框。

3. 在列表选择一个或多个驱动器。

在列表中选择或取消选择驱动器时、“选定总容量”字段将更新。此字段显示删除选定驱动器后产生的池或SSD缓存的总容量。

4. 单击\*删除\*、然后确认要删除这些驱动器。

#### 结果

池和卷组视图反映了池或SSD缓存容量新减少的情况。

在适用于vCenter的SANtricity存储插件中为池或卷组启用安全性

您可以为池或卷组启用驱动器安全性、以防止未经授权访问池或卷组中驱动器上的数据。

只有使用安全密钥配置的控制器才能对驱动器进行读写访问。

#### 开始之前

- 必须启用驱动器安全功能。
- 必须创建安全密钥。
- 池或卷组必须处于最佳状态。
- 池或卷组中的所有驱动器都必须是支持安全的驱动器。

#### 关于此任务

如果要使用驱动器安全性、请选择一个支持安全的池或卷组。池或卷组可以同时包含支持安全和不支持安全的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。

启用安全性后、只能通过删除池或卷组并擦除驱动器来删除它。

#### 步骤

1. 从管理页面中、选择具有池或卷组的存储阵列。

2. 选择菜单：配置[配置池和卷组]。

3. 选择要启用安全性的池或卷组、然后单击菜单：更多[启用安全性]。

此时将显示确认启用安全性对话框。

4. 确认要为选定池或卷组启用安全性、然后单击\*启用\*。

## 删除适用于vCenter的SANtricity存储插件

您可以从 vCenter Server 设备中删除此插件，并从应用程序主机中卸载此插件 Web 服务器。

以下是两个不同的步骤，您可以按任意顺序执行。但是，如果您选择在注销插件之前从应用程序主机中删除插件 Web 服务器，则注册脚本将在此过程中被删除，并且无法使用方法 1 取消注册。

### 从 vCenter Server 设备取消注册此插件

要从 vCenter Server 设备取消注册插件，请选择以下方法之一：

- [\[方法1: 执行注册脚本\]](#)
- [方法2: 使用vCenter Server移动页面](#)

#### 方法1: 执行注册脚本

1. 通过命令行打开提示符并导航到以下目录：

```
` <install directory>\vCenter-register\bin`
```

2. 执行 vCenter-register.bat 文件：

```
vcenter-register.bat ^
```

```
` 操作未注册插件 ^`
```

```
` -vcenterHostname <vCenter FQDN> ^`
```

```
` 用户名 < 管理员用户名 > ^`
```

3. 验证脚本是否成功。

这些日志将保存到 `%install\_dir%/log/vc-registration.log` 中。

#### 方法2: 使用vCenter Server移动页面

1. 打开 Web 浏览器并输入以下 URL：

```
https://<FQDN[ vCenter Server 的数量 >/mob
```

2. 使用管理员凭据登录。
3. 查找 extsionManager 的属性名称，然后单击与该属性关联的链接。
4. 单击 \* 更多 \*... 展开属性列表 链接。
5. 验证扩展名 plugin.netapp.eseries 是否位于列表中。
6. 如果存在，请单击 Method UnregisterExtension。
7. 在对话框中输入值 plugin.netapp.eseries，然后单击 \* 调用方法 \*。
8. 关闭对话框并刷新 Web 浏览器。

## 9. 验证 `plugin.netapp.eseries` 扩展名是否不在列表中。



此操作步骤会从 vCenter Server 设备中取消注册此插件，但不会从服务器中删除插件软件包文件。要删除软件包文件，请使用SSH访问vCenter Server设备并导航到以下目录： ```etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenace/vsphere-serenity`。然后删除与此插件关联的目录。

### 从应用程序主机中删除插件 **Web** 服务器

要从应用程序主机中删除插件软件，请执行以下步骤：

1. 在应用程序服务器中，导航到 \* 控制面板 \*。
2. 转至 \* 应用程序和功能 \*，然后选择 \* 适用于 vCenter 的 SANtricity 存储插件 \*。
3. 单击 \* 卸载 / 更改 \*。

此时将打开确认对话框。

4. 单击 \* 卸载 \*。

卸载完成后，将显示一条确认消息。

5. 单击 \* 完成 \*。

## SANtricity Storage Plugin for vCenter 的常见问题解答

如果您只是想快速了解问题解答，此常见问题解答会很有帮助。

### 导入了哪些设置？

导入设置功能是一个批处理操作、可将配置从一个存储阵列加载到多个存储阵列。

在此操作期间导入的设置取决于源存储阵列在System Manager中的配置方式。可以将以下设置导入到多个存储阵列：

- 电子邮件警报-设置包括邮件服务器地址和警报收件人的电子邮件地址。
- 系统日志警报-设置包括系统日志服务器地址和UDP端口。
- \* SNMP警报\*-设置包括SNMP服务器的社区名称和IP地址。
- \* AutoSupport \*—设置包括不同的功能(基本AutoSupport、AutoSupport OnDemand和远程诊断)、维护窗口、交付方法、和派单计划。
- 目录服务—配置包括LDAP (轻型目录访问协议)服务器的域名和URL、以及LDAP服务器用户组与存储阵列预定义角色的映射。
- 存储配置—配置包括卷(仅厚卷和非存储库卷)、卷组、池和热备用驱动器分配。
- 系统设置-配置包括卷的介质扫描设置、控制器的SSD缓存以及自动负载平衡(不包括主机连接报告)。

### 为什么我看不到所有存储阵列？

在导入设置操作期间、某些存储阵列可能在目标选择对话框中不可用。

存储阵列可能不会显示、原因如下：

- 固件版本低于8.50。
- 存储阵列已脱机。
- 系统无法与该阵列进行通信(例如、该阵列存在证书、密码或网络问题)。

为什么这些卷不与工作负载关联？

如果卷是使用命令行界面(CLI)创建的、或者已从其他存储阵列迁移(导入/导出)、则卷不会与工作负载关联。

选定工作负载对卷创建有何影响？

在创建卷期间、系统会提示您提供有关工作负载使用情况的信息。系统会使用此信息为您创建最佳卷配置、您可以根据需要对其进行编辑。或者、您也可以卷创建序列中跳过此步骤。

工作负载是指支持应用程序的存储对象。您可以为每个应用程序定义一个或多个工作负载或实例。对于某些应用程序、系统会将工作负载配置为包含具有类似底层卷特征的卷。这些卷特征会根据工作负载支持的应用程序类型进行优化。例如、如果您创建了一个支持Microsoft SQL Server应用程序的工作负载、然后为该工作负载创建了卷、则底层卷特征将进行优化以支持Microsoft SQL Server。

- 应用程序专用—当您使用应用程序专用工作负载创建卷时、系统可能会建议优化卷配置、以最大程度地减少应用程序工作负载I/O与应用程序实例中的其他流量之间的争用。对于为以下应用程序类型创建的工作负载、系统会自动建议并优化卷特征、例如I/O类型、区块大小、控制器所有权以及读写缓存。
  - Microsoft SQL Server
  - Microsoft Exchange Server
  - 视频监控应用程序
  - VMware ESXi (适用于要与虚拟机文件系统结合使用的卷)

您可以使用添加/编辑卷对话框查看建议的卷配置以及编辑、添加或删除系统建议的卷和特征。

- 其他(或不支持特定卷创建的应用程序)- 其他工作负载使用的卷配置、您必须在创建与特定应用程序无关的工作负载时手动指定、或者如果您要在存储阵列上使用的应用程序没有内置优化功能、则必须手动指定。您必须使用添加/编辑卷对话框手动指定卷配置。

为什么我看不到所有卷、主机或主机集群？

具有已启用DA的基础卷的Snapshot卷不能分配给不支持数据保证(Data Assurance、DA)的主机。您必须先基础卷上禁用DA、然后才能将快照卷分配给不支持DA的主机。

对于要将快照卷分配到的主机、请考虑以下准则：

- 如果主机通过不支持DA的I/O接口连接到存储阵列、则该主机将不支持DA。
- 如果主机集群至少有一个主机成员不支持DA、则此主机集群不支持DA。



您不能在与快照(一致性组、快照组、快照映像和快照卷)、卷副本、和镜像。必须先删除所有关联的预留容量和快照对象、然后才能在基础卷上禁用DA。

为什么无法删除选定工作负载？

此工作负载由一组使用命令行界面(CLI)创建或从其他存储阵列迁移(导入/导出)的卷组成。因此、此工作负载中的卷不会与特定于应用程序的工作负载关联、因此无法删除此工作负载。

应用程序特定的工作负载如何帮助我管理存储阵列？

应用程序特定工作负载的卷特征决定了该工作负载如何与存储阵列的组件进行交互、并有助于确定给定配置下环境的性能。

应用程序是指SQL Server或Exchange等软件。您可以定义一个或多个工作负载来支持每个应用程序。对于某些应用程序、系统会自动建议一种可优化存储的卷配置。卷配置包括I/O类型、区块大小、控制器所有权以及读写缓存等特征。

要识别扩展的容量、我需要执行哪些操作？

如果增加卷的容量、则主机可能无法立即识别卷容量的增加。

大多数操作系统都会识别扩展后的卷容量、并在启动卷扩展后自动进行扩展。但是、有些可能不会。如果操作系统无法自动识别扩展的卷容量、则可能需要执行磁盘重新扫描或重新启动。

扩展卷容量后、必须手动增加文件系统大小以匹配。如何执行此操作取决于所使用的文件系统。

有关更多详细信息、请参见主机操作系统文档。

稍后要在何时使用分配主机选项？

如果要加快创建卷的过程、可以跳过主机分配步骤、使新创建的卷脱机初始化。

必须初始化新创建的卷。系统可以使用以下两种模式之一对其进行初始化：即即时可用格式(Immediate Available Format、IAF)后台初始化过程或脱机过程。

将卷映射到主机时、它会强制该组中所有初始化的卷过渡到后台初始化。此后台初始化过程允许并发主机I/O、这有时可能非常耗时。

如果未映射卷组中的任何卷、则会执行脱机初始化。脱机过程比后台进程快得多。

关于主机块大小要求、我需要了解哪些信息？

对于EF300和EF600系统、可以将卷设置为支持512字节或4KiB块大小(也称为"扇区大小")。您必须在创建卷期间设置正确的值。如果可能、系统会建议适当的默认值。

在设置卷块大小之前、请阅读以下限制和准则。

- 某些操作系统和虚拟机(尤其是VMware、目前)需要512字节的块大小、并且不支持4KiB、因此请确保在创建卷之前了解主机要求。通常、可以通过将卷设置为显示4KiB块大小来实现最佳性能；但是、请确保主机允许4KiB(或"4Kn")块。
- 为池或卷组选择的驱动器类型还决定了支持的卷块大小、如下所示：
  - 如果使用写入512字节块的驱动器创建卷组、则只能创建包含512字节块的卷。
  - 如果使用写入4KiB块的驱动器创建卷组、则可以创建包含512字节或4KiB块的卷。

- 如果阵列具有iSCSI主机接口卡、则所有卷都将限制为512字节的块(无论卷组块大小如何)。这是由于实施了特定的硬件造成的。
- 设置块大小后、您将无法更改块大小。如果需要更改块大小、则必须删除卷并重新创建它。

### 为什么需要创建主机集群?

如果要使两个或更多主机共享对同一组卷的访问、则需要创建主机集群。通常、各个主机都安装了集群软件来协调卷访问。

### 如何知道哪种主机操作系统类型正确?

主机操作系统类型字段包含主机的操作系统。您可以从下拉列表中选择建议的主机类型。

下拉列表中显示的主机类型取决于存储阵列型号和固件版本。最新版本会首先显示最常见的选项、最有可能是最合适的选项。此列表中的显示并不表示完全支持此选项。



有关主机支持的详细信息、请参见 "[NetApp 互操作性表工具](#)"。

列表中可能会显示以下某些主机类型:

主机操作系统类型	操作系统(OS)和多路径驱动程序
Linux DM-MP (内核3.10或更高版本)	支持使用设备映射程序多路径故障转移解决方案和3.10或更高版本内核的Linux操作系统。
VMware ESXi	支持使用VMware内置存储阵列类型策略模块sap_alUA运行原生 多路径插件(NMP)架构的VMware ESXi操作系统。
Windows (集群或非集群)	支持未运行ATTO多路径驱动程序的Windows集群或非集群配置。
ATTO集群(所有操作系统)	支持使用ATTO Technology、 Inc.多路径驱动程序的所有集群配置。
Linux (Veritas DMP)	支持使用Veritas DMP多路径解决方案 的Linux操作系统。
Linux (ATTO)	支持使用ATTO Technology、 Inc.多路径驱动程序的Linux操作系统。
Mac OS	支持使用ATTO Technology、 Inc.多路径驱动程序的Mac OS版本。
Windows (ATTO)	支持使用ATTO Technology、 Inc.多路径驱动程序的Windows操作系统。
IBM服务	支持IBM SAN卷控制器配置。
出厂默认值	为存储阵列的初始启动预留。如果您的主机操作系统类型设置为出厂默认值、请将其更改为与所连接主机上运行的主机操作系统和多路径驱动程序匹配。
Linux DM-MP (Kernal 3.9或更早版本)	支持使用具有3.9或更早内核的设备映射程序多路径故障转移解决方案 的Linux操作系统。

主机操作系统类型	操作系统(OS)和多路径驱动程序
窗口集群(已弃用)	如果主机操作系统类型设置为此值、请改用Windows (集群或非集群)设置。

### 如何将主机端口与主机匹配?

如果要手动创建主机、则必须首先使用主机上可用的相应主机总线适配器(HBA)实用程序来确定与主机中安装的每个HBA关联的主机端口标识符。

获得此信息后、请从创建主机对话框中提供的列表中选择已登录到存储阵列的主机端口标识符。



确保为要创建的主机选择适当的主机端口标识符。如果关联的主机端口标识符不正确、则可能会发生原因 从另一台主机意外访问此数据。

### 默认集群是什么?

默认集群是一个系统定义的实体、它允许登录到存储阵列的任何未关联主机端口标识符访问分配给默认集群的卷。

未关联的主机端口标识符是指与特定主机没有逻辑关联、但实际安装在主机中并登录到存储阵列的主机端口。



如果您希望主机对存储阵列中的某些卷具有特定访问权限、则不能使用默认集群。而是必须将主机端口标识符与其对应的主机相关联。此任务可以在创建主机操作期间手动完成。然后、将卷分配给单个主机或主机集群。

只有在外部存储环境有利于允许所有主机以及连接到存储阵列的所有已登录主机端口标识符都能够访问所有卷的特殊情况下、才应使用默认集群(完全访问模式)而不是专门使存储阵列或用户界面知道这些主机。

最初、您只能通过命令行界面(CLI)将卷分配给默认集群。但是、在将至少一个卷分配给默认集群后、此实体(称为默认集群)将显示在用户界面中、您可以在此界面中管理此实体。

### 什么是冗余检查?

冗余检查可确定池或卷组中卷上的数据是否一致。如果池或卷组中的某个驱动器发生故障、则可以使用冗余数据快速重建替代驱动器上的信息。

一次只能对一个池或卷组执行此检查。卷冗余检查将执行以下操作:

- 扫描RAID 3卷、RAID 5卷或RAID 6卷中的数据块、然后检查每个块的冗余信息。(只能使用命令行界面将RAID 3分配给卷组。)
- 比较RAID 1镜像驱动器上的数据块。
- 如果控制器固件确定数据不一致、则返回冗余错误。



立即对同一个池或卷组运行冗余检查可能会出现发生原因 错误。要避免此问题、请等待一到两分钟、然后再对同一个池或卷组运行另一个冗余检查。

什么是保留容量？

保留容量是指池中为支持潜在驱动器故障而预留的容量(驱动器数量)。

创建池时、系统会根据池中的驱动器数量自动预留默认保留容量。

池会在重建期间使用保留容量、而卷组则会出于相同目的使用热备用驱动器。与热备用驱动器相比、保留容量方法有所改进、因为它可以更快地进行重建。对于热备用驱动器、保留容量会分布在池中的多个驱动器上、而不是分布在一个驱动器上、因此您不会受到一个驱动器的速度或可用性的限制。

哪种RAID级别最适合我的应用程序？

要最大程度地提高卷组的性能、必须选择适当的RAID级别。

您可以通过了解正在访问卷组的应用程序的读写百分比来确定适当的RAID级别。使用性能页面可获取这些百分比。

#### RAID级别和应用程序性能

RAID依靠一系列称为级别的配置来确定如何从驱动器写入和检索用户和冗余数据。每个RAID级别提供不同的性能功能。由于RAID 5和RAID 6配置具有出色的读取性能、读取百分比较高的应用程序在使用RAID 5卷或RAID 6卷时性能良好。

读取百分比较低(写入密集型)的应用程序在RAID 5卷或RAID 6卷上的性能较差。性能下降是由于控制器将数据和冗余数据写入RAID 5卷组或RAID 6卷组中的驱动器的方式造成的。

根据以下信息选择RAID级别。

### RAID 0

问题描述：

- 非冗余条带化模式。
- RAID 0可在卷组中的所有驱动器之间对数据进行条带化。

数据保护功能：

- 不建议使用RAID 0来满足高可用性需求。RAID 0更适合非关键数据。
- 如果卷组中的一个驱动器发生故障、则所有关联卷都会发生故障、并且所有数据都将丢失。

驱动器编号要求：

- RAID级别0至少需要一个驱动器。
- RAID 0卷组可以包含30个以上的驱动器。
- 您可以创建一个包含存储阵列中所有驱动器的卷组。

### RAID 1或RAID 10

问题描述：

- 条带化/镜像模式。

工作原理：

- RAID 1使用磁盘镜像将数据同时写入两个重复磁盘。
- RAID 10使用驱动器条带化功能在一组镜像驱动器对之间条带化数据。

数据保护功能：

- RAID 1和RAID 10可提供高性能和最佳数据可用性。
- RAID 1和RAID 10使用驱动器镜像从一个驱动器精确复制到另一个驱动器。
- 如果驱动器对中的一个驱动器发生故障、存储阵列可以立即切换到另一个驱动器、而不会丢失任何数据或服务。
- 单个驱动器故障会导致关联卷降级。镜像驱动器允许访问数据。
- 卷组中的驱动器对故障会导致所有关联卷出现故障、并且可能会发生数据丢失。

驱动器编号要求：

- RAID 1至少需要两个驱动器：一个驱动器用于用户数据、一个驱动器用于镜像数据。
- 如果选择四个或更多驱动器、则会在卷组中自动配置RAID 10：两个驱动器用于用户数据、两个驱动器用于镜像数据。
- 卷组中的驱动器数量必须为偶数。如果驱动器数量不是偶数、并且还有一些未分配的驱动器、请转到\*池和卷组\*向卷组添加其他驱动器、然后重试此操作。
- RAID 1和RAID 10卷组可以包含30个以上的驱动器。可以创建一个包含存储阵列中所有驱动器的卷组。

## RAID 5

问题描述：

- 高I/O模式。

工作原理：

- 用户数据和冗余信息(奇偶校验)在驱动器之间进行条带化。
- 一个驱动器的等效容量用于提供冗余信息。

数据保护功能

- 如果RAID 5卷组中的一个驱动器发生故障、则所有关联卷都会降级。冗余信息允许仍访问数据。
- 如果RAID 5卷组中的两个或更多驱动器发生故障、则所有关联卷都会发生故障、并且所有数据都将丢失。

驱动器编号要求：

- 卷组中必须至少有三个驱动器。
- 通常、卷组中最多只能包含30个驱动器。

## RAID 6

问题描述：

- 高I/O模式。

工作原理：

- 用户数据和冗余信息(双奇偶校验)在驱动器之间进行条带化。
- 两个驱动器的等效容量用于提供冗余信息。

数据保护功能：

- 如果RAID 6卷组中的一个或两个驱动器发生故障、则所有关联卷都会降级、但冗余信息仍允许访问数据。
- 如果RAID 6卷组中的三个或更多驱动器发生故障、则所有关联卷都会发生故障、并且所有数据都将丢失。

驱动器编号要求：

- 卷组中必须至少有五个驱动器。
- 通常、卷组中最多只能包含30个驱动器。



您不能更改池的RAID级别。用户界面会自动将池配置为RAID 6。

#### RAID级别和数据保护

RAID 1、RAID 5和RAID 6向驱动器介质写入冗余数据以实现容错。冗余数据可以是数据的副本(镜像)、也可以是从数据派生的错误更正代码。如果驱动器发生故障、您可以使用冗余数据快速重建替代驱动器上的信息。

您可以在一个卷组中配置一个RAID级别。该卷组的所有冗余数据都存储在该卷组中。卷组的容量等于成员驱动器的聚合容量减去为冗余数据预留的容量。冗余所需的容量取决于使用的RAID级别。

为什么某些驱动器不显示？

在添加容量对话框中、并非所有驱动器都可用于向现有池或卷组添加容量。

驱动器不符合条件的原因如下：

- 驱动器必须已取消分配、并且未启用安全保护。驱动器已属于另一个池、另一个卷组或配置为热备用磁盘不符合条件。如果某个驱动器未分配但已启用安全保护、则必须手动擦除该驱动器才能使其符合条件。
- 处于非最佳状态的驱动器不符合条件。
- 如果驱动器容量太小、则不符合条件。
- 驱动器介质类型必须在池或卷组中匹配。您不能混用以下内容：
  - 采用固态硬盘(SSD)的硬盘驱动器(HDD)
  - 采用SAS驱动器的NVMe
  - 卷块大小为512字节和4 KiB的驱动器
- 如果池或卷组包含所有支持安全的驱动器、则不会列出不支持安全的驱动器。
- 如果池或卷组包含所有联邦信息处理标准(FIPS)驱动器、则不会列出非FIPS驱动器。
- 如果池或卷组包含支持所有数据保证(DA)的驱动器、并且池或卷组中至少有一个已启用DA的卷、则不支持DA的驱动器将不符合条件、因此无法将其添加到该池或卷组。但是、如果池或卷组中没有启用了DA的卷、则可以将不支持DA的驱动器添加到该池或卷组中。如果决定混用这些驱动器、请记住、您不能创建任

何已启用DA的卷。



可以通过添加新驱动器或删除池或卷组来增加存储阵列中的容量。

为什么我不能增加我的保留容量？

如果已在所有可用容量上创建卷、则可能无法增加保留容量。

保留容量是指池中为支持潜在驱动器故障而预留的容量(驱动器数量)。创建池时、系统会根据池中的驱动器数量自动预留默认保留容量。如果已在所有可用容量上创建卷、则在不通过添加驱动器或删除卷向池添加容量的情况下、无法增加保留容量。

您可以从池和卷组更改保留容量。选择要编辑的池。单击\*查看/编辑设置\*、然后选择\*设置\*选项卡。



保留容量指定为多个驱动器、即使实际保留容量分布在池中的驱动器之间也是如此。

什么是数据保证？

数据保证(Data Assurance、DA)实施了T10保护信息(Protection Information、PI)标准、该标准可通过检查并更正正在I/O路径上传输数据时可能发生的错误来提高数据完整性。

通常情况下、使用数据保证功能将检查控制器和驱动器之间I/O路径的部分。DA功能在池和卷组级别提供。

启用此功能后、存储阵列会向卷中的每个数据块附加错误检查代码(也称为循环冗余检查或CRC)。移动数据块后、存储阵列会使用这些CRC代码来确定传输期间是否发生任何错误。可能损坏的数据既不会写入磁盘、也不会返回到主机。如果要使用DA功能、请在创建新卷时选择一个支持DA的池或卷组(在Pool and volume group candidates表中的\* DA\*旁边查找\*是\*)。

请确保使用支持DA的I/O接口将这些启用了DA的卷分配给主机。支持DA的I/O接口包括光纤通道、SAS、基于TCP/IP的iSCSI、NVMe/FC、NVMe/IB、基于InfiniBand的NVMe/RoCE和iSER(适用于RDMA/IB的iSCSI扩展)。基于InfiniBand的SRP不支持DA。

什么是FDE/Fips安全性？

FDE/Fips安全性是指在写入期间对数据进行加密的安全驱动器、以及在读取期间使用唯一加密密钥对数据进行解密的驱动器。

这些支持安全的驱动器可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。支持安全的驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。FIPS驱动器已通过认证测试。



对于需要FIPS支持的卷、请仅使用FIPS驱动器。在卷组或池中混用FIPS和FDE驱动器将导致所有驱动器被视为FDE驱动器。此外、FDE驱动器不能添加到纯FIPS卷组或池中或用作备用磁盘。

什么是安全功能(驱动器安全)？

驱动器安全性是一项功能、可防止在从存储阵列中删除启用了安全功能的驱动器上的数据时未经授权进行访问。

这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。

如何查看和解释所有SSD缓存统计信息？

您可以查看SSD缓存的标称统计信息和详细统计信息。

标称统计信息是详细统计信息的一部分。只有在将所有SSD统计信息导出到.csv文件时、才能查看详细统计信息。在查看和解释统计信息时、请记住、某些解释是通过结合统计信息得出的。

标称统计信息

要查看SSD缓存统计信息、请转到\*管理\*页面。选择菜单：配置[配置池和卷组]。选择要查看统计信息的SSD缓存、然后选择菜单：更多(查看统计信息)。标称统计信息显示在"查看SSD缓存统计信息"对话框中。



EF600或EF300存储系统不支持此功能。

此列表包含标称统计信息、这些统计信息是详细统计信息的一部分。

详细统计信息

详细统计信息包括名义统计信息和其他统计信息。这些附加统计信息会与标称统计信息一起保存、但与标称统计信息不同、它们不会显示在"查看SSD缓存统计信息"对话框中。只有在将统计信息导出到.csv文件后、才能查看详细统计信息。

详细统计信息列在标称统计信息之后。

什么是磁盘架丢失保护和抽屉丢失保护？

磁盘架丢失保护和抽屉丢失保护是池和卷组的属性、可用于在单个磁盘架或抽屉发生故障时保持数据访问。

磁盘架丢失保护

磁盘架是指包含驱动器或驱动器和控制器的机箱。磁盘架丢失保护功能可确保在与单个驱动器磁盘架完全失去通信时能够访问池或卷组中卷上的数据。完全失去通信的一个示例可能是驱动器架断电或两个I/O模块(IOM)均发生故障。



如果池或卷组中的驱动器已发生故障、则无法保证磁盘架丢失保护。在这种情况下、如果无法访问某个驱动器架以及池或卷组中的另一个驱动器、则会导致数据丢失。

磁盘架丢失保护的标准取决于保护方法、如下表所述。

级别	磁盘架丢失保护的标准	所需的最小磁盘架数
池	该池必须包含至少来自五个磁盘架的驱动器、并且每个磁盘架中的驱动器数量必须相等。磁盘架丢失保护不适用于大容量磁盘架；如果您的系统包含大容量磁盘架、请参阅"抽屉丢失保护"。	5.
RAID 6	卷组在一个抽屉中包含的驱动器不超过两个。	3.
RAID 3或RAID 5	卷组中的每个驱动器都位于一个单独的磁盘架中。	3.

级别	磁盘架丢失保护的标准	所需的最小磁盘架数
RAID 1	RAID 1对中的每个驱动器都必须位于一个单独的磁盘架中。	2.
RAID 0	无法实现磁盘架丢失保护。	不适用

#### 抽盒丢失保护

抽盒是拉出以访问驱动器的磁盘架的一个隔室。只有大容量磁盘架才具有抽盒。抽盒丢失保护功能可确保在与单个抽盒完全失去通信时能够访问池或卷组中卷上的数据。完全失去通信的一个示例可能是抽盒断电或抽盒内的内部组件发生故障。



如果池或卷组中的驱动器已发生故障、则不保证提供抽盒丢失保护。在这种情况下、如果无法访问某个抽盒(以及池或卷组中的另一个驱动器)、则会导致数据丢失。

抽盒丢失保护的标准取决于保护方法、如下表所述：

级别	抽盒丢失保护的标准	所需的最小抽盒数量
池	候选池必须包含所有抽盒中的驱动器、并且每个抽盒中的驱动器数量必须相等。池中必须至少包含五个抽盒中的驱动器、并且每个抽盒中的驱动器数量必须相等。如果池包含15、20、25、30、35、40、45、50、55或60个驱动器。首次创建后、可以将增量以5的倍数添加到池中。	5.
RAID 6	卷组在一个抽盒中包含的驱动器不超过两个。	3.
RAID 3或5	卷组中的每个驱动器都位于一个单独的抽盒中	3.
RAID 1	镜像对中的每个驱动器都必须位于一个单独的抽盒中。	2.
RAID 0	无法实现抽盒丢失保护。	不适用

#### 如何维护磁盘架和抽盒丢失保护？

要为池或卷组维护磁盘架和抽盒丢失保护、请使用下表中指定的标准。

级别	磁盘架/抽盒丢失保护的标准	所需的最小磁盘架/抽盒数
池	对于磁盘架、池中一个磁盘架中的驱动器不能超过两个。对于抽盒、池中每个抽盒中必须包含相同数量的驱动器。	6个用于磁盘架5个用于抽盒
RAID 6	卷组在一个磁盘架或抽盒中包含的驱动器不超过两个。	3.

级别	磁盘架/抽屉丢失保护的标准	所需的最小磁盘架/抽屉数
RAID 3或RAID 5	卷组中的每个驱动器都位于一个单独的磁盘架或抽屉中。	3.
RAID 1	镜像对中的每个驱动器都必须位于单独的磁盘架或抽屉中。	2.
RAID 0	无法实现磁盘架/抽屉丢失保护。	不适用



如果池或卷组中的驱动器已发生故障、则不会保持磁盘架/抽屉丢失保护。在这种情况下、如果无法访问某个驱动器架或抽盒、进而无法访问池或卷组中的另一个驱动器、则会导致数据丢失。

### 什么是池的优化容量？

如果未分配一部分容量、SSD驱动器的使用寿命将会延长、并且最大写入性能也会提高。

对于与池关联的驱动器、未分配的容量由池的保留容量、可用容量(卷未使用的容量)以及作为额外优化容量而预留的部分可用容量组成。额外的优化容量可通过减少可用容量来确保最低的优化容量级别、因此不可用于创建卷。

创建池时、系统会生成一个建议的优化容量、以便在性能、驱动器使用寿命和可用容量之间实现平衡。通过位于Pool Settings对话框中的Additional Optimization Capacity滑块、可以调整池的优化容量。调整滑块可以提高性能和驱动器磨损寿命、而不会影响可用容量、也不会影响性能和驱动器磨损寿命。



附加优化容量滑块仅适用于EF600和EF300存储系统。

### 卷组的优化容量是多少？

如果未分配一部分容量、SSD驱动器的使用寿命将会延长、并且最大写入性能也会提高。

对于与卷组关联的驱动器、未分配的容量由卷组的可用容量(卷未使用的容量)以及作为优化容量预留的部分可用容量组成。额外的优化容量可通过减少可用容量来确保最低的优化容量级别、因此不可用于创建卷。

创建卷组时、系统会生成一个建议的优化容量、以便在性能、驱动器使用寿命和可用容量之间取得平衡。通过"卷组设置"对话框中的"其他优化容量"滑块、可以调整卷组的优化容量。调整滑块可以提高性能和驱动器磨损寿命、而不会影响可用容量、也不会影响性能和驱动器磨损寿命。



其他优化容量滑块仅适用于EF600和EF300存储系统。

### 什么是资源配置功能？

资源配置是EF300和EF600存储阵列中提供的一项功能、可在不执行后台初始化过程的情况下立即使用卷。

资源配置卷是SSD卷组或池中的厚卷、在创建卷时会分配(分配给卷)驱动器容量、但会取消分配(取消映射)驱动器块。相比之下、在传统厚卷中、所有驱动器块都会在后台卷初始化操作期间映射或分配、以便初始化数据保证保护信息字段并使每个RAID条带中的数据和RAID奇偶校验保持一致。对于资源配置的卷、不会进行有时间限制的后台初始化。而是在首次写入条带中的卷块时初始化每个RAID条带。

只有SSD卷组和池支持资源配置的卷、其中组或池中的所有驱动器都支持NVMe已取消分配或未写入逻辑块错误启用(DULBE)错误恢复功能。创建资源配置的卷时、分配给该卷的所有驱动器块都会进行取消分配(未映射)。此外、主机还可以使用NVMe Dataset Management命令取消分配卷中的逻辑块。取消分配块可以延长SSD的使用

寿命并提高最大写入性能。性能提升因驱动器型号和容量而异。

关于资源配置卷功能、我需要了解哪些信息？

资源配置是EF300和EF600存储阵列中提供的一项功能、可在不执行后台初始化过程的情况下立即使用卷。



此时、资源配置功能不可用。在某些视图中、组件可能会报告为具有资源配置功能、但创建资源配置卷的功能已被禁用、直到可以在将来的更新中重新启用为止。

#### 资源配置的卷

资源配置卷是SSD卷组或池中的厚卷、在创建卷时会分配(分配给卷)驱动器容量、但会取消分配(取消映射)驱动器块。相比之下、在传统厚卷中、所有驱动器块都会在后台卷初始化操作期间映射或分配、以便初始化数据保证保护信息字段并使每个RAID条带中的数据和RAID奇偶校验保持一致。对于资源配置的卷、不会进行有时间限制的后台初始化。而是在首次写入条带中的卷块时初始化每个RAID条带。

只有SSD卷组和池支持资源配置的卷、其中组或池中的所有驱动器都支持NVMe已取消分配或未写入逻辑块错误启用(DULBE)"错误恢复功能。创建资源配置的卷时、分配给该卷的所有驱动器块都会进行取消分配(未映射)。此外、主机还可以使用NVMe Dataset Management命令取消分配卷中的逻辑块。取消分配块可以延长SSD的使用寿命并提高最大写入性能。性能提升因驱动器型号和容量而异。

#### 启用和禁用此功能

在驱动器支持DULBE"的系统上、默认情况下会启用资源配置。您可以从"池和卷组"中禁用此默认设置。禁用资源配置是对现有卷执行的一项永久操作、无法反转(即、您无法为这些卷组和池重新启用资源配置)。

但是、如果要为您创建的任何新卷重新启用资源配置、则可以从菜单：Settings[系统]执行此操作。请注意、在重新启用资源配置时、仅会影响新创建的卷组和池。任何现有卷组和池将保持不变。如果需要、您还可以从菜单：Settings[系统]再次禁用资源配置。

#### 内部安全密钥与外部安全密钥管理有何区别？

在实施驱动器安全功能时、当从存储阵列中删除启用了安全保护的驱动器时、您可以使用内部安全密钥或外部安全密钥锁定数据。

安全密钥是一个字符串、在存储阵列中启用了安全保护的驱动器和控制器之间共享。内部密钥会保留在控制器的永久性内存上。外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上维护。

#### 在创建安全密钥之前、我需要了解哪些信息？

安全密钥由存储阵列中的控制器和启用了安全保护的驱动器共享。如果从存储阵列中删除了启用了安全保护的驱动器、则安全密钥可防止数据遭受未经授权的访问。

您可以使用以下方法之一创建和管理安全密钥：

- 控制器永久性内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

## 内部密钥管理

内部密钥会在控制器永久性内存上的不可访问位置进行维护和“隐藏”。在创建内部安全密钥之前、必须执行以下操作：

1. 在存储阵列中安装支持安全保护的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
2. 确保已启用驱动器安全功能。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。

然后、您可以创建内部安全密钥、其中包括定义标识符和密码短语。标识符是与安全密钥关联的字符串、存储在控制器以及与该密钥关联的所有驱动器上。密码短语用于对安全密钥进行加密、以用于备份。完成后、安全密钥将存储在控制器上不可访问的位置。然后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

## 外部密钥管理

外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上维护。在创建外部安全密钥之前、必须执行以下操作：

1. 在存储阵列中安装支持安全保护的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
2. 确保已启用驱动器安全功能。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明
3. 获取签名的客户端证书文件。客户端证书用于验证存储阵列的控制器、以便密钥管理服务器可以信任其KMIP请求。
  - a. 首先、您需要完成并下载客户端证书签名请求(CSR)。转到菜单：设置[证书>密钥管理>完成CSR]。
  - b. 接下来、您需要从密钥管理服务器信任的CA请求签名客户端证书。(您也可以使用下载的CSR文件从密钥管理服务器创建和下载客户端证书。)
  - c. 拥有客户端证书文件后、将该文件复制到要访问System Manager的主机。
4. 从密钥管理服务器检索证书文件、然后将该文件复制到要访问System Manager的主机。密钥管理服务器证书用于验证密钥管理服务器、以便存储阵列可以信任其IP地址。您可以对密钥管理服务器使用根证书、中间证书或服务器证书。

然后、您可以创建外部密钥、其中包括定义密钥管理服务器的IP地址以及用于KMIP通信的端口号。在此过程中、您还可以加载证书文件。完成后、系统将使用您输入的凭据连接到密钥管理服务器。然后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

## 为什么需要定义密码短语？

密码短语用于对存储在本地管理客户端上的安全密钥文件进行加密和解密。如果没有密码短语、则无法对安全密钥进行解密、并使用此安全密钥从启用了安全功能的驱动器中解锁数据、如果此驱动器重新安装在另一个存储阵列中。

# 传统解决方案

## 云连接器

## SANtricity® Cloud Connector 概述

SANtricity 云连接器是一款基于主机的 Linux 应用程序，可用于对 S3 投诉帐户（例如 Amazon Simple Storage Service 和 NetApp StorageGRID）和 NetApp AltaVault 设备执行基于块和基于文件的完整备份和恢复。

SANtricity 云连接器可安装在 RedHat 和 SUSE Linux 平台上，它是一个打包的解决方案（.bin 文件）。安装 SANtricity 云连接器后，您可以对应用程序进行配置，以便将 E 系列卷的备份和还原作业备份到 AltaVault 设备或现有 Amazon S3 或 StorageGRID 帐户。通过 SANtricity 云连接器执行的所有作业都使用基于 REST 的 API。



SANtricity 云连接器工具已弃用、不再可供下载。

### 注意事项

在使用这些过程时，请注意：

- 这些过程中所述的配置和备份 / 还原作业适用于 SANtricity 云连接器的图形用户界面版本。
- 这些过程不会介绍 SANtricity 云连接器应用程序的 REST API 工作流。对于有经验的开发人员，API 文档提供了每个 SANtricity Cloud Connector 操作的端点。可通过浏览器导航到 <http://<hostname.domain>:<port>/docs> 来访问 API 文档。

### 备份类型

SANtricity 云连接器提供两种类型的备份：基于映像的备份和基于文件的备份。

- \* 基于映像的备份 \*

基于映像的备份会从快照卷读取原始数据块，并将其备份到称为映像的文件。快照卷上的所有数据块都会进行备份，包括空块，已删除文件占用的块，与分区相关的块以及文件系统元数据。映像备份的优势是，无论 Snapshot 卷上的分区方案或文件系统如何，都可以将所有信息存储在该卷中。

此映像不会作为单个文件存储在备份目标上，而是会划分为一系列数据块，这些数据块的大小为 64 MB。数据块允许 SANtricity Cloud Connector 使用多个连接到备份目标，从而提高备份过程的性能。

对于 StorageGRID 和 Amazon Web Services（S3）的备份，每个数据块使用单独的加密密钥对该区块进行加密。该密钥是一个 SHA256 哈希，由用户提供的密码短语和用户数据的 SHA256 哈希组合而成。对于 AltaVault 备份，SANtricity 云连接器不会对数据块进行加密，因为 AltaVault 会执行此操作。

- \* 基于文件的备份 \*

基于文件的备份会读取文件系统分区中包含的文件，并将其备份到一系列大小为 64 MB 的数据块中。基于文件的备份不会备份已删除的文件或分区和文件系统元数据。与基于映像的备份一样，数据块允许 SANtricity Cloud Connector 使用多个连接到备份目标，从而提高备份过程的性能。

对于 StorageGRID 和 Amazon Web Services 的备份，每个数据块都使用一个单独的加密密钥对该块进行加密。该密钥是一个 SHA256 哈希，由用户提供的密码短语和用户数据的 SHA256 哈希组合而成。对于 AltaVault 备份，SANtricity 云连接器不会对数据块进行加密，因为 AltaVault 会执行此操作。

## SANtricity云连接器的系统要求

您的系统必须满足 SANtricity 云连接器的兼容性要求。

### 主机硬件要求

您的硬件必须满足以下最低要求：

- 至少 5 GB 的内存； 4 GB 表示已配置的最大堆大小
- 软件安装至少需要 5 GB 的可用磁盘空间

您必须安装 SANtricity Web 服务代理才能使用 SANtricity 云连接器。您可以在本地安装 Web 服务代理，也可以在其他服务器上远程运行应用程序。有关安装 SANtricity Web 服务代理的信息，请参见 "[Web 服务代理主题](#)"。

### 支持的浏览器

SANtricity 云连接器应用程序支持以下浏览器（请注意最低版本）：

- Firefox v31
- Google Chrome V47
- Microsoft Internet Explorer v11
- Microsoft Edge ， EdgeHTML 12
- Safari v9



在 Microsoft Internet Explorer v11 浏览器中使用兼容性视图设置时，不会加载 SANtricity 云连接器应用程序的 API 文档。为了确保 API 文档在 Microsoft Internet Explorer v11 浏览器下正确显示，建议禁用兼容性视图设置。

### 兼容的存储阵列和控制器固件

在使用 SANtricity 云连接器应用程序之前，您应验证存储阵列和固件的兼容性。

有关 SANtricity 云连接器的所有兼容存储阵列和固件的完整最新列表，请参见 "[NetApp 互操作性表工具](#)"。

### 兼容的操作系统

SANtricity 云连接器 4.0 应用程序与以下操作系统兼容并受其支持：

操作系统	version	架构
Red Hat Enterprise Linux ( RHEL )	7.x	64 位
SUSE Linux Enterprise Server ( SLES )	12.x	64 位

### 支持的文件系统

您必须使用支持的文件系统通过 SANtricity 云连接器应用程序执行备份和还原。

SANtricity 云连接器应用程序支持以下文件系统进行备份和还原操作：

- ext2
- ext3
- ext4

## 安装 SANtricity 云连接器

SANtricity 云连接器软件包解决方案（.bin 文件）仅适用于 RedHat 和 SUSE Linux 平台。

您可以通过图形模式或控制台模式在兼容的 Linux 操作系统上安装 SANtricity 云连接器应用程序。在安装过程中，您必须为 SANtricity 云连接器指定非 SSL 和 SSL 端口号。安装后，SANtricity 云连接器将作为守护进程运行。



SANtricity 云连接器工具已弃用、不再可供下载。

开始之前

查看以下注释：

- 如果 SANtricity Web 服务代理已安装在与 SANtricity 云连接器相同的服务器上，则非 SSL 端口号和 SSL 端口号之间将发生冲突。在这种情况下，请在 SANtricity 云连接器安装期间为非 SSL 端口和 SSL 端口选择适当的数字。
- 如果对主机执行了任何硬件更改，请重新安装 SANtricity 云连接器应用程序以确保加密一致性。
- 通过 SANtricity Cloud Connector 应用程序 3.1 版创建的备份与 SANtricity Cloud Connector 应用程序 4.0 版不兼容。如果要维护这些备份，则必须继续使用先前版本的 SANtricity 云连接器。为了确保成功安装单独的 SANtricity 云连接器 3.1 和 4.0 版，必须为每个应用程序版本分配唯一的端口号。

## 安装设备映射程序多路径（DM-MP）

运行 SANtricity 云连接器的任何主机还必须运行 Linux 设备映射程序多路径（DM-MP）并安装多路径工具包。

SANtricity 云连接器发现过程依靠多路径工具包来发现和识别要备份或还原的卷和文件。有关如何设置和配置设备映射程序的详细信息，请参见下 SANtricity 适用于您所使用的 SANtricity 版本的 [\\_Storage Manager 多路径驱动程序指南 "E 系列和 SANtricity 文档资源"](#)。

## 安装 Cloud Connector

您可以在图形模式或控制台模式下在 Linux 操作系统上安装 SANtricity 云连接器。

### 图形模式

您可以使用图形模式在 Linux 操作系统上安装 SANtricity 云连接器。

开始之前

为 SANtricity 云连接器安装指定主机位置。

步骤

1. 将 SANtricity 云连接器安装文件下载到所需的主机位置。

2. 打开终端窗口。
3. 导航到包含 SANtricity Cloud Connector 安装文件的目录文件。
4. 启动 SANtricity 云连接器安装过程：

```
./cloudconnector-xxxx.bin -i gui
```

在此命令中，xxxx 指定应用程序的版本号。

此时将显示安装程序窗口。

5. 查看简介陈述，然后单击 \* 下一步 \*。

安装程序窗口中会显示 NetApp， Inc. 软件的许可协议。

6. 接受许可协议的条款，然后单击 \* 下一步 \*。

此时将显示使用先前版本的 SANtricity 云连接器创建的备份页面。

7. 要确认使用先前版本的 SANtricity 云连接器创建的备份消息，请单击 \* 下一步 \*。



要在维护先前版本的同时安装 SANtricity 云连接器 4.0 版，必须为每个应用程序版本分配唯一的端口号。

此时将在安装程序窗口中显示选择安装页面。Where would you like to Install 字段会显示以下默认安装文件夹：opt/NetApp/SANtricity cloud connector4/

8. 选择以下选项之一：

- 要接受默认位置，请单击 \* 下一步 \*。
- 要更改默认位置，请输入新的文件夹位置。此时将显示输入非 SSL Jetty 端口号页面。为非 SSL 端口分配默认值 8080。

9. 选择以下选项之一：

- 要接受默认 SSL 端口号，请单击 \* 下一步 \*。
- 要更改默认 SSL 端口号，请输入新的所需端口号值。

10. 选择以下选项之一：

- 要接受默认的非 SSL 端口号，请单击 \* 下一步 \*。
- 要更改默认的非 SSL 端口号，请输入新的所需端口号值。此时将显示 " 安装前摘要 " 页面。

11. 查看显示的 安装前摘要，然后单击 \* 安装 \*。

此时将开始安装 SANtricity 云连接器，并显示 Webserver 守护进程设置提示符。

12. 单击 \* 确定 \* 确认 Webserver 守护进程设置提示。

此时将显示安装完成消息。

13. 单击 \* 完成 \* 退出 SANtricity 云连接程序安装程序。

## 控制台模式

您可以使用控制台模式在 Linux 操作系统上安装 SANtricity 云连接器。

### 开始之前

为 SANtricity 云连接器安装指定主机位置。

### 步骤

1. 将 SANtricity 云连接器安装文件下载到所需的 IO 主机位置。
2. 打开终端窗口。
3. 导航到包含 SANtricity Cloud Connector 安装文件的目录文件。
4. 启动 SANtricity 云连接器安装过程：

```
./cloudconnector-xxxx.bin -i console
```

在此命令中，xxxx 表示应用程序的版本号。

SANtricity 云连接器的安装过程已初始化。

5. 按 \* 输入 \* 继续安装过程。

安装程序窗口中会显示 NetApp , Inc. 软件的最终用户许可协议。



要随时取消安装过程，请在安装程序窗口下键入 quit 。

6. 按 \* 输入 \* 继续完成最终用户许可协议的每个部分。

安装程序窗口下会显示许可协议接受声明。

7. 要接受最终用户许可协议的条款并继续安装 SANtricity 云连接器，请输入 y 并在安装程序窗口下按 \* 输入 \* 。

此时将显示使用先前版本的 SANtricity 云连接器创建的备份页面。



如果您不接受最终用户协议的条款，请键入 N 并按 \* 输入 \* 以终止 SANtricity 云连接器的安装过程。

8. 要确认使用先前版本的 SANtricity 云连接器创建的备份消息，请按 \* 输入 \* 。



要在维护先前版本的同时安装 SANtricity 云连接器 4.0 版，必须为每个应用程序版本分配唯一的端口号。

此时将显示一条 Choose Install Folder 消息，其中包含 SANtricity 云连接器的以下默认安装文件夹：  
/opt/netapp/SANtricity cloud connector4/sn 。

9. 选择以下选项之一：

- 要接受默认安装位置，请按 \* 输入 \*。
- 要更改默认安装位置，请输入新文件夹位置。此时将显示输入非 SSL Jetty 端口号消息。为非 SSL 端口分配默认值 8080。

10. 选择以下选项之一：

- 要接受默认 SSL 端口号，请按 \* 下一步 \*。
- 要更改默认 SSL 端口号，请输入新的所需端口号值。

11. 选择以下选项之一：

- 要接受默认的非 SSL 端口号，请按 \* 输入 \*。
- 要更改默认的非 SSL 端口号，请输入新的端口号值。此时将显示 SANtricity 云连接器的安装前摘要。

12. 查看显示的安装前摘要，然后按 \* 输入 \*。

13. 按 \* 输入 \* 确认 Webserver 守护进程设置提示。

此时将显示安装完成消息。

14. 按 \* 输入 \* 退出 SANtricity 云连接程序安装程序。

将服务器证书和 CA 证书添加到密钥库中

要使用从浏览器到 SANtricity 云连接器主机的安全 https 连接，您可以接受来自 SANtricity 云连接器主机的自签名证书，或者添加浏览器和 SANtricity 云连接器应用程序均可识别的证书和信任链。

开始之前

SANtricity 云连接器应用程序必须安装在主机上。

步骤

1. 使用 `systemctl` 命令停止服务。
2. 从默认安装位置访问工作目录。



SANtricity 云连接器的默认安装位置为 `/opt/netapp/SANtricity cloud connector4``。

3. 使用 `keytool` 命令创建服务器证书和证书签名请求（CSR）。

- 示例 \*

```
keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company, L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA" -sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore keystore_cloudconnect.jks -storepass changeit
keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks -storepass changeit -file cloudconnect.csr
```

4. 将生成的 CSR 发送给您选择的证书颁发机构（CA）。

证书颁发机构对证书请求签名并返回签名证书。此外，您还会从 CA 本身收到证书。必须将此 CA 证书导入到密钥库中。

5. 将证书和 CA 证书链导入到应用程序密钥库中：`/<install Path>/working/keystore`

◦ 示例 \*

```
keytool -import -alias ca-root -file root-ca.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
-keystore keystore_cloudconnect.jks -storepass <password>
```

6. 重新启动服务。

将 **StorageGRID** 证书添加到密钥库中

如果要将 StorageGRID 配置为 SANtricity 云连接器应用程序的目标类型，则必须先将 StorageGRID 证书添加到 SANtricity 云连接器密钥库中。

开始之前

- 您已拥有签名的 StorageGRID 证书。
- 您已在主机上安装 SANtricity 云连接器应用程序。

步骤

1. 使用 `systemctl` 命令停止服务。
2. 从默认安装位置访问工作目录。



SANtricity 云连接器的默认安装位置为 `/opt/netapp/SANtricity cloud connector4`。

3. 将 StorageGRID 证书导入到应用程序密钥库中：`/<install Path>/wing/keystore`

◦ 示例 \*

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
/home/ictlabs01.cer -keystore
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

4. 重新启动服务。

首次配置 **SANtricity** 云连接器

成功安装后，您可以通过配置向导设置 SANtricity 云连接器应用程序。首次登录到 SANtricity 云连接器后，将显示配置向导。

## 首次登录到 SANtricity 云连接器

首次初始化 SANtricity 云连接器时，必须输入默认密码才能访问此应用程序。

### 开始之前

确保您有权访问连接到 Internet 的浏览器。

### 步骤

1. 打开支持的浏览器。
2. 连接到已配置的 SANtricity 云连接器服务器（例如，`http://localhost:8080/`）。

此时将显示 SANtricity 云连接器应用程序的初始登录页面。

3. 在管理员密码字段中，输入默认密码 password。
4. 单击 \* 登录 \*。

此时将显示 SANtricity 云连接器配置向导。

### 使用配置向导

成功初始登录到 SANtricity 云连接器后，将显示配置向导。

通过配置向导，您可以为 SANtricity 云连接器设置管理员密码，Web 服务代理登录管理凭据，所需的备份目标类型以及加密密码短语。

### 第 1 步：设置管理员密码

您可以通过设置管理员密码页面自定义用于后续登录到 SANtricity 云连接器的密码。

通过 "设置管理员密码" 页面创建密码可以有效地替代 SANtricity Cloud Connector 应用程序首次登录时使用的默认密码。

### 步骤

1. 在设置管理员密码页面的 \* 输入新管理员密码 \* 字段中输入 SANtricity 云连接器所需的登录密码。
2. 在 \* 重新输入新管理员密码 \* 字段中，从第一个字段重新输入密码。
3. 单击 \* 下一步 \*。

此时将接受 SANtricity 云连接器的密码设置，并在配置向导下显示设置密码短语页面。



完成配置向导后，才会设置用户定义的管理员密码。

### 第 2 步：设置密码短语

在输入加密密码短语页面下，您可以指定一个介于 8 到 32 个字符之间的字母数字密码短语。

在 SANtricity 云连接器应用程序使用的数据加密密钥中，需要使用用户指定的密码短语。

### 步骤

1. 在 \* 定义密码短语 \* 字段中，输入所需的密码短语。
2. 在 \* 重新输入密码短语 \* 字段中，重新输入第一个字段中的密码短语。
3. 单击 \* 下一步 \* 。

系统将接受为 SANtricity 云连接器应用程序输入的密码短语，并显示配置向导的选择目标类型页面。

### 第 3 步：选择目标类型

通过 SANtricity 云连接器，可以为 Amazon S3，AltaVault 和 StorageGRID 目标类型提供备份和还原功能。您可以在 " 选择目标类型 " 页面下为 SANtricity 云连接器应用程序指定所需的存储目标类型。

开始之前

请确保您拥有以下选项之一：AltaVault 挂载点，Amazon AWS 帐户或 StorageGRID 帐户。

步骤

1. 在下拉菜单中，选择以下选项之一：
  - Amazon AWS
  - AltaVault
  - StorageGRID

此时将在配置向导中显示选定选项的目标类型页面。

2. 请参见适用于 AltaVault，Amazon AWS 或 StorageGRID 的相应配置说明。

### 配置 AltaVault 设备

在选择目标类型页面下选择 AltaVault 设备选项后，将显示 AltaVault 目标类型的配置选项。

开始之前

- 您具有 AltaVault 设备的 NFS 挂载路径。
- 您已将 AltaVault 设备指定为目标类型。

步骤

1. 在 \* NFS 挂载路径 \* 字段中，输入 AltaVault 目标类型的挂载点。



"\* NFS 挂载路径 \*" 字段中的值必须采用 Linux 路径格式。

2. 选中 \* 在此目标上保存配置数据库的备份 \* 复选框，以便在选定目标类型上创建配置数据库的备份。



如果在测试连接时检测到指定目标类型上的现有数据库配置，您可以选择将 SANtricity 云连接器主机上的现有数据库配置信息替换为在配置向导中输入的新备份信息。

3. 单击 \* 测试连接 \* 以测试指定 AltaVault 设置的连接。
4. 单击 \* 下一步 \* 。

接受为 SANtricity 云连接器指定的目标类型，并在配置向导中显示 Web 服务代理页面。

5. 继续执行 " 步骤 4：连接到 Web 服务代理 "。

### 配置 Amazon AWS 帐户

在选择目标类型页面下选择 Amazon AWS 选项后，将显示 Amazon AWS 目标类型的配置选项。

#### 开始之前

- 您已建立 Amazon AWS 帐户。
- 您已指定 Amazon AWS 作为目标类型。

#### 步骤

1. 在 \* 访问密钥 ID\* 字段中，输入 Amazon AWS 目标的访问 ID 。
2. 在 \* 机密访问密钥 \* 字段中，输入目标的机密访问密钥。
3. 在 \* 分段名称 \* 字段中，输入目标的分段名称。
4. 选中 \* 在此目标上保存配置数据库的备份 \* 复选框可在选定目标类型上创建配置数据库的备份。



建议启用此设置，以确保在数据库丢失时可以还原备份目标中的数据。



如果在测试连接时检测到指定目标类型上的现有数据库配置，您可以选择将 SANtricity 云连接器主机上的现有数据库配置信息替换为在配置向导中输入的新备份信息。

5. 单击 \* 测试连接 \* 以验证输入的 Amazon AWS 凭据。
6. 单击 \* 下一步 \*。

接受为 SANtricity 云连接器指定的目标类型，并在配置向导下显示 Web 服务代理页面。

7. 继续执行 " 步骤 4：连接到 Web 服务代理 "。

### 配置 StorageGRID 帐户

在选择目标类型页面下选择 StorageGRID 选项后，将显示 StorageGRID 目标类型的配置选项。

#### 开始之前

- 您已建立 StorageGRID 帐户。
- 您在 SANtricity 云连接器密钥库中拥有一个签名的 StorageGRID 证书。
- 您已指定 StorageGRID 作为目标类型。

#### 步骤

1. 在 \* URL \* 字段中，输入 Amazon S3 云服务的 URL
2. 在 \* 访问密钥 ID\* 字段中，输入 S3 目标的访问 ID 。
3. 在 \* 机密访问密钥 \* 字段中，输入 S3 目标的机密访问密钥。
4. 在 \* 分段名称 \* 字段中，输入 S3 目标的分段名称。
5. 要使用路径模式访问，请选中 \* 使用路径模式访问 \* 复选框。



如果未选中，则会使用虚拟主机模式访问。

6. 选中 \* 在此目标上保存配置数据库的备份 \* 复选框可在选定目标类型上创建配置数据库的备份。



建议启用此设置，以确保在数据库丢失时可以还原备份目标中的数据。



如果在测试连接时检测到指定目标类型上的现有数据库配置，您可以选择将 SANtricity 云连接器主机上的现有数据库配置信息替换为在配置向导中输入的新备份信息。

7. 单击 \* 测试连接 \* 以验证输入的 S3 凭据。



某些符合 S3 的帐户可能需要安全的 HTTP 连接。有关在密钥库中放置 StorageGRID 证书的信息，请参见 ["将 StorageGRID 证书添加到密钥库中"](#)。

8. 单击 \* 下一步 \*。

接受为 SANtricity 云连接器指定的目标类型，并在配置向导下显示 Web 服务代理页面。

9. 继续执行 "步骤 4：连接到 Web 服务代理"。

#### 第 4 步：连接到 **Web** 服务代理

与 SANtricity 云连接器结合使用的 Web 服务代理的登录和连接信息可通过输入 Web 服务代理 URL 和凭据页面输入。

开始之前

确保已与 SANtricity Web 服务代理建立连接。

步骤

1. 在 \* URL \* 字段中，输入用于 SANtricity 云连接器的 Web 服务代理的 URL。
2. 在 \* 用户名 \* 字段中，输入 Web 服务代理连接的用户名。
3. 在 \* 密码 \* 字段中，输入 Web 服务代理连接的密码。
4. 单击 \* 测试连接 \* 以验证所输入 Web 服务代理凭据的连接。
5. 通过测试连接验证输入的 Web 服务代理凭据后。
6. 单击 \* 下一步 \*

此时将接受 SANtricity 云连接器的 Web 服务代理凭据，并在配置向导中显示选择存储阵列页面。

#### 第 5 步：选择存储阵列

根据通过配置向导输入的 SANtricity Web 服务代理凭据，选择存储阵列页面下将显示可用存储阵列的列表。通过此页面，您可以选择 SANtricity 云连接器用于备份和还原作业的存储阵列。

开始之前

确保已为 SANtricity Web 服务代理应用程序配置存储阵列。



SANtricity 云连接器应用程序检测到无法访问的存储阵列会导致日志文件中出现 API 异常。这是 SANtricity Cloud Connector 应用程序在从无法访问的阵列中提取卷列表时的预期行为。为了避免日志文件中出现这些 API 异常，您可以直接使用存储阵列解析根问题描述，或者从 SANtricity Web 服务代理应用程序中删除受影响的存储阵列。

#### 步骤

1. 选中要分配给 SANtricity 云连接器应用程序以执行备份和还原操作的存储阵列旁边的每个复选框。
2. 单击 \* 下一步 \*。

此时将接受选定存储阵列，并在配置向导中显示选择主机页面。



您必须为在选择存储阵列页面下选择的任何存储阵列配置有效密码。您可以通过 SANtricity Web 服务代理 API 文档配置存储阵列密码。

### 第 6 步：选择主机

根据通过配置向导选择的 Web 服务代理托管的存储阵列，您可以通过选择主机页面选择一个可用主机，以便将备份和还原候选卷映射到 SANtricity 云连接器应用程序。

#### 开始之前

确保您有一个可通过 SANtricity Web 服务代理访问的主机。

#### 步骤

1. 在列出的存储阵列的下拉菜单中，选择所需主机。
2. 对 Select Host 页面下列出的任何其他存储阵列重复步骤 1。
3. 单击 \* 下一步 \*。

此时将接受为 SANtricity 云连接器选择的主机，并在配置向导中显示 " 查看 " 页面。

### 第 7 步：查看初始配置

SANtricity 云连接器配置向导的最后一页提供了输入结果的摘要，供您查看。

查看经验证的配置数据的结果。

- 如果所有配置数据均已成功验证和建立，请单击 \* 完成 \* 以完成配置过程。
- 如果无法验证配置数据的任何部分，请单击 \* 返回 \* 导航到配置向导的适用页面以修改提交的数据。

### 登录到 SANtricity 云连接器

您可以在支持的浏览器中通过配置的服务器访问 SANtricity 云连接器应用程序的图形用户界面。确保您已建立 SANtricity Cloud Connector 帐户。

#### 步骤

1. 在支持的浏览器中，连接到已配置的 SANtricity 云连接器服务器（例如，`http://localhost:8080/`）。

此时将显示 SANtricity 云连接器应用程序的登录页面。

2. 输入您配置的管理员密码。
3. 单击 \* 登录 \*。

此时将显示 SANtricity 云连接器应用程序的登录页面。

## 使用SANtricity云连接器创建和管理E系列卷备份

您可以访问 SANtricity 云连接器应用程序左侧导航面板中的备份选项。备份选项将显示备份页面，在此可以创建新的基于映像或基于文件的备份作业。

使用 SANtricity 云连接器应用程序的 \* 备份 \* 页面创建和处理 E 系列卷的备份。您可以创建基于映像或基于文件的备份，然后立即或稍后执行这些操作。此外，您还可以根据上次执行的完整备份选择执行完整备份或增量备份。根据上次通过 SANtricity 云连接器应用程序执行的完整备份，最多可以执行六个增量备份。



SANtricity 云连接器应用程序下列出的备份和还原作业的所有时间戳均使用本地时间。

### 创建新的基于映像的备份

您可以通过 SANtricity 云连接器应用程序的备份页面上的创建功能创建新的基于映像的备份。

#### 开始之前

确保已将 Web 服务代理中的存储阵列注册到 SANtricity 云连接器。

#### 步骤

1. 在备份页面中，单击 \* 创建 \*。

此时将显示创建备份窗口。

2. 选择 \* 创建基于映像的备份 \*。
3. 单击 \* 下一步 \*。

此时将在创建备份窗口中显示可用 E 系列卷的列表。

4. 选择所需的 E 系列卷并单击 \* 下一步 \*。

此时将显示创建备份确认窗口的 \* 为备份命名并提供问题描述 \* 页面。

5. 要修改自动生成的备份名称，请在 \* 作业名称 \* 字段中输入所需名称。
6. 如果需要，请在 \* 作业问题描述 \* 字段中为备份添加问题描述。



您应输入作业问题描述，以便于识别备份的内容。

7. 单击 \* 下一步 \*。

创建备份窗口的 \* 查看备份信息 \* 页面将显示选定基于映像的备份的摘要。

8. 查看选定备份，然后单击 \* 完成 \*。

此时将显示创建备份窗口的确认页面。

9. 选择以下选项之一：

- \* 是 \* —为选定备份启动完整备份。
- \* 否 \* - 不会对选定基于映像的备份执行完整备份。



可以稍后通过备份页面上的运行功能为选定的基于映像的备份执行完整备份。

10. 单击 \* 确定 \*。

此时将启动选定 E 系列卷的备份，此任务的状态将显示在备份页面的结果列表部分下。

#### 创建新的基于文件夹 / 文件的备份

您可以通过 SANtricity 云连接器应用程序的备份页面上的创建功能创建基于文件夹 / 文件的新备份。

#### 开始之前

确保已将 Web 服务代理中的存储阵列注册到 SANtricity 云连接器。

基于文件的备份会无条件备份您指定的文件系统上的所有文件。但是，您可以选择性地还原文件和文件夹。

#### 步骤

1. 在备份页面中，单击 \* 创建 \*。

此时将显示创建备份窗口。

2. 选择 \* 创建文件夹 / 基于文件的备份 \*。

3. 单击 \* 下一步 \*。

创建备份窗口中会显示包含可供备份的文件系统的卷列表。

4. 选择所需的卷并单击 \* 下一步 \*。

创建备份窗口将显示选定卷上可用文件系统的列表。



如果未显示您的文件系统，请验证 SANtricity 云连接器应用程序是否支持您的文件系统类型。有关详细信息，请参见 ["支持的文件系统"](#)。

5. 选择包含要备份的文件夹或文件的所需文件系统，然后单击 \* 下一步 \*。

此时将显示创建备份确认窗口的 \* 为备份命名并提供问题描述 \* 页面。

6. 要修改自动生成的备份名称，请在 \* 作业名称 \* 字段中输入所需名称。

7. 如果需要，请在 \* 作业问题描述 \* 字段中为备份添加问题描述。



您应输入作业问题描述，以便于识别备份的内容。

8. 单击 \* 下一步 \*。

创建备份窗口的 \* 查看备份信息 \* 页面将显示选定文件夹 / 基于文件的备份的摘要。

9. 查看选定的基于文件夹 / 文件的备份，然后单击 \* 完成 \*。

此时将显示创建备份窗口的确认页面。

10. 选择以下选项之一：

- \* 是 \* —为选定备份启动完整备份。
- \* 否 \* —不对选定备份执行完整备份。



也可以稍后通过备份页面上的运行功能为选定的基于文件的备份执行完整备份。

11. 单击 \* 关闭 \*。

此时将启动选定 E 系列卷的备份，此任务的状态将显示在备份页面的结果列表部分下。

#### 运行完整备份和增量备份

您可以通过备份页面上的运行功能执行完整备份和增量备份。增量备份仅适用于基于文件的备份。

#### 开始之前

确保您已通过 SANtricity 云连接器创建备份作业。

#### 步骤

1. 在备份选项卡中，选择所需的备份作业，然后单击 \* 运行 \*。



只要选择了基于映像的备份作业或未执行先前初始备份的备份作业，就会自动执行完整备份。

此时将显示 Run Backup 窗口。

2. 选择以下选项之一：

- \* 完整 \* —备份选定基于文件的备份的所有数据。
- \* 增量 \* —仅备份自上次执行备份以来所做的更改。



根据通过 SANtricity 云连接器应用程序执行的最后一次完整备份，最多可以执行六个增量备份。

3. 单击 \* 运行 \*。

备份请求已启动。

#### 删除备份作业

删除功能将删除选定备份的指定目标位置的备份数据以及备份集。

开始之前

确保备份的状态为已完成，失败或已取消。

步骤

1. 在备份页面中，选择所需的备份，然后单击 \* 删除 \*。



如果选择删除完整基础备份，则所有关联的增量备份也会被删除。

此时将显示确认删除窗口。

2. 在 \* 键入 delete\* 字段中，键入 Delete 确认删除操作。
3. 单击 \* 删除 \*。

选定备份将被删除。

在SANtricity云连接器中创建基于映像或基于文件的新恢复

您可以访问 SANtricity 云连接器应用程序左侧导航面板中的还原选项。"Restore" 选项将显示 "Restore" 页面，在此可以创建新的基于映像或基于文件的还原作业。

SANtricity 云连接器使用作业概念执行 E 系列卷的实际还原。在执行还原之前，您必须确定要用于此操作的 E 系列卷。将要还原的 E 系列卷添加到 SANtricity 云连接器主机后，您可以使用 SANtricity 云连接器应用程序的还原 页面创建和处理还原。



SANtricity 云连接器应用程序下列出的备份和还原作业的所有时间戳均使用本地时间。

创建新的基于映像的还原

您可以通过 SANtricity 云连接器应用程序的 " 还原 " 页面上的 " 创建 " 功能创建新的基于映像的还原。

开始之前

确保您可以通过 SANtricity 云连接器使用基于映像的备份。

步骤

1. 在 SANtricity 云连接器应用程序的还原页面中，单击 \* 创建 \*。

此时将显示还原窗口。

2. 选择所需的备份。
3. 单击 \* 下一步 \*。

此时将在还原窗口中显示选择备份点页面。

4. 选择所需的已完成备份。
5. 单击 \* 下一步 \*。

此时将在还原窗口中显示选择还原目标页面。

6. 选择还原卷并单击 \* 下一步 \* 。

此时将在还原窗口中显示 Review 页面。

7. 查看选定的还原操作，然后单击 \* 完成 \* 。

此时将启动对选定目标主机卷的还原，此任务的状态将显示在还原页面的结果列表部分中。

#### 创建新的基于文件的还原

您可以通过 SANtricity 云连接器应用程序的 " 还原 " 页面中的 " 创建 " 功能创建新的基于文件的还原。

#### 开始之前

确保您可以通过 SANtricity 云连接器使用基于文件的备份。

#### 步骤

1. 在 SANtricity 云连接器应用程序的还原页面中，单击 \* 创建 \* 。

此时将显示还原窗口。

2. 在还原窗口中，选择所需的基于文件的备份。
3. 单击 \* 下一步 \* 。

此时将在创建还原作业窗口中显示选择备份点页面。

4. 在选择备份点页面中，选择所需的已完成备份。
5. 单击 \* 下一步 \* 。

此时将在还原窗口中显示可用文件系统或文件夹 / 文件页面的列表。

6. 选择要还原的所需文件夹或文件，然后单击 \* 下一步 \* 。

此时将在还原窗口中显示选择还原目标页面。

7. 选择还原卷并单击 \* 下一步 \* 。

此时将在还原窗口中显示 Review 页面。

8. 查看选定的还原操作，然后单击 \* 完成 \* 。

此时将启动对选定目标主机卷的还原，此任务的状态将显示在还原页面的结果列表部分中。

#### 删除还原

您可以使用删除功能从还原页面的结果列表部分中删除选定还原项。

#### 开始之前

确保存在状态为已完成，失败或已取消的还原作业。

#### 步骤

1. 在还原页面中，单击 \* 删除 \*。

此时将显示确认删除窗口。

2. 在 \* 键入 delete\* 字段中，键入 delete 确认删除操作。
3. 单击 \* 删除 \*。



您不能删除已暂停的还原。

选定还原将被删除。

## 修改 SANtricity 云连接器设置

通过设置选项，您可以修改应用程序的 S3 帐户，受管存储阵列和主机以及 Web 服务代理凭据的当前配置。您还可以通过设置选项更改 SANtricity 云连接器应用程序的密码。

### 修改 S3 帐户设置

您可以在 "S3 帐户设置 " 窗口中修改 SANtricity 云连接器应用程序的现有 S3 设置。

#### 开始之前

修改 URL 或 S3 存储分段标签设置时，请注意，对通过 SANtricity 云连接器配置的任何现有备份的访问将受到影响。

#### 步骤

1. 在左侧工具栏中，单击 \* 设置 > 配置 \*。

此时将显示设置 - 配置页面。

2. 单击 S3 帐户设置的 \* 查看 / 编辑设置 \*。

此时将显示 "S3 Account Settings" 页面。

3. 在 URL 文件中，输入 S3 云服务的 URL。
4. 在 \* 访问密钥 ID\* 字段中，输入 S3 目标的访问 ID。
5. 在 \* 机密访问密钥 \* 字段中，输入 S3 目标的访问密钥。
6. 在 \* S3 Bucket Name\* 字段中，输入 S3 目标的存储分段名称。
7. 如果需要，选中 \* 使用路径模式访问 \* 复选框。
8. 单击 \* 测试连接 \* 以验证所输入 S3 凭据的连接。
9. 单击 \* 保存 \* 以应用修改。

此时将应用修改后的 S3 帐户设置。

### 管理存储阵列

您可以在管理存储阵列页面中从注册到 SANtricity 云连接器主机的 Web 服务代理添加或删除存储阵列。

"管理存储阵列" 页面显示可向 SANtricity 云连接器主机注册的 Web 服务代理中的存储阵列列表。

#### 步骤

1. 在左侧工具栏中，单击 \* 设置 > 存储阵列 \*。

此时将显示设置 - 存储阵列屏幕。

2. 要将存储阵列添加到 SANtricity 云连接器，请单击 \* 添加 \*。
  - a. 在添加存储阵列窗口中，从结果列表中选中所需存储阵列旁边的每个复选框。
  - b. 单击 \* 添加 \*。

选定存储阵列将添加到 SANtricity 云连接器中，并显示在设置 - 存储阵列屏幕的结果列表部分中。

3. 要修改已添加存储阵列的主机，请单击 "设置 - 存储阵列" 屏幕的结果列表部分中的行项 \* 编辑 \*。
  - a. 在关联主机下拉菜单中，选择存储阵列所需的主机。
  - b. 单击 \* 保存 \*。

选定主机将分配给存储阵列。

4. 要从 SANtricity 云连接器主机中删除现有存储阵列，请从底部结果列表中选择所需的存储阵列，然后单击 \* 删除 \*。
  - a. 在确认删除存储阵列字段中，键入 `remove`。
  - b. 单击 \* 删除 \*。

选定存储阵列将从 SANtricity 云连接器主机中删除。

#### 修改 Web 服务代理设置

您可以在 "Web 服务代理设置" 窗口中修改 SANtricity 云连接器应用程序的现有 Web 服务代理设置。

#### 开始之前

与 SANtricity 云连接器结合使用的 Web 服务代理需要添加适当的阵列并设置相应的密码。

#### 步骤

1. 在左侧工具栏中，单击 \* 菜单：设置 [ 配置 ] \*。

此时将显示 Settings - Configuration 屏幕。

2. 单击 Web 服务代理的 \* 查看 / 编辑设置 \*。

此时将显示 Web 服务代理设置屏幕。

3. 在 URL 字段中，输入用于 SANtricity 云连接器的 Web 服务代理的 URL。
4. 在用户名字段中，输入 Web 服务代理连接的用户名。
5. 在密码字段中，输入 Web 服务代理连接的密码。
6. 单击 \* 测试连接 \* 以验证所输入 Web 服务代理凭据的连接。

7. 单击 \* 保存 \* 以应用修改。

### 更改 SANtricity 云连接器密码

您可以在更改密码屏幕中更改 SANtricity 云连接器应用程序的密码。

#### 步骤

1. 在左侧工具栏中，单击 \* 菜单：设置 [ 配置 ] \*。

此时将显示 Settings - Configuration 屏幕。

2. 单击 \* 更改 SANtricity 云连接器的密码 \*。

此时将显示更改密码屏幕。

3. 在当前密码字段中，输入 SANtricity 云连接器应用程序的当前密码。
4. 在新密码字段中，输入 SANtricity 云连接器应用程序的新密码。
5. 在确认新密码字段中，重新输入新密码。
6. 单击 \* 更改 \* 以应用新密码。

修改后的密码将应用于 SANtricity Cloud Connector 应用程序。

### 卸载 SANtricity 云连接器

您可以通过图形卸载程序或控制台模式卸载 SANtricity 云连接器。

#### 使用图形模式卸载

您可以使用图形模式在 Linux 操作系统上卸载 SANtricity 云连接器。

#### 步骤

1. 在终端窗口中，导航到包含 SANtricity Cloud Connector 卸载文件的目录。

SANtricity 云连接器的卸载文件位于以下默认目录位置：

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. 从包含 SANtricity 云连接器卸载文件的目录中，运行以下命令：

```
./uninstall_cloud_connector4 -i gui
```

SANtricity 云连接器的卸载过程已初始化。

3. 在卸载窗口中，单击 \* 卸载 \* 继续卸载 SANtricity 云连接器。

卸载过程已完成，SANtricity 云连接器应用程序将在 Linux 操作系统中卸载。

## 使用控制台模式卸载

您可以使用控制台模式在 Linux 操作系统上卸载 SANtricity 云连接器。

### 步骤

1. 在终端窗口中，导航到包含 SANtricity Cloud Connector 卸载文件的目录。

SANtricity 云连接器的卸载文件位于以下默认目录位置：

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. 从包含 SANtricity 云连接器卸载文件的目录中，运行以下命令：

```
./uninstall_cloud_connector4 -i console
```

SANtricity 云连接器的卸载过程已初始化。

3. 在卸载窗口中，按 \* 输入 \* 继续卸载 SANtricity 云连接器。

卸载过程已完成，SANtricity 云连接器应用程序将在 Linux 操作系统中卸载。

## 版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

## 商标信息

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