SANtricity 软件 12.10 文档

SANtricity software

NetApp
September 28, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/e-series-santricity/index.html on September 28, 2026. Always check docs.netapp.com for the latest.

目录

SANtricity 软件 12.10 文档 1
发行说明 2
SANtricity OS 12.10 中的新增功能 2
版本 12.10 中的新增功能 2
版本 12.0R1 中的新增功能 2
版本 12.0 中的新增功能 3
发行说明 3
入门 5
了解SANtricity软件 5
SANtricity 系统管理器 5
SANtricity 统一管理器 6
SANtricity 软件浏览器和操作系统支持 7
浏览器 7
操作系统 8
SANtricity系统管理器设置 8
访问 SANtricity 系统管理器 8
了解 SANtricity System Manager 安装向导 9
SANtricity System Manager 的存储系统设置常见问题解答 10
SANtricity Unified Manager设置 11
安装SANtricity统一管理器 11
访问SANtricity统一管理器 12
使用 SANtricity System Manager 12.10 进行单阵列管理 13
主接口 13
了解 SANtricity System Manager 界面 13
查看性能数据 14
在 SANtricity System Manager 中查看存储层次结构 19
管理接口设置 20
管理通知 23
SANtricity System Manager 管理界面常见问题解答 26
池和卷组 29
了解 SANtricity System Manager 中的池和卷组 29
概念 30
配置存储 37
管理存储 46
修改池和组设置 51
管理SSD缓存 56
管理预留容量 61
SANtricity System Manager 的池和卷组常见问题解答 68
卷和工作负载 78

了解 SANtricity System Manager 中的卷和工作负载 78
概念 79
配置存储 92
管理卷 99
管理设置 104
使用复制服务 109
SANtricity System Manager 卷和工作负载常见问题解答 113
主机和主机集群 116
了解 SANtricity 软件中的主机和主机集群 116
概念 117
配置主机访问 120
管理主机和集群 124
管理设置 126
SANtricity System Manager 的主机系统和主机集群常见问题解答 131
快照 133
了解 SANtricity System Manager 中的快照 133
概念 134
创建快照和快照对象 144
管理快照计划 153
管理快照映像 155
管理快照一致性组 159
管理快照卷 162
SANtricity System Manager 快照常见问题解答 166
镜像 168
概述 168
异步概念 170
同步概念 179
管理异步镜像一致性组 186
管理异步镜像对 191
管理同步镜像对 194
停用镜像 197
SANtricity System Manager 异步镜像常见问题解答 198
SANtricity System Manager 同步镜像常见问题解答 203
远程存储 206
了解 SANtricity System Manager 中的远程存储功能 206
概念 206
管理远程存储 210
SANtricity System Manager 远程存储常见问题解答 213
硬件组件 215
在 SANtricity System Manager 中查看和管理硬件组件 215
相关信息 216

概念 . . . 216
管理磁盘架组件 . . . 221
管理控制器 . . . 225
执行恢复操作 . . . 443
管理 AutoSupport . . . 445
查看事件 . . . 451
管理升级 . . . 453
使用脚本编辑器 . . . 462
SANtricity System Manager 的 AutoSupport 常见问题解答 . . . 465
使用 SANtricity Unified Manager 8 进行多阵列管理 . . . 471
主接口 . . . 471
了解 SANtricity Unified Manager . . . 471
SANtricity Unified Manager 支持的浏览器 . . . 472
了解 SANtricity Unified Manager 中的管理员密码保护 . . . 472
在 SANtricity Unified Manager 中更改管理员密码 . . . 472
在 SANtricity Unified Manager 中管理会话超时 . . . 473
存储阵列 . . . 474
了解 SANtricity Unified Manager 中的发现 . . . 474
概念 . . . 474
发现阵列 . . . 476
管理阵列 . . . 479
设置导入 . . . 480
了解如何在 SANtricity Unified Manager 中导入存储阵列设置 . . . 480
概念 . . . 481
使用批量导入 . . . 482
SANtricity Unified Manager 导入设置常见问题解答 . . . 487
阵列组 . . . 487
了解 SANtricity Unified Manager 中的组概述 . . . 487
在 SANtricity Unified Manager 中配置存储阵列组 . . . 488
从 SANtricity Unified Manager 中的组中删除存储阵列 . . . 488
在 SANtricity Unified Manager 中删除存储阵列组 . . . 489
在 SANtricity Unified Manager 中重命名存储阵列组 . . . 489
升级 . . . 489
了解 SANtricity Unified Manager 中的升级中心 . . . 489
升级软件和固件 . . . 491

SANtricity 软件 12.10 文档

发行说明

SANtricity OS 12.10 中的新增功能

下表介绍了 SANtricity System Manager 12.10 中的新功能。

版本 12.10 中的新增功能

新增功能	Description
EF50 和 EF80 存储系统的 SAS 扩展支持	EF50 和 EF80 存储系统现在支持 SAS 扩展，从而提高了存储容量和灵活性。借助 SAS 扩展，您可以将其他存储盘柜连接到 EF50 和 EF80 系统，从而根据需要扩展存储环境。此功能对于需要高容量存储解决方案并希望在 EF50 和 EF80 平台上实现投资最大化的组织尤其有益。
对 E 系列存储系统的 NVMe over TCP 支持	E 系列存储系统现在支持 NVMe over TCP，为高性能存储访问提供额外的主机接口选项。NVMe over TCP 允许在存储系统和连接的主机之间进行高效、低延迟的通信，充分利用 NVMe 协议在标准 TCP/IP 网络上的优势。这一支持增强了 E 系列系统的多功能性，使组织能够在首选或需要 NVMe over TCP 的环境中部署这些系统。
SANtricity System Manager 的用户界面增强功能	SANtricity System Manager 用户界面获得了额外的增强功能，以提高导航、可用性和整体用户体验。这些增强功能包括更新的管理任务布局和组织，以及用于常见存储管理操作的更直观的工作流程。
扩展的 E 系列平台支持新的 SANtricity System Manager 用户界面	SANtricity System Manager 的新用户界面在针对 EF80 和 EF50 存储系统的 SANtricity 12.00 版本中引入，现已扩展以支持其他 E-Series 存储平台。这意味着管理更广泛的 E-Series 存储系统的用户现在可以从现代化的界面和增强的可用性功能中受益。扩展的支持包括与特定型号的 E-Series 存储系统的兼容性，使用户能够在更多存储基础架构中利用改进的导航功能和简化的管理任务。
EF80 和 EF50 系统的混合性能和容量驱动器支持	EF80 和 EF50 存储系统现在支持在同一存储阵列中使用性能型和容量型 NVMe SSD 驱动器，但须满足最低驱动器数量要求（性能型为 6 个，容量型为 12 个）。性能型和容量型驱动器必须分别保存在各自的池和卷组中。
增加了标准卷名和精简卷名的字符限制	标准和精简卷名的字符限制已从 30 个字符增加到 60 个字符。 如果存在名称长于 30 个字符的标准卷或精简卷，则不支持降级到 SANtricity 操作系统软件版本 11.90 或更早版本。如果您计划降级到 SANtricity 操作系统软件版本 11.90 或更早版本，请在降级前更改名称长于 30 个字符的任何标准卷或精简卷的名称。
SANtricity System Manager 用户界面的最小非活动超时限制现在为 10 分钟	SANtricity System Manager 用户界面的非活动超时限制已更新为至少 10 分钟。此前，非活动超时的最小限制为 15 分钟。此更改通过确保用户界面在 10 分钟不活动后自动注销，有助于增强安全性。

版本 12.0R1 中的新增功能

此版本仅包含小的更改，没有新功能。有关此版本中更改的更多信息，请参见 E-Series SANtricity 操作系统 12.0R1 README。

版本 12.0 中的新增功能

SANtricity OS 12.0 版本仅与新的 EF80 和 EF50 全闪存存储系统兼容。如果使用的是 SANtricity OS 11.9 或更早版本，请参阅 "已知问题" 以获取以前版本中的新功能列表。

新增功能	Description
新存储系统型号 – EF80 和 EF50 全闪存存储系统	此版本引入了 EF80 和 EF50 全 NVMe 闪存存储系统。EF80 和 EF50 支持 24 个 NVME SSD 驱动器和每个控制器一个控制器间镜像卡。支持的 NVMe over Fabrics 主机接口包括 NVMe over RoCE、NVMe over IB、EF80 的 NVMe over FC 和 EF50 的 NVMe over FC。支持的 SCSI 接口是两个系统的光纤通道。EF50 支持每个控制器最多两个主机接口卡，而 EF80 支持每个控制器最多三个主机接口卡。 EF80 和 EF50 也支持 30TB 或 60TB 大小的大容量 NVMe SSD 驱动器。EF80 和 EF50 只能在阵列装有 30TB 或 60TB 驱动器时使用动态磁盘池。
SANtricity System Manager 的新用户界面	对于新的 EF80 和 EF50 控制器，SANtricity System Manager 用户界面经过重新设计，以提供更现代的外观和感觉。新界面包括左侧面板导航和增强的可用性，以简化管理任务。 新的用户界面目前仅适用于带有 SANtricity 12.00 版本的 EF80 和 EF50 存储系统。如果使用的是 SANtricity 11.9 或更早版本，请参阅 "SANtricity系统管理器11.9." 使用旧版用户界面的说明。
服务器证书的使用者备用名称 (SAN) 现在仅允许字母、数字和连字符	在 SANtricity System Manager 或 Unified Manager 中创建或编辑服务器证书时，使用者备用名称 (SAN) 字段现在只允许使用字母、数字和连字符。此更改可增强安全性，并确保与 SSL/TLS 证书的行业标准兼容。
对于基于 SSD 和 NVMe 的系统，动态磁盘池段大小现在默认为 32K	对于基于 SSD 和 NVMe 的系统上的动态磁盘池，默认数据段大小已更改为 32K。以前，这些系统的动态磁盘池默认段大小固定为 128K。此更改可优化涉及小型和大型 I/O 操作混合的工作负载的性能。
现在可在 SANtricity System Manager 中使用脚本编辑器	SANtricity System Manager 中现在提供了新的脚本编辑器。脚本编辑器允许您创建或编辑脚本文件，将脚本文件保存到存储管理站的本地磁盘，或从磁盘加载脚本文件。脚本编辑器提供用于管理存储系统的语法检查和命令执行功能。有关详细信息，请参见 "使用脚本编辑器"。

发行说明

此站点以外的站点提供了发行说明。系统将提示您使用 NetApp 支持站点凭据登录。

- "12.10 发行说明"
- "11.90发行说明"
- "11.80发行说明"
- "11.70 发行说明"
- "11.60 发行说明"

- "11.50 发行说明"

入门

了解SANtricity软件

E 系列系统包括用于存储配置和其他任务的 SANtricity 软件。

此站点介绍如何使用以下SANtricity 管理接口：

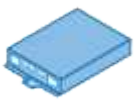
- System Manager --一种基于Web的界面，用于管理网络中的单个存储阵列。
- Unified Manager —一种基于 Web 的界面，用于查看和管理网络中的所有存储阵列。

EF80、EF50、EF600/EF600C 和 EF300/EF300C 存储阵列不支持同步镜像或精简卷。

SANtricity 系统管理器

System Manager 是嵌入在每个控制器上的基于 Web 的管理软件。要访问用户界面，请将浏览器指向控制器的 IP 地址。设置向导可帮助您开始进行系统配置。

System Manager 提供了多种管理功能，包括：

 性能
查看长达 30 天的性能数据，包括 I/O 延迟， IOPS ， CPU 利用率和吞吐量。
 存储
使用池或卷组配置存储，并创建应用程序工作负载。
 数据保护
使用快照，卷副本和远程镜像执行备份和灾难恢复。
 硬件
检查组件状态并执行与这些组件相关的某些功能，例如分配热备用驱动器。

 警报
向管理员通知存储阵列上发生的重要事件。可以通过电子邮件， SNMP 陷阱和系统日志发送警报。
 访问管理
配置用户身份验证，以要求用户使用分配的凭据登录到系统。
 系统设置
配置其他系统性能功能，例如 SSD 缓存和自动加载平衡。
 支持
查看诊断数据，管理升级和配置 AutoSupport ，此功能可监控存储阵列的运行状况并将自动派单发送给技术支持。

SANtricity 统一管理器

Unified Manager 是基于 Web 的软件，用于管理整个域。从中央视图中，您可以查看所有较新 E 系列和 EF 系列阵列的状态，例如 EF80、EF50、E4000、EF300、EF600、EF300C 和 EF600C。您还可以对选定的存储阵列执行批处理操作。

Unified Manager 与 Web 服务代理一起安装在管理服务器上。要访问 Unified Manager ，请打开浏览器并输入指向安装了 Web 服务代理的服务器的 URL 。

Unified Manager 提供了多种管理功能，包括：

 发现存储阵列
找到并添加要在组织网络中管理的存储阵列。然后，您可以从一个页面查看所有存储阵列的状态。
 发布
打开 System Manager 实例，对特定存储阵列执行单独的管理操作。

 导入设置
执行从一个存储阵列到多个阵列的批量导入，包括警报， AutoSupport 和目录服务的设置。
 镜像
在两个存储阵列之间配置异步或同步镜像对。
 管理组
将存储阵列组织成组，以便于管理。
 升级中心
升级多个存储阵列上的 SANtricity OS 软件。
 证书
为多个存储阵列创建证书签名请求（ CSR ），导入证书以及管理现有证书。
 访问管理
配置用户身份验证，以要求用户使用分配的凭据登录到 Unified Manager 。

SANtricity 软件浏览器和操作系统支持

SANtricity 软件支持多种类型的浏览器和操作系统。

浏览器

支持以下浏览器和版本。

浏览器	最低版本
Google Chrome	120
Mozilla Firefox	120
Safari	16

浏览器	最低版本
Microsoft Edge	120

对于Unified Manager、必须安装Web服务代理并可供浏览器使用。有关详细信息，请参见 "SANtricity Web 服务代理概述"

操作系统

支持以下操作系统和版本。

操作系统	最低版本/架构
Red Hat Enterprise Linux （ RHEL ）	8.x (SP10)、9.x (SP6、SP7)、10.x (GA、SP1) / 64 位
SUSE Linux Enterprise Server (SLES)	15.x (SP6、SP7)、16.x (GA) / 64 位
Oracle Linux (OL)	8.x (U10)、9.x (U6、U7)、10.x (GA、SP1) / 64 位
Windows服务器	2019、2022、2025 / 64 位
Ubuntu	20.04、22.04/64 位

SANtricity系统管理器设置

访问 SANtricity 系统管理器

要访问SANtricity系统管理器用户界面、请在浏览器中指向控制器的IP地址。设置向导可帮助您开始进行系统配置。

开始之前

- 按照其中一个快速配置指南中所述安装和配置硬件：
  - "Linux 快速配置"
  - "VMware 快速配置"
  - "Windows 快速配置"
- 配置满足以下要求的管理工作站：
  - 连接到速度为1 Gbps或更快的网络。
  - 与存储管理端口连接到同一子网。
  - 用作单独的工作站、而不是用于数据管理的主机(I/O连接)。
  - 设置带外管理、在该管理中、存储管理工作站通过控制器的以太网连接向存储系统发送命令。
  - 使用支持的浏览器进行设置。请参见 "支持的浏览器和操作系统"。

步骤

1. 在浏览器中、输入以下URL：`https://<IPAddress>`

   `IPAddress` 是一个存储阵列控制器的地址。

首次在尚未配置的阵列上打开System Manager时、将显示设置管理员密码提示符。

2. 在设置管理员密码和确认密码字段中输入管理员角色的 System Manager 密码，然后单击 * 设置密码 * 。

   首次登录时、设置向导将启动。

3. 使用设置向导执行以下任务：
   - * 验证硬件（控制器和驱动器） * —验证存储阵列中的控制器和驱动器数量。为阵列分配一个名称。
   - * 验证主机和操作系统 * - 验证存储阵列可以访问的主机和操作系统类型。
   - * 接受池 * - 接受快速安装方法建议的池配置。池是一组逻辑驱动器。
   - * 配置警报 * - 允许 System Manager 在存储阵列出现问题时自动接收通知。
   - * 启用 AutoSupport * - 自动监控存储阵列的运行状况，并将派单发送给技术支持。

有关设置向导的详细信息、请参见 "设置向导概述"。

了解 SANtricity System Manager 安装向导

使用设置向导配置存储阵列、包括硬件、主机、应用程序、工作负载、 池、警报和AutoSupport。

首次设置

首次打开System Manager时、设置向导将启动。设置向导会提示您执行基本配置任务、例如命名存储阵列、配置主机、选择应用程序以及创建存储池。

> 在继续初始设置之前，请转到升级中心（**Support › Upgrade center**），并确保您的 SANtricity 操作系统软件是最新的。如果需要，请升级到最新版本并刷新浏览器以继续设置。有关详细信息，请参见"升级中心概述"。

如果取消此向导、则无法手动重新启动它。在打开 System Manager 或刷新浏览器且至少满足以下条件之一时，向导将自动重新启动：

- 未检测到池和卷组。
- 未检测到工作负载。
- 未配置任何通知。

术语

设置向导使用以下术语。

期限	**Description**
应用程序	应用程序是一种软件程序、例如Microsoft SQL Server或Microsoft Exchange。
警报	警报会向管理员通知存储阵列上发生的重要事件。可以通过电子邮件、SNMP陷阱或系统日志发送警报。
AutoSupport	AutoSupport 功能可监控存储阵列的运行状况、并向技术支持发送自动派单。

期限	Description
硬件	存储系统硬件包括存储阵列、控制器和驱动器。
主机	主机是指向存储阵列上的卷发送I/O的服务器。
对象	对象是任何逻辑或物理存储组件。逻辑对象包括卷组、池和卷。物理对象包括存储阵列、阵列控制器、主机和驱动器。
池	池是指一组按逻辑分组的驱动器。您可以使用池创建一个或多个可供主机访问的卷。(您可以从池或卷组创建卷。)
Volume	卷是应用程序，数据库和文件系统用于存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。 卷是使用池或卷组中的可用容量创建的。卷已定义容量。尽管一个卷可能包含多个驱动器、但一个卷在主机中显示为一个逻辑组件。
卷组	卷组是具有共享特征的卷的容器。卷组已定义容量和RAID级别。您可以使用卷组创建一个或多个可供主机访问的卷。(您可以从卷组或池创建卷。)
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。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。

SANtricity System Manager 的存储系统设置常见问题解答

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。

如果我没有看到所有硬件组件怎么办?

如果验证硬件对话框中未显示所有硬件组件、则可能表示驱动器架连接不正确或存储阵列中安装了不兼容的磁盘架。

验证所有驱动器架是否均已正确连接。如果您不确定哪些驱动器架兼容、请联系技术支持。

如果我没有看到所有主机怎么办?

如果未看到已连接的主机、则自动检测失败、主机连接不正确或当前未连接任何主机。

完成设置后、您可以稍后配置主机。您可以按如下所示手动创建主机：

- 您可以转到菜单：Storage[Hosts]手动创建主机并关联相应的主机端口标识符。手动创建的主机也会显示在*初始设置*向导中。
- 必须为目标和主机配置主机端口类型(例如、iSCSI或基于RoCE的NVMe)、并且在自动检测之前与存储建立的会话将起作用。

识别应用程序如何帮助我管理存储阵列?

您可以按应用程序和工作负载查看性能数据，以评估应用程序及其相关工作负载的延迟、IOPS 和 MiB/s，从而优化性能。卷配置中包括 I/O 类型、段大小、控制器所有权以及读写缓存等特征。

什么是工作负载?

对于网络中的某些应用程序、例如SQL Server或Exchange、您可以定义一个工作负载来优化该应用程序的存储。

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。

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。

如何配置**AutoSupport** 的交付方法?

要访问 AutoSupport 交付方式的配置任务，请转到菜单：支持[AutoSupport]。

支持以下协议：HTTPS和SMTP。

如何知道是否应接受建议的池配置?

是否接受建议的池配置取决于几个因素。

回答以下问题、确定最符合您要求的存储类型：

- 您是否更喜欢容量较小的多个池、而不是可能的最大池?
- 您是否更喜欢RAID卷组而不是池?
- 您是否更愿意手动配置驱动器、而不是建议您使用的配置?

如果您对上述任一问题回答是、请考虑拒绝建议的池配置。

SANtricity系统管理器未检测到任何主机。我该怎么办?

如果未看到已连接的主机、则自动检测失败、主机连接不正确或当前未连接任何主机。

完成设置后、您可以稍后配置主机。您可以按如下所示手动创建主机：

- 您可以转到菜单：Storage[Hosts]手动创建主机并关联相应的主机端口标识符。手动创建的主机也会显示在*初始设置*向导中。
- 必须为目标和主机配置主机端口类型(例如、iSCSI或基于RoCE的NVMe)、并且在自动检测之前与存储建立的会话将起作用。

SANtricity Unified Manager设置

安装**SANtricity**统一管理器

SANtricity统一管理器包含在Web服务代理中、该代理是单独安装在主机系统上的一个API服务器、用于管理NetApp E系列存储系统。

要安装Web服务代理和Unified Manager、请参见E系列和SANtricity 文档中心中的以下说明：

1. "查看安装和升级要求"
2. "下载并安装 Web 服务代理文件"

访问SANtricity统一管理器

安装Web服务代理后、您可以访问SANtricity统一管理器、以便在一个基于Web的界面中管理多个存储系统。

有关支持的浏览器、请参见 "支持的浏览器和操作系统"。

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 "访问管理的工作原理"。

使用 SANtricity System Manager 12.10 进行单阵列管理

主接口

了解 SANtricity System Manager 界面

SANtricity系统管理器是一个基于Web的界面、可用于在一个视图中管理存储阵列。

信息板

控制面板提供了存储阵列日常管理的摘要视图。当您登录到 System Manager 时，控制面板是显示的第一个屏幕。

仪表板视图包括三个摘要区域，其中包含有关存储阵列状态和运行状况的关键信息。您可以在摘要区域找到更多信息。

区域	Description
性能	通过"性能"区域、您可以比较和对比一段时间内的资源使用情况。您可以查看存储阵列的响应时间(IOPS)、传输速率(MiB/秒)和正在使用的处理容量(CPU)性能指标。
Capacity	容量区域显示存储阵列中已分配容量、可用存储容量和未分配存储容量的图表视图。
存储层次结构	"存储层次结构"区域提供了存储阵列管理的各种硬件组件和存储对象的有序视图。单击下拉箭头对该硬件组件或存储对象执行特定操作。

通知区域

通知区域可通过窗口上角的铃铛图标访问。通知区域显示指示存储阵列及其组件状态的问题通知。此外，此部分还会显示自动警报，以帮助您在问题影响存储环境的其他区域之前对其进行故障排除。

接口设置

您可以从主界面更改显示首选项和其他设置。

用户登录和密码

当前登录系统的用户将显示在用户设置中。

有关用户和密码的详细信息、请参见：

- "设置管理员密码保护"
- "更改密码"

查看性能数据

了解 SANtricity System Manager 中的性能概述

"性能"页面提供了监控存储阵列性能的简单方法。

我可以从性能数据中了解哪些内容?

性能图形和表几乎实时显示性能数据、这有助于您确定存储阵列是否遇到问题。您还可以保存性能数据以构建存储阵列的历史视图、并确定问题发生的时间或导致问题的原因。

了解更多信息。

- "性能图和准则"
- "性能术语"

如何查看性能数据?

可从仪表板和"监控" > "性能"页面获取性能数据。

了解更多信息。

- "查看图形性能数据"
- "查看并保存表格性能数据"
- "解读性能数据"

了解 SANtricity System Manager 中的性能图表和指南

"性能"页面提供了数据图形和表、可用于评估存储阵列在多个关键领域的性能。

通过性能功能、您可以完成以下任务：

- 近乎实时地查看性能数据、以帮助您确定存储阵列是否遇到问题。
- 导出性能数据以构建存储阵列的历史视图、并确定问题发生的时间或导致问题的原因。
- 选择要查看的对象、性能指标和时间范围。
- 比较指标。

您可以通过以下三种格式查看性能数据：

- 实时图形—以近乎实时的方式在图形上绘制性能数据。
- 接近实时表格-以接近实时的方式在表中列出性能数据。
- 导出的**CSV**文件—用于将表格性能数据保存在一个逗号分隔值文件中、以供进一步查看和分析。

性能数据格式的特征

性能监控类型	采样间隔	显示的时间长度	显示的最大对象数	能够保存数据
实时图形、实时 实时图形、历史	10秒(实时) 5分钟(历史) 显示的数据点取决于选定的时间范围	默认时间范围为1小时。 选项： • 5 分钟 • 1 小时 • 8 小时 • 1天 • 7天 • 30天	5.	否
近乎实时的表格(表视图)	10秒-1小时	最新值	无限制	是的。
逗号分隔值(CSV)文件	取决于选定的时间范围	取决于选定的时间范围	无限制	是的。

查看性能数据的准则

- 性能数据收集始终处于打开状态。无法关闭此选项。
- 每次经过采样间隔后、都会查询存储阵列并更新数据。
- 对于图形数据、5分钟时间范围支持10秒更新、平均更新时间为5分钟。所有其他时间范围每5分钟更新一次、并在选定时间范围内平均更新一次。
- 图形视图中的性能数据会实时更新。表视图中的性能数据会近乎实时地进行更新。
- 如果在收集数据期间受监控对象发生更改、则该对象可能没有一组跨越选定时间范围的完整数据点。例如、卷集可能会随着卷的创建、删除、分配或取消分配而发生更改；或者驱动器可能会添加、删除或出现故障。

了解 **SANtricity** 软件中的性能术语

了解性能术语如何应用于存储阵列。

期限	**Description**
应用程序	应用程序是一种软件程序、例如SQL或Exchange。
CPU	CPU是"中央处理单元"的缩写。 CPU表示正在使用的存储阵列处理容量的百分比。
主机	主机是指向存储阵列上的卷发送I/O的服务器。
IOPS	IOPS表示每秒输入/输出操作数。
延迟	延迟是指读取或写入命令等请求与主机或存储阵列响应之间的时间间隔。
LUN	逻辑单元号(LUN)是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。

期限	Description
MIB	MIB是兆字节(megb二进制字节)的缩写。一个MIB为220或1、048、576字节。请比较MB、它表示基数为10。1 MB等于1、024字节。
对象	对象是任何逻辑或物理存储组件。 逻辑对象包括卷组、池和卷。物理对象包括存储阵列、阵列控制器、主机和驱动器。
池	池是指一组按逻辑分组的驱动器。您可以使用池创建一个或多个可供主机访问的卷。(您可以从池或卷组创建卷。)
读取	Read是"读取操作"的缩写、当主机从存储阵列请求数据时会发生此操作。
Volume	卷是应用程序，数据库和文件系统用于存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。 卷是使用池或卷组中的可用容量创建的。卷已定义容量。尽管一个卷可能包含多个驱动器、但一个卷在主机中显示为一个逻辑组件。
Volume name	卷名是创建卷时分配给卷的字符串。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存储在卷中的数据类型。标准卷和精简卷名称的最大长度为 60 个字符。名称必须是唯一的。只有标准卷和精简卷的名称可以超过 30 个字符。 如果存在名称大于 30 个字符的标准卷或精简卷，则不支持降级到 SANtricity 操作系统软件版本 11.90 或更早版本。如果您计划降级到 SANtricity 操作系统软件版本 11.90 或更早版本，请在降级前更改名称大于 30 个字符的任何标准卷或精简卷的名称。
卷组	卷组是具有共享特征的卷的容器。卷组已定义容量和RAID级别。您可以使用卷组创建一个或多个可供主机访问的卷。(您可以从卷组或池创建卷。)
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。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。
写入	写入是"写入操作"的缩写、当数据从主机发送到阵列进行存储时。

在 **SANtricity System Manager** 中查看图形性能数据

您可以查看逻辑对象、物理对象、应用程序和工作负载的图形性能数据。

关于此任务

性能图显示了历史数据以及当前正在捕获的实时数据。图形上标记为实时更新的竖线可将历史数据与实时数据区分开。

信息板视图

仪表板包含一个显示存储阵列级别性能的图表。您可以从此视图中选择有限的指标，也可以单击 **View Performance Details** 转到 **Monitoring › Performance** 并选择所有可用的指标。

详细视图

"性能"页面中提供的图表基于您的选择：

- 对象类型 — 选择要包括的对象类别（例如，存储阵列、控制器、池和卷组、应用程序、工作负载、卷、通道和驱动器）。
- 对象 — 为选定对象类型最多选择五个特定对象。

步骤

1. 选择菜单：监控[性能]。
2. 使用*对象类型*和*对象*选择要显示的数据。最多可以选择五个对象；使用*对象*列表中的搜索字段查找对象名称或部分名称。

   并非所有指标都适用于所有对象类型。存储阵列和控制器不报告延迟，只有控制器报告 CPU 利用率，只有控制器和通道报告余量。

3. 使用*时间范围*选择要显示的期间。
4. 单击 **Refresh**。
5. 可选： 在单个图形上，使用*比较*覆盖相同对象的另一种指标类型。
6. 根据需要、使用其他选项查看性能数据。

▼ 其他选项

选项	**Description**
时间范围	选择要查看的时间长度(5分钟、1小时、8小时、1天、7天、 或30天)。默认值为1小时。 加载 30 天时间范围内的性能数据可能需要几分钟的时间。加载数据时，请勿离开网页、刷新网页或关闭浏览器。
数据点详细信息	将光标悬停在图上可查看特定数据点的指标。
滚动条	使用图形下方的滚动条查看较早或较晚的时间跨度。
缩放条	在图形下方、拖动缩放条控点可在一个时间范围内进行缩小。缩放条越宽、图形详细信息的粒度越低。 要重置图形、请选择一个时间范围选项。
拖放	在图形上、将光标从一个时间点拖动到另一个时间点以放大某个时间范围。 要重置图形、请选择一个时间范围选项。

在 **SANtricity System Manager** 中查看和保存表格性能数据

您可以以表格形式查看和保存性能图形数据。这样、您可以筛选要显示的数据。

步骤

1. 在 Performance 页面中，单击 **Go to table view**。

   此时将显示一个表、其中列出了选定对象的所有性能数据。

2. 使用*对象类型*和*时间范围*选择要显示的数据，然后单击*刷新*。
3. 单击*显示/隐藏列*按钮以选择要包含在表中的列。

   您可以单击每个复选框以选择或取消选择某个项目。

4. 从表格菜单中选择 **Export to CSV**，将表格视图保存为逗号分隔值 (CSV) 文件。

   根据您的浏览器设置、文件将被保存、或者系统会提示您选择文件的名称和位置。

   默认文件名格式为 `performanceStatistics-<storage array name>-yyyy-mm-dd_hh-mm-ss.csv`，其中包括存储阵列名称以及导出文件的日期和时间。

解读 **SANtricity System Manager** 中的性能数据

性能数据可以指导您调整存储阵列的性能。

在解释性能数据时、请记住、影响存储阵列性能的因素有多种。下表介绍了需要考虑的主要方面。

性能数据	对性能调整的影响
延迟(毫秒或毫秒)	监控特定对象的I/O活动。 可能会发现瓶颈对象： • 如果一个卷组在多个卷之间共享、则各个卷可能需要自己的卷组来提高驱动器的顺序性能并降低延迟。 • 使用池时、延迟会增加、驱动器之间可能存在不平衡的工作负载、因此延迟值的意义会降低、而且通常会更高。 • 驱动器类型和速度会影响延迟。使用随机I/O时、旋转速度更快的驱动器在磁盘上不同位置之间的移动时间更短。 • 驱动器太少会导致排队的命令增多、驱动器处理命令的时间也会延长、从而增加系统的一般延迟。 • 由于传输数据需要额外的时间、I/O越大、延迟越长。 • 较高的延迟可能表示I/O模式本质上是随机的。与使用顺序流的驱动器相比、具有随机I/O的驱动器的延迟更大。 • 一个通用卷组中的驱动器或卷之间的延迟差异可能表示驱动器速度较慢。

性能数据	对性能调整的影响
IOPS	影响每秒输入/输出操作数(IOPS或IOS/sec)的因素包括： • 访问模式(随机或顺序) • I/O大小 • RAID级别 • 缓存块大小 • 是否启用读取缓存 • 是否启用写入缓存 • 动态缓存读取预取 • 区块大小 • 卷组或存储阵列中的驱动器数量 缓存命中率越高、I/O速率就越高。与禁用写入缓存相比、启用写入缓存时的写入I/O速率更高。在确定是否为单个卷启用写入缓存时、请查看当前IOPS和最大IOPS。顺序I/O模式的速率应高于随机I/O模式。无论I/O模式如何、都可以启用写入缓存、以最大程度地提高I/O速率并缩短应用程序响应时间。 您可以看到因更改卷的IOPS统计信息中的区块大小而导致的性能提升。尝试确定最佳区块大小、或者使用文件系统大小或数据库块大小。
MiB/秒	传输速率或吞吐量速率由应用程序I/O大小和I/O速率决定。一般来说、小型应用程序I/O请求会降低传输速率、但I/O速率更快、响应时间更短。对于较大的应用程序I/O请求、可以提高吞吐量。 了解典型的应用程序I/O模式有助于确定特定存储阵列的最大I/O传输速率。
CPU	此值表示正在使用的处理容量的百分比。 您可能会发现相同类型的对象的CPU使用率存在差异。例如、一个控制器的CPU使用率较高或随着时间的推移而增加、而另一个控制器的CPU使用率则较轻或较稳定。在这种情况下、您可能需要将一个或多个卷的控制器所有权更改为CPU百分比较低的控制器。 您可能需要监控存储阵列中的CPU。如果随着时间的推移、CPU会继续增加、而应用程序性能会降低、则可能需要添加存储阵列。通过向企业添加存储阵列、您可以继续以可接受的性能级别满足应用程序需求。
余量	性能余量是指控制器、控制器主机通道和控制器驱动器通道的剩余性能。此值以百分比表示、表示这些对象能够提供的最大可能性能与当前性能级别之间的差距。 • 对于控制器、余量是指最大可能IOPS的百分比。 • 对于通道、余量是最大吞吐量的百分比或MiB/秒计算中包括读取吞吐量、写入吞吐量和双向吞吐量。

在 **SANtricity System Manager** 中查看存储层次结构

主界面上的存储层次结构可提供存储阵列所管理的各种硬件组件和存储对象的有序视图。

要查看存储层次结构，请转到仪表板，然后单击存储阵列组件或存储对象上的下拉箭头。存储阵列由物理组件和逻辑组件的集合组成。

物理组件

此表介绍了存储阵列的物理组件。

组件	Description
控制器	控制器由主板，固件和软件组成。它控制驱动器并实施 System Manager 功能。
磁盘架	磁盘架是安装在机柜或机架中的机箱。它包含存储阵列的硬件组件。磁盘架有两种类型：控制器磁盘架和驱动器磁盘架。控制器架包括控制器和驱动器。驱动器架包括输入 / 输出模块（ IOM ）和驱动器。 如果存储阵列包含不同的介质类型或不同的接口类型、则会显示每种驱动器类型的驱动器架。
驱动器	驱动器是一种为数据提供物理存储介质的机械设备或固态内存设备。
主机	主机是指向存储阵列上的卷发送I/O的服务器。
主机总线适配器(HBA)	主机总线适配器(HBA)是驻留在主机中并包含一个或多个主机端口的板。
主机端口	主机端口是主机总线适配器(HBA)上的一个端口、用于与控制器建立物理连接并用于I/O操作。
管理客户端	管理客户端是指安装了浏览器以访问System Manager的计算机。

逻辑组件

存储阵列中的驱动器可为数据提供物理存储容量。使用System Manager将物理容量配置为逻辑组件、例如池、卷组和卷。这些组件是用于配置、存储、维护和保留存储阵列上的数据的工具。此表介绍了存储阵列的逻辑组件。

组件	Description
池	池是指一组按逻辑分组的驱动器。您可以使用池创建一个或多个可供主机访问的卷。(您可以从池或卷组创建卷。)
卷组	卷组是具有共享特征的卷的容器。卷组已定义容量和RAID级别。您可以使用卷组创建一个或多个可供主机访问的卷。(您可以从卷组或池创建卷。)
Volume	卷是应用程序，数据库和文件系统用于存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。
逻辑单元号(LUN)	逻辑单元号(LUN)是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。

管理接口设置

在 **SANtricity System Manager** 中管理密码保护

您必须为存储阵列配置密码、以防止其遭受未经授权的访问。

设置和更改密码

首次启动System Manager时、系统会提示您设置管理员密码。具有管理员密码的任何用户都可以对存储阵列进行配置更改、例如添加、更改或删除对象或设置。要在初始启动期间设置管理员密码、请参见 "访问System Manager"。

出于安全原因、您只能在存储阵列进入"锁定"状态之前尝试输入五次密码。在此状态下、存储阵列将拒绝后续的密码尝试。您必须等待10分钟、使存储阵列重置为"正常"状态、然后才能再次尝试输入密码。

除了管理员密码之外、存储阵列还包括预定义的用户配置文件、其中包含一个或多个映射到这些配置文件的角色。有关详细信息，请参见 "映射角色的权限"。无法更改用户配置文件和映射。只能修改密码。如果要更改管理员密码或其他用户密码、请参见 "更改密码"。

在会话超时后重新输入密码

系统仅会在单个管理会话期间提示您输入密码一次。但是、如果会话处于非活动状态30分钟、则会超时、此时您必须再次输入密码。如果从另一个管理客户端管理同一存储阵列的另一用户在会话期间更改了密码、则在下次尝试配置操作或查看操作时、系统会提示您输入密码。

您可以调整会话超时、也可以完全禁用会话超时。请参见 "管理会话超时"。

删除驱动器或密码保护

如果删除受密码保护的驱动器或要禁用密码保护、请注意以下事项：

- 如果删除具有密码保护的驱动器-密码存储在存储阵列上每个驱动器的保留区域。如果从存储阵列中删除所有驱动器、则其密码将不再起作用。要更正此情况、请将原始驱动器之一重新安装到存储阵列。
- 如果要删除密码保护-如果您不再希望命令受密码保护、请输入当前管理员密码、并将新密码文本框留空。

> 在存储阵列上运行配置命令可能会造成发生原因 严重损坏、包括数据丢失。因此、您应始终为存储阵列设置管理员密码。请使用长度较长的管理员密码并至少包含15个字母数字字符、以提高安全性。

在 **SANtricity System Manager** 中设置容量值的默认单位

SANtricity系统管理器可以吉字节(GiB)或兆字节(TiB)为单位显示容量值。

首选项存储在浏览器的本地存储中、因此所有用户都可以拥有自己的设置。

步骤

1. 单击窗口右上角的 **User Settings** 图标。
2. 在显示容量值下拉列表中，选择 **Gibibytes** 或 **Tebibytes**。

   有关缩写词和值、请参见下表。

缩写	价值
GIB	1、024[3]字节
TIB	1、024[4]字节

在 **SANtricity System Manager** 中设置性能图的默认时间范围

您可以更改性能图显示的默认时间范围。

关于此任务

控制面板和"性能"页面上显示的性能图表最初显示的时间范围为 1 小时。首选项存储在浏览器的本地存储中，因此所有用户都可以拥有自己的设置。

步骤

1. 单击窗口右上角的 **User Settings** 图标。
2. 在默认性能图时间范围显示下拉列表中，选择 **5 minutes**、**1 hour**、**8 hours**、**1 day** 或 **7 days**，并确认要执行此操作。

在 **SANtricity System Manager** 中配置登录横幅

您可以创建一个登录横幅、在用户在SANtricity 系统管理器中建立会话之前、该横幅将呈现给用户。横幅可以包括咨询通知和同意消息。

关于此任务

创建横幅时、它会显示在对话框的登录屏幕之前。

步骤

1. 从左侧面板中，选择 **System**。
2. 在常规部分下、选择*配置登录横幅*。

   此时将打开配置登录横幅对话框。

3. 输入要显示在登录横幅中的文本。

   请勿使用HTML或其他标记标记标记进行格式化。

4. 单击 * 保存 * 。

结果

用户下次登录到System Manager时、文本将在对话框中打开。用户必须单击*确定*才能继续进入登录屏幕。

在 **SANtricity System Manager** 中管理会话超时

您可以在SANtricity 系统管理器中配置超时、以便在指定时间后断开用户的非活动会话。

关于此任务

默认情况下、System Manager的会话超时为30分钟。您可以调整该时间、也可以完全禁用会话超时。

如果使用阵列中嵌入的安全断言标记语言(SAML)功能配置访问管理、则当用户的SSO会话达到其最大限制时、可能会发生会话超时。可能会在System Manager会话超时之前发生这种情况。

步骤

1. 从左侧面板中，选择 **System**。
2. 在常规部分下、选择*启用/禁用会话超时*。

   此时将打开启用/禁用会话超时对话框。

3. 使用spinner控件以分钟为单位增加或减少时间。

   您可以为 System Manager 设置的最小超时时间为 10 分钟。

   要禁用会话超时、请取消选中*设置时间长度…*复选框。

4. 单击 * 保存 * 。

管理通知

了解 **SANtricity System Manager** 问题通知

SANtricity系统管理器使用图标和其他几种方法来通知您存储阵列存在问题。

图标

System Manager可使用这些图标指示存储阵列及其组件的状态。

图标。	**Description**
	最佳
	非最佳或出现故障
	需要注意或修复
	小心

System Manager会在不同位置显示这些图标。

- 通知区域（窗口顶部的铃铛图标）
- 在组件页面上、驱动器和控制器的图形显示故障图标。

警报和**LED**

此外、System Manager还会通过其他方式通知您问题。

- System Manager会发送SNMP通知或电子邮件错误消息。
- 硬件上的"Service Action Required LED"亮起。

收到问题通知后、请使用Recovery Guru帮助您解决问题。如有必要、请使用硬件文档以及恢复步骤来更换故障

组件。

查看并执行 **SANtricity System Manager** 中正在进行的操作

要查看长时间运行的操作并对其执行操作、请使用操作进行中页面。

关于此任务

对于"Operations in Progress"页面上列出的每个操作、将显示完成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。您也可以从列表中清除已完成的卷复制操作。

步骤

1. 从左侧面板中，选择 **Monitoring › Operations in progress**。

   此时将显示操作进行中页面。

2. 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。

   您可以停止卷复制操作或更改其优先级。

3. 卷复制操作完成后、您可以选择*清除*将其从列表中删除。

   操作完成后，通知区域中将显示信息消息和黄色扳手图标，可通过窗口上角的铃铛图标查看。此消息包含一个链接，允许您从"正在进行的操作"页面中清除操作。

"Operations in Progress"页面上显示的操作包括以下内容：

操作	操作的可能状态	可以执行的操作
卷副本	已完成	清除
卷副本	正在进行中	• 更改优先级 • 停止
卷副本	待定	清除
卷副本	失败	• 清除 • 重新复制
卷副本	已停止	• 清除 • 重新复制
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 _
异步镜像组初始同步	正在进行中	暂停
异步镜像组初始同步	已暂停	恢复
同步镜像	正在进行中	暂停

操作	操作的可能状态	可以执行的操作
同步镜像	已暂停	恢复
Snapshot映像回滚	正在进行中	取消
Snapshot映像回滚	待定	取消
Snapshot映像回滚	已暂停	• 取消 • 恢复
驱动器清空	正在进行中	取消(取决于驱动器清空类型)
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 _
精简卷回收	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 _
对卷组进行碎片整理	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 _
驱动器副本	正在进行中	无 _
数据重建	正在进行中	无 _
回写	正在进行中	无 _
驱动器擦除	正在进行中	无 _
远程存储导入	正在进行中	• 更改优先级 • 停止
远程存储导入	已停止	• 恢复 • 断开连接
远程存储导入	失败	• 恢复 • 断开连接
远程存储导入	已完成	断开连接

使用 **SANtricity System Manager Recovery Guru** 恢复问题

恢复专家是SANtricity系统管理器的一个组件、用于诊断存储阵列问题并建议用于修复问题的恢复过程。

步骤

1. 在左侧面板中，选择 主页。

2. 单击 **Bell** 图标，然后单击窗口中间顶端标有 **Recover from *n* problems** 的链接。

   此时将显示Recovery Guru对话框。

3. 选择摘要列表中显示的第一个问题、然后按照恢复操作步骤 中的说明更正此问题。如有必要、请按照更换说明更换出现故障的组件。对列出的每个问题重复此步骤。

   一个存储阵列中的多个问题可能是相关的。在这种情况下、更正问题的顺序可能会影响结果。按问题在摘要列表中的列出顺序选择并更正问题。

   一个电源箱的多个故障会分组在一起、并作为一个问题列在摘要列表中。风扇箱的多个故障也列为一个问题。

4. 要确保恢复操作步骤 成功、请单击*重新检查*。

   如果您为异步镜像组或异步镜像组的成员选择了问题、请先单击*清除*以从控制器中清除故障、然后单击*重新检查*以从Recovery Guru中删除此事件。

   如果所有问题均已解决、则存储阵列图标最终会从需要注意过渡到最佳状态。对于某些问题、在执行重建等操作时会显示一个修复图标。

5. *可选：*要将Recovery Guru信息保存到文件中、请单击*保存*图标。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `recoveryGuru-failureName-arrayName-yyyy-mm-dd-hh-mm-ss.html`。

SANtricity System Manager 管理界面常见问题解答

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。

支持哪些浏览器?

SANtricity系统管理器支持这些浏览器版本。

浏览器	最低版本
Google Chrome	120
Mozilla Firefox	120
Safari	16
Microsoft Edge	120

什么是键盘快捷键?

您可以仅使用键盘在SANtricity系统管理器中导航。

整体导航

Action	键盘快捷方式
移至下一项。	选项卡

Action	键盘快捷方式
移至上一项。	Shift + Tab
选择一个项目。	输入 …
下拉列表—移动到下一个或上一个项目。	向下箭头或向上箭头
复选框—选择一个项目。	空格键
单选按钮—在项目之间切换。	向下箭头或向上箭头
可扩展文本—展开或缩减项目。	输入 …

表导航

Action	键盘快捷方式
选择一行。	按Tab键选择行、然后按Enter键
向上或向下滚动。	向下箭头/向上箭头或向下翻页/向上翻页
更改列的排序顺序。	按Tab键选择列标题、然后按Enter键

日历导航

Action	键盘快捷方式
移至上个月。	向上翻页
移至下个月。	下一页
移至上一年。	Control + Page Up
迁移到下一年。	Control + Page Down
如果已关闭、请打开日期选择器。	控制+主页
移至当前月份。	控制/命令+主页
移至前一天。	控制/命令+左侧
移至第二天。	控制/命令+右
移至上一周。	控制/命令+启动
移至下一周。	控制/命令+关闭
选择关注的日期。	输入 …
关闭日期选择器并擦除日期。	控制/命令+结束
关闭日期选择器而不进行选择。	转义

各个卷的性能统计信息与总数有何关系？

池和卷组的统计信息是通过聚合所有卷计算得出的、包括预留容量卷。

预留容量由存储系统内部使用、用于支持精简卷、快照和异步镜像、不会对I/O主机可见。因此、池、控制器和存储阵列统计信息的总和可能不等于可查看卷的总和。

但是、对于应用程序和工作负载统计信息、只会聚合可见的卷。

为什么数据在图形和表中显示为零?

如果在图形和表中为某个数据点显示零、则表示该对象在该时间点没有I/O活动。发生这种情况的原因可能是主机未向该对象启动I/O、或者该对象本身存在问题。

仍可查看对象的历史数据。一旦对象开始发生I/O活动、图形和表将显示非零数据。

下表列出了任何给定对象的数据点值可能为零的最常见原因。

阵列级别的对象类型	原因数据显示为零
Volume	• 卷未分配主机。
卷组	• 正在导入卷组。 • 卷组不包含分配给主机的卷、*卷组和_*卷组不包含任何预留容量。
驱动器	• 驱动器出现故障。 • 已删除驱动器。 • 驱动器处于未知状态。
控制器	• 控制器已脱机。 • 控制器出现故障。 • 已删除控制器。 • 控制器处于未知状态。
存储阵列	• 存储阵列不包含卷。

延迟图显示了什么内容?

延迟图提供了卷、卷组、池、应用程序和工作负载的延迟统计信息，以毫秒 (ms) 为单位。此图形显示在"逻辑视图"、"物理视图"和"应用程序和工作负载视图"选项卡中。

延迟是指读取或写入数据时发生的任何延迟。将光标悬停在图形上的某个点上、可查看该时间点的以下值(以毫秒(ms)为单位)：

- 读取时间。
- 写入时间。
- 平均I/O大小。

IOPS图显示了什么?

IOPS 图表显示每秒输入/输出操作的统计信息。在仪表板上，此图表显示存储阵列的统计信息。在"性能"页面的"逻辑视图"、"物理视图"和"应用程序和工作负载视图"选项卡中，此图表显示存储阵列、卷、卷组、池、应用程序和工作负载的统计信息。

IOPS是_input/output (I/O) operations per second_的缩写。将光标悬停在图形上的某个点上、可查看该时间点的以下值：

- 读取操作的数量。
- 写入操作的数量。
- 读取和写入操作总数的总和。

MIB/s图显示什么？

MiB/s 图表以每秒兆字节（mebibytes）为单位显示传输速度统计信息。在仪表板上，此图表显示存储阵列的统计信息。在"性能"页面的"逻辑视图"、"物理视图"和"应用程序和工作负载视图"选项卡中，此图表显示存储阵列、卷、卷组、池、应用程序和工作负载的统计信息。

MiB/秒是_mebibytes per second_的缩写、即1、048、576字节/秒。将光标悬停在图形上的某个点上、可查看该时间点的以下值：

- 读取的数据量。
- 写入的数据量。
- 读取和写入的总数据量。

CPU图形显示了什么？

CPU 图表显示每个控制器（控制器 A 和控制器 B）的处理能力统计信息。CPU 是_中央处理器_的缩写。在仪表板上，此图表显示存储阵列的统计信息。在性能页面的物理视图选项卡上，此图表显示存储阵列和驱动器的统计信息。

CPU图形显示了阵列上的操作所使用的CPU处理容量百分比。即使没有发生外部I/O、CPU利用率百分比也可以不为零、因为存储操作系统可能正在执行后台操作和监控。将光标悬停在图形上的某个点上、可查看该时间点所使用的处理能力百分比。

性能余量图显示了哪些内容？

净空图与存储阵列控制器的剩余性能相关。此图表在控制面板和"性能"页面的"物理视图"选项卡上可见。

性能余量图显示了存储系统中物理对象的剩余性能。将光标悬停在图中的某个点上方、可查看控制器A和控制器B的剩余IOPS和MiB/秒功能百分比

在哪里可以找到有关显示首选项的详细信息？

要查找有关可用显示选项的信息、请执行以下操作：

- 要阅读有关显示容量值的默认单位的详细信息、请参见 "设置容量值的默认单位"。
- 要阅读有关显示性能图形的默认时间范围的详细信息、请参见 "设置性能图形的默认时间范围"。

池和卷组

了解 **SANtricity System Manager** 中的池和卷组

您可以从存储阵列中未分配的部分驱动器创建逻辑存储容量。此逻辑容量可以采用池或卷组的形式、具体取决于您的环境需求。

什么是池和卷组?

池_是一组逻辑分组的驱动器。卷组_是具有共享特征的卷的容器。您可以使用池或卷组创建可供主机访问的卷。

了解更多信息。

- "池和卷组的工作原理"
- "容量术语"
- "确定是使用池还是卷组"

如何创建池?

您可以允许 System Manager 在检测到存储阵列中的未分配容量时自动创建池。或者，当自动创建无法确定最佳配置时，您可以从菜单：Storage[Pools and volume groups] 手动创建池。

了解更多信息。

- "自动创建池与手动创建池"
- "自动创建池"
- "手动创建池"
- "向池或卷组添加容量"

如何创建卷组?

您可以从菜单：Storage[Pools and volume groups] 创建卷组。

了解更多信息。

- "创建卷组"
- "向池或卷组添加容量"

相关信息

详细了解与池和卷组相关的概念：

- "预留容量的工作原理"
- "SSD缓存的工作原理"

概念

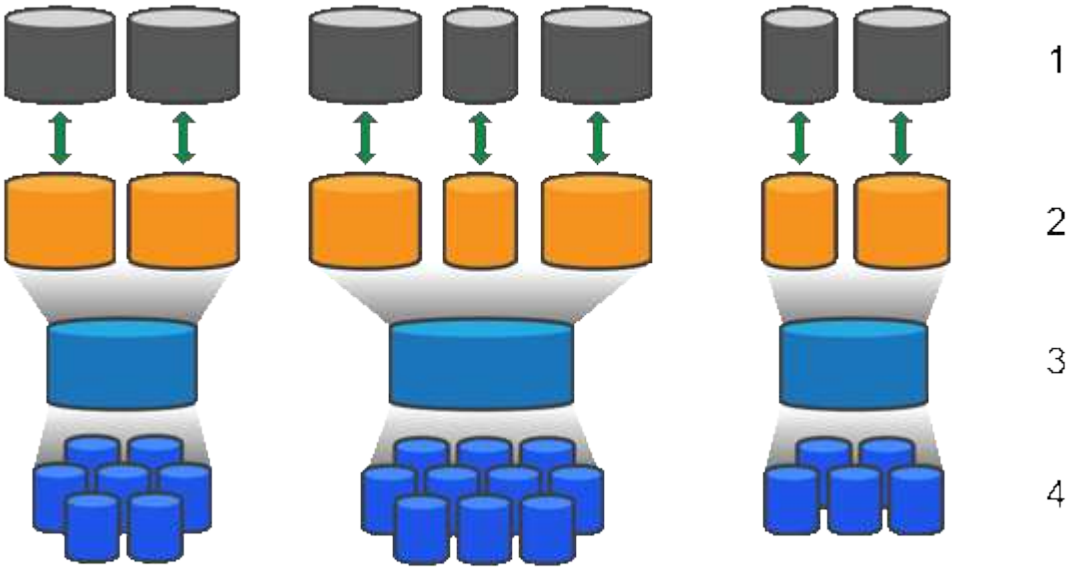
池和卷组在 **SANtricity** 软件中的工作原理

要配置存储、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)或固态磁盘(SSD)驱动器。

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
- RAID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。下图说明了这一概念。



[1]主机LUN；[2]卷；[3]卷组或池；[4] HDD或SSD驱动器

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。如果某个驱动器丢失或添加、System Manager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、System Manager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 HDD 或 SSD 用于池；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，因此您必须确保拥有足够数量的驱动器以支持所选技术。在 EF80 和 EF50 系统上，性能型和容量型 NVMe SSD 驱动器被视为不同的驱动器类型；它们可以共存于同一存储阵列中，但必须位于不同的池中。

管理故障驱动器

池的最小容量为 11 个驱动器；但是，在发生驱动器故障时，会保留一个驱动器的容量用于备用容量。这种备用容量称为"`preservation capacity`。"在 EF80 和 EF50 系统上，性能池至少需要 6 个驱动器，容量池至少需要 12 个驱动器。对于容量-DDP 池，RAID1-DDP 保护最多使用 10 个驱动器，然后在 11 个或更多驱动器时过渡到 RAID6-DDP，最小容量-DDP 池大小为 8 个驱动器。

创建池时、会保留一定的容量以供紧急使用。此容量以System Manager中的多个驱动器表示、但实际实施范围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容量或容量更多或更少、甚至可以将其设置为无保留容量(0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。

最大容量

每个存储阵列支持的最大动态磁盘池（DDP）容量取决于控制器型号和安装的 SANtricity 操作系统版本。

操作系统版本	**EF50**	**EF80**	**E4000**	**EF300**	**EF600**	**E280x**	**E5700**
11.90 R6及更低版本	不适用	不适用	6	• 12 (NVMe) • 6 (SAS)	• 12 (NVMe) • 6 (SAS)	6	6
11.90 R7	不适用	不适用	6	• 12 (NVMe) • 6 (SAS)	• 16 (NVMe) • 8 (SAS)	6	8
12.00 GA	12	12	不适用	不适用	不适用	不适用	不适用
12.10及更高版本	• 12 (NVMe) • 6 (SAS)	• 16 (NVMe) • 8 (SAS)	6	• 12 (NVMe) • 6 (SAS)	• 16 (NVMe) • 8 (SAS)	不适用	不适用

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。

您不能混合使用不同的驱动器技术（HDD 和 SSD 驱动器）。在 EF80 和 EF50 系统上，性能和容量 NVMe SSD 驱动器是不同的驱动器类型，不能在同一卷组中混合使用；性能的最小驱动器数量为 6，容量的最小驱动器数量为 12。RAID 3、5 和 6 最多限制为 30 个驱动器。RAID 1 和 RAID 10 使用镜像，因此这些卷组必须具有偶数个磁盘。

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。

了解 **SANtricity** 软件中的容量术语

了解容量术语如何应用于存储阵列。

存储对象

以下术语介绍了可与存储阵列交互的不同类型的存储对象。

存储对象	**Description**
主机	主机是指向存储阵列上的卷发送I/O的服务器。
LUN	逻辑单元号(LUN)是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。
镜像一致性组	镜像一致性组是一个或多个镜像对的容器。对于异步镜像操作、必须创建镜像一致性组。
镜像卷对	镜像对由两个卷组成、一个是主卷、一个是二级卷。
池	池是指一组按逻辑分组的驱动器。您可以使用池创建一个或多个可供主机访问的卷。(您可以从池或卷组创建卷。)
Snapshot一致性组	快照一致性组是创建快照映像时视为单个实体的卷的集合。其中每个卷都有自己的快照映像、但所有映像都是在同一时间点创建的。
Snapshot组	快照组是一组来自单个基础卷的快照映像。
Snapshot卷	主机可通过Snapshot卷访问Snapshot映像中的数据。快照卷包含自己的预留容量、这样可以在不影响原始快照映像的情况下保存对基础卷所做的任何修改。
Volume	卷是应用程序，数据库和文件系统用于存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。
卷组	卷组是具有共享特征的卷的容器。卷组已定义容量和RAID级别。您可以使用卷组创建一个或多个可供主机访问的卷。(您可以从卷组或池创建卷。)

存储容量

以下术语介绍了存储阵列上使用的不同容量类型。

容量类型	**Description**
已分配容量	已分配容量是指从池或卷组中的驱动器分配的物理容量。 您可以使用已分配的容量创建卷并执行复制服务操作。

容量类型	Description
可用容量	可用容量是指池或卷组中尚未分配给卷创建或复制服务操作和存储对象的可用容量。
池或卷组容量	池、卷或卷组容量是指存储阵列中已分配给池或卷组的容量。此容量用于创建卷并满足副本服务操作和存储对象的各种容量需求。
池不可用容量	池不可用容量是指池中由于驱动器大小不匹配而无法使用的空间。
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)。
已报告容量	报告的容量是指向主机报告并可由主机访问的容量。
预留容量	预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。
SSD 缓存	SSD缓存是一组固态磁盘(SSD)驱动器、您可以在存储阵列中对这些驱动器进行逻辑分组。SSD缓存功能可将最常访问的数据("热"数据)缓存到延迟较低的SSD驱动器上、以动态加速应用程序工作负载。
未分配的容量	未分配容量是指存储阵列中已*未*分配给池或卷组的空间。
写入容量	写入容量是指从为精简卷分配的预留容量中写入的容量。

了解 **SANtricity** 软件中的池和卷组

您可以使用池或卷组创建卷。最佳选择主要取决于关键存储要求、例如预期I/O工作负载、性能要求和数据保护要求。

选择池或卷组的原因

选择池

- 如果您需要更快的驱动器重建和简化的存储管理、需要精简卷和/或具有高度随机的工作负载。
- 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。

池和卷组之间的功能差异

下表提供了卷组和池之间的功能比较。

使用 ...	池	卷组
随机工作负载	更好	良好

使用 ...	池	卷组
工作负载顺序	良好	更好
驱动器重建时间	速度更快	速度较慢
性能(最佳模式)	好：最适合小型块、随机工作负载。	好：最适合大型块、顺序工作负载
性能(驱动器重建模式)	优于：通常优于RAID 6	降级：性能下降高达40%
多个驱动器故障	更强的数据保护：更快地按优先级重建	数据保护更少：重建速度较慢、数据丢失风险较高
添加驱动器	更快：即时添加到池中	slower：需要动态容量扩展操作
精简卷支持	是的。	否
固态磁盘(SSD)支持	是的。	是的。
简化管理	是：没有要配置的热备用磁盘或RAID设置	No：must allocate hotspares 、configure RAID
可调性能	否	是的。

池和卷组的功能比较

池和卷组的功能和用途相同。这两个对象都是一组驱动器、这些驱动器在存储阵列中逻辑分组在一起、用于创建主机可以访问的卷。

下表可帮助您确定池或卷组是否最适合您的存储需求。

功能	池	卷组
支持不同的RAID级别	否在System Manager中始终使用RAID 6。	是的。RAID 0、1、10、5和6可用。
支持的精简卷	是的。	否
支持全磁盘加密(FDE)	是的。	是的。
支持数据保证(Data Assurance 、DA)	是的。	是的。
支持磁盘架丢失保护	是的。	是的。
支持抽盒丢失保护	是的。	是的。
支持混合驱动器速度	建议相同、但不是必需的。最慢的驱动器决定了所有驱动器的速度。	建议相同、但不是必需的。最慢的驱动器决定了所有驱动器的速度。
支持混合驱动器容量	建议相同、但不是必需的。最小驱动器决定了所有驱动器的容量。	建议相同、但不是必需的。最小驱动器决定了所有驱动器的容量。
最小驱动器数	11.	取决于RAID级别。RAID 0需要1 。RAID 1或10需要2 (需要偶数) 。RAID 5最小值为3。RAID 6最小值为5。
最大驱动器数	最高可达存储阵列的最大限制	RAID 1和10—最多达到存储阵列RAID 5的最大限制、6-30个驱动器

功能	池	卷组
可以在创建卷时选择单个驱动器	否	是的。
可以在创建卷时指定分段大小	是的。支持128 K。	是的。
可以在创建卷时指定I/O特征	否	是的。支持文件系统、数据库、多媒体和自定义。
驱动器故障保护	在池中的每个驱动器上使用保留容量、从而加快重建速度。	使用热备用驱动器。重建受驱动器IOPS的限制。
达到容量限制时显示警告	是的。可以在已用容量达到最大容量的百分比时设置警报。	否
支持迁移到其他存储阵列	否要求您先迁移到卷组。	是的。
动态区块大小(DSS)	否	是的。
可以更改RAID级别	否	是的。
卷扩展(增加容量)	是的。	是的。
容量扩展（添加容量）	是的。	是的。
容量减少	是的。	否

池或卷组均不支持混合驱动器类型(HDD、SSD)。

了解 **SANtricity System Manager** 中的自动池创建与手动池创建

您可以自动或手动创建池、以便对物理存储进行分组、然后根据需要动态分配。创建池时、您可以添加物理驱动器。

自动创建

当System Manager检测到存储阵列中的未分配容量时、将启动自动池创建。检测到未分配的容量后、System Manager会自动提示您创建一个或多个池、或者将未分配的容量添加到现有池、或者同时添加这两者。

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。

池中的每个驱动器必须具有相同的驱动器类型（HDD 或 SSD）并具有相似的容量。在 EF80 和 EF50 系统上，性能和容量 NVMe SSD 驱动器被视为不同的驱动器类型；当两者都存在时，System Manager 会为每种类型创建单独的池。System Manager 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盒丢失保护状态。

如果存储阵列上有多个应用程序、而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。

配置存储

在 **SANtricity System Manager** 中自动创建池

当SANtricity系统管理器检测到存储阵列中的未分配驱动器时、系统会自动启动池创建。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。

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

请记住以下几点：

- 向存储阵列添加驱动器时、System Manager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System Manager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、System Manager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。

您可以使用以下任一方法启动池自动配置对话框：

- 检测到未分配的容量时，池自动配置建议会显示在通知区域（窗口顶端的铃铛图标）。单击 **View Pool Auto-Configuration** 以启动对话框。
- 您还可以从"池和卷组"页面启动"池自动配置"对话框、如以下任务所述。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击菜单：省略号图标 [Launch pool auto-configuration]。

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。

System Manager将执行以下任务：

- 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。

> 在 EF80 和 EF50 系统中，性能和容量 NVMe SSD 驱动器被视为单独的驱动器类型。System Manager 为性能和容量驱动器创建不同的池，而不会将它们混合到同一个池中。性能的最小池大小为 6 个驱动器，容量的最小池大小为 12 个驱动器。

1. 要查看池的其他特征，请单击显示的池名称。

   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。

2. 单击 * 接受 * 。

在 **SANtricity System Manager** 中手动创建池

如果池自动配置功能不提供满足您需求的池、您可以从一组候选对象手动创建池。

池可提供必要的逻辑存储容量、您可以从中创建各个卷、然后使用这些卷托管应用程序。

开始之前

- 您必须具有相同类型的最小驱动器数量。对于 EF80 和 EF50 系统，性能池最少需要 6 个驱动器，容量池最少需要 12 个驱动器；在混合性能和容量阵列中，容量至少需要 12 个驱动器，而性能至少需要 2 个驱动器。对于所有其他系统，最少 11 个驱动器。
- 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。目前、System Manager允许在创建卷组时在"高级"功能下选择驱动器。要创建池、建议使用存储阵列中的所有驱动器。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击菜单：创建[池]。

   此时将显示创建池对话框。

3. 键入池的名称。
4. *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。

5. 根据以下特征找到要使用的池候选，然后单击*创建*。

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)容量也会分布在整个池中、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。 System Manager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、System Manager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： • 512—512字节扇区大小。 • 4k—4、096字节扇区大小。
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。 • 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。 • 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。 • 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功能、也可能不支持安全功能、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。 不支持在同一存储阵列中混合使用 FDE 和 FIPS 驱动器。系统中所有具有安全功能的驱动器必须具有相同的类型。
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。 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。

特性	使用 ...
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。 如果所有驱动器都支持 DA，则启用 DA。创建卷后，可以通过选择菜单禁用 DA：存储[卷 > 省略号图标 > 禁用数据保证]。
资源调配功能（仅限 EF80、EF50、EF300 和 EF600）	显示资源调配是否可用于此池候选。资源调配是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。
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： • 512n—512字节原生。 • 512e—模拟512字节。 • 4 k—4、096字节。

在 **SANtricity System Manager** 中创建卷组

您可以使用卷组创建一个或多个可供主机访问的卷。卷组是指具有RAID级别和容量等共享特征的卷的容器。

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。

开始之前

在创建卷组之前、请查看以下准则：

- 您至少需要一个未分配的驱动器。
- 一个卷组中可以包含的驱动器数量存在限制。这些限制因RAID级别而异。
- 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。
- 如果您使用的是EF600或EF300存储阵列、并且计划手动创建卷组、请确保每个控制器都可以访问前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。目前、System Manager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。

不支持在同一存储阵列中混合使用 FDE 和 FIPS 驱动器。系统中所有具有安全功能的驱动器必须具有相同的类型。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击菜单：创建[卷组]。

   此时将显示创建卷组对话框。

3. 键入卷组的名称。
4. 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。

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。

   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。

6. *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。

   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。

   只有了解驱动器冗余和最佳驱动器配置的专家才应使用手动方法。

7. 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。

   ▼ 自动方法驱动器特征

特性	使用 ...
可用容量	显示可用容量(以GiB为单位)。选择一个具有满足应用程序存储需求的容量的卷组候选项。
驱动器总数	显示可用于此卷组的驱动器数量。选择包含所需驱动器数量的卷组候选项。
驱动器块大小(仅限EF300和EF600)	显示了组中的驱动器可以写入的块大小(扇区大小)。值可能包括： • 512—512字节扇区大小。 • 4k—4、096字节扇区大小。

特性	使用 ...
支持安全保护	指示此卷组候选项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。 • 您可以使用驱动器安全保护卷组、但所有驱动器都必须具有安全功能才能使用此功能。 • 如果要创建仅FDE卷组、请在安全功能列中查找*是- FDE*。如果要创建仅FIPS卷组、请查找*是- FIPS-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、卷组将在较低的安全级别(140-2)下运行。 • 您可以创建一个由驱动器组成的卷组、这些驱动器可能支持安全功能、也可能不支持安全功能、或者混合了多种安全级别。如果卷组中的驱动器包含不支持安全的驱动器、则无法确保卷组的安全。
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。如果卷组具有安全功能、并且您已设置安全密钥、则可以选中此复选框来启用驱动器安全性。 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卷组并擦除驱动器。
支持DA	指示数据保证(Data Assurance、DA)是否可用于此组。数据保证(Data Assurance、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的卷组。(对于支持DA的驱动器、在池中创建的卷会自动启用DA。) 卷组可以包含支持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。
支持资源调配（仅限 EF80、EF50、EF300 和 EF600）	显示资源调配是否可用于此组。资源调配是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。
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磁盘架完全失去通信时能够访问卷组中卷上的数据。
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。如果与驱动器架中的单个抽盒完全失去通信、则抽盒丢失保护功能可确保能够访问卷组中卷上的数据。
支持的卷块大小(仅限EF300和EF600)	显示了可为组中的卷创建的块大小： • 512n—512字节原生。 • 512e—模拟512字节。 • 4 k—4、096字节。

▼ 手动方法驱动器特征

特性	使用 ...
介质类型	指示介质类型。支持以下介质类型： • 硬盘驱动器 • 固态磁盘(SSD) 一个卷组中的所有驱动器都必须具有相同的介质类型(所有SSD或所有硬盘驱动器)。卷组不能混合使用介质类型或接口类型。
驱动器块大小(仅限EF300和EF600)	显示了组中的驱动器可以写入的块大小(扇区大小)。值可能包括： • 512—512字节扇区大小。 • 4k—4、096字节扇区大小。
驱动器容量	指示驱动器容量。 • 尽可能选择容量等于卷组中当前驱动器容量的驱动器。 • 如果您必须添加容量较小的未分配驱动器、请注意、卷组中当前每个驱动器的可用容量会减少。因此、卷组中的驱动器容量相同。 • 如果您必须添加容量更大的未分配驱动器、请注意、添加的未分配驱动器的可用容量会减少、以便与卷组中驱动器的当前容量匹配。
托盘	指示驱动器的托盘位置。
插槽	指示驱动器的插槽位置。
转速(rpm)	指示驱动器的速度。
逻辑扇区大小	指示扇区大小和格式。
支持安全保护	指示此卷组候选项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。 • 您可以使用驱动器安全保护卷组、但所有驱动器都必须具有安全功能才能使用此功能。 • 如果要创建仅FDE卷组、请在安全功能列中查找*是- FDE*。如果要创建仅FIPS卷组、请查找*是- FIPS-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、卷组将在较低的安全级别(140-2)下运行。 • 您可以创建一个由驱动器组成的卷组、这些驱动器可能支持安全功能、也可能不支持安全功能、或者混合了多种安全级别。如果卷组中的驱动器包含不支持安全的驱动器、则无法确保卷组的安全。
支持DA	指示数据保证(Data Assurance、DA)是否可用于此组。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的卷组。(对于支持DA的驱动器、在池中创建的卷会自动启用DA。) 卷组可以包含支持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。

特性	使用 ...
支持的卷块大小(仅限EF300和EF600)	显示了可为组中的卷创建的块大小： • 512n—512字节原生。 • 512e—模拟512字节。 • 4 k—4、096字节。
支持资源调配（仅限 EF80、EF50、EF300 和 EF600）	显示资源调配是否可用于此组。资源调配是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。

在 **SANtricity System Manager** 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。

扩展会导致池或卷组包含额外的可用容量。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。

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）。对于 EF80 和 EF50 系统，性能和容量 NVMe SSD 驱动器可以共存于同一存储阵列中，但不能混合在同一池或卷组中。
- 池或卷组必须处于最佳状态。
- 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 卷（EF80、EF600 和 EF600C）
  - 1,024 卷（EF50 和 EF300）
  - 512 卷 (E4000)
- 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。
- 添加的驱动器容量必须等于或大于池或卷组中最小驱动器的容量。
- 您添加的驱动器的 PCIe 速度和驱动器类型（性能或容量）必须与池或卷组中的现有驱动器匹配。性能和容量驱动器不能在同一池或卷组中混合使用。

关于此任务

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系统的最大限制。)

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。

避免使用具有 Data Assurance (DA) 功能的驱动器向不具有 DA 功能的池或卷组添加容量。池或卷组无法利用具有 DA 功能的驱动器的功能。在这种情况下，请考虑使用不具有 DA 功能的驱动器。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 找到要添加驱动器的池或卷组，然后单击菜单：省略号图标[Add capacity]。

   此时将显示添加容量页面。仅显示与池或卷组兼容的未分配驱动器。

3. 在 **Select drives to Add capacity…** 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)	指示驱动器容量。 • 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。 • 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。 • 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。
支持安全保护	指示驱动器是否支持安全保护。 • 要使用驱动器安全功能保护池或卷组、所有驱动器都必须具有安全功能。 • 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。 • 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。 • 报告为支持安全的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。 • 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。

字段	Description
支持DA	指示驱动器是否支持数据保证(Data Assurance、DA)。 • 不建议使用不支持 Data Assurance (DA) 的驱动器向支持 DA 的池或卷组添加容量。池或卷组将不再具有 DA 功能，并且您不再可以选择在池或卷组内新创建的卷上启用 DA。 • 不建议使用支持 Data Assurance (DA) 的驱动器向不支持 DA 的池或卷组添加容量，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。
支持DULBE	指示驱动器是否具有取消分配或未写入逻辑块错误 (DULBE) 的选项。DULBE 是 NVMe 驱动器上的一个选项，允许 EF80、EF50、EF300 或 EF600 存储阵列支持资源调配的卷。

4. 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

   *目前、在向具有磁盘架丢失保护或抽盒丢失保护的池添加驱动器时、不会显示确认对话框。

1. 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。

管理存储

在 **SANtricity System Manager** 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。

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

检查卷冗余功能目前仅适用于 Legacy System Manager 界面中的操作。

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击要检查的池或卷组的菜单:省略号图标 [Check volume redundancy]。

   此时将显示检查冗余对话框。
3. 选择要检查的卷、然后键入`check`确认要执行此操作。
4. 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。

   ▼ 有关冗余检查状态的更多信息

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 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。

Status	Description
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。

5. 检查池或卷组中的最后一个卷后、单击*完成*。

在 **SANtricity System Manager** 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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 从列表中选择一个池或卷组。

   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。

3. 选择菜单：省略号图标 [Delete] 并确认。

结果

System Manager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 **SANtricity System Manager** 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：

- 当为卷组检测到至少一个可用容量区域时，"合并可用容量"建议将显示在通知区域中，可通过窗口上角的铃形图标访问。单击*合并可用容量*链接以启动对话框。
- 您还可以从池和卷组页面启动 Consolidate Free Capacity 对话框，如以下任务中所述。

▼ 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。在卷组中创建具有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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击菜单：省略号图标 [Consolidate volume group free capacity]。

   此时将显示整合可用容量对话框。

3. 键入`consolidate`确认要执行此操作。
4. 单击*整合*。

   System Manager会开始将卷组的可用容量区域整合(碎片整理)为一个连续的容量、以便执行后续的存储配置任务。

完成后

选择菜单：监控[正在进行的操作]以查看"合并空闲容量"操作的进度。此操作可能耗时较长，并可能影响系统性能。

在 **SANtricity CLI** 中导出/导入卷组

通过卷组迁移、您可以导出卷组、以便将卷组导入到其他存储阵列。

SANtricity System Manager用户界面不支持导出/导入功能。您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

在 **SANtricity System Manager** 中打开池、卷组或 **SSD** 缓存中的定位器灯

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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 找到要查找的池、卷组或 SSD Cache，然后单击菜单：省略号图标[打开定位器指示灯]。

   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。

3. 成功找到驱动器后、单击*关闭*。

从 **SANtricity System Manager** 中的池或 **SSD** 缓存中删除容量

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。已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。

▼ 了解潜在的性能影响

- 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。

▼ 了解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、则池中将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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 找到池或 SSD 缓存，然后单击菜单：省略号图标[Remove capacity]。

   此时将显示删除容量对话框。

3. 在列表中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。

   池和卷组视图反映了池或SSD缓存容量新减少的情况。

修改池和组设置

在 **SANtricity System Manager** 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System Manager界面更改池的RAID级别。System Manager会自动将池配置为RAID 6。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 找到要编辑的池，然后单击 **ellipsis icon › Edit Settings**。

   此时将显示编辑池设置窗口。

3. 根据需要编辑池设置。

   ▼ 字段详细信息

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	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、System Manager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。 警报显示在通知区域，可通过窗口上角的铃铛图标访问，并可通过电子邮件和 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： • 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。 • 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。

正在设置 ...	Description
修改优先级	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。 • 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。 • 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。 • 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。
保留容量(EF600或EF300的"优化容量")	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。 • 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。 • 如果减少保留容量、则增加可用于池卷的容量。 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、未分配的容量包括池的保留容量、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。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。

4. 单击 * 保存 * 。

在 **SANtricity System Manager** 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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 找到要编辑的卷组，然后单击 **ellipsis icon › Edit Settings**。

   此时将显示 Edit Volume Group Settings（编辑卷组设置）窗口。

3. 根据需要编辑卷组设置。

   ▼ 字段详细信息

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	从下拉菜单中选择新的RAID级别。 • * 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型逻辑驱动器。 • * RAID 1镜像*—提供高性能和最佳数据可用性、适用于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。 • * RAID 10条带化/镜像*-提供RAID 0 (条带化)和RAID 1 (镜像)的组合、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。 • * 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。 • * 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。
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。

4. 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、System Manager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 **SANtricity System Manager** 中启用或禁用现有卷组和池的资源配置

对于任何支持DULBE-的驱动器、您可以在池或卷组中的现有卷上启用或禁用资源配置。

资源调配是 EF80、EF50、EF300/EF300C 和 EF600/EF600C 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。分配给卷的所有驱动器块都将被取消分配（未映射），这可以提高 SSD 的磨损寿命并提高最大写入性能。

默认情况下、在驱动器支持DULBE"的系统上启用资源配置。除非您先前已禁用资源配置、否则无需启用该配置。

开始之前

- 您必须具有 EF80、EF50、EF300 或 EF600 存储阵列。
- 您必须具有SSD卷组或池、其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(DULBEe)错误恢复功能。否则、资源配置选项将不可用。

关于此任务

在为现有卷组和池启用资源配置时、选定卷组或池中的所有卷都会发生更改、以允许取消分配这些块。此过程可能涉及后台操作、以确保在取消映射粒度处分配一致。此操作不会取消映射任何空间。后台操作完成后、操作系统需要取消映射任何未使用的块以创建可用空间。

在为现有卷组或池禁用资源配置时、后台操作会重新写入每个卷中的所有逻辑块。现有数据保持不变。写入操作将在与卷组或池关联的驱动器上映射或配置块。

> 对于新的卷组和池，可以从菜单启用或禁用资源调配：System[Additional settings > Configure resource-provisioned volumes]。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击*省略号*图标，然后为选定的池或卷组选择*启用资源调配*或*禁用资源调配*。
3. 在对话框中、确认操作。

> 如果您重新启用**DULBE**-后台操作完成后、您可能需要重新启动主机以检测到DULBE*配置更改、然后重新挂载所有文件系统。

在 **SANtricity System Manager** 中启用或禁用新卷组或池的资源配置

如果您先前已禁用资源配置的默认功能、则可以为您创建的任何新SSD卷组或池重新启用此功能。您也可以再次禁用此设置。

资源调配是 EF80、EF50、EF300/EF300C 和 EF600/EF600C 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。分配给卷的所有驱动器块都将被取消分配（未映射），这可以提高 SSD 的磨损

寿命并提高最大写入性能。

默认情况下、在驱动器支持DULBE"的系统上启用资源配置。

开始之前

- 您必须具有 EF80、EF50、EF300 或 EF600 存储阵列。
- 您必须具有SSD卷组或池、其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(DULBEe)错误恢复功能。

关于此任务

在为新卷组或池重新启用资源配置时、仅会影响新创建的卷组和池。启用了资源配置的任何现有卷组和池将保持不变。

步骤

1. 从左侧面板中，选择 **System**。
2. 向下滚动到*其他设置*、然后单击*启用/禁用资源配置卷*。

   设置问题描述 指示当前是启用还是禁用资源配置。

3. 在对话框中、确认操作。

结果

启用或禁用资源配置仅会影响您创建的新SSD池或卷组。现有池或卷组保持不变。

在 **SANtricity System Manager** 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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 找到要启用安全性的池或卷组，然后单击菜单：省略号图标[Enable security]。

   此时将显示确认启用安全性对话框。

3. 确认要为选定池或卷组启用安全性、然后单击*启用*。

管理SSD缓存

SSD 缓存在 SANtricity 软件中的工作原理

SSD缓存功能是一种基于控制器的解决方案 、可将最常访问的数据("热"数据)缓存到延迟较低的固态驱动器(SSD)上、以动态提高系统性能。SSD缓存仅用于主机读取。

SSD缓存与主缓存

SSD缓存是一种二级缓存、可与控制器动态随机存取存储器(DRAM)中的主缓存结合使用。

SSD缓存的运行方式与主缓存不同：

- 对于主缓存、每个I/O操作都必须通过缓存暂存数据才能执行此操作。

  在主缓存中、数据会在主机读取后存储在DRAM中。

- 只有在将数据置于缓存中有利于提高整体系统性能时、才会使用SSD缓存。

  在SSD缓存中、数据会从卷中复制并存储在两个内部RAID卷(每个控制器一个)上、这两个卷在创建SSD缓存时会自动创建。

内部RAID卷用于内部缓存处理。这些卷不可访问或显示在用户界面中。但是、这两个卷会计入存储阵列中允许的卷总数。

如何使用SSD缓存

智能缓存会将数据放置在低延迟驱动器中、以便能够更快地响应未来对该数据的请求。如果某个程序请求缓存中的数据(称为"`cache hit`")、则延迟较低的驱动器可以处理该事务。否则、将出现"`cache miss`"、并且必须从速度较慢的原始驱动器访问数据。随着缓存命中次数的增加、整体性能也会提高。

当主机程序访问存储阵列的驱动器时、数据存储在SSD缓存中。当主机程序再次访问相同的数据时、系统会从SSD缓存而非硬盘驱动器中读取这些数据。通常访问的数据存储在SSD缓存中。只有在无法从SSD缓存读取数据时、才会访问硬盘驱动器。

只有在将数据置于缓存中有利于提高整体系统性能时、才会使用SSD缓存。

当CPU需要处理读取数据时、它会执行以下步骤：

1. 检查DRAM缓存。
2. 如果在DRAM缓存中未找到、请检查SSD缓存。
3. 如果在SSD缓存中未找到、请从硬盘驱动器获取。如果认为数据值得缓存、请复制到SSD缓存。

提高了性能

将访问量最多的数据(热点)复制到SSD缓存可以提高硬盘运行效率、降低延迟并加快读取和写入速度。使用高性能SSD缓存HDD卷中的数据可提高I/O性能和响应时间。

使用简单的卷I/O机制将数据移入和移出SSD缓存。在缓存数据并将其存储在SSD上后、随后会在SSD缓存上执

行这些数据的读取、从而无需访问HDD卷。

SSD缓存和驱动器安全功能

要在同时使用驱动器安全(已启用安全保护)的卷上使用SSD缓存、该卷的驱动器安全功能必须与SSD缓存匹配。如果不匹配、则此卷将不会启用安全保护。

实施SSD缓存

要实施SSD缓存、请执行以下操作：

1. 创建SSD缓存。
2. 将SSD缓存与要实施SSD读取缓存的卷相关联。

> 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。

了解 SANtricity 软件中的 SSD 缓存限制

了解在存储阵列上使用SSD缓存时的限制。

限制

- 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。
- 目前、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缓存容量为10 TB。
- 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。
- 要删除SSD缓存中的最后一个驱动器、必须先删除SSD缓存。

驱动器安全限制

- 只有在创建SSD缓存时、才能在SSD缓存上启用安全性。您稍后无法像在卷上那样启用安全性。
- 如果将支持安全的驱动器与SSD缓存中不支持安全的驱动器混合使用、则无法为这些驱动器启用驱动器安全性。
- 启用了安全保护的卷必须具有启用了安全保护的SSD缓存。

在 SANtricity System Manager 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。

关于此任务

创建新的SSD缓存时、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。

创建新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。
- 如果只有一个卷启用了SSD缓存、则整个SSD缓存将分配给该卷所属的控制器。
- 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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 单击菜单：创建SSD缓存。

   此时将显示创建SSD缓存对话框。

3. 键入SSD缓存的名称。
4. 根据以下特征选择要使用的SSD缓存候选项。

特性	使用 ...
Capacity	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。 启用后、将无法禁用安全性。您只能在创建SSD缓存时启用安全性、而不能稍后启用。

特性	使用 ...
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。

5. 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。

6. 单击 * 创建 * 。

在 **SANtricity System Manager** 中更改 **SSD** 缓存设置

您可以编辑 SSD Cache 的设置。可通过"查看设置"选项访问 SSD 缓存的当前设置。

步骤

1. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 选择要编辑的 SSD Cache，然后单击菜单：省略号图标[编辑设置]。

   此时将显示编辑 SSD 缓存设置窗口。

3. 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： • 最佳 • 未知 • 已降级 • 失败(失败状态会导致严重的MEL事件。) • 已暂停

正在设置 ...	Description
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： • 最多1 GiB • 1 GiB到2 GiB • 2 GiB到4 GiB • 超过4 GiB
安全性和DA	显示SSD缓存的驱动器安全性和数据保证状态。 • 支持安全-指示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。 • 已启用安全-指示是否已在SSD缓存上启用安全性。 • *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。
关联对象	显示了与SSD缓存关联的卷和驱动器。

4. 单击 * 保存 * 。

在 **SANtricity System Manager** 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。

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. 从左侧面板中，选择菜单：Storage[Pools and volume groups]。
2. 选择要查看其统计信息的 SSD Cache，然后单击菜单：省略号图标[View statistics]。

   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

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。

设置	Description
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)。

3. 单击*取消*关闭对话框。

管理预留容量

SANtricity 软件中的预留容量工作原理

在为卷提供复制服务操作(例如快照或异步镜像操作)时、系统会自动创建预留容量。

预留容量的目的是、在出现问题时、将数据更改存储在这些卷上。与卷一样、预留容量也是从池或卷组创建的。

复制使用预留容量的服务对象

预留容量是以下副本服务对象使用的底层存储机制：

- Snapshot组
- 读/写Snapshot卷
- 一致性组成员卷
- 镜像对卷

创建或扩展这些副本服务对象时、必须从池或卷组创建新的预留容量。对于快照操作、预留容量通常为基础卷的40%、对于异步镜像操作、预留容量通常为基础卷的20%。但是、预留容量会根据原始数据的更改次数而有所不同。

精简卷和预留容量

对于精简卷、如果已达到报告的最大容量256 TiB、则无法增加其容量。确保精简卷的预留容量设置为大于报告的最大容量的大小。(精简卷始终采用精简配置、这意味着在将数据写入卷时会分配容量。)

如果使用池中的精简卷创建预留容量、请查看以下预留容量操作和结果：

- 如果精简卷的预留容量发生故障、精简卷本身不会自动过渡到故障状态。但是、由于精简卷上的所有I/O操作都需要访问预留容量卷、因此I/O操作始终会导致将检查条件返回给发出请求的主机。如果可以解决预留容量卷的根本问题、预留容量卷将返回到最佳状态、精简卷将再次正常运行。
- 如果使用现有精简卷完成异步镜像对、则该精简卷将使用新的预留容量卷重新初始化。在初始同步过程中、仅传输主端配置的块。

容量警报

副本服务对象具有可配置的容量警告和警报阈值、并在预留容量已满时提供可配置的响应。

当副本服务对象卷的预留容量接近填充点时、系统会向用户发出警报。默认情况下、如果预留容量卷已满75%、则会发出此警报；但是、您可以根据需要上调或下调此警报点。如果您收到此警报、则可以在此时增加预留容量卷的容量。在这方面、可以单独配置每个副本服务对象。

孤立的预留容量卷

孤立预留容量卷是指由于其关联的副本服务对象已被删除而不再存储用于复制服务操作的数据的卷。删除副本服务对象时、其预留容量卷也应被删除。但是、无法删除预留容量卷。

由于任何主机都不会访问孤立的预留容量卷、因此它们是可回收的候选卷。手动删除孤立的预留容量卷、以便可以将其容量用于其他操作。

System Manager 通过通知区域中的"Reclaim unused capacity"消息提醒您注意孤立的保留容量卷，该通知区域可通过窗口上角的铃铛图标访问。您可以单击 **Reclaim unused capacity** 以显示 Reclaim Unused Capacity 对话框，从而删除孤立的保留容量卷。

预留容量的特征

- 在创建卷期间、需要考虑为预留容量分配的容量、以保留足够的可用容量。
- 预留容量可以小于基础卷(最小大小为8 MiB)。
- 元数据占用了一些空间、但空间非常小(192 KiB)、因此在确定预留容量卷的大小时无需考虑这些空间。
- 预留容量不能直接从主机读取或写入。
- 每个读/写Snapshot卷、快照组、一致性组成员卷和镜像对卷都有预留容量。

增加 **SANtricity System Manager** 中的预留容量

您可以增加预留容量、这是物理分配的容量、用于对存储对象执行任何复制服务操作。

对于快照操作、通常为基础卷的40%；对于异步镜像操作、通常为基础卷的20%。通常、当您收到存储对象的预留容量即将满的警告时、您可以增加预留容量。

开始之前

- 池或卷组中的卷必须处于最佳状态、并且不能处于任何修改状态。
- 要用于增加容量的池或卷组中必须存在可用容量。

  如果任何池或卷组上没有可用容量、则可以将未使用的驱动器形式的未分配容量添加到池或卷组中。

关于此任务

对于以下存储对象、只能以8 GiB为增量增加预留容量：

- Snapshot组
- Snapshot卷
- 一致性组成员卷
- 镜像对卷

如果您认为主卷会发生许多更改、或者某个特定副本服务操作的生命周期很长、请使用较高的百分比。



您不能增加只读快照卷的预留容量。只有读写Snapshot卷才需要预留容量。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要增加预留容量的存储对象，然后单击 **ellipsis icon › Increase reserved capacity**。

   此时将显示增加预留容量对话框。
3. 使用spinner框调整容量百分比。

   如果包含所选存储对象的池或卷组上不存在可用容量、并且存储阵列具有未分配的容量、则可以创建新的池或卷组。然后、您可以使用该池或卷组上的新可用容量重试此操作。
4. 单击 * 增加 * 。

结果

System Manager将执行以下操作：

- 增加存储对象的预留容量。
- 显示新添加的预留容量。

减少 **SANtricity System Manager** 中的预留容量

您可以使用减少容量选项减少以下存储对象的预留容量：Snapshot组、Snapshot卷和一致性组成员卷。您只能将预留容量减少为您用于增加的容量。

开始之前

- 存储对象必须包含多个预留容量卷。
- 存储对象不能是镜像对卷。
- 如果存储对象是快照卷、则必须是已禁用的快照卷。
- 如果存储对象是快照组、则不能包含任何关联的快照映像。

关于此任务

请查看以下准则：

- 只能按与添加时相反的顺序删除预留容量卷。
- 您不能减少只读快照卷的预留容量、因为它没有任何关联的预留容量。只有读写Snapshot卷才需要预留容量。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要降低预留容量的存储对象，然后单击菜单：省略号图标 [Decrease Capacity]。

   此时将显示减少保留容量页面。

3. 选择要减少预留容量的容量、然后单击*减少*。

结果

System Manager将执行以下操作：

- 更新存储对象的容量。
- 显示存储对象新更新的预留容量。
- 当您减少快照卷的容量时、System Manager会自动将快照卷过渡到"Disabled"状态。Disabled表示快照卷当前未与快照映像关联、因此无法为I/O分配给主机

在 **SANtricity System Manager** 中更改快照组的预留容量设置

您可以更改快照组的设置、以更改其名称、自动删除设置、允许的最大快照映像数、SANtricity系统管理器发送预留容量警报通知的百分比或预留容量达到最大定义百分比时要使用的策略。

在创建快照组期间、系统会创建预留容量来存储组中所有快照映像的数据。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要编辑的快照组，然后单击 **ellipsis icon › Edit settings**。

   此时将显示"编辑快照组设置"窗口。

3. 根据需要更改快照组的设置。

   ▼ 字段详细信息

正在设置 …	**Description**
• Snapshot组设置*	Name
快照组的名称。需要为快照组指定名称。	快照镜像自动删除
一种将组中的快照映像总数保持在或低于用户定义的最大值的设置。启用此选项后、System Manager会在创建新快照时自动删除组中最早的快照映像、以符合组允许的最大快照映像数。	Snapshot映像限制
一个可配置的值、用于指定快照组允许的最大快照映像数。	预留容量设置

正在设置 …	Description
在以下情况下提醒我…	使用spinner框调整当快照组的预留容量接近全满时System Manager发送警报通知的百分比。 当快照组的预留容量超过指定阈值时、System Manager会发送警报、以便您有时间增加预留容量或删除不必要的对象。
预留容量全满的策略	您可以选择以下策略之一： • 清除最旧的快照映像- System Manager会自动清除快照组中最旧的快照映像、从而释放快照映像预留容量、以便在组中重复使用。 • 拒绝向基础卷写入数据-当预留容量达到其最大定义百分比时、System Manager将拒绝向基础卷发出的任何I/O写入请求、此请求会触发预留容量访问。

4. 单击*保存*将所做的更改应用于快照组设置。

在 **SANtricity System Manager** 中更改快照卷的预留容量设置

您可以更改快照卷的设置、以调整当快照卷的预留容量接近全满时系统发送警报通知的百分比点。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要编辑的快照卷，然后单击 **ellipsis icon › Edit settings**。

   此时将显示 Edit Snapshot Volume Reserved Capacity Settings（编辑快照卷保留容量设置）窗口。

3. 根据需要更改快照卷的预留容量设置。

   ▼ 字段详细信息

正在设置 …	Description
在以下情况下提醒我…	使用spinner框调整当成员卷的预留容量接近全满时系统发送警报通知的百分比点。 当快照卷的预留容量超过指定阈值时、系统会发送警报、以便您有时间增加预留容量或删除不必要的对象。

4. 单击*保存*将更改应用于快照卷预留容量设置。

在 **SANtricity System Manager** 中更改一致性组成员卷的预留容量设置

您可以更改一致性组成员卷的设置、以调整SANtricity系统管理器在成员卷的预留容量接近全满时发送警报通知的百分比值、并更改在预留容量达到其最大定义百分比时要使用的策略。

关于此任务

更改单个成员卷的预留容量设置还会更改与一致性组关联的所有成员卷的预留容量设置。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要编辑的一致性组成员卷，然后单击菜单：省略号图标[编辑设置]。

   此时将显示编辑一致性组成员卷窗口。

3. 根据需要更改成员卷的预留容量设置。

   ▼ 字段详细信息

正在设置 ...	Description
预留容量已满警报阈值	使用此栏可调整 System Manager 在成员卷的保留容量接近满时发送警报通知的百分比点。 当成员卷的预留容量超过指定阈值时、System Manager会发送警报、以便您有时间增加预留容量或删除不必要的对象。 更改一个成员卷的警报设置将更改属于同一一致性组的_all_成员卷的警报设置。
预留容量全满的策略	您可以选择以下策略之一： • 清除最旧的快照映像- System Manager会自动清除一致性组中最早的快照映像、从而释放成员的预留容量、以便在组中重复使用。 • 拒绝向基础卷写入数据-当预留容量达到其最大定义百分比时、System Manager将拒绝向基础卷发出的任何I/O写入请求、此请求会触发预留容量访问。

4. 单击*保存*以应用所做的更改。

结果

System Manager会更改成员卷的预留容量设置、以及一致性组中所有成员卷的预留容量设置。

在 **SANtricity System Manager** 中更改镜像对卷的预留容量设置

您可以更改镜像对卷的设置、以调整SANtricity系统管理器在镜像对卷的预留容量接近全满时发送警报通知的百分比。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要编辑的镜像对卷，然后单击 **ellipsis icon › Edit settings**。

   此时将显示 Edit Mirrored Pair Volume Reserved Capacity Settings（编辑镜像对卷保留容量设置）窗口。

3. 根据需要更改镜像对卷的预留容量设置。

   ▼ 字段详细信息

正在设置 ...	Description
预留容量已满警报阈值	当镜像对的保留容量接近满时，使用条形图调整 System Manager 发送警报通知的百分比点。 当镜像对的预留容量超过指定阈值时、System Manager将发送警报、以便有时间增加预留容量。 更改一个镜像对的警报设置会更改属于同一镜像一致性组的所有镜像对的警报设置。

4. 单击*保存*以应用所做的更改。

取消 SANtricity System Manager 中的待处理快照映像

您可以在待定快照映像完成之前将其取消。快照会异步执行、快照的状态为待定、直到快照完成为止。同步操作完成后、快照映像即会完成。

关于此任务

由于以下并发条件、快照映像处于"Pending"状态：

- 某个快照组的基础卷或包含此快照映像的一致性组的一个或多个成员卷是异步镜像组的成员。
- 卷当前正在执行异步镜像同步操作。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要取消挂起快照映像的快照组，然后单击菜单：省略号图标[取消挂起快照映像]。
3. 单击*是*确认要取消待定快照映像。

在 SANtricity System Manager 中删除快照组

如果要永久删除快照组的数据并将其从系统中删除、则可以删除该快照组。删除快照组会回收预留容量、以便在池或卷组中重复使用。

关于此任务

删除快照组后、该组中的所有快照映像也会被删除。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要删除的快照组，然后单击菜单：省略号图标 [Delete]。

   此时将显示确认删除Snapshot组对话框。

3. 键入`delete`进行确认。

结果

System Manager将执行以下操作：

- 删除与快照组关联的所有快照映像。
- 禁用与快照组的映像关联的任何快照卷。
- 删除为快照组预留的容量。

SANtricity System Manager 的池和卷组常见问题解答

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。

什么是卷组?

卷组是具有共享特征的卷的容器。卷组已定义容量和RAID级别。您可以使用卷组创建一个或多个可供主机访问的卷。(您可以从卷组或池创建卷。)

什么是池?

池是指一组按逻辑分组的驱动器。您可以使用池创建一个或多个可供主机访问的卷。(您可以从池或卷组创建卷。)

通过池、管理员无需监控每个主机上的使用情况、即可确定存储空间何时可能用尽、并避免传统的磁盘大小调整中断。当池即将耗尽时、可以无中断地向池中添加更多驱动器、并且容量增长对主机是透明的。

对于池、数据会自动重新分布以保持平衡。通过在池中分布奇偶校验信息和备用容量、可以使用池中的每个驱动器重建故障驱动器。此方法不使用专用热备用驱动器、而是在整个池中保留保留(备用)容量。驱动器发生故障时、系统会读取其他驱动器上的区块以重新创建数据。然后、选择一个新驱动器来写入故障驱动器上的每个区块、以便在驱动器之间保持数据分布。

什么是预留容量?

预留容量是指物理分配的容量、用于存储Snapshot映像、一致性组成员卷和镜像对卷等副本服务对象的数据。

与复制服务操作关联的预留容量卷位于池或卷组中。您可以从池或卷组创建预留容量。

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。

池和卷组之间有何区别?

池与卷组类似、但存在以下差异。

- 池中的数据随机存储在池中的所有驱动器上、而卷组中的数据则存储在同一组驱动器上。
- 驱动器发生故障时、池的性能下降较小、重建所需时间也较短。
- 池具有内置的保留容量、因此不需要专用的热备用驱动器。
- 池允许对大量驱动器进行分组。
- 池不需要指定的RAID级别。

为什么要手动配置池?

以下示例说明了您希望手动配置池的原因。

- 如果存储阵列上有多个应用程序、并且不希望它们争用相同的驱动器资源、则可以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。

  要手动创建池：选择 **Storage**，然后选择 **Pools and volume groups**。从 All Capacity 选项卡中，单击菜单：Create[Pool]。

- 如果存在多个驱动器类型相同的池、则会显示一条消息、指示System Manager无法自动为池推荐驱动器。但是、您可以手动将驱动器添加到现有池。

  要手动将驱动器添加到现有池：从池和卷组页面，找到池，然后单击 **Add capacity**。

容量警报为何重要?

容量警报指示何时向池添加驱动器。池需要足够的可用容量才能成功执行存储阵列操作。您可以通过将SANtricity系统管理器配置为在池的可用容量达到或超过指定百分比时发送警报来防止这些操作中断。

在使用*池自动配置*选项或*创建池*选项创建池时，可以设置此百分比。如果您选择自动选项，默认设置会自动确定您何时收到警报通知。如果选择手动创建池，则可以确定警报通知设置；如果愿意，则可以接受默认设置。您可以稍后从 **Storage › Pools and volume groups** 调整这些设置。选择池，单击 **ellipsis icon › Edit settings**，然后更新*容量警报设置*。

当池中的可用容量达到指定百分比时、将使用您在警报配置中指定的方法发送警报通知。

为什么我无法提高我的保存能力？

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 **View/Edit Settings**，然后选择 **Settings** 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。

可以从池中删除的驱动器数量是否有限制？

SANtricity系统管理器会为您可以从池中删除的驱动器数量设置限制。

- 您不能将池中的驱动器数量减少到最低阈值以下。对于 EF80 和 EF50 系统，性能池最少为 6 个驱动器，容量池最少为 12 个驱动器。对于所有其他系统，最少 11 个驱动器。
- 如果池中没有足够的可用容量来容纳已删除驱动器中的数据、则在将该数据重新分配到池中的其余驱动器时、您无法删除驱动器。
- 一次最多可以删除60个驱动器。如果选择的驱动器超过60个、则删除驱动器选项将被禁用。如果需要删除60个以上的驱动器、请重复执行删除驱动器操作。

驱动器支持哪些介质类型？

支持以下介质类型：硬盘驱动器(HDD)和固态磁盘(SSD)。

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：
  - 采用固态磁盘(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
  - 性能和容量 NVMe SSD 驱动器（仅限 EF80 和 EF50 系统）
- 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。

如何维护磁盘架/抽屉丢失保护?

要为池或卷组维护磁盘架/抽屉丢失保护、请使用下表中指定的标准。

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
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。

池和卷组的最佳驱动器定位是什么?

创建池和卷组时、请确保在上部和下部驱动器插槽之间平衡驱动器选择。

对于EF600和EF300控制器、驱动器插槽0-11连接到一个PCI网桥、而插槽12-23连接到另一个PCI网桥。为了获得最佳性能、您应平衡驱动器选择、使其包含上插槽和下插槽中的驱动器数量大致相等。这种定位可确保卷不会比需要时更早地达到带宽限制。

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_levels_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。
- 工作原理
  - 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。
  - 卷组中必须有偶数个驱动器。如果您没有偶数个驱动器，并且还有一些未分配的驱动器，请转到*池和卷组*以向卷组添加其他驱动器，然后重试该操作。
  - 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。

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、查找"DA"旁边的"Yes")。

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、 NVMe/RoCE和iSER over InfiniBand (适用于RDMA/IB的iSCSI扩展)。基于InfiniBand的SRP不支持DA。

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。

增加预留容量需要了解哪些信息?

通常、当您收到警告、指出预留容量可能会变满时、应增加容量。您只能以8 GiB为增量增加预留容量。

- 池或卷组中必须有足够的可用容量、以便可以根据需要进行扩展。

  如果任何池或卷组上没有可用容量、则可以将未使用的驱动器形式的未分配容量添加到池或卷组中。

- 池或卷组中的卷必须处于最佳状态、并且不能处于任何修改状态。
- 要用于增加容量的池或卷组中必须存在可用容量。
- 您不能增加只读快照卷的预留容量。只有读写Snapshot卷才需要预留容量。

对于快照操作、预留容量通常为基础卷的40%。对于异步镜像操作、预留容量通常为基础卷的20%。如果您认为基础卷会发生许多更改、或者存储对象的复制服务操作的预计预期寿命很长、请使用较高的百分比。

为什么我不能选择其他要减少的金额?

您只能将预留容量减少到用于增加的容量。只能按与添加成员卷相反的顺序删除为其预留的容量。

如果存在以下条件之一、则不能减少存储对象的预留容量：

- 存储对象是镜像对卷。
- 存储对象仅包含一个用于预留容量的卷。存储对象必须至少包含两个用于预留容量的卷。
- 存储对象是已禁用的快照卷。
- 存储对象包含一个或多个关联的快照映像。

您只能按与添加卷相反的顺序删除预留容量卷。

您不能减少只读快照卷的预留容量、因为它没有任何关联的预留容量。只有读写Snapshot卷才需要预留容量。

为什么需要为每个成员卷预留容量?

快照一致性组中的每个成员卷都必须有自己的预留容量、才能将主机应用程序所做的任何修改保存到基础卷、而不会影响引用的一致性组快照映像。通过预留容量、主机应用程序可以对成员卷中指定为读写的数据副本进行写入访问。

主机无法直接读取或写入一致性组快照映像。而是使用快照映像仅保存从基础卷捕获的数据。

在创建指定为读写的一致性组快照卷期间、System Manager会为一致性组中的每个成员卷创建一个预留容量。通过此预留容量、主机应用程序可以对一致性组快照映像中所含数据的副本进行写入访问。

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 Cache 统计信息，请从左侧面板中选择菜单：Storage[Pools and volume groups]。选择要查看其统计信息的 SSD Cache，然后单击菜单：省略号图标[View statistics]。标称统计信息显示在 View Statistics 页面上。

以下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。

标称统计信息	**Description**
读取/写入	主机从启用了SSD缓存的卷读取数据或主机写入数据的总数。比较读取与写入之间的关系。要实现有效的SSD缓存操作、读取次数必须大于写入次数。读取与写入的比率越大、缓存的运行就越好。
缓存命中	缓存命中数的计数。
缓存命中率(%)	派生自缓存命中/(读取+写入)。对于有效的SSD缓存操作、缓存命中百分比应大于50%。少量数字可能表示以下几个方面： • 读取与写入的比率太小 • 不会重复读取 • 缓存容量太小
缓存分配(%)	分配的SSD缓存存储容量、以此控制器可用的SSD缓存存储的百分比表示。源自已分配的字节/可用字节。缓存分配百分比通常显示为100%。如果此数字小于100%、则表示缓存尚未预热或SSD缓存容量大于所访问的所有数据。在后一种情况下、较小的SSD缓存容量可以提供相同级别的性能。请注意、这并不表示缓存的数据已放置到SSD缓存中；它只是一个准备步骤、然后才能将数据放置到SSD缓存中。
缓存利用率(%)	包含已启用卷中的数据的SSD缓存存储容量、以分配的SSD缓存存储百分比表示。此值表示SSD缓存的利用率或密度、该缓存是从用户数据字节/已分配字节派生的。缓存利用率百分比通常低于100%、可能要低得多。此数字显示已填充缓存数据的SSD缓存容量百分比。此数字低于100%、因为SSD缓存的每个分配单元(SSD缓存块)都划分为称为子块的较小单元、这些子块在一定程度上是独立填充的。数字越高通常越好、但即使数字越小、性能也会显著提高。

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。

查看`.csv`文件时、请注意、详细统计信息列在标称统计信息之后：

详细统计信息	**Description**
读取块	主机读取中的块数。
写入块	主机写入的块数。
完整命中块	缓存命中中的块数。完整命中块表示已从SSD缓存中完全读取的块数。SSD缓存只会对完全缓存命中的操作的性能产生影响。
部分命中	至少有一个块(而不是所有块)位于SSD缓存中的主机读取次数。部分命中是SSD缓存*未命中*、其中从基础卷读取的结果已满足。
Partial Hits—块	部分命中中的块数。部分缓存命中和部分缓存命中块是由于在SSD缓存中仅包含一部分数据的操作而导致的。在这种情况下、操作必须从缓存的硬盘驱动器(HDD)卷中获取数据。SSD缓存不会为这种类型的命中带来任何性能优势。如果部分缓存命中块数高于完整缓存命中块数、则不同的I/O特征类型(文件系统、数据库或Web服务器)可以提高性能。在SSD缓存预热期间、与缓存命中相比、部分命中和未命中的数量预计会更多。
未命中	SSD缓存中没有块的主机读取次数。如果满足从基础卷读取的要求、则会发生SSD缓存未命中。在SSD缓存预热期间、与缓存命中相比、部分命中和未命中的数量预计会更多。
未命中—块	未命中的块数。
填充操作(主机读取)	将数据从基础卷复制到SSD缓存的主机读取次数。
填充操作(主机读取)—块	填充操作(主机读取)中的块数。
填充操作(主机写入)	将数据从基础卷复制到SSD缓存的主机写入次数。对于因写入I/O操作而未填充缓存的缓存配置设置、填充操作(主机写入)计数可能为零。
填充操作(主机写入)—块	填充操作(主机写入)中的块数。
使操作失效	数据失效或从SSD缓存中删除的次数。对于每个主机写入请求、每个具有强制单元访问(FUA)的主机读取请求、每个验证请求以及某些其他情况、都会执行缓存失效操作。
回收操作	SSD缓存块重新用于另一个基础卷和/或不同逻辑块寻址(Logical Block Addressing、LBA)范围的次数。为了有效地执行缓存操作、与读取和写入操作的总数相比、回收的数量必须较小。如果回收操作的数量接近读取和写入的总数、则SSD缓存将会达到最大值。需要增加缓存容量或工作负载不适合与SSD缓存一起使用。
可用字节数	SSD缓存中可供此控制器使用的字节数。
已分配字节	此控制器从SSD缓存分配的字节数。从SSD缓存分配的字节数可能为空、或者可能包含基础卷中的数据。
用户数据字节	SSD缓存中包含基础卷中的数据的已分配字节数。可用字节数、已分配字节数和用户数据字节数用于计算缓存分配百分比和缓存利用率百分比。

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、未分配的容量包括池的保留容量、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。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。"池设置"对话框中的"其他优化容量"滑块可用于调整池的优化容量。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 EF80、EF50、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。

附加优化容量滑块仅适用于 EF80、EF50、EF600 和 EF300 存储系统。

什么是资源配置功能?

资源调配是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。

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命令或SCSI Unmap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?

资源调配是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。

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命令或SCSI Unmap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。

默认情况下，在驱动器支持 DULBE 的系统上，资源调配处于启用状态。您可以从*池和卷组*禁用该默认设置。

卷和工作负载

了解 **SANtricity System Manager** 中的卷和工作负载

您可以将卷创建为容器、以便应用程序、数据库和文件系统存储数据。创建卷时、您还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。

什么是卷和工作负载?

卷是使用特定容量为主机创建的逻辑组件、可供主机访问。尽管一个卷可能包含多个驱动器、但一个卷在主机中显示为一个逻辑组件。定义卷后、您可以将其添加到工作负载中。工作负载_是支持SQL Server或Exchange等应用程序的存储对象、您可以使用此对象优化该应用程序的存储。

了解更多信息。

- "卷的工作原理"
- "工作负载的工作原理"
- "卷术语"
- "如何为卷分配容量"
- "您可以对卷执行的操作"

如何创建卷和工作负载?

首先、创建工作负载。转到菜单：Storage[Volumes]、然后打开一个向导以指导您完成这些步骤。接下来、您可以使用池或卷组中的可用容量创建卷、然后分配您创建的工作负载。

了解更多信息。

- "用于创建卷的工作流"
- "创建工作负载"
- "创建卷"
- "将卷添加到工作负载"

相关信息

详细了解与卷相关的概念：

- "卷的数据完整性和数据安全性"
- "SSD缓存和卷"
- "精简卷监控"

概念

SANtricity 软件中的卷工作原理

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、并轻松组织和使用系统资源。这一概念类似于在计算机上使用文件夹/目录来组织文件、以便于轻松快速地访问。

卷是主机唯一可见的数据层。在SAN环境中、卷会映射到主机可以看到的逻辑单元号(LUN)。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(包括FC、iSCSI和SAS)访问的用户数据。

可以从池和卷组创建的卷类型

卷从池或卷组中提取容量。您可以从存储阵列上的池或卷组创建以下类型的卷。

- 从池—您可以从池中创建卷、使其成为_Fully Provisioned (thick) volumes_或_thiny-provisioned (thin) volumes_

> System Manager界面不提供创建精简卷的选项。如果要创建精简卷、请使用命令行界面(CLI)。

- 从卷组—您只能从卷组创建卷作为完全配置(厚)卷_。

厚卷和精简卷通过不同方式从存储阵列中提取容量：

- 厚卷的容量是在创建该卷时分配的。
- 写入到精简卷时、精简卷的容量将作为数据进行分配。

精简配置有助于避免浪费已分配的容量、并可节省企业前期存储成本。但是、完全配置的优势在于延迟更短、因为在创建厚卷时会一次性分配所有存储。

> EF80、EF50、EF600/EF600C 和 EF300/EF300C 存储系统不支持精简配置。

卷的特征

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`"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。

- 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。

SANtricity 软件中的工作负载工作原理

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。

创建工作负载

您必须手动指定何时要创建未与特定应用程序关联的工作负载。您还必须使用添加卷页面手动指定卷配置。

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SANtricity 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 Volumes 页面中的 **Applications and workloads** 选项卡，以查看按工作负载和工作负载关联的应用程序类型分组的存储阵列的卷。
- 您可以选择性能页面中的*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 MB ）。对象按应用程序和相关工作负载分组。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，这有助于调查与 I/O 性能相关的问题。

了解 **SANtricity** 软件中的卷术语

了解卷术语如何应用于存储阵列。

所有卷类型

期限	**Description**
已分配容量	您可以使用已分配的容量创建卷并执行复制服务操作。 对于厚卷、分配的容量和报告的容量相同、但对于精简卷、分配的容量和报告的容量不同。对于厚卷、物理分配的空间等于向主机报告的空间。对于精简卷、报告的容量是指向主机报告的容量、而分配的容量是指当前为写入数据而分配的驱动器空间量。
应用程序	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。
Capacity	容量是指可存储在卷中的数据量。

期限	Description
控制器所有权	控制器所有权用于定义指定为卷的拥有或主控制器的控制器。卷可以具有一个"`拥有`"卷的首选控制器(A或B)。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。
动态缓存读取预取	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。 对于精简卷、动态缓存读取预取始终处于禁用状态、并且无法更改。
可用容量区域	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。在卷组中创建具有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。 通过整合可用容量、您可以从卷组中的最大可用容量创建更多卷。
主机	主机是指向存储阵列上的卷发送I/O的服务器。
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。
热备用驱动器	只有卷组才支持热备用驱动器。热备用驱动器不包含任何数据、并在卷组中包含的RAID 1、RAID 3、RAID 5或RAID 6卷中的驱动器发生故障时充当备用驱动器。热备用驱动器可为存储阵列添加另一个冗余级别。
LUN	逻辑单元号(LUN)是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。
介质扫描	通过介质扫描、可以在正常读取或写入驱动器期间检测到驱动器介质错误。介质扫描作为后台操作执行、并扫描定义的用户卷中的所有数据和冗余信息。
命名空间	命名空间是指为块访问而格式化的NVM存储。它类似于SCSI中的逻辑单元、它与存储阵列中的卷相关。
池	池是指一组按逻辑分组的驱动器。您可以使用池创建一个或多个可供主机访问的卷。(您可以从池或卷组创建卷。)
池或卷组容量	池、卷或卷组容量是指存储阵列中已分配给池或卷组的容量。此容量用于创建卷并满足副本服务操作和存储对象的各种容量需求。
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。

期限	Description
已报告容量	报告的容量是指向主机报告并可由主机访问的容量。 对于厚卷、报告的容量和分配的容量相同、但对于精简卷、报告的容量和分配的容量不同。对于厚卷、物理分配的空间等于向主机报告的空间。对于精简卷、报告的容量是指向主机报告的容量、而分配的容量是指当前为写入数据而分配的驱动器空间量。
区块大小	区块是指存储阵列移至条带中的下一个驱动器(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。
条带化	条带化是一种将数据存储在存储阵列上的方式。条带化会将数据流拆分为特定大小的块(称为"块大小")、然后将这些块逐个写入驱动器。这种数据存储方式用于在多个物理驱动器之间分布和存储数据。条带化是RAID 0的同义词、它会在RAID组中的所有驱动器之间分布数据、而不进行奇偶校验。
Volume	卷是应用程序，数据库和文件系统用于存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。
卷分配	卷分配是将主机LUN分配给卷的方式。
Volume name	卷名是创建卷时分配给卷的字符串。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存储在卷中的数据类型。标准卷和精简卷名称的最大长度为 60 个字符。名称必须是唯一的。只有标准卷和精简卷的名称可以超过 30 个字符。 如果存在名称大于 30 个字符的标准卷或精简卷，则不支持降级到 SANtricity 操作系统软件版本 11.90 或更早版本。如果您计划降级到 SANtricity 操作系统软件版本 11.90 或更早版本，请在降级前更改名称大于 30 个字符的任何标准卷或精简卷的名称。
卷组	卷组是具有共享特征的卷的容器。卷组已定义容量和RAID级别。您可以使用卷组创建一个或多个可供主机访问的卷。(您可以从卷组或池创建卷。)
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。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。
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。
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。
无电池写入缓存	不使用电池的写入缓存设置允许写入缓存继续运行、即使电池缺失、出现故障、已完全放电或未完全充电也是如此。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。

特定于精简卷

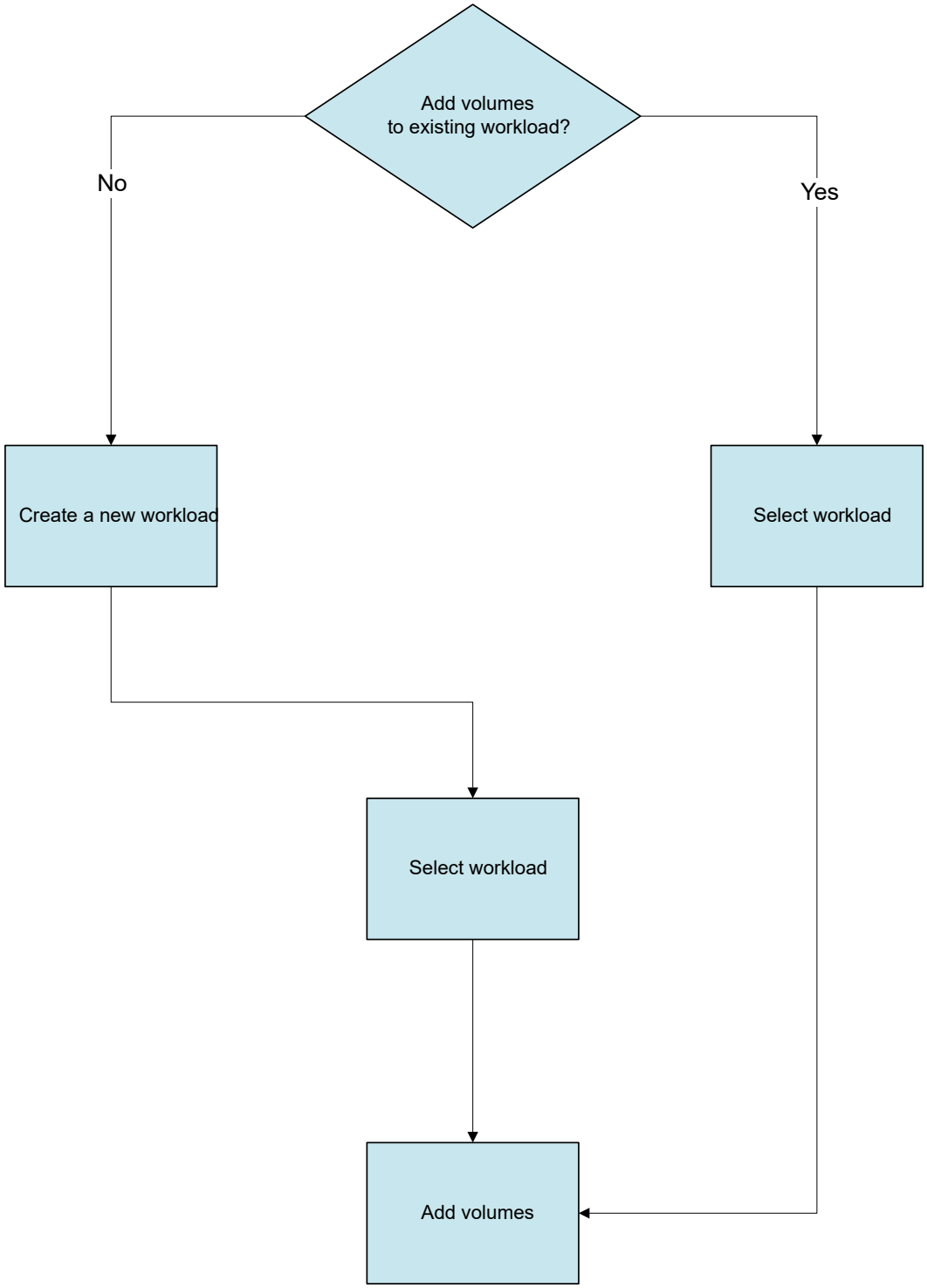
System Manager不提供创建精简卷的选项。如果要创建精简卷、请使用命令行界面(CLI)。

EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上没有可用的精简卷。

期限	**Description**
已分配容量限制	已分配容量限制是指为精简卷分配的物理容量增长的上限。
写入容量	写入容量是指从为精简卷分配的预留容量中写入的容量。
警告阈值	您可以设置一个警告阈值警报、以便在为精简卷分配的容量达到全满百分比(警告阈值)时发出此警报。

如何在 **SANtricity System Manager** 中创建卷

在SANtricity 系统管理器中、您可以按照以下步骤创建卷。


Add volumes
to existing workload?
No
Yes
Create a new workload
Select workload
Select workload
Add volumes

您可以使卷使用数据保证(Data Assurance、DA)功能和驱动器安全功能。这些功能在池和卷组级别提供。

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、查找"DA"旁边的"Yes")。

驱动器安全性

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、也可以是经认证符合联邦信息处理标准140-2级别2 (FIPS驱动器)的驱动器。

驱动器安全在驱动器级别的工作原理

支持安全的驱动器(FDE或FIPS)可在写入期间对数据进行加密、并在读取期间对数据进行解密。此加密和解密不会影响性能或用户工作流。每个驱动器都有自己唯一的加密密钥、永远不能从该驱动器传输该密钥。

驱动器安全在卷级别的工作原理

从支持安全的驱动器创建池或卷组时、您还可以为这些池或卷组启用驱动器安全性。"驱动器安全性"选项可确保驱动器以及关联的卷组和池的安全-*enabled*.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。

如何实施驱动器安全性

要实施驱动器安全性、请执行以下步骤。

1. 为存储阵列配备支持安全保护的驱动器、可以是FDE驱动器、也可以是FIPS驱动器。(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。)
2. 创建一个安全密钥、该密钥是一个字符串、由控制器和驱动器共享、用于进行读/写访问。您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。对于外部密钥管理、必须使用密钥管理服务器建立身份验证。
3. 为池和卷组启用驱动器安全性：
   - 创建池或卷组(在候选项表的*安全功能*列中查找*是*)。
   - 创建新卷时、请选择池或卷组(在Pool and volume group candidates表中、查找*安全功能*旁边的*是*)。

     使用驱动器安全功能、您可以创建一个安全密钥、该安全密钥可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。无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。

了解 **SANtricity** 软件中的 **SSD** 缓存和卷

您可以将卷添加到SSD缓存中以提高只读性能。SSD缓存由一组固态磁盘(SSD)驱动器组成、这些驱动器会在存储阵列中进行逻辑分组。

Volumes

使用简单的卷I/O机制将数据移入和移出SSD缓存。在缓存数据并将其存储在SSD上后、随后会在SSD缓存上执行这些数据的读取、从而无需访问HDD卷。

SSD缓存是一种二级缓存、可与控制器动态随机存取存储器(DRAM)中的主缓存结合使用。

- 在主缓存中、数据会在主机读取后存储在DRAM中。
- 在SSD缓存中、数据会从卷中复制并存储在两个内部RAID卷(每个控制器一个)上、这两个卷在创建SSD缓存时会自动创建。

内部RAID卷用于内部缓存处理。这些卷不可访问或显示在用户界面中。但是、这两个卷会计入存储阵列中允许的卷总数。



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。

驱动器安全功能

要在同时使用驱动器安全(已启用安全保护)的卷上使用SSD缓存、该卷的驱动器安全功能必须与SSD缓存匹配。如果不匹配、则此卷将不会启用安全保护。

您可以在 **SANtricity System Manager** 中对卷执行的操作

您可以对卷执行多种不同的操作：增加容量、删除、复制、初始化、重新分发、 更改所有权、更改缓存设置以及更改介质扫描设置。

增加容量

您可以通过两种方式扩展卷的容量：

- 使用池或卷组中的可用容量。

  您可以通过从左侧面板中选择菜单：Storage[Volumes]，然后为该卷选择菜单：ellipsis icon[Increase capacity] 来向卷添加容量。

- 将未分配的容量(以未使用的驱动器的形式)添加到卷的池或卷组。如果池或卷组中没有可用容量、请使用此选项。

  您可以通过选择菜单：Storage[Pools and volume groups > Add capacity]，将未分配的容量添加到池或卷组。

  如果池或卷组中没有可用容量、则无法增加卷的容量。您必须先增加池或卷组的大小、或者删除未使用的卷。

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。

删除

通常、如果创建的卷参数或容量不正确、不再满足存储配置需求或不再需要用于备份或应用程序测试的快照映像、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。删除卷还会删除任何关联的快照映像、计划和快照卷、并删除任何镜像关系。

复制

复制卷时，需要在同一存储阵列上创建两个独立卷（源卷和目标卷）的时间点副本。您可以通过选择菜单：Storage[Volumes]，然后选择菜单：省略号图标[Copy volume] 来复制卷。

初始化

初始化卷会擦除卷中的所有数据。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。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。

您可以通过选择菜单：Storage[Volumes > 省略号图标 > Initialize volumes] 来初始化卷。

重新分布

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。

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。

您可以通过选择菜单：Storage[Volumes > 省略号图标 > Redistribute volumes] 来重新分配卷。

更改卷所有权

更改卷的所有权会更改卷的首选控制器所有权。卷的首选控制器所有者列在菜单：Storage[Volumes > ellipsis icon > View settings]下。

您可以通过选择菜单：Storage[Volumes > 省略号图标 > Change volume ownership] 来更改卷的所有权。

镜像和卷所有权

如果镜像对的主卷属于控制器A、则二级卷也属于远程存储阵列的控制器A。更改主卷的所有者将自动更改二级卷的所有者、以确保这两个卷都属于同一控制器。主端的当前所有权更改会自动传播到辅端的相应当前所有权更改。

如果镜像一致性组包含一个本地二级卷且控制器所有权发生更改、则在首次写入操作时、二级卷会自动传输回其原始控制器所有者。您不能使用*更改所有权*选项更改二级卷的控制器所有权。

复制卷和卷所有权

在复制卷操作期间、同一控制器必须同时拥有源卷和目标卷。有时、在复制卷操作开始时、两个卷都没有相同的首选控制器。因此、目标卷的所有权会自动传输到源卷的首选控制器。卷复制完成或停止后、目标卷的所有权将

恢复到其首选控制器。

如果在复制卷操作期间更改了源卷的所有权、则也会更改目标卷的所有权。在某些操作系统环境下、可能需要先重新配置多路径主机驱动程序、然后才能使用I/O路径。(某些多路径驱动程序需要进行编辑才能识别I/O路径。有关详细信息、请参见驱动程序文档。)

更改缓存设置

缓存是控制器上的临时易失性存储(RAM)区域、其访问速度比驱动器介质更快。如果使用缓存、则可以提高整体I/O性能、原因如下：

- 从主机请求读取的数据可能已位于先前操作的缓存中、因此无需访问驱动器。
- 写入数据最初会写入缓存、这样、应用程序就可以继续运行、而无需等待数据写入驱动器。

选择菜单：Storage[Volumes > 省略号图标 > Change cache settings] 以更改以下缓存设置：

- 读取和写入缓存—读取缓存是一个缓冲区、用于存储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。

- 使用镜像写入缓存-如果写入一个控制器的缓存内存中的数据也写入另一个控制器的缓存中、则使用镜像进行写入缓存。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。
- 无电池写入缓存—无电池写入缓存设置允许写入缓存继续运行、即使电池缺失、出现故障、已完全放电或未完全充电也是如此。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。

  只有在启用写入缓存时、此设置才可用。此设置不适用于精简卷。

- 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。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。

  对于精简卷、动态缓存读取预取始终处于禁用状态、并且无法更改。

更改介质扫描设置

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。如果池或卷组中的其他驱动器发生故障、则此扫描可以防止发生数据丢失、因为故障驱动器的数据是使用池或卷组中其他驱动器的冗余信息和数据重建的。

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。

您可以通过选择菜单：Storage[卷 > 省略号图标 > 更改介质扫描设置]来启用和设置介质扫描运行的持续时间。

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。

如何在 **SANtricity System Manager** 中分配卷容量

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。

使用容量创建和扩展卷

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、您要在已有的池或卷组上创建额外的卷。

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。

厚卷和精简卷的容量类型

您可以创建厚卷或精简卷。对于厚卷、报告的容量和分配的容量相同、但对于精简卷、报告的容量和分配的容量不同。

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

- 对于精简卷、报告的容量是指向主机报告的容量、而分配的容量是指当前为写入数据而分配的驱动器空间量。

  报告的容量可能大于存储阵列上分配的容量。可以调整精简卷的大小以适应增长、而不考虑当前可用资产。

> SANtricity System Manager不提供创建精简卷的选项。如果要创建精简卷、请使用命令行界面(CLI)。

厚卷的容量限制

厚卷的最小容量为1 MiB、最大容量由池或卷组中驱动器的数量和容量决定。

增加厚卷的报告容量时、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。

精简卷的容量限制

您可以创建报告容量较大且分配容量相对较小的精简卷、这有利于提高存储利用率和效率。精简卷有助于简化存储管理、因为分配的容量可以随着应用程序需求的变化而增加、而不会中断应用程序、从而提高存储利用率。

除了报告的容量和分配的容量之外、精简卷还包含写入容量。写入容量是指从为精简卷分配的预留容量中写入的容量。

下表列出了精简卷的容量限制。

容量类型	最小大小	最大大小
已报告	32 MiB	256 TiB
已分配	4 MiB	64 TiB

对于精简卷、如果已达到报告的最大容量256 TiB、则无法增加其容量。确保精简卷的预留容量设置为大于报告的最大容量的大小。

系统会根据已分配的容量限制自动扩展已分配的容量。通过分配的容量限制、您可以将精简卷的自动增长限制为低于报告的容量。当写入的数据量接近分配的容量时、您可以更改分配的容量限制。

要更改分配的容量限制，请选择菜单：Storage[Thin volume monitoring > Change Limit]。

由于System Manager在创建精简卷时不会分配全部容量、因此池中可能存在不足的可用容量。空间不足不仅会阻止对精简卷的写入、还会阻止对需要池中容量的其他操作(例如、快照映像或快照卷)的写入。但是、您仍然可以从池执行读取操作。如果发生这种情况、您将收到警报阈值警告。

了解 **SANtricity** 软件中的精简卷监控

您可以监控精简卷的空间并生成适当的警报、以防止出现容量不足的情况。

精简配置的环境可以比底层物理存储分配更多的逻辑空间。您可以选择菜单：存储[精简卷监控]，以监控精简卷在达到分配容量最大限制之前的增长程度。

您可以使用"精简监控"视图执行以下操作：

- 定义限制精简卷可自动扩展到的已分配容量的限制。
- 设置将警报（超过警告阈值）发送到通知区域的百分比点，当精简卷接近最大分配容量限制时，可通过窗口上角的铃铛图标访问该区域。

要增加精简卷的容量、请增加其报告的容量。

System Manager不提供创建精简卷的选项。如果要创建精简卷、请使用命令行界面(CLI)。

EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上没有可用的精简卷。

了解 **SANtricity** 软件中的厚卷和薄卷

厚卷始终为完全配置卷、这意味着在创建卷时会分配所有容量。精简卷始终采用精简配置、这意味着在将数据写入卷时会分配容量。

System Manager不提供创建精简卷的选项。如果要创建精简卷、请使用命令行界面(CLI)。

Volume type	Description
厚卷	• 厚卷是从池或卷组创建的。 • 对于厚卷、预先提供大量存储空间、以满足未来的存储需求。 • 厚卷是使用创建卷时在物理存储上预先分配的卷的整个大小创建的。这种预分配意味着、创建100 GiB卷实际上会占用驱动器上已分配的100 GiB容量。但是、此空间可能会保持未使用状态、从而导致存储容量利用率不足。 • 创建厚卷时、请确保不要为单个卷过度分配容量。单个卷的容量过度分配可能会迅速占用系统中的所有物理存储。 • 请注意、复制服务(Snapshot映像、Snapshot卷、卷副本和异步镜像)也需要存储容量、因此请勿将所有容量分配给厚卷。空间不足可能会阻止对池或卷组的写入。如果发生这种情况、您将收到可用容量警报阈值警告。
精简卷	• 精简卷仅从池创建、而不是从卷组创建。 • 精简卷必须为RAID 6。 • EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上没有可用的精简卷。 • 您必须使用命令行界面创建精简卷。 • 与厚卷不同、精简卷所需的空间不会在创建期间分配、而是在稍后按需提供。 • 精简卷允许您过度分配其大小。也就是说、您可以分配大于卷大小的LUN。然后、您可以根据需要扩展卷(如有必要、可在此过程中添加驱动器)、而无需扩展LUN大小、因此无需断开用户连接。 • 您可以使用精简配置块空间回收(UNMAP)通过主机发出的SCSI UNMAP命令回收存储阵列上精简配置卷的块。支持精简配置的存储阵列可以重新利用回收的空间来满足同一存储阵列中其他精简配置卷的分配请求、从而可以更好地报告磁盘空间使用情况并更高效地利用资源。

精简卷限制

精简卷支持所有厚卷操作、但以下情况除外：

- 您不能更改精简卷的区块大小。
- 您不能为精简卷启用预读取冗余检查。
- 在复制卷操作中、不能使用精简卷作为目标卷。
- 您只能在异步镜像对的主端更改精简卷的已分配容量限制和警告阈值。主端对这些参数所做的任何更改都会自动传播到二级端。

配置存储

在 **SANtricity System Manager** 中创建工作负载

您可以为任何类型的应用程序创建工作负载。

关于此任务

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。

步骤

1. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 选择菜单：创建[工作负载]。

   此时将显示 Create Application Workload 页面。

3. 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。
4. 单击 * 创建 * 。

完成后

您已准备好向创建的工作负载添加存储容量。使用*创建卷*选项为应用程序创建一个或多个卷、并为每个卷分配特定容量。

在 **SANtricity System Manager** 中创建卷

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。此外、卷创建顺序还提供了一些选项、用于为要创建的每个卷分配特定容量。

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。某些应用程序类型在创建卷时应用了智能配置。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。System Manager可使用此信息为您创建最佳卷配置、并可根据需要对其进行编辑。

创建卷的过程分为多步操作步骤。

第**1**步：为卷选择主机

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。此外、卷创建顺序还提供了一些选项、用于为要创建的每个卷分配特定容量。

开始之前

- 主机页面下存在有效的主机或主机集群。
- 已为主机定义主机端口标识符。
- 在创建启用了DA的卷之前、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。

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. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 选择菜单：创建[卷]。

   此时将显示 Create Volumes 页面。
3. 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。
4. 要继续为选定主机或主机集群创建卷、请单击*下一步*、然后转到 [第2步：为卷选择工作负载]。

   此时将显示选择工作负载对话框。

第2步：为卷选择工作负载

选择一个工作负载以自定义特定应用程序的存储阵列配置、例如Microsoft SQL Server、Microsoft Exchange、视频监控应用程序或VMware。如果未列出要在此存储阵列上使用的应用程序、则可以选择"其他应用程序"。

关于此任务

此任务介绍如何为现有工作负载创建卷。

- 当您使用特定于应用程序的工作负载创建卷时，系统可能会推荐优化的卷配置，以最大限度地减少应用程序工作负载 I/O 与来自应用程序实例的其他流量之间的竞争。您可以使用"添加卷"页面查看推荐的卷配置，并编辑、添加或删除系统推荐的卷和特性。
- _使用"其他"_应用程序（或没有特定卷创建支持的应用程序）创建卷时，请使用"添加卷"页面手动指定卷配置。

步骤

1. 执行以下操作之一：
   - 选择*为现有工作负载创建卷*选项可为现有工作负载创建卷。
   - 选择*创建新工作负载*选项可为支持的应用程序或"其他"应用程序定义新的工作负载。
     - 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受支持的应用程序类型相关联，请输入所请求的信息；否则，请转到 步骤 3：添加卷。

步骤 **3**：添加卷

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 卷（EF80、EF600 和 EF600C）
  - 1,024 卷（EF50、EF300 和 EF300C）
  - 512 卷 (E4000)
- 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。

  ▼ 选择具有安全功能的池或卷组

  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System Manager的池和卷组级别提供。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。

  ▼ 选择具有安全功能的池或卷组

  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*)。

  驱动器安全功能在System Manager的池和卷组级别提供。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_encryption key_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

您可以从池或卷组创建卷。添加卷页面显示存储阵列上所有符合条件的池和卷组。对于每个符合条件的池和卷组，将显示可用的驱动器数量和可用总容量。

步骤

1. 在要用于创建一个或多个卷的每个池或卷组中，单击*添加新卷*。

   ▼ 字段详细信息

字段	Description
卷名称	在卷创建顺序期间，System Manager 将为卷分配默认名称。您可以接受默认名称，也可以提供更具描述性的名称来指示存储在卷中的数据类型。标准卷和精简卷名称的最大长度为 60 个字符。只有标准卷和精简卷的名称可以超过 30 个字符。名称必须是唯一的。 如果存在名称大于 30 个字符的标准卷或精简卷，则不支持降级到 SANtricity 操作系统软件版本 11.90 或更早版本。如果您计划降级到 SANtricity 操作系统软件版本 11.90 或更早版本，请在降级前更改名称大于 30 个字符的任何标准卷或精简卷的名称。
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。 池中的容量会根据驱动器类型以4 GiB或8 GiB为增量进行分配。分配的容量不是4 GiB或8 GiB的倍数、但不可用。要确保整个容量可用、请以4 GiB或8 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： • 512—512字节 • 4 k—4、096字节
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- System Manager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： • 主机的 I/O 负载 • 卷的修改优先级 • 卷组中的驱动器数量 • 驱动器通道的数量 • 存储阵列控制器的处理能力 更改卷的区块大小时， I/O 性能会受到影响，但数据仍可用。

字段	Description
支持安全保护	只有当池或卷组中的驱动器支持安全时、"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。
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。
资源调配（仅限 EF80 、EF50、EF300 和 EF600）	仅当驱动器支持此选项时，"Resource provisioned" 旁边才会显示 **Yes** 。Resource Provisioning 是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。

◦ 特定于应用程序的工作负载 — 单击 编辑卷 以更改、添加或删除选定工作负载的系统推荐卷和特性。

▼ 字段详细信息

字段	Description
卷名称	在卷创建顺序期间，System Manager 将为卷分配默认名称。您可以接受默认名称，也可以提供更具描述性的名称来指示存储在卷中的数据类型。标准卷和精简卷名称的最大长度为 60 个字符。名称必须是唯一的。只有标准卷和精简卷的名称可以超过 30 个字符。 如果存在名称大于 30 个字符的标准卷或精简卷，则不支持降级到 SANtricity 操作系统软件版本 11.90 或更早版本。如果您计划降级到 SANtricity 操作系统软件版本 11.90 或更早版本，请在降级前更改名称大于 30 个字符的任何标准卷或精简卷的名称。

字段	Description
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。 池中的容量会根据驱动器类型以4 GiB或8 GiB为增量进行分配。分配的容量不是4 GiB或8 GiB的倍数、但不可用。要确保整个容量可用、请以4 GiB或8 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	卷类型指示为应用程序特定工作负载创建的卷类型。
卷块大小（仅限 EF80、EF50、EF300 和 EF600 ）	显示了可为卷创建的块大小： • 512—512字节 • 4 k—4、096字节
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- System Manager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： • 主机的 I/O 负载 • 卷的修改优先级 • 卷组中的驱动器数量 • 驱动器通道的数量 • 更改卷的区块大小时存储阵列控制器的处理能力、I/O性能会受到影响、但数据仍可用。

字段	Description
支持安全保护	只有当池或卷组中的驱动器支持安全时、"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。
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。
资源调配（仅限 EF80、EF50、EF300 和 EF600 ）	仅当驱动器支持此选项时，"Resource Provisioned"旁边才会显示 **Yes**。Resource Provisioning 是 EF80、EF50、EF300 和 EF600 存储阵列中提供的一项功能，它允许卷立即投入使用，而无需后台初始化过程。

2. 要继续为选定应用程序创建卷、请单击*下一步*、然后转到 [第4步：查看卷配置]。

第4步：查看卷配置

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。单击*返回*进行任何更改。
2. 对卷配置感到满意后，单击 * 完成 * 。

结果

System Manager会在选定池和卷组中创建新卷、然后在所有卷表中显示新卷。

完成后

- 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 可直接通过 SANtricity System Manager 获取。此可下载版本的 SMcli 可在 EF80、EF50、E4000 、EF600、EF600C、EF300 和 EF300C 控制器上使用。要在 SANtricity System Manager 中下载 SMcli，请选择 **System** 和 **Add-ons** > **Download command line interface**。

在 **SANtricity System Manager** 中将卷添加到工作负载

对于当前未与工作负载关联的卷、您可以将一个或多个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. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 选择菜单：省略号图标 [Add volumes to workload]。

   此时将显示 Applications and workloads 视图。
3. 选择*添加到工作负载*。

   此时将显示选择工作负载对话框。
4. 请执行以下操作：
   - 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。
5. 选择要添加到工作负载的卷。
6. 查看要添加到选定工作负载的卷。
7. 对工作负载配置感到满意后，单击 添加。

管理卷

增加 **SANtricity System Manager** 中卷的容量

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

- 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。
- 对于精简卷、尚未达到报告的最大容量256 TiB。
- 卷中未使用任何热备用驱动器。（仅适用于卷组中的卷。）

> 一次最多只能将卷容量扩展到128 TiB。

关于此任务

请记住、此池或卷组中的其他卷将来可能会有任何容量要求。请确保您提供足够的可用容量来创建快照映像、快照卷或远程镜像。

> 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. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 找到要增加容量的卷，然后单击 **ellipsis icon › Increase Capacity**。

   此时将显示确认增加容量页面。

3. 选择 * 是 * 继续。

   此时将显示"增加报告容量"页面。

   此页面显示卷的当前报告容量和卷的关联池或卷组中的可用容量。

4. 使用*通过添加…增加报告容量*框将容量添加到当前可用报告容量。您可以更改以 mebibytes (MiB) 、gibibytes (GiB) 或 tebibytes (TiB) 显示的容量值。
5. 单击 * 增加 * 。

结果

- System Manager会根据您的选择增加卷的容量。
- 选择菜单：监控[正在进行的操作]以查看当前为选定卷运行的增加容量操作的进度。此操作可能耗时较长，并可能影响系统性能。

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 **SANtricity System Manager** 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。
- 此卷处于最佳状态、并且此卷上没有正在进行的修改操作。

操作启动后、您将无法取消。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。

以下类型的卷_cannot _ be initialized：

- 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

本主题仅适用于从池或卷组创建的标准卷。

步骤

1. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 单击菜单：省略号图标 [Initialize volumes]。

   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。
3. 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

System Manager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)。

选择菜单：Monitoring[Operations in progress]，查看当前为选定卷运行的初始化操作的进度。此操作可能耗时较长，并可能影响系统性能。

在 **SANtricity System Manager** 中重新分配卷

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、则必须停止卷_while the redistribution operation is in progress_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. 从左侧面板中，选择菜单：Storage[Volumes]。

2. 单击菜单：省略号图标 [Redistribute volumes]。

   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。

3. 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

System Manager会将选定卷移动到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 **SANtricity System Manager** 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. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 单击菜单：省略号图标 [Change volume ownership]。

   此时将显示 Change Volume Ownership（更改卷所有权）窗口。存储阵列上的所有卷都将显示在此对话框中。

3. 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

- System Manager会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 **SANtricity System Manager** 中删除卷

通常、如果创建的卷参数或容量不正确、不再满足存储配置需求或不再需要用于备份或应用程序测试的快照映像、则可以删除这些卷。

删除卷会增加池或卷组中的可用容量。您可以选择一个或多个要删除的卷。

开始之前

在计划删除的卷上、确保满足以下条件：

- 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

您不能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"。

删除卷会导致这些卷上的所有数据丢失。

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

步骤

1. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 找到要删除的卷，然后单击 **ellipsis icon › Delete**。

   此时将显示删除卷对话框。

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

结果

System Manager将执行以下操作：

- 删除任何关联的快照映像、计划和快照卷。
- 删除任何镜像关系。
- 增加池或卷组中的可用容量。

在 **SANtricity System Manager** 中更改精简卷的分配容量限制

对于能够按需分配空间的精简卷、您可以更改限制精简卷自动扩展到的已分配容量的限制。

当精简卷接近分配的容量限制时，您还可以通过窗口上角的铃铛图标更改将警报（超过警告阈值）发送到通知区域的百分比点。您可以选择启用或禁用此警报通知。

此功能不适用于 EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统。

系统会根据已分配的容量限制自动扩展已分配的容量。通过分配的容量限制、您可以将精简卷的自动增长限制为低于报告的容量。当写入的数据量接近分配的容量时、您可以更改分配的容量限制。

更改精简卷的已分配容量限制和警告阈值时、必须考虑卷的用户数据和副本服务数据要占用的空间。

步骤

1. 从左侧面板中，选择菜单：存储[Thin volume monitoring]。

   此时将显示精简卷监控视图。

2. 选择要更改的精简卷、然后选择*更改限制*。

   此时将显示更改限制对话框。此时将在此对话框中显示为选定精简卷分配的容量限制和警告阈值设置。

3. 根据需要更改分配的容量限制和警告阈值。

   ▼ 字段详细信息

正在设置 …	Description
将分配的容量限制更改为…	写入失败的阈值、可防止精简卷占用额外资源。此阈值是卷报告的容量大小的百分比。
在以下情况下提醒我… (警告阈值)	如果希望系统在精简卷接近分配容量限制时生成警报，请选中此复选框。警报将发送到通知区域，可通过窗口上角的铃铛图标访问。此阈值是卷的报告容量大小的百分比。 清除此复选框可禁用警告阈值警报通知。

4. 单击 * 保存 * 。

管理设置

更改 **SANtricity System Manager** 中的卷设置

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

要更改的卷处于最佳状态。

在对卷设置进行更改时、某些操作可能不可用

步骤

1. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 找到要更改的卷，然后单击 **ellipsis icon › Edit Settings**。

   此时将显示 Edit Volume Settings（编辑卷设置）窗口，其中显示选定卷的配置设置。

3. 根据需要配置卷设置：

   ▼ 字段详细信息

正在设置 ...	Description
Name	显示卷的名称。当当前名称不再有意义或不再适用时，更改卷的名称。标准卷和精简卷名称的最大长度为 60 个字符。只有标准卷和精简卷的名称可以超过 30 个字符。名称必须是唯一的。 如果存在名称大于 30 个字符的标准卷或精简卷，则不支持降级到 SANtricity 操作系统软件版本 11.90 或更早版本。如果您计划降级到 SANtricity 操作系统软件版本 11.90 或更早版本，请在降级前更改名称大于 30 个字符的任何标准卷或精简卷的名称。
主机	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。 • 已分配给-标识可访问选定卷的主机或主机集群。 • * 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。 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NVM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)。
分段规模估算	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- System Manager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： • 主机的 I/O 负载 • 卷的修改优先级 • 卷组中的驱动器数量 • 驱动器通道的数量 • 更改卷的区块大小时存储阵列控制器的处理能力、I/O性能会受到影响、但数据仍可用。

正在设置 …	Description
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。

4. 单击 * 保存 * 。

   System Manager会根据您的选择更改卷的设置。

完成后

选择菜单：监控[正在进行的操作]以查看当前为选定卷运行的更改操作的进度。

在 **SANtricity System Manager** 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。如果当前名称不再有意义或适用、请更改工作负载的名称。

步骤

1. 从左侧面板中，选择菜单：Storage[Applications and workloads]。

   此时将显示 Applications and workloads 视图。

2. 选择要更改的工作负载，然后单击 **ellipsis icon › Edit Settings**。

   此时将显示"应用程序和工作负载设置"对话框。

3. *可选：*更改用户提供的工作负载名称。
4. 单击 * 保存 * 。

在 **SANtricity System Manager** 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标准卷或所有精简卷的缓存设

置。

步骤

1. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 单击菜单：省略号图标 [Change volume cache settings]。

   此时将显示更改卷缓存设置窗口。存储阵列上的所有卷都将显示在此对话框中。

3. 选中要更改其缓存设置的每个卷旁边的框，或选中表头中的框以选择所有卷。

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。
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。 对于精简卷、动态缓存读取预取始终处于禁用状态、并且无法更改。
不使用电池的写缓存	不使用电池的写入缓存设置允许写入缓存继续运行、即使电池缺失、出现故障、已完全放电或未完全充电也是如此。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。 可能丢失数据-如果选择此选项而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。 只有在启用写入缓存时、此设置才可用。此设置不适用于精简卷。
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。 只有在启用写入缓存时、此设置才可用。此设置不适用于精简卷。

4. 单击 **Save** 以更改缓存设置

在 **SANtricity System Manager** 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。

默认介质扫描期限设置为120天。

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. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 单击菜单：省略号图标 [Change volume media scan settings]。

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

3. 要启用媒体扫描，请选中 **Media scan** 复选框。

   禁用介质扫描复选框会暂停所有介质扫描设置。

4. 指定要运行介质扫描的天数。
5. 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。

   System Manager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。

6. 单击 * 保存 * 。

System Manager会根据您的选择对后台介质扫描应用更改。

使用复制服务

了解 **SANtricity System Manager** 中的复制卷

通过复制卷功能、您可以在同一存储阵列上创建两个单独的卷、即源卷和目标卷、从而创建卷的时间点副本。

此功能会逐字节执行从源卷到目标卷的复制、从而使目标卷上的数据与源卷上的数据完全相同。

复制数据以提高访问能力

随着卷的存储要求发生变化、您可以使用复制卷功能将数据从使用较小容量驱动器的池或卷组复制到使用较大容量驱动器的池或卷组。例如、您可以使用复制卷功能执行以下操作：

- 将数据移动到更大的驱动器。
- 更改为数据传输速率较高的驱动器。
- 使用新技术更改驱动器以提高性能。
- 将精简卷更改为厚卷。

副本源卷和目标卷必须具有相同的报告主机可寻址/逻辑块大小(扇区大小)。

报告的卷块大小为：

- 本机块大小—卷的块大小与驱动器块大小匹配、可以是512或4K。
- 模拟**512**块大小—驱动器为4 k、但报告的块大小为512。

将精简卷更改为厚卷

如果要将精简卷更改为厚卷、请使用复制卷操作创建精简卷的副本。复制卷操作的目标始终是厚卷。

System Manager不提供创建精简卷的选项。如果要创建精简卷、请使用命令行界面(CLI)。

备份数据

通过复制卷功能、您可以通过将数据从一个卷复制到同一存储阵列上的另一个卷来备份卷。您可以使用目标卷作为源卷的备份、用于系统测试或备份到其他设备、例如磁带驱动器。

将**Snapshot**卷数据还原到基础卷

如果需要将数据从关联的Snapshot卷还原到基础卷、可以使用复制卷功能将数据从快照卷复制到基础卷。您可以为快照卷上的数据创建卷副本、然后将数据复制到基础卷。

源卷和目标卷

下表指定了可用于具有复制卷功能的源卷和目标卷的卷类型。

Volume type	使卷副本源卷脱机	联机卷副本源卷	目标卷联机和脱机
池中的厚卷	是的。	是的。	是的。
卷组中的厚卷	是的。	是的。	是的。
精简卷	是[1]	是的。	否
Snapshot卷	是[2]	否	否
Snapshot基础卷	是的。	是的。	否
远程镜像主卷	是[3]	是的。	否

[1]目标卷的容量必须等于或大于精简卷报告的容量。

[2]在联机复制操作完成之前、您无法使用Snapshot卷副本。

[3]如果源卷为主卷、则目标卷的容量必须等于或大于源卷的可用容量。

了解 **SANtricity** 软件中的复制卷操作类型

您可以执行_offline"复制卷"操作或"_online"复制卷操作。脱机操作会从源卷读取数据并将其复制到目标卷。联机操作使用快照卷作为源卷、并将其数据复制到目标卷。

为确保数据完整性、在任何一种类型的复制卷操作期间、目标卷的所有I/O活动都将暂停。发生此暂停的原因是、在操作步骤 完成之前、目标卷上的数据状态不一致。

下面介绍了脱机和联机复制卷操作。

脱机复制卷操作

脱机复制卷关系位于源卷与目标卷之间。脱机副本将从源卷读取数据并将其复制到目标卷、同时暂停对正在进行的源卷进行的所有更新。源卷的所有更新都将暂停、以防止在目标卷上创建按时间顺序排列的不一致。

有关脱机副本操作的信息	
读取和写入请求	• 参与脱机副本的源卷可用于只读I/O活动、而复制卷操作的状态为"正在进行"或"待定"。 • 脱机副本完成后、允许写入请求。 • 为防止出现写保护错误消息、请勿访问状态为正在进行的复制卷操作中的源卷。
日志记录文件系统	• 如果源卷已使用日志文件系统进行格式化、则存储阵列控制器可能会拒绝任何对源卷执行问题描述 读取请求的尝试、并可能会显示错误消息。 • 日志文件系统驱动程序会在尝试对读取请求进行问题描述 之前发出写入请求。控制器拒绝写入请求、并且可能由于写入请求被拒绝而无法发出读取请求。此情况可能会导致显示错误消息、指示源卷受写保护。 • 要防止发生此问题描述 、请勿在复制卷操作的状态为正在进行时尝试访问参与脱机副本的源卷。

联机复制卷关系位于快照卷和目标卷之间。您可以在源卷联机并可用于数据写入的情况下启动复制卷操作。此功能可通过创建卷的快照并使用该快照作为副本的实际源卷来实现。

在对源卷启动复制卷操作时、System Manager会为基础卷创建一个快照映像、并在基础卷的快照映像与目标卷之间创建一个复制关系。使用快照映像作为源卷可以使存储阵列在复制过程中继续向源卷写入数据。

在联机复制操作期间、由于写入时复制操作步骤 、会对性能产生影响。联机副本完成后、将还原基础卷性能。

有关联机副本操作的信息	
可以使用哪种类型的卷?	• 创建时间点映像的卷称为基础卷、必须是存储阵列上的标准卷或精简卷。 • 目标卷可以是卷组中的标准卷、也可以是池中的标准卷。目标卷不能是精简卷或快照组中的基础卷。 • 您可以使用联机复制卷功能将数据从精简卷复制到位于同一存储阵列中的池中的标准卷。但是、您不能使用复制卷功能将数据从标准卷复制到精简卷。
基本卷性能	• 如果用作副本源的Snapshot卷处于活动状态、则由于写入时复制操作、基础卷性能将下降。复制完成后、快照将被禁用、并还原基础卷性能。尽管快照已禁用、但预留容量卷和副本关系仍保持不变。
创建的卷类型	• 在联机复制操作期间、系统会创建一个快照卷和一个预留容量卷。 • 快照卷不是包含数据的实际卷、而是指某个卷在特定时间包含的数据。 • 对于所创建的每个快照、系统会创建一个预留容量卷来存放快照的数据。预留容量卷仅用于管理快照映像。
预留容量卷	• 在修改源卷上的数据块之前、要修改的数据块的内容会复制到预留容量卷中以供安全保存。 • 由于预留容量卷会将原始数据的副本存储在这些数据块中、因此对这些数据块进行的进一步更改仅会写入源卷。 • 联机副本操作使用的磁盘空间少于完整物理副本、因为存储在预留容量卷中的数据块仅为自创建快照以来发生更改的数据块。

在 **SANtricity System Manager** 中复制卷

您可以将数据从一个卷复制到同一存储阵列中的另一个卷、并为源卷创建物理时间点副本(克隆)。

开始之前

- 必须停止源卷和目标卷的所有I/O活动。
- 必须卸载源卷和目标卷上的任何文件系统。
- 如果您之前在复制卷操作中使用过目标卷、则不再需要该数据或已备份数据。

关于此任务

源卷是接受主机I/O并存储应用程序数据的卷。启动复制卷后、源卷中的数据将全部复制到目标卷。

目标卷是一个标准卷、用于维护源卷中的数据副本。复制卷操作完成后、目标卷与源卷相同。目标卷必须与源卷具有相同或更大的容量；但是、它可以具有不同的RAID级别。

▼ 有关联机和脱机副本的更多信息

联机副本

联机副本会为存储阵列中的任何卷创建一个时间点副本、同时仍可在副本正在进行时向卷写入数据。此功能可通过创建卷的快照并使用该快照作为副本的实际源卷来实现。创建时间点映像的卷称为基础卷、可以是存储阵列中的标准卷或精简卷。

脱机副本

脱机副本将从源卷读取数据并将其复制到目标卷、同时暂停对正在进行的源卷进行的所有更新。源卷的所有更新都将暂停、以防止在目标卷上创建按时间顺序排列的不一致。脱机卷副本关系位于源卷和目标卷之间。

复制卷操作会覆盖目标卷上的数据、并使与目标卷关联的所有快照卷失败(如果存在)。

步骤

1. 从左侧面板中，选择菜单：Storage[Volumes]。
2. 找到要用作"复制卷"操作的源的卷，然后单击 **ellipsis icon › Copy volume**。

   此时将显示 Copy Volume 窗口。
3. 选择要将数据复制到的目标卷。

   此对话框中显示的表列出了所有符合条件的目标卷。
4. 使用滑块栏为复制卷操作设置复制优先级。

   与服务I/O请求相比、复制优先级可确定用于完成复制卷操作的系统资源的数量。

   ▼ 有关副本优先级速率的更多信息

   复制优先级有五种：

   - 最低
   - 低
   - 中等
   - 高
   - 最高

   如果将副本优先级设置为最低速率、则会优先处理I/O活动、并且复制卷操作所需时间会更长。如果将副本优先级设置为最高比率、则会优先执行复制卷操作、但存储阵列的I/O活动可能会受到影响。
5. 选择是要创建联机副本还是脱机副本。要创建联机副本、请选中"*在复制操作期间保持源卷联机"*复选框。
6. 执行以下操作之一：
   - 要执行_online _复制操作、请单击*下一步*继续显示*预留容量*对话框。
   - 要执行_offline_副本操作、请单击*完成*以启动脱机副本。
7. 如果选择创建联机副本、请设置用于存储联机副本的数据和其他信息所需的预留容量、然后单击*完成*启动联机副本。

卷候选表仅显示支持指定预留容量的候选卷。预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

按照以下准则分配预留容量：

- 预留容量的默认设置为基础卷容量的40%、通常此容量已足够。
- 但是、预留容量会根据原始数据的更改次数而有所不同。存储对象处于活动状态的时间越长、预留容量就越大。

结果

System Manager 将所有数据从源卷复制到目标卷。

完成后

选择菜单：监控[正在进行的操作]以查看"复制卷"操作的进度。此操作可能耗时较长，并可能影响系统性能。

在 **SANtricity System Manager** 中对复制卷操作采取行动

您可以查看正在执行的复制卷操作、并停止、更改优先级、重新复制或清除复制卷操作。

步骤

1. 从左侧面板中，选择 **Monitoring › Operations in progress**。

   此时将显示操作进行中对话框。

2. 找到要对其执行操作的复制卷操作、然后单击*操作*列中的链接以执行以下操作之一。

   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。

Action	Description
停止	当复制卷操作的状态为"正在进行"、"待定"或"失败"时、您可以停止此操作。 停止复制卷后、所有映射的主机都对源卷具有写入访问权限。如果数据写入源卷、则目标卷上的数据将不再与源卷上的数据匹配。
更改优先级	您可以在复制卷操作的状态为In progress时更改此操作的优先级、以选择复制卷操作完成的速率。
重新复制	如果您停止了复制卷操作并希望重新启动该操作、或者复制卷操作失败或暂停、则可以重新复制卷。复制卷操作从头开始。 重新复制操作会覆盖目标卷上的现有数据、并使与目标卷关联的所有快照卷失败(如果存在)。
清除	当复制卷操作的状态为"正在进行"、"待定"或"失败"时、您可以删除该操作。 在选择*清除*之前、请确保要执行此操作。没有确认对话框。

SANtricity System Manager 卷和工作负载常见问题解答

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。

什么是卷?

卷是应用程序，数据库和文件系统用于存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。

卷是使用池或卷组中的可用容量创建的。卷已定义容量。尽管一个卷可能包含多个驱动器、但一个卷在主机中显示为一个逻辑组件。

当卷组中有足够的可用容量来创建卷时、为什么会出现容量过度分配错误?

选定卷组可能具有一个或多个可用容量区域。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。

在卷组中创建具有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。

如果卷组具有可用容量区域、则卷组图形包含一个链接、指示现有可用容量区域的数量。选择此链接可显示一个弹出窗口、指示每个区域的容量。

通过整合可用容量、您可以从卷组中的最大可用容量创建更多卷。您可以使用以下方法之一整合选定卷组上的现有可用容量：

- 当为卷组检测到至少一个可用容量区域时，"合并可用容量"建议将显示在通知区域中，可通过窗口上角的铃形图标访问。单击*合并可用容量*链接以启动对话框。
- 您还可以从左侧面板中选择菜单：Storage[Pools and volume groups]，然后选择菜单：省略号图标[Consolidate volume group free capacity] 以启动对话框。

如果要使用特定的可用容量区域、而不是最大可用容量区域、请使用命令行界面(CLI)。

为什么这些卷与工作负载没有关联?

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。

为什么我无法删除选定的工作负载?

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。

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。

为什么我看不到所有池和/或卷组?

无法将卷移动到的任何池或卷组不会显示在列表中。

由于以下任一原因、池或卷组均不符合条件：

- 池或卷组池的数据保证(Data Assurance、DA)功能不匹配。
- 池或卷组处于非最佳状态。
- 池或卷组的容量太小。

什么是区块大小?

区块是指存储阵列移至条带中的下一个驱动器(RAID组)之前存储在驱动器上的数据量(以千字节(KiB)为单位)。区块大小仅适用于卷组、而不适用于池。

区块大小由其包含的数据块数定义。在确定区块大小时、您必须了解要在卷中存储的数据类型。如果应用程序通常使用小型随机读取和写入(IOPS)、则较小的区块大小通常效果会更好。或者、如果应用程序具有较大的顺序读取和写入(吞吐量)、则较大的区块大小通常会更好。

无论应用程序使用小型随机读取和写入还是大型顺序读取和写入、如果区块大小大于典型的数据块区块大小、存储阵列的性能都会更高。这通常可以使驱动器更轻松、更快地访问数据、这对于提高存储阵列性能非常重要。

IOPS性能非常重要的环境

在每秒I/O操作数(IOPS)环境中、如果使用的区块大小大于读取/写入到驱动器的典型数据块大小(“chunk”)、则存储阵列的性能会更好。这样可确保每个区块写入一个驱动器。

吞吐量非常重要的环境

在吞吐量环境中、数据区块大小应为数据驱动器总数的偶数部分、也应为典型数据区块大小(I/O大小)。这样、数据就会作为一个条带在卷组中的驱动器之间分布、从而加快读取和写入速度。

什么是首选控制器所有权?

首选控制器所有权用于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。

例如、如果一个控制器主要读取大型连续数据块、而另一个控制器具有频繁读取和写入的小型数据块、则负载会截然不同。通过了解哪些卷包含哪种类型的数据、您可以在两个控制器之间平均平衡I/O传输。

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、您可以通过将卷设置为显示4KiB块大小来实现最佳性能；但是、请确保主机支持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。

主机和主机集群

了解 **SANtricity** 软件中的主机和主机集群

您可以配置主机和主机集群、从而定义存储阵列与数据服务器之间的连接。

什么是主机和主机集群?

_host_是一种向存储阵列上的卷发送I/O的服务器。主机集群_是一组主机、您可以创建这些主机来将相同的卷分配给多个主机。

了解更多信息。

- "主机术语"
- "访问卷"
- "LUN 的最大数量"

如何配置主机和主机集群?

要定义主机连接、您可以转到菜单：Storage[Hosts]以手动配置主机。如果您希望两个或更多主机共享对同一组卷的访问、则可以定义一个集群并将这些卷分配给该集群。

了解更多信息。

- "手动创建主机"

- "如何将卷分配给主机和主机集群"
- "用于创建主机和分配卷的工作流"
- "手动创建主机"
- "创建主机集群"
- "将卷分配给主机"

相关信息

详细了解与主机相关的任务：

- "设置自动负载平衡"
- "设置主机连接报告"
- "更改默认主机类型"

概念

了解 **SANtricity** 软件中的主机术语

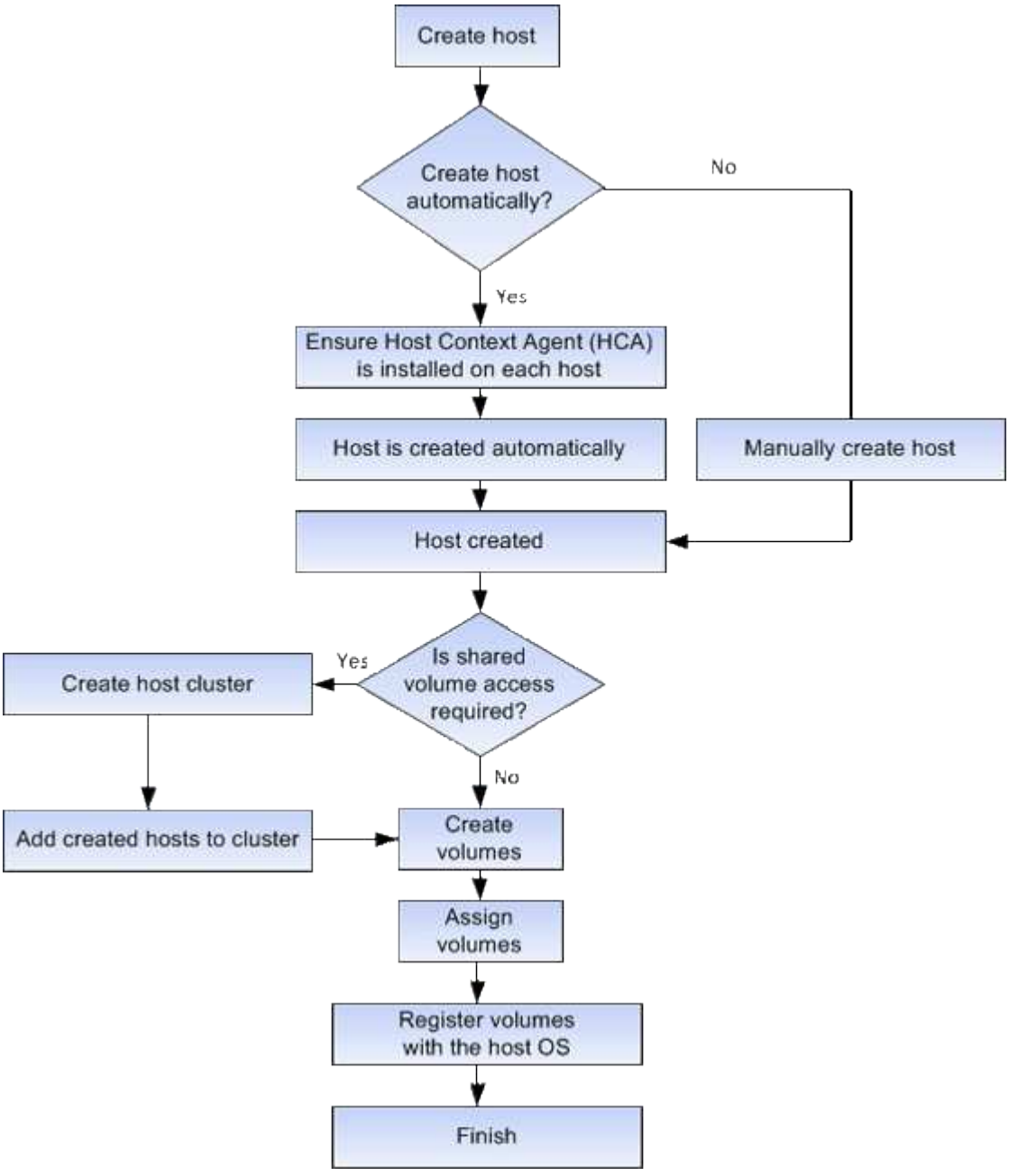
了解主机术语如何应用于存储阵列。

组件	定义
主机	主机是指向存储阵列上的卷发送I/O的服务器。
主机名	主机名应等于主机的系统名称。
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。
主机接口协议	主机接口协议是指控制器与主机之间的连接(例如光纤通道、iSCSI等)。
HBA或网络接口卡(NIC)	主机总线适配器(HBA)是驻留在主机中并包含一个或多个主机端口的板。
主机端口	主机端口是主机总线适配器(HBA)上的一个端口、用于与控制器建立物理连接并用于I/O操作。
主机端口标识符	主机端口标识符是与主机总线适配器(HBA)上的每个主机端口关联的唯一全球通用名称。 • Internet小型计算机系统接口(iSCSI)主机端口标识符必须包含1到233个字符。iSCSI主机端口标识符以标准IQN格式显示(例如、`iqn.xxx.com.xxx:8b3ad`)。 • 光纤通道和串行连接SCSI (SAS)等非iSCSI主机端口标识符每两个字符(例如、`xx：yy：zz`)后显示为以冒号分隔。光纤通道主机端口标识符必须包含16个字符。
主机操作系统类型	主机操作系统类型是一种配置设置、用于定义存储阵列中的控制器如何根据主机的操作系统(或变体)对I/O做出响应。这有时也称为_host type_、简称为。
控制器主机端口	控制器主机端口是控制器上的一个端口、用于与主机建立物理连接并用于I/O操作。

组件	定义
LUN	逻辑单元号(LUN)是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。

SANtricity System Manager 中的主机创建和卷分配的工作原理

下图说明了如何配置主机访问。



了解 **SANtricity System Manager** 中的手动主机创建

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。您只

能手动创建主机。

手动创建

通过手动创建主机、您可以确保存储阵列控制器检测到的主机端口标识符与主机正确关联。

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。

如何在 **SANtricity** 软件中将卷分配给主机和主机集群

要使主机或主机集群向卷发送I/O、必须将此卷分配给主机或主机集群。

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。

访问 **SANtricity System Manager** 中的卷

访问卷是存储阵列上出厂配置的卷、用于通过主机I/O连接与存储阵列和主机进行通信。访问卷需要一个逻辑单元号(Logical Unit Number、LUN)。

访问卷用于以下实例：

- 带内管理—访问卷用于带内连接以管理存储阵列。只有在使用命令行界面(CLI)管理存储阵列时、才能执行此操作。

> 使用 Access 卷的带内管理不适用于 EF80、EF50、E4000、EF600/EF600C 或 EF300/EF300C 存储系统。

首次将卷分配给主机时、系统会自动创建访问卷。例如、如果将Volume_1和Volume_2分配给主机、则在查看分配结果时、您会看到三个卷(Volume_1、Volume_2和Access)。

如果您不是使用命令行界面自动创建主机或带内管理存储阵列、则不需要访问卷、您可以通过删除访问卷来释放LUN。此操作将删除卷到LUN的分配以及与主机的任何带内管理连接。

了解 **SANtricity** 软件中的最大 **LUN** 数量

存储阵列具有可用于每个主机的最大逻辑单元号(LUN)数。

最大数量取决于主机的操作系统。存储阵列会跟踪已使用的LUN数量。如果您尝试将卷分配给超过最大LUN数的

主机、则该主机将无法访问该卷。

了解 SANtricity 软件中的默认主机操作系统类型

首次连接主机时、存储阵列会使用默认主机类型。它定义了在访问卷时存储阵列中的控制器如何与主机的操作系统配合使用。

如果需要更改存储阵列相对于与其连接的主机的运行方式、则可以更改主机类型。通常、在将主机连接到存储阵列或连接其他主机之前、您会更改默认主机类型。

请牢记以下准则：

- 如果计划连接到存储阵列的所有主机都具有相同的操作系统(同构主机环境)、则更改主机类型以与操作系统匹配。
- 如果您计划将具有不同操作系统的主机连接到存储阵列(异构主机环境)、请更改主机类型以匹配大多数主机的操作系统。

  例如、如果要将八个不同的主机连接到存储阵列、并且其中六个主机运行的是Windows操作系统、则必须选择Windows作为默认主机操作系统类型。

- 如果大多数已连接主机混合使用不同的操作系统、请将主机类型更改为出厂默认值。

  例如、如果要将八个不同的主机连接到存储阵列、并且其中两个主机运行的是Windows操作系统、则三个主机运行的是VMware操作系统、 另外三个主机运行Linux操作系统、您必须选择出厂默认作为默认主机操作系统类型。

配置主机访问

在 SANtricity System Manager 中手动创建主机

对于无法自动发现的主机、您可以手动创建主机。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。

关于此任务

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. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 单击菜单：创建 [主机] 。

   此时将显示创建主机对话框。

3. 单击 **+Add Host Port** 以访问主机端口字段并添加主机的主机端口标识符。您可以添加一个或多个主机端口

标识符以与主机关联。

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。
标识符	执行以下操作之一： • * 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。 • * 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、也可以从实用程序(一次一个)将其复制/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。
CHAP启动程序	(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* CHAP initiator*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： • 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。 • 如果不需要主机身份验证，请将此字段留空。 目前、System Manager使用的唯一iSCSI身份验证方法是CHAP。

5. 单击 * 创建 * 。

结果

成功创建主机后，系统会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<Hostname_Port number>。例如，为 主机 IPT 创建的第一个端口的默认别名是 ipt_1 。

在 SANtricity System Manager 中创建主机集群

当两个或更多主机需要对相同卷进行I/O访问时、您可以创建一个主机集群。

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. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择菜单：创建[主机集群]。

   此时将显示创建主机集群对话框。

3. 根据需要选择主机集群的设置。

   ▼ 字段详细信息

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。

4. 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。

在 SANtricity System Manager 中将卷分配给主机

您必须将卷分配给主机或主机集群、以便用于I/O操作。此分配将授予主机或主机集群对存储阵列中一个或多个卷的访问权限。

关于此任务

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，如果等到创建并初始化所有卷后再将其分配给主机，则会缩短卷初始化时间。请记住，一旦映射了与卷组相关联的卷，*all* 卷将恢复到较慢的初始化。可以从菜单中检查初始化进度：Monitoring[Operations in progress]。

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。

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。

步骤

1. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择要分配卷的主机或主机集群，然后单击菜单：省略号图标[Assign Volumes]。

   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或在 * 筛选器 * 框中键入内容，以便于查找特定卷。

3. 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。
4. 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。

管理主机和集群

在 **SANtricity System Manager** 中更改默认主机类型

使用更改默认主机操作系统设置更改存储阵列级别的默认主机类型。通常、在将主机连接到存储阵列或连接其他主机之前、您会更改默认主机类型。

关于此任务

请牢记以下准则：

- 如果计划连接到存储阵列的所有主机都具有相同的操作系统(同构主机环境)、则更改主机类型以与操作系统匹配。
- 如果您计划将具有不同操作系统的主机连接到存储阵列(异构主机环境)、请更改主机类型以匹配大多数主机的操作系统。

  例如、如果要将八个不同的主机连接到存储阵列、并且其中六个主机运行的是Windows操作系统、则必须选择Windows作为默认主机操作系统类型。

- 如果大多数已连接主机混合使用不同的操作系统、请将主机类型更改为出厂默认值。

  例如、如果要将八个不同的主机连接到存储阵列、并且其中两个主机运行的是Windows操作系统、则三个主机运行的是VMware操作系统、 另外三个主机运行Linux操作系统、您必须选择出厂默认作为默认主机操作系统类型。

步骤

1. 从左侧面板中，选择 **System**。
2. 向下滚动到*其他设置*、然后单击*更改默认主机操作系统类型*。
3. 选择要用作默认值的主机操作系统类型。
4. 单击 * 更改 * 。

在 **SANtricity System Manager** 中取消分配卷

如果不再需要从主机或主机集群对该卷进行I/O访问、请从主机或主机集群中取消分配卷。

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. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择要编辑的主机或主机群集，然后单击菜单：省略号图标[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。

3. 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。
4. 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 **SANtricity System Manager** 中删除主机或主机集群

您可以删除主机或主机集群。

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. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择要删除的主机或主机群集，然后单击菜单：省略号图标 [Delete]。

   此时将显示确认对话框。

3. 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。

在 **SANtricity System Manager** 中设置主机连接报告

您可以启用主机连接报告、以便存储阵列持续监控控制器与已配置主机之间的连接、然后

在连接中断时向您发出警报。默认情况下，此功能处于启用状态。

关于此任务

如果禁用主机连接报告、则系统将不再监控连接到存储阵列的主机的连接或多路径驱动程序问题。

禁用主机连接报告还会禁用自动负载平衡、从而监控和平衡控制器资源利用率。

步骤

1. 从左侧面板中，选择 **System**。
2. 向下滚动到*其他设置*、然后单击*启用/禁用主机连接报告*。

   此选项下方的文本指示此选项当前是启用还是禁用。

   此时将打开确认对话框。

3. 单击 * 是 * 继续。

   通过选择此选项、您可以在已启用/已禁用之间切换此功能。

管理设置

在 **SANtricity System Manager** 中更改主机的设置

您可以更改主机的名称、主机操作系统类型以及关联的主机集群。

步骤

1. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择要编辑的主机，然后单击菜单：省略号图标 [Edit Settings]。

   此时会出现一个窗口，显示当前的主机设置。

3. 如果尚未选择此选项、请单击*属性*选项卡。
4. 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： • 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。 • **<Host Cluster>**—系统将主机与选定集群关联。
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。

5. 单击 * 保存 * 。

在 **SANtricity System Manager** 中更改主机群集的设置

您可以更改主机集群名称、或者在主机集群中添加或删除主机。

步骤

1. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择要编辑的主机群集，然后单击菜单：省略号图标[编辑设置]。

   此时将显示一个窗口，其中显示当前主机群集设置。

3. 根据需要更改主机集群的设置。

   ▼ 字段详细信息

正在设置 ...	**Description**
Name	您可以指定用户提供的主机集群名称。需要为集群指定名称。
关联主机	要添加主机、请单击*关联主机*框、然后从下拉列表中选择一个主机名。您不能手动输入主机名。 要删除主机、请单击主机名旁边的* X *。

4. 单击 * 保存 * 。

在 **SANtricity System Manager** 中更改主机的主机端口标识符

如果要更改主机端口标识符上的用户标签、向主机添加新的主机端口标识符或从主机中删除主机端口标识符、请更改主机端口标识符。

关于此任务

更改主机端口标识符时、请记住以下准则：

- 添加—添加主机端口时、要将主机端口标识符与为连接到存储阵列而创建的主机相关联。您可以使用主机总线适配器(HBA)实用程序手动输入端口信息。
- 编辑—您可以编辑主机端口以将主机端口移动(关联)到其他主机。您可能已将主机总线适配器或iSCSI启动程序移动到其他主机、因此必须将主机端口移动(关联)到新主机。
- 删除—您可以删除主机端口以从主机中删除(取消关联)主机端口。

步骤

1. 在左侧面板中，选择菜单： Storage [Hosts]。
2. 选择要关联端口的主机，然后单击菜单：省略号图标 [Edit Settings]。

   如果要将端口添加到主机群集中的主机，请选择所需的主机。无法在主机群集级别添加端口。

   此时会显示编辑主机设置屏幕，其中显示当前的主机设置。

3. 根据需要更改主机端口标识符设置。

正在设置 ...	Description
主机端口	您可以选择以下选项之一： • 添加主机端口 — 单击 添加主机端口 将新的主机端口标识符关联到主机。主机端口标识符名称的长度由主机接口技术决定。Fibre Channel 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。端口必须是唯一的。不允许使用已配置的端口号。 • 删除（**X** 图标） — 单击 **X** 图标以删除（取消关联）主机端口标识符。删除选项不会物理删除主机端口。此选项删除主机端口和主机之间的关联。除非您卸下主机总线适配器或 iSCSI 启动程序，否则控制器仍可识别主机端口。 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。
Name	如果需要，您可以更改端口标签名称。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。 System Manager使用质询握手身份验证协议(Challenge Handshake Authentication Protocol、CHAP)方法、在初始链接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。

4. 单击 * 保存 * 。

更改主机 **I/O** 模块协议

当您需要在现有 I/O 模块上使用不同的协议时，作为 I/O 模块升级的一部分，或者当新存储系统安装或控制器升级中新控制器的默认协议不是您想要的协议时，您可以更改控制器的主机 I/O 模块上的协议。

关于此任务

- 通过准备、停止主机 I/O 操作、更改协议，然后将主机配置为使用新协议，来更改主机 I/O 模块上的协议。
- 已更改存储系统中所有主机 I/O 模块上的协议。
- 更改主机 I/O 模块上的协议时，将暂时中断主机对所有卷的访问，并在重新启动期间使存储系统不可用，这需要几分钟的时间。

步骤 **1**：为协议变更做好准备

通过验证当前使用的协议，确定是否需要更改协议，如果需要，则安排停机维护窗口，准备更改主机 I/O 模块上的协议。

步骤

1. 如果不知道存储系统中主机 I/O 模块上的当前协议，请使用 SANtricity System Manager 进行验证。
   a. 选择*System*。
   b. 在 其他设置 部分中，单击 更改主机 **I/O** 协议 以打开该页面。
   c. 请参阅 **Host I/O Protocol** 字段中显示的默认协议。

如果要查看主机 I/O 模块的可用协议列表，请选择 **Host I/O Protocol** 字段中的下拉菜单。协议列表基于当前安装的主机 I/O 模块。

2. 下一步取决于默认协议是否是您想要的协议：

条件	操作
默认协议是您想要的协议	无需采取操作。您可以退出此过程。
默认协议不是您想要的协议	继续此过程以更改协议。

3. 请为此过程安排一个停机维护窗口。

步骤 **2**：停止主机 **I/O** 操作

更改协议之前，必须停止主机的所有 I/O 操作，然后从存储系统中删除所有定义的主机。

在成功完成协议更改之前，您无法访问存储系统上的数据。

步骤

1. 确保存储系统与所有连接的主机之间没有发生 I/O 操作。例如，您可以执行以下步骤：
   - 停止所有涉及从存储映射到主机的 LUN 的进程。
   - 请确保没有应用程序将数据写入从存储映射到主机的任何 LUN。
   - 卸载与存储系统上的卷关联的所有文件系统。

   停止主机 I/O 操作的确切步骤取决于主机操作系统和配置，这超出了本说明的范围。如果您不确定如何停止环境中的主机 I/O 操作，请考虑关闭主机或联系 "NetApp 支持"。

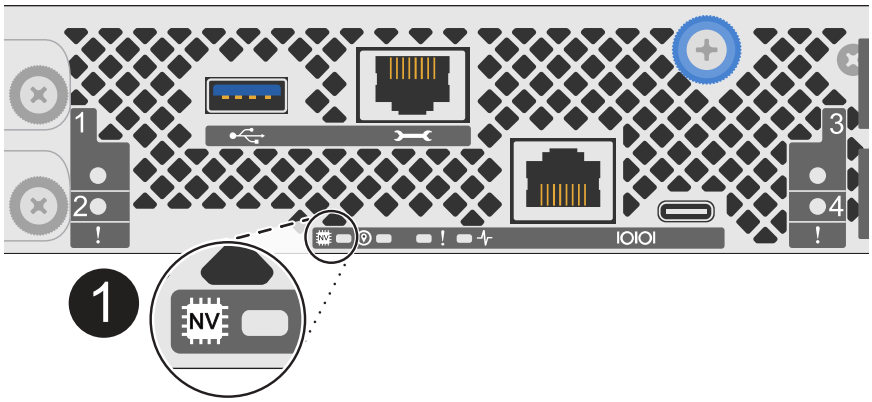
   可能的数据丢失 — 如果在 I/O 操作发生时继续此过程，则可能会丢失数据。

2. 在每个控制器上，确保 NV Caching Active（绿色）LED 熄灭。

   当 NV 缓存活动（绿色）LED 熄灭时，缓存内存中的任何数据都已写入驱动器，可以安全地继续此过程。

   如果 NV Caching Active（绿色）LED 指示灯亮起，则缓存数据正在写入驱动器。您必须等待过程完成，并且 NV Caching Active（绿色）LED 指示灯关闭。但是，如果 LED 指示灯持续亮起超过五分钟，请 "NetApp 支持"，然后再继续此过程。

   NV 缓存活动（绿色）LED 位于控制器上的 NV 图标旁边。



1	控制器上的 NV 图标和 NV 缓存活动指示灯

3. 确认控制器上的操作已在 SANtricity System Manager 中完成：
   a. 选择*监控* > *正在进行的操作*以查看概览屏幕。
   b. 等待所有操作完成，概览屏幕显示 当前没有正在进行的操作，然后继续下一步。
4. 从存储系统中删除所有定义的主机。

   有关删除主机的详细信息，请参见 "删除主机或主机集群"。

步骤 **3**：更改协议

使用 SANtricity System Manager 更改主机 I/O 模块上的协议，等待控制器完成其重新启动周期，确认其状态为 Optimal，然后重新创建主机定义。

步骤

1. 选择*System*。
2. 在 其他设置 部分中，单击 更改主机 **I/O** 协议 以打开该页面。
3. 在 **Host I/O Protocol** 字段中，单击下拉菜单并选择要使用的协议。

   协议列表基于当前安装的主机 I/O 模块。
4. 在打开的字段中键入 **CHANGE** 以确认更改。
5. 选择 **Change** 按钮。
6. 等待控制器完成重新启动周期。

   此过程可能需要大约五分钟时间。
7. 当控制器恢复联机时，请使用 SANtricity System Manager 确认其状态为最佳。
8. 重新创建主机定义。

   有关创建主机的详细信息，请参见 "创建主机或主机集群" 过程。

步骤 **4**：配置主机以使用新协议

更改主机端口的协议后，必须将主机配置为使用新协议。

1. 有关分步说明，请参见适用于您的存储系统的指南：
   - "Linux 快速配置"
   - "VMware 快速配置"
   - "Windows 快速配置"

   具体设置可能有所不同。有关解决方案的具体说明和其他建议设置，请参阅 "NetApp 互操作性表"。

SANtricity System Manager 的主机系统和主机集群常见问题解答

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。

什么是主机和主机集群?

主机是指向存储阵列上的卷发送I/O的服务器。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。

您可以单独定义主机。它可以是一个独立的实体、也可以添加到主机集群中。您可以将卷分配给单个主机、也可以将主机作为主机集群的一部分、与主机集群中的其他主机共享对一个或多个卷的访问权限。

主机集群是您在SANtricity 系统管理器中创建的逻辑实体。您必须先将主机添加到主机集群、然后才能分配卷。

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。

主机操作系统类型	操作系统**(OS)**和多路径驱动程序
Mac OS (ATTO)	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 (内核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。
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。

什么是**HBA**和适配器端口?

主机总线适配器(HBA)是驻留在主机中并包含一个或多个主机端口的板。主机端口是主机总线适配器(HBA)上的一个端口、用于与控制器建立物理连接并用于I/O操作。

HBA上的适配器端口称为主机端口。大多数HBA都有一个或两个主机端口。HBA具有唯一的全球通用标识符(World Wide Identifier、WWID)、每个HBA主机端口都有一个唯一的WWID。通过SANtricity系统管理器手动创建主机时、可以使用主机端口标识符将相应的HBA与物理主机相关联。

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。

如何创建**CHAP**密码?

如果在连接到存储阵列的任何iSCSI主机上设置质询握手身份验证协议(CHAP)身份验证、则必须为每个iSCSI主机重新输入该启动程序CHAP密钥。

为此、您可以在创建主机操作中使用System Manager、也可以通过查看/编辑设置选项使用System Manager。

如果使用 CHAP 相互身份验证，则还必须在系统页面中为存储阵列定义目标 CHAP 密码，然后在每个 iSCSI 主机上重新输入该目标 CHAP 密码。

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、则必须使用默认集群。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。

在特殊情况下、如果外部存储环境有利于允许连接到存储阵列的所有主机和所有已登录主机端口标识符都能够访问所有卷、则应使用默认集群(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。

什么是主机连接报告?

启用主机连接报告后、存储阵列会持续监控控制器与已配置主机之间的连接、然后在连接中断时向您发出警报。

如果主机出现松动、损坏或缺失的缆线或其他问题、可能会中断连接。在这些情况下、系统可能会打开Recovery Guru消息：

- "Host Redundancy Lost"(主机冗余丢失)*—如果任一控制器无法与主机进行通信、则会打开。
- 主机类型不正确—如果在存储阵列上错误指定主机类型、则会打开此窗口、从而可能导致故障转移问题。

如果重新启动控制器所需时间可能超过连接超时、您可能需要禁用主机连接报告。禁用此功能将禁止恢复消息。

禁用主机连接报告还会禁用自动负载平衡、从而监控和平衡控制器资源使用情况。但是、如果重新启用主机连接报告、则不会自动重新启用自动负载平衡功能。

快照

了解 SANtricity System Manager 中的快照

通过Snapshot功能、您可以为存储阵列卷创建时间点映像、以用于备份或测试。

什么是**Snapshot**映像?

_snapshot image_是在特定时间点捕获的卷数据的逻辑副本。与还原点一样，您可以通过快照映像回滚到已知正常的数据集。尽管主机可以访问快照映像、但它无法直接对其进行读写。

了解更多信息。

- "快照存储的工作原理"
- "Snapshot术语"
- "基本卷、预留容量和快照组"
- "Snapshot计划和一致性组"
- "Snapshot卷"

如何创建快照?

您可以从基本卷或快照一致性组手动创建快照映像。此过程可从菜单：Snapshots[Snapshot images] 获得。

了解更多信息。

- "快照的要求和准则"
- "用于创建快照映像和卷的工作流"
- "创建快照映像"
- "计划快照映像"
- "创建快照一致性组"
- "创建快照卷"

如何从快照回滚数据?

rollback 是将基本卷中的数据返回到上一个时间点的过程。您可以从 **Snapshots › Snapshot images** 回滚快照数据。

了解更多信息。

- "Snapshot回滚"
- "为基础卷启动Snapshot映像回滚"
- "为一致性组成员启动Snapshot映像回滚"

相关信息

详细了解与快照相关的任务：

- "更改快照卷的预留容量"
- "更改快照组的预留容量"

概念

快照存储在 **SANtricity** 软件中的工作原理

Snapshot功能使用写时复制技术存储快照映像并使用分配的预留容量。

如何使用快照映像

Snapshot映像是在特定时间点捕获的卷内容的逻辑只读副本。您可以使用快照防止数据丢失。

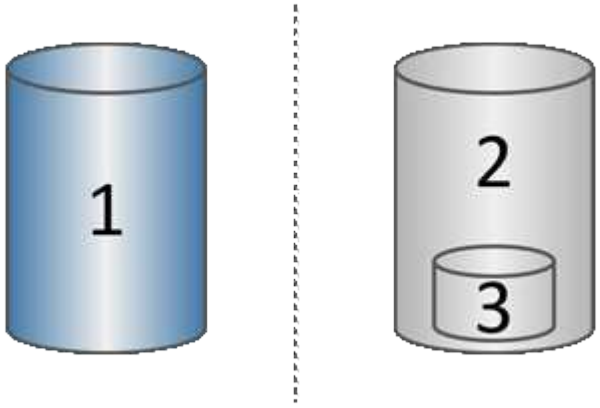
Snapshot映像对于测试环境也很有用。通过创建数据的虚拟副本、您可以使用快照测试数据、而无需更改实际卷本身。此外、主机对快照映像没有写入访问权限、因此您的快照始终是一个安全的备份资源。

创建快照

创建快照时、Snapshot功能会按如下方式存储映像数据：

- 创建快照映像时、该映像与基础卷完全匹配。Snapshot功能使用写时复制技术。创建快照后、首次写入基础卷上的任何块或块集将导致原始数据复制到预留容量、然后再将新数据写入基础卷。
- 后续快照仅包含已更改的数据块。在基础卷上覆盖数据之前、Snapshot功能会使用其写入时复制技术将受影

响扇区的所需映像保存到Snapshot预留容量中。



[1]基础卷(物理磁盘容量)；[2] Snapshot (逻辑磁盘容量)；[3]预留容量(物理磁盘容量)

- 预留容量用于存储在创建快照后发生更改的基础卷部分的原始数据块、并包含用于跟踪更改的索引。通常、预留容量的大小默认为基础卷的40%。(如果需要更多预留容量、可以增加预留容量。)
- Snapshot映像会根据其时间戳按特定顺序进行存储。只能手动删除基础卷中最早的快照映像。

Snapshot还原

要将数据还原到基础卷、您可以使用Snapshot卷或Snapshot映像：

- 快照卷-如果需要检索已删除的文件、请使用已知正常的快照映像创建快照卷、然后将其分配给主机。
- * Snapshot映像*-如果需要将基础卷还原到特定时间点、请使用先前的快照映像将数据回滚到基础卷。

了解 **SANtricity** 软件中的快照术语

了解快照术语如何应用于存储阵列。

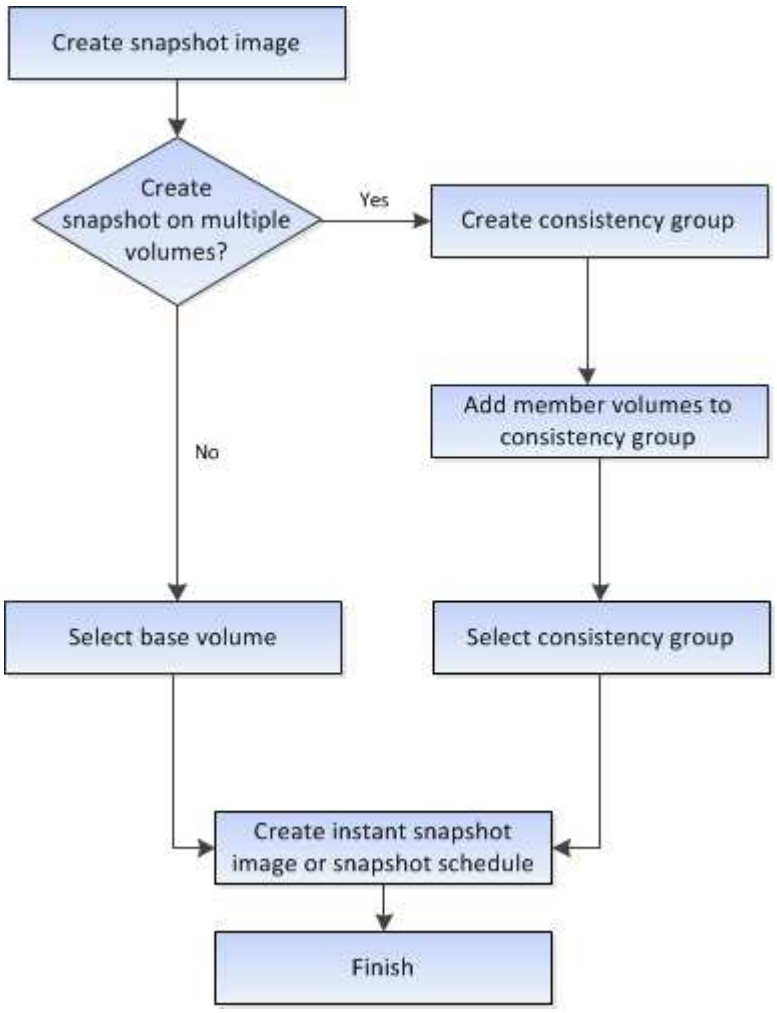
期限	Description
Snapshot功能	Snapshot功能用于创建和管理卷的映像。
Snapshot映像	快照映像是指在特定时间点捕获的卷数据的逻辑副本。与还原点一样，您可以通过快照映像回滚到已知正常的数据集。尽管主机可以访问快照映像、但它无法直接对其进行读写。
基础卷	基础卷是创建快照映像的源卷。它可以是厚卷或精简卷、通常分配给主机。基础卷可以位于卷组或磁盘池中。
Snapshot卷	主机可通过Snapshot卷访问Snapshot映像中的数据。快照卷包含自己的预留容量、这样可以在不影响原始快照映像的情况下保存对基础卷所做的任何修改。
Snapshot组	快照组是一组来自单个基础卷的快照映像。
预留容量卷	预留容量卷可跟踪覆盖基础卷中的哪些数据块以及这些数据块中保留的内容。
Snapshot计划	快照计划是创建自动快照映像的时间表。通过该计划、您可以控制创建映像的频率。

期限	Description
Snapshot一致性组	快照一致性组是创建快照映像时视为单个实体的卷的集合。其中每个卷都有自己的快照映像、但所有映像都是在同一时间点创建的。
Snapshot一致性组成员卷	属于快照一致性组的每个卷都称为成员卷。将卷添加到快照一致性组时、System Manager会自动创建与此成员卷对应的新快照组。
回滚	回滚是指将基础卷中的数据返回到上一时间点的过程。
预留容量	预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

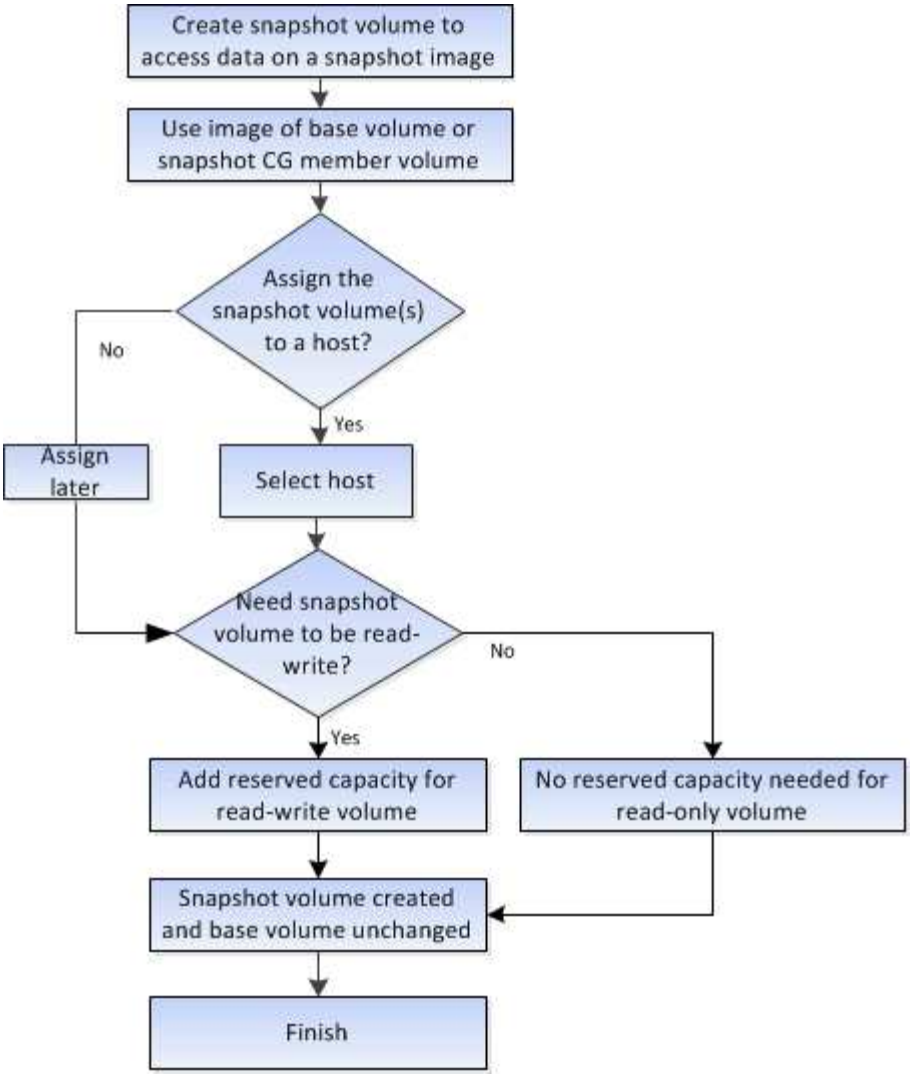
如何在 **SANtricity System Manager** 中创建快照映像和快照卷

在SANtricity系统管理器中、您可以按照以下步骤创建快照映像和快照卷。

创建快照映像的工作流



用于创建快照卷的工作流



SANtricity System Manager 中的快照要求和指南

创建和使用快照时、请查看以下要求和准则。

Snapshot映像和**Snapshot**组

- 每个快照映像仅与一个快照组相关联。
- 首次为关联对象创建计划的或即时的快照映像时、系统会创建快照组。这将创建预留容量。

  您可以从池和卷组页面查看快照组。

- 当存储阵列脱机或关闭电源时、不会发生计划的快照映像。
- 如果删除具有快照计划的快照组、则该快照计划也会被删除。
- 如果您的快照卷不再需要、则可以重复使用它以及任何关联的预留容量、而不是删除它。这样就会为同一个基础卷创建不同的快照卷。您可以将快照卷或快照一致性组快照卷与相同的快照映像或不同的快照映像重新关联、前提是快照映像位于同一个基础卷中。

Snapshot一致性组

- 对于属于快照一致性组的每个卷、快照一致性组包含一个快照组。
- 您只能将一个快照一致性组与一个计划相关联。
- 如果删除具有快照计划的快照一致性组、则该快照计划也会被删除。
- 您不能单独管理与快照一致性组关联的快照组。而是必须在快照一致性组级别执行管理操作(创建快照映像、删除快照映像或快照组以及回滚快照映像)。

基础卷

- 快照卷必须与关联的基础卷具有相同的数据保证(Data Assurance、DA)和安全设置。
- 您不能为发生故障的基础卷创建快照卷。
- 如果基础卷驻留在卷组上、则任何关联快照一致性组的成员卷都可以驻留在池或卷组上。
- 如果基础卷驻留在池中、则任何关联快照一致性组的所有成员卷都必须与基础卷驻留在同一个池中。

预留容量

- 预留容量仅与一个基本卷相关联。
- 使用计划可能会生成大量快照映像。确保为计划的快照预留了足够的容量。
- 快照一致性组的预留容量卷必须与快照一致性组成员卷的关联基础卷具有相同的数据保证(Data Assurance、DA)和安全设置。

待定快照映像

在以下情况下、快照映像创建可能会保持"Pending"状态：

- 包含此快照映像的基础卷是异步镜像组的成员。
- 基础卷当前正在执行同步操作。同步操作完成后、快照映像创建即完成。

最大快照映像数

- 如果某个卷是快照一致性组的成员、则System Manager会为该成员卷创建一个快照组。此快照组计入每个基础卷允许的最大快照组数。
- 如果您尝试在快照组或快照一致性组上创建快照映像、但关联组已达到其最大快照映像数、您可以选择两个选项：
  - 为快照组或快照一致性组启用自动删除。
  - 手动从快照组或快照一致性组中删除一个或多个快照映像、然后重试此操作。

自动删除

如果启用了快照组或快照一致性组自动删除、则System Manager会在系统为该组创建新快照映像时删除最旧的快照映像。

回滚操作

- 正在执行回滚操作时、您无法执行以下操作：

- 删除用于回滚的快照映像。
- 为参与回滚操作的基础卷创建新的快照映像。
- 更改关联快照组的存储库已满策略。

- 如果正在执行以下任一操作、则无法启动回滚操作：
  - 容量扩展(向池或卷组添加容量)
  - 卷扩展(增加卷的容量)
  - 卷组的RAID级别更改
  - 卷的区块大小更改
- 如果基础卷参与卷副本、则无法启动回滚操作。
- 如果基础卷是远程镜像中的二级卷、则无法启动回滚操作。
- 如果关联的Snapshot存储库卷中的任何已用容量包含无法读取的扇区、则回滚操作将失败。

了解 **SANtricity System Manager** 中的基本卷、预留容量和快照组

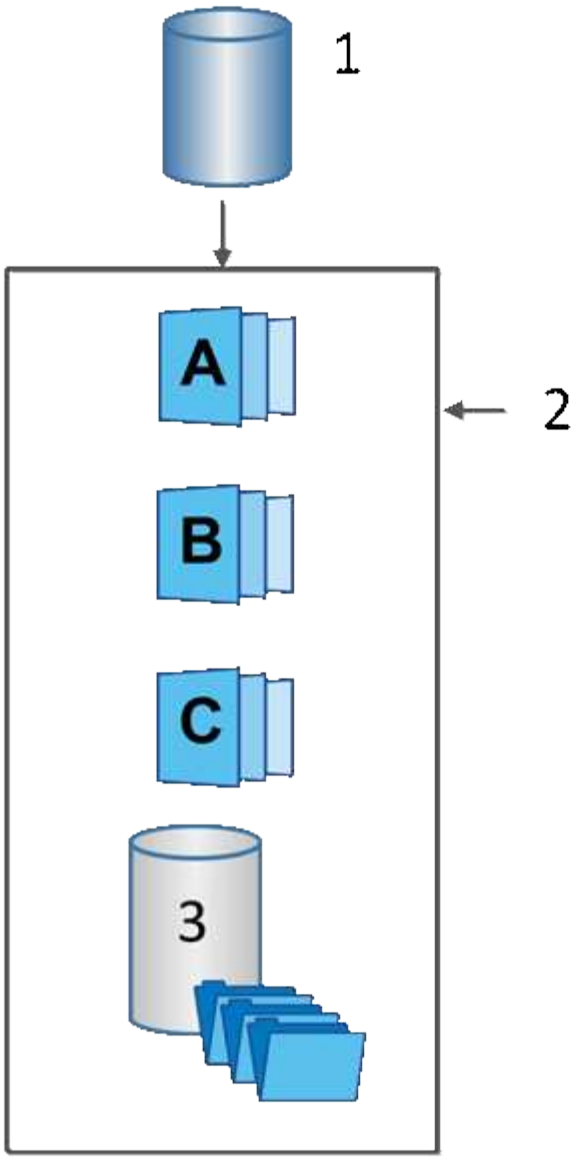
Snapshot功能可使用基础卷、预留容量和快照组。

基础卷

a _base volume"是用作快照映像源的卷。基础卷可以是厚卷、也可以是精简卷、并且可以驻留在池或卷组中。

要为基础卷创建快照、您可以随时创建即时映像、也可以通过为快照定义定期计划来自动执行此过程。

下图显示了快照对象与基础卷之间的关系。



[1]基础卷；[2]组中的Snapshot对象(映像和预留容量)；[3] Snapshot组的预留容量。

预留容量和快照组

System Manager会将快照映像组织为_snapshot groups_.当System Manager建立快照组时、它会自动创建关联的_reserved capacity_、以存放组的快照映像并跟踪后续对其他快照所做的更改。

如果基础卷驻留在卷组中、则预留的容量可以位于池或卷组中。如果基础卷驻留在池中、则预留容量必须与基础卷位于同一池中。

Snapshot组无需用户操作、但您可以随时调整Snapshot组上的预留容量。此外、在满足以下条件时、系统可能会提示您创建预留容量：

- 每当为尚未创建快照组的基础卷创建快照时、System Manager都会自动创建快照组。此操作还会为用于存储后续快照映像的基础卷创建预留容量。
- 每当为基础卷创建快照计划时、System Manager都会自动创建快照组。

自动删除

使用快照时、请使用默认选项启用自动删除。自动删除功能会在快照组达到32个映像的快照组限制时自动删除最旧的快照映像。如果关闭自动删除、则最终会超过快照组限制、您必须手动执行操作来配置快照组设置并管理预留容量。

了解 **SANtricity System Manager** 中的快照计划和快照一致性组

使用计划收集快照映像、并使用快照一致性组管理多个基础卷。

要轻松管理基础卷的快照操作、您可以使用以下功能：

- 快照计划—自动为单个基础卷创建快照。
- 快照一致性组—将多个基础卷作为一个实体进行管理。

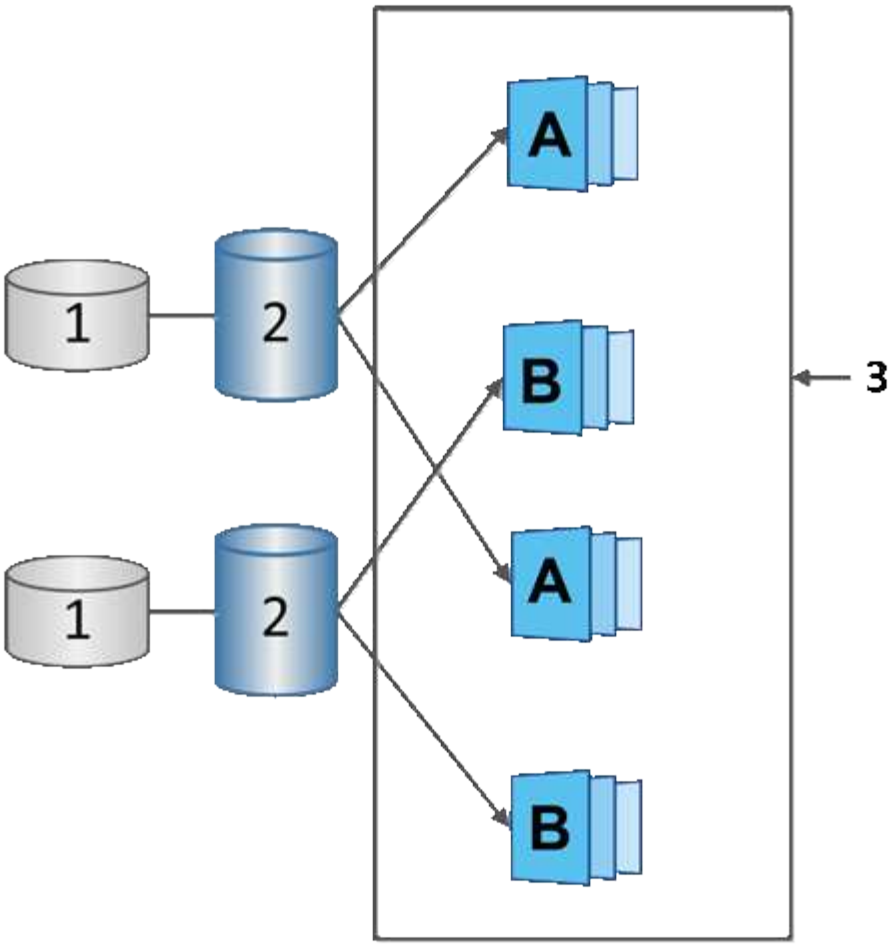
Snapshot计划

如果要自动为基础卷创建快照、可以创建计划。例如、您可以定义一个计划、以便在每个星期六的午夜、每个月的第一个或您决定的任何日期和时间生成快照映像。在一个计划达到最多32个快照后、您可以暂停计划快照、创建更多预留容量、也可以删除快照。可以手动删除快照、也可以通过自动删除过程来删除快照。删除快照映像后、可以重复使用额外的预留容量。

Snapshot一致性组

如果要确保同时在多个卷上创建快照映像、请创建快照一致性组。快照映像操作作为一个整体对快照一致性组执行。例如、您可以为所有卷计划具有相同时间戳的同步快照。Snapshot一致性组非常适合跨越多个卷的应用程序、例如将日志存储在一个卷上的数据库应用程序和将数据库文件存储在另一个卷上的数据库应用程序。

快照一致性组中包含的卷称为成员卷。将卷添加到一致性组时、System Manager会自动创建与该成员卷对应的新预留容量。您可以定义一个计划来自动为每个成员卷创建快照映像。



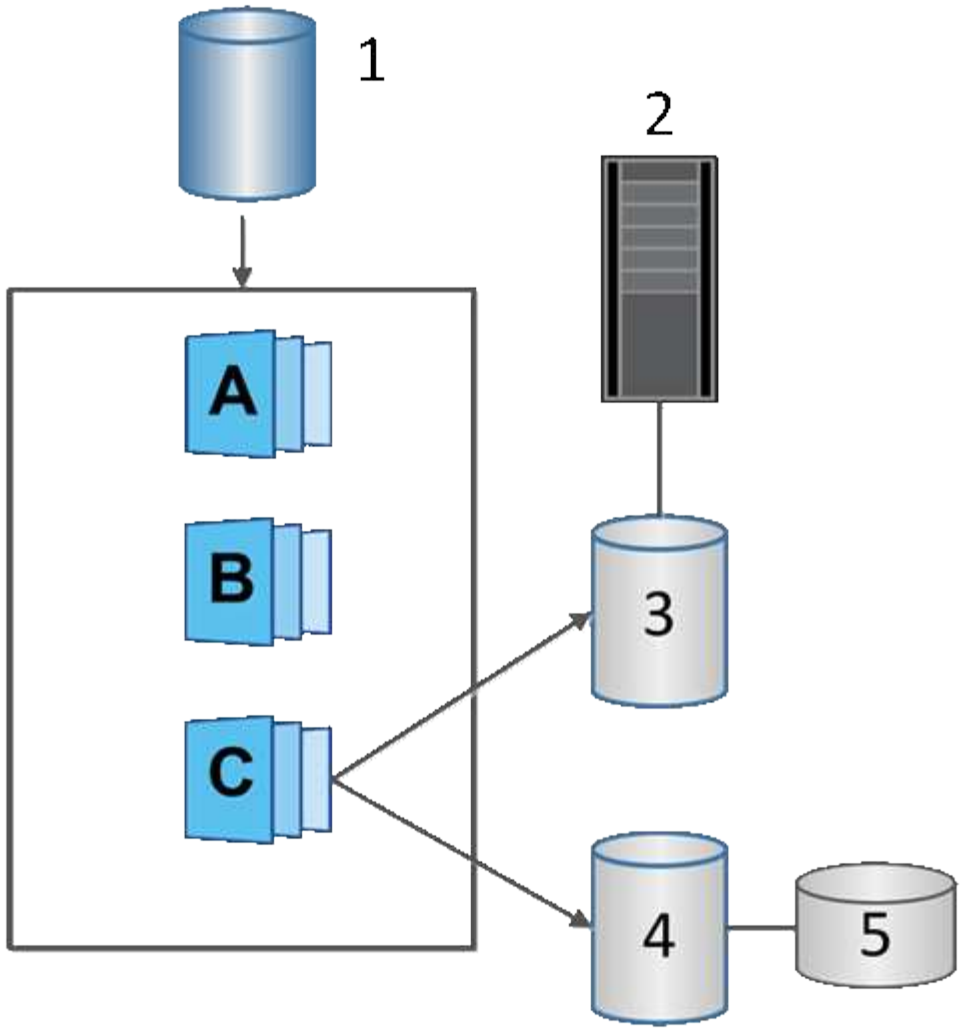
[1]预留容量；[2]成员卷；[3]一致性组快照映像

了解 **SANtricity** 软件中的快照卷

如果要读取或写入快照数据、您可以创建快照卷并将其分配给主机。快照卷与基础卷具有相同的特征(RAID级别、I/O特性等)。

创建快照卷时、您可以将其指定为_read-onl_y或_read-write accessible_。

创建只读Snapshot卷时、不需要添加预留容量。创建读写Snapshot卷时、必须添加预留容量以提供写入访问。



[1]基本卷；[2]主机；[3]只读快照卷；[4]读写快照卷；[5]预留容量

了解 **SANtricity** 软件中的快照回滚

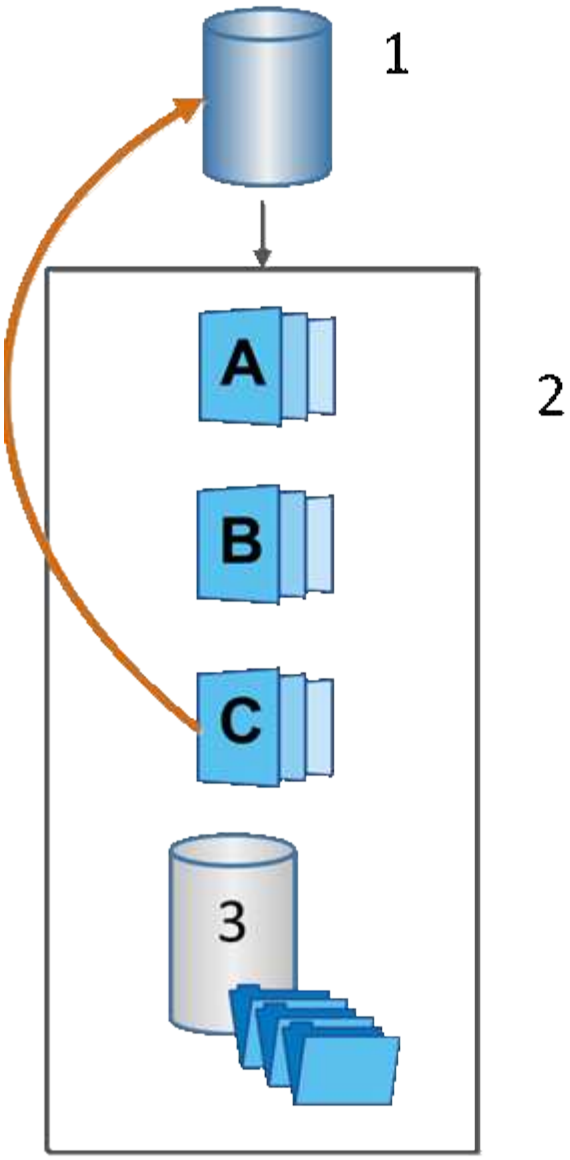
回滚操作会将基础卷返回到先前的状态、此状态由选定快照决定。

对于回滚、您可以从以下任一源选择快照映像：

- 快照映像回滚、用于完全还原基础卷。
- * Snapshot一致性组回滚*、可用于回滚一个或多个卷。

回滚期间、Snapshot功能会保留组中的所有快照映像。此外、如果I/O操作需要、还允许主机在此过程中访问基础卷。

启动回滚后、后台进程会扫描基础卷的逻辑块地址(Logical Block Address、LBA)、然后在要还原的回滚快照映像中查找写时复制数据。由于基础卷可通过主机访问进行读取和写入、并且所有先前写入的数据均可立即使用、因此预留容量卷必须足够大、以便在回滚过程中包含所有更改。数据传输将作为后台操作继续进行、直到回滚完成。



[1]基本卷；[2]组中的Snapshot对象；[3] Snapshot组预留容量

创建快照和快照对象

在 **SANtricity System Manager** 中创建快照映像

您可以从基础卷或快照一致性组手动创建快照映像。这也称为_instant snapshot_或_instant image_。

开始之前

- 基础卷必须是最佳卷。
- 驱动器必须是最佳驱动器。
- 不能将快照组指定为"`re提供服务"。`
- 预留容量卷必须与快照组的关联基础卷具有相同的数据保证(Data Assurance、DA)设置。

步骤

1. 要创建快照映像、请执行以下操作之一：
   - 从左侧面板中，选择菜单：Storage[Volumes]。选择对象（基本卷或快照一致性组），然后单击菜单：省略号图标[Create instant snapshot]。
   - 从左侧面板中，选择菜单：Snapshots[Snapshot images]，然后选择菜单：Create[Instant snapshot Image]。

     此时将显示创建Snapshot映像对话框。选择对象(基础卷或快照一致性组)、然后单击*下一步*。如果为卷或快照一致性组创建了先前的快照映像、则系统会立即创建即时快照。否则、如果这是首次为卷或快照一致性组创建快照映像、则会显示确认创建Snapshot映像对话框。

2. 单击*创建*接受需要预留容量的通知、然后继续执行预留容量步骤。

   此时将显示预留容量对话框。

3. 使用spinner框调整容量百分比、然后单击*下一步*以接受表中突出显示的候选卷。

   此时将显示编辑设置对话框。

4. 根据需要选择快照映像的设置、然后确认要执行此操作。

   ▼ 字段详细信息

正在设置 ...	Description
• Snapshot映像设置*	Snapshot映像限制
如果要在指定限制后自动删除快照映像、请保持选中此复选框；使用spinner框更改此限制。如果清除此复选框、则在创建32个映像后将停止创建快照映像。	预留容量设置
在以下情况下提醒我…	使用spinner框调整当快照组的预留容量接近全满时系统发送警报通知的百分比点。 如果快照组的预留容量超过指定阈值、请使用提前通知增加预留容量或删除不必要的对象、以免剩余空间用尽。
预留容量全满的策略	选择以下策略之一： • 清除最旧的快照映像-系统会自动清除快照组中最旧的快照映像、从而释放快照映像预留容量、以便在组中重复使用。 • 拒绝向基础卷写入数据-当预留容量达到其最大定义百分比时、系统会拒绝向基础卷发出的任何I/O写入请求、这些请求会触发预留容量访问。

结果

- System Manager会在Snapshot映像表中显示新的快照映像。此表按时间戳以及关联的基础卷或快照一致性组列出了新映像。

- 由于以下情况、快照创建可能仍处于"Pending"状态：
  - 包含此快照映像的基础卷是异步镜像组的成员。
  - 基础卷当前正在执行同步操作。同步操作完成后、快照映像创建即完成。

在 **SANtricity System Manager** 中安排快照映像

您可以创建快照计划、以便在基础卷出现问题时进行恢复、并执行计划备份。可以在一天中的任意时间按每日、每周或每月计划创建基础卷或快照一致性组的快照。

开始之前

基础卷必须是最佳卷。

关于此任务

此任务介绍如何为现有快照一致性组或基础卷创建快照计划。

您还可以在创建基础卷或快照一致性组的快照映像的同时创建快照计划。

步骤

1. 执行以下操作之一以创建快照计划：
   - 从左侧面板中，选择菜单：Storage[Volumes]。

     为此快照计划选择对象(卷或快照一致性组)、然后选择菜单：复制服务[创建快照计划]。
   - 从左侧面板中，选择菜单：Snapshots[Snapshot schedules]，然后单击*Create*。
2. 为此快照计划选择对象(卷或快照一致性组)、然后单击*下一步*。

   此时将显示创建Snapshot计划对话框。
3. 执行以下操作之一：
   - 使用来自另一个快照对象的先前定义的计划。

     确保显示高级选项。单击*显示更多选项*。单击*导入计划*、选择具有要导入计划的对象、然后单击*导入*。
   - 修改基本或高级选项。

     在对话框右上角、单击*显示更多选项*以显示所有选项、然后参阅下表。

▼ 字段详细信息

字段	**Description**
基本设置	选择天
为快照映像选择一周中的各个日期。	开始时间

字段	Description
从下拉列表中、为每日快照选择一个新的开始时间(所选时间以半小时为间隔)。开始时间默认为比当前时间提前半小时。	时区
从下拉列表中、选择阵列的时区。	• 高级设置 *
天/月	选择以下选项之一： • 每日/每周-为同步快照选择单独的日期。如果要设置每日计划、也可以选中右上角的*选择所有日期*复选框。 • 每月/每年-为同步快照选择单个月。在*日期*字段中、输入月中要进行同步的天数。有效条目为* 1 到 31 和*最后一个。您可以使用逗号或分号分隔多天。使用连字符表示包含的日期。例如：1、3、4、10-15、last。如果您希望使用每月计划、也可以选中右上角的*选择所有月份*复选框。
开始时间	从下拉列表中、为每日快照选择一个新的开始时间(所选时间以半小时为间隔)。开始时间默认为比当前时间提前半小时。
时区	从下拉列表中、选择阵列的时区。
每日快照数/快照之间的时间	选择每天要创建的快照映像数。如果选择多个、还可以选择快照映像之间的时间。对于多个快照映像、请确保预留了足够的容量。
是否立即创建快照映像？	选中此复选框可创建即时映像以及要计划的自动映像。
开始/结束日期或无结束日期	输入开始同步的开始日期。此外、请输入结束日期或选择*无结束日期*。

4. 执行以下操作之一：
   - 如果对象是快照一致性组、请单击*创建*以接受设置并创建计划。
   - 如果对象是卷、请单击*下一步*为快照映像分配预留容量。

     卷候选表仅显示支持指定预留容量的候选卷。预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

5. 使用spinner框为快照映像分配预留容量。执行以下操作之一：
   - 接受默认设置。

     使用此建议选项可使用默认设置为快照映像分配预留容量。

   - 分配您自己的预留容量设置以满足您的数据存储需求。

     如果更改默认预留容量设置、请单击*刷新候选容量*以刷新指定预留容量的候选列表。

     按照以下准则分配预留容量：

     - 预留容量的默认设置为基础卷容量的40%。通常、此容量足以满足要求。

- 所需容量因卷I/O写入的频率和大小以及快照映像收集的数量和持续时间而异。

6. 单击 * 下一步 * 。

   此时将显示编辑设置对话框。

7. 根据需要编辑快照计划的设置、然后单击*完成*。

   ▼ 字段详细信息

正在设置 …	Description
• Snapshot映像限制*	在以下情况下启用Snapshot映像自动删除…
如果要在指定限制后自动删除快照映像、请保持选中此复选框；使用spinner框更改此限制。如果清除此复选框、则在创建32个映像后将停止创建快照映像。	预留容量设置
在以下情况下提醒我…	使用spinner框调整当计划的预留容量接近全满时系统发送警报通知的百分比点。 如果计划的预留容量超过指定阈值、请使用提前通知增加预留容量或删除不必要的对象、以免剩余空间用尽。
预留容量全满的策略	选择以下策略之一： • 清除最旧的快照映像-系统会自动清除最旧的快照映像、从而释放快照映像预留容量、以便在快照组中重复使用。 • 拒绝向基础卷写入数据-当预留容量达到其最大定义百分比时、系统会拒绝向基础卷发出的任何I/O写入请求、这些请求会触发预留容量访问。

在 **SANtricity System Manager** 中创建快照一致性组

为了确保副本一致、您可以创建一组多个卷、称为_snapshot一致性组_。

通过此组、您可以同时为所有卷创建快照映像、以确保一致性。属于快照一致性组的每个卷都称为_member volume"。将卷添加到快照一致性组时、系统会自动创建与此成员卷对应的新快照组。

关于此任务

通过快照一致性组创建序列、您可以为组选择成员卷并为成员卷分配容量。

创建快照一致性组的过程包括多步操作步骤。

第**1**步：向快照一致性组添加成员

选择成员以指定构成快照一致性组的一组卷。对快照一致性组执行的任何操作都会统一扩展到选定的成员卷。

开始之前

成员卷必须是最佳卷。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot consistency groups]。
2. 选择菜单：创建[Snapshot一致性组]。

   此时将显示创建Snapshot一致性组对话框。

3. 找到要作为成员卷添加到快照一致性组的卷。
4. 单击*下一步*、然后转到 [第2步：为快照一致性组预留容量]。

第2步：为快照一致性组预留容量

将预留容量与快照一致性组相关联。System Manager会根据快照一致性组的属性建议卷和容量。您可以接受建议的预留容量配置或自定义分配的存储。

关于此任务

在预留容量对话框中、卷候选表仅显示支持指定预留容量的候选卷。预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

步骤

1. 使用spinner框为快照一致性组分配预留容量。执行以下操作之一：
   - 接受默认设置。

     使用此建议选项可使用默认设置为每个成员卷分配预留容量。

   - 分配您自己的预留容量设置以满足您的数据存储需求。

     按照以下准则分配预留容量。

     - 预留容量的默认设置为基础卷容量的40%。通常、此容量足以满足要求。
     - 所需容量因卷I/O写入的频率和大小以及快照映像收集的数量和持续时间而异。
2. *可选：*如果更改默认预留容量设置、请单击*刷新候选容量*以刷新指定预留容量的候选列表。
3. 单击*下一步*、然后转到 [第3步：编辑快照一致性组的设置]。

第3步：编辑快照一致性组的设置

接受或选择快照一致性组的自动删除设置和预留容量警报阈值。

关于此任务

通过快照一致性组创建序列、您可以为组选择成员卷并为成员卷分配容量。

步骤

1. 根据需要接受或更改快照一致性组的默认设置。

   ▼ 字段详细信息

正在设置 ...	Description
• Snapshot一致性组设置*	Name

正在设置 …	Description
指定快照一致性组的名称。	在以下情况下启用Snapshot映像自动删除…
如果要在指定限制后自动删除快照映像、请保持选中此复选框；使用spinner框更改此限制。如果清除此复选框、则在创建32个映像后将停止创建快照映像。	预留容量设置
在以下情况下提醒我…	使用spinner框调整在快照一致性组的预留容量接近全满时系统发送警报通知的百分比点。 如果快照一致性组的预留容量超过指定阈值、请使用提前通知增加预留容量或删除不必要的对象、以免剩余空间用尽。
预留容量全满的策略	选择以下策略之一： • 清除最旧的快照映像-系统会自动清除快照一致性组中最早的快照映像、从而释放快照映像预留容量、以便在组中重复使用。 • 拒绝向基础卷写入数据-当预留容量达到其最大定义百分比时、系统会拒绝向基础卷发出的任何I/O写入请求、这些请求会触发预留容量访问。

2. 对快照一致性组配置感到满意后、单击*完成*。

在 **SANtricity System Manager** 中创建快照卷

您可以创建一个快照卷、以使主机能够访问卷或快照一致性组的快照映像。您可以将快照卷指定为只读或读写卷。

关于此任务

通过快照卷创建序列、您可以从快照映像创建快照卷、并提供在卷为读/写卷时分配预留容量的选项。快照卷可以指定为以下卷之一：

- 只读快照卷使主机应用程序可以对快照映像中所含数据的副本进行读取访问、但无法修改快照映像。只读Snapshot卷没有关联的预留容量。
- 读写Snapshot卷使主机应用程序能够对快照映像中所含数据的副本进行写入访问。它具有自己的预留容量、用于将主机应用程序后续所做的任何修改保存到基础卷、而不会影响引用的快照映像。

创建快照卷的过程包括多步操作步骤。

第**1**步：查看快照卷的成员

选择基础卷的快照映像或快照一致性组。如果选择快照一致性组快照映像、则会显示快照一致性组的成员卷以供查看。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。

2. 选择 * 创建 * 。

   此时将显示创建Snapshot卷对话框。

3. 选择要转换为快照卷的快照映像(卷或快照一致性组)、然后单击*下一步*。在*筛选器*字段中使用文本条目缩小列表范围。

   如果选择的是快照一致性组快照映像、则会显示查看成员对话框。

   在查看成员对话框中、查看选择转换为快照卷的卷列表、然后单击*下一步*。

4. 转至 [第2步：将快照卷分配给主机]。

第2步：将快照卷分配给主机

选择特定的主机或主机集群以将其分配给快照卷。此分配将授予主机或主机集群对快照卷的访问权限。如果需要、您可以选择稍后分配主机。

开始之前

- 主机页面下存在有效的主机或主机集群。
- 必须已为主机定义主机端口标识符。
- 在创建启用了DA的卷之前、请验证计划的主机连接是否支持数据保证(Data Assurance、DA)功能。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。

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。
- 您可以为存储阵列中的每个快照卷定义一个主机分配。
- 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)两次来访问快照卷。您必须使用唯一的LUN。

> 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. 在*分配给主机*对话框中、选择要分配给新卷的主机或主机集群。如果要在不分配主机的情况下创建卷、请从下拉列表中选择*稍后分配*。
2. 选择访问模式。选择以下选项之一：
   - 读/写—此选项为主机提供对快照卷的读/写访问权限、并需要预留容量。
   - 只读—此选项为主机提供对快照卷的只读访问权限、而不需要预留容量。
3. 单击*下一步*、然后执行以下操作之一：
   - 如果快照卷为读/写卷、则会显示查看容量对话框。转至 [第3步：为快照卷预留容量]。
   - 如果快照卷为只读卷、则会显示编辑优先级对话框。转至 [第4步：编辑快照卷的设置]。

第3步：为快照卷预留容量

将预留容量与读/写Snapshot卷关联。System Manager会根据基础卷或快照一致性组的属性建议卷和容量。您可以接受建议的预留容量配置或自定义分配的存储。

关于此任务

您可以根据需要增加或减少为快照卷预留的容量。如果发现Snapshot预留容量大于所需容量、则可以减小其大小以释放其他逻辑卷所需的空间。

步骤

1. 使用spinner框为快照卷分配预留容量。

   卷候选表仅显示支持指定预留容量的候选对象。

   执行以下操作之一：

   - 接受默认设置。

     使用此建议选项可使用默认设置为快照卷分配预留容量。

   - 分配您自己的预留容量设置以满足您的数据存储需求。

     如果更改默认预留容量设置、请单击*刷新候选容量*以刷新指定预留容量的候选列表。

     按照以下准则分配预留容量。

     - 预留容量的默认设置为基础卷容量的40%、通常此容量已足够。
     - 所需容量因卷I/O写入的频率和大小以及快照映像收集的数量和持续时间而异。

2. *可选：*如果要为快照一致性组创建快照卷、"更改候选项"选项将显示在"预留容量候选项"表中。单击*更改候选项*以选择备用预留容量候选项。
3. 单击*下一步*、然后转到 [第4步：编辑快照卷的设置]。

第4步：编辑快照卷的设置

更改快照卷的设置、例如名称、缓存、预留容量警报阈值等。

关于此任务

您可以将卷添加到固态磁盘(SSD)缓存中、以提高只读性能。SSD缓存由一组SSD驱动器组成、这些驱动器会在存储阵列中进行逻辑分组。

步骤

1. 根据需要接受或更改快照卷的设置。

   ▼ 字段详细信息

正在设置 ...	Description
• Snapshot卷设置*	Name

正在设置 …	Description
指定快照卷的名称。卷名称最多可包含 30 个字符。名称必须是唯一的。	启用SSD缓存
选择此选项可在SSD上启用只读缓存。	预留容量设置
在以下情况下提醒我…	仅对读/写**Snapshot**卷显示。 使用spinner框调整当快照组的预留容量接近全满时系统发送警报通知的百分比点。 如果快照组的预留容量超过指定阈值、请使用提前通知增加预留容量或删除不必要的对象、以免剩余空间用尽。

2. 查看快照卷配置。单击*返回*进行任何更改。
3. 对快照卷配置感到满意后、单击*完成*。

管理快照计划

更改 **SANtricity System Manager** 中的快照计划设置

对于快照计划、您可以更改自动收集时间或收集频率。

关于此任务

您可以从现有快照计划导入设置、也可以根据需要修改设置。

由于快照计划与快照组或快照一致性组关联、因此、计划设置更改可能会影响预留的容量。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot schedules]。
2. 选择要更改的快照计划、然后单击*编辑*。

   此时将显示编辑Snapshot计划对话框。

3. 执行以下操作之一：
   - 使用其他快照对象中先前定义的计划-单击*导入计划*、选择具有要导入计划的对象、然后单击*导入*。
   - 编辑计划设置—请参见下面的字段详细信息。

     ▼ 字段详细信息

正在设置 ...	Description
天/月	选择以下选项之一： • 每日/每周-为同步快照选择单独的日期。如果要设置每日计划、也可以选中右上角的*选择所有日期*复选框。 • 每月/每年-为同步快照选择单个月。在*日期*字段中、输入月中要进行同步的天数。有效条目为* 1 到 31 和*最后一个。您可以使用逗号或分号分隔多天。使用连字符表示包含的日期。例如：1、3、4、10-15、last。如果您希望使用每月计划、也可以选中右上角的*选择所有月份*复选框。
开始时间	从下拉列表中、为每日快照选择新的开始时间。所选内容以半小时为间隔提供。开始时间默认为比当前时间提前半小时。
时区	从下拉列表中、选择存储阵列的时区。
每天创建快照 快照之间的时间	选择每天要创建的快照映像数。 如果选择多个、还可以选择还原点之间的时间。对于多个还原点、请确保预留了足够的容量。
Start date End date 无结束日期	输入开始同步的开始日期。此外、请输入结束日期或选择*无结束日期*。

4. 单击 * 保存 * 。

在 **SANtricity System Manager** 中激活和暂停快照计划

如果需要节省存储空间、您可以暂时暂停按计划收集快照映像。此方法比删除快照计划并稍后重新创建快照计划的效率更高。

关于此任务

快照计划的状态将保持暂停、直到您使用*激活*选项恢复计划的快照活动为止。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot schedules]。

   这些计划将在页面上列出。

2. 选择要暂停的活动快照计划、然后单击*激活/暂停*。

   状态列状态将更改为*已暂停*、并且快照计划将停止收集所有快照映像。

3. 要恢复收集快照映像、请选择要恢复的已暂停快照计划、然后单击*激活/暂停*。

   状态列状态更改为*活动*。

在 **SANtricity System Manager** 中删除快照计划

如果您不再需要收集快照映像、则可以删除现有快照计划。

关于此任务

删除快照计划时、不会同时删除关联的快照映像。如果您认为快照映像的收集可能在某个时刻恢复、则应暂停快照计划、而不是将其删除。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot schedules]。
2. 选择要删除的快照计划，单击 **Delete**，并确认操作。

结果

系统会从基础卷或快照一致性组中删除所有计划属性。

管理快照映像

在 **SANtricity System Manager** 中查看快照映像设置

您可以查看分配给每个快照映像的属性、状态、预留容量和关联对象。

关于此任务

快照映像的关联对象包括此快照映像为还原点的基础卷或快照一致性组、关联的快照组以及从快照映像创建的任何快照卷。使用快照设置确定是要复制还是转换快照映像。

步骤

1. 从左侧面板中，选择 **Snapshots › Snapshot images**。
2. 选择要查看的快照映像、然后单击*查看设置*。

   此时将显示Snapshot映像设置对话框。

3. 查看快照映像的设置。

在 **SANtricity System Manager** 中启动基本卷的快照映像回滚

您可以执行回滚操作来更改基础卷的内容、使其与保存在快照映像中的内容匹配。

回滚操作不会更改与基础卷关联的快照映像的内容。

开始之前

- 预留的容量足以启动回滚操作。
- 选定快照映像为最佳映像、选定卷为最佳卷。
- 选定卷尚未执行回滚操作。

关于此任务

通过回滚开始顺序、您可以在提供添加存储容量选项的同时、对基础卷的快照映像开始回滚。不能同时为基础卷启动多个回滚操作。

主机可以立即访问新的回滚基础卷、但在回滚开始后、现有基础卷不允许主机读写访问。您可以在开始回滚之前创建基础卷的快照、以保留回滚前的基础卷以供恢复。

步骤

1. 从左侧面板中，选择 **Snapshots › Snapshot images**。
2. 选择快照映像、然后选择菜单：Rollback[启动]。

   此时将显示确认开始回滚对话框。

3. *可选：*如果需要、选择*增加容量*选项。

   此时将显示增加预留容量对话框。

   a. 使用spinner框调整容量百分比。

      如果包含所选存储对象的池或卷组上不存在可用容量，且存储阵列具有未分配容量，则可以添加容量。您可以创建新的池或卷组，然后使用该池或卷组上的新可用容量重试此操作。

   b. 单击 * 增加 * 。
4. 确认要执行此操作、然后单击*回滚*。

结果

System Manager将执行以下操作：

- 还原包含保存在选定快照映像上的内容的卷。
- 使回滚卷可立即供主机访问。您无需等待回滚操作完成。

完成后

选择菜单：Monitoring[Operations in progress]以查看回滚操作的进度。

如果回滚操作不成功、此操作将暂停。您可以恢复已暂停的操作、如果仍不成功、请按照Recovery Guru操作步骤 更正问题或联系技术支持。

在 **SANtricity System Manager** 中启动快照一致性组成员卷的快照映像回滚

您可以执行回滚操作、以更改快照一致性组成员卷的内容、使其与保存在快照映像中的内容匹配。

回滚操作不会更改与快照一致性组关联的快照映像的内容。

开始之前

- 预留的容量足以启动回滚操作。
- 选定快照映像为最佳映像、选定卷为最佳卷。
- 选定卷尚未执行回滚操作。

关于此任务

通过回滚开始序列、您可以在快照一致性组的快照映像上开始回滚、同时提供添加存储容量的选项。不能同时为

快照一致性组启动多个回滚操作。

> 主机可以立即访问新的回滚卷、但在回滚开始后、现有成员卷不再允许主机读写访问。您可以在开始回滚之前创建成员卷的快照映像、以保留回滚前的基本卷以供恢复使用。

开始回滚快照一致性组的快照映像的过程是一个多步骤操作步骤。

第1步：选择成员

您必须选择要回滚的成员卷。

步骤

1. 从左侧面板中，选择 **Snapshots › Snapshot images**。
2. 选择快照一致性组快照映像、然后选择菜单：Rollback[启动]。

   此时将显示开始回滚对话框。

3. 选择一个或多个成员卷。
4. 单击*下一步*、然后执行以下操作之一：
   - 如果任何选定成员卷与多个存储快照映像的预留容量对象关联、则会显示查看容量对话框。转至 [第2步：查看容量]。
   - 如果选定成员卷均未与多个存储快照映像的预留容量对象关联、则会显示编辑优先级对话框。转至 [第3步：编辑优先级]。

第2步：查看容量

如果您选择了与多个预留容量对象关联的成员卷、例如快照组和预留容量卷、则可以查看并增加回滚卷的预留容量。

步骤

1. 在预留容量极低(或为零)的任何成员卷旁边、单击*编辑*列中的*增加容量*链接。

   此时将显示增加预留容量对话框。

2. 使用spinner框调整容量百分比、然后单击*增加*。

   如果包含所选存储对象的池或卷组上不存在可用容量，且存储阵列具有未分配容量，则可以添加容量。您可以创建新的池或卷组，并使用该池或卷组上的新可用容量重试此操作。

3. 单击*下一步*、然后转到 [第3步：编辑优先级]。

   此时将显示编辑优先级对话框。

第3步：编辑优先级

您可以根据需要编辑回滚操作的优先级。

关于此任务

回滚优先级决定了在牺牲系统性能的情况下专用于回滚操作的系统资源数量。

步骤

1. 使用滑块根据需要调整回滚优先级。
2. 确认要执行此操作、然后单击*完成*。

结果

System Manager将执行以下操作：

- 还原包含保存在选定快照映像上的内容的快照一致性组成员卷。
- 使回滚卷可立即供主机访问。您无需等待回滚操作完成。

完成后

选择菜单：Monitoring[Operations in progress]以查看回滚操作的进度。

如果回滚操作不成功、此操作将暂停。您可以恢复已暂停的操作、如果仍不成功、请按照Recovery Guru操作步骤 更正问题或联系技术支持。

在 **SANtricity System Manager** 中恢复快照映像回滚

如果在快照映像回滚操作期间发生错误、则此操作会自动暂停。您可以恢复处于暂停状态的回滚操作。

步骤

1. 从左侧面板中，选择 **Snapshots › Snapshot images**。
2. 突出显示已暂停的回滚、然后选择菜单：Rollback[恢复]。

   操作将恢复。

结果

System Manager将执行以下操作：

- 如果回滚操作成功恢复、您可以在操作进行中窗口中查看回滚操作的进度。
- 如果回滚操作不成功、则此操作将再次暂停。您可以按照Recovery Guru操作步骤 更正问题、也可以联系技术支持。

在 **SANtricity System Manager** 中取消快照映像回滚

您可以取消正在进行的活动回滚(主动复制数据)、正在等待资源启动的待定队列中的待定回滚或由于错误而暂停的回滚。

关于此任务

取消正在进行的回滚操作后、基础卷将恢复为不可用状态并显示为失败。因此、请考虑仅在存在用于还原基础卷内容的恢复选项时取消回滚操作。

> 如果快照映像所在的快照组具有一个或多个已自动清除的快照映像、则用于回滚操作的快照映像可能无法用于将来的回滚。

步骤

1. 从左侧面板中，选择 **Snapshots › Snapshot images**。
2. 选择活动或暂停的回滚、然后选择菜单：Rollback[Cancel]。

   此时将显示确认取消回滚对话框。

3. 单击*是*进行确认。

结果

System Manager将停止回滚操作。基础卷可用、但其数据可能不一致或不完整。

完成后

取消回滚操作后、必须执行以下操作之一：

- 重新初始化基础卷的内容。
- 执行新的回滚操作、以使用取消回滚操作中使用的相同快照映像或使用不同的快照映像来还原基础卷、以执行新的回滚操作。

在 **SANtricity System Manager** 中删除快照映像

您可以删除快照映像、以便从快照组或快照一致性组中清理最旧的快照映像。

关于此任务

您可以删除单个快照映像、也可以从创建时间戳相同的快照一致性组中删除快照映像。您还可以从快照组中删除快照映像。

如果快照映像不是关联基础卷或快照一致性组中最旧的快照映像、则无法删除该快照映像。

步骤

1. 从左侧面板中，选择 **Snapshots › Snapshot images**。
2. 选择要删除的快照映像、然后确认要执行此操作。

   如果选择了快照一致性组的快照映像、请选择要删除的每个成员卷、然后确认要执行此操作。

3. 单击 * 删除 * 。

结果

System Manager将执行以下操作：

- 从存储阵列中删除快照映像。
- 释放预留容量、以便在快照组或快照一致性组中重复使用。
- 禁用已删除快照映像的所有关联快照卷。
- 从快照一致性组删除中、将与已删除的快照映像关联的任何成员卷移至已停止状态。

管理快照一致性组

在 SANtricity System Manager 中将成员卷添加到快照一致性组

您可以将新成员卷添加到现有快照一致性组。添加新成员卷时、还必须为成员卷预留容量。

开始之前

- 成员卷必须是最佳卷。
- 快照一致性组必须小于允许的最大卷数(根据您的配置定义)。
- 每个预留容量卷都必须与关联成员卷具有相同的数据保证(Data Assurance、DA)和安全设置。

关于此任务

您可以向快照一致性组添加标准卷或精简卷。基础卷可以驻留在池或卷组中。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot consistency groups]。

   此时将显示此表、并显示与存储阵列关联的所有快照一致性组。

2. 选择要修改的快照一致性组、然后单击*添加成员*。

   此时将显示添加成员对话框。

3. 选择要添加的成员卷、然后单击*下一步*。

   此时将显示预留容量步骤。卷候选表仅显示支持指定预留容量的候选对象。

4. 使用spinner框为成员卷分配预留容量。执行以下操作之一：
   - 接受默认设置。

     使用此建议选项可使用默认设置为成员卷分配预留容量。

   - 分配您自己的预留容量设置以满足您的数据存储需求。

     如果更改默认预留容量设置、请单击*刷新候选容量*以刷新指定预留容量的候选列表。

     按照以下准则分配预留容量。

     - 预留容量的默认设置为基础卷容量的40%、通常此容量已足够。
     - 所需容量因卷I/O写入的频率和大小以及快照映像收集的数量和持续时间而异。
5. 单击*完成*以添加成员卷。

从 SANtricity System Manager 中的快照一致性组中删除成员卷

您可以从现有快照一致性组中删除成员卷。

关于此任务

从快照一致性组中删除成员卷时、System Manager会自动删除与该成员卷关联的快照对象。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot consistency groups]。
2. 通过选择要修改的快照一致性组旁边的加号(+)展开该组。
3. 选择要删除的成员卷、然后单击*删除*。
4. 确认要执行此操作、然后单击*删除*。

结果

System Manager将执行以下操作：

- 删除与成员卷关联的所有快照映像和快照卷。
- 删除与成员卷关联的快照组。
- 不会以其他方式更改或删除成员卷。

在 **SANtricity System Manager** 中更改快照一致性组的设置

如果要更改快照一致性组的名称、自动删除设置或允许的最大快照映像数、请更改该组的设置。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot consistency groups]。
2. 选择要编辑的快照一致性组、然后单击*查看/编辑设置*。

   此时将显示Snapshot一致性组设置对话框。

3. 根据需要更改快照一致性组的设置。

   ▼ 字段详细信息

正在设置 …	**Description**
• Snapshot一致性组设置*	Name
您可以更改快照一致性组的名称。	自动删除
如果要在指定限制后自动删除快照映像、请保持选中此复选框；使用spinner框更改此限制。如果清除此复选框、则在创建32个映像后将停止创建快照映像。	Snapshot映像限制
您可以更改快照组允许的最大快照映像数。	Snapshot计划
此字段指示计划是否与快照一致性组关联。	关联对象

正在设置 ...	Description
成员卷	您可以查看与快照一致性组关联的成员卷数量。

4. 单击 * 保存 * 。

在 SANtricity System Manager 中删除快照一致性组

您可以删除不再需要的快照一致性组。

开始之前

确认备份或测试不再需要所有成员卷的映像。

关于此任务

此操作将删除与快照一致性组关联的所有快照映像或计划。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot consistency groups]。
2. 选择要删除的快照一致性组、然后选择菜单：uncommon Tasks[Delete]。

   此时将显示确认删除Snapshot一致性组对话框。

3. 确认要执行此操作、然后单击*删除*。

结果

System Manager将执行以下操作：

- 从快照一致性组中删除所有现有快照映像和快照卷。
- 删除此快照一致性组中每个成员卷存在的所有关联快照映像。
- 删除Snapshot一致性组中每个成员卷存在的所有关联Snapshot卷。
- 删除快照一致性组中每个成员卷的所有关联预留容量(如果已选中)。

管理快照卷

在 SANtricity System Manager 中将快照卷转换为读写模式

如果需要、您可以将只读快照卷或快照一致性组快照卷转换为读写模式。

转换为读写可访问的Snapshot卷包含其自身的预留容量。此容量用于将主机应用程序随后所做的任何修改保存到基础卷、而不会影响引用的快照映像。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。

   此时将显示Snapshot Volumes表、其中显示了与存储阵列关联的所有Snapshot卷。

2. 选择要转换的只读Snapshot卷、然后单击*转换为读/写*。

此时将显示转换为读/写对话框、并激活*预留容量*步骤。卷候选表仅显示支持指定预留容量的候选对象。

3. 要为读写Snapshot卷分配预留容量、请执行以下操作之一：
   - 接受默认设置-使用此建议选项使用默认设置为快照卷分配预留容量。
   - 分配您自己的预留容量设置以满足数据存储需求-按照以下准则分配预留容量。
     - 预留容量的默认设置为基础卷容量的40%、通常此容量已足够。
     - 所需容量因向卷写入I/O的频率和大小而异。
4. 选择*下一步*以查看或编辑设置。

   此时将显示编辑设置对话框。

5. 根据需要接受或指定快照卷的设置、然后选择*完成*以转换快照卷。

   ▼ 字段详细信息

正在设置 ...	Description
预留容量设置	在以下情况下提醒我…

在 **SANtricity System Manager** 中更改快照卷的卷设置

您可以更改快照卷或快照一致性组快照卷的设置以对其进行重命名、启用或禁用SSD缓存、或者更改主机、主机集群或逻辑单元号(LUN)分配。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。
2. 选择要更改的快照卷、然后单击*查看/编辑设置*。

   此时将显示Snapshot Volume Settings对话框。

3. 根据需要查看或编辑快照卷的设置。

   ▼ 字段详细信息

正在设置 ...	Description
快照卷	Name
您可以更改快照卷的名称。卷名称最多可包含 30 个字符。名称必须是唯一的。	已分配给
您可以更改快照卷的主机或主机集群分配。	LUN
您可以更改快照卷的LUN分配。	SSD 缓存
您可以在固态磁盘(SSD)上启用/禁用只读缓存。	关联对象

正在设置 ...	Description
Snapshot映像	您可以查看与快照卷关联的快照映像。快照映像是指在特定时间点捕获的卷数据的逻辑副本。与还原点一样，您可以通过快照映像回滚到已知正常的数据集。尽管主机可以访问快照映像、但它无法直接对其进行读写。
基础卷	您可以查看与快照卷关联的基础卷。基础卷是创建快照映像的源卷。它可以是厚卷或精简卷、通常分配给主机。基础卷可以位于卷组或磁盘池中。
Snapshot组	您可以查看与快照卷关联的快照组。快照组是一组来自单个基础卷的快照映像。

在 **SANtricity System Manager** 中复制快照卷

您可以对快照卷或快照一致性组快照卷执行复制卷进程。

关于此任务

您可以在正常的复制卷操作中将快照卷复制到目标卷。但是、在复制卷过程中、Snapshot卷不能保持联机。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。

   此时将显示Snapshot Volumes表、其中显示了与存储阵列关联的所有Snapshot卷。

2. 选择要复制的快照卷、然后选择*复制卷*。

   此时将显示复制卷对话框、提示您选择目标。

3. 选择要用作复制目标的目标卷、然后单击*完成*。

在 **SANtricity System Manager** 中重新创建快照卷

您可以重新创建先前禁用的快照卷或快照一致性组快照卷。与创建新快照卷相比、重新创建快照卷所需时间更短。

开始之前

- 快照卷必须处于最佳或已禁用状态。
- 在重新创建快照一致性组快照卷之前、所有成员快照卷都必须处于已禁用状态。

关于此任务

您不能重新创建单个成员快照卷；只能重新创建整体快照一致性组快照卷。

如果快照卷或快照一致性组快照卷属于联机副本关系、则无法对卷执行重新创建选项。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。

   此时将显示Snapshot Volumes表、其中显示了与存储阵列关联的所有Snapshot卷。

2. 选择要重新创建的快照卷、然后选择菜单：uncommon Tasks[重新创建]。

此时将显示重新创建Snapshot卷对话框。

3. 选择以下选项之一：
   - *从卷<name>*创建的现有快照映像

     选择此选项可指示要从中重新创建快照卷的现有快照映像。

   - *卷<name>*的新(即时)快照映像

     选择此选项可创建新的快照映像、以便从中重新创建快照卷。

4. 单击*重新创建*。

结果

System Manager将执行以下操作：

- 删除任何关联Snapshot存储库卷上的所有`write`数据。
- Snapshot卷或Snapshot一致性组Snapshot卷参数与先前禁用的卷参数保持不变。
- 保留快照卷或快照一致性组快照卷的原始名称。

在 **SANtricity System Manager** 中禁用快照卷

如果您不再需要快照卷或希望暂时停止使用快照一致性组中的快照卷、可以将其禁用。

关于此任务

如果满足以下条件之一、请使用"Disable"选项：

- 您目前已完成快照卷或快照一致性组快照卷的使用。
- 您打算稍后重新创建快照卷或快照一致性组快照卷(指定为读写)、并希望保留关联的预留容量、以便不再需要重新创建它。
- 您希望通过停止对读写Snapshot卷的写入活动来提高存储阵列性能。

如果快照卷或快照一致性组快照卷指定为读写卷、则此选项还允许您停止对其关联的预留容量卷执行任何进一步的写入活动。如果您决定重新创建快照卷或快照一致性组快照卷、则必须从同一个基础卷中选择一个快照映像。

如果快照卷或快照一致性组快照卷属于联机副本关系、则无法对卷执行禁用选项。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。

   System Manager将显示与存储阵列关联的所有快照卷。

2. 选择要禁用的快照卷、然后选择菜单：uncommon Tasks[Disable]。
3. 确认要执行此操作、然后单击*禁用*。

结果

- 快照卷与其基础卷保持关联。

- 快照卷将保留其全球通用名称(WWN)。
- 如果为读写、则快照卷会保留其关联的预留容量。
- 快照卷会保留所有主机分配和访问权限。但是、读写请求会失败。
- 快照卷与其快照映像失去关联。

在 **SANtricity System Manager** 中删除快照卷

您可以删除备份或软件应用程序测试不再需要的快照卷或快照一致性组快照卷。

您还可以指定是要删除与`read-write` snapshot卷关联的Snapshot预留容量卷、还是将Snapshot预留容量卷保留为未分配的卷。

关于此任务

删除基础卷会自动删除任何关联的快照卷或一致性组快照卷。不能删除状态为*进行中*的卷副本中的快照卷。

步骤

1. 从左侧面板中，选择菜单：Snapshots[Snapshot volumes]。

   System Manager将显示与存储阵列关联的所有快照卷。

2. 选择要删除的快照卷、然后选择菜单：uncommon Tasks[Delete]。
3. 确认要执行此操作、然后单击*删除*。

结果

System Manager将执行以下操作：

- 删除所有成员Snapshot卷(对于快照一致性组快照卷)。
- 删除所有关联的主机分配。

SANtricity System Manager 快照常见问题解答

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。

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。您必须先在基础卷上禁用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。

什么是快照映像?

快照映像是在特定时间点捕获的卷内容的逻辑副本。Snapshot映像使用的存储空间极少。

Snapshot映像数据存储如下：

- 创建快照映像时、该映像与基础卷完全匹配。创建快照后、如果对基础卷上的任何块或块集发出首次写入请求、则在将新数据写入基础卷之前、原始数据会复制到快照预留容量。
- 后续快照仅包含自创建第一个快照映像以来发生更改的数据块。在将新数据写入基础卷之前、后续的每次写入时复制操作都会将基础卷上即将覆盖的原始数据保存到Snapshot预留容量中。

为什么使用**Snapshot**映像?

您可以使用快照防止数据意外或恶意丢失或损坏、并允许从这种情况中恢复。

选择一个基础卷或一组称为快照一致性组的基础卷、然后通过以下一种或多种方式捕获快照映像：

- 您可以为一个基础卷或一个由多个基础卷组成的快照一致性组创建快照映像。
- 您可以手动创建快照、也可以为基础卷或快照一致性组创建计划、以自动捕获定期快照映像。
- 您可以为快照映像创建主机可访问的快照卷。
- 您可以执行回滚操作以还原快照映像。

系统会保留多个快照映像作为还原点、您可以使用这些映像在特定时间点回滚到已知正常的数据集。回滚功能可防止数据意外删除和数据损坏。

可以使用哪些类型的卷来创建快照?

标准卷和精简卷是唯一可用于存储快照映像的卷类型。不能使用非标准卷。基础卷可以驻留在池或卷组上。

为什么要创建快照一致性组?

如果要确保同时在多个卷上创建快照映像、请创建快照一致性组。

例如、如果数据库由多个卷组成、并且需要保持一致才能进行恢复、则需要使用快照一致性组来收集所有卷的协调快照、并使用这些快照还原整个数据库。

快照一致性组中包含的卷称为_member volumes_。

您可以对快照一致性组执行以下快照操作：

- 创建快照一致性组的快照映像、以同时获取成员卷的映像。
- 为快照一致性组创建一个计划、以自动捕获成员卷的定期并发映像。
- 为快照一致性组映像创建主机可访问的快照卷。
- 对快照一致性组执行回滚操作。

什么是**Snapshot**卷？何时需要预留容量?

主机可通过Snapshot卷访问Snapshot映像中的数据。快照卷包含自己的预留容量、这样可以在不影响原始快照映像的情况下保存对基础卷所做的任何修改。主机无法读取或写入Snapshot映像。如果要读取或写入快照数

据、请创建一个快照卷并将其分配给主机。

您可以创建两种类型的快照卷。Snapshot卷的类型决定了它是否使用预留容量。

- 只读—创建为只读的快照卷可以使主机应用程序对快照映像中所含数据的副本具有读取访问权限。只读Snapshot卷不使用预留容量。
- 读写—创建为读写的快照卷可以在不影响引用的快照映像的情况下对快照卷进行更改。读写Snapshot卷使用预留容量存储这些更改。您可以随时将只读快照卷转换为读写卷。

什么是快照组?

Snapshot组是一个关联基础卷的时间点快照映像的集合。

System Manager会将快照映像组织为_snapshot groups_.Snapshot组无需用户操作、但您可以随时调整Snapshot组上的预留容量。此外、在满足以下条件时、系统可能会提示您创建预留容量:

- 每当为尚未创建快照组的基础卷创建快照时、System Manager都会自动创建快照组。这样会为基础卷创建预留容量、用于存储后续的快照映像。
- 每当为基础卷创建快照计划时、System Manager都会自动创建快照组。

为什么要禁用**Snapshot**卷?

如果要为快照映像分配不同的快照卷、则可以禁用快照卷。您可以预留已禁用的快照卷以供日后使用。

如果您不再需要快照卷或一致性组快照卷、并且不打算稍后重新创建该卷、则应删除该卷、而不是将其禁用。

什么是**"**已禁用**"**状态?

当前未将处于已禁用状态的快照卷分配给快照映像。要启用快照卷、必须使用重新创建操作为已禁用的快照卷分配新的快照映像。

快照卷的特征由分配给它的快照映像定义。在处于已禁用状态的快照卷上、读写活动将暂停。

为什么要暂停快照计划?

暂停计划后、不会按计划创建快照映像。您可以暂停快照计划以节省存储空间、然后稍后恢复计划的快照。

如果不需要快照计划、应删除该计划、而不是暂停该计划。

镜像

概述

了解 **SANtricity** 软件中的异步镜像

异步镜像功能提供了一种基于固件的控制器级别机制、用于在本地存储阵列和远程存储阵列之间进行数据复制。

什么是异步镜像?

_Asynchronous mirroring _捕获主卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。可以立即更新主站点、并在带宽允许的情况下更新二级站点。此信息将在网络资源可用时进行缓存并稍后发送。

异步镜像是按卷创建的、但在组级别进行管理、这样您就可以将一个不同的远程镜像卷与给定存储阵列上的任何主卷关联起来。这种类型的镜像最适合满足无中断操作的需求、而且通常对于定期流程来说、网络效率更高。

了解更多信息。

- "异步镜像的工作原理"
- "异步镜像术语"
- "异步镜像状态"
- "卷所有权"
- "镜像一致性组的角色更改"

如何配置异步镜像?

您必须使用Unified Manager界面在阵列之间执行初始镜像配置。配置后、您可以在System Manager中管理镜像对和一致性组。

了解更多信息。

- "使用异步镜像的要求"
- "异步镜像卷的工作流"
- "创建异步镜像对(在Unified Manager中)"

相关信息

详细了解与异步镜像相关的概念:

- "创建镜像一致性组之前需要了解的信息"
- "创建镜像对之前需要了解的信息"
- "异步镜像与同步镜像有何不同"

了解 **SANtricity** 软件中的同步镜像

同步镜像功能可在存储阵列之间远程进行联机实时数据复制。

此功能不适用于 EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统。

什么是同步镜像?

_Synchronous mirroring _实时复制数据卷以确保持续可用性。存储阵列控制器负责管理镜像操作、该操作对主机和软件应用程序是透明的。

这种类型的镜像非常适合用于灾难恢复等业务连续性目的。

了解更多信息。

- "同步镜像的工作原理"
- "同步镜像术语"
- "同步镜像状态"
- "卷所有权"
- "镜像对中的卷之间的角色更改"

如何配置同步镜像?

您必须使用Unified Manager界面在阵列之间执行初始镜像配置。配置后、您可以在System Manager中管理镜像对。

了解更多信息。

- "使用同步镜像的要求"
- "同步镜像卷的工作流"
- "创建同步镜像对(在Unified Manager中)"

相关信息

详细了解与同步镜像相关的概念：

- "创建镜像对之前需要了解的信息"
- "异步镜像与同步镜像有何不同"

异步概念

异步镜像在 **SANtricity System Manager** 中的工作方式

异步镜像可按需或按计划复制数据卷、从而最大限度地减少或避免因数据损坏或丢失而导致的停机时间。

异步镜像可捕获主卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。可以立即更新主站点、并在带宽允许的情况下更新二级站点。此信息将在网络资源可用时进行缓存并稍后发送。

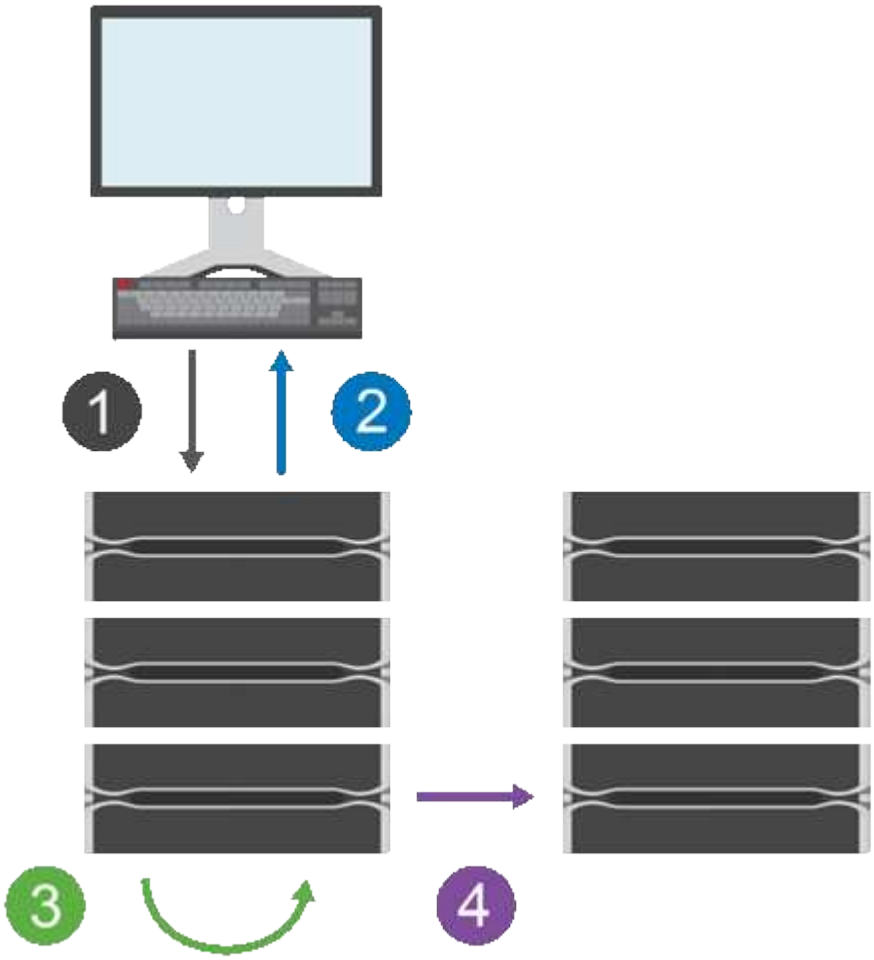
这种类型的镜像最适合满足无中断操作的需求、而且通常对于备份和归档等定期过程来说、网络效率更高。使用异步镜像的原因如下：

- 远程备份整合。
- 防止发生本地或广域灾难。
- 在实时数据的时间点映像上进行应用程序开发和测试。

异步镜像会话

异步镜像可捕获主卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。通过异步镜像、可以立即更新主站点、并在带宽允许的情况下更新二级站点。此信息将在网络资源可用时进行缓存并稍后发送。

活动异步镜像会话有四个主要步骤。



1. 首先在主卷的存储阵列上执行写入操作。
2. 操作的状态将返回给主机。
3. 系统会记录并跟踪主卷上的所有更改。
4. 所有更改都会作为后台进程发送到二级卷的存储阵列。

这些步骤会根据定义的同步间隔重复、如果未定义任何间隔、也可以手动重复这些步骤。

异步镜像只会按设定的时间间隔将数据传输到远程站点、因此本地I/O不会受到网络连接速度较慢的影响。由于此传输与本地I/O无关、因此不会影响应用程序性能。因此、异步镜像可以使用iSCSI等速度较慢的连接、并在本地和远程存储系统之间运行较长的距离。

存储阵列的最低固件版本必须为7.84。(它们可以分别运行不同的操作系统版本。)

镜像一致性组和镜像对

您可以创建镜像一致性组、以便在本地存储阵列和远程存储阵列之间建立镜像关系。异步镜像关系由一个镜像对组成：一个存储阵列上的主卷和另一个存储阵列上的二级卷。

包含主卷的存储阵列通常位于主站点、并为活动主机提供服务。包含二级卷的存储阵列通常位于二级站点、并保存数据的副本。二级卷通常包含数据的备份副本、用于灾难恢复。

同步设置

创建镜像对时、还需要定义同步优先级和重新同步策略、镜像对使用该策略在通信中断后完成重新同步操作。

创建镜像一致性组时、还可以为组中的所有镜像对定义同步优先级和重新同步策略。镜像对使用同步优先级和重新同步策略在通信中断后完成重新同步操作。

如果主卷的存储阵列无法向二级卷写入数据、则镜像对中的主卷和二级卷可能会变得不同步。此情况可能由以下问题引起：

- 本地和远程存储阵列之间的网络问题。
- 二级卷发生故障。
- 正在镜像对上手动暂停同步。
- 镜像组角色冲突。

您可以手动或自动同步远程存储阵列上的数据。

预留容量和异步镜像

预留容量用于跟踪未进行同步时主卷与二级卷之间的差异。它还会跟踪每个镜像对的同步统计信息。

镜像对中的每个卷都需要自己的预留容量。

配置和管理

要在两个阵列之间启用和配置镜像、必须使用Unified Manager界面。启用镜像后、您可以在System Manager中管理镜像对和同步设置。

了解 **SANtricity** 软件中的异步镜像术语

了解异步镜像术语如何应用于存储阵列。

期限	**Description**
本地存储阵列	本地存储阵列是您要对其执行操作的存储阵列。 如果本地角色列中显示*主*、则表示存储阵列包含在镜像关系中担任主角色的卷。如果本地角色列中显示*二级*、则表示存储阵列包含在镜像关系中具有二级角色的卷。
镜像一致性组	镜像一致性组是一个或多个镜像对的容器。对于异步镜像操作、必须创建镜像一致性组。
镜像对	镜像对由两个卷组成、一个是主卷、一个是二级卷。 在异步镜像中、镜像对始终属于镜像一致性组。首先对主卷执行写入操作、然后将其复制到二级卷。镜像一致性组中的每个镜像对共享相同的同步设置。
主卷	镜像对的主卷是要镜像的源卷。
远程存储阵列	远程存储阵列通常指定为二级站点、该站点通常在镜像配置中保存数据的副本。
预留容量	预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

期限	Description
角色更改	角色更改会将主角色分配给二级卷、反之亦然。
二级卷	镜像对的二级卷通常位于二级站点、并保存数据的副本。
同步	在本地存储阵列与远程存储阵列之间进行初始同步时进行同步。如果在通信中断后主卷和二级卷未同步、则也会发生同步。当通信链路重新工作时、任何未复制的数据都会同步到二级卷的存储阵列。

在 **SANtricity** 软件中异步镜像卷

您可以使用以下工作流配置异步镜像。

1. 在Unified Manager中执行初始配置：
   a. 选择本地存储阵列作为数据传输的源。
   b. 创建或选择现有镜像一致性组、该组是本地阵列上主卷和远程阵列上二级卷的容器。主卷和二级卷称为"镜像对"。 如果您是首次创建镜像一致性组、则可以指定是要执行手动同步还是计划同步。
   c. 从本地存储阵列中选择主卷、然后确定其预留容量。预留容量是为复制操作分配的物理容量。
   d. 选择一个远程存储阵列作为传输的目标、一个二级卷、然后确定其预留容量。
   e. 开始从主卷到二级卷的初始数据传输。根据卷大小、此初始传输可能需要几小时的时间。
2. 检查初始同步的进度：
   a. 在Unified Manager中、为本地阵列启动System Manager。
   b. 在System Manager中、查看镜像操作的状态。镜像完成后、镜像对的状态为"最佳"。
3. *可选：*您可以在System Manager中重新计划或手动执行后续数据传输。只有新的块和更改的块才会从主卷传输到二级卷。

> 由于异步复制是定期进行的、因此系统可以整合更改的块并节省网络带宽。对写入吞吐量和写入延迟的影响最小。

在 **SANtricity** 软件中使用异步镜像的要求

如果您计划使用异步镜像、请记住以下要求。

Unified Manager

要在两个阵列之间启用和配置镜像、必须使用Unified Manager界面。Unified Manager与Web服务代理一起安装在主机系统上。

- Web服务代理服务必须正在运行。
- Unified Manager必须通过HTTPS连接在本地主机上运行。
- Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

存储阵列

- 您必须有两个存储阵列。
- 每个存储阵列必须具有两个控制器。
- 必须在Unified Manager中发现这两个存储阵列。
- 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
- 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
- 您必须知道本地和远程存储阵列的密码。
- 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
- 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。

支持的连接

异步镜像可以使用FC或iSCSI连接、也可以同时使用这两种连接在本地和远程存储系统之间进行通信。在创建镜像一致性组时、如果这两个组都连接到远程存储阵列、则管理员可以为此组选择FC或iSCSI。不会从一种通道类型故障转移到另一种通道类型。

异步镜像使用存储阵列的主机端I/O端口将镜像数据从主端传输到二级端。

- 通过光纤通道**(FC)**接口镜像

  存储阵列的每个控制器都将其编号最高的FC主机端口专用于镜像操作。

  如果控制器同时具有基本FC端口和主机接口卡(HIC) FC端口、则编号最高的端口位于HIC上。登录到专用端口的任何主机都将注销、并且不接受任何主机登录请求。只有参与镜像操作的控制器才会接受此端口上的I/O请求。

  专用镜像端口必须连接到支持目录服务和名称服务接口的FC网络结构环境。特别是、不支持将FC-AL和点对点作为参与镜像关系的控制器之间的连接选项。

- 通过**iSCSI**接口镜像

  与FC不同、iSCSI不需要专用端口。在iSCSI环境中使用异步镜像时、无需将存储阵列的任何前端iSCSI端口专用于异步镜像；这些端口可用于异步镜像流量和主机到阵列I/O连接。

  控制器会维护一个远程存储系统列表、iSCSI启动程序会尝试与这些系统建立会话。成功建立iSCSI连接的第一个端口将用于此后与该远程存储阵列进行的所有通信。如果通信失败、则会尝试使用所有可用端口进行新会话。

  iSCSI端口在阵列级别逐个端口进行配置。用于配置消息传送和数据传输的控制器间通信使用全局设置、包括以下设置：

  - VLAN：本地系统和远程系统必须具有相同的VLAN设置才能进行通信
  - iSCSI侦听端口
  - 巨型帧

    建议使用巨型帧以提高 CPU 性能、吞吐量和功能稳定性。

◦ 以太网优先级

iSCSI控制器间通信必须使用主机连接端口、而不是管理以太网端口。

异步镜像使用存储阵列的主机端I/O端口将镜像数据从主端传输到二级端。由于异步镜像适用于延迟较高、成本较低的网络、因此iSCSI (以及基于TCP/IP的连接)非常适合它。在iSCSI环境中使用异步镜像时、无需将阵列的任何前端iSCSI端口专用于异步镜像；这些端口可用于异步镜像流量和主机到阵列I/O连接

E4000 使用 iSCSI 协议时不支持异步镜像。

镜像卷候选项

- 异步镜像对的主卷和二级卷上的RAID级别、缓存参数和区块大小可能不同。

对于EF600和EF300控制器、异步镜像对中的主卷和二级卷必须匹配相同的协议、托盘级别、区块大小、安全类型和RAID级别。不符合条件的异步镜像对不会显示在可用卷列表中。

- 二级卷必须至少与主卷大小相同。
- 一个卷只能参与一个镜像关系。
- 卷候选项必须共享相同的数据安全功能。
  - 如果主卷支持FIPS、则二级卷必须支持FIPS。
  - 如果主卷支持FDE、则二级卷必须支持FDE。
  - 如果主卷未使用驱动器安全、则二级卷不得使用驱动器安全。
- 主卷和二级卷必须共享相同的驱动器类型。不支持在主卷和二级卷之间混用NVMe和SAS驱动器。
- 主卷和辅助卷不得启用资源调配。

预留容量

- 主卷和镜像对中的二级卷需要预留容量卷、以便记录写入信息、以便从控制器重置和其他临时中断中恢复。
- 由于镜像对中的主卷和二级卷都需要额外的预留容量、因此您必须确保镜像关系中的两个存储阵列都具有可用容量。
- 预留容量卷必须与其关联的镜像卷共享相同的驱动器类型。
  - 如果预留容量卷是在NVMe驱动器上创建的、则其镜像卷也必须在NVMe驱动器上创建。
  - 如果预留容量卷是在SAS驱动器上创建的、则其镜像卷也必须在SAS驱动器上创建。

驱动器安全功能

- 如果您使用的是支持安全的驱动器、则主卷和二级卷必须具有兼容的安全设置。此限制不会强制实施；因此、您必须自行验证。
- 如果使用的是支持安全的驱动器、则主卷和二级卷应使用相同的驱动器类型。此限制不会强制实施；因此、您必须自行验证。
- 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。

在 **SANtricity System Manager** 中查看异步镜像状态

镜像状态用于定义镜像一致性组和镜像卷对的状态。

镜像一致性组的状态

Status	Description
同步(初始同步)	在镜像卷对之间完成的初始数据同步的进度。 在初始同步期间、卷可以过渡到以下状态：已降级/失败/最佳/未知。
同步(间隔同步)	在镜像卷对之间完成的定期数据同步的进度。
系统已暂停	存储系统在镜像一致性组级别暂停同步所有镜像对上的数据。 镜像一致性组中至少有一个镜像对处于已停止或失败状态。
用户已暂停	在镜像一致性组级别、用户暂停同步所有镜像对上的数据。 此状态有助于减少在将本地存储阵列上的任何更改数据复制到远程存储阵列时可能对主机应用程序产生的任何性能影响。
已暂停	由于访问远程存储阵列时出错、数据同步过程已暂时暂停。
孤立	如果在一致性镜像组的一端(主端或二级端)上删除了一致性镜像组中的成员卷、而不是在另一端删除了该成员卷、则会存在孤立的镜像对卷。 在恢复阵列间通信且镜像配置的两端协调镜像参数时、系统会检测到孤立的镜像对卷。 您可以删除镜像对以更正孤立的镜像对状态。
角色更改待定/进行中	镜像一致性组之间的角色更改处于待定状态或正在进行中。 角色反转更改(对主角色或二级角色)会影响选定镜像一致性组中的所有异步镜像对。 您可以取消待定角色更改、但不能取消正在进行的角色更改。
角色冲突	在角色更改操作期间、由于本地存储阵列与远程存储阵列之间存在通信问题、镜像一致性组之间发生角色冲突。 解决通信问题后、将发生角色冲突。使用Recovery Guru从此错误中恢复。 解决角色冲突时、不允许强制升级。

镜像对的状态

镜像对的状态指示主卷和二级卷上的数据是否已同步。

Status	Description
正在同步	在镜像对之间完成的初始或定期数据同步的进度。 同步有两种类型：初始同步和定期同步。初始同步进度也会显示在长时间运行操作对话框中。
最佳	镜像对中的卷会进行同步、这表示存储阵列之间的连接正常运行、并且每个卷都处于所需的工作状态。
未完成	远程存储阵列上的异步镜像对不完整、因为镜像对创建序列是在System Manager不支持的存储阵列上启动的、而镜像对尚未在二级存储阵列上完成。 将卷添加到远程存储阵列上的镜像一致性组后、镜像对创建过程完成。此卷将成为异步镜像对中的二级卷。 如果远程存储阵列由System Manager管理、则镜像对将自动完成。
失败	由于主卷、二级卷或镜像预留容量出现故障、异步镜像操作无法正常运行。
孤立	如果在一致性镜像组的一端(主端或二级端)上删除了一致性镜像组中的成员卷、而不是在另一端删除了该成员卷、则会存在孤立的镜像对卷。 在两个存储阵列之间恢复通信且镜像配置的两端协调镜像参数时、系统会检测到孤立的镜像对卷。 您可以删除镜像对以更正孤立的镜像对状态。
已停止	镜像对处于stopped状态、因为镜像一致性组处于系统暂停状态。

了解 **SANtricity** 软件中异步镜像的卷所有权

您可以更改镜像对中的首选控制器所有者。

如果镜像对的主卷属于控制器A、则二级卷也属于远程存储阵列的控制器A。更改主卷的所有者将自动更改二级卷的所有者、以确保这两个卷都属于同一控制器。主端的当前所有权更改会自动传播到辅端的相应当前所有权更改。

例如、主卷由控制器A拥有、然后将控制器所有者更改为控制器B在这种情况下、下次远程写入会将二级卷的控制器所有者从控制器A更改为B由于二级控制器所有权更改由主控制、因此不需要存储管理员进行任何特殊干预。

控制器重置

控制器重置会导致主端的卷所有权从首选控制器所有者更改为存储阵列中的备用控制器。

有时、远程写入会因控制器重置或存储阵列重新启动而中断、然后才能写入二级卷。在这种情况下、控制器不需要对镜像对执行完全同步。

如果在控制器重置期间远程写入中断、则主端的新控制器所有者将读取存储在首选控制器所有者的预留容量卷中的日志文件中的信息。然后、新控制器所有者将受影响的数据块从主卷复制到二级卷、从而无需对镜像卷进行完全同步。

在 SANtricity 软件中更改镜像一致性组角色

您可以更改镜像一致性组中镜像对之间的角色。为此、您可以将主镜像一致性组降级为二级角色、或者将二级镜像一致性组提升为主角色。

查看有关角色更改操作的以下信息：

- 角色更改会影响选定镜像一致性组中的所有镜像对。
- 当镜像一致性组降级到二级角色时、该镜像一致性组中的所有镜像对也会降级到二级角色、反之亦然。
- 当主镜像一致性组降级为二级角色时、已分配给该组中成员卷的主机将不再具有对其的写入访问权限。
- 将镜像一致性组提升为主角色后、访问该组中成员卷的所有主机现在都可以向其写入数据。
- 如果本地存储阵列无法与远程存储阵列通信、您可以在本地存储阵列上强制更改角色。

强制更改角色

如果本地存储阵列与远程存储阵列之间的通信问题阻止提升二级镜像一致性组中的成员卷或使主镜像一致性中的成员卷降级、则可以强制更改镜像一致性组之间的角色 组。

您可以强制二级端上的镜像一致性组过渡到主角色。之后、恢复主机便可访问该镜像一致性组中新提升的成员卷、业务运营便可继续进行。

何时允许和不允许强制促销?

只有在镜像一致性组的所有成员卷均已同步且具有一致的恢复点时、才允许强制提升镜像一致性组。

在以下情况下、不允许强制提升镜像一致性组：

- 镜像一致性组的任何成员卷都正在进行初始同步。
- 镜像一致性组的任何成员卷都没有恢复点的时间点映像(例如、由于预留的容量全满错误)。
- 镜像一致性组不包含成员卷。
- 镜像一致性组处于Failed、Role-Change-Pending或Role-Change-in-progress状态、或者任何关联成员卷或预留容量卷出现故障。

镜像组角色冲突

解决本地和远程存储阵列之间的通信问题后、将发生镜像组角色冲突情况。使用Recovery Guru从此错误中恢复。解决双重角色冲突时、不允许强制升级。

要避免出现镜像组角色冲突情况并执行后续恢复步骤、请等待存储阵列之间的连接正常运行、以强制更改角色。

角色更改正在进行中状态

如果镜像配置中的两个存储阵列断开连接、并且镜像一致性组的主端强制降级为二级角色、而镜像一致性组的二级端强制提升为主角色、 然后、在恢复通信后、两个存储阵列上的镜像一致性组将置于Role-Change-in-progress状态。

系统将通过传输更改日志、重新同步、将镜像一致性组状态设置回正常运行状态以及继续定期同步来完成角色更改过程。

同步概念

SANtricity System Manager 中的同步镜像工作原理

同步镜像可实时复制数据卷、以确保持续可用性。

EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储阵列上不提供同步镜像。

同步镜像可在两个存储阵列之一发生灾难时为重要数据提供一份副本、从而实现零丢失数据的恢复点目标(RPO)。副本与生产数据在每一刻都是相同的、因为每次对主卷执行写入时、都会对二级卷执行写入。在使用主卷上所做的更改成功更新二级卷之前、主机不会收到写入成功的确认。

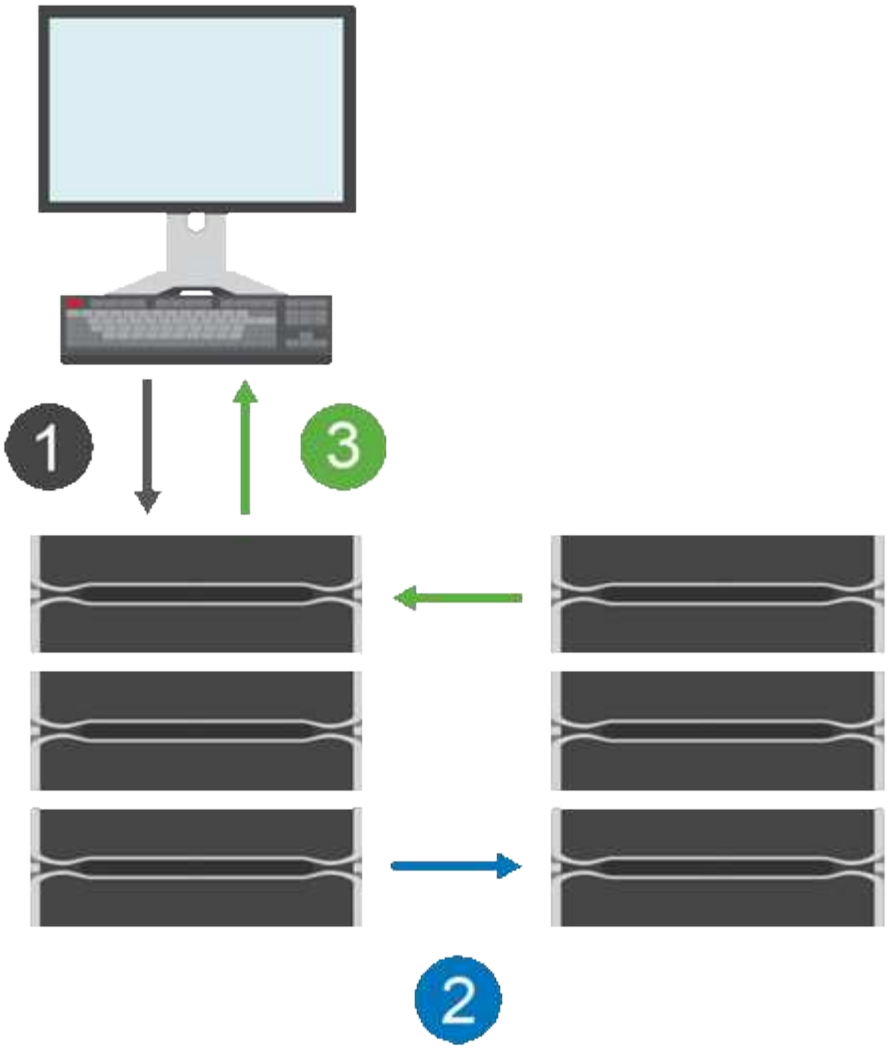
这种类型的镜像非常适合用于灾难恢复等业务连续性目的。

同步镜像关系

同步镜像关系由一个主卷和一个位于不同存储阵列上的二级卷组成。包含主卷的存储阵列通常位于主站点、并为活动主机提供服务。包含二级卷的存储阵列通常位于二级站点、并保存数据的副本。如果主卷的存储阵列因完全断电、火灾或主站点的硬件故障等原因而不可用、则会使用二级卷。

同步镜像会话

同步镜像配置过程涉及将卷配置成对。创建镜像对后、您可以启动同步镜像、该镜像对由一个存储阵列上的主卷和另一个存储阵列上的二级卷组成。同步镜像的步骤如下所示。



1. 写入来自主机。
2. 写入将提交到主卷、并传播到远程系统、然后提交到二级卷。
3. 主卷的存储阵列会向主机系统_after_发送一条I/O完成消息、两个写入操作均已成功完成。

预留容量用于记录有关从主机传入的写入请求的信息。

当主卷的当前控制器所有者收到来自主机的写入请求时、控制器会首先将有关写入的信息记录到主卷的预留容量中。然后、它会将数据写入主卷。接下来、控制器将启动远程写入操作、将受影响的数据块复制到远程存储阵列上的二级卷。

由于主机应用程序必须等待本地存储阵列上以及远程存储阵列上的网络上发生写入、 要在不会过度降低本地I/O性能的情况下保持镜像关系、需要在本地存储阵列与远程存储阵列之间建立非常快速的连接。

灾难恢复

同步镜像可维护物理上远离数据所在站点的数据副本。如果主站点发生灾难、例如断电或洪灾、可以从二级站点快速访问数据。

在同步镜像操作期间、二级卷不可用于托管应用程序、因此、如果本地存储阵列发生灾难、您可以故障转移到远程存储阵列。要进行故障转移、请将二级卷提升为主角色。之后、恢复主机便可访问新提升的卷、业务运营便可继续进行。

同步设置

创建镜像对时、还需要定义同步优先级和重新同步策略、镜像对使用该策略在通信中断后完成重新同步操作。

如果两个存储阵列之间的通信链路停止工作、主机将继续从本地存储阵列接收确认、以防止访问丢失。当通信链路重新工作时、任何未复制的数据都可以自动或手动重新同步到远程存储阵列。

数据是否自动重新同步取决于镜像对的重新同步策略。自动重新同步策略允许镜像对在链路重新工作时自动重新同步。手动重新同步策略要求您在出现通信问题后手动恢复同步。建议使用手动重新同步策略。

您只能在包含主卷的存储阵列上编辑镜像对的同步设置。

未同步的数据

如果主卷的存储阵列无法向二级卷写入数据、则主卷和二级卷将不同步。这可能是由于以下问题导致的：

- 本地和远程存储阵列之间的网络问题
- 二级卷发生故障
- 正在镜像对上手动暂停同步

孤立镜像对

如果在一端(主端或二级端)删除了成员卷、而在另一端未删除、则会存在孤立的镜像对卷。

在恢复阵列间通信且镜像配置的两端协调镜像参数时、系统会检测到孤立的镜像对卷。

您可以删除镜像对以更正孤立的镜像对状态。

配置和管理

要在两个阵列之间启用和配置镜像、必须使用Unified Manager界面。启用镜像后、您可以在System Manager中管理镜像对和同步设置。

了解 **SANtricity** 软件中的同步镜像术语

了解同步镜像术语如何应用于存储阵列。

期限	**Description**
本地存储阵列	本地存储阵列是您要对其执行操作的存储阵列。 如果本地角色列中显示*主*、则表示存储阵列包含在镜像关系中担任主角色的卷。如果本地角色列中显示*二级*、则表示存储阵列包含在镜像关系中具有二级角色的卷。
镜像对	镜像对由两个卷组成、一个是主卷、一个是二级卷。
主卷	镜像对的主卷是要镜像的源卷。
恢复点目标(RPO)	恢复点目标(Recovery Point Objective、RPO)表示一个目标、表示镜像对中的主卷和二级卷之间的差异可接受。RPO为零表示主卷与二级卷之间不能存在任何差异。如果RPO大于零、则表示二级卷的电流较低或滞后于主卷。
远程存储阵列	远程存储阵列通常指定为二级站点、该站点通常在镜像配置中保存数据的副本。

期限	Description
预留容量	预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。
角色更改	角色更改会将主角色分配给二级卷、反之亦然。
二级卷	镜像对的二级卷通常位于二级站点、并保存数据的副本。
同步	在本地存储阵列与远程存储阵列之间进行初始同步时进行同步。如果在通信中断后主卷和二级卷未同步、则也会发生同步。当通信链路重新工作时、任何未复制的数据都会同步到二级卷的存储阵列。

在 **SANtricity** 软件中同步镜像卷

您可以使用以下工作流配置同步镜像。

此功能不适用于 EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统。

1. 在Unified Manager中执行初始配置：
   a. 选择一个本地存储阵列作为数据传输的源。
   b. 从本地存储阵列中选择主卷。
   c. 选择一个远程存储阵列作为数据传输的目标、然后选择一个二级卷。
   d. 选择同步和重新同步优先级。
   e. 开始从主卷到二级卷的初始数据传输。根据卷大小、此初始传输可能需要几小时的时间。
2. 检查初始同步的进度：
   a. 在Unified Manager中、为本地阵列启动System Manager。
   b. 在System Manager中、查看镜像操作的状态。镜像完成后、镜像对的状态为"最佳"。 这两个阵列会尝试通过正常操作保持同步。只有新的块和更改的块才会从主卷传输到二级卷。
3. *可选：*您可以在System Manager中更改同步设置。

由于同步复制是持续的、因此两个站点之间的复制链路必须提供足够的带宽功能。

在 **SANtricity** 软件中使用同步镜像的要求

如果您计划使用同步镜像、请记住以下要求。

Unified Manager

要在两个阵列之间启用和配置镜像、必须使用Unified Manager界面。Unified Manager与Web服务代理一起安装在主机系统上。

- Web服务代理服务必须正在运行。
- Unified Manager必须通过HTTPS连接在本地主机上运行。
- Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

存储阵列

EF80、EF50、EF300/EF300C 或 EF600/EF600C 存储阵列上不提供同步镜像。

- 您必须有两个存储阵列。
- 每个存储阵列必须具有两个控制器。
- 必须在Unified Manager中发现这两个存储阵列。
- 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
- 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
- 您必须知道本地和远程存储阵列的密码。
- 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
- 本地和远程存储阵列通过光纤通道网络结构进行连接。

支持的连接

只有具有光纤通道(FC)主机端口的控制器才支持同步镜像通信。

同步镜像使用本地存储阵列和远程存储阵列上每个控制器上编号最高的主机端口。控制器主机总线适配器(HBA)主机端口4通常预留用于镜像数据传输。

镜像卷候选项

- 同步镜像对的主卷和二级卷上的RAID级别、缓存参数和区块大小可能不同。
- 同步镜像对中的主卷和二级卷必须是标准卷。它们不能是精简卷或快照卷。
- 二级卷必须至少与主卷大小相同。
- 在卷复制操作中、只有主卷可以具有关联的快照和/或源卷或目标卷。
- 一个卷只能参与一个镜像关系。
- 给定存储阵列上支持的卷数量存在限制。确保存储阵列上已配置的卷数小于支持的限制。当同步镜像处于活动状态时、创建的两个预留容量卷将计入卷限制。

预留容量

- 主卷和二级卷需要预留容量、以便记录写入信息、以便从控制器重置和其他临时中断中恢复。
- 激活同步镜像后、系统会自动创建预留容量的卷。由于镜像对中的主卷和二级卷都需要预留容量、因此您必须确保参与同步镜像关系的两个存储阵列上都有足够的可用容量。

驱动器安全功能

- 如果您使用的是支持安全的驱动器、则主卷和二级卷必须具有兼容的安全设置。此限制不会强制实施；因此、您必须自行验证。
- 如果使用的是支持安全的驱动器、则主卷和二级卷应使用相同的驱动器类型。此限制不会强制实施；因此、您必须自行验证。
  - 如果主卷使用全磁盘加密(Full Disk Encryption、FDE)驱动器、则二级卷应使用FDE驱动器。
  - 如果主卷使用经联邦信息处理标准140-2 (FIPS)验证的驱动器、则二级卷应使用经FIPS 140-2验证的驱

动器。

- 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。

了解 **SANtricity System Manager** 中的同步镜像状态

同步镜像对的状态指示主卷和二级卷上的数据是否已同步。镜像状态与镜像对中卷的组件状态无关。

此功能不适用于 EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统。

同步镜像对可以具有以下状态之一：

- 最佳

  指示镜像对中的卷已同步、这意味着存储阵列之间的网络结构连接正常运行、并且每个卷都处于所需的工作状态。

- 正在同步

  显示了镜像对之间的数据同步进度。此状态也会在初始同步期间显示。

  在通信链路中断后、只有在链路中断期间主卷上发生更改的数据块才会复制到二级卷。

- 未同步

  指示主卷的存储阵列无法向远程阵列写入传入数据。本地主机可以继续向主卷写入数据、但不会进行远程写入。不同的情况可能会阻止主卷的存储阵列将传入数据写入二级卷、例如：

  - 无法访问此二级卷。
  - 无法访问远程存储阵列。
  - 无法访问存储阵列之间的网络结构连接。
  - 无法使用新的全球通用标识符(World Wide Identifier、WWID)更新二级卷。

- 已暂停

  指示同步镜像操作已被用户暂停。暂停镜像对后、不会尝试访问二级卷。对主卷的任何写入都会持久记录在镜像预留容量卷中。

- 失败

  表示由于主卷、二级卷或镜像预留容量出现故障、同步镜像操作无法正常运行。

了解 **SANtricity** 软件中同步镜像的卷所有权

您可以更改镜像对中的首选控制器所有者。

此功能不适用于 EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上的同步镜像。

如果镜像对的主卷属于控制器A、则二级卷也属于远程存储阵列的控制器A。更改主卷的所有者将自动更改二级

卷的所有者、以确保这两个卷都属于同一控制器。主端的当前所有权更改会自动传播到辅端的相应当前所有权更改。

例如、主卷由控制器A拥有、然后将控制器所有者更改为控制器B在这种情况下、下次远程写入会将二级卷的控制器所有者从控制器A更改为B由于二级控制器所有权更改由主控制、因此不需要存储管理员进行任何特殊干预。

控制器重置

控制器重置会导致主端的卷所有权从首选控制器所有者更改为存储阵列中的备用控制器。

有时、远程写入会因控制器重置或存储阵列重新启动而中断、然后才能写入二级卷。在这种情况下、控制器不需要对镜像对执行完全同步。

如果在控制器重置期间远程写入中断、则主端的新控制器所有者将读取存储在首选控制器所有者的预留容量卷中的日志文件中的信息。然后、新控制器所有者将受影响的数据块从主卷复制到二级卷、从而无需对镜像卷进行完全同步。

了解 **SANtricity** 软件中镜像对中的卷角色变化

您可以更改镜像对中卷之间的角色。为此、您可以将主卷降级为二级角色或将二级卷提升为主角色。

EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

查看有关角色更改操作的以下信息：

- 当主卷降级为二级角色时、该镜像对中的二级卷将提升为主角色、反之亦然。
- 当主卷降级为二级角色时、已分配给该卷的主机将不再具有对该卷的写入访问权限。
- 当二级卷提升为主角色时、访问该卷的所有主机现在都能够向该卷写入数据。
- 如果本地存储阵列无法与远程存储阵列通信、您可以在本地存储阵列上强制更改角色。

强制更改角色

如果本地存储阵列与远程存储阵列之间的通信问题导致无法提升二级卷或使主卷降级、则可以强制在镜像对中的卷之间更改角色。

您可以强制二级卷过渡到主角色。然后、恢复主机可以访问新提升的卷、业务运营可以继续进行。

当远程存储阵列已恢复且任何通信问题均已解决时、将发生同步镜像-主卷冲突情况。恢复步骤包括重新同步卷。使用Recovery Guru从此错误中恢复。

何时允许和不允许强制促销?

在以下情况下、不允许强制提升镜像对中的卷：

- 镜像对中的任何卷都正在进行初始同步。
- 镜像对处于Failed、Role-Change-Pending或Role-Change-in-progress状态、或者任何关联的预留容量卷出现故障。

角色更改正在进行中状态

如果镜像配置中的两个存储阵列断开连接、并且镜像对的主卷强制降级为二级角色、而镜像对的二级卷强制提升为主角色、 然后、在恢复通信后、两个存储阵列上的卷将置于Role-Change-in-progress状态。

系统将通过传输更改日志、重新同步、将镜像对状态设置回正常运行状态以及继续同步来完成角色更改过程。

管理异步镜像一致性组

在 **SANtricity System Manager** 中测试镜像一致性组的通信

您可以测试通信链路、以诊断本地存储阵列与与镜像一致性组关联的远程存储阵列之间可能存在的通信问题。

开始之前

要测试的镜像一致性组必须位于本地和远程存储阵列上。

关于此任务

您可以运行四种不同的测试：

- 连接-验证两个控制器是否具有通信路径。连接测试会在存储阵列之间发送一条阵列间消息、然后验证远程存储阵列上的相应镜像一致性组是否存在。它还会验证远程存储阵列上的镜像一致性组的成员卷是否与本地存储阵列上的镜像一致性组的成员卷匹配。
- 延迟-向与镜像一致性组关联的远程存储阵列上的每个镜像卷发送SCSI测试单元命令、以测试最小、平均和最大延迟。
- 带宽—向远程存储阵列发送两条阵列间消息、以测试执行测试的阵列上端口的最小、平均和最大带宽以及协商的链路速度。
- 端口连接-显示本地存储阵列上用于镜像的端口以及远程存储阵列上接收镜像数据的端口。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡、然后选择要测试的镜像一致性组。
3. 选择*测试通信*。

   此时将显示测试通信对话框。
4. 选择一个或多个要在与选定镜像一致性组关联的本地和远程存储阵列之间执行的通信测试、然后单击*测试*。
5. 查看结果窗口中显示的信息。

通信测试状态	**Description**
正常、无错误	镜像一致性组正在正确通信。
已通过状态(但不正常)	请检查可能的网络或连接问题、然后重试此测试。
失败状态	指示失败的原因。要更正此问题、请参见Recovery Guru。

通信测试状态	Description
端口连接错误	原因可能是本地存储阵列未连接或无法联系远程存储阵列。要更正此问题、请参见Recovery Guru。

结果

通信测试完成后、此对话框将显示正常状态、已通过状态或失败状态。

如果通信测试返回失败状态、则在关闭此对话框后、此测试将继续运行、直到镜像一致性组之间的通信恢复为止。

在 SANtricity System Manager 中暂停或恢复镜像一致性组的同步

您可以暂停或恢复镜像一致性组中所有镜像对上的数据同步、这比暂停或恢复单个镜像对上的同步效率更高。

关于此任务

暂停和恢复组同步有助于减少对主机应用程序的任何性能影响、在将本地存储阵列上的任何更改数据复制到远程存储阵列时、可能会发生这种情况。

镜像一致性组及其镜像对的状态将保持暂停状态、直到您使用恢复选项恢复同步活动为止。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   此时将显示镜像一致性组表、并显示与存储阵列关联的所有镜像一致性组。
3. 选择要暂停或恢复的镜像一致性组、然后选择菜单：更多(暂停)或菜单：更多(恢复)。

   系统将显示确认信息。
4. 选择*是*进行确认。

结果

System Manager将执行以下操作：

- 暂停或恢复镜像一致性组中所有镜像对之间的数据传输、而不删除镜像关系。
- 记录暂停镜像组时写入镜像一致性组主端的所有数据、并在恢复镜像组后自动将数据写入镜像一致性组的二级端。不需要完全同步。
- 对于_suspended_mirror一致性组、在镜像一致性组表中显示*用户已暂停*。
- 对于_resumed_mirror consistency组、在镜像一致性组暂停期间写入主卷的数据将立即写入二级卷。如果设置了自动同步间隔、则定期同步将恢复。

在 SANtricity System Manager 中更改镜像一致性组的同步设置

您可以更改本地存储阵列上的镜像一致性组在初始同步数据或在异步镜像操作期间重新同步数据时使用的同步设置和警告阈值。

关于此任务

更改同步设置会影响镜像一致性组中所有镜像对的同步操作。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   此时将显示镜像一致性组表、并显示与存储阵列关联的所有镜像一致性组。

3. 选择要编辑的镜像一致性组、然后选择菜单：更多[编辑设置]。

   系统将显示编辑设置对话框。

4. 根据需要编辑同步和警报设置、然后单击*保存*。

   ▼ 字段详细信息

字段	Description
正在同步镜像对…	指定是要手动还是自动同步远程存储阵列上的镜像对。 • *手动—选择此选项可手动同步远程存储阵列上的镜像对。 • 自动、间隔—选择此选项可通过指定从上次更新开始到下次更新开始的时间间隔自动同步远程存储阵列上的镜像对。默认间隔为10分钟。
提醒我…	如果将同步方法设置为自动进行、请设置以下警报： • "*同步"—设置System Manager在同步未完成时发送警报的时间长度。 • 远程恢复点—设置一个时间限制、超过此时间限制后、System Manager将发送一条警报、指示远程存储阵列上的恢复点数据早于您定义的时间限制。定义上次更新结束后的时间限制。 • "预留容量阈值"—定义预留容量、System Manager将在该容量时发送警报、指出您即将达到预留容量阈值。按剩余容量百分比定义阈值。

结果

System Manager会更改镜像一致性组中每个镜像对的同步设置。

在 **SANtricity System Manager** 中手动重新同步镜像一致性组

您可以手动为镜像一致性组中的所有镜像对启动重新同步。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   此时将显示镜像一致性组表、并显示与存储阵列关联的所有镜像一致性组。

3. 选择要重新同步的镜像一致性组、然后选择菜单：更多(手动重新同步)。

   系统将显示确认信息。

4. 选择*是*进行确认。

结果

系统将执行以下操作：

- 启动对选定镜像一致性组中所有镜像对上的数据的重新同步。
- 将修改后的数据从本地存储阵列更新到远程存储阵列。

在 **SANtricity System Manager** 中查看镜像一致性组之间不同步的数据量

您可以查看本地存储阵列和远程存储阵列上的镜像一致性组之间未同步的数据量。当镜像一致性组处于"未同步"状态时、不会发生任何镜像活动。

关于此任务

如果选定镜像一致性组包含镜像对、并且当前未进行同步、则可以执行此任务。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   此时将显示镜像一致性组表、并显示与存储阵列关联的所有镜像一致性组。

3. 单击菜单：更多(查看未同步的数据量)。

   如果存在未同步的数据、则表值将反映此情况。"data Amount "列列出了未同步的数据量、以MIB为单位。

在 **SANtricity System Manager** 中更新远程存储阵列 **IP** 地址

您可以更新远程存储阵列的iSCSI IP地址、以重新与本地存储阵列建立连接。

开始之前

必须使用iSCSI连接为本地存储阵列和远程存储阵列配置异步镜像。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   镜像一致性组表显示与存储阵列关联的所有镜像一致性组。

3. 选择要更新的镜像一致性组、然后选择菜单：更多[更新远程IP地址]。

   系统将显示更新远程IP地址对话框。

4. 选择*更新*以更新远程存储阵列的iSCSI IP地址。

结果

系统会重置远程存储阵列的IP地址、以便重新与本地存储阵列建立连接。

在 **SANtricity System Manager** 中将镜像一致性组角色更改为主或辅助

您可以出于管理目的或在本地存储阵列发生灾难时更改镜像一致性组之间的角色。

关于此任务

在本地存储阵列上创建的镜像一致性组具有主要角色。在远程存储阵列上创建的镜像一致性组具有二级角色。您可以将本地镜像一致性组降级为二级角色、也可以将远程镜像一致性组提升为主角色。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   此时将显示镜像一致性组表、并显示与存储阵列关联的所有镜像一致性组。

3. 选择要更改角色的镜像一致性组、然后选择菜单：更多(将角色更改为<主卷>二级卷>]*)。

   系统将显示确认信息。

4. 确认要更改镜像一致性组的角色、然后单击*更改角色*。

   请求更改角色时、系统会显示无法联系存储阵列对话框、但无法联系远程存储阵列。单击*是*强制更改角色。

结果

System Manager将执行以下操作：

- 镜像一致性组表会在正在进行角色更改的镜像一致性组旁边显示状态"待定"或"正在进行"。您可以单击表单元格中的*取消*链接来取消待定的角色更改操作。
- 如果可以联系关联的镜像一致性组、则镜像一致性组之间的角色会发生变化。System Manager会将二级镜像一致性组提升为主角色、或者将主镜像一致性组降级为二级角色(具体取决于您的选择)。角色更改会影响选定镜像一致性组中的所有镜像对。

在 **SANtricity System Manager** 中删除镜像一致性组

您可以删除本地存储阵列和远程存储阵列上不再需要的镜像一致性组。

开始之前

必须从镜像一致性组中删除所有镜像对。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择*镜像一致性组*选项卡。

   此时将显示镜像一致性组表、并显示与存储阵列关联的所有镜像一致性组。

3. 选择要删除的镜像一致性组、然后选择菜单：uncommon Tasks[Delete]。

   系统将显示确认信息。

4. 选择*是*可删除镜像一致性组。

结果

System Manager将执行以下操作：

- 首先删除本地存储阵列上的镜像一致性组、然后删除远程存储阵列上的镜像一致性组。
- 从镜像一致性组表中删除镜像一致性组。

完成后

有时、可能会从本地存储阵列成功删除镜像一致性组、但通信错误会阻止从远程存储阵列中删除镜像一致性组。在这种情况下、您必须访问远程存储阵列以删除相应的镜像一致性组。

管理异步镜像对

在 **SANtricity System Manager** 中删除异步镜像关系

您可以删除镜像对、以便从本地存储阵列上的主卷和远程存储阵列上的二级卷删除镜像关系。

关于此任务

查看有关孤立镜像对的以下信息：

- 如果在一端(本地存储阵列端或远程存储阵列端)删除了一致性镜像组中的成员卷、而不是在另一端删除了该成员卷、则会存在孤立镜像对。
- 在恢复阵列间通信且镜像配置的两端协调镜像参数时、系统会检测到孤立镜像对。
- 您可以删除镜像对以更正孤立的镜像对状态。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirrored pairs]。
2. 选择*镜像对*选项卡。

   此时将显示镜像对表、并显示与存储阵列关联的所有镜像对。

3. 选择要删除的镜像对、然后单击*删除*。
4. 确认要删除镜像对、然后单击*删除*。

结果

System Manager将执行以下操作：

- 从本地存储阵列和远程存储阵列上的镜像一致性组中删除镜像关系、并删除预留的容量。
- 将主卷和二级卷返回到主机可访问的非镜像卷。
- 删除异步镜像对后更新异步镜像磁贴。

增加 **SANtricity System Manager** 中的预留容量

您可以增加预留容量、这是物理分配的容量、用于对存储对象执行任何复制服务操作。

对于快照操作、通常为基础卷的40%；对于异步镜像操作、通常为基础卷的20%。通常、当您收到存储对象的预留容量即将满的警告时、您可以增加预留容量。

开始之前

- 池或卷组中的卷必须处于最佳状态、并且不能处于任何修改状态。
- 要用于增加容量的池或卷组中必须存在可用容量。

  如果任何池或卷组上没有可用容量、则可以将未使用的驱动器形式的未分配容量添加到池或卷组中。

关于此任务

对于以下存储对象、只能以8 GiB为增量增加预留容量：

- Snapshot组
- Snapshot卷
- 一致性组成员卷
- 镜像对卷

如果您认为主卷会发生许多更改、或者某个特定副本服务操作的生命周期很长、请使用较高的百分比。

您不能增加只读快照卷的预留容量。只有读写Snapshot卷才需要预留容量。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。
2. 选择要增加预留容量的存储对象，然后单击 **ellipsis icon › Increase reserved capacity**。

   此时将显示增加保留容量页面。

3. 使用spinner框调整容量百分比。

   如果包含所选存储对象的池或卷组上不存在可用容量、并且存储阵列具有未分配的容量、则可以创建新的池或卷组。然后、您可以使用该池或卷组上的新可用容量重试此操作。

4. 单击 * 增加 * 。

结果

System Manager将执行以下操作：

- 增加存储对象的预留容量。
- 显示新添加的预留容量。

在 **SANtricity System Manager** 中更改镜像对卷的预留容量设置

您可以更改镜像对卷的设置、以调整SANtricity系统管理器在镜像对卷的预留容量接近全满时发送警报通知的百分比。

步骤

1. 从左侧面板中，选择菜单：Storage[Reserved capacity]。

2. 选择要编辑的镜像对卷，然后单击 **ellipsis icon › Edit settings**。

   此时将显示镜像对卷预留容量设置对话框。

3. 根据需要更改镜像对卷的预留容量设置。

   ▼ 字段详细信息

正在设置 …	Description
在以下情况下提醒我…	使用spinner框调整在镜像对的预留容量接近全满时System Manager发送警报通知的百分比。 当镜像对的预留容量超过指定阈值时、System Manager将发送警报、以便有时间增加预留容量。 更改一个镜像对的警报设置会更改属于同一镜像一致性组的所有镜像对的警报设置。

4. 单击*保存*以应用所做的更改。

在 **SANtricity System Manager** 中完成在旧系统上创建的主卷的镜像对

如果您在旧存储阵列上创建了无法由SANtricity System Manager管理的主卷、则可以使用SANtricity System Manager在此阵列上创建二级卷。

关于此任务

您可以在使用不同接口的原有阵列与可由System Manager管理的较新阵列之间执行异步镜像。

- 如果要在使用System Manager的两个存储阵列之间进行镜像、则可以跳过此任务、因为您已在镜像对创建序列中完成镜像对。
- 在远程存储阵列上执行此任务。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirrored pairs]。
2. 选择*镜像对*选项卡。

   此时将显示镜像对表、并显示与存储阵列关联的所有镜像对。

3. 找到状态为未完成的镜像对卷、然后单击镜像对列中显示的*完整镜像对*链接。
4. 选择以下单选按钮之一、选择是要自动还是手动完成镜像对创建序列：
   - 自动—创建新的二级卷。

     通过选择要在其中创建二级卷的现有池或卷组、接受镜像对远程端的默认设置。使用此建议选项可使用默认设置为二级卷分配预留容量。

   - 手动-选择现有卷。

     为二级卷定义您自己的参数。

i. 单击*下一步*以选择二级卷。

ii. 选择要用作二级卷的现有卷、然后单击*下一步*以分配预留容量。

iii. 分配预留容量。执行以下操作之一：

- 接受默认设置。

  预留容量的默认设置为基础卷容量的20%、通常此容量已足够。

- 分配您自己的预留容量设置、以满足与异步镜像相关的数据存储需求。

  所需容量因向主卷写入I/O的频率和大小以及保留容量所需的时间而异。通常、如果存在以下一种或两种情况、请为预留容量选择更大的容量：

  - 您打算将镜像对保留很长时间。
  - 由于I/O活动繁重、主卷上的数据块会发生很大一部分更改。使用历史性能数据或其他操作系统实用程序帮助您确定主卷的典型I/O活动。

5. 选择*完成*。

结果

System Manager将执行以下操作：

- 在远程存储阵列上创建二级卷、并为镜像对的远程端分配预留容量。
- 开始在本地存储阵列和远程存储阵列之间进行初始同步。
- 如果要镜像的卷是精简卷、则在初始同步期间、只会将分配的块传输到二级卷。此传输可减少完成初始同步所需传输的数据量。
- 在本地存储阵列和远程存储阵列上为镜像对创建预留容量。

管理同步镜像对

在 **SANtricity System Manager** 中测试同步镜像的通信

您可以测试本地存储阵列与远程存储阵列之间的通信、以诊断参与同步镜像的镜像对可能存在的通信问题。

关于此任务

运行两种不同的测试：

- 通信-验证两个存储阵列是否具有通信路径。通信测试将验证本地存储阵列是否可以与远程存储阵列通信、以及与镜像对关联的二级卷是否位于远程存储阵列上。
- 延迟-向与镜像对关联的远程存储阵列上的二级卷发送SCSI测试单元命令、以测试最小、平均和最大延迟。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Synchronous mirroring]。
2. 选择要测试的镜像对、然后选择*测试通信*。
3. 查看结果窗口中显示的信息、如有必要、请按照指示的更正操作进行操作。

如果通信测试失败、则在关闭此对话框后、此测试将继续运行、直到镜像对之间的通信恢复为止。

在 **SANtricity System Manager** 中暂停和恢复镜像对的同步

您可以使用暂停选项和恢复选项来控制何时同步镜像对中主卷和二级卷上的数据。

关于此任务

如果手动暂停镜像对、则镜像对在手动恢复之前不会同步。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Synchronous mirroring]。
2. 选择要暂停或恢复的镜像对、然后选择菜单：更多(暂停)或菜单：更多(恢复)。

   系统将显示确认信息。

3. 选择*是*进行确认。

结果

System Manager将执行以下操作：

- 暂停或恢复镜像对之间的数据传输、而不删除镜像关系。
- 对于_suspended_mirrored对：
  - 在镜像对表中显示*已暂停*。
  - 记录在暂停同步时写入镜像对的主卷的所有数据。
- 对于_resumed_mirrored对、在恢复同步时、会自动将数据写入镜像对的二级卷。不需要完全同步。

在 **SANtricity System Manager** 中更改镜像对中卷之间的角色

您可以在镜像对中参与同步镜像的两个卷之间执行角色反转。出于管理目的或在本地存储阵列发生灾难时、可能需要执行此任务。

关于此任务

您可以将主卷降级为二级角色、也可以将二级卷提升为主角色。正在访问主卷的所有主机均可对该卷进行读/写访问。当主卷成为二级卷时、只会向该卷写入由主控制器启动的远程写入。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Synchronous mirroring]。
2. 选择包含要更改角色的卷的镜像对、然后选择菜单：更多(更改角色)。

   系统将显示确认信息。

3. 确认要更改卷的角色、然后选择*更改角色*。

如果本地存储阵列无法与远程存储阵列通信、则在请求角色更改时、系统会显示无法联系存储阵列对话框、但无法联系远程存储阵列。单击*是*强制更改角色。

结果

System Manager将执行以下操作：

- 如果可以访问镜像对中的关联卷、则卷之间的角色会发生变化。System Manager会将镜像对中的二级卷提升为主角色、或者将镜像对中的主卷降级为二级角色(具体取决于您的选择)。

在 **SANtricity System Manager** 中更改镜像对的同步设置

您可以更改镜像对在通信中断后用于完成重新同步操作的同步优先级和重新同步策略。

关于此任务

您只能在包含主卷的存储阵列上编辑镜像对的同步设置。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Synchronous mirroring]。
2. 选择要编辑的镜像对、然后选择菜单：更多[编辑设置]。

   系统将显示查看/编辑设置对话框。

3. 使用滑块栏编辑同步优先级。

   同步优先级用于确定在通信中断后完成重新同步操作所使用的系统资源与服务I/O请求相比所使用的系统资源量。

   ▼ 有关同步速率的更多信息

   同步优先级速率有五种：

   - 最低
   - 低
   - 中等
   - 高
   - 最高

   如果将同步优先级设置为最低速率、则会优先处理I/O活动、并且重新同步操作所需时间会更长。如果将同步优先级设置为最高比率、则会优先执行重新同步操作、但存储阵列的I/O活动可能会受到影响。

4. 根据需要编辑重新同步策略。

   您可以手动或自动重新同步远程存储阵列上的镜像对。

   - 手动(建议选项)—选择此选项可要求在恢复与镜像对的通信后手动恢复同步。此选项提供了恢复数据的最佳机会。
   - 自动—选择此选项可在与镜像对的通信恢复后自动开始重新同步。

5. 选择 * 保存 * 。

在 **SANtricity System Manager** 中删除同步镜像关系

您可以删除镜像对、以便从本地存储阵列上的主卷和远程存储阵列上的二级卷删除镜像关系。

关于此任务

您还可以删除镜像对以更正孤立的镜像对状态。查看有关孤立镜像对的以下信息：

- 如果在一端(本地/远程)删除了成员卷、而不是在另一端删除了成员卷、则会存在孤立镜像对。
- 恢复阵列间通信时、系统会检测到孤立的镜像对。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Synchronous mirroring]。
2. 选择要删除的镜像对、然后选择菜单：uncommon Tasks[Remove]。

   此时将显示删除镜像关系对话框。

3. 确认要删除镜像对、然后单击*删除*。

结果

System Manager将执行以下操作：

- 从本地存储阵列和远程存储阵列上的镜像对中删除镜像关系。
- 将主卷和二级卷返回到主机可访问的非镜像卷。
- 删除同步镜像对后更新同步镜像区块。

停用镜像

在 **SANtricity System Manager** 中停用异步镜像

您可以在本地和远程存储阵列上停用异步镜像、以重新建立存储阵列上专用端口的正常使用。

开始之前

- 您必须已删除所有镜像关系。验证是否已从本地和远程存储阵列中删除所有镜像一致性组和镜像对。
- 本地存储阵列和远程存储阵列必须通过光纤通道网络结构或iSCSI接口进行连接。

关于此任务

停用异步镜像时、本地和远程存储阵列上不会发生镜像活动。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Asynchronous mirror consistency groups]。
2. 选择菜单：不常见任务[停用]。

   系统将显示确认信息。

3. 选择*是*进行确认。

结果

- 控制器专用于异步镜像通信的HBA主机通道现在可以接受主机读写请求。
- 此存储阵列中的所有卷都无法作为主卷或二级卷参与镜像关系。

在 **SANtricity System Manager** 中停用同步镜像

您可以在存储阵列上停用同步镜像功能、以重新建立主机总线适配器(HBA)主机端口4的正常使用、该端口是为镜像数据传输预留的。

开始之前

您必须已删除所有同步镜像关系。验证是否已从存储阵列中删除所有镜像对。

步骤

1. 从左侧面板中，选择菜单：Mirroring[Synchronous mirroring]。
2. 选择菜单：不常见任务[停用]。

   系统将显示确认信息。

3. 选择*是*进行确认。

结果

- 控制器的HBA主机端口4专用于同步镜像通信、现在可以接受主机读写请求。
- 存储阵列上的预留容量卷将被删除。

SANtricity System Manager 异步镜像常见问题解答

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。

异步镜像与同步镜像有何不同?

异步镜像功能与同步镜像功能在一个基本方面有所不同：它可以捕获源卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。

使用同步镜像时、不会在某个时间点捕获主卷的状态、而是反映主卷上对二级卷所做的所有更改。二级卷每次与主卷相同、因为使用此类镜像时、每次对主卷执行写入时、都会对二级卷执行写入。在使用主卷上所做的更改成功更新二级卷之前、主机不会收到写入成功的确认。

使用异步镜像时、远程存储阵列与本地存储阵列未完全同步、因此、如果应用程序因丢失本地存储阵列而需要过渡到远程存储阵列、则某些事务可能会丢失。

镜像功能之间的比较：

异步镜像	同步镜像
复制方法	• 时间点 镜像可按需执行、也可根据用户定义的计划自动执行。可以按分钟的粒度定义计划。两次同步的最短时间为10分钟。
• 持续 镜像会自动持续执行、每次写入主机时都会复制数据。	预留容量
• 多个 每个镜像对都需要一个预留容量的卷。	• * 单个 * 所有镜像卷都需要一个预留容量卷。
通信	• * iSCSI和光纤通道* 支持存储阵列之间的iSCSI和光纤通道接口。
• 光纤通道 仅支持存储阵列之间的光纤通道接口。	距离
• 无限制 支持在本地存储阵列和远程存储阵列之间设置几乎无限的距离、而距离通常仅受网络功能和通道扩展技术的限制。	• 受限 通常、距离本地存储阵列不超过10公里(6.2英里)、以满足延迟和应用程序性能要求。

为什么我无法访问我选择的镜像功能?

镜像可在SANtricity统一管理器界面中配置。

EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储阵列上不提供同步镜像。

要在两个阵列之间启用和配置镜像、请验证以下内容：

- Web服务代理服务必须正在运行。(Unified Manager与Web服务代理一起安装在主机系统上。)
- Unified Manager必须通过HTTPS连接在本地主机上运行。
- 必须在Unified Manager中发现要用于镜像的两个存储阵列。
- Unified Manager必须具有适用于存储阵列的有效SSL证书。您可以从Unified Manager接受自签名证书或安装CA签名证书。

有关配置说明、请参见以下内容：

- "创建异步镜像对(在Unified Manager中)"
- "创建同步镜像对(在Unified Manager中)"

在创建镜像一致性组之前、我需要了解哪些信息？

在创建镜像一致性组之前、请遵循以下准则。

EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

您可以在Unified Manager中的创建镜像对向导中创建一致性组。

满足以下Unified Manager要求：

- Web服务代理服务必须正在运行。
- Unified Manager必须通过HTTPS连接在本地主机上运行。
- Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

此外、请确保满足以下存储阵列要求：

- 必须在Unified Manager中发现这两个存储阵列。
- 每个存储阵列必须具有两个控制器。
- 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
- 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
- 您必须知道本地和远程存储阵列的密码。
- 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。

异步镜像—在创建镜像对之前、我需要了解哪些信息？

您可以在SANtricity统一管理器界面中配置镜像对、然后在SANtricity系统管理器中管理这些对。

创建镜像对之前、请遵循以下准则。

- 您必须有两个存储阵列。
- 每个存储阵列必须具有两个控制器。
- 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
- 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。
- 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
- 您必须知道本地和远程存储阵列的密码。
- 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
- 您已安装Web服务代理和Unified Manager。镜像对在Unified Manager界面中进行配置。
- 这两个存储阵列会在Unified Manager中发现。
- 存储阵列必须至少包含一个镜像一致性组。您可以在Unified Manager中的创建镜像对向导中创建一致性组。

在增加镜像对卷上的预留容量之前、我需要了解哪些信息？

通常、当您收到警告、指出镜像对的预留容量已满时、应增加预留容量。您只能以8 GiB为增量增加预留容量。

对于异步镜像操作、预留容量通常为基础卷的20%。如果存在以下一种或两种情况、请为预留容量选择更大的容量：

- 您打算将镜像对保留很长时间。
- 由于I/O活动繁重、主卷上的数据块会发生很大一部分更改。使用历史性能数据或其他操作系统实用程序帮助您确定主卷的典型I/O活动。

您可以通过执行以下操作之一来增加镜像对的预留容量：

- 通过选择菜单：Storage[池和卷组]并单击*预留容量*选项卡来调整镜像对卷的容量百分比。
- 使用池或卷组上的可用容量创建新卷。

  如果任何池或卷组上没有可用容量、则可以将未配置的容量以未使用驱动器的形式添加到池或卷组中。

为什么我无法将预留容量增加到我请求的数量？

您只能以4 GiB为增量增加预留容量。

请查看以下准则：

- 池或卷组中必须有足够的可用容量、以便可以根据需要进行扩展。

  如果任何池或卷组上没有可用容量、则可以将未使用的驱动器形式的未分配容量添加到池或卷组中。

- 池或卷组中的卷必须处于最佳状态、并且不能处于任何修改状态。
- 要用于增加容量的池或卷组中必须存在可用容量。

对于异步镜像操作、预留容量通常为基础卷的20%。如果您认为基础卷会发生许多更改、或者存储对象的复制服务操作的预计预期寿命很长、请使用较高的百分比。

为什么要更改此百分比？

对于快照操作、预留容量通常为基础卷的40%、对于异步镜像操作、预留容量通常为基础卷的20%。

通常、此容量足以满足要求。所需容量因向基础卷写入I/O的频率和大小以及要使用存储对象的副本服务操作的时间而异。

通常、如果存在以下一种或两种情况、请选择较大的预留容量百分比：

- 如果特定存储对象的复制服务操作的生命周期很长。
- 如果由于I/O活动繁重而导致基础卷上的大量数据块发生更改、使用历史性能数据或其他操作系统实用程序帮助您确定基础卷的典型I/O活动。

为什么我会看到多个预留容量候选项？

如果一个池或卷组中有多个卷满足为存储对象选择的容量百分比量、则会显示多个候选卷。

您可以通过更改要在基础卷上为复制服务操作预留的物理驱动器空间百分比来刷新建议候选对象列表。根据您的选择显示最佳候选对象。

为什么表中显示的值不可用？

此表列出了无法显示远程存储阵列上的数据时的不可用值。

要显示远程存储阵列数据、请从Unified Manager启动System Manager。

为什么我看不到所有的池和卷组？

为异步镜像对创建二级卷时、系统会显示一个列表、其中列出了该异步镜像对符合条件的所有池和卷组。不符合使用条件的任何池或卷组不会显示在该列表中。

由于以下任何原因、池或卷组可能不符合条件。

- 池或卷组的安全功能不匹配。
- 池或卷组处于非最佳状态。
- 池或卷组的容量太小。

异步镜像 - 为什么我看不到所有卷？

为镜像对选择主卷时、列表将显示所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

- 此卷不是最佳卷。
- 此卷已加入镜像关系。
- 对于精简卷、必须启用自动扩展。

对于EF600和EF300控制器、异步镜像对中的主卷和二级卷必须匹配相同的协议、托盘级别、区块大小、安全类型和RAID级别。不符合条件的异步镜像对不会显示在可用卷列表中。

异步镜像 - 为什么我看不到远程存储阵列上的所有卷？

在远程存储阵列上选择二级卷时、列表将显示该镜像对的所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

- 此卷不是最佳卷。
- 此卷已加入镜像关系。
- 主卷与二级卷之间的精简卷属性不匹配。
- 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。
  - 如果主卷已启用DA、则二级卷必须已启用DA。
  - 如果主卷未启用DA、则二级卷不能启用DA。

为什么要更新远程存储阵列的 **IP** 地址?

如果iSCSI端口的IP地址发生变化、而本地存储阵列无法与远程存储阵列通信、则可以更新远程存储阵列的IP地址。

在与iSCSI连接建立异步镜像关系时、本地和远程存储阵列会在异步镜像配置中存储远程存储阵列的IP地址记录。如果iSCSI端口的IP地址发生变化、尝试使用该端口的远程存储阵列将遇到通信错误。

IP地址已更改的存储阵列会向与配置为通过iSCSI连接进行镜像的镜像一致性组关联的每个远程存储阵列发送一条消息。接收此消息的存储阵列会自动更新其远程目标IP地址。

如果IP地址已更改的存储阵列无法向远程存储阵列发送其阵列间消息、则系统会向您发送连接问题描述 警报。使用Update Remote IP Address选项重新与本地存储阵列建立连接。

SANtricity System Manager 同步镜像常见问题解答

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。

异步镜像与同步镜像有何不同?

异步镜像功能与同步镜像功能在一个基本方面有所不同：它可以捕获源卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。

使用同步镜像时、不会在某个时间点捕获主卷的状态、而是反映主卷上对二级卷所做的所有更改。二级卷每次与主卷相同、因为使用此类镜像时、每次对主卷执行写入时、都会对二级卷执行写入。在使用主卷上所做的更改成功更新二级卷之前、主机不会收到写入成功的确认。

使用异步镜像时、远程存储阵列与本地存储阵列未完全同步、因此、如果应用程序因丢失本地存储阵列而需要过渡到远程存储阵列、则某些事务可能会丢失。

镜像功能之间的比较：

异步镜像	同步镜像
复制方法	• 时间点 镜像可按需执行、也可根据用户定义的计划自动执行。可以按分钟的粒度定义计划。两次同步的最短时间为10分钟。
• 持续 镜像会自动持续执行、每次写入主机时都会复制数据。	预留容量
• 多个 每个镜像对都需要一个预留容量的卷。	• * 单个 * 所有镜像卷都需要一个预留容量卷。
通信	• * iSCSI和光纤通道* 支持存储阵列之间的iSCSI和光纤通道接口。

异步镜像	同步镜像
• 光纤通道 仅支持存储阵列之间的光纤通道接口。	距离
• 无限制 支持在本地存储阵列和远程存储阵列之间设置几乎无限的距离、而距离通常仅受网络功能和通道扩展技术的限制。	• 受限 通常、距离本地存储阵列不超过10公里(6.2英里)、以满足延迟和应用程序性能要求。

同步镜像 - 为什么我看不到所有卷？

为镜像对选择主卷时、列表将显示所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

- 此卷是非标准卷、例如Snapshot卷或精简卷。
- 此卷不是最佳卷。
- 此卷已加入镜像关系。

同步镜像 - 为什么我看不到远程存储阵列上的所有卷？

在远程存储阵列上选择二级卷时、列表将显示该镜像对的所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

- 此卷是非标准卷、例如Snapshot卷或精简卷。
- 此卷不是最佳卷。
- 此卷已加入镜像关系。
- 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。
  - 如果主卷已启用DA、则二级卷必须已启用DA。
  - 如果主卷未启用DA、则二级卷不能启用DA。

同步镜像—在创建镜像对之前、我需要了解哪些信息？

您可以在SANtricity统一管理器界面中配置镜像对、然后在SANtricity系统管理器中管理这些对。

创建镜像对之前、请遵循以下准则：

- 您必须有两个存储阵列。
- 每个存储阵列必须具有两个控制器。
- 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
- 本地和远程存储阵列通过光纤通道网络结构进行连接。
- 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)

- 您必须知道本地和远程存储阵列的密码。
- 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
- 您已安装Web服务代理和Unified Manager。镜像对在Unified Manager界面中进行配置。
- 这两个存储阵列会在Unified Manager中发现。

同步优先级对同步速率有何影响?

同步优先级用于定义为同步活动分配的处理时间与系统性能相关。

主卷的控制器所有者在后台执行此操作。同时、控制器所有者会处理对主卷的本地I/O写入以及对二级卷的相关远程写入。由于重新同步会使控制器处理资源偏离I/O活动、因此重新同步可能会影响主机应用程序的性能。

请牢记以下准则、以帮助您确定同步优先级可能需要多长时间以及同步优先级如何影响系统性能。

▼ 关于同步优先级速率

可以使用以下优先级：

- 最低
- 低
- 中等
- 高
- 最高

最低优先级速率支持系统性能、但重新同步所需时间较长。最高优先级速率支持重新同步、但系统性能可能会受到影响。

这些准则大致近似于优先级之间的差异。

完全同步的优先级速率	与最高同步速率相比所用时间
最低	约为最高优先级速率的八倍。
低	约为最高优先级速率的六倍。
中等	大约是最高优先级速率的三倍半。
高	大约是最高优先级速率时的两倍。

卷大小和主机I/O速率负载会影响同步时间比较。

为什么建议使用手动同步策略?

建议使用手动重新同步、因为它可以让您以最佳机会恢复数据的方式管理重新同步过程。

如果使用自动重新同步策略、并且在重新同步期间发生间歇性通信问题、则二级卷上的数据可能会暂时损坏。重新同步完成后、数据将得到更正。

远程存储

了解 SANtricity System Manager 中的远程存储功能

如果您具有远程存储功能、则可以将数据从远程存储系统导入到存储阵列。

什么是远程存储功能?

使用_Remote Storage_功能、您可以将数据从远程存储系统导入到本地E系列存储系统。远程系统可以是其他E系列系统、也可以是其他供应商提供的系统。如果您希望简化数据迁移并最大限度地减少停机时间、例如在设备升级期间、此功能将非常有用。

要使用远程存储、必须在子型号ID (SMID)中启用此功能。

了解更多信息。

- "远程存储的工作原理"
- "远程存储术语"
- "远程存储要求"
- "远程存储卷要求"

如何使用此功能导入数据?

使用远程存储向导、可以将远程存储设备(数据导入的源)映射到E系列系统上的目标卷。此向导可从菜单：Storage[远程存储]中访问。

了解更多信息。

- "导入远程存储"
- "管理数据导入的进度"

概念

远程存储在 SANtricity 软件中的工作原理

通过远程存储功能、您可以将数据从远程存储系统导入到本地E系列存储系统。如果您希望简化数据迁移并最大限度地减少停机时间、例如在设备升级期间、此功能将非常有用。

要配置远程存储功能、必须先设置硬件、然后使用System Manager创建远程存储对象。完成此配置后、导入过程将开始。

硬件设置

使用以下工作流准备硬件连接。

有关这些步骤的详细信息、请参见E系列和SANtricity 文档中心上的《远程存储功能用户指南》 "远程存储卷概述"和中的 "远程存储技术报告"。

SANtricity远程存储卷目前在E4000系统上不受支持。

在本地E系列存储系统上：

1. 确保每个控制器都与远程存储系统建立iSCSI连接。通过此连接、本地E系列系统充当iSCSI启动程序、可将其设置为远程系统上的主机。
2. 为导入操作创建目标卷。确保卷的容量等于或大于远程存储系统上的源卷、块大小匹配且未映射。请参见 "创建卷"。
3. 从其 System Manager 界面收集本地 E 系列系统的 iSCSI 限定名称 (IQN)。IQN 稍后将用于将本地 E 系列系统设置为远程存储系统上的主机。在 System Manager 中，转到：**System › iSCSI settings › Target IQN**。

在远程存储系统上：

1. 使用IQN将本地E系列系统设置为远程系统上的主机。请确保设置适当的主机类型、如下所示：
   - 如果远程系统为E系列型号、请参见 "主机和主机集群概述"。使用主机类型"出厂默认值"。
   - 如果远程系统来自其他供应商、请根据可用选项选择适当的主机类型。
2. 停止所有I/O、卸载任何文件系统、并删除对源卷的主机或应用程序的任何分配。
3. 将卷分配给新创建的本地E系列存储系统主机。
4. 对于选定源卷、从远程存储系统收集以下信息、以便创建导入：
   - iSCSI限定名称(IQN)
   - iSCSI IP地址
   - 源卷的LUN编号

System Manager设置

使用以下工作流为导入创建远程存储对象：

1. 使用System Manager界面中的远程存储向导、将远程存储设备(数据导入的源)映射到E系列系统上的目标卷。选择*完成*后、导入过程将开始。
2. 从"查看操作"对话框或"正在执行的操作"面板监控导入。如有必要、您还可以暂停并恢复此过程。
3. (可选)在导入完成后断开源卷和目标卷之间的连接、或者保持连接以供将来导入。

了解 **SANtricity** 软件中的远程存储术语

了解远程存储术语如何应用于存储阵列。

期限	Description
IQN	iSCSI限定名称(IQN)标识符、是iSCSI启动程序或目标的唯一名称。
LUN	逻辑单元号、用于标识可提供给主机进行访问的逻辑单元。
远程存储系统	数据最初所在的存储系统。远程存储系统可以是E系列型号、也可以是其他供应商提供的系统。

期限	Description
远程存储设备	数据最初存储在远程系统上的物理或逻辑设备。在E系列存储系统中、此卷称为"卷"。
远程存储对象	一个对象、其中包含允许E系列系统识别并连接到远程存储系统的信息。此信息包括远程存储系统的IQN和IP地址。远程存储对象表示远程存储系统与E系列系统之间的通信。
远程存储卷	E系列系统上的一种标准卷、允许对远程存储设备进行数据访问。
Volume	存储数据的容器。它是为主机创建的逻辑组件、用于访问数据。

了解 **SANtricity** 软件中的远程存储功能要求

在使用远程存储功能之前、请查看以下要求和限制。

支持的协议

支持以下协议：

- iSCSI
- IPv4

有关最新的E系列支持和配置信息、请参见 "NetApp 互操作性表工具"。

硬件要求

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。其中必须包括：

- 支持iSCSI的接口

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。

了解 **SANtricity** 软件中的远程存储卷要求

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，动态区块大小，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，导入完成后可以映射）。

- 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。

管理远程存储

在 **SANtricity System Manager** 中导入远程存储

要启动从远程系统到本地E系列存储系统的存储导入、请使用导入远程存储向导。

开始之前

- 必须将 E 系列存储系统配置为与远程存储系统进行通信。

> 有关硬件配置的信息、请参见《远程存储功能用户指南》、该指南可从E系列和SANtricity 文档中心获得、网址为 "配置硬件"和中的 "远程存储技术报告"。

- 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。请参见 "创建卷"。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 "远程存储卷要求"。

- *建议：*在开始导入过程之前、请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、因此建议您首先执行较小的"`test`"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. 选择菜单：Storage[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。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 * 。

   ▼ 字段详细信息

正在设置 ...	Description
Name	输入远程存储设备的名称、以便在System Manager界面中进行标识。 名称最多可包含30个字符、并且只能包含字母、数字和以下特殊字符：下划线(_)、短划线(-)和哈希符号(#)。名称不能包含空格。
iSCSI连接属性	输入远程存储设备的连接属性： • * iSCSI限定名称(IQN)*：输入iSCSI IQN。 • * IP地址*：输入IPv4地址。 • 端口：输入用于源设备与目标设备之间通信的端口号。默认情况下、端口号为3260。

单击*下一步*后、将显示配置源面板的*步骤1b*。

4. 在* LUN 字段中、选择要用作源的远程存储设备的**LUN**编号、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. 从"审阅"面板中、验证设置是否准确、然后单击*完成*以启动导入。

   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*将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。

结果

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。

完成后

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。

在 SANtricity System Manager 中管理远程存储导入的进度

导入过程开始后，您可以查看其进度并对其执行操作。

关于此任务

对于每个导入操作、"正在执行的操作"对话框会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。

您还可以通过菜单：监控[正在进行的操作]查看正在进行的操作。

步骤

1. 从远程存储页面中、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。
   - 更改优先级-选择*更改优先级*以更改正在进行或待定操作的处理优先级。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 * 。此操作不会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。

在 SANtricity System Manager 中修改远程存储的连接设置

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。

关于此任务

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. 选择菜单：Storage[远程存储]。
2. 从列表中、选择要修改的远程存储对象。
3. 单击 * 查看 / 编辑设置 * 。

   此时将显示远程存储设置对话框。

4. 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。

5. 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。

6. 单击 * 保存 * 。

   修改后的连接设置将应用于远程存储对象。

在 **SANtricity System Manager** 中删除远程存储对象

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。

开始之前

确保没有与要删除的远程存储对象关联的导入。

关于此任务

删除远程存储对象后、本地设备与远程设备之间的连接将被删除。

步骤

1. 选择菜单：Storage[远程存储]。
2. 从列表中、选择要删除的远程存储对象。
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。

SANtricity System Manager 远程存储常见问题解答

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。

在创建远程存储连接之前、我需要了解哪些信息？

要配置远程存储功能、您必须通过iSCSI直接连接远程设备和目标存储系统。

要设置iSCSI系统连接、请参见：

- "配置iSCSI端口"
- "远程存储技术报告"

为什么系统会提示我删除远程卷？

当远程卷达到其最大数量时、存储系统会自动检测任何未使用的远程卷并提示您删除这些卷。

在某些情况下、未使用的远程卷在创建过程中不会被清理。在开始任何其他导入操作之前、请验证您的系统是否最佳且网络连接是否稳定。

为什么我看不到目标阵列上的所有卷？

在为远程存储功能配置导入时、您可能会注意到、由于块大小、容量或卷可用性、某些卷不会显示在目标候选卷列表中。

要显示在列表中、卷候选项必须具有：

- 容量等于或大于远程卷。
- 与远程卷相同的块大小。
- 当前最佳状态。

如果候选卷具有以下特性、则这些候选卷将从列表中排除：

- 以下任意关系：卷副本、快照或镜像。
- 正在执行重新配置操作。
- 映射到其他设备(主机或主机集群)。
- 已启用读取闪存缓存。

需要了解有关导入中的远程卷的哪些信息？

使用远程存储功能时、请注意、远程卷是数据源。

导入过程中、数据将从远程卷传输到目标存储系统上的目标卷。这两个卷必须具有匹配的块大小。

在开始远程存储导入之前、我需要了解哪些信息？

通过远程存储功能、您可以将数据从远程存储系统复制到本地E系列存储系统上的卷。在使用此功能之前、请查看以下准则。

Configuration

在创建远程存储导入之前、您必须完成以下操作并验证以下条件：

- 确保本地E系列存储系统的每个控制器都与远程存储系统建立了iSCSI连接。
- 在本地E系列存储系统上、为导入操作创建一个目标卷。确保卷的容量等于或大于源卷、块大小与源卷匹配且未映射。请参见 "创建卷"。
- 使用其 iSCSI 限定名称 (IQN) 将本地 E 系列存储系统设置为远程系统上的主机。您可以从菜单中查看 IQN：系统[iSCSI 设置 > 目标 IQN]。此外，请务必根据所使用的系统设置适当的主机类型。
- 停止所有I/O、卸载任何文件系统、并删除对远程存储系统上选定卷的主机或应用程序的任何分配。
- 将卷分配给远程存储系统、并分配给新创建的本地E系列存储系统主机。
- 从远程存储系统收集以下信息、以便创建导入：
  - iSCSI限定名称(IQN)
  - iSCSI IP地址
  - 源数据所在的远程存储设备的LUN编号
- 导入过程开始后、整个本地目标卷将被复制的数据覆盖。创建导入后、写入本地目标卷的任何新数据都会传

播到远程存储设备上的卷。因此、建议您在开始导入过程之前备份远程存储系统上的卷。

导入过程

以下步骤概述了导入过程。

1. 访问System Manager界面、然后转到*远程存储*页面。选择*导入*以开始创建新的导入。有关详细说明、请参见 "导入远程存储"。

   如果要执行脱机导入、请在导入完成后再映射目标卷。

2. 监控导入进度。

   导入开始后、便可映射目标卷。完成导入操作所需的时间取决于远程存储设备(源卷)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、目标卷将与源卷重复。

3. 准备好中断映射关系后、从*正在执行的操作*面板对导入对象执行*断开连接*。

导入断开后、本地目标的性能将恢复正常、不再受远程连接的影响。

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。

追加信息

有关远程存储功能的详细信息、请参见 "远程存储技术报告"。

硬件组件

在 SANtricity System Manager 中查看和管理硬件组件

您可以在硬件页面上检查组件状态、并执行与这些组件相关的某些功能。

我可以管理哪些组件？

您可以检查组件状态并执行与这些组件相关的某些功能：

- "磁盘架"-_shelf_是一个组件、其中包含存储阵列的硬件(控制器、电源/风扇箱和驱动器)。磁盘架有三种大小、最多可容纳12、24或60个驱动器。
- "控制器"-_controller_是实施存储阵列和管理功能的硬件和固件的组合。它包括缓存内存、驱动器支持以及用于主机连接的端口。
- "驱动器"-驱动器_可以是硬盘驱动器(HDD)或固态驱动器(SSD)。根据磁盘架大小、最多可以在磁盘架中安装12个、24个或60个驱动器。

了解更多信息。

- "硬件页面"
- "硬件术语"

如何查看硬件组件？

转到硬件页面，其中提供了存储阵列物理组件的图形描述。您可以通过选择磁盘架视图右上角的*驱动器*或*控制器和组件*选项卡，在阵列磁盘架的前视图和后视图之间切换。

了解更多信息。

- "查看磁盘架组件状态和设置"
- "查看控制器设置"
- "查看驱动器状态和设置"

相关信息

详细了解与硬件相关的概念：

- "控制器状态"
- "驱动器状态"
- "磁盘架丢失保护和抽盒丢失保护"

概念

SANtricity System Manager 硬件页面和组件

硬件页面以图形方式描绘了存储阵列的物理组件。您可以从此处检查组件状态并执行与这些组件相关的某些功能。

磁盘架

磁盘架是一个组件、其中包含存储阵列的硬件(控制器、电源/风扇箱和驱动器)。磁盘架有两种类型：

- 控制器架-包含驱动器、电源/风扇箱和控制器。

- 驱动器架(或*扩展架*)-包含驱动器、电源/风扇箱和两个输入/输出模块(IOM)。IOM (也称为环境服务模块(ESM))包括将驱动器架连接到控制器架的SAS端口。

磁盘架有三种大小、最多可容纳12、24或60个驱动器。每个磁盘架都包含一个ID编号、该ID编号由控制器固件分配。此ID显示在磁盘架视图的左上角。

硬件页面上的磁盘架视图显示正面或背面的组件。您可以通过从磁盘架视图右上角选择*驱动器*或*控制器和组件*选项卡，在两个视图之间切换。您也可以从页面底部选择*显示所有正面*或*显示所有背面*。正面和背面视图显示以下内容：

- 前组件—驱动器和空驱动器托架。
- 后端组件—控制器和电源/风扇箱(用于控制器架)或IOM和电源/风扇箱(用于驱动器架)。

您可以执行以下与磁盘架相关的功能：

- 打开磁盘架的定位灯、以便找到磁盘架在机柜或机架中的物理位置。
- 更改磁盘架视图左上方显示的ID编号。
- 查看磁盘架设置、例如安装的驱动器类型和序列号。
- 上移或下移磁盘架视图以匹配存储阵列中的物理布局。

控制器

控制器是指实施存储阵列和管理功能的硬件和固件的组合。它包括缓存内存、驱动器支持和主机接口支持。

您可以执行与控制器相关的以下功能：

- 为管理端口配置IP地址和速度。
- 配置iSCSI主机连接(如果有iSCSI主机)。
- 配置网络时间协议(NTP)服务器和域名系统(DNS)服务器。
- 查看控制器状态和设置。
- 允许局域网外部的用户启动SSH会话并更改控制器上的设置。
- 将控制器置于脱机、联机或服务模式。

驱动器

存储阵列可以包括硬盘驱动器(HDD)或固态驱动器(SSD)。根据磁盘架大小、最多可以在磁盘架中安装12个、24个或60个驱动器。

您可以执行以下与驱动器相关的功能：

- 打开驱动器的定位灯、以便找到驱动器在磁盘架中的物理位置。
- 查看驱动器状态和设置。
- 重新分配驱动器(从逻辑上将故障驱动器替换为未分配的驱动器)、并在必要时手动重建驱动器。
- 手动使驱动器出现故障、以便您可以更换它。(如果某个驱动器发生故障、您可以在更换之前复制该驱动器的内容。)
- 分配或取消分配热备用磁盘。

- 擦除驱动器。

了解 **SANtricity** 软件中使用的硬件术语

以下硬件术语适用于存储阵列。

▼ 常规硬件术语：

组件	**Description**
托架	托架是指安装驱动器或其他组件的磁盘架中的插槽。
控制器	控制器由主板，固件和软件组成。它控制驱动器并实施 System Manager 功能。
控制器架	控制器架包含一组驱动器和一个或多个控制器箱。控制器箱用于存放控制器、主机接口卡(Host Interface Card、HIC)和电池。
驱动器	驱动器是一种为数据提供物理存储介质的机械设备或固态内存设备。
驱动器架	驱动器架也称为扩展架、其中包含一组驱动器和两个输入/输出模块(IOM)。IOM包含SAS端口、用于将驱动器架连接到控制器架或其他驱动器架。
IOM (ESM)	IOM是一个输入/输出模块、其中包含SAS端口、用于将驱动器架连接到控制器架。在以前的控制器型号中、IOM称为环境服务模块(ESM)。
电源/风扇箱	电源 / 风扇箱是一个可滑入磁盘架的组件。它包括一个电源和一个集成风扇。
SFP	SFP是一种小型可插拔(SFP)收发器。
磁盘架	磁盘架是安装在机柜或机架中的机箱。它包含存储阵列的硬件组件。磁盘架有两种类型：控制器磁盘架和驱动器磁盘架。控制器架包括控制器和驱动器。驱动器架包括输入 / 输出模块（ IOM ）和驱动器。
存储阵列	存储阵列包括磁盘架、控制器、驱动器、软件和固件。

▼ 控制器术语：

组件	**Description**
控制器	控制器由主板，固件和软件组成。它控制驱动器并实施 System Manager 功能。
控制器架	控制器架包含一组驱动器和一个或多个控制器箱。控制器箱用于存放控制器、主机接口卡(Host Interface Card、HIC)和电池。
DHCP	动态主机配置协议(DHCP)是Internet协议(IP)网络上使用的一种协议、用于动态分布网络配置参数、例如IP地址。
DNS	域名系统(Domain Name System、DNS)是一种命名系统、用于命名连接到Internet或专用网络的设备。DNS服务器维护一个域名目录、并将其转换为Internet协议(IP)地址。
双工配置	双工是存储阵列中的双控制器模块配置。双工系统在控制器、逻辑卷路径和磁盘路径方面是完全冗余的。如果一个控制器发生故障、另一个控制器将接管其I/O以保持可用性。双工系统还具有冗余风扇和电源。
全双工/半双工连接	全双工和半双工是指连接模式。在全双工模式下、两个设备可以同时双向通信。在半双工模式下、设备可以一次单向通信(一个设备发送消息、而另一个设备接收消息)。
HIC	可以选择将主机接口卡（ HIC ）安装在控制器箱中。控制器中内置的主机端口称为基板主机端口。HIC 中内置的主机端口称为 HIC 端口。

组件	Description
ICMP ping响应	Internet控制消息协议(Internet Control Message Protocol、ICMP)是网络计算机的操作系统用来发送消息的协议。ICMP消息可确定主机是否可访问以及从该主机获取数据包所需的时间。
MAC 地址	以太网使用介质访问控制标识符(MAC地址)来区分连接同一物理传输网络接口上两个端口的不同逻辑通道。
管理客户端	管理客户端是指安装了浏览器以访问System Manager的计算机。
MTU	最大传输单元(Maximum Transmission Unit、MTU)是可在网络中发送的最大数据包或帧。
NTP	网络时间协议(NTP)是一种网络协议、用于在数据网络中的计算机系统之间进行时钟同步。
单工配置	单工是存储阵列中的单控制器模块配置。单工系统不提供控制器或磁盘路径冗余、但具有冗余风扇和电源。
VLAN	虚拟局域网(VLAN)是一种逻辑网络、其行为与相同设备(交换机、路由器等)支持的其他网络在物理上是分开的。

▼ 驱动器术语：

组件	Description
da.	数据保证(Data Assurance、DA)是一项功能、用于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。可以在池或卷组级别启用数据保证、主机使用光纤通道等具有DA功能的I/O接口。
驱动器安全功能	驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS ）驱动器提供额外的安全层。如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。
驱动器架	驱动器架也称为扩展架、其中包含一组驱动器和两个输入/输出模块(IOM)。IOM包含SAS端口、用于将驱动器架连接到控制器架或其他驱动器架。
DULBE	Deallocated or Unwritten Logical Block Error (DULBE) 是 NVMe 驱动器上的一个选项，允许 EF80、EF50、EF300/EF300C 或 EF600/EF600C 存储阵列支持资源调配的卷。
FDE驱动器	全磁盘加密(Full Disk Encryption、FDE)驱动器在硬件级别对磁盘驱动器执行加密。硬盘驱动器包含一个ASIC芯片、用于在写入期间对数据进行加密、然后在读取期间对数据进行解密。
FIPS驱动器	FIPS驱动器使用联邦信息处理标准(FIPS) 140-2级别2。它们本质上是FDE驱动器、符合美国政府标准、可确保强大的加密算法和方法。FIPS驱动器的安全标准高于FDE驱动器。
HDD	硬盘驱动器（ HDD ）是指使用带有磁性层的旋转金属盘的数据存储设备。
热备用驱动器	热备用磁盘在RAID 1、RAID 5或RAID 6卷组中充当备用驱动器。它们是功能完备的驱动器、不包含任何数据。如果卷组中的驱动器发生故障、控制器会自动将故障驱动器中的数据重新构建为热备用磁盘。

组件	Description
NVMe	Non-Volatile Memory Express (NVMe)是一种专为SSD驱动器等基于闪存的存储设备设计的接口。与以前的逻辑设备接口相比、NVMe可降低I/O开销并提高性能。
（ SAS ）。	串行连接 SCSI （ SAS ）是一种点对点串行协议，可将控制器直接链接到磁盘驱动器。
支持安全的驱动器	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、这些驱动器可在写入期间对数据进行加密、并在读取期间对数据进行解密。这些驱动器被视为安全驱动器-*capable"*、因为可以使用驱动器安全功能提高安全性。如果为这些驱动器使用的卷组和池启用了驱动器安全功能、则这些驱动器将变为*secure—_enabled*.
已启用安全保护的驱动器	启用了安全保护的驱动器与驱动器安全功能结合使用。启用驱动器安全功能后、如果将驱动器安全应用于安全-*capable"*驱动器上的池或卷组、则这些驱动器将变为安全-enabled__。只能通过配置了正确安全密钥的控制器进行读写访问。这种增强的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。
SSD	固态磁盘（ SSD ）是指使用固态内存（ Flash ）持久存储数据的数据存储设备。SSD 可模拟传统硬盘驱动器，并可与硬盘驱动器使用相同的接口。

▼ **iSCSI**术语：

期限	Description
CHAP	质询握手身份验证协议(CHAP)方法可在初始链路期间验证目标和启动程序的身份。身份验证基于名为CHAP *secret*的共享安全密钥。
控制器	控制器由主板，固件和软件组成。它控制驱动器并实施 System Manager 功能。
DHCP	动态主机配置协议(DHCP)是Internet协议(IP)网络上使用的一种协议、用于动态分布网络配置参数、例如IP地址。
IB	InfiniBand （ IB ）是高性能服务器和存储系统之间数据传输的一种通信标准。
ICMP ping响应	Internet控制消息协议(Internet Control Message Protocol、ICMP)是网络计算机的操作系统用来发送消息的协议。ICMP消息可确定主机是否可访问以及从该主机获取数据包所需的时间。
IQN	iSCSI限定名称(IQN)标识符是iSCSI启动程序或iSCSI目标的唯一名称。
iSER	适用于RDMA的iSCSI扩展(iSER)是一种协议、用于扩展iSCSI协议、以便在InfiniBand或以太网等RDMA传输上运行。
iSNS	Internet存储名称服务(iSNS)是一种协议、允许在TCP/IP网络上自动发现、管理和配置iSCSI和光纤通道设备。
MAC 地址	以太网使用介质访问控制标识符(MAC地址)来区分连接同一物理传输网络接口上两个端口的不同逻辑通道。
管理客户端	管理客户端是指安装了浏览器以访问System Manager的计算机。
MTU	最大传输单元(Maximum Transmission Unit、MTU)是可在网络中发送的最大数据包或帧。
RDMA	远程直接内存访问(RDMA)是一项技术、允许网络计算机在主内存中交换数据、而无需涉及任一计算机的操作系统。

期限	Description
未命名的发现会话	启用未命名发现会话选项后、无需iSCSI启动程序指定目标IQN来检索控制器的信息。

▼ **NVMe**术语：

期限	Description
InfiniBand	InfiniBand （ IB ）是高性能服务器和存储系统之间数据传输的一种通信标准。
命名空间	命名空间是指为块访问而格式化的NVM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	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)。
NQN	NVMe限定名称(NQN)用于标识远程存储目标(存储阵列)。
NVM	非易失性内存(NVM)是许多类型的存储设备中使用的永久性内存。
NVMe	Non-Volatile Memory Express (NVMe)是一种专为SSD驱动器等基于闪存的存储设备设计的接口。与以前的逻辑设备接口相比、NVMe可降低I/O开销并提高性能。
NVMe-oF	基于网络结构的非易失性Memory Express (NVMe-oF)是一种规范、可使NVMe命令和数据通过网络在主机和存储之间传输。
NVMe控制器	NVMe控制器是在主机连接过程中创建的。它可在主机与存储阵列中的命名空间之间提供访问路径。
NVMe队列	队列用于通过NVMe接口传递命令和消息。
NVMe 子系统	具有NVMe主机连接的存储阵列。
RDMA	通过在网络接口卡(NIC)硬件中实施传输协议、远程直接内存访问(Remote Direct Memory Access、RDMA)可以更直接地将数据移入和移出服务器。
RoCE	基于融合以太网的 RDMA （ RoCE ）是一种网络协议，允许通过以太网远程直接内存访问（ RDMA ）。
SSD	固态磁盘（ SSD ）是指使用固态内存（ Flash ）持久存储数据的数据存储设备。SSD 可模拟传统硬盘驱动器，并可与硬盘驱动器使用相同的接口。

管理磁盘架组件

在 **SANtricity System Manager** 中查看硬件组件

"硬件"页面提供了排序和筛选功能、便于查找组件。

步骤

1. 在左侧面板中，选择 **Hardware**。
2. 使用下表中所述的功能查看硬件组件。

功能	Description
驱动器、控制器和组件视图	要在驱动器和控制器磁盘架视图之间切换，请从左侧面板选择菜单：硬件[驱动器]或菜单：硬件[控制器和组件]。驱动器*视图显示驱动器和任何空的驱动器托架。*控制器和组件*视图显示控制器以及任何 **IOM (ESM)** 模块、电源/风扇箱或空控制器托架。在驱动器视图中，您还可以选择*显示所有驱动器。
驱动器视图筛选器	如果存储阵列包含具有不同类型的物理和逻辑属性的驱动器、则*硬件*页面将包含驱动器视图筛选器。通过限制页面上显示的驱动器类型、这些筛选字段可帮助您快速找到特定驱动器。在*显示驱动器…下、单击左侧的筛选字段(默认情况下、显示*任何驱动器类型)以查看物理属性(例如容量和速度)的下拉列表。单击右侧的筛选器字段(默认情况下、显示*存储阵列中的任意位置*)以查看逻辑属性的下拉列表(例如、卷组分配)。您可以同时使用这些筛选器、也可以单独使用这些筛选器。 如果存储阵列中的驱动器都共享相同的物理属性、则不会显示左侧的*任何驱动器类型*字段。如果所有驱动器都位于同一逻辑位置、则右侧的*存储阵列中的任意位置*字段不会显示。
图例	这些组件会以特定颜色显示、以描述其角色状态。要展开和折叠这些状态的说明、请单击*图例*。
显示状态图标详细信息	状态指示器可以包含可用性状态的文本说明。单击*显示状态图标详细信息*可显示或隐藏此状态文本。
磁盘架/磁盘架图标	每个磁盘架视图均提供一个相关命令列表以及属性和状态。单击*磁盘架*可查看命令的下拉列表。您还可以选择顶部的一个图标来查看各个组件的状态和属性：控制器、IOM (ESM)、电源、风扇、温度、 电池和SFP。
磁盘架顺序	可以在硬件页面上重新排列这些磁盘架。使用每个磁盘架视图右上角的向上和向下箭头更改磁盘架的顶部/底部顺序。

在 **SANtricity System Manager** 中显示或隐藏组件状态

您可以显示驱动器、控制器、风扇和电源的状态说明。

步骤

1. 从左侧面板中，选择 **Hardware › Drives** 或 **Hardware › Controllers and components**，具体取决于要查看的组件。
2. 要查看或隐藏弹出状态说明、请执行以下操作：
   - 如果要查看状态图标的弹出问题描述 、请单击磁盘架视图右上角的*显示状态图标详细信息*(选中复选框)。
   - 要隐藏弹出说明、请再次单击*显示状态图标详细信息*(清除此复选框)。
3. 如果要查看完整状态详细信息、请在磁盘架视图中选择组件、然后选择*查看设置*。

更改 **SANtricity System Manager** 中架子的视图顺序

您可以更改硬件页面上显示的磁盘架顺序、以匹配机柜中磁盘架的物理顺序。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 选择货架的下拉列表，然后选择*Change order*以重新排列"硬件"页面上显示的货架顺序。

在 **SANtricity System Manager** 中打开机架定位灯

要查找硬件页面上显示的磁盘架的物理位置、您可以打开磁盘架的定位灯。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 选择控制器架或驱动器架的下拉列表、然后选择*打开定位灯*。

   磁盘架的定位灯亮起。

3. 在物理定位磁盘架后、返回对话框并选择*关闭*。

在 **SANtricity System Manager** 中更改架子 **ID**

磁盘架ID是一个数字、用于唯一标识存储阵列中的磁盘架。每个磁盘架视图的左上角会连续编号、从00或01开始。

关于此任务

控制器固件会自动分配磁盘架ID、但如果要创建其他订购方案、您可以更改此编号。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 选择控制器架或驱动器架的下拉列表、然后选择*更改ID*。
3. 在更改货架 ID 对话框中，选择下拉列表以显示可用编号。

   此对话框不会显示当前分配给活动磁盘架的ID。

4. 选择一个可用数字、然后单击*保存*。

   根据您选择的数量、可以在硬件页面上重新排列磁盘架顺序。如果需要、可以使用每个磁盘架右上角的向上/向下箭头重新调整顺序。

在 **SANtricity System Manager** 中查看机架组件状态和设置

硬件页面提供了磁盘架组件的状态和设置、包括电源、风扇和电池。

关于此任务

可用组件取决于磁盘架类型：

- 驱动器架-在一个磁盘架中包含一组驱动器、电源/风扇箱、输入/输出模块(IOM)以及其他支持组件。
- 控制器架—在一个磁盘架中包含一组驱动器、一个或两个控制器箱、电源/风扇箱以及其他支持组件。

步骤

1. 在左侧面板中，选择 **Hardware**。
2. 选择"控制器架"或"驱动器架"的下拉列表，然后选择 **View settings**。

   此时将打开 Shelf 设置面板，其中包含显示与磁盘架组件相关的状态和设置的部分。根据所选磁盘架类型，

表格中描述的某些部分可能不会显示。

选项卡	Description
磁盘架	*磁盘架*选项卡显示以下属性： • 磁盘架**ID**—用于唯一标识存储阵列中的磁盘架。控制器固件会分配此编号、但您可以通过选择菜单：Shelf[Change ID]来更改此编号。 • 磁盘架路径冗余-指定磁盘架与控制器之间的连接是否具有备用方法(是)或非(否)。 • 当前驱动器类型-显示驱动器中内置的技术类型(例如、支持安全的SAS驱动器)。如果存在多种驱动器类型、则会显示这两种技术。 • 序列号-显示磁盘架的序列号。
IOM (ESM)	"IOM (ESM)*"选项卡显示输入/输出模块(IOM)的状态、也称为环境服务模块(ESM)。它可监控驱动器架中组件的状态、并充当驱动器托盘和控制器之间的连接点。 状态可以是"最佳"、"失败"、"最佳"(连线错误)或"未认证"。其他信息包括固件版本和配置设置版本。 选择*显示更多设置*可查看最大和当前数据速率以及卡通信状态(是或否)。 您也可以通过选择IOM图标来查看此状态  、磁盘架下拉列表旁边。
电源	*电源*选项卡显示电源箱和电源本身的状态。状态可以是"最佳"、"失败"、"已删除"或"未知"。它还会显示电源的部件号。 您也可以通过选择电源图标来查看此状态  、磁盘架下拉列表旁边。
风扇	*风扇*选项卡显示风扇箱和风扇本身的状态。状态可以是"最佳"、"失败"、"已删除"或"未知"。 您也可以通过选择风扇图标来查看此状态  、磁盘架下拉列表旁边。
温度	*温度*选项卡显示磁盘架组件的温度状态、例如传感器、控制器和电源/风扇箱。状态可以是"最佳"、"已超过标称温度"、"已超过最大温度"或"未知"。 您也可以通过选择"温度"图标来查看此状态  、磁盘架下拉列表旁边。
电池	*电池*选项卡显示控制器电池的状态。状态可以是"最佳"、"失败"、"已删除"或"未知"。其他信息包括电池使用时间、更换前的天数、学习周期以及学习周期之间的周数。 您也可以通过选择电池图标来查看此状态  、磁盘架下拉列表旁边。

选项卡	Description
SFP	"* SFF*"选项卡显示了控制器上小型可插拔(SFP)收发器的状态。状态可以是"最佳"、"失败"或"未知"。 选择*显示更多设置*可查看部件号、序列号和SFP供应商。 您也可以通过选择SFP图标来查看此状态 、磁盘架下拉列表旁边。

3. 单击 * 关闭 * 。

在 **SANtricity System Manager** 中更新电池学习周期

学习周期是指自动校准智能电池电量表的周期。这些周期按计划在同一天和时间自动开始、间隔为8周(每个控制器)。如果要设置其他计划、可以调整学习周期。

关于此任务

更新学习周期会同时影响两个控制器电池。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 选择控制器架的下拉列表、然后选择*查看设置*。
3. 选择*电池*选项卡。
4. 选择*更新电池学习周期*。

   此时将打开更新电池学习周期对话框。
5. 从下拉列表中、选择新的日期和时间。
6. 单击 * 保存 * 。

管理控制器

了解 **SANtricity System Manager** 中的控制器状态

您可以将控制器置于三种不同的状态：联机、脱机和服务模式。

联机状态

联机状态是控制器的正常运行状态。这意味着控制器运行正常、可用于I/O操作。

将控制器置于联机状态时、其状态将设置为最佳。

脱机状态

如果存储阵列中有两个控制器、则脱机状态通常用于准备要更换的控制器。控制器可以通过两种方式进入脱机状态：您可以问题描述 显式命令、否则控制器可能会失败。控制器只能通过发出另一个显式命令或更换发生故障的控制器来退出脱机状态。只有当存储阵列中有两个控制器时、才能使控制器脱机。

如果控制器处于脱机状态、则满足以下条件：

- 此控制器不可用于I/O
- 您不能通过该控制器管理存储阵列。
- 当前由该控制器拥有的任何卷将移至另一个控制器。
- 已禁用缓存镜像、并且所有卷均已更改为通过缓存模式写入。

服务模式

通常、只有技术支持才会使用服务模式将所有存储阵列卷移动到一个控制器、以便对另一个控制器进行诊断。控制器必须手动置于服务模式、并且必须在服务操作完成后手动重新联机。

如果控制器处于服务模式、则满足以下条件：

- 此控制器不可用于I/O
- 技术支持可以通过串行端口或网络连接访问控制器、以分析潜在问题。
- 当前由该控制器拥有的任何卷将移至另一个控制器。
- 已禁用缓存镜像、并且所有卷均已更改为通过缓存模式写入。

了解 **E** 系列控制器的 **IP** 地址分配

默认情况下、控制器在发货时会在两个网络端口上启用DHCP。您可以分配静态IP地址、使用默认静态IP地址或使用DHCP分配的IP地址。您也可以使用IPv6无状态自动配置。

默认情况下、新控制器上会禁用IPv6、但您可以使用其他方法配置管理端口IP地址、然后使用System Manager在管理端口上启用IPv6。

当网络端口处于"链路关闭"状态时、即与LAN断开连接时、系统会将其配置报告为静态、显示IP地址0.0.0.0 (早期版本)、或者已启用DHCP且未报告IP地址(后续版本)。在网络端口处于"链路启动"状态(即连接到LAN)后、它会尝试通过DHCP获取IP地址。

如果控制器无法在给定网络端口上获取DHCP地址、则它将还原为默认IP地址、该地址可能需要长达3分钟的时间。默认IP地址如下：

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

分配IP地址时：

- 预留控制器上的端口2以供客户支持使用。请勿更改默认网络设置(已启用DHCP)。
- 要为E4000、E2800 (EOA)和E5700 (EOA)控制器设置静态IP地址，请使用SANtricity System Manager。
- 要使用DHCP分配控制器的IP地址、请将控制器连接到可以处理DHCP请求的网络。使用永久DHCP租约。

> 默认地址不会在链路关闭事件中保留。如果控制器上的网络端口设置为使用DHCP、则控制器会尝试在每次链路启动事件(包括插入缆线、重新启动和重新加电)时获取DHCP地址。每当DHCP尝试失败时、都会使用该端口的默认静态IP地址。

在 **SANtricity System Manager** 中配置管理端口

此控制器包含一个用于系统管理的以太网端口。如有必要、您可以更改其传输参数和IP地址。

关于此任务

在此操作步骤 期间、您可以选择端口1、然后确定速度和端口寻址方法。端口1连接到管理客户端可访问控制器和System Manager的网络。

> 请勿使用任一控制器上的端口2。端口2已保留供技术支持使用。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 单击包含要配置的管理端口的控制器。

   此时将显示控制器的上下文菜单。
3. 选择*配置管理端口*。

   配置管理端口页面打开。
4. 确保显示端口1、然后单击*下一步*。
5. 选择配置端口设置，然后单击 * 下一步 * 。

   ▼ 字段详细信息

字段	**Description**
速度和双工模式	如果您希望System Manager确定存储阵列与网络之间的传输参数、或者如果您知道网络的速度和模式、请从下拉列表中选择参数、请保留自动协商设置。列表中仅显示有效的速度和双工组合。
启用 IPv4/Enable IPv6	选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。

   如果您选择*启用 IPv4*，单击*下一步*后将显示*配置 IPv4*步骤。如果您选择*启用 IPv6*，单击*下一步*后将显示*配置 IPv6*步骤。如果同时选择两个选项，则首先显示*配置 IPv4*步骤，然后单击*下一步*后，显示*配置 IPv6*步骤。
6. 自动或手动配置 IPv4 和 / 或 IPv6 设置。

▼ 字段详细信息

字段	Description
自动从 DHCP 服务器获取配置	选择此选项可自动获取配置。
手动指定静态配置	选择此选项、然后输入控制器的IP地址。(如果需要、可以剪切地址并将其粘贴到字段中。) 对于IPv4、请包括网络子网掩码和网关。对于 IPv6 ，请包括可路由的 IP 地址和路由器 IP 地址。 如果更改IP地址配置、则会丢失存储阵列的管理路径。如果您使用SANtricity 统一管理器全局管理网络中的阵列、请打开用户界面并转到菜单：管理[发现]。如果您使用的是SANtricity 存储管理器、则必须从企业管理窗口(EMW)中删除此设备、并通过选择菜单：编辑(添加存储阵列)将其重新添加到EMW中、然后输入新的IP地址。

7. 单击 * 完成 * 。

结果

管理端口配置显示在控制器设置的*管理端口设置*部分。

在 **SANtricity System Manager** 中配置 **NTP** 服务器地址

您可以配置与网络时间协议(NTP)服务器的连接、以便控制器定期查询NTP服务器以更新其内部时间时钟。

开始之前

- 必须在网络中安装和配置NTP服务器。
- 您必须知道主NTP服务器和可选备份NTP服务器的地址。这些地址可以是完全限定域名、IPv4地址或IPv6地址。

如果输入NTP服务器的一个或多个域名、则还必须配置DNS服务器以解析NTP服务器地址。您只需要在配置了NTP并提供了域名的控制器上配置DNS服务器。

关于此任务

通过NTP、存储阵列可以使用简单网络时间协议(Simple Network Time Protocol、SNTP)自动将控制器的时钟与外部主机同步。控制器会定期查询已配置的NTP服务器、然后使用结果更新其内部时间时钟。如果只有一个控制器启用了NTP、则备用控制器会定期将其时钟与启用了NTP的控制器同步。如果这两个控制器均未启用NTP、则这些控制器会定期同步各自的时钟。

您无需在两个控制器上配置NTP；但是、这样做可以提高存储阵列在发生硬件或通信故障期间保持同步的能力。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 单击要配置的控制器。

此时将显示控制器的上下文菜单。

3. 选择*配置NTP服务器*。

   此时将打开配置网络时间协议(NTP)服务器页面。

4. 选中*启用 NTP* 复选框。

   页面上会显示其他选项。

5. 选择以下选项之一：

   - 自动从**DHCP**服务器获取**NTP**服务器地址-显示检测到的NTP服务器地址。

     如果存储阵列设置为使用静态NTP地址、则不会显示任何NTP服务器。

   - 手动指定**NTP**服务器地址-输入主NTP服务器地址和备份NTP服务器地址。备份服务器是可选的。(选择单选按钮后、将显示这些地址字段。) 服务器地址可以是完全限定域名、IPv4地址或IPv6地址。

6. *可选：*输入备份NTP服务器的服务器信息和身份验证凭据。

7. 单击 * 保存 * 。

结果

NTP 服务器配置显示在控制器设置的*网络时间协议(NTP)服务器设置*部分。

在 **SANtricity System Manager** 中配置 **DNS** 服务器地址

域名系统(Domain Name System、DNS)用于解析控制器和网络时间协议(Network Time Protocol、NTP)服务器的完全限定域名。存储阵列上的管理端口可以同时支持IPv4或IPv6协议。

开始之前

- 必须在网络中安装和配置DNS服务器。
- 您知道主DNS服务器的地址以及可选的备份DNS服务器。这些地址可以是IPv4地址或IPv6地址。

关于此任务

此操作步骤 介绍如何指定主DNS服务器地址和备份DNS服务器地址。可以选择将备份DNS服务器配置为在主DNS服务器出现故障时使用。

如果您已使用动态主机配置协议(DHCP)配置存储阵列的管理端口、并且您有一个或多个与DHCP设置关联的DNS或NTP服务器、则无需手动配置DNS或NTP。在这种情况下、存储阵列应已自动获取DNS/NTP服务器地址。但是、您仍应按照以下说明打开对话框、并确保检测到正确的地址。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。

   此时将显示控制器的上下文菜单。

2. 选择*配置DNS服务器*。

配置域名系统(DNS)服务器页面打开。

3. 选择以下选项之一：
   - 自动从**DHCP**服务器获取**DNS**服务器地址-显示检测到的DNS服务器地址。

     如果存储阵列设置为使用静态DNS地址、则不会显示任何DNS服务器。

   - 手动指定**DNS**服务器地址-输入主DNS服务器地址和备用DNS服务器地址。备份服务器是可选的。(选择单选按钮后、将显示这些地址字段。) 这些地址可以是IPv4地址或IPv6地址。
4. 单击 * 保存 * 。
5. 对另一个控制器重复上述步骤。

结果

DNS 配置显示在控制器设置的*域名系统 (DNS) 服务器设置*部分。

在 **SANtricity System Manager** 中查看控制器设置

您可以查看有关控制器的信息、例如主机接口、驱动器接口和管理端口的状态。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 执行以下操作之一以显示控制器设置：
   - 单击控制器以显示上下文菜单、然后选择*查看设置*。
   - 选择控制器图标(在*磁盘架*下拉列表旁边)。对于双工配置、从对话框中选择*控制器A*或*控制器B*、然后单击*下一步*。

     控制器设置滑动菜单打开。
3. 请查看各部分以在控制器属性设置之间移动。

▼ 字段详细信息

部分	**Description**
详细信息	显示控制器状态、日期/时间、型号名称和更换零件号。
当前配置	显示当前固件版本和 NVRAM 版本。
数据缓存	显示数据缓存总计。
数据缓存模块	显示缓存模块位置、状态和容量。
处理器缓存	显示处理器缓存总计。
缓存备份设备	显示缓存备份设备位置、状态和容量。
主机接口	显示每个端口的主机接口信息和链路状态。
驱动器接口	显示每个端口的驱动器接口信息和链路状态。
管理端口设置	显示管理端口详细信息，包括控制器主机名、远程登录和 IP 网络设置。

部分	Description
域名系统 (DNS) 服务器设置	显示 DNS 配置、主 DNS 服务器和备份 DNS 服务器。
网络时间协议 (NTP) 服务器设置	显示 NTP 服务和 NTP 服务器配置详细信息。

4. 单击 * 关闭 * 。

在 **SANtricity System Manager** 中配置远程登录 **(SSH)**

通过启用远程登录、您可以允许局域网外部的用户启动控制器上的SSH会话和访问设置。

对于SANtricity 11.74及更高版本、您还可以通过要求用户输入SSH密钥和/或SSH密码来配置多因素授权(Multifactor Authorization、MFA)。对于SANtricity 11.73及更早版本、此功能不包含使用SSH密钥和密码进行多因素授权的选项。

安全风险-出于安全原因、只有技术支持人员才应使用远程登录功能。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。

   此图将发生变化，以显示控制器，而不是驱动器。

2. 单击要为其配置远程登录的控制器。

   此时将显示控制器的上下文菜单。

3. 选择*配置远程登录(SSH)。**(**对于**SANtricity 11.73**及更早版本、此菜单项为*更改远程登录。)**

   配置远程登录 (SSH) 页面打开。

4. 选中*启用远程登录*复选框。

   此设置提供远程登录、并提供三个授权选项：

   - 仅限密码。对于此选项、您已完成并可以单击*保存*。如果您使用的是双工系统、则可以按照上述步骤在第二个控制器上启用远程登录。
   - * SSH密钥或密码*。对于此选项、请继续执行下一步。
   - 密码和**SSH**密钥。对于此选项、选中*需要授权的公有 密钥和密码才能进行远程登录*复选框、然后继续下一步。

5. 填写 **Authorized public keys** 字段。此字段包含采用 OpenSSH **authorized_keys** 文件格式的授权公钥列表。

   填写*授权公钥*字段时，请注意以下准则：

   - *授权公钥*字段适用于两个控制器，只需在第一个控制器上配置。
   - *授权密钥*文件每行只能包含一个密钥。以#开头的行和空行将被忽略。有关文件格式的详细信息、请参见 "为OpenSSH配置授权密钥"。

◦ 一个*授权密钥*文件应类似于以下示例：

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

6. 完成后、单击*保存*。
7. 对于双工系统、您可以按照上述步骤在第二个控制器上启用远程登录。如果要为密码和SSH密钥配置选项、请务必再次选中*需要授权的公有 密钥和密码才能进行远程登录*复选框。
8. 技术支持完成故障排除后，您可以通过返回配置远程登录 (SSH) 页面并取消选中*启用远程登录*复选框来禁用远程登录。如果在第二个控制器上启用了远程登录，则会打开一个确认对话框，允许您同时禁用第二个控制器上的远程登录。

   禁用远程登录将终止任何当前SSH会话并拒绝任何新的登录请求。

在 **SANtricity System Manager** 中将控制器置于联机状态

如果控制器处于脱机状态或服务模式、您可以将其重新联机。

步骤

1. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
2. 单击处于脱机状态或服务模式的控制器。

   此时将显示控制器的上下文菜单。

3. 选择*置于联机状态*、然后确认要执行此操作。

结果

多路径驱动程序检测到已还原的首选路径可能需要长达10分钟的时间。

在收到每个卷的I/O请求时、最初由该控制器拥有的任何卷都会自动移回控制器。在某些情况下、您可能需要使用*重新分布卷*命令手动重新分布卷。

在 **SANtricity System Manager** 中将控制器置于脱机状态

如果系统要求您这样做、则可以将控制器置于脱机状态。

开始之前

- 存储阵列必须具有两个控制器。未置于脱机状态的控制器必须处于联机状态（处于最佳状态）。
- 请确保未使用任何卷，或者在使用这些卷的所有主机上安装了多路径驱动程序。

```
[CAUTION]
====
```

请勿将控制器置于脱机状态、除非`Recovery Guru`或技术支持指示您这样做。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击要置于脱机状态的控制器。
+
此时将显示控制器的上下文菜单。

. 选择*置于脱机状态*、然后确认要执行此操作。

.结果
System
Manager可能需要几分钟的时间才能将控制器状态更新为脱机。更新状态之前，请勿开始任何其他操作。

[[IDfe9052ccce49d51fa96705ac92302e64]]
= 在 SANtricity System Manager 中将控制器置于服务模式
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果系统要求您执行此操作、则可以将控制器置于服务模式。

.开始之前
* 存储阵列必须具有两个控制器。未置于服务模式的控制器必须处于联机状态(处于最佳状态)。
* 请确保未使用任何卷，或者在使用这些卷的所有主机上安装了多路径驱动程序。

[NOTE]
====
将控制器置于服务模式可能会显著降低性能。请勿将控制器置于服务模式、除非技术支持指示您这样做。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击要置于服务模式的控制器。
+
此时将显示控制器的上下文菜单。

. 选择*置于服务模式*、然后确认要执行此操作。

[[IDd115ef502e8aa859d2c1c1b7084ee12c]]
= 在 SANtricity System Manager 中重置（重新启动）控制器
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
某些问题需要重置（重新启动）控制器。您可以重置控制器、即使您无法对其进行物理访问也是如此。

.开始之前
* 存储阵列必须具有两个控制器。不需要重置的控制器必须处于联机状态（处于最佳状态）。
* 请确保未使用任何卷，或者在使用这些卷的所有主机上安装了多路径驱动程序。

.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击要重置的控制器。
+
此时将显示控制器的上下文菜单。

. 选择*重置*、然后确认要执行此操作。

:leveloffset: -1

= 管理iSCSI端口

:leveloffset: +1

[[ID7054341eed559d7d295e11fcb65ab316]]
= 在 SANtricity System Manager 中配置 iSCSI 端口
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果控制器包含iSCSI主机连接、则可以从硬件页面配置iSCSI端口设置。

.开始之前
* 控制器必须包含iSCSI端口；否则、iSCSI设置不可用。
* 您必须知道网络速度(端口与主机之间的数据传输速率)。

[NOTE]
====
只有当存储阵列支持iSCSI时、才会显示iSCSI设置和功能。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击包含要配置的 iSCSI 端口的控制器。
+
此时将显示控制器的上下文菜单。

. 选择 * 配置 iSCSI 端口 * 。
+
[NOTE]
====
只有在System Manager检测到控制器上的iSCSI端口时、才会显示*配置iSCSI端口*选项。

====
+
此时将打开配置 iSCSI 端口对话框。

. 在下拉列表中，选择要配置的端口，然后单击 * 下一步 * 。
. 选择配置端口设置，然后单击 * 下一步 * 。
+
要查看所有端口设置，请单击对话框右侧的 * 显示更多端口设置 * 链接。

+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 端口设置 | Description

a|
配置的以太网端口速度（仅适用于某些类型的主机接口卡）
a|
在端口上选择与SFP速度功能匹配的速度。

a|
正向错误更正(FEC)模式(仅针对某些类型的主机接口卡显示)
a|
如果需要、请为指定主机端口选择一种FEC模式。

NOTE: Reed Solomon模式不支持25 Gbps端口速度。

a|
启用 IPv4/Enable IPv6
a|
选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。

NOTE: 如果要禁用端口访问、请取消选中这两个复选框。

a|
TCP 侦听端口（可通过单击 * 显示更多端口设置 * 来使用。）
a|
如有必要，请输入新的端口号。

侦听端口是控制器用于侦听主机 iSCSI 启动程序的 iSCSI 登录的 TCP 端口号。默认侦听端口为 3260 。您必须输入 3260 或 49152 到 65535 之间的值。

a|
MTU 大小（可通过单击 * 显示更多端口设置 * 来获取。）
a|
如有必要，请为最大传输单元（ Maximum Transmission Unit ， MTU ）输入一个新大小（以字节为单位）。

默认最大传输单元（ Maximum Transmission Unit ， MTU ）大小为每帧 1500 字节。您必须输入一个介于 1500 和 9000 之间的值。

a|
启用 ICMP ping 响应
a|
选择此选项可启用 Internet 控制消息协议（ Internet Control Message Protocol ， ICMP ）。网络计算机的操作系统使用此协议发送消息。这些 ICMP 消息可确定主机是否可访问以及从该主机获取数据包所需的时间。

|===
====
+
如果选择了 * 启用 IPv* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv4 设置。如果选择了 * 启用 IPv6* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv6 设置。如果同时选择了这两个选项，则 IPv4 设置对话框将首先打开，然后单击 * 下一步 * ， IPv6 设置对话框将打开。

. 自动或手动配置 IPv4 和 / 或 IPv6 设置。要查看所有端口设置，请单击对话框右侧的 * 显示更多设置 * 链接。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 端口设置 | Description

 a|
自动获取配置
 a|
选择此选项可自动获取配置。

 a|
手动指定静态配置
 a|
选择此选项，然后在字段中输入静态地址。（如果需要、可以剪切地址并将其粘贴到字段中。） 对于 IPv4、请包括网络子网掩码和网关。对于 IPv6 ，请包括可路由的 IP 地址和路由器 IP 地址。

 a|
启用 VLAN 支持（可通过单击 * 显示更多设置 * 来获取。）
 a|
选择此选项可启用 VLAN 并输入其 ID 。VLAN 是一种逻辑网络，其行为与相同交换机，相同路由器或这两者所支持的其他物理和虚拟局域网（ LAN ）在物理上是分开的。

 a|
启用以太网优先级（单击 *Show more settings* 即可使用。）
 a|

选择此选项可启用用于确定网络访问优先级的参数。使用滑块选择介于1 （最低）和7 （最高）之间的优先级。

在以太网等共享局域网（ LAN ）环境中，许多工作站可能会争用网络访问权限。访问权限按先到先得原则提供。两个工作站可能会同时尝试访问网络，这会导致两个工作站重新关闭并等待，然后再重试。对于只有一个工作站连接到交换机端口的交换式以太网，此过程会最小化。

|===
====
. 单击 * 完成 * 。

[[ID85a02fe7bc49616cf6f315c58daaae10]]
= 在 SANtricity System Manager 中配置 iSCSI 身份验证
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
为了提高iSCSI网络的安全性、您可以在控制器（目标）和主机（启动程序）之间设置身份验证。

System Manager使用质询握手身份验证协议（Challenge Handshake Authentication Protocol、CHAP）方法、在初始链接期间验证目标和启动程序的身份。身份验证基于名为_CHAP secret_的共享安全密钥。

.开始之前
您可以在为目标（控制器）设置CHAP密钥之前或之后为启动程序（iSCSI主机）设置CHAP密钥。在按照此任务中的说明进行操作之前、您应等待主机先建立iSCSI连接、然后在各个主机上设置CHAP密钥。建立连接后、主机的IQN名称及其CHAP密钥将在iSCSI身份验证对话框中列出（如本任务所述）、您无需手动输入它们。

.关于此任务
您可以启用 CHAP 身份验证，然后为单向身份验证指定目标 CHAP 密钥，也可以同时指定启动器 CHAP 密钥以用于控制器和 iSCSI 主机之间的双向身份验证。

单向身份验证允许控制器对 iSCSI 主机的身份进行验证（单向身份验证）。

双向身份验证允许控制器和 iSCSI 主机执行身份验证（双向身份验证）。此选项通过使控制器能够验证 iSCSI 主机的身份，进而使 iSCSI 主机能够验证控制器的身份，从而提供第二级安全保障。

.步骤

. 从左侧面板中，选择 *System*。
. 在 *iSCSI 设置* 下，单击 *配置 iSCSI 身份验证*。
+
此时将显示 Configure Authentication （配置身份验证）窗口。

. 选中 *Enable CHAP authentication* 复选框以启用身份验证。
+
如果不想启用 CHAP 身份验证，请不要选中此框。

. 如果启用了单向身份验证，请输入*目标 CHAP 密码*
，用于对连接到目标的启动器进行身份验证。CHAP 密码必须介于 12 到 57 个可打印的 ASCII 字符之间。
+
在 Confirm target CHAP secret 字段下，重新输入相同的 CHAP 密码进行确认。

. 如果要在控制器和 iSCSI 主机之间启用双向身份验证，请输入*启动器 CHAP 密码
*以由启动器对控制器进行身份验证。CHAP 密码必须介于 12 到 57 个可打印的 ASCII 字符之间。
. 单击 * 保存 * 。

.结果
除非未指定身份验证、否则在控制器和iSCSI主机之间的iSCSI登录序列期间会进行身份验证。

[[ID3b4d3e40f925855497a05c139c31161a]]
= 在 SANtricity System Manager 中启用 iSCSI 发现设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以启用与在iSCSI网络中发现存储设备相关的设置。

通过目标发现设置、您可以使用Internet存储名称服务(iSNS)协议注册存储阵列的iSCSI信息、还可以确定是否允许未命名的发现会话。

.开始之前
如果iSNS服务器使用静态IP地址、则该地址必须可用于iSNS注册。支持IPv4和IPv6。

.关于此任务
您可以启用与iSCSI发现相关的以下设置：

* *启用iSNS服务器以注册目标*-启用后、存储阵列将从iSNS服务器注册其iSCSI限定名称

(IQN)和端口信息。此设置允许iSNS发现、以便启动程序可以从iSNS服务器检索IQN和端口信息。
* *启用未命名的发现会话*-启用未命名的发现会话后、启动程序(iSCSI主机
)无需在发现类型连接的登录顺序期间提供目标(控制器)的IQN。禁用后、主机需要提供IQN、以便与控制器建立发现会话。但是、正常(I/O轴承)会话始终需要目标IQN。禁用此设置可以防止未经授权的iSCSI主机仅使用其IP地址连接到控制器。

[NOTE]
====
只有当您的存储阵列支持 iSCSI 时，iSCSI 设置和功能才会显示在"系统"页面上。

====
.步骤
. 从左侧面板中，选择 *System*。
. 在 *iSCSI 设置* 下，单击 *配置目标发现设置*。
+
此时将显示配置 iSCSI 目标发现设置页面。在 *启用 iSNS 服务器*……
字段下方，页面指示控制器是否已注册。

. 要注册控制器、请选择*启用iSNS服务器以注册我的目标*、然后选择以下选项之一：
+
** *从 DHCP 服务器自动获取 IPv4 服务器地址* -- 如果要使用动态主机配置协议 (DHCP)
服务器配置 iSNS 服务器，请选择此选项。请注意，如果使用此选项，则控制器上的所有 iSCSI
端口也必须配置为使用 DHCP。如有必要，请更新您的控制器 iSCSI 端口设置以启用此选项。
+
[NOTE]
====
要使DHCP服务器提供iSNS服务器地址、必须将DHCP服务器配置为使用选项43 -"`Vendor Specific Information"。` 此选项需要包含iSNS服务器IPv4地址、以数据字节0xA-0xd (10-13)为单位。

====
** *手动指定 IPv4 服务器地址* -- 如果要为 iSNS 服务器输入静态 IP
地址，请选择此选项。（如果需要，您可以将地址剪切并粘贴到字段中。）在字段中，输入 IPv4 地址或 IPv6 地址。如果两者都已配置，则默认为 IPv4。同时输入 TCP 侦听端口（使用默认值 3205
或输入介于 49152 和 65535 之间的值）。

. 要允许存储阵列参与未命名的发现会话、请选择*启用未命名的发现会话*。
+
** 启用后、无需iSCSI启动程序指定目标IQN即可检索控制器的信息。
** 禁用后、除非启动程序提供目标IQN、否则会阻止发现会话。禁用未命名的发现会话可提高安全性。

. 单击 * 保存 * 。

.结果
当System Manager尝试向
iSNS服务器注册控制器时、会显示一个进度条。此过程可能需要长达五分钟的时间。

[[ID643a4adaaed2a1fb78aa42bd4da0c9aa]]
= 在 SANtricity System Manager 中查看 iSCSI 统计信息
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以查看与存储阵列的iSCSI连接的相关数据。

.关于此任务
System Manager将显示这些类型的iSCSI统计信息。所有统计信息均为只读、无法设置。

NOTE: System Manager中显示的统计信息类型取决于存储阵列的可用统计信息。

* *以太网MAC统计信息*-提供介质访问控制(MAC)的统计信息。MAC还提供了一种称为物理地址或
MAC地址的寻址机制。MAC地址是分配给每个网络适配器的唯一地址。MAC地址有助于将数据包传送到子网络中的目标。
* *以太网TCP/IP统计信息*—提供TCP/IP的统计信息、即iSCSI设备的传输控制协议(Transmission Control Protocol、TCP)和Internet协议(Internet Protocol、IP)。通过
TCP、联网主机上的应用程序可以创建彼此的连接、并通过这些连接以数据包的形式交换数据。IP是一种面向数据的协议、用于在数据包交换的网络间通信数据。IPv4统计信息和IPv6统计信息分别显示。
* *Ethernet Kernel STATISTIMENTS*--提供
iSCSI设备的平台内核驱动程序的统计信息。内核统计信息显示的网络数据与TCP/IP统计信息选项类似。但是、内核统计信息数据是从平台内核驱动程序收集的、而不是直接从iSCSI硬件收集的。
* *本地目标/启动程序(协议)统计信息*—显示
iSCSI目标的统计信息、该目标可对其存储介质进行块级访问、并显示在异步镜像操作中用作启动程序时存储阵列的iSCSI统计信息。
* * DCBX运行状态统计信息*-显示各种数据中心桥接交换(DCBX)功能的运行状态。
* * LLDP TLV统计信息*-显示链路层发现协议(Link Layer Discovery Protocol、
LLDP)类型长度值(TLV)统计信息。
* * DCBX TLV统计信息*-显示用于标识数据中心桥接(Data Center Bridging、
DCB)环境中的存储阵列主机端口的信息。此信息将与网络对等方共享、以便于识别和使用。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

.步骤
. 从左侧面板中，选择 *System*。
. 选择*查看 iSCSI 统计信息*。
. 单击一个选项卡可查看不同的统计信息集。
. 要设置基线、请单击*设置新基线*。
+
设置基线将为统计信息的收集设置一个新的起点。所有iSCSI统计信息都使用相同的基线。

[[ID0109307f2bf2ac9346ce1edfa6590409]]
= 在 SANtricity System Manager 中查看 iSCSI 会话
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以查看有关与存储阵列的iSCSI连接的详细信息。iSCSI会话可以与异步镜像关系中的主机或远程存储阵列进行。

.步骤
. 从左侧面板中，选择 *System*。
. 选择*查看/结束 iSCSI 会话*。
+
此时将显示当前iSCSI会话的列表。

. *可选：*要查看有关特定iSCSI会话的追加信息 、请选择一个会话、然后单击*查看详细信息*。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 项目 | Description

a|
会话标识符(SSID)
a|
一个十六进制字符串、用于标识iSCSI启动程序与iSCSI目标之间的会话。SSID由ISID和TPGT组成。

a|
启动程序会话ID (ISID)
a|
会话标识符的启动程序部分。启动程序将在登录期间指定ISID。

a|
目标门户组
a|
iSCSI目标。

a|
目标门户组标记(TPGT)
a|
会话标识符的目标部分。iSCSI目标门户组的16位数字标识符。

a|
启动程序iSCSI名称
a|
启动程序的全球唯一名称。

a|
启动程序iSCSI标签
a|
System Manager中设置的用户标签。

a|
启动程序iSCSI别名
a|
也可以与iSCSI节点关联的名称。此别名允许组织将用户友好型字符串与iSCSI名称相关联。但是、别名不能替代iSCSI名称。启动程序iSCSI别名只能在主机上设置、而不能在System Manager中设置

a|
主机
a|

向存储阵列发送输入和输出的服务器。

a|
连接ID (CID)
a|
启动程序与目标之间会话中连接的唯一名称。启动程序将生成此ID、并在登录请求期间将其呈现给目标。在注销以关闭连接期间、也会显示连接ID。

a|
端口标识符
a|
与连接关联的控制器端口。

a|
启动程序IP地址
a|
启动程序的IP地址。

a|
协商登录参数
a|
在iSCSI会话登录期间处理的参数。

a|
身份验证方法
a|
对要访问iSCSI网络的用户进行身份验证的技术。有效值为* CHAP *和*无*。

a|
标题摘要方法
a|
显示iSCSI会话可能的标头值的技术。HeaderDigest和DataDigest可以是*无*或* CRC32C*。两者的默认值均为*无*。

a|
数据摘要方法
a|
用于显示iSCSI会话的可能数据值的技术。HeaderDigest和DataDigest可以是*无*或*CRC32C*。两者的默认值均为*无*。

a|
最大连接数
a|
iSCSI会话允许的最大连接数。最大连接数可以是1到4。默认值为*。

a|
目标别名
a|
与目标关联的标签。

a|
启动程序别名
a|
与启动程序关联的标签。

a|
目标IP地址
a|
iSCSI会话的目标的IP地址。不支持DNS名称。

a|
初始R2T
a|
初始传输就绪状态。状态可以是*是*或*否*。

a|
最大突发长度
a|

此iSCSI会话的最大SCSI有效负载(以字节为单位)。最大突发长度可以介于512到262、144 (256 KB)之间。默认值为* 262、144 (256 KB)*。

a|
第一个突发长度
a|
此iSCSI会话中未经请求的数据的SCSI有效负载(以字节为单位)。第一个突发长度可以介于512到131、072 (128 KB)之间。默认值为*、65、536 (64 KB)*。

a|
默认等待时间
a|
在连接终止或连接重置后尝试建立连接之前等待的最小秒数。默认等待时间值可以介于0到3600之间。默认值为*。2

a|
要保留的默认时间
a|
连接终止或连接重置后仍可进行连接的最大秒数。默认保留时间可以为0到3600。默认值为*20*。

a|
最大未完成R2T
a|
此iSCSI会话未完成的最大"可传输"数。最大未完成的可传输值可以介于1到16之间。默认值为* 1 *。

a|
错误恢复级别
a|
此iSCSI会话的错误恢复级别。错误恢复级别值始终设置为*。

a|
最大接收数据段长度
a|
启动程序或目标可以在任何iSCSI有效负载数据单元(PDU)中接收的最大数据量。

a|
目标名称
a|
目标的官方名称(而不是别名)。格式为_iqn_的目标名称。

a|
启动程序名称
a|
启动程序的官方名称(而不是别名)。使用_iqn_或_eui_格式的启动程序名称。

|===
====
. *可选：*要将报告保存到文件中、请单击*保存*。
+
此文件将保存在浏览器的"Downloads"文件夹中、文件名为`iscsi-session-connections.txt`。

[[ID114eb94b54984b717ac559e3967a5f58]]
= 在 SANtricity System Manager 中结束 iSCSI 会话
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以结束不再需要的iSCSI会话。iSCSI会话可以与异步镜像关系中的主机或远程存储阵列进行。

.关于此任务
您可能希望结束iSCSI会话的原因如下：

* *未经授权的访问*-如果iSCSI启动程序已登录且无法访问、您可以结束iSCSI会话以强制iSCSI启动程序退出存储阵列。iSCSI启动程序可能已登录、因为无身份验证方法可用。
* *系统停机时间*-如果需要关闭存储阵列、但您发现iSCSI启动程序仍处于登录状态、则可以结束iSCSI会话以将iSCSI启动程序从存储阵列中移出。

.步骤
. 从左侧面板中，选择 *System*。

. 在 *iSCSI 设置* 下，选择 *查看/结束 iSCSI 会话*。
+
此时将显示当前iSCSI会话的列表。

. 选择要结束的会话
. 单击*结束会话*、然后确认要执行此操作。

[[ID284cb5c6ce38278e892838d64297e4e3]]
= 在 SANtricity System Manager 中配置 iSER over InfiniBand 端口
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果控制器包含基于InfiniBand的iSER端口、则可以配置与主机的网络连接。

.开始之前
* 控制器必须包含基于InfiniBand端口的iSER；否则、基于InfiniBand的iSER设置在System Manager中不可用。
* 您必须知道主机连接的IP地址。

.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击具有要配置的iSER over InfiniBand端口的控制器。
+
此时将显示控制器的上下文菜单。

. 选择*通过InfiniBand端口配置iSER *。
+
此时将打开Configure iSER over InfiniBand Ports对话框。

. 在下拉列表中、选择要配置的HIC端口、然后输入主机的IP地址。
. 单击 * 保存 * 。
. 完成配置、然后单击*是*重置基于InfiniBand的iSER端口。

[[ID83d6e9c5e192e6877d7267c3497c002f]]
= 在 SANtricity System Manager 中查看 InfiniBand 上的 iSER 统计数据
:allow-uri-read:

:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果存储阵列的控制器包含基于InfiniBand的iSER端口、则可以查看有关主机连接的数据。

.关于此任务
System Manager会显示以下类型的基于InfiniBand的
iSER统计信息。所有统计信息均为只读、无法设置。

* *本地目标(协议)统计信息*—提供基于InfiniBand的
iSER目标的统计信息、其中显示了对其存储介质的块级访问。
* *基于InfiniBand接口的iSER统计信息*-提供InfiniBand接口上所有
iSER端口的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

.步骤
. 从左侧面板中，选择 *System*。
. 选择*查看基于 InfiniBand 的 iSER 统计信息*。
. 单击一个选项卡可查看不同的统计信息集。
. *可选：*要设置基线、请单击*设置新基线*。
+
设置基线将为统计信息的收集设置一个新的起点。所有基于InfiniBand的iSER统计信息都使用相同的基线。

:leveloffset: -1

= 管理NVMe端口

:leveloffset: +1

[[ID5bd0270a8a8f0777fd3a91b912affe9d]]
= 了解 NVMe 和 SANtricity 软件
:allow-uri-read:
:icons: font

:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
某些控制器包含一个端口、用于在网络结构上实施NVMe （非易失性内存快速协议）。
NVMe支持主机与存储阵列之间的高性能通信。

[[what-is-nvme]]
== 什么是NVMe?

_NVM_表示"非易失性内存"、是许多类型的存储设备中使用的永久性内存。_NVME （NVM Express）是一种标准化接口或协议、专为与NVM设备进行高性能多队列通信而设计。

[[what-is-nvme-over-fabrics]]
== 什么是基于网络结构的NVMe?

基于网络结构的NVMe （NVMe-oF）_是一种技术规范、可通过网络在主机计算机和存储之间传输基于NVMe消息的命令和数据。NVMe存储阵列（称为_subsystem_）可由使用网络结构的主机访问。NVMe命令已启用并封装在主机端和子系统端的传输抽象层中。这样可以将高性能NVMe接口从主机端到端扩展到存储、并对命令集进行标准化和简化。

NVMe-oF存储作为本地块存储设备提供给主机。卷（称为_namespacage_）可以与任何其他块存储设备一样挂载到文件系统。您可以使用REST API、SMcli或SANtricity 系统管理器根据需要配置存储。

[[what-is-an-nvme-qualified-name-nqn]]
== 什么是NVMe限定名称（NQN）?

NVMe限定名称（NQN）用于标识远程存储目标。存储阵列的NVMe限定名称始终由子系统分配、不能修改。整个阵列只有一个NVMe限定名称。NVMe限定名称的长度限制为223个字符。您可以将其与iSCSI限定名称进行比较。

[[what-is-a-namespace-and-a-namespace-id]]
== 什么是命名空间和命名空间ID?

命名空间相当于SCSI中与阵列中的卷相关的逻辑单元。命名空间ID （NSID）相当于SCSI中的逻辑单元号（LUN）。您可以在创建命名空间时创建NSID、并将其设置为1到255之间的值。

[[what-is-an-nvme-controller]]
== 什么是NVMe控制器?

与SCSI I_T Nexus类似、SCSI I_T Nexus表示从主机启动程序到存储系统目标的路径、在主机连接过程中创建的NVMe控制器可在主机与存储阵列中的命名空间之间提供访问路径。主机的NQN加上主机端口标识符可唯一标识NVMe控制器。虽然NVMe控制器只能与单个主机关联、但它可以访问多个命名空间。

您可以使用SANtricity 系统管理器配置哪些主机可以访问哪些命名空间、并为主机设置命名空间ID。然后、在创建NVMe控制器时、将创建可由NVMe控制器访问的命名空间ID列表、并使用这些ID配置允许的连接。

[[ID68fd3264d96b70c94a67fd2c41856000]]
= 在 SANtricity System Manager 中配置 NVMe over InfiniBand 端口
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果控制器包含基于InfiniBand的NVMe连接、则可以从硬件页面配置NVMe端口设置。

.开始之前
* 您的控制器必须包含基于InfiniBand的NVMe主机端口；否则、System Manager中不提供基于InfiniBand的NVMe设置。
* 您必须知道主机连接的IP地址。

[NOTE]
====
只有当存储阵列的控制器包含基于InfiniBand的NVMe端口时、才会显示基于InfiniBand的NVMe设置和功能。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击具有要配置的基于InfiniBand的NVMe端口的控制器。
+
此时将显示控制器的上下文菜单。

. 选择 * 配置基于 InfiniBand 端口的 NVMe * 。
+

此时将打开通过 InfiniBand 端口配置 NVMe 对话框。

. 从下拉列表中选择要配置的HIC端口、然后输入IP地址。
+
如果要为EF600存储阵列配置支持200 GB的HIC、则此对话框会显示两个IP
地址字段、一个用于物理端口(外部)、一个用于虚拟端口(内部)。您应为这两个端口分配唯一的IP地址。通过这些设置、主机可以在每个端口之间建立一条路径、并使HIC实现最高性能。如果不为虚拟端口分配IP地址、HIC将以大约一半的速度运行。

. 单击 * 配置 * 。
. 完成配置、然后单击*是*重置基于InfiniBand的NVMe端口。

[[IDb7bed2f45fcecc891a7557a15421af96]]
= 在 SANtricity System Manager 中配置 NVMe over RoCE 端口
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您的控制器包括通过RoCE连接NVMe (基于融合以太网的RDMA)、则可以从硬件页面配置NVMe端口设置。

.开始之前
* 您的控制器必须包含一个基于RoCE的NVMe主机端口；否则、System Manager中不提供基于RoCE的NVMe设置。
* 您必须知道主机连接的IP地址。

.步骤
. 从左侧面板中，选择菜单：Hardware[Controllers and components]。
. 单击具有要配置的基于 RoCE 的 NVMe 端口的控制器。
+
此时将显示控制器的上下文菜单。

. 选择 * 配置基于 RoCE 的 NVMe 端口 * 。
+
此时将打开通过 RoCE 端口配置 NVMe 对话框。

. 在下拉列表中、选择要配置的HIC端口。
. 单击 * 下一步 * 。
+
要查看所有端口设置，请单击对话框右侧的 * 显示更多端口设置 * 链接。

+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 端口设置 | Description

a|
已配置以太网端口速度
a|
在端口上选择与SFP速度功能匹配的速度。

a|
启用 IPv4/Enable IPv6
a|
选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。

NOTE: 如果要禁用端口访问、请取消选中这两个复选框。

a|
MTU 大小（可通过单击 * 显示更多端口设置 * 来获取。）
a|
如有必要，请为最大传输单元（ Maximum Transmission Unit ， MTU ）输入一个新大小（以字节为单位）。

默认最大传输单元（ Maximum Transmission Unit ， MTU ）大小为每帧 1500 字节。您必须输入一个介于 1500 和 9000 之间的值。

|===
====
+
如果选择了 * 启用 IPv* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv4 设置。如果选择了 * 启用 IPv6* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv6 设置。如果同时选择了这两个选项，则 IPv4 设置对话框将首先打开，然后单击 * 下一步 * ， IPv6 设置对话框将打开。

. 自动或手动配置 IPv4 和 / 或 IPv6 设置。
+
.字段详细信息

[%collapsible]
====
[cols="25h,~"]
|===
| 端口设置 | Description

a|
自动获取配置
a|
选择此选项可自动获取配置。

a|
手动指定静态配置
a|
选择此选项，然后在字段中输入静态地址。(如果需要、可以剪切地址并将其粘贴到字段中。) 对于IPv4、请包括网络子网掩码和网关。对于 IPv6 ，请包括可路由的 IP 地址和路由器 IP 地址。如果要为EF600存储阵列配置支持200 GB的HIC、则此对话框会显示两组网络参数字段、一组用于物理端口(外部)、一组用于虚拟端口(内部)。您应为这两个端口分配唯一的参数。通过这些设置、主机可以在每个端口之间建立一条路径、并使HIC实现最高性能。如果不为虚拟端口分配IP地址、HIC将以大约一半的速度运行。

|===
====
. 单击 * 完成 * 。

[[IDb7b817c25d89493c5fcd463cd386cdd1]]
= 在 SANtricity System Manager 中查看 NVMe over Fabrics 统计信息
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以查看有关通过网络结构连接到存储阵列的NVMe的数据。

.关于此任务
System Manager会显示这些类型的基于网络结构的NVMe统计信息。所有统计信息均为只读、无法设置。

* *NVMe 子系统* -- 显示 NVMe 控制器及其队列的统计信息。NVMe

控制器提供主机与存储阵列中的命名空间之间的访问路径。您可以查看连接失败、重置和关闭等项目的 NVMe 子系统统计信息。
* *RDMA statistics* -- 提供 RDMA 接口上所有 NVMe over Fabrics 端口的统计数据，其中包括与每个交换机端口关联的性能统计数据和链路错误信息。此选项卡仅在 NVMe over Fabrics 端口可用时显示。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

.步骤
. 从左侧面板中，选择 *System*。
. 选择 *View NVMe over Fabrics statistics*。
. *可选：*要设置基线、请单击*设置新基线*。
+
设置基线将为统计信息的收集设置一个新的起点。所有NVMe统计信息都使用相同的基线。

:leveloffset: -1

= 管理驱动器

:leveloffset: +1

[[IDdc7a3d459ba82af7d897246fa3b2d382]]
= 了解 SANtricity System Manager 中的驱动器状态
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity系统管理器会报告驱动器的各种状态。

[[accessibility-states]]
== 可访问性状态

[cols="25h,~"]
|===

| State | 定义

a|
已绕过
a|
驱动器在物理上存在、但控制器无法通过任一端口与其通信。

a|
不兼容
a|
存在以下条件之一：

* 此驱动器未通过认证、无法在存储阵列中使用。
* 驱动器具有不同的扇区大小。
* 此驱动器具有较旧或较新固件版本中的不可用配置数据。

a|
已删除
a|
已从存储阵列中错误地删除此驱动器。

a|
存在
a|
控制器可以通过两个端口与驱动器进行通信。

a|
无响应
a|
驱动器未响应命令。

|===

[[role-states]]
== 角色状态

```
[cols="25h,~"]
|===
| State | 定义


 a|
已分配
 a|
驱动器是池或卷组的成员。


 a|
正在使用热备盘
 a|
当前正在使用此驱动器替代出现故障的驱动器。热备用磁盘仅在卷组中使用、而不在池中使用。


 a|
热备用
 a|
该驱动器已准备好用于替代出现故障的驱动器。热备用磁盘仅在卷组中使用、而不在池中使用。


 a|
未分配
 a|
此驱动器不是池或卷组的成员。

|===


[[availability-states]]
== 可用性状态

[cols="25h,~"]
|===
| State | 定义


 a|
失败
 a|
驱动器不工作。驱动器上的数据不可用。
```

 a|
即将发生故障
 a|
已检测到驱动器可能会很快出现故障。驱动器上的数据仍然可用。

 a|
脱机
 a|
此驱动器不可用于存储数据、通常是因为它属于要导出的卷组或正在进行固件升级。

 a|
最佳
 a|
驱动器工作正常。

|===

[[ID935aa5a90f583a10cb3a6003094e27c1]]
= 了解 SANtricity System Manager 中的固态磁盘 (SSD)
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
固态磁盘（ SSD ）是指使用固态内存（ Flash ）持久存储数据的数据存储设备。SSD 可模拟传统硬盘驱动器，并可与硬盘驱动器使用相同的接口。

[[advantages-of-ssds]]
== SSD的优势

与硬盘驱动器相比、SSD的优势包括：

* 启动速度更快(无转速)
* 延迟更短
* 每秒I/O操作数(IOPS)更高

* 可靠性更高、移动部件更少
* 更低的电耗
* 产生的热量更少、所需的散热也更少

[[identifying-ssds]]
== 识别SSD

从"硬件" > "驱动器"页面，您可以在前架视图中找到
SSD。查找显示闪电图标的驱动器托架，该图标表示已安装 SSD。

[[volume-groups]]
== 卷组

一个卷组中的所有驱动器都必须具有相同的介质类型(所有SSD或所有硬盘驱动器)。卷组不能混合使用介质类型或接口类型。

[[caching]]
== 缓存

控制器的写入缓存始终为SSD启用。写入缓存可提高性能并延长SSD的使用寿命。

除了控制器缓存之外、您还可以实施SSD缓存功能来提高整体系统性能。在SSD缓存中、数据会从卷复制并存储在两个内部RAID卷上(每个控制器一个)。

[[ID993146b2261358387c2742971a76acba]]
= 在 SANtricity System Manager 中筛选驱动器视图
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果存储阵列包含具有不同类型的物理和逻辑属性的驱动器、则硬件页面将提供筛选字段、以帮助您限制驱动器视图并查找特定驱动器。

.关于此任务
驱动器筛选器可以将视图限制为在某些逻辑位置(例如卷组1)仅查看某些类型的物理驱动器(例如、所有SA

S）以及某些安全属性（例如、支持安全）。您可以同时使用这些筛选器、也可以单独使用这些筛选器。

[NOTE]
====
如果所有驱动器共享相同的物理属性，则不会显示 *Show drives that are...*
筛选字段。如果所有驱动器共享相同的逻辑属性，则逻辑位置选项不会出现在筛选字段中。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 在第一个筛选器字段（在*显示驱动器...*下）中、单击下拉箭头以显示可用的驱动器类型和安全属性。
+
驱动器类型可能包括：

+
** 驱动器介质类型（SSD、HDD）
** 驱动器接口类型
** 驱动器容量（最高到最低）
** 驱动器速度（最高到最低）安全属性可能包括：
** 支持安全保护
** 已启用安全保护
** 支持DA （数据保证）
** 符合 FIPS
** 符合FIPS （FIPS 140-2）
** 符合FIPS （FIPS 140-3）
+
如果所有驱动器的这些属性中有任何一个都相同、则它们不会显示在下拉列表中。例如、如果存储阵列包含SAS接口且速度为15000 RPM的所有SSD驱动器、但某些
SSD具有不同的容量、则下拉列表仅显示容量作为筛选选项。

+
从字段中选择一个选项后、与您的筛选条件不匹配的驱动器将在图形视图中灰显。

. 在同一个筛选器字段中，单击下拉箭头以显示驱动器的可用逻辑位置。
+
[NOTE]
====
如果需要清除筛选条件、请选择筛选框最右侧的*清除*。

====
+
逻辑位置可能包括：

+
** 池

** 卷组
** 热备用磁盘
** SSD 缓存
** 未分配
+
从字段中选择一个选项后、与您的筛选条件不匹配的驱动器将在图形视图中灰显。

. 或者，您可以在过滤器字段最右侧选择*打开定位灯*，以打开显示驱动器的定位灯。
+
此操作可帮助您以物理方式查找存储阵列中的驱动器。

[[ID6cb597ce18dfa2f95ed148303a62fb96]]
= 在 SANtricity System Manager 中打开驱动器定位器指示灯
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在硬件页面中、您可以打开定位器指示灯以查找驱动器在存储阵列中的物理位置。

.关于此任务
您可以找到硬件页面上显示的单个或多个驱动器。

.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 要查找一个或多个驱动器、请执行以下操作之一：
+
** *单个驱动器* --
从货架图形中，找到要在阵列中实际定位的驱动器。单击驱动器以显示其上下文菜单，然后选择*打开定位灯*。
+
驱动器的定位灯亮起。找到驱动器后、返回对话框并选择*关闭*。

** *多个驱动器* --
在筛选器字段中，选择物理驱动器类型和逻辑驱动器类型。符合条件的驱动器数量显示在该字段的最右侧。接下来，单击*打开定位灯*。物理定位驱动器后，返回对话框并选择*关闭*。

[[ID37769136a7bd3dd501e9a83d7843846a]]
= 在 SANtricity System Manager 中查看驱动器状态和设置
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以查看驱动器的状态和设置、例如介质类型、接口类型和容量。

.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 选择要查看其状态和设置的驱动器。
+
此时将打开驱动器的上下文菜单。

. 选择 * 查看设置 * 。
+
驱动器设置面板打开。

. 要查看所有设置，请滚动浏览"驱动器设置"面板。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | Description

 a|
Status
 a|
显示最佳、脱机、非关键故障和故障。最佳状态表示所需的工作条件。

 a|
模式
 a|
显示已分配、未分配、热备用备用或热备用正在使用。

a|
位置
a|
显示驱动器所在的磁盘架和托架编号。

a|
已分配给/可以保护/保护
a|
如果将驱动器分配给池、卷组或SSD缓存、则此字段将显示"已分配给"。
此值可以是池名称、卷组名称或SSD缓存名称。如果驱动器已分配给热备用磁盘且其模式为备用、则此字段将显示"可保护"。
如果热备用磁盘可以保护一个或多个卷组、则会显示卷组名称。如果无法保护卷组、则显示0个卷组。

如果驱动器已分配给热备用磁盘且其模式正在使用中、则此字段将显示"正在保护"。
此值是受影响卷组的名称。

如果未分配此驱动器、则不会显示此字段。

a|
介质类型
a|
显示驱动器使用的录制介质类型、可以是硬盘驱动器(HDD)或固态磁盘(SSD)。

a|
已用持久性百分比(仅在存在SSD驱动器时显示)
a|
迄今为止写入驱动器的数据量除以理论写入总限制。

a|
接口类型
a|
显示驱动器使用的接口类型、例如SAS。

a|
驱动器路径冗余
a|

显示驱动器与控制器之间的连接是否为冗余(是)或非冗余(否)。

a|
容量(GiB)
a|
显示驱动器的可用容量(总配置容量)。

a|
速度（ RPM ）
a|
以RPM为单位显示速度(对于SSD不显示)。

a|
当前数据速率
a|
显示驱动器与存储阵列之间的数据传输速率。

a|
逻辑扇区大小(字节)
a|
显示驱动器使用的逻辑扇区大小。

a|
物理扇区大小(字节)
a|
显示驱动器使用的物理扇区大小。通常、硬盘驱动器的物理扇区大小为4096字节。

a|
驱动器固件版本
a|
显示了驱动器固件的修订版级别。

a|

全球范围的标识符

a|
显示了驱动器的唯一十六进制标识符。

a|
产品ID

a|
显示制造商分配的产品标识符。

a|
序列号

a|
显示驱动器的序列号。

a|
制造商

a|
显示了驱动器的供应商。

a|
制造日期

a|
显示驱动器的构建日期。

NOTE： 不适用于NVMe驱动器。

a|
支持安全保护

a|
显示驱动器是否支持安全(是)(否)。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(级别140-2或140-3)、用于在写入期间对数据进行加密、并在读取期间对数据进行解密。这些驱动器被视为安全驱动器-_capable"、因为可以使用驱动器安全功能提高安全性。如果为这些驱动器使用的卷组和池启用了驱动器安全功能、则这些驱动器将变为secure—_enabled_.

a|
已启用安全保护
a|
显示驱动器是否已启用安全保护(是)(否)。启用了安全保护的驱动器与驱动器安全功能结合使用。启用驱动器安全功能后、如果将驱动器安全应用于安全-
_capable"驱动器上的池或卷组、则这些驱动器将变为安全-
enabled。只能通过配置了正确安全密钥的控制器进行读写访问。这种增强的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。

a|
可读/写
a|
显示驱动器是否可读/写(是)(否)。

a|
驱动器安全密钥标识符
a|
显示了已启用安全的驱动器的安全密钥。驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS
）驱动器提供额外的安全层。如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。

a|
支持数据保证(Data Assurance、DA)
a|
显示数据保证(Data Assurance、DA)功能是否已启用(Yes)或未启用(No)。数据保证(Data Assurance、DA)是一项功能、用于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。可以在池或卷组级别启用数据保证、主机使用光纤通道等具有DA功能的I/O接口。

a|
支持DULBE
a|
指示是否启用已取消分配或未写入逻辑块错误 (DULBE) 选项（是）或未启用（否）。DULBE 是 NVMe 驱动器上的一个选项，允许 EF80、EF50、EF300 或 EF600 存储阵列支持资源调配的卷。

|===
====
. 单击 * 关闭 * 。

[[IDb1daa212ab2d7e4c4abf05421707944a]]
= 在 SANtricity System Manager 中逻辑替换驱动器
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果某个驱动器发生故障或您出于任何其他原因需要更换该驱动器、您可以从逻辑上将该故障驱动器替换为未分配的驱动器或完全集成的热备用驱动器。

.关于此任务
在逻辑上替换某个驱动器时、该驱动器将变为已分配、然后成为关联池或卷组的永久成员。

您可以使用logical replace选项替换以下类型的驱动器：

* 故障驱动器
* 缺少驱动器
* Recovery Guru通知您即将停产的SSD驱动器
* Recovery Guru通知您驱动器即将发生故障的硬盘驱动器
* 已分配的驱动器(仅适用于卷组中的驱动器、而不适用于池中的驱动器)

.开始之前
替代驱动器必须具有以下特征：

* 处于最佳状态
* 处于未分配状态
* 与要更换的驱动器具有相同的属性(介质类型、接口类型等)
* 相同的FDE功能(建议、但不要求)
* 相同的DA功能(建议使用、但不要求使用)

.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 单击要在逻辑上替换的驱动器。
+
此时将显示驱动器的上下文菜单。

. 单击*逻辑替换*。
. *可选：*选中*更换后故障驱动器*复选框、以便在更换后使原始驱动器发生故障。
+
只有在原始分配的驱动器未出现故障或不缺失时、才会启用此复选框。

. 从*选择替代驱动器*表中、选择要使用的替代驱动器。
+
此表仅列出与要更换的驱动器兼容的驱动器。如果可能、请选择一个将保持磁盘架丢失保护和抽屉丢失保护的驱动器。

. 单击*替换*。
+
如果原始驱动器出现故障或丢失、则会使用奇偶校验信息在替代驱动器上重建数据。此重建将自动开始。驱动器的故障指示灯熄灭、池或卷组中驱动器的活动指示灯开始闪烁。

+
如果原始驱动器未出现故障或丢失、则其数据将复制到替代驱动器。此复制操作将自动开始。复制操作完成后、系统会将原始驱动器过渡到未分配状态、或者如果选中了复选框、则过渡到故障状态。

[[IDf8c01a3d99cc6cc95a9b1d86584660e6]]
= 在 SANtricity System Manager 中手动重建驱动器
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
更换驱动器后、驱动器重建通常会自动开始。如果驱动器重建未自动启动、您可以手动启动重建。

[NOTE]
====
只有在技术支持或 Recovery Guru 指示执行此操作时，才能执行此操作。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 单击要手动重建的驱动器。
+
此时将显示驱动器的上下文菜单。

. 选择*重建*、然后确认您要执行此操作。

[[IDd232e9f7551250e61b42593173322a1f]]
= 在 SANtricity System Manager 中初始化（格式化）驱动器
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果将分配的驱动器从一个存储阵列移动到另一个存储阵列、则必须先初始化（格式化）驱动器、然后才能在新存储阵列中使用它们。

.关于此任务
初始化会从驱动器中删除先前的配置信息、并将其返回到未分配状态。然后、可以将此驱动器添加到新存储阵列中的新池或卷组中。

移动单个驱动器时、请使用初始化驱动器操作。如果要将整个卷组从一个存储阵列移动到另一个存储阵列、则无需初始化驱动器。

[CAUTION]
====
可能的数据丢失—初始化驱动器时、驱动器上的所有数据都将丢失。只有在技术支持要求时、才执行此操作。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 单击要初始化的驱动器。
+
此时将显示驱动器的上下文菜单。

. 选择*初始化*、然后确认要执行此操作。

[[IDefec548be5c04d008a69ab7bc1604522]]
= 在 SANtricity System Manager 中手动关闭驱动器
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果系统要求您这样做、您可以手动使驱动器出现故障。

.关于此任务
System Manager可监控存储阵列中的驱动器。如果检测到驱动器生成大量错误、Recovery Guru会通知您驱动器即将发生故障。如果发生这种情况、并且您有可用的替代驱动器、则可能需要使该驱动器发生故障以采取预防性措施。如果没有可用的替代驱动器、您可以等待驱动器自行出现故障。

[CAUTION]
====
可能丢失数据访问-此操作可能会导致数据丢失或数据冗余丢失。只有在技术支持或 Recovery Guru 指示执行此操作时，才能执行此操作。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 单击要失败的驱动器。
+
此时将显示驱动器的上下文菜单。

. 选择*失败*。
. 保持选中*在故障前复制驱动器内容*复选框。
+
只有已分配的驱动器和非RAID 0卷组才会显示复制选项。

+
在驱动器出现故障之前、请确保复制驱动器的内容。根据您的配置、如果不先复制驱动器的内容、可能会丢失关联池或卷组上的所有数据或数据冗余。

+
与重建相比、复制选项可以加快驱动器恢复速度、并减少在复制操作期间另一个驱动器发生故障时卷发生故障的可能性。

. 确认要使驱动器出现故障。
+
驱动器发生故障后、请至少等待60秒、然后再将其删除。

[[ID1a25fc0e68642d42e0e28604aa69699b]]
= 在 SANtricity System Manager 中擦除驱动器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以使用擦除选项准备要从系统中删除的未分配驱动器。此操作步骤
会永久删除数据、以确保无法再次读取数据。

.开始之前
驱动器必须处于未分配状态。

.关于此任务
只有在要永久删除驱动器上的所有数据时、才使用擦除选项。如果驱动器已启用安全保护、则擦除选项将执行加密擦除、并将驱动器的安全属性重置回支持安全保护的属性。

[NOTE]
====
擦除功能不支持某些旧型号的驱动器。如果您尝试擦除其中一个较旧的型号、则会显示一条错误消息。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 您也可以使用筛选器字段查看磁盘架中所有未分配的驱动器。从*显示驱动器...*下拉列表中、选择*未分配*。
+
磁盘架视图仅显示未分配的驱动器；所有其他驱动器均显示为灰色。

. 要打开驱动器的上下文菜单、请单击要擦除的驱动器。
（如果要选择多个驱动器、可以在擦除驱动器对话框中执行此操作。）
+
[CAUTION]
====
可能的数据丢失-擦除操作无法撤消。确保在操作步骤 期间选择正确的驱动器。

====
. 从上下文菜单中，选择 *Erase*。
+
此时将打开擦除驱动器页面，显示擦除操作的所有符合条件的驱动器。

. 如果需要、请从表中选择其他驱动器。您不能选择
_all_驱动器；请确保仍有一个驱动器处于未选中状态。
. 通过键入 `erase`确认操作，然后单击 *Erase*。
+
[CAUTION]
====
请务必继续执行此操作。在下一个对话框中单击是后、此操作将无法中止。

====

. 在擦除驱动器估计完成时间对话框中，单击 *擦除* 以继续执行擦除操作。

.结果
擦除操作可能需要几分钟或几个小时。您可以在菜单中查看状态：监控[正在进行的操作]。擦除操作完成后，驱动器可以在另一个卷组或磁盘池或另一个存储阵列中使用。

.完成后
如果要再次使用该驱动器、必须先对其进行初始化。要执行此操作、请从驱动器的上下文菜单中选择*初始化*。

[[ID3e7c20e2b084fd912a9dadbe5a105f8f]]
= 在 SANtricity System Manager 中解锁或重置锁定的 NVMe 或 FIPS 驱动器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您将一个或多个锁定的NVMe或FIPS驱动器插入存储阵列、则可以通过添加与这些驱动器关联的安全密钥文件来解锁驱动器数据。如果您没有安全密钥、则可以通过输入每个锁定驱动器的物理安全ID (PSID)对其执行重置、以重置其安全属性并擦除驱动器数据。

.开始之前
* 对于"解锁"选项，请确保安全密钥文件（扩展名为 `.slk`）在管理客户端（使用浏览器访问 System Manager 的系统）上可用。您还必须知道与密钥关联的密码短语。
* 对于"Reset"选项、您必须在要重置的每个驱动器上找到PSID。要找到PSID、请物理卸下驱动器、并在驱动器标签上找到PSID字符串(最多32个字符)、然后重新安装驱动器。

.关于此任务
此任务介绍如何通过将安全密钥文件导入到存储阵列中来解锁NVMe或FIPS驱动器中的数据。如果安全密钥不可用、此任务还会介绍如何对锁定的驱动器执行重置。

[NOTE]
====
如果使用外部密钥管理服务器锁定驱动器，请在 SANtricity System Manager 中选择菜单：System[Security key management]，以配置外部密钥管理并解锁驱动器。

====
您可以从硬件页面或 menu:System[Security key management] 访问解锁功能。以下任务提供了硬件页面的操作说明。

.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 选择要解锁或重置的NVMe或FIPS驱动器。
+
此时将打开驱动器的上下文菜单。

. 选择*解锁*以应用安全密钥文件；如果没有安全密钥文件、则选择*重置*。
+
只有在选择锁定的NVMe或FIPS驱动器时、才会显示这些选项。

+
[CAUTION]
====
在重置操作期间、所有数据都会被擦除。只有在没有安全密钥的情况下、才能执行重置。重置锁定驱动器会永久删除驱动器上的所有数据、并将其安全属性重置为"支持安全"、但未启用。*此操作不可逆。*

====
. 执行以下操作之一：
+
.. *解锁*：在*解锁安全驱动器
*页面上，选择要解锁的驱动器对应的安全密钥文件。接下来，输入密码，然后单击*解锁*。
.. *重置*：在*重置锁定驱动器*对话框中，在字段中输入 PSID 字符串，然后键入 `RESET`以确认。单击*重置*。
+
对于解锁操作、只需执行一次此操作即可解锁所有NVMe或FIPS驱动器。对于重置操作、您必须分别选择要重置的每个驱动器。

.结果
现在、该驱动器可在另一个卷组或磁盘池中使用、也可在另一个存储阵列中使用。

:leveloffset: -1

= 管理热备件

:leveloffset: +1

[[IDf66b5896a782973df836ecd7bc8a6186]]
= 了解 SANtricity System Manager 中的热备用驱动器
:allow-uri-read:

:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
热备件在SANtricity系统管理器的RAID 1、RAID 5或RAID 6卷组中用作备用驱动器。

它们是功能完备的驱动器、不包含任何数据。如果卷组中的某个驱动器发生故障、控制器会自动将故障驱动器中的数据重新构建到分配为热备用驱动器的驱动器中。

热备用磁盘不专用于特定卷组。它们可用于存储阵列中的任何故障驱动器、只要热备用驱动器和驱动器共享以下属性：

* 容量相等（或热备用磁盘容量更大）
* 相同介质类型（例如HDD或SSD）
* 相同的接口类型（例如SAS）

[[how-to-identify-hot-spares]]
== 如何识别热备用磁盘

您可以通过初始设置向导或硬件页面分配热备用磁盘。要确定是否已分配热备用磁盘、请转到硬件页面并查找以粉色显示的任何驱动器托架。

[[how-hot-spare-coverage-works]]
== 热备用磁盘覆盖的工作原理

热备用磁盘覆盖范围如下：

* 您可以将未分配的驱动器预留为RAID 1、RAID 5或RAID 6卷组的热备用驱动器。
+
[NOTE]
====
热备用磁盘不能用于具有不同数据保护方法的池。池会在池的每个驱动器中预留备用容量（称为_preservation
capacity_）、而不是预留额外的驱动器。如果池中的驱动器发生故障、则控制器将以该备用容量重建数据。

====
* 如果RAID 1、RAID 5或RAID
6卷组中的驱动器发生故障、控制器将自动使用冗余数据重建故障驱动器中的数据。热备用磁盘会自动替换故障驱动器、而无需物理交换。

*
在物理更换故障驱动器后、会从热备用驱动器到更换的驱动器执行回写操作。如果已将热备用驱动器指定为卷组的永久成员、则不需要执行回写操作。
*
卷组的托盘丢失保护和抽盒丢失保护是否可用取决于卷组中驱动器的位置。由于驱动器发生故障以及热备用驱动器的位置、托盘丢失保护和抽盒丢失保护可能会丢失。要确保托盘丢失保护和抽盒丢失保护不受影响、您必须更换故障驱动器以启动回写过程。
* 在更换故障驱动器时、存储阵列卷将保持联机并可访问、因为热备用驱动器会自动替换故障驱动器。

[[considerations-for-hot-spare-drive-capacity]]
== 热备用驱动器容量注意事项

选择容量等于或大于要保护的驱动器总容量的驱动器。例如、如果您有一个配置容量为8 GiB的18 GiB驱动器、则可以使用一个9 GiB或更大的驱动器作为热备用驱动器。通常、除非驱动器的容量等于或大于存储阵列中最大驱动器的容量、否则不要将其分配为热备用驱动器。

[NOTE]
====
如果没有具有相同物理容量的热备用磁盘、则如果驱动器的"已用容量"等于或小于热备用驱动器的容量、则可以将容量较低的驱动器用作热备用磁盘。

====

[[considerations-for-media-and-interface-types]]
== 介质和接口类型的注意事项

用作热备用磁盘的驱动器必须与要保护的驱动器共享相同的介质类型和接口类型。例如、HDD驱动器不能用作SSD驱动器的热备用磁盘。

[[considerations-for-secure-capable-drives]]
== 支持安全的驱动器的注意事项

支持安全的驱动器(例如FDE或FIPS)可用作具有或不具有安全功能的驱动器的热备用磁盘。但是、不支持安全的驱动器不能用作具有安全功能的驱动器的热备用磁盘。

如果您选择一个已启用安全保护的驱动器来用作热备用磁盘、则System Manager会提示您先执行安全擦除、然后才能继续操作。安全擦除会将驱动器的安全属性重置为支持安全但未启用安全。

[NOTE]

====
启用驱动器安全功能后、如果从支持安全的驱动器创建池或卷组、则这些驱动器将变为_secure enabled"。只能通过配置了正确安全密钥的控制器进行读写访问。这种增强的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。

====

[[recommended-number-of-hot-spare-drives]]
== 建议的热备用驱动器数量

如果您使用初始设置向导自动创建热备用磁盘、则System Manager会为特定介质类型和接口类型的每30个驱动器创建一个热备用磁盘。否则、您可以在存储阵列中的卷组之间手动创建热备用驱动器。

[[ID4e97033074006b66489e71a4da09ffa4]]
= 在 SANtricity System Manager 中分配热备件
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以在RAID 1、RAID 5或RAID 6卷组中将热备用磁盘分配为备用驱动器、以实现额外的数据保护。如果其中一个卷组中的驱动器发生故障、则控制器会将故障驱动器中的数据重新构建到热备用磁盘中。

.开始之前
* 必须创建RAID 1、RAID 5或RAID 6卷组。
(热备用磁盘不能用于池。相反、池会使用每个驱动器中的备用容量来保护其数据。)
* 必须具有满足以下条件的驱动器：
+
** 未分配、状态为最佳。
** 与卷组中的驱动器类型相同(例如SSD)。
** 与卷组中的驱动器的接口类型相同(例如、SAS)。
** 容量等于或大于卷组中驱动器的已用容量。

.关于此任务
此任务介绍如何从硬件页面手动分配热备用磁盘。建议覆盖的范围是每个驱动器集两个热备件。

[NOTE]
====

也可以通过初始设置向导分配热备用磁盘。您可以通过在硬件页面上查看以粉色显示的驱动器托架来确定是否已分配热备用磁盘。

====
.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 选择要用作热备用磁盘的未分配驱动器(以灰色显示)。
+
此时将打开驱动器的上下文菜单。

. 选择*分配热备用磁盘*。
+
如果驱动器已启用安全功能，则会打开"安全擦除驱动器"对话框。要将启用安全的驱动器用作热备盘，您必须首先执行安全擦除操作以删除其所有数据并重置其安全属性。

+
[CAUTION]
====
可能的数据丢失—确保选择的驱动器正确无误。完成安全擦除操作后、您将无法恢复任何数据。

====
+
如果驱动器*未*启用安全功能，则会打开"分配热备盘驱动器"对话框。

. 查看对话框中的文本、然后确认操作。
+
驱动器在硬件页面上以粉色显示、表示它现在是热备用磁盘。

.结果
如果RAID 1、RAID 5或RAID
6卷组中的驱动器发生故障、控制器会自动使用冗余数据将故障驱动器中的数据重建到热备用磁盘。

[[ID648e459bad971e332a8d69bffb475610]]
= 在 SANtricity System Manager 中取消分配热备用
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将热备用磁盘重新更改为未分配的驱动器。

.开始之前
热备用磁盘必须处于最佳待机状态。

.关于此任务
您不能取消分配当前接管故障驱动器的热备用磁盘。如果热备用磁盘未处于最佳状态、请按照Recovery Guru过程更正所有问题、然后再尝试取消分配驱动器。

.步骤
. 从左侧面板中，选择菜单：Hardware[Drives]。
. 选择要取消分配的热备用驱动器(以粉色显示)。
+
如果粉色驱动器托架中存在对角线、则表示热备用磁盘当前正在使用中、无法取消分配。

+
此时将打开驱动器的上下文菜单。

. 从驱动器的下拉列表中、选择*取消分配热备用磁盘*。
+
此对话框将显示因删除此热备用磁盘而受影响的任何卷组、以及是否有任何其他热备用磁盘对其进行保护。

. 确认取消分配操作。

.结果
驱动器将恢复为未分配(以灰色显示)。

```
:leveloffset: -1

[[ID8de9268e257be4f9b310142a041a8fba]]
= SANtricity System Manager 存储架常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
```
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。

```
[[what-is-shelf-loss-protection-and-drawer-loss-protection]]
```

== 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盒丢失保护是池和卷组的属性、可用于在单个磁盘架或抽盒发生故障时保持数据访问。

[[shelf-loss-protection]]
=== 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。

[NOTE]
====
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:

[cols="1a,1a,1a"]
|===
| 级别 | 磁盘架丢失保护的标准 | 所需的最小磁盘架数

 a|
池
 a|
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高容量磁盘架；如果您的系统包含高容量磁盘架、请参阅"抽屉丢失保护"。
 a|
5.

 a|
RAID 6
 a|
卷组在一个磁盘架中包含的驱动器不超过两个。
 a|
3.

 a|

RAID 3或RAID 5
 a|
卷组中的每个驱动器都位于一个单独的磁盘架中。
 a|
3.

 a|
RAID 1
 a|
RAID 1对中的每个驱动器都必须位于一个单独的磁盘架中。
 a|
2.

 a|
RAID 0
 a|
无法实现磁盘架丢失保护。
 a|
不适用

|===

[[drawer-loss-protection]]
=== 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。

[NOTE]
====
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：

[cols="1a,1a,1a"]
|===
| 级别 | 抽盒丢失保护的标准 | 所需的最小抽盒数量

a|
池
a|
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。
a|
5.

a|
RAID 6
a|
卷组在一个抽屉中包含的驱动器不超过两个。
a|
3.

a|
RAID 3或RAID 5
a|
卷组中的每个驱动器都位于一个单独的抽盒中。
a|
3.

a|
RAID 1
a|
镜像对中的每个驱动器都必须位于一个单独的抽盒中。
a|
2.

a|
RAID 0
a|
无法实现抽盒丢失保护。
a|
不适用

|===

[[what-are-battery-learn-cycles]]
== 什么是电池学习周期?

学习周期是指自动校准智能电池电量表的周期。

学习周期包括以下阶段：

* 受控电池放电
* 休息时间
* 收费

电池将放电至预定的阈值。在此阶段、将校准电池电量表。

学习周期需要以下参数：

* 电池电量已满
* 无过热电池

双工控制器系统的学习周期会同时进行。对于使用多个电池或一组电池供电的控制器、学习周期按顺序进行。

学习周期按计划定期在一周中的同一时间和同一天自动启动。周期之间的间隔以周为单位进行说明。

[NOTE]
====
学习周期可能需要几个小时才能完成。

====

[[IDe40fa28463b86b9349cb13bbb0f7e770]]
= SANtricity System Manager 的存储控制器常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

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。

[[what-is-auto-negotiation]]
== 什么是自动协商?

自动协商是指网络接口能够自动将其自身的连接参数(速度和双工)与另一个网络接口进行协调。

自动协商通常是配置管理端口的首选设置；但是、如果协商失败、不匹配的网络接口设置可能会严重影响网络性能。如果这种情况不可接受、您应手动将网络接口设置为正确的配置。自动协商由控制器的以太网管理端口执行。iSCSI主机总线适配器不会执行自动协商。

[NOTE]
====
如果自动协商失败、控制器将尝试在10BASE-T半双工位置建立连接、这是最低的通用分母。

====

[[what-is-ipv6-stateless-address-auto-configuration]]
== 什么是IPv6无状态地址自动配置?

使用无状态自动配置时、主机不会从服务器获取地址和其他配置信息。

IPv6中的无状态自动配置功能包括链路本地地址、多播和邻居发现(ND)协议。IPv6可以从底层数据链路层地址生成地址的接口ID。

无状态自动配置与有状态自动配置互为补充。例如、主机可以使用无状态自动配置来配置自己的地址、但可以使用有状态自动配置来获取其他信息。有状态自动配置允许主机从服务器获取地址和其他配置信息。Internet协议版本6 (IPv6)还定义了一种方法、可通过此方法一次性重新编号网络上的所有IP地址。IPv6为网络上的设备定义了一种无需服务器即可自动配置其IP地址和其他参数的方法。

使用无状态自动配置时、设备会执行以下步骤：

. *生成链路本地地址*-设备生成链路本地地址、地址有10位、后跟54个零、后跟64位接口ID。
. *测试链路本地地址的唯一性
*—节点将进行测试、以确保其生成的链路本地地址未在本地网络上使用。节点使用NDD协议发送邻居请求消息。作为响应、本地网络会侦听邻居公告消息、这表示另一个设备已在使用链路本地地址。如果是、则必须生成新的链路本地地址或自动配置失败、并且必须使用另一种方法。
. *分配链路本地地址*-如果设备通过唯一性测试、则设备会将链路本地地址分配给其IP接口。链路本地地址可用于在本地网络上进行通信、但不能通过Internet进行通信。
. *联系路由器
*—节点尝试联系本地路由器、以了解有关继续配置的详细信息。执行此联系的方法是、侦听路由器定期发送的路由器公告消息、或者发送特定的路由器请求消息以要求路由器提供有关下一步操作的信息。
. *向节点提供方向*-
路由器向节点提供如何继续自动配置的方向。或者、路由器会告知主机如何确定全局Internet地址。

. *配置全局地址*—主机使用其全局唯一
Internet地址对自身进行配置。此地址通常由路由器提供给主机的网络前缀构成。

[[which-do-i-choose-dhcp-or-manual-configuration]]
== 我该选择哪一个——DHCP 还是手动配置?

网络配置的默认方法是动态主机配置协议(Dynamic Host Configuration Protocol、DHCP)。除非您的网络没有DHCP服务器、否则请始终使用此选项。

[[what-is-a-dhcp-server]]
== 什么是DHCP服务器?

动态主机配置协议(Dynamic Host Configuration Protocol、DHCP)是一种可自动执行Internet协议(IP)地址分配任务的协议。

必须为连接到TCP/IP网络的每个设备分配一个唯一的IP地址。这些设备包括存储阵列中的控制器。

如果没有DHCP、网络管理员可以手动输入这些IP地址。使用DHCP时、当客户端需要启动TCP/IP操作时、客户端会广播地址信息请求。DHCP服务器接收请求、在称为租赁期的指定时间段内分配新地址、并将该地址发送给客户端。使用DHCP时、设备每次连接到网络时都可以具有不同的IP地址。在某些系统中、即使设备仍处于连接状态、设备的IP地址也会发生更改。

[[how-do-i-configure-my-dhcp-server]]
== 如何配置DHCP服务器?

您必须将动态主机配置协议(DHCP)服务器配置为对存储阵列中的控制器使用静态Internet协议(IP)地址。

DHCP服务器分配的IP地址通常是动态的、可能会发生更改、因为它们的租赁期已到期。某些设备(例如服务器和路由器)需要使用静态地址。存储阵列中的控制器还需要静态IP地址。

有关如何分配静态地址的信息、请参见DHCP服务器的文档。

[[why-do-i-need-to-change-the-controller-network-configuration]]
== 为什么需要更改控制器网络配置?

使用带外管理时、您必须为每个控制器设置网络配置、包括其Internet协议(IP)地址、子网掩码(子网掩码)和网关。

您可以使用动态主机配置协议(DHCP)服务器设置网络配置。如果您不使用DHCP服务器、则必须手动输入网络配置。

[[where-do-i-get-the-network-configuration]]
== 从何处获取网络配置?

您可以从网络管理员处获取Internet协议(IP)地址、子网掩码(子网掩码)和网关信息。

在控制器上配置端口时需要此信息。

[[what-are-icmp-ping-responses]]
== 什么是ICMP ping响应?

Internet控制消息协议(Internet Control Message Protocol、ICMP)是TCP/IP套件的协议之一。

`ICMP echo request`和`ICMP echo reply`消息通常称为`ping`消息。`Ping`是一款故障排除工具、系统管理员可使用此工具手动测试网络设备之间的连接、并测试网络延迟和数据包丢失。`ping`命令会将`ICMP echo request`发送到网络上的设备、并且设备会立即响应`ICMP echo reply`。有时、公司的网络安全策略要求在所有设备上禁用`ping`(`ICMP echo reply`)、以使未经授权的人员更难发现这些设备。

[[when-should-i-refresh-the-port-configuration]]
== 何时应刷新端口配置?

随时修改或升级DHCP服务器、并且与当前存储阵列和要使用的存储阵列相关的DHCP信息已更改、请刷新此服务器。

具体而言、如果您知道DHCP服务器将分配不同的地址、请从DHCP服务器刷新端口配置或iSNS服务器。

[NOTE]
====
刷新端口配置会对该端口上的所有iSCSI连接造成破坏。

====

[[what-should-i-do-after-configuring-the-management-ports]]
== 配置管理端口后应执行什么操作?

如果更改了存储阵列的IP地址、则可能需要在SANtricity 统一管理器中更新全局阵列视图。

要在Unified Manager中更新全局阵列视图、请打开界面并转到菜单：Manage （管理）[Discover（发现）。

如果您仍在使用SANtricity 存储管理器、请转到企业管理窗口(EMW)、其中必须删除并重新添加新的IP地址。

[[why-is-the-storage-system-in-non-optimal-mode]]
== 为什么存储系统处于非最佳模式?

存储系统处于非最佳模式是由于系统配置无效状态所致。尽管处于此状态、但完全支持对现有卷进行正常I/O访问；但是、SANtricity系统管理器将禁止某些操作。

存储系统可能会过渡到"系统配置无效"、原因如下：

* 此控制器不合规、可能是因为其子型号ID (SMID)代码不正确或已超过高级功能限制。
* 正在执行内部服务操作、例如驱动器固件下载。
* 控制器超过奇偶校验错误阈值并进入锁定状态。
* 发生常规锁定情况。

[[ID352ec9acd8ab9f90bfa92440add99cf7]]
= SANtricity System Manager 的 iSCSI 协议常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[what-happens-when-i-use-an-isns-server-for-registration]]
== 使用iSNS服务器进行注册时会发生什么情况?

使用Internet存储名称服务(iSNS)服务器信息时、可以将主机(启动程序)配置为查询iSNS服务器以从目标(控制器)检索信息。

此注册可为iSNS服务器提供控制器的iSCSI限定名称(IQN)和端口信息、并允许在启动程序(iSCSI主机)和目标(控制器)之间进行查询。

[[which-registration-methods-are-automatically-supported-for-iscsi]]
== iSCSI自动支持哪些注册方法?

iSCSI实施支持Internet存储名称服务(iSNS)发现方法或使用发送目标命令。

iSNS方法允许在启动程序(iSCSI主机)和目标(控制器)之间进行iSNS发现。您注册目标控制器以向iSNS服务器提供控制器的iSCSI限定名称(IQN)和端口信息。

如果不配置iSNS、则iSCSI主机可以在iSCSI发现会话期间发送发送目标命令。作为响应、控制器将返回端口信息(例如目标IQN、端口IP地址、侦听端口和目标端口组)。如果使用iSNS、则不需要此发现方法、因为主机启动程序可以从iSNS服务器检索目标IP。

[[how-do-i-interpret-iser-over-infiniband-statistics]]
== 如何解读基于InfiniBand统计信息的iSER?

View iSER over InfiniBand statistics 对话框显示本地目标（协议）统计数据和 iSER over InfiniBand (IB) 接口统计数据。所有统计信息均为只读，无法设置。

* *本地目标(协议)统计信息*—提供基于InfiniBand的
iSER目标的统计信息、其中显示了对其存储介质的块级访问。
* * iSER over InfiniBand Interface statistics*—提供InfiniBand
接口上所有基于InfiniBand端口的iSER的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

[[what-else-do-i-need-to-do-to-configure-or-diagnose-iser-over-infiniband]]
== 要通过InfiniBand配置或诊断iSER、还需要执行哪些操作?

下表列出了可用于配置和管理基于InfiniBand会话的iSER的SANtricity系统管理器功能。

[NOTE]
====
只有当存储阵列的控制器包含基于InfiniBand的iSER主机管理端口时、iSER over InfiniBand设置才可用。

====
[cols="35h,~"]
|===
| Action | 位置

 a|
通过InfiniBand端口配置iSER
 a|
. 选择菜单：Hardware[Controllers and components]。
. 选择一个控制器。
. 选择*通过InfiniBand端口配置iSER *。

或

. 选择*System*。
. 向下滚动到 *iSER over InfiniBand settings*，然后选择 *Configure iSER over InfiniBand ports*。

 a|
查看基于InfiniBand的iSER统计信息
 a|
. 选择*System*。
. 向下滚动到 *iSER over InfiniBand settings*，然后选择 *View iSER over InfiniBand statistics*。

|===

[[what-else-do-i-need-to-do-to-configure-or-diagnose-iscsi]]
== 配置或诊断iSCSI还需要执行哪些操作?

iSCSI会话可以与异步镜像关系中的主机或远程存储阵列进行。下表列出了可用于配置和管理这些iSCSI会话的SANtricity系统管理器功能。

[NOTE]
====
只有当存储阵列支持iSCSI时、iSCSI设置才可用。

====

[[configure-iscsi]]
=== 配置iSCSI

[cols="1a,1a"]
|===
| Action | 位置

a|
管理iSCSI设置
a|
. 选择*System*。
. 向下滚动到* iSCSI设置*可查看所有管理功能。

a|
配置iSCSI端口
a|
. 选择 * 硬件 * 。
. 选择*控制器和组件*选项卡。
. 选择一个控制器。
. 选择 * 配置 iSCSI 端口 * 。

a|
设置主机CHAP密钥
a|
. 选择*System*。
. 向下滚动到 *iSCSI 设置*，然后选择*通过 InfiniBand 身份验证配置 iSCSI/iSER*。

或

. 选择菜单： Storage[Hosts] 。
. 选择一个主机成员。
. 单击菜单：查看/编辑设置[主机端口]选项卡。

|===

[[diagnose-iscsi]]
=== 诊断iSCSI

[cols="1a,1a"]
|===
| Action | 位置

 a|
查看或结束iSCSI会话
 a|
. 选择*System*。
. 向下滚动到 *iSCSI 设置*，然后选择 *查看/结束 iSCSI 会话*。

或

. 选择菜单：Support[Diagnostics]。
. 选择*查看/结束 iSCSI 会话*。

 a|
查看iSCSI统计信息
 a|
. 选择*System*。
. 向下滚动到 *iSCSI 设置*，然后选择 *查看 iSCSI 统计信息*。

或

. 选择菜单：Support[Diagnostics]。
. 选择*查看 iSCSI 统计信息*。

|===

[[IDeb252de11ee9715ccf9ec2c52cf33e9b]]
= SANtricity System Manager 的 NVMe 协议常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[how-do-i-interpret-nvme-over-fabrics-statistics]]
== 如何解读基于网络结构的NVMe统计信息？

View NVMe over Fabrics 统计信息对话框显示 NVMe 子系统和 RDMA 接口的统计信息。所有统计信息均为只读，无法设置。

* * NVMe子系统统计信息*-显示NVMe控制器及其队列的统计信息。
NVMe控制器可在主机与存储阵列中的命名空间之间提供访问路径。您可以查看连接故障、重置和关闭等项的NVMe子系统统计信息。有关这些统计信息的详细信息、请单击*查看表标题的图例*。
* * RDMA接口统计信息*-提供RDMA接口上所有基于网络结构的NVMe端口的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。只有当基于网络结构的NVMe端口可用时、才会显示此选项卡。有关统计信息的详细信息、请单击*查看表标题的图例*。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

[[what-else-do-i-need-to-do-to-configure-or-diagnose-nvme-over-infiniband]]
== 要配置或诊断基于InfiniBand的NVMe、还需要执行哪些操作？

下表列出了可用于配置和管理基于InfiniBand的NVMe会话的SANtricity系统管理器功能。

[NOTE]
====
只有当存储阵列的控制器包含基于InfiniBand的NVMe端口时、基于InfiniBand的NVMe设置才可用。

====
[cols="35h,~"]
|===
| Action | 位置

 a|
配置基于InfiniBand的NVMe端口
 a|
. 选择菜单：Hardware[Controllers and components]。
. 选择一个控制器。
. 选择 * 配置基于 InfiniBand 端口的 NVMe * 。

或

. 选择*System*。
. 向下滚动到 *NVMe over InfiniBand settings*，然后选择 *Configure NVMe over InfiniBand ports*。

 a|
查看基于InfiniBand的NVMe统计信息
 a|
. 选择*System*。
. 向下滚动到 *NVMe over InfiniBand settings*，然后选择 *View NVMe over Fabrics statistics*。

|===

[[what-else-do-i-need-to-do-to-configure-or-diagnose-nvme-over-roce]]
== 要通过RoCE配置或诊断NVMe、还需要执行哪些操作?

您可以从硬件和系统页面配置和管理 NVMe over RoCE。

[NOTE]
====
只有当存储阵列的控制器包含基于RoCE的NVMe端口时、基于RoCE的NVMe设置才可用。

====
[cols="35h,~"]
|===
| Action | 位置

 a|
配置基于RoCE的NVMe端口
 a|
. 选择 * 硬件 * 。
. 选择*控制器和组件*选项卡。
. 选择一个控制器。
. 选择 * 配置基于 RoCE 的 NVMe 端口 * 。

或

. 选择*System*。

. 向下滚动到 *NVMe over RoCE settings*，然后选择 *Configure NVMe over RoCE ports*。

a|
查看基于网络结构的NVMe统计信息
a|
. 选择*System*。
. 向下滚动到 *NVMe over RoCE 设置*，然后选择 *View NVMe over Fabrics statistics*。

|===

[[why-are-there-two-ip-addresses-for-one-physical-port]]
== 为什么一个物理端口有两个IP地址?

EF600存储阵列可以包含两个HIC—一个外部HIC和一个内部HIC。

在此配置中、外部HIC连接到内部辅助HIC。您可以从外部HIC访问的每个物理端口都具有来自内部HIC的关联虚拟端口。

要获得最大200 GB性能、必须为物理端口和虚拟端口分配唯一的
IP地址、以便主机可以与每个端口建立连接。如果不为虚拟端口分配IP地址、HIC将以大约一半的速度运行。

[[why-are-there-two-sets-of-parameters-for-one-physical-port]]
== 为什么一个物理端口有两组参数?

EF600存储阵列可以包含两个HIC—一个外部HIC和一个内部HIC。

在此配置中、外部HIC连接到内部辅助HIC。您可以从外部HIC访问的每个物理端口都具有来自内部HIC的关联虚拟端口。

要获得最大200
GB的性能、您必须为物理端口和虚拟端口分配参数、以便主机可以与每个端口建立连接。如果不为虚拟端口分配参数、HIC将以大约一半的可用速度运行。

[[ID7c7aab1c9de3c2f45e2a195d49a095dd]]
= SANtricity System Manager 存储驱动器常见问题解答
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
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。

```
[[what-is-a-hot-spare-drive]]
```
== 什么是热备用驱动器?

热备用磁盘在RAID 1、RAID 5或RAID
6卷组中充当备用驱动器。它们是功能完备的驱动器、不包含任何数据。如果卷组中的驱动器发生故障、控制器会自动将故障驱动器中的数据重新构建为热备用磁盘。

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。

热备盘驱动器不专用于特定的卷组。相反，您可以为存储阵列中容量相同或较小的任何故障驱动器使用热备盘驱动器。热备盘驱动器必须与其保护的驱动器具有相同的介质类型（HDD 或 SSD）。在 EF80 和 EF50 系统中，热备盘驱动器还必须与容量驱动器类型相匹配。

```
[NOTE]
====
```
池不支持热备用驱动器。池使用构成池的每个驱动器中的保留容量、而不是热备用驱动器。

```
====
```

```
[[what-is-preservation-capacity]]
```
== 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。

```
[[why-would-i-logically-replace-a-drive]]
```

== 为什么要从逻辑上更换驱动器?

如果某个驱动器发生故障或您出于任何其他原因需要更换它、并且您的存储阵列中有一个未分配的驱动器、则可以从逻辑上将故障驱动器替换为未分配的驱动器。如果您没有未分配的驱动器、则可以改用物理方式更换该驱动器。

原始驱动器中的数据将复制或重建到替代驱动器上。

[[where-can-i-view-the-status-of-a-drive-undergoing-reconstruction]]
== 在何处可以查看正在重建的驱动器的状态?

您可以从正在执行的操作仪表板查看驱动器重建状态。

从左侧面板中，选择 menu:Monitoring[Operations in progress]。

根据驱动器的不同、完全重建可能需要相当长的时间。如果卷所有权发生变化、则可能会进行完全重建、而不是快速重建。

:leveloffset: -1

= 警报

:leveloffset: +1

[[IDd1411b97d891f1cd1d5a6209ef1902a6]]
= 了解 SANtricity System Manager 中的警报
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将SANtricity系统管理器配置为通过电子邮件、SNMP陷阱和系统日志消息发送存储阵列警报。

[[what-are-alerts]]
== 什么是警报?

_Alerts_向管理员通知存储阵列上发生的重要事件。事件可能包括电池故障、组件从最佳状态移至脱机状态或控制器出现冗余错误等问题。所有严重事件以及一些警告和信息性事件均视为"可处理"。

了解更多信息。

* xref:{relative_path}how-alerts-work.html["警报的工作原理"]
* xref:{relative_path}alerts-terminology.html["警报术语"]

[[how-do-i-configure-alerts]]
== 如何配置警报?

您可以将警报配置为作为消息发送到一个或多个电子邮件地址、作为 SNMP 陷阱发送到 SNMP 服务器或作为消息发送到 syslog 服务器。警报配置可从 menu:Alerts[] 获得。

了解更多信息。

* xref:{relative_path}configure-mail-server-and-recipients-for-alerts.html["为警报配置邮件服务器和收件人"]
* xref:{relative_path}configure-syslog-server-for-alerts.html["为系统日志服务器配置警报"]
* xref:{relative_path}configure-snmp-alerts.html["配置SNMP警报"]

[[related-information]]
== 相关信息

详细了解与警报相关的概念:

* xref:{relative_path}../sm-support/overview-event-log.html["事件日志概述"]
* xref:{relative_path}why-are-timestamps-inconsistent-between-the-array-and-alerts.html["时间戳不一致"]

= 概念

:leveloffset: +1

[[IDd3f6abd2a06dd07fb5b5e78242faa3ba]]
= SANtricity System Manager 中的警报工作原理

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
警报会向管理员通知存储阵列上发生的重要事件。可以通过电子邮件， SNMP 陷阱和系统日志发送警报。

警报过程的工作原理如下：

. 管理员在System Manager中配置以下一种或多种警报方法：
+
** *电子邮件*-将消息发送到电子邮件地址。
** * SNMP *- SNMP陷阱将发送到SNMP服务器。
** *系统日志*-将消息发送到系统日志服务器。

.
当存储阵列的事件监视器检测到问题时，它将有关该问题的信息写入事件日志（可从菜单：Monitoring[Event log]）。例如，问题可能包括电池故障、组件从 Optimal 变为 Offline 或控制器中的冗余错误等事件。
. 如果事件监控器确定该事件为"可处理"事件、则会使用配置的警报方法(电子邮件、SNMP和/或系统日志)发送通知。所有严重事件以及一些警告和信息性事件均视为"可处理"。

```
[[alerts-configuration]]
```
== 警报配置

您可以从初始设置向导（仅适用于电子邮件警报）或从警报页面配置警报。要访问警报页面，请从左侧面板转到 menu:Alerts[]。

```
[[alerts-information]]
```
== 警报信息

警报可以包括以下类型的信息：

* 存储阵列的名称。
* 与事件日志条目相关的事件错误类型。
* 事件发生的日期和时间。
* 事件的简短问题描述。

[NOTE]
====
系统日志警报遵循RFC 5424消息传送标准。

====

[[ID0291d0636a27fb698402b9ff65656302]]
= 了解 SANtricity 软件中的警报术语
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解警报术语如何应用于存储阵列。

[cols="25h,~"]
|===
| 组件 | Description

 a|
事件监控器
 a|
事件监控器位于存储阵列上、并作为后台任务运行。当事件监控器检测到存储阵列上的异常时、它会将有关问题的信息写入事件日志。问题可能包括电池故障、组件从最佳状态移至脱机状态或控制器出现冗余错误等事件。如果事件监控器确定该事件为"可处理"事件、则会使用配置的警报方法(电子邮件、SNMP和/或系统日志)发送通知。所有严重事件以及一些警告和信息性事件均视为"可处理"。

 a|
邮件服务器
 a|
邮件服务器用于发送和接收电子邮件警报。服务器使用简单邮件传输协议(SMTP)。

 a|
SNMP
 a|
简单网络管理协议(Simple Network Management Protocol、SNMP)是一种Internet标准协议、用于在IP网络上的设备之间管理和共享信息。

a|
SNMP陷阱
a|
SNMP陷阱是发送到SNMP服务器的通知。此陷阱包含有关存储阵列重大问题的信息。

a|
SNMP 陷阱目标
a|
SNMP陷阱目标是运行SNMP服务的服务器的IPv4或IPv6地址。

a|
社区名称
a|
团体名称是一个字符串、其作用类似于SNMP环境中网络服务器的密码。

a|
MIB文件
a|
管理信息库(Management Information Base、
MIB)文件定义了要在存储阵列中监控和管理的数据。必须使用SNMP服务应用程序在服务器上复制和编译此文件。此MIB文件随System Manager软件一起提供、位于支持站点上。

a|
MIB变量
a|
管理信息库(Management Information Base、MIB)
变量可以返回存储阵列名称、阵列位置以及响应SNMP GetRequests的联系人等值。

a|
系统日志
a|
系统日志是网络设备用于向日志记录服务器发送事件消息的协议。

 a|
UDP
 a|
用户数据报协议(User Datagram Protocol、
UDP)是一种传输层协议、用于在其数据包标头中指定源端口号和目标端口号。

|===

:leveloffset: -1

= 管理电子邮件警报

:leveloffset: +1

[[ID902535b50e7d64a0da6d2fb12b121fd8]]
= 在 SANtricity System Manager 中配置邮件服务器和警报收件人
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置电子邮件警报、您必须指定邮件服务器地址和警报收件人的电子邮件地址。最多允许20个电子邮件地址。

.开始之前
* 邮件服务器的地址必须可用。该地址可以是IPv4或IPv6地址、也可以是完全限定域名。
+
[NOTE]
====
要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从硬件页面配置DNS服务器。

====
* 要用作警报发件人的电子邮件地址必须可用。此地址显示在警报消息的"发件人"字段中。
SMTP协议中需要提供发件人地址；如果没有此地址、则会导致错误。
*
警报收件人的电子邮件地址必须可用。收件人通常是网络管理员或存储管理员的地址。您最多可以输入20个电子邮件地址。

.关于此任务
此任务介绍如何配置邮件服务器、输入发件人和收件人的电子邮件地址，以及测试从"电子邮件警报"页面输入的所有电子邮件地址。

[NOTE]
====
也可以从初始设置向导配置电子邮件警报。

====
.步骤
. 从左侧面板中，选择菜单：警报[Email alerts]。
+
如果尚未配置电子邮件服务器，页面将显示"Configure Mail Server"。

. 选择*配置邮件服务器*。
+
此时将打开配置邮件服务器对话框。

. 输入邮件服务器信息、然后单击*保存*。
+
** *邮件服务器地址*-输入邮件服务器的完全限定域名、IPv4地址或IPv6地址。
+
[NOTE]
====
要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从硬件页面配置DNS服务器。

====
** *电子邮件发件人地址*-
输入要用作电子邮件发件人的有效电子邮件地址。此地址将显示在电子邮件的"发件人"字段中。
** *加密*—如果要对消息进行加密、请选择* SMTPS*或*
STARTTLS作为加密类型、然后选择加密消息的端口号。否则、请选择*无*。
** *用户名和密码*-如果需要、请输入用户名和密码、以便向传出发件人和邮件服务器进行身份验证。
** *在电子邮件中包含联系信息*-
要在警报消息中包含发件人的联系信息、请选择此选项、然后输入姓名和电话号码。
+
点击*保存*后，电子邮件地址将显示在电子邮件提醒页面上。

. 选择*添加电子邮件*。
+
此时将打开添加电子邮件对话框。

. 输入警报收件人的一个或多个电子邮件地址、然后单击*添加*。
+
电子邮件地址将显示在"电子邮件提醒"页面上。

. 如果要确保电子邮件地址有效、请单击*测试所有电子邮件*向收件人发送测试消息。

.结果
配置电子邮件警报后、每当发生可警报的事件时、事件监控器都会向指定的收件人发送电子邮件消息。

[[ID4244b4b44dd89f3c4100eb0fd1192a6c]]
= 在 SANtricity System Manager 中编辑警报的电子邮件地址
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以更改接收电子邮件警报的收件人的电子邮件地址。

.开始之前
您要编辑的电子邮件地址必须在"电子邮件警报"页面上定义。

.步骤
. 从左侧面板中，选择菜单：警报[Email alerts]。
. 从*电子邮件地址*表中、选择要更改的地址、然后单击最右侧的*编辑*(铅笔)图标。
+
该行将变为可编辑字段。

. 输入新地址、然后单击*保存*(复选标记)图标。
+
[NOTE]
====
如果要取消更改、请选择*取消*(X)图标。

====

.结果
电子邮件警报页面显示更新后的电子邮件地址。

[[ID25fa24908e0080aca11e31a1320ddb44]]
= 在 SANtricity System Manager 中添加警报的电子邮件地址
:allow-uri-read:
:experimental:

:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您最多可以为电子邮件警报添加20个收件人。

.步骤
. 从左侧面板中，选择菜单：警报[Email alerts]。
. 选择*添加电子邮件*。
+
此时将打开添加电子邮件对话框。

. 在空字段中、输入新的电子邮件地址。如果要添加多个地址、请选择*添加其他电子邮件*以打开另一个字段。
. 单击 * 添加 * 。

.结果
电子邮件警报页面将显示新电子邮件地址。

[[ID338c2815b2b73b670256c794788f67f8]]
= 在 SANtricity System Manager 中删除警报的邮件服务器或电子邮件地址
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以删除先前定义的邮件服务器、以使警报不再发送到电子邮件地址、也可以删除各个电子邮件地址。

.步骤
. 从左侧面板中，选择菜单：警报[Email alerts]。
. 从表中、执行以下操作之一：
+
** 要删除邮件服务器以使警报不再发送到电子邮件地址、请选择邮件服务器所在的行。
**
要删除电子邮件地址以使警报不再发送到此地址、请选择要删除的电子邮件地址所在的行。表右上角的*删除*按钮可供选择。

. 单击*删除*、然后确认操作。

[[IDd1e1ae25b28628bf20ade37800299a5f]]
= 在 SANtricity System Manager 中编辑警报邮件服务器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以更改用于电子邮件警报的邮件服务器地址和电子邮件发件人地址。

.开始之前
您要更改的邮件服务器的地址必须可用。该地址可以是IPv4或IPv6地址、也可以是完全限定域名。

[NOTE]
====
要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从硬件页面配置DNS服务器。

====
.步骤
. 从左侧面板中，选择菜单：警报[Email alerts]。
. 选择*配置邮件服务器*。
+
此时将打开配置邮件服务器对话框。

. 编辑邮件服务器地址、发件人信息和联系信息。
+
** *邮件服务器地址*-编辑邮件服务器的完全限定域名、IPv4地址或IPv6地址。
+
[NOTE]
====
要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从硬件页面配置DNS服务器。

====
** *电子邮件发件人地址*-编辑要用作电子邮件发件人的电子邮件地址。此地址将显示在电子邮件的"发件人"字段中。
** *在电子邮件中包括联系信息*-要编辑发件人的联系信息、请选择此选项、然后编辑姓名和电话号码。

. 单击 * 保存 * 。

:leveloffset: -1

= 管理SNMP警报

:leveloffset: +1

[[ID6bec9603cac94b63a13b7f7e0ebab577]]
= 在 SANtricity System Manager 中配置 SNMP 警报
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置简单网络管理协议(Simple Network Management Protocol、SNMP)警报、您必须至少确定一台存储阵列的事件监控器可以发送SNMP陷阱的服务器。此配置需要社区名称或用户名以及服务器的IP地址。

.开始之前
* 必须为网络服务器配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
* 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。
+
如果您没有MIB文件、可以从NetApp支持站点获取：

+
** 转至 https://mysupport.netapp.com/site/global/dashboard["NetApp 支持"^]。
** 单击*下载*选项卡、然后选择*下载*。
** 单击* E系列SANtricity 操作系统控制器软件*。
** 选择*下载最新版本*。
** 登录。
** 接受警告声明和许可协议。
** 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

.关于此任务
此任务介绍如何识别陷阱目标的SNMP服务器、然后测试您的配置。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
首次设置时，页面显示"配置社区/用户"。

. 选择*配置社区/用户*。
+
此时将打开选择SNMP版本对话框。

. 为警报选择SNMP版本、可以是* SNMPv2c*或* SNMPv3 *。
+
根据您的选择、将打开配置社区对话框或配置SNMPv3用户对话框。

. 按照SNMPv2c （社区）或SNMPv3 （用户）的相应说明进行操作：
+
** * SNMPv2c （社区
）*—在配置社区对话框中、为网络服务器输入一个或多个社区字符串。社区名称是一个字符串、用于标识一组已知的管理工作站、通常由网络管理员创建。它仅包含可打印的ASCII字符。您最多可以添加256个社区。完成后、单击*保存*。
** * SNMPv3 （用户）*—在配置SNMPv3用户对话框中、单击*添加*、然后输入以下信息：
+
*** *用户名*-输入一个名称以标识用户、该名称最长可达31个字符。
*** *引擎ID*-选择引擎ID、此
ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择*本地*。如果您使用的是非标准配置、请选择*自定义*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
*** *身份验证凭据*-
选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
*** *隐私凭据*-
选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。完成后、单击*添加*、然后单击*关闭*。

. 单击*添加陷阱目的地*。
+
此时将打开添加陷阱目标对话框。

. 输入一个或多个陷阱目标、选择其关联的社区名称或用户名、然后单击*添加*。
+
** *陷阱目标*-输入运行SNMP服务的服务器的IPv4或IPv6地址。
** *社区名称或用户名*-从下拉列表中、为此陷阱目标选择社区名称(SNMPv2c)或用户名(SNMPv3)。(如果您仅定义了一个、则此名称已显示在此字段中。)
** *发送身份验证失败陷阱* -- 如果要在 SNMP
请求因无法识别的社区名称或用户名而被拒绝时向陷阱目标发出警报，请选择此选项（复选框）。单击*添

加*后，陷阱目标和相关名称将显示在 *SNMP 警报*页面上。

. 要确保陷阱有效、请从表中选择一个陷阱目标、然后单击*测试陷阱目标*向配置的地址发送测试陷阱。

.结果
每当发生可更改的事件时、事件监控器都会向服务器发送SNMP陷阱。

[[IDc550923e1d8ecd1bce365553e0c992f6]]
= 在 SANtricity System Manager 中为 SNMP 警报添加陷阱目标
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您最多可以添加10个服务器来发送SNMP陷阱。

.开始之前
* 要添加的网络服务器必须配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
* 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。
+
如果您没有MIB文件、可以从NetApp支持站点获取：

+
** 转至 https://mysupport.netapp.com/site/global/dashboard["NetApp 支持"^]。
** 单击*下载*、然后选择*下载*。
** 单击* E系列SANtricity 操作系统控制器软件*。
** 选择*下载最新版本*。
** 登录。
** 接受警告声明和许可协议。
** 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
表中将显示当前定义的陷阱目标。

. 选择 *Add Trap Destinations*。
+
此时将打开添加陷阱目标对话框。

. 输入一个或多个陷阱目标、选择其关联的社区名称或用户名、然后单击*添加*。
+
** *陷阱目标*-输入运行SNMP服务的服务器的IPv4或IPv6地址。
** *社区名称或用户名*-从下拉列表中、为此陷阱目标选择社区名称(SNMPv2c)或用户名(SNMPv3)。(如果您仅定义了一个、则此名称已显示在此字段中。)
** *发送身份验证失败陷阱*-如果要在SNMP请求因社区名称或用户名无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击*添加*后、陷阱目标以及关联的社区名称或用户名将显示在表中。

. 要确保陷阱有效、请从表中选择一个陷阱目标、然后单击*测试陷阱目标*向配置的地址发送测试陷阱。

.结果
每当发生可更改的事件时、事件监控器都会向服务器发送SNMP陷阱。

[[IDee4edb3cf179c8fdcaac5da57f96f98e]]
= 在 SANtricity System Manager 中配置 SNMP MIB 变量
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于SNMP警报、您可以选择配置SNMP陷阱中显示的管理信息库(Management Information Base、MIB)变量。这些变量可以返回存储阵列名称、阵列位置和联系人。

.开始之前
必须使用SNMP服务应用程序在服务器上复制和编译MIB文件。

如果您没有MIB文件、可以按如下所示获取它：

* 转至 https://mysupport.netapp.com/site/global/dashboard["NetApp 支持"^]。
* 单击*下载*、然后选择*下载*。
* 单击* E系列SANtricity 操作系统控制器软件*。
* 选择*下载最新版本*。
* 登录。
* 接受警告声明和许可协议。

* 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

.关于此任务
此任务介绍如何为SNMP陷阱定义MIB变量。这些变量可返回以下值以响应SNMP GetRequests：

* `sysName`(存储阵列的名称)
* `sysLocation`(存储阵列的位置)
* `sysContact`(管理员姓名)

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
. 选择*配置SNMP MIB变量*。
+
此时将打开配置SNMP MIB变量对话框。

. 输入以下一个或多个值、然后单击*保存*。
+
** *名称*- MIB变量`sysName`的值。例如、输入存储阵列的名称。
** *位置*- MIB变量`sysLocation`的值。例如、输入存储阵列的位置。
** *联系人*- MIB变量`sysContact`的值。例如、输入负责存储阵列的管理员。

.结果
这些值显示在存储阵列警报的SNMP陷阱消息中。

[[ID616d57e1e1308bb89a8444da3fe3b6fa]]
= 在 SANtricity System Manager 中编辑 SNMPv2c 陷阱的社区
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以编辑SNMPv2c陷阱的社区名称。

.开始之前
必须创建社区名称。

.步骤

. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目标和社区名称将显示在表中。

. 选择*配置社区*。
. 输入新的社区名称、然后单击*保存*。团体名称只能包含可打印的ASCII字符。

.结果
SNMP 警报页面显示更新的社区名称。

[[ID28daf7b7999c2b78142e02795cea0122]]
= 在 SANtricity System Manager 中编辑 SNMPv3 陷阱的用户设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以编辑SNMPv3陷阱的用户定义。

.开始之前
必须为SNMPv3陷阱创建用户。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目标和用户名显示在表中。

. 要编辑用户定义、请在表中选择用户、然后单击*配置用户*。
. 在对话框中、单击*查看/编辑设置*。
. 编辑以下信息：
+
** *用户名*-更改标识用户的名称、该名称最长可达31个字符。
** *引擎ID*-选择引擎ID、此
ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择*本地*。如果您使用的是非标准配置、请选择*自定义*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
** *身份验证凭据*-
选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
** *隐私凭据*-
选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。

密码长度必须介于8到128个字符之间。

.结果
SNMP 警报页面将显示更新后的设置。

[[IDc3d1be88b8029c984e4e5301ebb9fd6f]]
= 在 SANtricity System Manager 中为 SNMPv2c 陷阱添加社区
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您最多可以为SNMPv2c陷阱添加256个社区名称。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目标和社区名称将显示在表中。

. 选择*配置社区*。
+
此时将打开配置社区对话框。

. 选择*添加其他社区*。
. 输入新的社区名称、然后单击*保存*。

.结果
新的社区名称将显示在 SNMP 警报页面上。

[[ID5b81f620015aaca7f4ba811bdce4533a]]
= 在 SANtricity System Manager 中为 SNMPv3 陷阱添加用户
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于SNMPv3陷阱、您最多可以添加256个用户。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目标和用户名显示在表中。

. 选择*配置用户*。
+
此时将打开配置SNMPv3用户对话框。

. 选择 * 添加 * 。
. 输入以下信息、然后单击*添加*。
+
** *用户名*-输入一个名称以标识用户、该名称最长可达31个字符。
** *引擎ID*-选择引擎ID、此
ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择*本地*。如果您使用的是非标准配置、请选择*自定义*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
** *身份验证凭据*-
选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
** *隐私凭据*-
选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。

[[ID7d8b7827c2a263841d109c194efc8ed2]]
= 在 SANtricity System Manager 中删除 SNMPv2c 陷阱的社区
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以删除SNMPv2c陷阱的社区名称。

.步骤

. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目的地和社区名称显示在 *SNMP 警报* 页面上。

. 选择*配置社区*。
+
此时将打开配置社区对话框。

. 选择要删除的社区名称、然后单击最右侧的*删除*(X)图标。
+
如果陷阱目标与此社区名称关联、则确认删除社区对话框将显示受影响的陷阱目标地址。

. 确认此操作、然后单击*删除*。

.结果
社区名称及其关联的陷阱目标将从 SNMP 警报页面中删除。

[[ID452bda3d08bd032b868c5d902e828f9c]]
= 在 SANtricity System Manager 中删除 SNMPv3 陷阱的用户
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以删除SNMPv3陷阱的用户。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目标和用户名显示在 SNMP 警报页面上。

. 选择*配置用户*。
+
此时将打开配置SNMPv3用户对话框。

. 选择要删除的用户名、然后单击*删除*。
. 确认此操作、然后单击*删除*。

.结果
用户名及其关联的陷阱目标将从 SNMP 警报页面中删除。

[[ID68d82d892caa626af30e5aa21e792b3e]]
= 在 SANtricity System Manager 中删除陷阱目标
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以删除陷阱目标地址、以便存储阵列的事件监控器不再向该地址发送SNMP陷阱。

.步骤
. 从左侧面板中，选择菜单：Alerts[SNMP alerts]。
+
陷阱目标地址将显示在表中。

. 选择陷阱目标、然后单击页面右上角的*删除*。
. 确认此操作、然后单击*删除*。
+
目标地址不再显示在 SNMP 警报页面上。

.结果
已删除的陷阱目标不再从存储阵列的事件监控器接收SNMP陷阱。

:leveloffset: -1

= 管理系统日志警报

:leveloffset: +1

[[IDc7d7f564539514f150fe9ab12045aa45]]
= 在 SANtricity System Manager 中配置 syslog 服务器以接收警报
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置系统日志警报、必须输入系统日志服务器地址和UDP端口。最多允许五个系统日志服务器。

.开始之前
* 系统日志服务器地址必须可用。此地址可以是完全限定域名、IPv4地址或IPv6地址。
* 系统日志服务器的UDP端口号必须可用。此端口通常为514。

.关于此任务
此任务介绍如何输入系统日志服务器的地址和端口、然后测试您输入的地址。

.步骤
. 从左侧面板中，选择菜单：Alerts[Syslog alerts]。
+
如果尚未定义 syslog 服务器，页面将显示"添加 syslog 服务器"。

. 单击*添加系统日志服务器*。
+
此时将打开添加系统日志服务器对话框。

. 输入一个或多个系统日志服务器的信息(最多五个)、然后单击*添加*。
+
** *服务器地址*-输入完全限定域名、IPv4地址或IPv6地址。
** * UDP端口*-通常、系统日志的UDP端口为514。此表显示了已配置的系统日志服务器。

. 要向服务器地址发送测试警报、请选择*测试所有系统日志服务器*。

.结果
每当发生可警报的事件时、事件监控器都会向系统日志服务器发送警报。要进一步配置审核日志的系统日志设置、请参见 https://docs.netapp.com/us-en/e-series-santricity/sm-settings/configure-syslog-server-for-audit-logs.html["为审核日志配置系统日志服务器"]。

NOTE: 如果配置了多个系统日志服务器、则所有已配置的系统日志服务器都会收到审核日志。

[[IDe17c1e85afba1312cadd9ae59e339257]]
= 在 SANtricity System Manager 中编辑警报的系统日志服务器
:allow-uri-read:
:experimental:
:icons: font

:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以编辑用于接收系统日志警报的服务器地址。

.步骤
. 从左侧面板中，选择菜单：Alerts[Syslog alerts]。
. 从表中选择系统日志服务器地址、然后单击最右侧的*编辑*（铅笔）图标。
+
该行将变为可编辑字段。

. 编辑服务器地址和UDP端口号、然后单击*保存*（复选标记）图标。

.结果
更新后的服务器地址将显示在表中。

[[IDa50a028984f788f1e7baaa3c20e42fcc]]
= 在 SANtricity System Manager 中添加用于警报的系统日志服务器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
最多可以为系统日志警报添加五个服务器。

.开始之前
* 系统日志服务器地址必须可用。此地址可以是完全限定域名、IPv4地址或IPv6地址。
* 系统日志服务器的UDP端口号必须可用。此端口通常为514。

.步骤
. 从左侧面板中，选择菜单：Alerts[Syslog alerts]。
. 选择*添加系统日志服务器*。
+
此时将打开添加系统日志服务器对话框。

. 选择*添加另一个系统日志服务器*。
. 输入系统日志服务器的信息、然后单击*添加*。
+

** *系统日志服务器地址*-输入完全限定域名、IPv4地址或IPv6地址。
** * UDP端口*-通常、系统日志的UDP端口为514。

+

NOTE：您最多可以配置五个系统日志服务器。

.结果
系统日志服务器地址将显示在表中。

[[ID9c3f14be3fc460be777e3264a5851ef9]]
= 删除 SANtricity System Manager 中警报的系统日志服务器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以删除系统日志服务器、使其不再接收警报。

.步骤
. 从左侧面板中，选择菜单：Alerts[Syslog alerts]。
. 选择系统日志服务器地址、然后单击右上角的*删除*。
+
此时将打开确认删除系统日志服务器对话框。

. 确认此操作、然后单击*删除*。

.结果
删除的服务器不再从事件监控器接收警报。

:leveloffset: -1

[[ID10c12d68303ea059f135fa0b2e5a49cf]]
= SANtricity System Manager 的存储系统警报常见问题解答
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
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。

```
[[what-if-alerts-are-disabled]]
```
== 如果警报已禁用、该怎么办?

如果您希望管理员接收有关存储阵列中发生的重要事件的通知、则必须配置警报方法。

对于使用SANtricity System Manager管理的存储阵列、您可以从警报页面配置警报。可以通过电子邮件、SNMP陷阱或系统日志消息发送警报通知。此外、还可以通过初始设置向导配置电子邮件警报。

```
[[how-do-i-configure-snmp-or-syslog-alerts]]
```
== 如何配置SNMP或系统日志警报?

除了电子邮件警报之外、您还可以将警报配置为通过简单网络管理协议(Simple Network Management Protocol、SNMP)陷阱或系统日志消息发送。

要配置 SNMP 或 syslog 警报，请转到 menu:Alerts[]。

```
[[why-are-timestamps-inconsistent-between-the-array-and-alerts]]
```
== 阵列和警报之间的时间戳为何不一致?

存储阵列发送警报时、接收警报的目标服务器或主机的时区不正确。相反、存储阵列会使用本地时间(GMT)创建用于警报记录的时间戳。因此、您可能会看到存储阵列的时间戳与接收警报的服务器或主机之间不一致。

由于在发送警报时存储阵列的时区不正确、因此警报上的时间戳是与GMT相关的、其时区偏移为零。要计算适合您当地时区的时间戳、您应确定GMT的小时偏移量、然后在时间戳中添加或减去该值。

```
:leveloffset: -1
```

= 阵列设置

:leveloffset: +1

[[ID10c8f48a38e2b73a29dfb1c7317a6fee]]
= 了解 SANtricity System Manager 中的设置概述
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以为SANtricity系统管理器配置一些常规阵列设置和附加功能。

[[what-settings-can-i-configure]]
== 我可以配置哪些设置?

阵列设置包括：

* xref:{relative_path}cache-settings-and-performance.html["缓存设置和性能"]
* xref:{relative_path}automatic-load-balancing-overview.html["自动负载平衡"]
* xref:{relative_path}how-add-on-features-work.html["附加功能"]
* xref:{relative_path}overview-drive-security.html["驱动器安全性"]

[[related-tasks]]
== 相关任务

详细了解与系统设置相关的任务：

* xref:{relative_path}download-cli.html["下载命令行界面(CLI)"]
* xref:{relative_path}create-internal-security-key.html["创建内部安全密钥"]
* xref:{relative_path}create-external-security-key.html["创建外部安全密钥"]
* xref:{relative_path}../sm-hardware/configure-iscsi-ports-hardware.html["配置iSCSI端口"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-infiniband-ports-hardware.html["配置基于IB的NVMe端口"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-roce-ports-hardware.html["配置基于RoCE的NVMe端口"]

= 概念

:leveloffset: +1

[[ID4897a32fccb91c66a1e873a8d46ec246]]
= 了解 SANtricity 软件中的缓存设置和性能
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
缓存是控制器上临时易失性存储的一个区域、其访问速度比驱动器介质更快。

使用缓存时、整体I/O性能可按以下方式提高：

* 从主机请求读取的数据可能已位于先前操作的缓存中、因此无需访问驱动器。
* 写入数据最初会写入缓存、这样、应用程序就可以继续运行、而无需等待数据写入驱动器。

默认缓存设置可满足大多数环境的要求、但您可以根据需要进行更改。

[[storage-array-cache-settings]]
== 存储阵列缓存设置

对于存储阵列中的所有卷、您可以在系统页面中指定以下值：

* *Start demand cache flushing* —
缓存中触发缓存刷新（写入磁盘）的未写入数据的百分比。当缓存中未写入数据达到指定的启动百分比时，将触发刷新。默认情况下，当缓存达到 80% 时，控制器将开始刷新缓存。
* *缓存块大小
*—每个缓存块的最大大小、该块是一个用于缓存管理的组织单位。默认情况下、缓存块大小为8 KiB、但可以设置为4、8、16或32 KiB。理想情况下、缓存块大小应设置为应用程序的主要I/O大小。文件系统或数据库应用程序通常使用较小的大小、而较大的大小则适合需要大型数据传输或顺序I/O的应用程序

[[volume-cache-settings]]
== 卷缓存设置

对于存储阵列中的单个卷、您可以从卷页面(菜单：Storage[Volumes])中指定以下值：

* *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。
+
** *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。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。

* *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。
+
[CAUTION]
====
可能丢失数据-如果启用*不使用电池的写入缓存
*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。

====
+
** *无电池写入缓存
*—无电池写入缓存设置允许写入缓存继续运行、即使电池缺失、出现故障、已完全放电或未完全充电也是如此。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。
** *使用镜像写入缓存*-
如果写入一个控制器的缓存内存中的数据也写入另一个控制器的缓存中、则使用镜像进行写入缓存。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。

[[ID526cba5a82267e6ba4dd29bc6079bd93]]
= 了解 SANtricity 软件中的自动负载平衡
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
自动负载平衡可随着时间的推移对负载变化做出动态响应、并自动调整卷控制器所有权、以便在工作负载在控制器之间移动时更正任何负载不平衡问题、从而改进I/O资源管理。

系统会持续监控每个控制器的工作负载、并在主机上安装的多路径驱动程序的配合下、在必要时自动实现平衡。在控制器之间自动重新平衡工作负载时、存储管理员无需再承担手动调整卷控制器所有权以适应存储阵列上的负载变化的负担。

启用自动负载平衡后、它将执行以下功能：

* 自动监控和平衡控制器资源利用率。
* 根据需要自动调整卷控制器所有权、从而优化主机和存储阵列之间的I/O带宽。

[[enabling-and-disabling-automatic-load-balancing]]
== 启用和禁用自动负载平衡

默认情况下、所有存储阵列都会启用自动负载平衡。

您可能需要在存储阵列上禁用自动负载平衡、原因如下：

* 您不希望自动更改特定卷的控制器所有权以平衡工作负载。
*
您正在高度调整的环境中运行、在此环境中、负载分布会有针对性地进行设置、以便在控制器之间实现特定的分布。

[[host-types-that-support-the-automatic-load-balancing-feature]]
== 支持自动负载平衡功能的主机类型

即使在存储阵列级别启用了自动负载平衡、您为主机或主机集群选择的主机类型也会直接影响此功能的运行方式。

在控制器之间平衡存储阵列的工作负载时、自动负载平衡功能会尝试移动两个控制器均可访问且仅映射到能够支持自动负载平衡功能的主机或主机集群的卷。

此行为可防止主机因负载平衡过程而无法访问卷；但是、映射到不支持自动负载平衡的主机的卷会影响存储阵列平衡工作负载的能力。要使自动负载平衡平衡平衡工作负载、多路径驱动程序必须支持TPG、并且下表中必须包括主机类型。

[NOTE]

====
要将主机集群视为能够自动负载平衡、该组中的所有主机都必须能够支持自动负载平衡。

====
[cols="1a,1a"]
|===
| 支持自动负载平衡的主机类型 | 使用此多路径驱动程序

 a|
Windows或Windows集群模式
 a|
MPIO与NetApp E系列DSM

 a|
Linux DM-MP (内核3.10或更高版本)
 a|
DM-MP与`sCSI DH_ALUA`设备处理程序

 a|
VMware
 a|
采用`VMW_SATA_ALUA存储阵列类型`插件的原生 多路径插件(NMP)

|===
[NOTE]
====
除次要例外情况外、不支持自动负载平衡的主机类型继续正常运行、无论是否启用了此功能。一个例外情况是、如果系统发生故障转移、则当数据路径返回时、存储阵列会将未映射或未分配的卷移回所属控制器。不会移动映射或分配给非自动负载平衡主机的任何卷。

====
请参见 https://mysupport.netapp.com/matrix["互操作性表工具"^]
有关特定多路径驱动程序、操作系统级别和控制器驱动器托盘支持的兼容性信息。

[[verifying-os-compatibility-with-the-automatic-load-balancing-feature]]
== 验证操作系统与自动负载平衡功能的兼容性

在设置新系统(或迁移现有系统)之前、请验证操作系统与自动负载平衡功能的兼容性。

. 转至 https://mysupport.netapp.com/matrix["互操作性表工具"^] 以查找解决方案

并验证支持。
+
如果您的系统运行的是Red Hat Enterprise Linux 6或SUSE Linux Enterprise Server 11、请联系技术支持。

. 更新并配置`/etc/multipath.conf文件`。
. 确保适用的供应商和产品的`renet_attached _device_handler`和`detect_prio`均设置为`yes`、或者使用默认设置。

:leveloffset: -1

= 配置阵列设置

:leveloffset: +1

[[IDb41b90a4077a90e65d851f299255584f]]
= 在 SANtricity System Manager 中编辑存储阵列名称
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以更改SANtricity 系统管理器标题栏中显示的存储阵列名称。

.步骤
. 从左侧面板中，选择 *System*。
. 在*常规*下，单击*编辑存储阵列名称*。
+
此时将显示编辑存储阵列名称对话框。

. 在*名称*字段中输入新名称。
+
名称可以包含字母、数字以及特殊字符下划线(_)、短划线(-)和哈希符号(#)。名称不能包含空格。一个名称的最大长度可以为30个字符。此名称必须是唯一的。

. 单击 * 保存 * 。

.结果

新名称将显示在SANtricity 系统管理器的标题栏中。

[[ID70b16c2f996876e879b881b17a857085]]
= 在 SANtricity System Manager 中打开存储阵列定位器灯
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要查找存储阵列在机柜中的物理位置、您可以打开其定位器(LED)指示灯。

.步骤
. 从左侧面板中，选择 *System*。
. 在*常规*下，单击*打开存储阵列定位灯*。
+
此时将打开"打开定位器指示灯"对话框，相应存储阵列的定位器指示灯随即亮起。

. 物理定位存储阵列后，返回对话框并选择*关闭*。

.结果
定位器指示灯将熄灭、对话框将关闭。

[[IDe66e0d1e176c0b2066c2bc422776d9dc]]
= 在 SANtricity System Manager 中同步存储阵列时钟
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果未启用网络时间协议(NTP)、则可以手动设置控制器上的时钟、以便与管理客户端(用于运行访问SANtricity System Manager的浏览器的系统)同步。

.关于此任务
同步可确保事件日志中的事件时间戳与写入主机日志文件的时间戳匹配。在同步过程中、控制器仍保持可用和正常运行。

[NOTE]
====
如果在System Manager中启用了NTP、请勿使用此选项同步时钟。相反、NTP会使用SNTP（简单网络时间协议）自动将时钟与外部主机同步。

====
[NOTE]
====
同步后、您可能会注意到性能统计信息丢失或偏差、计划受到影响(ASUP、快照等)、日志数据中的时间戳发生偏差。使用NTP可避免此问题。

====
.步骤
. 从左侧面板中，选择 *System*。
. 在*常规*下，单击*同步存储阵列时钟*。
+
同步存储阵列时钟对话框打开。它显示控制器和用作管理客户端的计算机的当前日期和时间。

+
[NOTE]
====
对于单工存储阵列、仅显示一个控制器。

====
. 如果对话框中显示的时间不匹配、请单击*同步*。

.结果
同步成功后、事件日志和主机日志的事件时间戳相同。

[[IDd09045436a0602d9d8593ed5ff188cdc]]
= 在 SANtricity System Manager 中保存存储阵列配置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将存储阵列的配置信息保存在脚本文件中、以节省设置具有相同配置的其他存储阵列所需的时间。

.开始之前
存储阵列不得执行任何更改其逻辑配置设置的操作。这些操作的示例包括创建或删除卷、下载控制器固件、分配或修改热备用驱动器或向卷组添加容量(驱动器)。

.关于此任务
保存存储阵列配置会生成一个命令行界面(CLI)脚本、其中包含存储阵列设置、卷配置、主机配置或存储阵列的主机到卷分配。您可以使用此生成的命令行界面脚本将配置复制到具有完全相同硬件配置的另一个存储阵列。

但是、您不应使用此生成的命令行界面脚本进行灾难恢复。要执行系统还原、请使用手动创建的配置数据库备份文件、或者联系技术支持以从最新的AutoSupport数据中获取此数据。

此操作不会_保存以下设置：

* 电池的使用寿命
* 控制器的时间
* 非易失性静态随机存取存储器(NVSRAM)设置
* 任何高级功能
* 存储阵列密码
* 硬件组件的运行状态和状态
* 卷组的运行状态(最佳除外)和状态
* 复制服务、例如镜像和卷复制

[CAUTION]
====
应用程序错误的风险—如果存储阵列正在执行将更改任何逻辑配置设置的操作、请勿使用此选项。这些操作的示例包括创建或删除卷、下载控制器固件、分配或修改热备用驱动器或向卷组添加容量(驱动器)。

====
.步骤
. 从左侧面板中，选择 *System*。
. 选择*保存存储阵列配置*。
. 选择要保存的配置项：
+
** 存储阵列设置
** 卷配置
** 主机配置
** 主机到卷的分配（需要卷和主机配置）

+
[NOTE]
====
如果选择*主机到卷分配*项、则默认情况下也会选择*卷配置*项和*主机配置*项。如果不同时保存"卷配置"和"主机配置"、则无法保存"主机到卷分配"。

====
. 单击 * 保存 * 。
+

此文件将保存在浏览器的"Downloads"文件夹中、名为`storage-array-configuration.cfg`。

.完成后
要将已保存的存储阵列配置加载到另一个存储阵列、请使用带有`-f`选项的SANtricity命令行界面(SMcli)应用`.cfg`文件。

[NOTE]
====
此外、您还可以使用Unified Manager界面将存储阵列配置加载到其他存储阵列(选择菜单：管理[导入设置])。

====

[[ID667d5e86e0f07357a3a3323e3e817cf3]]
= 在 SANtricity System Manager 中清除存储阵列配置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果要从存储阵列中删除所有池、卷组、卷、主机定义和主机分配、请使用清除配置操作。

.开始之前
在清除存储阵列配置之前、请备份数据。

.关于此任务
有两个清晰的存储阵列配置选项：

* *卷
*—通常、您可以使用卷选项将测试存储阵列重新配置为生产存储阵列。例如、您可以配置要测试的存储阵列、然后在完成测试后、删除测试配置并为生产环境设置存储阵列。
* *存储阵列
*—通常、您可以使用存储阵列选项将存储阵列移动到其他部门或组。例如、您可能正在工程部门使用存储阵列、而工程部门现在正在获取一个新的存储阵列、因此您希望将当前存储阵列移动到要重新配置它的管理部门。
+
存储阵列选项会删除一些其他设置。

[cols="1a,1a,1a"]
|===
| | Volume | 存储阵列

a|
已清除ARVM
a|
X
a|
X

a|
删除池和卷组
a|
X
a|
X

a|
删除卷
a|
X
a|
X

a|
删除主机和主机集群
a|
X
a|
X

a|
删除主机分配
a|
X
a|
X

 a|
删除存储阵列名称
 a|
 a|
X

 a|
将存储阵列缓存设置重置为默认值
 a|
 a|
X

|===
[CAUTION]
====
数据丢失风险—此操作将删除存储阵列中的所有数据。（它不会执行安全擦除。）
此操作启动后、您将无法取消。只有在技术支持要求时、才执行此操作。

====
.步骤
. 从左侧面板中，选择 *System*。
. 在*常规*下，选择*清除存储阵列配置*。
. 在下拉列表中、选择*卷*或*存储阵列*。
. *可选：*如果要保存配置（而不是数据）、请使用对话框中的链接。
. 确认要执行此操作。

.结果
* 此时将删除当前配置、从而销毁存储阵列上的所有现有数据。
* 所有驱动器均已取消分配。
+

NOTE:
存储阵列将进入恢复模式。您必须先清除恢复模式，然后才能使用存储阵列。有关详细信息、请参见 https://docs.netapp.com/us-en/e-series-santricity/sm-support/clear-recovery-mode.html["清除恢复模式"^] 。

[[ID0a779f8e95447caf069efd8df7e4cdb8]]

= 在 SANtricity System Manager 中更改存储阵列缓存设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于存储阵列中的所有卷、您可以根据刷新和块大小调整缓存内存设置。

.关于此任务
缓存内存是控制器上的临时易失性存储区域、其访问速度比驱动器介质更快。要调整缓存性能、您可以调整以下设置：

[cols="25h,~"]
|===
| 缓存设置 | Description

a|
启动按需缓存刷新
a|
启动需求缓存刷新指定缓存中触发缓存刷新(写入磁盘)的未写入数据的百分比。默认情况下、当未写入的数据达到80%容量时、将开始缓存刷新。较高的百分比是主要执行写入操作的环境的理想选择、因此新的写入请求可以通过缓存进行处理、而无需转到磁盘。如果环境中的I/O不稳定(发生数据突发)、则设置越低越好、系统就会在数据突发之间频繁地刷新缓存。但是、如果开始百分比低于80%、则发生原因可能会降低性能。

a|
缓存块大小
a|
缓存块大小决定了每个缓存块的最大大小、该块是一个用于缓存管理的组织单位。默认情况下、块大小为32 KiB。系统允许缓存块大小为4、8、16或32 KiB。应用程序使用不同的块大小、这会影响存储性能。对于文件系统或数据库应用程序来说、较小的大小是一个不错的选择。较大的大小非常适合生成顺序I/O的应用程序、例如多媒体。

|===
.步骤
. 从左侧面板中，选择 *System*。
. 向下滚动到*其他设置*，然后单击*配置缓存设置*。
+
此时将打开"配置缓存设置"页面。

. 调整以下值：

+
** *启动按需缓存刷新*-选择一个适合您环境中使用的I/O的百分比。如果您选择的值低于80%、则可能会注意到性能下降。
** "**缓存块大小"-"*选择适合您的应用程序的大小"。

. 单击 * 保存 * 。

[[IDdca904f653a84005b5c5df882e7ccc7c]]
= 在 SANtricity System Manager 中设置自动负载平衡
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
自动负载平衡功能可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。默认情况下、此功能处于启用状态、但您可以从SANtricity系统管理器中将其禁用。

.关于此任务
启用自动负载平衡后、它将执行以下功能：

* 自动监控和平衡控制器资源利用率。
* 根据需要自动调整卷控制器所有权、从而优化主机和存储阵列之间的I/O带宽。

您可能需要在存储阵列上禁用自动负载平衡、原因如下：

* 您不希望自动更改特定卷的控制器所有权以平衡工作负载。
*
您正在高度调整的环境中运行、在此环境中、负载分布会有针对性地进行设置、以便在控制器之间实现特定的分布。

.步骤
. 从左侧面板中，选择 *System*。
. 向下滚动到*其他设置*，然后单击*配置自动负载平衡*。
+
此选项下方的文本指示此功能当前是启用还是禁用。

+
此时将打开配置自动负载平衡对话框。

. 选择或清除*启用自动负载平衡*。
. 单击 * 保存 * 。
+
通过选择此选项、您可以在已启用/已禁用之间切换此功能。

+
[NOTE]
====
如果将此功能从禁用更改为启用、则主机连接报告功能也会自动启用。

====

:leveloffset: -1

= 配置附加功能

:leveloffset: +1

[[IDc1f45f175eb7437eb7cba86912f09b10]]
= SANtricity System Manager 中的附加功能如何工作
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
加载项是SANtricity系统管理器标准配置中不包含的功能、可能需要密钥才能启用。附加功能可以是单个高级功能、也可以是捆绑的功能包。

以下步骤概述了如何启用高级功能或功能包：

. 获取以下信息：
+
** 机箱序列号和功能启用标识符、用于标识要安装的功能的存储阵列。这些项目可在System Manager中使用。
** 功能激活代码、购买此功能时可从支持站点获取。

.
请联系您的存储提供商或访问高级功能激活站点以获取功能密钥。提供机箱序列号、启用标识符和功能代

码以进行激活。
. 使用System Manager、使用功能密钥文件启用高级功能或功能包。

[[IDb83cf09585f1c71bffcfc5f7b2e6b890]]
= 了解 SANtricity 软件中的附加功能术语
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解附加功能术语如何应用于存储阵列。

[cols="25h,~"]
|===
| 期限 | Description

a|
功能启用标识符
a|
功能启用标识符是用于标识特定存储阵列的唯一字符串。此标识符可确保在您获得高级功能时、它仅与该特定存储阵列相关联。此字符串将显示在System页面的Add-Ons下。

a|
功能密钥文件
a|
功能密钥文件是指您收到的用于解锁和启用高级功能或功能包的文件。

a|
功能包
a|
功能包是更改存储阵列属性(例如、将协议从光纤通道更改为iSCSI)的捆绑包。要启用功能包、需要使用特殊密钥。

a|
高级功能

 a|
高级功能是一个额外的选项、需要使用密钥才能启用它。System Manager的标准配置不包括此功能。

|===

[[ID6b76fd2885005c67a5d7bdff84010537]]
= 在 SANtricity System Manager 中获取功能密钥文件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要在存储阵列上启用高级功能或功能包、必须先获取功能密钥文件。一个密钥仅与一个存储阵列相关联。

.关于此任务
此任务介绍如何收集功能所需的信息、然后发送功能密钥文件请求。所需信息包括：

* 机箱序列号
* 功能启用标识符
* 功能激活代码

.步骤
. 在 System Manager 中，找到并记录机箱序列号。从左侧面板转到 menu:Support[Support center]，然后向下滚动到 *View top storage array properties* 以查看机箱序列号。
. 在 System Manager 中，找到功能启用标识符。在左侧面板中，选择 *系统*，然后向下滚动到 *附加组件*。查找 *功能启用标识符*。记录功能启用标识符的编号。
. 找到并记录用于激活功能的代码。对于功能包、此代码将在执行转换的相应说明中提供。
+
对于高级功能、您可以从支持站点访问激活代码、如下所示：

+
.. 登录到 https://mysupport.netapp.com/site/global/dashboard["NetApp 支持"^]。
.. 请访问您的产品对应的*软件许可证*。
.. 输入存储阵列机箱的序列号、然后单击*执行*。
.. 在*许可证密钥*列中查找功能激活代码。
.. 记录所需功能的功能激活代码。

.
通过向存储供应商发送包含以下信息的电子邮件或文本文档来请求功能密钥文件：机箱序列号、启用标识符和功能激活代码。

+
您也可以转到 http://partnerspfk.netapp.com["NetApp
许可证激活：存储阵列高级功能激活"^] 并输入所需信息以获取功能或功能包。
（此站点上的说明适用于高级功能、而不适用于功能包。）

.完成后
如果您有功能密钥文件、则可以启用高级功能或功能包。

[[IDe3f2966bf66170167501e9702adfdb44]]
= 在 SANtricity System Manager 中启用高级功能
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
高级功能是一个额外的选项、需要启用密钥。

.开始之前
* 您已获取功能密钥。如有必要、请联系技术支持以获取密钥。
* 您已在管理客户端(具有用于访问System Manager的浏览器的系统)上加载密钥文件。

.关于此任务
此任务介绍如何使用System Manager启用高级功能。

[NOTE]
====
如果要禁用高级功能、必须使用Disable Storage Array feature命令 (`disable storageArray) (featurePack | feature=featureAttributeList`)。

====
.步骤
. 从左侧面板中，选择 *System*。
. 在*附加组件*下，选择*启用高级功能*。
+
此时将打开启用高级功能对话框。

. 单击*浏览*、然后选择密钥文件。
+
此时将在对话框中显示文件名。

. 单击 * 启用 * 。

[[IDdaa680ccd9b004b2e08b45e91242d432]]
= 在 SANtricity System Manager 中启用功能包
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
功能包是更改存储阵列属性(例如、将协议从光纤通道更改为iSCSI)的捆绑包。要启用功能包、需要使用特殊密钥。

.开始之前
*
您已按照说明转换和准备新存储阵列属性的相应说明进行操作。有关主机协议转换的说明、请参见适用于您的控制器型号的硬件维护指南。
* 存储阵列处于脱机状态、因此没有主机或应用程序正在访问它。
* 备份所有数据。
* 您已获取功能包文件。
+
功能包文件将加载到管理客户端(具有用于访问System Manager的浏览器的系统)上。

[NOTE]
====
您必须计划停机维护时段、并停止主机和控制器之间的所有I/O操作。此外、请注意、在成功完成转换之前、您无法访问存储阵列上的数据。

====
.关于此任务
此任务介绍如何使用System Manager启用功能包。完成后、必须重新启动存储阵列。

.步骤
. 从左侧面板中，选择 *System*。
. 在*附加组件*下，选择*更改功能包*。
. 单击*浏览*、然后选择密钥文件。
+
此时将在对话框中显示文件名。

. 在字段中键入 `CHANGE`。
. 单击 * 更改 * 。
+
功能包迁移将开始、控制器将重新启动。系统将删除未写入的缓存数据、从而确保不会发生I/O活动。两个控制器都会自动重新启动、以使新功能包生效。重新启动完成后，存储阵列将恢复为响应状态。

:leveloffset: -1

[[IDf643c6901a04147d6934895d435e1cd1]]
= 下载 SANtricity 命令行界面 (CLI)
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在SANtricity系统管理器中、您可以下载命令行界面(CLI)软件包。

CLI提供了一种基于文本的方法来配置和监控存储阵列。它通过https进行通信、并使用外部安装的管理软件包中提供的CLI语法。下载CLI不需要任何密钥。

.开始之前
要运行命令行界面命令的管理系统必须具有Java Runtime Environment (JRE) 8及更高版本。

.步骤
. 从左侧面板中，选择 *System*。
. 在*附加组件*下，选择*下载命令行界面*。
+
ZIP包将下载到浏览器。

. 将ZIP文件保存到要对存储阵列运行CLI命令的管理系统、然后提取该文件。
+
现在、您可以从操作系统提示符运行命令行界面命令、例如DOS C：提示符。可从System Manager用户界面右上角的帮助菜单中获取CLI命令参考。

[[ID846b76f54fb3289a65a6dfd0c1fe4608]]

= SANtricity System Manager 的存储阵列设置常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[what-is-automatic-load-balancing]]
== 什么是自动负载平衡?

自动负载平衡功能可实现自动I/O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。

自动负载平衡功能可以随着时间的推移对负载变化做出动态响应、并自动调整卷控制器所有权、以便在工作负载在控制器之间移动时更正任何负载不平衡问题、从而改进了I/O资源管理。

系统会持续监控每个控制器的工作负载、并在主机上安装的多路径驱动程序的配合下、在必要时自动实现平衡。在控制器之间自动重新平衡工作负载时、存储管理员无需再承担手动调整卷控制器所有权以适应存储阵列上的负载变化的负担。

启用自动负载平衡后、它将执行以下功能：

* 自动监控和平衡控制器资源利用率。
* 根据需要自动调整卷控制器所有权、从而优化主机和存储阵列之间的I/O带宽。

[NOTE]
====
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。

====

[[what-is-controller-cache]]
== 什么是控制器缓存?

控制器缓存是一种物理内存空间、可简化两种类型的I/O （输入/输出）操作：控制器和主机之间以及控制器和磁盘之间。

对于读写数据传输、主机和控制器通过高速连接进行通信。但是、从控制器后端到磁盘的通信速度较慢、因为磁盘是相对较慢的设备。

当控制器缓存接收数据时、控制器向主机应用程序确认它现在保存数据。这样、主机应用程序就无需等待I/O写入磁盘。相反、应用程序可以继续运行。服务器应用程序也可以轻松访问缓存的数据、从而无需额外的磁盘读取即可访问数据。

控制器缓存会通过多种方式影响存储阵列的整体性能：

* 缓存可用作缓冲区、因此无需同步主机和磁盘数据传输。
* 用于从主机执行读取或写入操作的数据可能位于先前操作的缓存中、因此无需访问磁盘。
* 如果使用了写入缓存、则主机可以在将先前写入操作中的数据写入磁盘之前发送后续写入命令。
*

如果启用了缓存预取、则会优化顺序读取访问。缓存预取使读取操作更有可能在缓存中找到其数据、而不是从磁盘读取数据。

[CAUTION]
====
可能丢失数据-如果启用*不使用电池的写入缓存
*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。

====

[[what-is-cache-flushing]]
== 什么是缓存刷新?

当缓存中未写入的数据量达到某个级别时、控制器会定期将缓存的数据写入驱动器。此写入过程称为"刷新"。

控制器使用两种算法来刷新缓存：基于需求和基于年龄。控制器使用基于需求的算法、直到缓存的数据量降至缓存刷新阈值以下。默认情况下、当80%的缓存正在使用时、将开始刷新。

在System Manager中、您可以设置"开始`S请求缓存刷新`"阈值、以便最适合您环境中使用的I/O类型。在以写入操作为主的环境中、您应将"开始需求缓存刷新`S`"百分比设置为高、以增加缓存处理任何新写入请求而无需转到磁盘的可能性。高百分比设置会限制缓存刷新的数量、以使更多数据保留在缓存中、从而增加缓存命中的几率。

在I/O不稳定(发生数据突发)的环境中、您可以使用低缓存刷新、以便系统在数据突发之间频繁地刷新缓存。在处理各种负载的多样化I/O环境中、或者在负载类型未知时、将阈值设置为50%、以作为一个良好的中间地带。请注意、如果您选择的起始百分比低于80%、则性能可能会降低、因为主机读取所需的数据可能不可用。选择较低的百分比还会增加保持缓存级别所需的磁盘写入次数、从而增加系统开销。

基于期限的算法指定写入数据在符合向磁盘转储的条件之前可以保留在缓存中的时间段。在达到缓存刷新阈值之前、控制器会使用基于期限的算法。默认值为10秒、但此时间段仅在非活动期间计算在内。您不能在System Manager中修改刷新计时、而是必须在命令行界面(CLI)中使用*设置存储阵列*命令。

[CAUTION]
====
可能丢失数据-如果启用*不使用电池的写入缓存
*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。

====

[[what-is-cache-block-size]]
== 什么是缓存块大小?

存储阵列的控制器将其缓存组织为"块"、这些块是一个内存块、大小可以为8、16、32 KiB。存储系统上的所有卷共享相同的缓存空间；因此、这些卷只能具有一个缓存块大小。

应用程序使用不同的块大小、这可能会影响存储性能。默认情况下、System Manager中的块大小为32 KiB、但您可以将该值设置为8、16、32 KiB。对于文件系统或数据库应用程序来说、较小的大小是一个不错的选择。对于需要大型数据传输、顺序I/O或高带宽(如多媒体)的应用程序来说、较大的大小是一个不错的选择。

[[when-should-i-synchronize-storage-array-clocks]]
== 何时应同步存储阵列时钟?

如果您发现SANtricity系统管理器中显示的时间戳与管理客户端(通过浏览器访问SANtricity系统管理器的计算机)中显示的时间戳不一致、则应手动同步存储阵列中的控制器时钟。只有在SANtricity系统管理器中未启用网络时间协议(Network Time Protocol、NTP)时、才需要执行此任务。

[NOTE]
====
强烈建议您使用NTP服务器、而不是手动同步时钟。NTP会使用SNTP (简单网络时间协议)自动将时钟与外部服务器同步。

====
您可以从同步存储阵列时钟对话框中检查同步状态、该对话框可从系统页面访问。如果对话框中显示的时间不匹配、请运行同步。您可以定期查看此对话框、此对话框指示控制器时钟显示的时间是否已偏离并不再同步。

:leveloffset: -1

= 驱动器安全性

:leveloffset: +1

[[IDdb6128f7f0a55731e7a3e5465d8b0f1e]]
= 了解 SANtricity System Manager 中的驱动器安全性
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以从安全密钥管理页面配置驱动器安全性和密钥管理。

[[what-is-drive-security]]
== 什么是驱动器安全性?

_Drive Security_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。从阵列中物理删除FDE或FIPS驱动器后、这些驱动器将无法运行、除非将其安装在另一个阵列中、此时、这些驱动器将处于安全锁定状态、直到提供正确的安全密钥为止。安全密钥_是指此类驱动器与存储阵列中的控制器之间共享的字符串。

了解更多信息。

* xref:{relative_path}how-the-drive-security-feature-works.html["驱动器安全功能的工作原理"]
* xref:{relative_path}how-security-key-management-works.html["安全密钥管理的工作原理"]
* xref:{relative_path}drive-security-terminology.html["驱动器安全术语"]

[[how-do-i-configure-key-management]]
== 如何配置密钥管理?

要实现驱动器安全，必须在阵列中安装 FDE 驱动器或 FIPS 驱动器。要配置这些驱动器的密钥管理，请转到 menu:System[Security key management]，您可以在其中从控制器的永久内存创建内部密钥，也可以从密钥管理服务器创建外部密钥。最后，通过在卷设置中选择"secure-capable"，为池和卷组启用驱动器安全。

了解更多信息。

```
* xref:{relative_path}create-internal-security-key.html["创建内部安全密钥"]
* xref:{relative_path}create-external-security-key.html["创建外部安全密钥"]
* xref:{relative_path}../sm-storage/create-pool-manually.html["手动创建池"]
* xref:{relative_path}../sm-storage/create-volume-group.html["创建卷组"]
```

```
[[how-do-i-unlock-drives]]
== 如何解锁驱动器?
```

如果您配置了密钥管理、然后将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将安全密钥重新分配给新存储阵列、才能访问驱动器上的加密数据。

了解更多信息。

```
* xref:{relative_path}unlock-drives-using-an-internal-security-
key.html["使用内部密钥管理时解锁驱动器"]
* xref:{relative_path}unlock-drives-using-an-external-security-
key.html["使用外部密钥管理时解锁驱动器"]
```

```
[[related-information]]
== 相关信息
```

详细了解与密钥管理相关的任务:

```
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-a-
key-management-server.html["使用CA签名的证书通过密钥管理服务器进行身份验证"]
* xref:{relative_path}back-up-security-key.html["备份安全密钥"]
```

```
= 概念

:leveloffset: +1

[[IDedab2a9907bb86e46283160778804 76b]]
= SANtricity System Manager 中的驱动器安全功能如何工作
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
```

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS ）驱动器提供额外的安全层。

如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。

[[how-to-implement-drive-security]]
== 如何实施驱动器安全性

要实施驱动器安全性、请执行以下步骤。

. 为存储阵列配备支持安全保护的驱动器、可以是FDE驱动器、也可以是FIPS驱动器。(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。)
. 创建一个安全密钥、该密钥是一个字符串、由控制器和驱动器共享、用于进行读/写访问。您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。对于外部密钥管理、必须使用密钥管理服务器建立身份验证。
. 为池和卷组启用驱动器安全性：
+
** 创建池或卷组(在候选项表的*安全功能*列中查找*是*)。
** 创建新卷时、请选择池或卷组(在Pool and volume group candidates表中、查找*安全功能*旁边的*是*)。

[[how-drive-security-works-at-the-drive-level]]
== 驱动器安全在驱动器级别的工作原理

支持安全的驱动器(FDE或FIPS)可在写入期间对数据进行加密、并在读取期间对数据进行解密。此加密和解密不会影响性能或用户工作流。每个驱动器都有自己唯一的加密密钥、永远不能从该驱动器传输该密钥。

驱动器安全功能可通过支持安全功能的驱动器提供额外的保护层。如果为驱动器安全选择了这些驱动器上的卷组或池、则这些驱动器会先查找安全密钥、然后再允许访问数据。您可以随时为池和卷组启用驱动器安全性、而不会影响驱动器上的现有数据。但是、如果不擦除驱动器上的所有数据、则无法禁用驱动器安全性。

[[how-drive-security-works-at-the-storage-array-level]]
== 驱动器安全性在存储阵列级别的工作原理

使用驱动器安全功能、您可以创建一个安全密钥、该安全密钥可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。无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。

如果从存储阵列中删除启用了安全保护的驱动器并将其重新安装在其他存储阵列中、则该驱动器将处于安全锁定状态。重新定位的驱动器会先查找安全密钥、然后再使数据可再次访问。要解锁数据、请应用源存储阵列中的安全密钥。成功解锁过程后、重新定位的驱动器将使用已存储在目标存储阵列中的安全密钥、并且不再需要导入的安全密钥文件。

[NOTE]
====
对于内部密钥管理、实际安全密钥存储在控制器上不可访问的位置。它不是以人为可读的格式提供的、也不是用户可访问的格式。

====

[[how-drive-security-works-at-the-volume-level]]
== 驱动器安全在卷级别的工作原理

从支持安全的驱动器创建池或卷组时、您还可以为这些池或卷组启用驱动器安全性。"驱动器安全性"选项可确保驱动器以及关联的卷组和池的安全-_enabled_.

在创建启用了安全保护的卷组和池之前、请牢记以下准则：

* 卷组和池必须全部由具有安全功能的驱动器组成。（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。）
* 卷组和池必须处于最佳状态。

[[IDe794cc66a3258b3cc04f48f287e1c2b4]]
= SANtricity System Manager 中的安全密钥管理工作原理
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在实施驱动器安全功能时、启用了安全保护的驱动器(FIPS或FDE)需要一个安全密钥才能进行数据访问。安全密钥是指这些类型的驱动器与存储阵列中的控制器之间共享的字符串。

无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。如果从存储阵列中删除启用了安全保护的驱动器、则该驱动器的数据将被锁定。在将驱动器重新安装到其他存储阵列中时、它会先查找安全密钥、然后再重新访问数据。要解锁数据、必须应用原始安全密钥。

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。

[[internal-key-management]]
== 内部密钥管理

在控制器永久性内存的不可访问位置维护内部密钥并"`hidden`"。要实施内部密钥管理、请执行以下步骤：

. 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。
.
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。
.
创建内部安全密钥，其中涉及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，存储在控制器和与密钥关联的所有驱动器上。密码短语用于加密安全密钥以进行备份。要创建内部密钥，请转到菜单：系统[创建内部安全密钥]。

安全密钥存储在控制器上的一个隐藏的不可访问位置。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。

[[external-key-management]]
== 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进行维护。要实施外部密钥管理、请执行以下步骤：

. 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。
.
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。
.
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。
+
.. 首先，完成并下载客户端证书签名请求 (CSR)。转到 menu:Certificates[Key management certificates]，然后选择 *Complete CSR*。
.. 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CSR文件从密钥管理服务器创建和下载客户端证书。)
.. 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。
.. 或者、您也可以使用私有密钥对和公共密钥对在外部生成证书签名请求。

. 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。
. 创建外部密钥，其中涉及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，您还会加载证书文件。要创建外部密钥，请转到菜单：系统[创建外部安全密钥]。

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。

[[ID24cac35dd58a6954d5f4c71bf99c2517]]
= 了解 SANtricity 软件中的驱动器安全术语
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解驱动器安全术语如何应用于存储阵列。

[cols="25h,~"]
|===
| 期限 | Description

a|
驱动器安全功能
a|

驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS ）驱动器提供额外的安全层。如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。

a|
FDE驱动器
a|
全磁盘加密(Full Disk Encryption、FDE)驱动器在硬件级别对磁盘驱动器执行加密。硬盘驱动器包含一个ASIC芯片、用于在写入期间对数据进行加密、然后在读取期间对数据进行解密。

a|
FIPS驱动器
a|
FIPS驱动器使用联邦信息处理标准(FIPS) 140-2级别2。它们本质上是FDE驱动器、符合美国政府标准、可确保强大的加密算法和方法。FIPS驱动器的安全标准高于FDE驱动器。

a|
管理客户端
a|
一种本地系统(计算机、平板电脑等)、其中包括用于访问System Manager的浏览器。

a|
密码短语
a|
密码短语用于对安全密钥进行加密、以用于备份。在因驱动器迁移或机头交换而导入备份的安全密钥时、必须提供用于加密安全密钥的相同密码短语。密码短语可以包含8到32个字符。

[NOTE]
====
驱动器安全密码短语与存储阵列的管理员密码无关。

====

a|

支持安全的驱动器

a|

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、这些驱动器可在写入期间对数据进行加密、并在读取期间对数据进行解密。这些驱动器被视为安全驱动器-_capable"、因为可以使用驱动器安全功能提高安全性。如果为这些驱动器使用的卷组和池启用了驱动器安全功能、则这些驱动器将变为secure—_enabled_.

NOTE：不支持在同一存储阵列中混合使用 FDE 和 FIPS 驱动器。系统中所有具有安全功能的驱动器必须具有相同的类型。

a|

已启用安全保护的驱动器

a|

启用了安全保护的驱动器与驱动器安全功能结合使用。启用驱动器安全功能后、如果将驱动器安全应用于安全-_capable"驱动器上的池或卷组、则这些驱动器将变为安全_-enabled__。只能通过配置了正确安全密钥的控制器进行读写访问。这种增强的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。

a|

安全密钥

a|

安全密钥是指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的字符串。无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。如果从存储阵列中删除启用了安全保护的驱动器、则该驱动器的数据将被锁定。在将驱动器重新安装到其他存储阵列中时、它会先查找安全密钥、然后再重新访问数据。要解锁数据、必须应用原始安全密钥。您可以使用以下方法之一创建和管理安全密钥：

* 内部密钥管理—在控制器的永久性内存上创建和维护安全密钥。
* 外部密钥管理—在外部密钥管理服务器上创建和维护安全密钥。

a|

安全密钥标识符

a|

安全密钥标识符是在创建密钥期间与安全密钥关联的字符串。标识符存储在控制器以及与安全密钥关联的所有驱动器上。

|===

:leveloffset: -1

= 配置安全密钥

:leveloffset: +1

[[ID04c58792113eb3e75d604f15696e7f37]]
= 在 SANtricity System Manager 中创建内部安全密钥
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要使用驱动器安全功能、您可以创建一个内部安全密钥、该密钥由存储阵列中的控制器和支持安全功能的驱动器共享。内部密钥会保留在控制器的永久性内存上。

.开始之前
* 存储阵列中必须安装支持安全功能的驱动器。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。
*
必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。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。

[NOTE]
====
如果存储阵列中同时安装了FDE和FIPS驱动器、则它们将共享同一个安全密钥。

====
.关于此任务
在此任务中、您可以定义要与内部安全密钥关联的标识符和密码短语。

[NOTE]
====
驱动器安全密码短语与存储阵列的管理员密码无关。

====
.步骤

. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*创建内部密钥*。
+
如果尚未生成安全密钥、则会打开创建安全密钥对话框。

. 在以下字段中输入信息：
+
** *定义安全密钥标识符*-您可以接受默认值
(存储阵列名称和时间戳、此名称和时间戳由控制器固件生成)、也可以输入您自己的值。最多可以输入189个字母数字字符、不带空格、标点符号或符号。
+
[NOTE]
====
系统会自动生成附加到您输入的字符串两端的其他字符。生成的字符可确保标识符是唯一的。

====
** *定义密码短语/重新输入密码短语*-输入并确认密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
+
*** 大写字母(一个或多个)。请注意、密码短语区分大小写。
*** 一个数字(一个或多个)。
*** 非字母数字字符、例如！、*、@(一个或多个)。

+
[CAUTION]
====
请务必记录您的条目以供日后使用。如果您需要从存储阵列移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

====
. 单击 * 创建 * 。
+
安全密钥存储在控制器上的不可访问位置。除了实际密钥之外、还会从浏览器下载一个加密密钥文件。

+
[NOTE]
====
下载文件的路径可能取决于浏览器的默认下载位置。

====
. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

.结果

现在、您可以创建启用了安全保护的卷组或池、也可以在现有卷组和池上启用安全性。

[NOTE]
====
每当关闭驱动器电源然后再次打开时、所有启用了安全保护的驱动器都会更改为安全锁定状态。在这种状态下、只有在驱动器初始化期间控制器应用正确的安全密钥后、才能访问数据。如果有人以物理方式删除已锁定的驱动器并将其安装到其他系统中、则安全锁定状态将阻止对其数据进行未经授权的访问。

====
.完成后
您应验证此安全密钥、以确保此密钥文件未损坏。

[[ID592d9b8938b0ee1193dc52a063f8c36b]]
= 在 SANtricity System Manager 中创建外部安全密钥
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要对密钥管理服务器使用驱动器安全功能、必须创建一个外部密钥、该密钥由密钥管理服务器和存储阵列中支持安全功能的驱动器共享。

.开始之前
* 阵列中必须安装支持安全功能的驱动器。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。
+
[NOTE]
====
如果存储阵列中同时安装了FDE和FIPS驱动器、则它们将共享同一个安全密钥。

====
*
必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。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。
* 您已为存储阵列的控制器创建一个签名客户端证书文件、并已将该文件复制到要访问System Manager的主机。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。
* 您必须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。
+

[NOTE]
====
有关服务器证书的详细信息、请参见密钥管理服务器的文档。

====

.关于此任务
在此任务中、您可以定义密钥管理服务器的IP地址及其使用的端口号、然后加载用于外部密钥管理的证书。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*创建外部密钥*。
+
[NOTE]
====
如果当前已配置内部密钥管理、则会打开一个对话框、要求您确认是否要切换到外部密钥管理。

====
+
此时将打开创建外部安全密钥对话框。

. 在*连接到密钥服务器*下、在以下字段中输入信息。
+
** *密钥管理服务器地址*—输入用于密钥管理的服务器的完全限定域名或IP地址(IPv4或IPv6)。
** *密钥管理端口号*-输入用于KMIP通信的端口号。用于密钥管理服务器通信的最常见端口号是5696。
+
*可选：*如果要配置备份密钥服务器、请单击*添加密钥服务器*、然后输入该服务器的信息。如果无法访问主密钥服务器、则会使用第二个密钥服务器。确保每个密钥服务器都可以访问同一个密钥数据库；否则、阵列将发布错误、并且无法使用备份服务器。

+

NOTE:
一次仅使用一个密钥服务器。如果存储阵列无法访问主密钥服务器、则该阵列将联系备份密钥服务器。请注意、必须在两个服务器之间保持奇偶校验；否则可能会导致错误。

** *选择客户端证书*-单击第一个*浏览*按钮以选择存储阵列控制器的证书文件。
** *选择专用密钥文件* -- 如果需要，单击第二个 *浏览*
按钮为存储阵列的控制器选择专用密钥文件。
** *选择密钥管理服务器的服务器证书*--单击第三个*浏览
*按钮选择密钥管理服务器的证书文件。您可以为密钥管理服务器选择根证书、中间证书或服务器证书。

. 单击 * 下一步 * 。
. 在*创建/备份密钥*下、您可以出于安全目的创建备份密钥。

+
** （建议）要创建备份密钥、请保持选中状态、然后输入并确认密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
+
*** 大写字母（一个或多个）。请注意、密码短语区分大小写。
*** 一个数字（一个或多个）。
*** 非字母数字字符、例如！、*、@（一个或多个）。

+
[CAUTION]
====
请务必记录您的条目以供日后使用。如果您需要从存储阵列中移动启用了安全保护的驱动器、则必须知道解锁驱动器数据的密码短语。

====
+
** 如果不想创建备份密钥、请取消选中此复选框。
+
[CAUTION]
====
请注意、如果您无法访问外部密钥服务器、并且没有备份密钥、则在将驱动器迁移到另一存储阵列时、您将无法访问这些驱动器上的数据。此选项是在System Manager中创建备份密钥的唯一方法。

====

. 单击 * 完成 * 。
+
系统将使用您输入的凭据连接到密钥管理服务器。然后、安全密钥的副本将存储在本地系统上。

+
[NOTE]
====
下载文件的路径可能取决于浏览器的默认下载位置。

====
. 记下您的密码短语以及下载的密钥文件的位置、然后单击*关闭*。
+
此页面将显示以下消息、其中包含用于外部密钥管理的其他链接：

+
`当前密钥管理方法：外部`

. 选择*测试通信*以测试存储阵列与密钥管理服务器之间的连接。

+
测试结果将显示在对话框中。

.结果
启用外部密钥管理后、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。

[NOTE]
====
每当关闭驱动器电源然后再次打开时、所有启用了安全保护的驱动器都会更改为安全锁定状态。在这种状态下、只有在驱动器初始化期间控制器应用正确的安全密钥后、才能访问数据。如果有人以物理方式删除已锁定的驱动器并将其安装到其他系统中、则安全锁定状态将阻止对其数据进行未经授权的访问。

====
.完成后
您应验证此安全密钥、以确保此密钥文件未损坏。

:leveloffset: -1

= 管理安全密钥

:leveloffset: +1

[[IDe1533d4f29c4af8785970f638b5dae81]]
= 在 SANtricity System Manager 中更改安全密钥
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以随时将安全密钥替换为新密钥。如果您的公司存在潜在的安全违规行为、并且希望确保未经授权的人员无法访问驱动器数据、您可能需要更改安全密钥。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*更改密钥*。
+
此时将打开更改安全密钥对话框。

. 在以下字段中输入信息。
+
** *定义安全密钥标识符*-(仅适用于内部安全密钥。) 接受默认值
(由控制器固件生成的存储阵列名称和时间戳)或输入您自己的值。最多可以输入189个字母数字字符、不带空格、标点符号或符号。
+
[NOTE]
====
系统会自动生成其他字符、并将其附加到您输入的字符串的两端。生成的字符有助于确保标识符是唯一的。

====
** *定义密码短语/重新输入密码短语*—在每个字段中输入您的密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符:
+
*** 大写字母(一个或多个)。请注意、密码短语区分大小写。
*** 一个数字(一个或多个)。
*** 非字母数字字符、例如!、*、@(一个或多个)。

. 对于外部安全密钥、如果要在创建新安全密钥时删除旧安全密钥、请选中对话框底部的"删除当前安全密钥..."复选框。
+
[CAUTION]
====
请务必记录您的条目以供日后使用-
如果您需要从存储阵列中移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

====
. 单击 * 更改 * 。
+
新的安全密钥会覆盖上一个密钥、而上一个密钥不再有效。

+
[NOTE]
====
下载文件的路径可能取决于浏览器的默认下载位置。

====
. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

.完成后
您应验证此安全密钥、以确保此密钥文件未损坏。

[[ID96efdc8943d64e2b48a70fcb76922f35]]
= 在 SANtricity System Manager 中从外部密钥管理切换到内部密钥管理
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将驱动器安全管理方法从外部密钥服务器更改为存储阵列使用的内部方法。然后、以前为外部密钥管理定义的安全密钥将用于内部密钥管理。

.关于此任务
在此任务中、您可以禁用外部密钥管理并将新的备份副本下载到本地主机。现有密钥仍用于驱动器安全、但将在存储阵列中进行内部管理。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*禁用外部密钥管理*。
+
此时将打开禁用外部密钥管理对话框。

. 在*定义密码短语/重新输入密码短语*中、输入并确认用于备份密钥的密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
+
** 大写字母(一个或多个)。请注意、密码短语区分大小写。
** 一个数字(一个或多个)。
** 非字母数字字符、例如！、*、@(一个或多个)。

+
[CAUTION]
====
请务必记录您的条目以供日后使用_。如果您需要从存储阵列移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

====
. 单击 * 禁用 * 。
+
备份密钥将下载到本地主机。

. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

.结果
现在、驱动器安全性可通过存储阵列在内部进行管理。

.完成后
您应验证此安全密钥、以确保此密钥文件未损坏。

[[IDcd90baa38b9b0b14c6414b6f0c4e4d17]]
= 在 SANtricity System Manager 中编辑密钥管理服务器设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您配置了外部密钥管理、则可以随时查看和编辑密钥管理服务器设置。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*查看/编辑密钥管理服务器设置*。
. 编辑以下字段中的信息：
+
** *密钥管理服务器地址*—输入用于密钥管理的服务器的完全限定域名或IP地址(IPv4或IPv6)。
** *密钥管理端口号*-输入用于密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)通信的端口号。
+
*可选：*您可以通过单击*添加密钥服务器*来包括另一个密钥服务器。

. 单击 * 保存 * 。

[[ID25fe4707c204cd958d8c6bd25de5fe36]]
= 在 SANtricity System Manager 中备份安全密钥
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
创建或更改安全密钥后、您可以为密钥文件创建备份副本、以防其损坏。

.关于此任务
此任务介绍如何备份先前创建的安全密钥。在此操作步骤
期间、您将为备份创建一个新的密码短语。此密码短语不需要与创建原始密钥或上次更改时使用的密码短语匹配。密码短语仅适用于您要创建的备份。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*备份密钥*。
+
此时将打开备份安全密钥对话框。

. 在*定义密码短语/重新输入密码短语*字段中、输入并确认此备份的密码短语。
+
此值可以包含8到32个字符、并且必须包括以下每个字符：

+
** 大写字母(一个或多个)
** 一个数字(一个或多个)
** 非字母数字字符、例如！、*、@(一个或多个)

+
[CAUTION]
====
请务必记录您的条目以供日后使用。要访问此安全密钥的备份、您需要使用密码短语。

====
. 单击*备份*。
+
安全密钥的备份将下载到本地主机、然后打开*确认/记录安全密钥备份*对话框。

+
[NOTE]
====
下载的安全密钥文件的路径可能取决于浏览器的默认下载位置。

====
. 在安全位置记下您的密码短语、然后单击*关闭*。

.完成后
您应验证备份安全密钥。

[[ID061545ae714ae3eb933e43a4f8b02dbb]]
= 在 SANtricity System Manager 中验证安全密钥
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以验证安全密钥、以确保其未损坏、并验证您是否具有正确的密码短语。

.关于此任务
此任务介绍如何验证您先前创建的安全密钥。这是确保密钥文件未损坏且密码短语正确的重要步骤、它可确保在将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列后、您可以访问驱动器数据。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*验证密钥*。
+
此时将打开验证安全密钥对话框。

. 单击*浏览*、然后选择密钥文件(例如、`drivesecury.slk`)。
. 输入与选定密钥关联的密码短语。
+
选择有效的密钥文件和密码短语后、*验证*按钮将变为可用。

. 单击*验证*。
+
验证结果将显示在对话框中。

. 如果结果显示"The security key validated successfully"、请单击*关闭*。如果显示错误消息、请按照对话框中显示的建议说明进行操作。

[[IDa74aa037c9025551d21cb5ecf214878a]]
= 在 SANtricity System Manager 中使用内部密钥管理时解锁驱动器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您配置了内部密钥管理、然后将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将安全密钥重新分配给新存储阵列、才能访问驱动器上的加密数据。

.开始之前
* 在源阵列(要删除驱动器的阵列)上、您已导出卷组并删除驱动器。在目标阵列上、您已重新安装驱动器。
+

NOTE: System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

+
有关迁移卷组的详细说明、请参见 https://kb.netapp.com/["NetApp 知识库"^]。请务必按照适用于System Manager管理的较新阵列或旧系统的相应说明进行操作。

*
必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。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。
* 您必须知道与要解锁的驱动器关联的安全密钥。
* 管理客户端(具有用于访问System Manager的浏览器的系统)上提供了安全密钥文件。如果要将驱动器移动到由其他系统管理的存储阵列、则需要将安全密钥文件移动到该管理客户端。

.关于此任务
使用内部密钥管理时、安全密钥将存储在本地存储在存储阵列上。安全密钥是指控制器和驱动器共享的字符串、用于进行读/写访问。如果从阵列中物理删除驱动器并将其安装在另一个阵列中、则这些驱动器将无法运行、除非您提供正确的安全密钥。

[NOTE]
====
您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。本主题介绍使用_internal_密钥管理时解锁数据。如果您使用的是_external_密钥管理、请参见xref:{relative_path}unlock-drives-using-an-external-security-key.html["使用外部密钥管理时解锁驱动器"]。如果要执行控制器升级并将所有控制器更换为最新硬件、则必须按照中E系列和SANtricity 文档中心所述的不同步骤进行操作link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["解锁驱动器"]。

====
在另一个阵列中重新安装启用了安全保护的驱动器后、该阵列将发现这些驱动器、并显示"需要注意"情况以及"需要安全密钥"状态。 要解锁驱动器数据、请选择安全密钥文件并输入密钥的密码短语。(此密码短语与存储阵列的管理员密码不同。)

如果新存储阵列中安装了其他启用了安全保护的驱动器、则这些驱动器使用的安全密钥可能与您要导入的

安全密钥不同。在导入过程中、旧安全密钥仅用于解锁要安装的驱动器的数据。成功完成解锁过程后、新安装的驱动器将重新密钥到目标存储阵列的安全密钥。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*解锁安全驱动器*。
+
此时将打开解除安全驱动器锁定对话框。表中显示了需要安全密钥的所有驱动器。

. *可选：*将鼠标悬停在驱动器编号上可查看驱动器的位置(磁盘架编号和托架编号)。
. 单击*浏览*、然后选择与要解锁的驱动器对应的安全密钥文件。
+
您选择的密钥文件将显示在对话框中。

. 输入与此密钥文件关联的密码短语。
+
输入的字符将被屏蔽。

. 单击*解锁*。
+
如果解锁操作成功、则对话框将显示："The associated secure drives have been unlocked"。

.结果
锁定并解除锁定所有驱动器后、存储阵列中的每个控制器都将重新启动。但是、如果目标存储阵列中已有一些未锁定的驱动器、则控制器不会重新启动。

.完成后
在目标阵列(包含新安装驱动器的阵列)上、您现在可以导入卷组。

NOTE: System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

有关迁移卷组的详细说明、请参见 https://kb.netapp.com/["NetApp 知识库"^]。

[[ID0c930de21455fa05176489f0e09d84e6]]
= 在 SANtricity System Manager 中使用外部密钥管理时解锁驱动器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您配置了外部密钥管理、然后将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将安全密钥重新分配给新存储阵列、才能访问驱动器上的加密数据。

.开始之前
* 在源阵列(要删除驱动器的阵列
)上、您已导出卷组并删除驱动器。在目标阵列上、您已重新安装驱动器。
+

NOTE: System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

+
有关迁移卷组的详细说明、请参见 https://kb.netapp.com/["NetApp 知识库
"^]。请务必按照适用于System Manager管理的较新阵列或旧系统的相应说明进行操作。

*
必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。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。
* 您必须知道密钥管理服务器的IP地址和端口号。
* 您已为存储阵列的控制器创建一个签名客户端证书文件、并已将该文件复制到要访问System Manager的主机。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。
* 您必须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。

[NOTE]
====
有关服务器证书的详细信息、请参见密钥管理服务器的文档。

====
.关于此任务
使用外部密钥管理时、安全密钥会存储在外部的服务器上、用于保护安全密钥。安全密钥是指控制器和驱动器共享的字符串、用于进行读/写访问。如果从阵列中物理删除驱动器并将其安装在另一个阵列中、则这些驱动器将无法运行、除非您提供正确的安全密钥。

[NOTE]
====
您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。本主题介绍使用_external_密钥管理时解锁数据。如果您使用_internal_密钥管理、请参见 xref:{relative_path}unlock-drives-using-an-internal-security-key.html["使用内部密钥管理时解锁驱动器"]。如果要执行控制器升级并将所有控制器更换为最新硬件、则必须按照中E系列和SANtricity 文档中心所述的不同步骤进行操作

link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["解锁驱动器"]。

====
在另一个阵列中重新安装启用了安全保护的驱动器后、该阵列将发现这些驱动器、并显示"需要注意"情况以及"需要安全密钥"状态。 要解锁驱动器数据、请导入安全密钥文件并输入密钥的密码短语。
(此密码短语与存储阵列的管理员密码不同。)
在此过程中、您可以将存储阵列配置为使用外部密钥管理服务器、然后便可访问安全密钥。您需要提供存储阵列连接和检索安全密钥所需的服务器联系信息。

如果新存储阵列中安装了其他启用了安全保护的驱动器、则这些驱动器使用的安全密钥可能与您要导入的安全密钥不同。在导入过程中、旧安全密钥仅用于解锁要安装的驱动器的数据。成功完成解锁过程后、新安装的驱动器将重新密钥到目标存储阵列的安全密钥。

.步骤
. 从左侧面板中，选择 *System*。
. 在*安全密钥管理*下、选择*创建外部密钥*。
. 使用前提条件连接信息和证书完成向导。
. 单击*测试通信*以确保能够访问外部密钥管理服务器。
. 选择*解锁安全驱动器*。
+
此时将打开解除安全驱动器锁定对话框。表中显示了需要安全密钥的所有驱动器。

. *可选：*将鼠标悬停在驱动器编号上可查看驱动器的位置(磁盘架编号和托架编号)。
. 单击*浏览*、然后选择与要解锁的驱动器对应的安全密钥文件。
+
您选择的密钥文件将显示在对话框中。

. 输入与此密钥文件关联的密码短语。
+
输入的字符将被屏蔽。

. 单击*解锁*。
+
如果解锁操作成功、则对话框将显示："The associated secure drives have been unlocked"。

.结果
锁定并解除锁定所有驱动器后、存储阵列中的每个控制器都将重新启动。但是、如果目标存储阵列中已有一些未锁定的驱动器、则控制器不会重新启动。

.完成后
在目标阵列(包含新安装驱动器的阵列)上、您现在可以导入卷组。

NOTE: System Manager用户界面不支持导出/导入功能；您必须使用命令行界面(CLI)将卷组导出/导入到其他存储阵列。

有关迁移卷组的详细说明、请参见 https://kb.netapp.com/["NetApp 知识库"^]。

:leveloffset: -1

[[ID3135a3d59a3e654176dad1a319856e8c]]
= SANtricity System Manager 存储驱动器安全常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[what-do-i-need-to-know-before-creating-a-security-key]]
== 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。

[[internal-key-management]]
=== 内部密钥管理

在控制器永久性内存的不可访问位置维护内部密钥并"`hidden`"。在创建内部安全密钥之前、必须执行以下操作：

. 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。

.
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。

[[external-key-management]]
=== 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进行维护。在创建外部安全密钥之前、必须执行以下操作：

. 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。
.
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。
.
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。
+
.. 首先，完成并下载客户端证书签名请求 (CSR)。转到 menu:Certificates[Key management certificates]，然后选择 *Complete CSR*。
.. 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。)
.. 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。

. 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。

[[why-do-i-need-to-define-a-pass-phrase]]
== 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。

[[why-is-it-important-to-record-security-key-information]]
== 为什么记录安全密钥信息很重要?

如果丢失安全密钥信息并且没有备份、则在重新定位启用了安全保护的驱动器或升级控制器时可能会丢失数据。您需要使用安全密钥来解锁驱动器上的数据。

请务必记录安全密钥标识符、关联的密码短语以及安全密钥文件保存在本地主机上的位置。

[[what-do-i-need-to-know-before-backing-up-a-security-key]]
== 备份安全密钥前需要了解哪些信息?

如果原始安全密钥损坏、并且您没有备份、则在驱动器从一个存储阵列迁移到另一个存储阵列时、您将无法访问这些驱动器上的数据。

备份安全密钥之前、请记住以下准则:

* 确保您知道原始密钥文件的安全密钥标识符和密码短语。
+
[NOTE]
====
只有内部密钥使用标识符。创建标识符时、系统会自动生成其他字符并将其附加到标识符字符串的两端。生成的字符可确保标识符是唯一的。

====
*
您可以为备份创建新的密码短语。此密码短语不需要与创建原始密钥或上次更改时使用的密码短语匹配。密码短语仅适用于您要创建的备份。
+
[NOTE]
====
驱动器安全密码短语不应与存储阵列的管理员密码相混淆。Drive Security的密码短语用于保护安全密钥的备份。管理员密码可保护整个存储阵列、防止未经授权的访问。

====
*
备份安全密钥文件将下载到管理客户端。下载文件的路径可能取决于浏览器的默认下载位置。请务必记录安全密钥信息的存储位置。

[[what-do-i-need-to-know-before-unlocking-secure-drives]]
== 在解除安全驱动器锁定之前、我需要了解哪些信息?

要从启用了安全的驱动器解锁数据、必须导入其安全密钥。

在解除锁定启用了安全保护的驱动器之前、请记住以下准则:

* 存储阵列必须已具有安全密钥。迁移的驱动器将重新密钥设置到目标存储阵列。
* 对于要迁移的驱动器、您必须知道安全密钥标识符以及与安全密钥文件对应的密码短语。
* 管理客户端(具有用于访问System Manager的浏览器的系统)上必须具有安全密钥文件。
* 如果要重置锁定的NVMe驱动器、必须输入驱动器的安全ID。要找到安全ID、您必须物理移除驱动器、并在驱动器标签上找到PSID字符串(最多32个字符)。在开始操作之前、请确保已重新安装驱动器。

[[what-is-readwrite-accessibility]]
== 什么是读/写可访问性?

驱动器设置窗口包含有关驱动器安全属性的信息。"读/写可访问"是驱动器数据已锁定时显示的属性之一。

要查看驱动器安全属性，请转到硬件页面。选择驱动器，单击 *查看设置*，然后单击 *显示更多设置*。在页面底部，驱动器解锁时，Read/Write Accessible 属性值为 *Yes* 。驱动器锁定时，Read/Write Accessible 属性值为 *No, invalid security key*。您可以通过导入安全密钥来解锁安全驱动器（转到 menu:System[Unlock secure drives]）。

[[what-do-i-need-to-know-about-validating-the-security-key]]
== 验证安全密钥时需要了解哪些信息?

创建安全密钥后、您应验证密钥文件以确保其未损坏。

如果验证失败、请执行以下操作:

* 如果安全密钥标识符与控制器上的标识符不匹配、请找到正确的安全密钥文件、然后重试验证。
*
如果控制器无法对安全密钥进行解密以进行验证、则您输入的密码短语可能不正确。仔细检查密码短语、必要时重新输入、然后重试验证。如果此错误消息再次出现、请选择密钥文件的备份(如果可用)、然后重试验证。
* 如果仍然无法验证安全密钥、则原始文件可能已损坏。创建密钥的新备份并验证该副本。

[[what-is-the-difference-between-internal-security-key-and-external-security-key-management]]
== 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进行维护。

:leveloffset: -1

= 访问管理

:leveloffset: +1

[[IDc94d2e9082994ec50e75be9ca92606e9]]
= 了解 SANtricity System Manager 中的访问管理
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
访问管理是在SANtricity System Manager中建立用户身份验证的一种方法。

[[what-authentication-methods-are-available]]
== 有哪些身份验证方法可用?

身份验证方法包括RBAC (基于角色的访问控制)、目录服务和安全断言标记语言(SAML):

* * RBAC /本地用户角色*—身份验证通过在存储阵列中强制实施的RBAC功能进行管理。本地用户角色包括预定义的用户配置文件以及具有特定访问权限的角色。
* *目录服务*—身份验证通过LDAP (轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)进行管理。
* * SAML *-身份验证通过使用SAML 2.0的身份提供程序(Identity Provider、IdP)进行管理。

了解更多信息。

```
* xref:{relative_path}how-access-management-works.html["访问管理的工作原理"]
* xref:{relative_path}access-management-terminology.html["访问管理术语"]
* xref:{relative_path}permissions-for-mapped-roles.html["映射角色的权限"]
* xref:{relative_path}access-management-with-local-user-roles.html["
本地用户角色"]
* xref:{relative_path}access-management-with-directory-services.html["
目录服务"]
* xref:{relative_path}access-management-with-saml.html["SAML"]
```

```
[[how-do-i-configure-authentication]]
== 如何配置身份验证?
```

存储阵列已预配置为使用本地用户角色，这是 RBAC
功能的实现。如果要配置其他方法，请转到菜单：Authentication[]。

了解更多信息。

```
* xref:{relative_path}add-directory-server.html["添加LDAP目录服务器"]
* xref:{relative_path}configure-saml.html["配置SAML"]
```

```
[[related-information]]
== 相关信息
```

详细了解与访问管理相关的任务：

```
* xref:{relative_path}change-passwords.html["更改密码"]
* xref:{relative_path}view-audit-log-activity.html["查看审核日志活动"]
* xref:{relative_path}configure-syslog-server-for-audit-
logs.html["为审核日志配置系统日志服务器"]
```

```
= 概念

:leveloffset: +1
```

[[IDe189f1c884604eb7a86924a403aa2dac]]
= SANtricity System Manager 中的访问管理工作原理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
访问管理是在SANtricity System Manager中建立用户身份验证的一种方法。

配置和用户身份验证的工作原理如下：

. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。
+
[NOTE]
====
首次登录时、系统会自动显示用户名`admin`、并且无法更改。`admin`用户可以完全访问系统中的所有功能。

====
. 管理员导航到用户界面中的身份验证。存储阵列已预配置为使用本地用户角色，这是RBAC（基于角色的访问控制）功能的实现。
. 管理员配置以下一种或多种身份验证方法：
+
** *本地用户角色*—身份验证通过在存储阵列中强制实施的RBAC功能进行管理。本地用户角色包括预定义的用户配置文件以及具有特定访问权限的角色。管理员可以使用这些本地用户角色作为单一身份验证方法、也可以将其与目录服务结合使用。除了为用户设置密码之外、无需进行任何配置。
** *目录服务*—身份验证通过LDAP（轻型目录访问协议）服务器和目录服务（例如Microsoft的Active Directory）进行管理。管理员连接到LDAP服务器、然后将LDAP用户映射到存储阵列中嵌入的本地用户角色。
** * SAML *-身份验证通过使用安全断言标记语言（SAML）2.0的身份提供程序（IdP）进行管理。管理员在IdP系统和存储阵列之间建立通信、然后将IdP用户映射到存储阵列中嵌入的本地用户角色。

. 管理员为用户提供System Manager的登录凭据。
. 用户通过输入凭据登录到系统。
+
[NOTE]
====
如果使用SAML和SSO（单点登录）管理身份验证、则系统可能会绕过System Manager登录对话框。

====
+
登录期间、系统将执行以下后台任务：

+
** 根据用户帐户对用户名和密码进行身份验证。
** 根据分配的角色确定用户的权限。
** 为用户提供对用户界面中任务的访问权限。
** 显示界面右上角的用户名。

[[tasks-available-in-system-manager]]
== System Manager中提供的任务

任务访问权限取决于用户分配的角色、这些角色包括：

* *存储管理*—对存储对象（例如卷和磁盘池）具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面（符号）的功能。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

不可用的任务将灰显或不显示在用户界面中。例如、具有"监控"角色的用户可以查看有关卷的所有信息、但无法访问用于修改该卷的功能。诸如*复制服务*和*添加到工作负载*等功能的选项卡将灰显；只有*查看/编辑设置*可用。

[[limitations-in-unified-manager-and-storage-manager]]
== Unified Manager和Storage Manager中的限制

如果为存储阵列配置了SAML、则用户无法通过Unified Manager或原有Storage Manager界面发现或管理该阵列的存储。

配置本地用户角色和目录服务后、用户必须输入凭据、然后才能执行以下任一功能：

* 重命名存储阵列
* 正在升级控制器固件
* 正在加载存储阵列配置
* 正在执行脚本
* 正在尝试在未使用的会话超时时时执行活动操作

[[ID0d84de212cba34501d44395363da6d0c]]
= 了解 SANtricity 软件中的访问管理术语
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解访问管理术语如何应用于存储阵列。

[cols="25h,~"]
|===
| 期限 | Description

a|
访问令牌
a|
访问令牌用于使用REST API或命令行界面
(CLI)进行身份验证、而不是使用用户名和密码。令牌与特定用户(包括LDAP用户)关联、并包括一组权限和到期时间。

a|
Active Directory
a|
Active Directory (AD)是一种Microsoft目录服务、使用LDAP进行Windows域网络。

a|
绑定
a|
绑定操作用于向目录服务器对客户端进行身份验证。绑定通常需要帐户和密码凭据、但某些服务器允许匿名绑定操作。

a|
CA
a|
证书颁发机构(Certificate Authority、
CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

a|
证书
a|
出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。

a|
IdP
a|
身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。

a|
LDAP
a|
轻型目录访问协议(Lightweight Directory Access Protocol、LDAP)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。此协议允许许多不同的应用程序和服务连接到LDAP服务器以验证用户。

a|
RBAC
a|
基于角色的访问控制(Role-Based Access Control、RBAC)是一种根据各个用户的角色来管理对计算机或网络资源的访问的方法。RBAC控制会在存储阵列上强制实施、并包括预定义的角色。

a|
SAML
a|
安全断言标记语言(SAML)是一种基于XML的标准、用于在两个实体之间进行身份验证和授权。SAML支持多因素身份验证、在这种身份验证中、用户必须提供两个或更多项来证明其身份(例如密码和指纹)。存储阵列的嵌入式SAML功能符合SAML2.0标准、可用于身份断言、身份验证和授权。

 a|
SP
 a|
服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。

 a|
SSO
 a|
单点登录(SSO)是一种身份验证服务、允许一组登录凭据访问多个应用程序。

|===

[[ID67d4324ea436c6ec17fe096f63d9a134]]
= 了解 SANtricity System Manager 中映射角色的权限
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在存储阵列上强制实施的RBAC (基于角色的访问控制)功能包括预定义的用户配置文件、其中一个或多个角色映射到这些配置文件。每个角色都具有访问SANtricity System Manager中任务的权限。

用户配置文件和映射角色可从任一 System Manager 用户界面中的菜单：身份验证[本地用户角色]访问。

这些角色可为用户提供对任务的访问权限、如下所示：

* *存储管理*—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

如果用户没有执行某个任务的权限、则该任务将灰显或不会显示在用户界面中。

[[IDa8ee8253a261e3504fb40ae9ccf3ed24]]
= 在 SANtricity System Manager 中使用本地用户角色配置访问管理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于访问管理、管理员可以使用在存储阵列中强制实施的RBAC （基于角色的访问控制）功能。这些功能称为"本地用户角色"。

[[configuration-workflow]]
== 配置工作流

已为存储阵列预先配置本地用户角色。要使用本地用户角色进行身份验证、管理员可以执行以下操作：

. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。
+
[NOTE]
====
`admin`用户可以完全访问系统中的所有功能。

====
. 管理员会查看用户配置文件、这些配置文件是预定义的、无法修改。
. 管理员也可以为每个用户配置文件分配新密码。
. 用户使用分配的凭据登录到系统。

[[management]]
== 管理

如果仅使用本地用户角色进行身份验证、则管理员可以执行以下管理任务：

* 更改密码。
* 设置密码的最小长度。
* 允许用户在不使用密码的情况下登录。

[[ID3208b5d998121ce994c4d3434ca644a2]]

= 使用 SANtricity System Manager 中的目录服务配置访问管理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于访问管理、管理员可以使用LDAP (轻型目录访问协议)服务器和目录服务、例如Microsoft的Active Directory。

[[configuration-workflow]]
== 配置工作流

如果在网络中使用LDAP服务器和目录服务、则配置的工作原理如下：

. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。
+
[NOTE]
====
`admin`用户可以完全访问系统中的所有功能。

====
. 管理员输入LDAP服务器的配置设置。设置包括域名、URL和绑定帐户信息。
. 如果LDAP服务器使用安全协议(LDAPS)、则管理员将上传证书颁发机构(CA)证书链、以便在LDAP服务器和存储阵列之间进行身份验证。
. 建立服务器连接后、管理员会将用户组映射到存储阵列的角色。这些角色是预定义的、无法修改。
. 管理员测试LDAP服务器与存储阵列之间的连接。
. 用户使用其分配的LDAP/Directory服务凭据登录到系统。

[[management]]
== 管理

使用目录服务进行身份验证时、管理员可以执行以下管理任务：

* 添加目录服务器。
* 编辑目录服务器设置。
* 将LDAP用户映射到本地用户角色。
* 删除目录服务器。

[[ID4d82a2049bbee1f4ee23342483e1fda3]]
= 在 SANtricity System Manager 中使用 SAML 配置访问管理
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于访问管理、管理员可以使用阵列中嵌入的安全断言标记语言(Security Assertion Markup Language、SAML) 2.0功能。

[[configuration-workflow]]
== 配置工作流

SAML配置的工作原理如下：

. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。
+
[NOTE]
====
`admin`用户可以完全访问System Manager中的所有功能。

====
. 管理员转到身份验证下的 *SAML* 页面。
. 管理员配置与身份提供程序(Identity Provider、IdP)的通信。
IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。要配置与存储阵列的通信、管理员将从IdP系统下载IdP元数据文件、然后使用System Manager将此文件上传到存储阵列。
. 管理员在服务提供商和
IdP之间建立信任关系。服务提供商负责控制用户授权；在这种情况下、存储阵列中的控制器充当服务提供商。要配置通信、管理员可以使用System
Manager导出每个控制器的服务提供商元数据文件。然后、管理员从IdP系统将这些元数据文件导入到IdP中。
+
[NOTE]
====
管理员还应确保IdP支持在身份验证时返回名称ID。

====
. 管理员会将存储阵列的角色映射到IdP中定义的用户属性。为此、管理员可以使用System Manager创建映射。
. 管理员测试对IdP URL的SSO登录。此测试可确保存储阵列和IdP能够进行通信。
+

[CAUTION]
====
启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
. 在System Manager中、管理员为存储阵列启用SAML。
. 用户使用其SSO凭据登录到系统。

[[management]]
== 管理

使用SAML进行身份验证时、管理员可以执行以下管理任务：

* 修改或创建新角色映射
* 导出服务提供商文件

[[access-restrictions]]
== 访问限制

启用SAML后、用户将无法通过Unified Manager或原有Storage Manager界面发现或管理该阵列的存储。

此外、以下客户端无法访问存储阵列服务和资源：

* 企业管理窗口(EMW)
* 软件开发人员套件(SDK)客户端
* 带内客户端
* 使用标准REST API端点登录

[[limited-connectivity-with-saml-enabled]]
=== 启用SAML的连接有限

启用SAML后、以下存储阵列功能与JSON Web令牌身份验证的连接将受到限制。

* 命令行界面（ CLI ）
* HTTP基本身份验证REST API客户端

[[ID2d46e3e9aae09c8c79466deaeaaae062]]
= 了解访问令牌和 SANtricity 软件
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
访问令牌提供了一种使用REST API或命令行界面
(CLI)进行身份验证的方法、而不会公开用户名和密码。令牌与特定用户(包括LDAP用户)关联、并包括一组权限和到期时间。

[[saml-and-json-web-token-access]]
== SAML和JSON Web令牌访问

默认情况下、启用了SAML的系统不允许访问传统命令行工具。REST API和CLI实际上无法运行、因为MFA工作流需要重定向到身份提供程序服务器进行身份验证。因此、您必须在System Manager中生成令牌、这要求用户通过MFA进行身份验证。

NOTE: 要使用Web令牌、无需启用SAML、但出于最高的安全性级别、建议使用SAML。

[[workflow-for-creating-and-using-tokens]]
== 用于创建和使用令牌的工作流

. 在System Manager中创建令牌并确定其到期日期。
. 将令牌文本复制到剪贴板或下载到文件中、然后将令牌文本保存在安全位置。
. 使用令牌、如下所示：
+
** * REST APi*：要在REST API请求中使用令牌、请在请求中添加HTTP标头。例如：
`Authorization: Bearer _<access-token-value>_`
** *安全命令行界面
*：要在命令行中使用令牌、请在命令行中添加令牌值或使用包含令牌值的文件的路径。例如：
+
*** 命令行上的令牌值： `-t _access-token-value_`
*** 包含令牌值的文件的路径： `-T _access-token-file_`

了解更多信息。

* xref:{relative_path}access-management-tokens-create.html["创建访问令牌"]
* xref:{relative_path}access-management-tokens-edit.html["编辑访问令牌"]
* xref:{relative_path}access-management-tokens-revoke.html["撤消访问令牌"]

:leveloffset: -1

= 使用本地用户角色

:leveloffset: +1

[[ID99e87401489d33023b10a9b85eea98a7]]
= 在 SANtricity System Manager 中查看本地用户角色
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
从"本地用户角色"页面，您可以查看用户配置文件到默认角色的映射。这些映射是在存储阵列中实施的基于角色的访问控制 (RBAC) 的一部分。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
无法更改用户配置文件和映射。只能修改密码。

.步骤
. 从左侧面板中，选择菜单：Authentication[Local user roles]。
+
下表显示了用户配置文件：

+
** * root
admin*(admin)—超级管理员、有权访问系统中的所有功能。此用户配置文件包含所有角色。

** *存储管理*(存储
)—负责所有存储配置的管理员。此用户配置文件包括以下角色：存储管理员、支持管理员和监控。
** *安全性管理*(安全性
)—负责安全配置的用户、包括访问管理、证书管理和启用了安全保护的驱动器功能。此用户配置文件包括以下角色：安全管理员和监控。
** *支持管理*(支持)—
负责硬件资源、故障数据和固件升级的用户。此用户配置文件包括以下角色：Support Admin
和Monitor。
** *监控*(监控)—对系统具有只读访问权限的用户。此用户配置文件仅包含监控角色。

[[ID759cbd3e6ed082c65ea85f2738c7ae3a]]
= 在 SANtricity System Manager 中更改密码
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以在Access Management中更改每个用户配置文件的用户密码。

.开始之前
* 您必须以本地管理员身份登录、其中包括root管理员权限。
* 您必须知道本地管理员密码。

.关于此任务
选择密码时、请记住以下准则：

* 任何新的本地用户密码必须满足或超过当前最低密码设置(在"查看/编辑设置"中)。
* 密码区分大小写。
* 设置密码时、密码中的后缀空格不会被删除。如果密码中包含空格、请小心操作。
* 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。

[NOTE]
====
在System Manager中更改密码也会在命令行界面(CLI)中进行更改。此外、密码还会将发生原因
用户的活动会话更改为终止。

====

.步骤
. 从左侧面板中，选择菜单：Authentication[Local user roles]。
. 从表中选择一个用户。
+
更改密码按钮将变为可用。

. 选择 * 更改密码 * 。
+
此时将打开更改密码对话框。

.
如果未为本地用户密码设置最小密码长度、则可以选中此框以要求选定用户输入密码以访问存储阵列、然后您可以键入选定用户的新密码。
. 输入本地管理员密码、然后单击*更改*。

.结果
如果用户当前已登录、则更改密码会导致用户的活动会话终止。

[[IDecab54886cd7673bea160dbec6bf486e]]
= 在 SANtricity System Manager 中更改本地用户密码设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以为存储阵列上的所有新的或更新的本地用户密码设置所需的最小长度。您还可以允许本地用户在不输入密码的情况下访问存储阵列。

.开始之前
您必须以本地管理员身份登录、其中包括root管理员权限。

.关于此任务
设置本地用户密码的最小长度时、请记住以下准则：

* 设置更改不会影响现有本地用户密码。
* 本地用户密码的最小长度设置必须介于0到30个字符之间。
* 任何新的本地用户密码都必须满足或超过当前的最小长度设置。
* 如果希望本地用户在未输入密码的情况下访问存储阵列、请勿设置密码的最小长度。

.步骤

. 从左侧面板中，选择菜单：Authentication[Local user roles]。
. 选择*查看/编辑设置*按钮。
+
此时将打开本地用户密码设置对话框。

. 执行以下操作之一：
+
** 要允许本地用户在不输入密码的情况下访问存储阵列、请取消选中"至少需要所有本地用户密码"复选框。
** 要为所有本地用户密码设置最小密码长度、请选中"要求所有本地用户密码至少为"复选框、然后使用spinner框设置所有本地用户密码所需的最小长度。
+
任何新的本地用户密码都必须满足或超过当前设置。

. 单击 * 保存 * 。

:leveloffset: -1

= 使用目录服务

:leveloffset: +1

[[ID117480388b9532e64128c38c20b7cd7f]]
= 在 SANtricity System Manager 中添加 LDAP 目录服务器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要为访问管理配置身份验证、您可以在存储阵列和LDAP服务器之间建立通信、然后将LDAP用户组映射到阵列的预定义角色。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 必须在目录服务中定义用户组。
* LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
* 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

.关于此任务
添加目录服务器分为两步。首先输入域名和URL。如果服务器使用安全协议、则如果CA证书由非标准签名颁发机构签名、则还必须上传此CA证书以进行身份验证。如果您拥有绑定帐户的凭据、则还可以输入您的用户帐户名称和密码。接下来、将LDAP服务器的用户组映射到存储阵列的预定义角色。

[NOTE]
====
在操作步骤 添加LDAP服务器期间、原有管理界面将被禁用。原有管理界面(符号)是存储阵列与管理客户端之间的一种通信方法。禁用后、存储阵列和管理客户端将使用更安全的通信方法(基于https的REST API)。

====
.步骤
. 从左侧面板中，选择菜单：Authentication[Directory services]，然后选择 *Add Directory Server*。
+
此时将打开添加目录服务器对话框。

. 在服务器设置选项卡中、输入LDAP服务器的凭据。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

a|
配置设置

a|
域
a|
输入LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(_username_@_domain_)以指定要对其进行身份验证的目录服务器。

a|
服务器URL
a|
输入用于访问LDAP服务器的URL、格式为`ldap：//*主机*：*端口*`。

a|
上传证书(可选)
a|

NOTE: 只有在上述服务器URL字段中指定了LDAPS协议时、才会显示此字段。

单击*浏览*并选择要上传的CA证书。这是用于对LDAP服务器进行身份验证的可信证书或证书链。

a|
绑定帐户(可选)
a|
输入一个只读用户帐户、用于对LDAP服务器进行搜索查询以及在组中进行搜索。以LDAP类型格式输入帐户名称。例如、如果绑定用户名为"bindAcct"、则可以输入"cn=bindAcct、cn=users、DC=cpoc、DC=local"等值。

a|
绑定密码(可选)
a|

NOTE: 输入上述绑定帐户时、将显示此字段。

输入绑定帐户的密码。

a|
添加前测试服务器连接
a|
如果要确保存储阵列可以与您输入的LDAP服务器配置进行通信、请选中此复选框。单击对话框底部的*添加*后、将进行测试。如果选中此复选框且测试失败、则不会添加配置。您必须解决此错误或取消选中此复选框、才能跳过测试并添加配置。

a|
权限设置*

a|

搜索基础DN
 a|
输入LDAP环境以搜索用户、通常采用的形式 `CN=Users, DC=cpoc, DC=local`。

 a|
username属性
 a|
输入绑定到用户ID的属性以进行身份验证。例如：`sAMAccountName`。

 a|
组属性
 a|
输入用户上的组属性列表、用于组到角色映射。例如：`memberOf、managedObjects`。

|===
====
. 单击"*角色映射"*选项卡。
. 将LDAP组分配给预定义角色。一个组可以分配多个角色。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

 a|
映射

 a|
组DN
 a|
为要映射的LDAP用户组指定组可分辨名称(DN)。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(`\`)进行转义：\.[] {} ()<>*+-=! ？ ^$...

 a|
角色
 a|

单击此字段、然后选择要映射到组DN的存储阵列角色之一。您必须单独为此组选择要包含的每个角色。要登录到SANtricity 系统管理器、需要将"监控"角色与其他角色结合使用。映射的角色包括以下权限：

** *存储管理*—对存储对象（例如卷和磁盘池）具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面（符号）的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+
[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System
Manager将无法正常运行。

====
. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
. 完成映射后、单击*添加*。
+
系统将执行验证、以确保存储阵列和LDAP服务器可以进行通信。如果显示错误消息、请检查在对话框中输入的凭据、并根据需要重新输入信息。

[[ID0c7c84174a50368ae8ddbad265af49db]]
= 在 SANtricity System Manager 中编辑目录服务器设置和角色映射
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您之前在Access
Management中配置了目录服务器、则可以随时更改其设置。设置包括服务器连接信息和组到角色映射。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 必须定义目录服务器。

.步骤
. 从左侧面板中，选择 menu:Authentication[Directory services]。
. 如果定义了多个服务器、请从表中选择要编辑的服务器。
. 选择*查看/编辑设置*。
+
此时将打开目录服务器设置对话框。

. 在服务器设置选项卡中、更改所需设置。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

a|
配置设置

a|
域
a|
LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(_username_@_domain_)以指定要对其进行身份验证的目录服务器。

a|
服务器URL
a|
用于以形式访问LDAP服务器的URL `ldap[s]://host:port`。

a|
绑定帐户(可选)
a|
用于对LDAP服务器进行搜索查询以及在组内进行搜索的只读用户帐户。

a|
绑定密码(可选)

a|
绑定帐户的密码。（输入绑定帐户时会显示此字段。）

a|
保存前测试服务器连接
a|
检查存储阵列是否可以与LDAP服务器配置进行通信。单击对话框底部的*保存*后、将进行测试。如果选中此复选框且测试失败、则不会更改配置。您必须解决此错误或取消选中此复选框、才能跳过测试并重新编辑配置。

a|
权限设置

a|
搜索基础DN
a|
用于搜索用户的LDAP环境、通常采用的形式 `CN=Users, DC=cpoc, DC=local`。

a|
username属性
a|
绑定到用户ID进行身份验证的属性。例如：`sAMAccountName`。

a|
组属性
a|
用户上的组属性列表、用于组到角色映射。例如：`memberOf、managedObjects`。

|===
====
. 在角色映射选项卡中、更改所需的映射。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===

| 正在设置 ... | Description

a|
映射

a|
组DN
a|
要映射的LDAP用户组的域名。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(`\`)进行转义：\.[] {} ()<>*+-=！？^$...

a|
角色
a|
要映射到组DN的存储阵列角色。您必须单独为此组选择要包含的每个角色。要登录到SANtricity系统管理器、需要将"监控"角色与其他角色结合使用。存储阵列的角色包括：

** *存储管理*—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+
[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

====
. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
. 单击 * 保存 * 。

.结果
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

[[ID5cbf58acd9d5ab3f7e6d9eec7c337e49]]
= 在 SANtricity System Manager 中删除目录服务器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要断开目录服务器和存储阵列之间的连接，可以从目录服务页面删除服务器信息。如果配置了新服务器，然后要删除旧服务器，则可能需要执行此任务。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

.步骤
. 从左侧面板中，选择 menu:Authentication[Directory services]。
. 从列表中、选择要删除的目录服务器。
. 单击 * 删除 * 。
+
此时将打开删除目录服务器对话框。

. 在字段中键入`remove`、然后单击*删除*。
+
此时将删除目录服务器配置设置、权限设置和角色映射。用户无法再使用此服务器的凭据登录。

:leveloffset: -1

= 使用SAML

:leveloffset: +1

[[IDd173a865bf1938966c065ed164d0515b]]
= 在 SANtricity System Manager 中配置 SAML
:allow-uri-read:
:experimental:

:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要为访问管理配置身份验证、您可以使用存储阵列中嵌入的安全断言标记语言(SAML)功能。此配置将在身份提供程序和存储提供程序之间建立连接。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 您必须知道存储阵列中每个控制器的IP地址或域名。
* IdP管理员已配置IdP系统。
* IdP管理员已确保IdP支持在身份验证时返回名称ID。
* 管理员已确保IdP服务器和控制器时钟保持同步(通过NTP服务器或通过调整控制器时钟设置)。
* IdP元数据文件从IdP系统下载、并可从用于访问System Manager的本地系统上获得。

.关于此任务
身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。要在IdP和存储阵列之间建立连接、您需要在这两个实体之间共享元数据文件。接下来、将IdP用户实体映射到存储阵列角色。最后、在启用SAML之前、您需要测试连接和SSO登录。

[NOTE]
====
* SAML和目录服务*。如果在将目录服务配置为身份验证方法时启用SAML、则SAML将取代System Manager中的目录服务。如果稍后禁用SAML、则目录服务配置将返回到其先前的配置。

====
[CAUTION]
====
*正在编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
配置SAML身份验证是一个多步骤操作步骤。

[[step-1-upload-the-idp-metadata-file]]
== 第1步：上传IdP元数据文件

要为存储阵列提供IdP连接信息、请将IdP元数据导入到System Manager中。
IdP系统需要使用此元数据将身份验证请求重定向到正确的URL并验证收到的响应。您只需为存储阵列上传

一个元数据文件、即使有两个控制器也是如此。

.步骤
. 从左侧面板中，选择菜单：Authentication[SAML]。
+
此页面将显示配置步骤的概述。

. 单击*导入身份提供程序(IdP)文件*链接。
+
此时将打开导入身份提供程序文件对话框。

. 单击*浏览*以选择您复制到本地系统的IdP元数据文件并将其上传。
+
选择文件后、将显示IdP实体ID。

. 单击 * 导入 * 。

[[step-2-export-service-provider-files]]
== 第2步：导出服务提供商文件

要在IdP和存储阵列之间建立信任关系、请将服务提供商元数据导入到IdP中。IdP需要使用此元数据与控制器建立信任关系并处理授权请求。此文件包含控制器域名或IP地址等信息、以便IdP可以与服务提供商进行通信。

.步骤
. 单击*导出服务提供商文件*链接。
+
此时将打开导出服务提供商文件对话框。

. 在*控制器A*字段中输入控制器IP地址或DNS名称、然后单击*导出
*将元数据文件保存到本地系统。如果存储阵列包含两个控制器、请对*控制器B*字段中的第二个控制器重复此步骤。
+
单击*导出*后、服务提供商元数据将下载到本地系统。记下文件的存储位置。

. 在本地系统中、找到您导出的服务提供商元数据文件。
+
每个控制器都有一个XML格式的文件。

. 从
IdP服务器导入服务提供商元数据文件以建立信任关系。您可以直接导入文件、也可以手动输入文件中的控制器信息。

[[step-3-map-roles]]
== 第3步：映射角色

要为用户提供对System Manager的授权和访问权限、您必须将
IdP用户属性和组成员资格映射到存储阵列的预定义角色。

.开始之前
* IdP管理员已在IdP系统中配置用户属性和组成员资格。
* IdP元数据文件将导入到System Manager中。
* 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。

.步骤
. 单击*映射System Manager*角色的链接。
+
此时将打开角色映射对话框。

. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

 a|
映射

 a|
用户属性
 a|
指定要映射的SAML组的属性(例如、"member for")。

 a|
属性值
 a|
指定要映射的组的属性值。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(`\`)进行转义：\.[] {} ()<>*+-=! ？ ^$...

 a|
角色
 a|
单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独选择要包括的每个角色。要登录到System Manager、需要将监控角色与其他角色结合使用。至少一个组还需要安全管理员角色。

映射的角色包括以下权限：

** *存储管理*—对存储对象（例如卷和磁盘池）具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面（符号）的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+
[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System
Manager将无法正常运行。

====
. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
+
[NOTE]
====
启用SAML后、可以修改角色映射。

====
. 完成映射后、单击*保存*。

[[step-4-test-sso-login]]
== 第4步：测试SSO登录

为了确保IdP系统和存储阵列可以进行通信、您可以选择测试SSO登录。在启用SAML的最后一步中、也会执行此测试。

.开始之前
* IdP元数据文件将导入到System Manager中。

* 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。

.步骤
. 选择*测试SSO登录*链接。
+
此时将打开一个对话框、用于输入SSO凭据。

. 输入具有安全管理员权限和监控权限的用户的登录凭据。
+
在系统测试登录时、将打开一个对话框。

. 查找Test Successful消息。如果测试成功完成、请转至下一步以启用SAML。
+
如果测试未成功完成、则会显示一条错误消息、其中包含更多信息。请确保：

+
** 该用户属于具有安全管理员和监控权限的组。
** 您为IdP服务器上传的元数据正确无误。
** SP元数据文件中的控制器地址正确。

[[step-5-enable-saml]]
== 第5步：启用SAML

最后一步是完成用户身份验证的SAML配置。在此过程中、系统还会提示您测试SSO登录。上一步介绍了SSO登录测试过程。

.开始之前
* IdP元数据文件将导入到System Manager中。
* 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。
* 至少配置了一个监控器和一个安全管理员角色映射。

[CAUTION]
====
*正在编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
.步骤
. 选择*启用 SAML* 链接。
+

此时将打开确认启用SAML对话框。

. 键入`enable`、然后单击*启用*。
. 输入用于SSO登录测试的用户凭据。

.结果
系统启用SAML后、它将终止所有活动会话并开始通过SAML对用户进行身份验证。

[[ID200f5fb0951d2511d34568200dc6b457]]
= 在 SANtricity System Manager 中更改 SAML 角色映射
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果先前已为访问管理配置SAML、则可以更改IdP组与存储阵列的预定义角色之间的角色映射。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* IdP管理员已在IdP系统中配置用户属性和组成员资格。
* 已配置并启用SAML。

.步骤
. 从左侧面板中，选择菜单：Authentication[SAML]。
. 选择 *Map System Manager roles*。
+
此时将打开角色映射对话框。

. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。
+
[CAUTION]
====
请注意、在启用SAML时、您不会删除权限、否则您将无法访问System Manager。

====
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]

|===
| 正在设置 ... | Description

a|
映射

a|
用户属性
a|
指定要映射的SAML组的属性(例如、"member for")。

a|
属性值
a|
指定要映射的组的属性值。

a|
角色
a|
单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独为此组选择要包含的每个角色。要登录到System
Manager、需要将监控角色与其他角色结合使用。必须至少将安全管理员角色分配给一个组。映射的角色包括以下权限：

** *存储管理*—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+

NOTE：包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System
Manager将无法正常运行。

. 或者、也可以单击*添加另一个映射*以输入更多组到角色的映射。

. 单击 * 保存 * 。

.结果
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

[[ID96024dbda4b0d599ba12030480dfe34d]]
= 在 SANtricity System Manager 中导出 SAML 服务提供商文件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如有必要、您可以导出存储阵列的服务提供商元数据并将文件重新导入到身份提供程序(Identity Provider、IdP)系统中。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 已配置并启用SAML。

.关于此任务
在此任务中、您将从控制器导出元数据(每个控制器一个文件)。IdP需要使用此元数据与控制器建立信任关系并处理身份验证请求。此文件包含IdP可用于发送请求的控制器域名或IP地址等信息。

.步骤
. 从左侧面板中，选择菜单：Authentication[SAML]。
. 选择*导出*。
+
此时将打开导出服务提供商文件对话框。

. 对于每个控制器、单击*导出*将元数据文件保存到本地系统。
+
[NOTE]
====
每个控制器的域名字段均为只读字段。

====
+
记下文件的存储位置。

. 在本地系统中、找到您导出的服务提供商元数据文件。

+
每个控制器都有一个XML格式的文件。

. 从
IdP服务器导入服务提供商元数据文件。您可以直接导入文件、也可以手动输入文件中的控制器信息。
. 单击 * 关闭 * 。

:leveloffset: -1

= 使用访问令牌

:leveloffset: +1

[[IDefe14bbca52299ffd5c2b0e665648b9a]]
= 在 SANtricity System Manager 中创建访问令牌
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以创建访问令牌、以使用REST API或命令行界面(CLI)进行身份验证、而不是使用用户名和密码。

NOTE: 令牌没有密码、因此您必须小心管理。

.步骤
. 从左侧面板中，选择菜单：Authentication[Access tokens]。
. 选择*查看/编辑访问令牌设置*。在对话框中、确保已选中*启用访问令牌*复选框。单击*保存
*以关闭对话框。
. 选择*创建访问令牌*。
. 在对话框中、选择令牌有效的持续时间。
+

NOTE: 令牌过期后、用户的身份验证尝试将失败。

. 单击 * 创建。 *
. 在对话框中、选择以下选项之一：
+
** *复制*将令牌文本保存到剪贴板。

** *下载*将令牌文本保存到文件中。
+

NOTE：请务必保存令牌文本。这是在关闭对话框之前查看文本的唯一机会。

. 单击 * 关闭 * 。
. 使用令牌、如下所示：
+
** * REST APi*：要在REST API请求中使用令牌、请在请求中添加HTTP标头。例如：
`Authorization: Bearer _<access-token-value>_`
** *安全命令行界面
*：要在命令行中使用令牌、请在命令行中添加令牌值或使用包含令牌值的文件的路径。例如：
+
*** 命令行上的令牌值： `-t _access-token-value_`
*** 包含令牌值的文件的路径： `-T _access-token-file_`
+

NOTE：如果未指定用户名、密码或令牌、则命令行界面会提示用户输入访问令牌值。

[[IDed04eb485d1d19f9e41989f6afc57d7a]]
= 在 SANtricity System Manager 中编辑访问令牌设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以编辑访问令牌的设置、包括到期时间和创建新令牌的功能。

.步骤
. 从左侧面板中，选择菜单：Authentication[Access tokens]。
. 选择*查看/编辑访问令牌设置*。
. 在对话框中、您可以执行以下一项或两项任务：
+
** 启用或禁用令牌创建。

** 更改现有令牌的到期时间。
+

NOTE: 取消选择*启用访问令牌
*设置后、它将同时阻止令牌创建和令牌身份验证。如果稍后重新启用此设置、则可以重新使用未过期的令牌。如果要永久撤消所有现有令牌、请参见 xref:{relative_path}access-management-tokens-revoke.html["撤消访问令牌"]。

. 单击 * 保存 * 。

[[ID927fd7c3b68ad970cbbc3a45b317155a]]
= 撤销 SANtricity System Manager 中的访问令牌
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您确定某个令牌已被泄露、或者您要对用于对访问令牌进行签名和验证的加密密钥执行手动密钥轮换、则可以撤消所有访问令牌。

此操作将重新生成用于对令牌进行签名的密钥。重置密钥后、_all_发出的令牌将立即失效。由于存储阵列不会跟踪令牌、因此无法撤消各个令牌。

.步骤
. 从左侧面板中，选择菜单：Authentication[Access tokens]。
. 选择*撤消所有访问令牌*。
. 在对话框中、单击*是*。

撤消所有令牌后、您可以创建新令牌并立即使用它们。

:leveloffset: -1

= 管理系统日志

:leveloffset: +1

[[ID777cef365749e4a39b9dea670c0508c8]]
= 在 SANtricity System Manager 中查看审计日志活动
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
通过查看审核日志、具有安全管理员权限的用户可以监控用户操作、身份验证失败、无效登录尝试以及用户会话生命周期。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.步骤
. 从左侧面板中，选择菜单：Monitoring[Audit log]。
+
审核日志活动以表格形式显示、其中包括以下信息列：

+
** *日期/时间*-存储阵列检测到事件的时间戳(GMT)。
** *用户名*-与事件关联的用户名。对于存储阵列上的任何未经身份验证的操作、"N/A"将显示为用户名。未经过身份验证的操作可能由内部代理或其他机制触发。
** *状态代码*—操作的HTTP状态代码(200、400等)以及与事件关联的描述性文本。
** "*已访问URL"*-完整URL (包括主机)和查询字符串。
** *客户端IP地址*-与事件关联的客户端的IP地址。
** *源*—与事件关联的日志记录源、可以是System Manager、CLI、Web服务或支持Shell。
** *问题描述 *-有关事件的追加信息 、如果适用。

. 使用"审核日志"页面上的选择来查看和管理事件。
+
.选择详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 选择 | Description

 a|
显示事件
 a|

按日期范围(过去24小时、过去7天、过去30天或自定义日期范围)显示的限制事件。

a|
筛选器
a|
限制按字段中输入的字符显示的事件。请使用引号("")来精确匹配字词、输入`或`返回一个或多个字词、或者输入短划线(-)来省略字词。

a|
刷新
a|
选择*刷新*可将页面更新为最新事件。

a|
查看/编辑设置
a|
选择*查看/编辑设置*以打开一个对话框、在此可以指定完整的日志策略以及要记录的操作级别。

a|
删除事件
a|
选择*删除*以打开一个对话框、在此可以从页面中删除旧事件。

a|
显示/隐藏列
a|
单击*显示/隐藏*列图标image:../media/sam-1140-ss-access-columns.gif["显示/隐藏列"]以选择要在表中显示的其他列。其他列包括：

** *方法*- HTTP方法(例如POST、GET、DELETE等)。
** *已执行命令行界面命令*—为安全命令行界面请求执行的命令行界面命令(语法)。
** *命令行界面返回状态*—命令行界面状态代码或客户端请求输入文件。
** *符号操作步骤 *—符号操作步骤 已执行。
** * SSH事件类型*-安全Shell (SSH)事件类型、例如login、logout和login_fail。
** * SSH会话PID*—SSH会话的进程ID号。
** * SSH会话持续时间*-用户登录的秒数。
** *身份验证类型*-类型可以包括本地用户、LDAP、SAML和访问令牌。

** *身份验证ID*-已身份验证会话的ID。

a|
切换列筛选器
a|
单击 *Toggle* 图标 image:../media/sam-1140-ss-access-toggle.gif["切换"]
打开每列的筛选字段。在列字段中输入字符，以限制这些字符显示的事件。再次单击图标关闭筛选字段。

a|
撤消更改
a|
单击*Undo*图标image:../media/sam-1140-ss-access-undo.gif["撤消
"]可将表恢复为默认配置。

a|
导出
a|
单击*导出*将表数据保存到逗号分隔值(CSV)文件。

|===
====

[[ID40278f85659260fc4ea647cacc375c93]]
= 在 SANtricity System Manager 中定义审计日志策略
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以更改覆盖策略以及审核日志中记录的事件类型。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
此任务介绍如何更改审核日志设置、其中包括用于覆盖旧事件的策略以及用于记录事件类型的策略。

.步骤
. 从左侧面板中，选择菜单：Monitoring[Audit log]。
. 选择*查看/编辑设置*。
+
此时将打开审核日志设置对话框。

. 更改覆盖策略或记录的事件类型。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

 a|
覆盖策略
 a|
确定达到最大容量时用于覆盖旧事件的策略：

** *允许在审核日志已满时覆盖审核日志中最早的事件*-当审核日志达到50、000条记录时覆盖旧事件。
** *需要手动删除审核日志事件*-
指定不会自动删除事件；而是以设置的百分比显示阈值警告。必须手动删除事件。
+

NOTE:
如果禁用了覆盖策略、并且审核日志条目达到最大限制、则没有安全管理员权限的用户将无法访问System Manager。要还原没有安全管理员权限的用户的系统访问权限、分配有安全管理员角色的用户必须删除旧事件记录。

+

NOTE： 如果为归档审核日志配置了系统日志服务器、则覆盖策略不适用。

 a|
要记录的操作级别
 a|
确定要记录的事件类型：

** *仅记录修改事件*-仅显示用户操作涉及在系统中进行更改的事件。
** *记录所有修改和只读事件*-显示所有事件、包括涉及读取或下载信息的用户操作。

|===
====
. 单击 * 保存 * 。

[[ID986152b368ec3dff21ef84b91a55dcb2]]
= 从 SANtricity System Manager 中的审核日志中删除事件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以清除旧事件的审核日志、从而使搜索事件更易于管理。删除后、您可以选择将旧事件保存到CSV（逗号分隔值）文件中。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.步骤
. 从左侧面板中，选择菜单：Monitoring[Audit log]。
. 选择 * 删除 * 。
+
此时将打开删除审核日志对话框。

. 选择或输入要删除的最旧事件的数量。
. 如果要将已删除的事件导出到CSV文件（建议）、请保持选中状态。在下一步中单击*删除*时、系统将提示您输入文件名和位置。否则、如果您不想将事件保存到CSV文件、请单击复选框以取消选中它。
. 单击 * 删除 * 。
+
此时将打开确认对话框。

. 在字段中键入`delete`、然后单击*删除*。
+
最早的事件将从审核日志页面中删除。

[[IDd279e26150f5894807308b4627e154fa]]
= 在 SANtricity System Manager 中为审计日志配置 syslog 服务器
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果要将审核日志归档到外部系统日志服务器、则可以配置该服务器与存储阵列之间的通信。建立连接后、审核日志会自动保存到系统日志服务器。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
* 如果您的服务器使用安全协议(例如TLS)、则本地系统上必须具有证书颁发机构(CA)证书。CA证书用于标识服务器和客户端之间安全连接的网站所有者。

.步骤
. 从左侧面板中，选择菜单：监控[Audit log]，然后选择 *Configure Syslog Servers*。
+
此时将打开配置系统日志服务器对话框。

. 单击 * 添加 * 。
+
此时将打开添加系统日志服务器对话框。

. 输入服务器的信息、然后单击*添加*。
+
** *服务器地址*-输入完全限定域名、IPv4地址或IPv6地址。
** *协议*-从下拉列表中选择一个协议(例如TLS、UDP或TCP)。
** *上传证书(可选)*—如果您选择了TLS协议但尚未上传签名的CA证书、请单击*浏览*上传证书文件。如果没有可信证书、则不会将审核日志归档到系统日志服务器。
+
[NOTE]
====
如果证书稍后变得无效，则 TLS 握手将失败。因此，错误消息将发布到审核日志，并且不再将消息发送到 syslog 服务器。要解决此问题，必须修复 syslog 服务器上的证书，然后转到菜单：监控[审核日志 > 配置 Syslog 服务器 > 测试全部]。

====

** *端口*-输入系统日志接收器的端口号。单击*添加*后、配置系统日志服务器对话框将打开、并在页面上显示已配置的系统日志服务器。

. 要测试服务器与存储阵列的连接、请选择*全部测试*。

.结果
配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。要进一步配置警报的系统日志设置、请参见 https://docs.netapp.com/us-en/e-series-santricity/sm-settings/configure-syslog-server-for-alerts.html["为系统日志服务器配置警报"]。

NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

[[ID4ba838f269afa3205a21eecb1f6288a8]]
= 在 SANtricity System Manager 中编辑审计日志记录的 syslog 服务器设置
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以更改用于归档审核日志的系统日志服务器的设置、也可以为该服务器上传新的证书颁发机构(CA)证书。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
* 如果要上传新的CA证书、则此证书必须在本地系统上可用。

.步骤
. 从左侧面板中，选择菜单：监控[Audit log]，然后选择 *Configure Syslog Servers*。
+
已配置的系统日志服务器将显示在页面上。

. 要编辑服务器信息、请选择服务器名称右侧的*编辑*(铅笔)图标、然后在以下字段中进行所需的更改：
+
** *服务器地址*-输入完全限定域名、IPv4地址或IPv6地址。
** *协议*-从下拉列表中选择一个协议(例如TLS、UDP或TCP)。
** *端口*-输入系统日志接收器的端口号。

. 如果将协议更改为安全TLS协议(从UDP或TCP)、请单击*导入可信证书*以上传CA证书。
. 要测试与存储阵列的新连接、请选择*全部测试*。

.结果
配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。

```
:leveloffset: -1

[[IDca6c88f4a57a7a6f9ad4cc7a9889cf00]]
= SANtricity System Manager 用户访问管理常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
```
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。

```
[[why-cant-i-log-in]]
== 为什么我无法登录?
```

如果在尝试登录到SANtricity系统管理器时收到错误、请查看这些可能的原因。

System Manager登录错误可能是由于以下原因之一：

* 您输入的用户名或密码不正确。
* 您的权限不足。
* 目录服务器(如果已配置)可能不可用。如果是这种情况、请尝试使用本地用户角色登录。
* 您尝试多次登录失败、从而触发锁定模式。等待10分钟以重新登录。
* 已触发锁定条件，您的审核日志可能已满。转到监控 > 审核日志，从审核日志中删除旧事件。
* 已启用SAML身份验证。刷新浏览器以登录。

由于以下原因之一、可能会在远程存储阵列上登录错误以执行镜像任务：

* 您输入的密码不正确。
* 您尝试多次登录失败、从而触发锁定模式。请等待10分钟以重新登录。

* 已达到控制器上使用的最大客户端连接数。检查是否存在多个用户或客户端。

[[what-do-i-need-to-know-before-adding-a-directory-server]]
== 在添加目录服务器之前、我需要了解哪些信息?

在Access Management中添加目录服务器之前、请确保满足以下要求。

* 必须在目录服务中定义用户组。
* LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
* 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

[[what-do-i-need-to-know-about-mapping-to-storage-array-roles]]
== 关于映射到存储阵列角色、我需要了解哪些信息?

在将组映射到角色之前、请查看以下准则。

存储阵列的嵌入式RBAC （基于角色的访问控制）功能包括以下角色：

* *存储管理*—对存储对象（例如卷和磁盘池）具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面（符号）的功能。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

[[directory-services]]
=== 目录服务

如果您使用的是LDAP （轻型目录访问协议）服务器和目录服务、请确保：

* 管理员已在目录服务中定义用户组。
* 您知道
LDAP用户组的组域名。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠（`\`）进行转义：
+
[listing]

\.[]{}()<>*+-=!?^$|

```
----
```
* 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

[[saml]]
=== SAML

如果您使用的是存储阵列中嵌入的安全断言标记语言(SAML)功能、请确保：

* 身份提供程序(Identity Provider、IdP)管理员已在IdP系统中配置用户属性和组成员资格。
* 您知道组成员资格名称。
*
您知道要映射的组的属性值。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(`\`)进行转义：
+
```
[listing]
----
\.[]{}()<>*+-=!?^$|
----
```
* 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

[[which-external-management-tools-may-be-affected-by-this-change]]
== 哪些外部管理工具可能会受到此更改的影响?

在SANtricity系统管理器中进行某些更改(例如切换管理接口或使用SAML进行身份验证方法)时、可能会限制使用某些外部工具和功能。

[[management-interface]]
=== 管理接口

除非启用旧版管理接口设置、否则直接与旧版管理界面(符号)通信的工具(例如SANtricity SMI-S Provider或OnCommand Insight (OCI))
无法正常工作。此外、如果禁用了此设置、则不能使用传统CLI命令或执行镜像操作。

有关详细信息，请联系技术支持。

[[saml-authentication]]
=== SAML 身份验证

启用SAML后、以下客户端将无法访问存储阵列服务和资源：

* 企业管理窗口(EMW)
* 命令行界面（ CLI ）
* 软件开发人员套件(SDK)客户端
* 带内客户端
* HTTP基本身份验证REST API客户端
* 使用标准REST API端点登录

有关详细信息，请联系技术支持。

[[what-do-i-need-to-know-before-configuring-and-enabling-saml]]
== 在配置和启用SAML之前、我需要了解哪些信息？

在配置和启用安全断言标记语言(SAML)身份验证功能之前、请确保满足以下要求并了解SAML限制。

[[requirements]]
=== 要求

开始之前、请确保：

* 已在网络中配置身份提供程序(Identity Provider、IdP)。
IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。您的安全团队负责维护IdP。
* IdP管理员已在IdP系统中配置用户属性和组。
* IdP管理员已确保IdP支持在身份验证时返回名称ID。
* 管理员已确保IdP服务器和控制器时钟保持同步(通过NTP服务器或通过调整控制器时钟设置)。
* IdP元数据文件从IdP系统下载、并可从用于访问System Manager的本地系统上获得。
* 您知道存储阵列中每个控制器的IP地址或域名。

[[restrictions]]
=== 限制

除了上述要求之外、请确保您了解以下限制：

* 启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑

SAML配置、请联系技术支持以获得帮助。建议您先测试SSO登录、然后再在最终配置步骤中启用SAML。（系统还会在启用SAML之前执行SSO登录测试。）
* 如果您将来禁用SAML、则系统会自动还原先前的配置（本地用户角色和/或目录服务）。
* 如果当前已为用户身份验证配置目录服务、则SAML将覆盖此配置。
* 配置SAML后、以下客户端将无法访问存储阵列资源：
+
** 企业管理窗口（EMW）
** 命令行界面（ CLI ）
** 软件开发人员套件（SDK）客户端
** 带内客户端
** HTTP基本身份验证REST API客户端
** 使用标准REST API端点登录

[[what-types-of-events-are-recorded-in-the-audit-log]]
== 审核日志中记录了哪些类型的事件？

审核日志可以记录修改事件、也可以同时记录修改和只读事件。

根据策略设置、将显示以下类型的事件：

* *修改事件*- System Manager中涉及系统更改的用户操作、例如配置存储。
* *修改和只读事件*-涉及系统更改的用户操作以及涉及查看或下载信息的事件、例如查看卷分配。

[[what-do-i-need-to-know-before-configuring-a-syslog-server]]
== 在配置系统日志服务器之前、我需要了解哪些信息？

您可以将审核日志归档到外部系统日志服务器。

在配置系统日志服务器之前、请记住以下准则。

* 确保您知道服务器地址、协议和端口号。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
* 如果您的服务器使用安全协议（例如TLS）、则本地系统上必须具有证书颁发机构（CA）证书。
CA证书用于标识服务器和客户端之间安全连接的网站所有者。
* 配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。
* 覆盖策略设置（可从*查看/编辑设置*获得）不会影响使用系统日志服务器配置管理日志的方式。
* 审核日志采用RFC 5424消息格式。

[[the-syslog-server-is-no-longer-receiving-audit-logs-what-do-i-do]]
== 系统日志服务器不再接收审核日志。我该怎么办?

如果您为系统日志服务器配置了TLS协议、则如果证书因任何原因而无效、则服务器将无法接收消息。审核日志中会发布一条有关此无效证书的错误消息。

要解决此问题，必须首先修复 syslog
服务器的证书。有效的证书链到位后，请转到菜单：Monitoring[Audit log > Configure Syslog Servers > Test All]。

:leveloffset: -1

= 证书

:leveloffset: +1

[[ID4b323215b43274db84ab2d3770676dd0]]
= 了解 SANtricity System Manager 中的证书
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以使用SANtricity系统管理器创建证书签名请求(Certificate signing Requests、CSV)、导入证书以及管理现有证书。

[[what-are-certificates]]
== 什么是证书?

_Certificates_是数字文件、用于标识网站和服务器等联机实体、以便在互联网上进行安全通信。证书有两种类型：_signed certificate"由证书颁发机构(CA)验证；_self-signed certificate"由实体所有者(而不是第三方)验证。

了解更多信息。

* xref:{relative_path}how-certificates-work-sam.html["证书的工作原理"]
* xref:{relative_path}certificate-terminology.html["证书术语"]

[[how-do-i-configure-signed-certificates]]
== 如何配置签名证书?

您可以从System Manager生成签名请求、也可以使用私钥和公共密钥对从外部生成签名请求。签名请求将发送到CA以生成证书文件。CA返回证书文件后、您可以使用System Manager导入这些文件。

了解更多信息。

* xref:{relative_path}use-ca-signed-certificates-for-controllers.html["对控制器使用CA签名的证书"]
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-a-key-management-server.html["使用CA签名的证书通过密钥管理服务器进行身份验证"]

[[related-information]]
== 相关信息

详细了解与证书相关的任务:

* xref:{relative_path}view-imported-certificates.html["查看导入的证书信息"]
* xref:{relative_path}enable-certificate-revocation-checking.html["启用证书撤消检查"]

= 概念

:leveloffset: +1

[[ID84582952ad6a58a7e6b2c504a8dbfb1a]]
= 证书在 SANtricity System Manager 中的工作方式
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

证书可确保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System Manager、您可以管理主机管理系统(充当客户端)上的浏览器与存储系统中的控制器(充当服务器)之间的证书。

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。

[NOTE]
====
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。

====

[[signed-certificates]]
== 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。

[[self-signed-certificates]]
== 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。但是、自签名证书与CA签名证书使用的信任链不同。

自签名证书不受浏览器"`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。

[[certificates-used-for-key-management-server]]
== 用于密钥管理服务器的证书

如果您使用的是具有驱动器安全功能的外部密钥管理服务器、则还可以管理用于在该服务器和控制器之间进行身份验证的证书。

[[IDbbeb20987909b5267aba3952094f6fb7]]
= 了解 SANtricity 软件中的证书术语
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
以下术语适用于证书管理。

[cols="25h,~"]
|===
| 期限 | Description

a|
CA
a|
证书颁发机构(Certificate Authority、
CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

a|
CSR
a|
证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述所需的信息。

a|
证书
a|
出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证（签名）的可信实体的身份。

a|
证书链
a|
一种文件层次结构、用于向证书添加一层安全保护。通常、此链包含一个位于层次结构顶部的根证书、一个或多个中间证书以及用于标识实体的服务器证书。

a|
客户端证书
a|
对于安全密钥管理、客户端证书会验证存储阵列的控制器、以便密钥管理服务器可以信任其IP地址。

a|
中间证书
a|
一个或多个中间证书从证书链中的根分支。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。

a|
密钥管理服务器证书
a|
对于安全密钥管理、密钥管理服务器证书会对服务器进行验证、以便存储阵列可以信任其IP地址。

a|
密钥库
a|
密钥库是主机管理系统上的存储库、其中包含私钥及其对应的公有
密钥和证书。这些密钥和证书用于标识您自己的实体、例如控制器。

a|
OCSP服务器
a|
联机证书状态协议(OCSP)服务器可确定证书颁发机构(CA)是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问服务器。

a|
根证书
a|
根证书位于证书链中的层次结构顶部、其中包含用于对其他证书签名的专用密钥。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。

a|
签名证书
a|
由证书颁发机构(CA)验证的证书。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。此外、签名证书还包括实体所有者的详细信息(通常为服务器或网站)以及由字母和数字组成的数字签名。签名证书使用信任链、因此最常用于生产环境。也称为"CA签名证书"或"管理证书"。

a|
自签名证书
a|
自签名证书由实体的所有者进行验证。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。它还包括由字母和数字组成的数字签名。自签名证书与CA签名证书使用的信任链不同、因此最常用于测试环境。也称为"预安装"证书。

a|
服务器证书
a|
服务器证书位于证书链的底部。它标识您的特定实体、例如网站或其他设备。存储系统中的每个控制器都需要一个单独的服务器证书。

|===

:leveloffset: -1

= 使用证书

:leveloffset: +1

[[ID6807828754f7a00f6a018e153337ce4a]]
= 在 SANtricity System Manager 中为控制器使用 CA 签名的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以获取CA签名的证书、以便控制器与用于访问SANtricity系统管理器的浏览器之间进行安全通信。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 您必须知道每个控制器的IP地址或DNS名称。

.关于此任务
使用CA签名证书是一个三步操作步骤。

[[step-1-complete-csrs-for-the-controllers]]
== 第1步：完成控制器的CSR

您必须先为存储阵列中的每个控制器生成证书签名请求(CSR)文件。

.关于此任务
此任务介绍如何从System Manager生成CSR文件。CSR可提供有关您的组织的信息、以及控制器的IP地址或DNS名称。在此任务期间、如果存储阵列具有一个控制器、则会生成一个CSR文件；如果存储阵列具有两个控制器、则会生成两个CSR文件。

[NOTE]
====
或者、您也可以使用OpenSSL等工具生成CSR文件、并可跳至 <<第2步：提交CSR文件>>。

====
.步骤
. 从左侧面板中，选择菜单：Certificates[Array management certificates]，然后选择*Complete CSR*。

+
[NOTE]
====
如果显示一个对话框、提示您接受第二个控制器的自签名证书、请单击*接受自签名证书*以继续。

====
. 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*—存储阵列或业务所在的城市。
** *省/自治区/直辖市(可选)*—存储阵列或业务所在的省/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。

+
[CAUTION]
====
某些字段可能会预先填充相应的信息、例如控制器的IP地址。请勿更改预先填充的值、除非您确定这些值不正确。例如、如果尚未完成CSR、则控制器IP地址将设置为"`localhost.`"。
在这种情况下、您必须将"`localhost`"更改为控制器的DNS名称或IP地址。

====
. 验证或输入有关存储阵列中控制器A的以下信息：
+
** *控制器A公用名*-默认情况下、显示控制器A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内容完全匹配、才能访问System Manager。DNS名称不能以通配符开头。
** *控制器A备用IP地址*-如果公用名称为IP地址、则可以选择为控制器A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。
** *控制器A备用DNS名称*-如果公用名是DNS名称、请为控制器A输入任何其他
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。如果存储阵列只有一个控制器、则可以使用*完成*按钮。
+
如果存储阵列有两个控制器、则可以使用*下一步*按钮。

+
[NOTE]
====
首次创建CSR请求时、请勿单击*跳过此步骤*链接。在错误恢复情况下提供此链接。在极少数情况下、一个控制器上的CSR请求可能会失败、而另一个控制器上的CSR请求则可能不会失败。通过此链接、您可以跳过在已定义的控制器A上创建CSR请求的步骤、并继续执行在控制器B上重新创建CSR请求的下一步

====
. 如果只有一个控制器、请单击*完成*。如果有两个控制器、请单击*下一步*以输入控制器B的信息(与上述相同)、然后单击*完成*。
+
对于单个控制器、会将一个CSR文件下载到本地系统。对于双控制器、将下载两个CSR文件。下载内容的文件夹位置取决于您的浏览器。

. 转至 <<第2步：提交CSR文件>>。

[[step-2-submit-the-csr-files]]
== 第2步：提交CSR文件

创建证书签名请求(CSR)文件后、请将这些文件发送到证书颁发机构(CA)。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
. 找到已下载的CSR文件。
. 将CSR文件提交到CA (例如VeriSign或DigiCert)、并请求PEM格式的签名证书。
+
[CAUTION]
====
*将CSR文件提交给CA后、请勿重新生成另一个CSR文件。*每当生成CSR时、系统都会创建一个专用和公有密钥对。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。

====
. 当CA返回签名证书时、转到 <<第3步：导入控制器的签名证书>>。

[[step-3-import-signed-certificates-for-controllers]]
== 第3步：导入控制器的签名证书

从证书颁发机构(CA)收到签名证书后、导入控制器的文件。

.开始之前
* CA返回签名证书文件。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用于标识控制器的服务器证书。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。
* 您已将证书文件复制到访问System Manager的主机系统。

.步骤
. 从左侧面板中选择菜单：Certificates[Array management certificates]，然后选择*Import*。
+
此时将打开一个对话框、用于导入证书文件。

. 单击*浏览*按钮、首先选择根证书和中间证书文件、然后选择控制器的每个服务器证书。两个控制器的根文件和中间文件相同。对于每个控制器、只有服务器证书是唯一的。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。

. 单击 * 导入 * 。
+
这些文件将上传并进行验证。

.结果
会话将自动终止。要使证书生效、您必须重新登录。重新登录后、新的CA签名证书将用于会话。

[[IDb2b0b762e555052936ebbc8c4e1e5b9c]]
= 在 SANtricity System Manager 中重置管理证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将控制器上的证书从使用CA签名证书还原到出厂设置的自签名证书。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 必须事先导入CA签名的证书。

.关于此任务
重置功能会从每个控制器中删除当前CA签名的证书文件。然后、这些控制器将还原为使用自签名证书。

.步骤

. 从左侧面板中，选择菜单：Certificates[Array management certificates]
，然后选择*Reset*。
+
此时将打开确认重置管理证书对话框。

. 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
控制器将还原为使用自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

[[ID4512a40df2672b714959409ed2cc30b4]]
= 在 SANtricity System Manager 中查看导入的证书信息
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在证书类别中，您可以查看存储阵列的证书类型、颁发机构以及证书的有效日期范围。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.步骤
. 从左侧面板中，选择 *Certificates*。
. 选择以下页面之一，以查看有关证书的信息。
+
[cols="25h,~"]
|===
| 页面 | Description

a|
menu:证书[阵列管理证书]
a|
查看有关为每个控制器导入的CA签名证书的信息、包括根文件、中间文件和服务器文件。

a|
菜单：证书[受信任的证书]
a|
查看有关为控制器导入的所有其他类型证书的信息。使用*显示证书...*下的筛选器字段可查看用户安装或预安装的证书。

** *用户安装*—用户上传到存储阵列的证书、如果控制器充当客户端(而不是服务器)、LDAPS证书和身份联合证书、则这些证书可能包括可信证书。
** *预安装*—存储阵列附带的自签名证书。

a|
menu:证书[密钥管理证书]
a|
查看有关为外部密钥管理服务器导入的CA签名证书的信息。

|===

[[IDedf963b4a05bf93893e9db3191640c7c]]
= 在 SANtricity System Manager 中充当客户端时导入控制器的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果控制器由于无法验证网络服务器的信任链而拒绝某个连接，则可以从"受信任的证书"页面导入一个允许控制器（作为客户端）接受来自该服务器的通信的证书。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 证书文件安装在本地系统上。

.关于此任务
如果要允许其他服务器联系控制器（例如，LDAP 服务器或使用 TLS 的 syslog 服务器），则可能需要从"受信任的证书"页面导入证书。

.步骤

. 从左侧面板中，选择菜单：Certificates[Trusted certificates]，然后选择 *Import*。
+
此时将打开一个对话框、用于导入可信证书文件。

. 单击*浏览*以选择控制器的证书文件。
+
文件名显示在对话框中。

. 单击 * 导入 * 。

.结果
这些文件将上传并进行验证。

[[IDac72378998b15485201c075222d8d77d]]
= 在 SANtricity System Manager 中启用证书吊销检查
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以启用对已撤销证书的自动检查、以便联机证书状态协议(OCSP)服务器阻止用户进行非安全连接。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 在两个控制器上都配置了DNS服务器、这样可以为
OCSP服务器使用完全限定域名。此任务可从硬件页面访问。
* 如果要指定自己的OCSP服务器、则必须知道该服务器的URL。

.关于此任务
如果CA颁发的证书不正确或私钥受到损坏、则自动撤消检查非常有用。

在此任务期间、您可以配置OCSP服务器或使用证书文件中指定的服务器。OCSP服务器会确定CA是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问站点。

.步骤
. 从左侧面板中，选择菜单：Certificates[Trusted certificates]。
+
[NOTE]
====
您还可以从*密钥管理证书*页面启用吊销检查。

====
. 单击*不常见任务*、然后从下拉菜单中选择*启用撤消检查*。
. 选择*我要启用撤消检查*、以便复选框中显示复选标记、对话框中显示其他字段。
. 在* OCSP响应器地址*字段中、您可以选择输入OCSP响应器服务器的
URL。如果不输入地址、系统将使用证书文件中的OCSP服务器URL。
. 单击*测试地址*以确保系统可以打开与指定URL的连接。
. 单击 * 保存 * 。

.结果
如果存储阵列尝试使用已撤销的证书连接到服务器、则连接将被拒绝并记录事件。

[[IDac51290151b5d3054a280f253288205f]]
= 在 SANtricity System Manager 中删除受信任的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以从"受信任"选项卡中删除先前导入的用户安装的证书。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 如果要使用新版本更新受信任证书、则必须先导入更新后的证书、然后才能删除旧证书。

[CAUTION]
====
如果在导入替代证书之前删除用于对控制器和其他服务器(例如LDAP服务器)进行身份验证的证书、则可能无法访问系统。

====
.关于此任务
此任务介绍如何删除用户安装的证书。无法删除预安装的自签名证书。

.步骤
. 从左侧面板中，选择菜单：Certificates[Trusted certificates]。
+
此表显示了存储阵列的受信任证书。

. 从表中、选择要删除的证书。

. 单击菜单：uncommon Tasks[Delete]。
+
此时将打开确认删除可信证书对话框。

. 在字段中键入`delete`、然后单击*删除*。

[[ID261b81f733e14e26d435790aadf05997]]
= 使用 CA 签名证书通过 SANtricity System Manager 中的密钥管理服务器进行身份验证
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要在密钥管理服务器和存储阵列控制器之间实现安全通信、您必须配置相应的证书集。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.关于此任务
在控制器和密钥管理服务器之间进行身份验证是一个两步操作步骤。

[[step-1-complete-and-submit-csr-for-authentication-with-a-key-management-server]]
== 第1步：完成并提交CSR、以便使用密钥管理服务器进行身份验证

您必须先生成证书签名请求(CSR)文件、然后使用CSR从密钥管理服务器信任的证书颁发机构(CA)请求签名客户端证书。您还可以使用下载的CSR文件从密钥管理服务器创建和下载客户端证书。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。

NOTE：通过私钥和公共密钥对在外部生成的CSR文件可以通过"Create External Security Key"(创建外部安全密钥)对话框导入。有关导入外部生成的CSR文件的详细信息，请参阅 https://docs.netapp.com/us-en/e-series-santricity/sm-settings/use-ca-signed-certificates-for-authentication-with-a-key-management-server.html#step-2-import-certificates-for-the-key-management-server["第2步：导入密钥管理服务器的证书"]。

.步骤

. 从左侧面板中，选择菜单：Certificates[Key management certificates]，然后选择*Complete CSR*。
. 输入以下信息：
+
** *公用名*--用于标识客户机的名称。常见做法是、将公用名中的内容与KMS服务器对客户端证书命名约定的要求进行匹配。公用名通常有助于KMS在握手期间提供客户端证书时识别该证书。
** *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*-组织所在的城市或位置。
** *省/自治区/直辖市(可选)*—组织所在的省/自治区/直辖市。
** *国家/地区ISO代码*—贵组织所在的两位数ISO (国际标准化组织)代码、例如美国。

. 单击 * 下载 * 。
+
此时、CSR文件将保存到本地系统。

. 从密钥管理服务器信任的CA请求签名客户端证书。
+

NOTE：密钥管理服务器通常具有直接生成签名证书的工具、因为它充当自己的CA。

. 拥有客户端证书后、请转到 <<第2步：导入密钥管理服务器的证书>>。

[[step-2-import-certificates-for-the-key-management-server]]
== 第2步：导入密钥管理服务器的证书

下一步是、在存储阵列和密钥管理服务器之间导入用于身份验证的证书。证书有两种类型：客户端证书用于验证存储阵列的控制器、而密钥管理服务器证书用于验证服务器。您必须加载控制器的客户端证书文件和密钥管理服务器的服务器证书文件。

.开始之前
* 您有一个签名的客户端证书文件(请参见 <<第1步：完成并提交CSR、以便使用密钥管理服务器进行身份验证>>)、并且您已将该文件复制到要访问System Manager的主机。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。
* 您必须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。
+
[NOTE]
====
有关服务器证书的详细信息、请参见密钥管理服务器的文档。

====

.步骤
. 从左侧面板中，选择菜单：Certificates[Key management certificates]
，然后选择*Import*。
+
此时将打开一个对话框、用于导入证书文件。

. 在*选择客户端证书*旁边、单击*浏览*按钮为存储阵列的控制器选择客户端证书文件。
+
此时、文件名将显示在对话框中。

. 如果使用私钥和公钥对在外部生成了证书文件，请单击*Select private key file*
旁边的*Browse*按钮，为存储阵列的控制器选择证书文件。
+
此时、文件名将显示在对话框中。

. 在*选择密钥管理服务器的服务器证书*旁边、单击*浏览
*按钮为密钥管理服务器选择服务器证书文件。您可以为密钥管理服务器选择根证书、中间证书或服务器证书。
+
此时、文件名将显示在对话框中。

. 单击 * 导入 * 。
+
这些文件将上传并进行验证。

[[ID9b08a88bfc36e0f394a2cc8372744dab]]
= 在 SANtricity System Manager 中导出密钥管理服务器证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将密钥管理服务器的证书保存到本地计算机。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

* 必须事先导入证书。

.步骤
. 从左侧面板中，选择菜单：Certificates[Key management certificates]。
. 从表中、选择要导出的证书、然后单击*导出*。
+
此时将打开保存对话框。

. 输入文件名并单击*保存*。

:leveloffset: -1

[[ID77b4e0777690dda585317dcbc8fbccab]]
= SANtricity System Manager 的 CA 签名证书和自签名证书常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[why-does-the-cannot-access-other-controller-dialog-box-appear]]
== 为什么会显示"无法访问其他控制器"对话框?

在执行与CA证书相关的某些操作(例如、导入证书)时、您可能会看到一个对话框、提示您接受第二个控制器的自签名证书。

在具有两个控制器的存储阵列(双工配置)中、如果SANtricity
系统管理器无法与第二个控制器通信、或者您的浏览器在操作的某个时间点无法接受证书、则有时会显示此对话框。

如果此对话框打开、请单击*接受自签名证书*以继续。如果另一个对话框提示您输入密码、请输入用于访问System Manager的管理员密码。

如果此对话框再次出现、并且您无法完成证书任务、请尝试以下过程之一：

* 使用其他浏览器类型访问此控制器、接受证书并继续。

* 使用System Manager访问第二个控制器、接受自签名证书、然后返回到第一个控制器并继续。

[[how-do-i-know-what-certificates-need-to-be-uploaded-to-santricity-system-manager-for-external-key-management]]
== 我如何知道需要将哪些证书上传到SANtricity系统管理器以进行外部密钥管理?

对于外部密钥管理、您可以导入两种类型的证书、以便在存储阵列和密钥管理服务器之间进行身份验证、从而使这两个实体可以相互信任。

客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。

要获取客户端证书、请使用System Manager为存储阵列完成CSR。您还可以使用私钥和公共密钥对在外部生成CSR。

然后、您可以将CSR上传到密钥管理服务器并从该服务器生成客户端证书。获得客户端证书后、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。从密钥管理服务器检索服务器证书文件、然后将该文件复制到要访问System Manager的主机。

[[what-do-i-need-to-know-about-certificate-revocation-checking]]
== 关于证书撤消检查、我需要了解哪些信息?

使用SANtricity系统管理器、您可以使用联机证书状态协议(Online Certificate Status Protocol、OCSP)服务器(而不是上传证书撤消列表(Certificate Revocation List、CRL))来检查是否存在已撤销的证书。

已撤销的证书不应再受信任。证书可能会因多种原因而被撤销；例如、如果证书颁发机构(CA)颁发的证书不正确、私钥被泄露或标识的实体不符合策略要求。

在System Manager中与OCSP服务器建立连接后、存储阵列将在连接到AutoSupport服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时执行撤消检查。存储阵列会尝试验证这些服务器的证书、以确保它们未被撤消。然后、服务器将为该证书返回"good "、"revoked"或"unknown"值。如果证书已撤销或阵列无法与OCSP服务器联系、则连接将被拒绝。

[NOTE]
====
在System Manager或命令行界面(CLI)中指定OCSP响应程序地址会覆盖在证书文件中找到的OCSP地址。

====

[[what-types-of-servers-will-revocation-checking-be-enabled-for]]
== 将为哪些类型的服务器启用撤消检查?

每当存储阵列连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时、它都会执行撤消检查。

:leveloffset: -1

= 支持

:leveloffset: +1

[[ID31fc6b8d537f976bce0d22bd9fcd693d]]
= 获取 SANtricity System Manager 支持
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
通过支持页面可以访问技术支持资源。

[[what-support-tasks-are-available]]
== 有哪些支持任务可用?

在支持中、您可以查看技术支持联系人、执行诊断、配置AutoSupport
、查看事件日志以及执行软件升级。

了解更多信息。

* xref:{relative_path}autosupport-feature-overview.html["AutoSupport 功能概述"]
* xref:{relative_path}overview-event-log.html["事件日志概述"]
* xref:{relative_path}overview-upgrade-center.html["升级中心概述"]

[[how-do-i-contact-technical-support]]
== 如何联系技术支持?

在主页，单击菜单：支持[Support resources]。技术支持联系信息列在界面右上角。

= 查看信息和诊断

:leveloffset: +1

[[ID8a57f93c95f0862bca44400f7568a9ed]]
= 在 SANtricity System Manager 中查看存储阵列的配置文件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
存储阵列配置文件可提供存储阵列的所有组件和属性的问题描述。

.关于此任务
您可以在恢复期间使用存储阵列配置文件作为辅助工具、也可以概述存储阵列的当前配置。您可能希望在管理客户端上保存存储阵列配置文件的副本、并在存储阵列中保留存储阵列配置文件的硬副本。如果配置发生更改、请为存储阵列配置文件创建一个新副本。

.步骤
. 从左侧面板中，选择菜单：Support[Support resources]。
. 向下滚动到 * 启动详细存储阵列信息 * ，然后选择 * 存储阵列配置文件 * 。
+
此时、报告将显示在您的屏幕上。

+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 部分 | Description

a|
存储阵列
a|
显示了您可以配置的所有选项以及存储阵列的系统静态选项。这些选项包括控制器数量、驱动器架、驱动器、磁盘池、卷组、 卷和热备用驱动器；允许的驱动器架、驱动器、固态磁盘(SSD)和卷的最大数量；快照组、快照映像、快照卷和一致性组的数量；功能信息；固件版本信息；机箱序列号信息；AutoSupport 状态和AutoSupport 计划信息；
用于自动支持数据收集和计划支持数据收集的设置；存储阵列全球通用标识符(World Wide Identifier、WWID)；以及介质扫描和缓存设置。

a|
存储
a|
显示了存储阵列中所有存储设备的列表。根据您的存储阵列配置、存储部分可能会显示这些子部分。

** *磁盘池*-显示存储阵列中所有磁盘池的列表。
** *卷组*-显示存储阵列中所有卷组的列表。卷和可用容量按创建顺序列出。
** *卷*-显示存储阵列中所有卷的列表。列出的信息包括卷名称、卷状态、容量、RAID级别、卷组或磁盘池、驱动器类型以及其他详细信息。
** *缺少卷*-
显示存储阵列中当前处于缺失状态的所有卷的列表。列出的信息包括每个缺少的卷的全球通用标识符(World Wide Identifier、WWID)。

a|
复制服务
a|
显示了用于存储阵列的所有副本服务的列表。根据您的存储阵列配置、复制服务部分可能会显示以下子部分：

** *卷副本*-
显示存储阵列中所有副本对的列表。列出的信息包括副本数量、副本对名称、状态、开始时间戳和其他详细信息。
** *快照组*-显示存储阵列中所有快照组的列表。
** *快照映像*-显示存储阵列中所有快照的列表。
** * Snapshot Volumes*—显示存储阵列中所有Snapshot卷的列表。
** *一致性组*-显示存储阵列中所有一致性组的列表。
** *成员卷*-显示存储阵列中所有一致性组成员卷的列表。
** *镜像组*-显示所有镜像卷的列表。
** *预留容量*-显示存储阵列中所有预留容量卷的列表。

a|
主机分配
a|
显示了存储阵列中的主机分配列表。列出的信息包括卷名称、逻辑单元号(LUN)、控制器ID、主机名或主机集群名称以及卷状态。列出的追加信息 包括拓扑定义和主机类型定义。

a|
硬件
a|
显示了存储阵列中所有硬件的列表。根据您的存储阵列配置、硬件部分可能会显示这些子部分。

** *控制器*-
显示存储阵列中所有控制器的列表、其中包括控制器位置、状态和配置。此外、它还包括驱动器通道信息、主机通道信息和以太网端口信息。
** *驱动器*-显示存储阵列中所有驱动器的列表。驱动器按磁盘架ID、抽盒ID、插槽ID顺序列出。列出的信息包括磁盘架ID、抽盒ID、插槽ID、状态、原始容量、每个驱动器的介质类型、接口类型、当前数据速率、产品ID和固件版本。驱动器部分还包括驱动器通道信息、热备用磁盘覆盖信息和使用寿命信息(仅适用于SSD驱动器)。损耗寿命信息包括已用持久性百分比、即迄今为止写入SSD驱动器的数据量除以驱动器的理论总写入限制。
** *驱动器通道*-显示存储阵列中所有驱动器通道的信息。列出的信息包括通道状态、链路状态(如果适用)、驱动器计数和累积错误计数。
** *磁盘架*-
显示存储阵列中所有磁盘架的信息。列出的信息包括驱动器类型以及磁盘架中每个组件的状态信息。磁盘架组件可能包括电池组、小型可插拔(SFP)收发器、电源风扇箱或输入/输出模块(IOM)箱。如果存储阵列使用了安全密钥、则硬件部分还会显示安全密钥标识符。

a|
功能
a|
显示了每个主机或主机集群安装的功能包列表以及允许的最大快照组、快照(原有)和卷数。功能部分中的信息还包括驱动器安全性、即存储阵列是启用了安全性还是禁用了安全性。

|===
====
. 要搜索存储阵列配置文件、请在*查找*文本框中键入搜索词、然后单击*查找*。
+
所有匹配的术语均会突出显示。要一次滚动浏览一个所有结果，请继续单击 * 查找 * 。

. 要保存存储阵列配置文件、请单击*保存*。
+
此文件将保存在浏览器的"Downloads"文件夹中、名称为`storage-array-profile.txt`。

[[ID9f8862ed461d2fe3f49993c94b5f19a6]]
= 在 SANtricity System Manager 中查看软件和固件清单
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
软件和固件清单列出了存储阵列中每个组件的固件版本。

.关于此任务
存储阵列由多个组件组成、其中可能包括控制器、驱动器、抽盒和输入/输出模块(IOM)。其中每个组件都包含固件。某些固件版本取决于其他固件版本。要捕获有关存储阵列中所有固件版本的信息、请查看软件和固件清单。技术支持可以分析软件和固件清单以检测任何固件不匹配。

.步骤
. 从左侧面板中，选择菜单：Support[Support resources]。
. 向下滚动到*启动详细存储阵列信息*、然后选择*软件和固件清单*。
+
此时将在屏幕上显示软件和固件清单报告。

. 要保存软件和固件清单、请单击*保存*。
+
此文件将保存在浏览器的"Downloads"文件夹中、文件名为`firmware-inventory.txt`。

. 按照技术支持提供的说明将文件发送给他们。

:leveloffset: -1

= 收集诊断数据

:leveloffset: +1

[[IDe6eecdf55cf8b1abc9a9ce710f763f87]]
= 在 SANtricity System Manager 中手动收集支持数据

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```
您可以在一个文件中收集有关存储阵列的各种类型的清单、状态和性能数据。技术支持可以使用该文件进行故障排除和进一步分析。

.关于此任务

如果启用了 AutoSupport 功能，您还可以转到菜单：支持[AutoSupport]并选择*发送 AutoSupport 派单*来收集此数据。

一次只能运行一个收集操作。如果您尝试启动另一个操作、则会收到一条错误消息。

只有在技术支持要求时、才执行此操作。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择 * 收集支持数据 * 。
3. 单击 * 收集 * 。

   此文件将保存在浏览器的 "Downloads" 文件夹中，名为 `support-data.7z` 。如果磁盘架包含抽盒、则该磁盘架的诊断数据将归档在名为`try-component-state-capture.7z`的单独压缩文件中。

4. 按照技术支持提供的说明将文件发送给他们。

在 **SANtricity System Manager** 中收集配置数据

您可以从控制器保存RAID配置数据、其中包括卷组和磁盘池的所有数据。然后、您可以联系技术支持以获得恢复数据的帮助。

关于此任务

此任务介绍如何保存RAID配置数据库的当前状态。此数据是从控制器的RPA内存位置检索的。

`s配置数据功能可保存与用于保存storageArray dbmDatabase`的命令行界面命令相同的信息。

只有在Recovery Guru操作或技术支持指示时、才应执行此任务。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择 * 收集配置数据 * 。
3. 在对话框中、单击*收集*。

文件`configurationData-<arrayName>-<DateTime>.7z`将保存在浏览器的"Downloads"文件夹中。

4. 有关向技术支持发送文件以及将数据加载回系统的详细信息、请联系技术支持。

在 **SANtricity System Manager** 中检索恢复支持文件

技术支持可以使用恢复支持文件对问题进行故障排除。SANtricity系统管理器会自动保存这些文件。

开始之前

技术支持已请求您向他们发送其他文件以进行故障排除。

关于此任务

恢复支持文件包括以下类型的文件：

- 支持数据文件
- AutoSupport 历史记录
- AutoSupport 日志
- SAS/RLS诊断文件
- 恢复配置文件数据
- 数据库捕获文件

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择*检索恢复支持文件*。

   此时将显示一个对话框、其中列出了存储阵列收集的所有恢复支持文件。要查找特定文件、您可以对任意列进行排序、也可以在*筛选器*框中键入字符。

3. 选择一个文件、然后单击*下载*。

   此文件将保存在浏览器的"Downloads"文件夹中。

4. 如果需要保存其他文件、请重复上述步骤。
5. 单击 * 关闭 * 。
6. 按照技术支持提供的说明将文件发送给他们。

在 **SANtricity System Manager** 中检索跟踪缓冲区

您可以从控制器中检索跟踪缓冲区、并将文件发送给技术支持进行分析。

关于此任务

固件使用跟踪缓冲区来记录处理情况、尤其是可能对调试有用的异常情况。您可以在不中断存储阵列操作的情况下检索跟踪缓冲区、并且对性能的影响最小。

只有在技术支持要求时、才执行此操作。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择*检索跟踪缓冲区*。
3. 选中要检索跟踪缓冲区的每个控制器旁边的复选框。

   您可以选择一个或两个控制器。如果复选框右侧的控制器状态消息为失败或已禁用、则此复选框将被禁用。

4. 单击 * 是 * 。

   此文件将保存在浏览器的"Downloads"文件夹中、文件名为`trace-builes.7z`。

5. 按照技术支持提供的说明将文件发送给他们。

在 **SANtricity System Manager** 中收集 **I/O** 路径统计信息

您可以保存I/O路径统计信息文件并将其发送给技术支持进行分析。

关于此任务

技术支持使用I/O路径统计信息来帮助诊断性能问题。应用程序性能问题可能是由内存利用率、CPU利用率、网络延迟、I/O延迟或其他问题引起的。在收集支持数据期间、系统会自动收集I/O路径统计信息、您也可以手动收集这些信息。此外、如果启用了AutoSupport 、则会自动收集I/O路径统计信息并将其发送给技术支持。

确认要收集I/O路径统计信息后、I/O路径统计信息的计数器将重置。即使随后取消操作、计数器也会重置。控制器重置(重新启动)时、计数器也会重置。

只有在技术支持要求时、才执行此操作。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择*收集I/O路径统计信息*。
3. 键入`Collect`确认要执行此操作、然后单击*收集*。

   此文件将保存在浏览器的"Downloads"文件夹中、文件名为`io-path-statistics.7z`。

4. 按照技术支持提供的说明将文件发送给他们。

在 **SANtricity System Manager** 中检索健康图像

您可以查看控制器的运行状况映像。运行状况映像是指控制器处理器内存的原始数据转储、技术支持可使用该数据转储来诊断控制器的问题。

关于此任务

固件在检测到某些错误时会自动生成运行状况映像。生成运行状况映像后、出现错误的控制器将重新启动、并在事件日志中记录事件。

如果已打开AutoSupport 、则运行状况映像会自动发送到技术支持。如果未打开AutoSupport 、您需要联系技术支持、了解有关检索运行状况映像并将其发送给它们进行分析的说明。

只有在技术支持要求时、才执行此操作。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择*检索运行状况映像*。

   您可以在下载文件之前查看详细信息部分以查看运行状况映像的大小。

3. 单击 * 收集 * 。

   此文件将保存在浏览器的"Downloads"文件夹中、名称为`health-image.7z`。

4. 按照技术支持提供的说明将文件发送给他们。

执行恢复操作

查看 **SANtricity System Manager** 中不可读扇区日志

您可以保存无法读取的扇区日志并将文件发送给技术支持以进行分析。

关于此任务

无法读取的扇区日志包含因驱动器报告不可恢复的介质错误而导致的无法读取扇区的详细记录。在正常I/O期间以及在重建等修改操作期间检测到不可读扇区。如果在存储阵列上检测到不可读扇区、则会针对该存储阵列显示Need Attention警报。Recovery Guru可区分需要关注哪些无法读取的扇区状况。无法恢复不可读扇区中包含的任何数据、应将其视为丢失。

无法读取的扇区日志最多可存储1、000个无法读取的扇区。如果无法读取的扇区日志达到1、000个条目、则会满足以下条件：

- 如果在重建期间检测到新的不可读扇区、则重建将失败、并且不会记录任何条目。
- 对于在I/O期间检测到的新不可读扇区、I/O将失败、并且不会记录任何条目。

这些操作包括在溢出之前成功完成的RAID 5写入和RAID 6写入。

可能的数据丢失—从无法读取的扇区恢复是一种复杂的操作步骤 、可能涉及多种不同的方法。只有在技术支持要求时、才执行此操作。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择*查看/清除不可读扇区*。
3. 要保存无法读取的扇区日志、请执行以下操作：

   a. 在表的第一列中、您可以选择要保存不可读扇区日志的单个卷(单击每个卷旁边的复选框)、也可以选择所有卷(选中表标题中的复选框)。

      要查找特定卷、您可以对任意列进行排序、也可以在*筛选器*框中键入字符。

b. 单击 * 保存 * 。

此文件将保存在浏览器的"Downloads"文件夹中、名称为`irrored-扇 区.txt`。

4. 如果技术支持指示您清除无法读取的扇区日志、请执行以下步骤：
   a. 在表的第一列中、您可以选择要清除不可读扇区日志的单个卷(单击每个卷旁边的复选框)、也可以选择所有卷(选中表标题中的复选框)。
   b. 单击*清除*、然后确认要执行此操作。

在 **SANtricity System Manager** 中重新启用驱动器端口

您可以向控制器指示已采取更正操作、以便从连线错误情况中恢复。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。
2. 选择*重新启用驱动器端口*、然后确认要执行此操作。

   只有在存储阵列已禁用驱动器端口时、才会显示此选项。

   控制器会重新启用检测到连线错误时禁用的所有SAS端口。

SANtricity 软件中的清除恢复模式

还原存储阵列配置后、请使用"Clear Recovery Mode"操作恢复存储阵列上的I/O并将其恢复为正常操作。

开始之前

- 如果要将存储阵列恢复到先前的配置、则必须先从备份还原配置、然后再清除恢复模式。
- 您必须执行验证检查或与技术支持人员核实、以确保还原成功。确定还原成功后、可以清除恢复模式。

关于此任务

存储阵列包含一个配置数据库、其中包含其逻辑配置(池、卷组、卷等)的记录。如果您有意清除存储阵列配置或配置数据库损坏、则存储阵列将进入恢复模式。恢复模式会停止I/O并冻结配置数据库、这样您就有时间执行以下操作之一：

- 从存储在控制器闪存设备中的自动备份还原配置。为此、您必须联系技术支持。
- 从先前的"保存配置数据库"操作还原配置。保存配置数据库操作可通过命令行界面(CLI)执行。
- 从头开始重新配置存储阵列。

还原或重新定义存储阵列配置并确认一切正常后、您必须手动清除恢复模式。

> 清除恢复模式操作启动后、您将无法取消该操作。清除恢复模式可能需要很长时间。只有在技术支持要求时、才执行此操作。

步骤

1. 从左侧面板中，选择菜单：Support[Diagnostics]。

2. 选择*清除恢复模式*、然后确认要执行此操作。

   只有当存储阵列处于恢复模式时、才会显示此选项。

管理 AutoSupport

了解 E 系列的 AutoSupport

AutoSupport 功能可监控存储阵列的运行状况、并向技术支持发送自动派单。

技术支持会主动使用AutoSupport 数据来加快客户问题的诊断和解决速度、并主动检测和避免潜在问题。

AutoSupport 数据包括有关存储阵列的配置、状态、性能和系统事件的信息。AutoSupport 数据不包含任何用户数据。可以立即或按计划(每天和每周)发送派单。

主要优势

AutoSupport 功能的一些主要优势包括：

- 加快案例解决时间
- 复杂的监控功能、可加快意外事件管理速度
- 根据计划自动报告、并自动报告关键事件
- 自动为选定组件(例如驱动器)请求硬件更换
- 非侵入式警报、用于通知您出现问题并向技术支持提供信息以采取更正措施
- AutoSupport 分析工具、用于监控派单中是否存在已知配置问题

单个**AutoSupport** 功能

AutoSupport 功能由三个单独启用的功能组成。

- *基本AutoSupport *—允许存储阵列自动收集数据并将其发送给技术支持。
- * AutoSupport OnDemand *—允许技术支持在对问题描述 进行故障排除时根据需要请求重新传输先前的AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的重新传输请求并做出相应的响应。
- 远程诊断—允许技术支持在对问题描述 进行故障排除时根据需要请求新的最新AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的新请求并做出相应的响应。

AutoSupport 与收集支持数据之间的区别

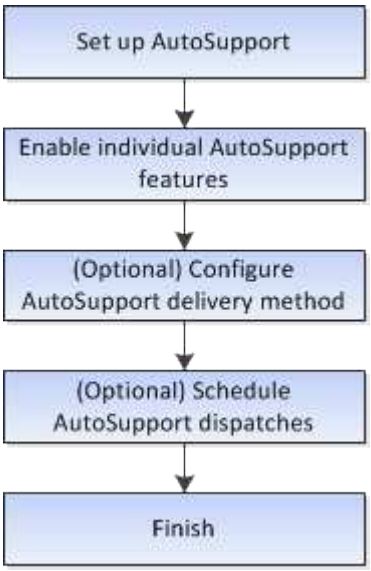
存储阵列中存在两种收集支持数据的方法：

- * AutoSupport 功能*—自动收集数据。
- 收集支持数据选项-必须手动收集和发送数据。

AutoSupport 功能更易于使用、因为数据会自动收集和发送。可以主动使用AutoSupport 数据、防止出现问题。AutoSupport 功能可以加快故障排除速度、因为技术支持已经可以访问数据。因此、AutoSupport 功能是首选的数据收集方法。

在 **SANtricity System Manager** 中配置 **AutoSupport**

在SANtricity 系统管理器中、您可以按照以下步骤配置AutoSupport 功能。



在 **SANtricity System Manager** 中启用或禁用 **AutoSupport** 功能

您可以在初始设置期间启用AutoSupport 功能和各个AutoSupport 功能、也可以稍后启用或禁用它们。

开始之前

如果要启用AutoSupport OnDemand或远程诊断、则AutoSupport 交付方法必须设置为HTTPS。

关于此任务

您可以随时禁用AutoSupport 功能、但强烈建议您保持启用状态。如果存储阵列出现问题、启用AutoSupport 功能可以显著加快确定和解决问题的速度。

AutoSupport 功能由三个单独启用的功能组成。

- *基本AutoSupport *—允许存储阵列自动收集数据并将其发送给技术支持。
- * AutoSupport OnDemand *—允许技术支持在对问题描述 进行故障排除时根据需要请求重新传输先前的AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的重新传输请求并做出相应的响应。
- 远程诊断—允许技术支持在对问题描述 进行故障排除时根据需要请求新的最新AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的新请求并做出相应的响应。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择*启用/禁用AutoSupport 功能*。
3. 选中要启用的AutoSupport 功能旁边的复选框。

   这些功能彼此相关、如对话框中各项的缩进所示。例如、您必须先启用AutoSupport OnDemand、然后才能

启用远程诊断。

4. 单击 * 保存 * 。

   如果禁用 AutoSupport，通知将显示在通知区域中，可通过窗口上角的铃铛图标访问。您可以通过单击 忽略来关闭通知。

在 **SANtricity System Manager** 中配置 **AutoSupport** 交付方法

AutoSupport功能支持使用HTTPS和SMTP协议向技术支持发送派单。

开始之前

- 必须启用AutoSupport 功能。您可以在AutoSupport 页面上查看它是否已启用。
- 必须在网络中安装和配置DNS服务器。必须在System Manager中配置DNS服务器地址(此任务可从硬件页面访问)。

关于此任务

查看不同的协议：

- * HTTPS *-允许您使用HTTPS直接连接到目标技术支持服务器。如果要启用AutoSupport OnDemand或远程诊断、则AutoSupport 交付方法必须设置为HTTPS。
- 电子邮件-用于使用电子邮件服务器作为发送AutoSupport 派单的传送方法。

> - HTTPS和电子邮件方法之间的差异*。使用SMTP的电子邮件传送方法与HTTPS传送方法有一些重要区别。首先、电子邮件方法的派单大小限制为5 MB、这意味着不会派送某些ASUP数据收集。其次、AutoSupport OnDemand功能仅适用于HTTPS交付方法。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择 * 配置 AutoSupport 交付方法 * 。

   此时将显示一个对话框、其中列出了派单交付方法。

3. 选择所需的交付方法、然后选择该交付方法的参数。执行以下操作之一：
   - 如果选择HTTPS、请选择以下交付参数之一：
     - 直接—此传送参数为默认选择。通过选择此选项、您可以使用HTTPS协议直接连接到目标技术支持系统。
     - 通过代理服务器-选择此选项可以指定与目标技术支持系统建立连接所需的HTTP代理服务器详细信息。您必须指定主机地址和端口号。但是、如果需要、您只需要输入主机身份验证详细信息(用户名和密码)。
     - 通过代理自动配置脚本**(PAC)**—指定代理自动配置(PAC)脚本文件的位置。通过PAC文件、系统可以自动选择适当的代理服务器、以便与目标技术支持系统建立连接。
   - 如果选择了电子邮件、请输入以下信息：
     - 作为完全限定域名、IPv4地址或IPv6地址的邮件服务器地址。
     - AutoSupport 派遣电子邮件的发件人字段中显示的电子邮件地址。

- 可选；如果要执行配置测试：AutoSupport 系统收到测试派单时发送确认的电子邮件地址。
- 如果要对消息进行加密、请选择* SMTPS 或 STARTTLS 作为加密类型、然后选择加密消息的端口号。否则、请选择*无。
- 如果需要、请输入用于向传出发件人和邮件服务器进行身份验证的用户名和密码。

4. 如果您的防火墙阻止了这些ASUP派单的交付、请将以下URL添加到您的白名单中：
`https://support.netapp.com/put/AsupPut/`
5. 单击*测试配置*、使用指定的传输参数测试与技术支持服务器的连接。如果启用了AutoSupport 按需功能、则系统还会测试AutoSupport 按需派单交付的连接。

   如果配置测试失败、请检查您的配置设置并重新运行测试。如果测试仍失败、请联系技术支持。

6. 单击 * 保存 * 。

在 **SANtricity System Manager** 中安排 **AutoSupport** 调度

SANtricity系统管理器会自动为AutoSupport派单创建默认计划。如果愿意、您可以指定自己的计划。

开始之前

必须启用AutoSupport 功能。您可以在AutoSupport 页面上查看它是否已启用。

关于此任务

- 每日时间-每天在您指定的时间范围内收集和发送派单。System Manager会在该范围内随机选择一个时间。所有时间均采用协调世界时(Coordinated Universal Time、UTC)、这可能与存储阵列的本地时间不同。您必须将存储阵列的本地时间转换为UTC时间。
- 每周日期-收集每周派单并每周发送一次。System Manager会从您指定的日期中随机选择一天。取消选择不希望每周派单发生的任何日期。System Manager会从允许的天数中随机选择一天。
- 每周时间-在您指定的时间范围内、每周收集并发送一次每周派单。System Manager会在该范围内随机选择一个时间。所有时间均采用协调世界时(Coordinated Universal Time、UTC)、这可能与存储阵列的本地时间不同。您必须将存储阵列的本地时间转换为UTC时间。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择*计划AutoSupport 派单*。

   此时将显示计划AutoSupport 卸载向导。

3. 按照向导中的步骤进行操作。

在 **SANtricity System Manager** 中发送 **AutoSupport** 调度

SANtricity系统管理器允许您将AutoSupport派单发送给技术支持、而无需等待计划的派单。

开始之前

必须启用AutoSupport 功能。您可以在AutoSupport 页面上查看它是否已启用。

关于此任务

此操作会收集支持数据并自动将其发送给技术支持、以便他们可以对问题进行故障排除。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择*发送AutoSupport 派遣*。

   此时将显示发送AutoSupport 派单对话框。

3. 选择*发送*确认操作。

在 **SANtricity System Manager** 中查看 **AutoSupport** 状态

AutoSupport 页面将显示AutoSupport 功能和各个AutoSupport 功能当前是否已启用。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 查看页面右侧选项卡下方、查看是否已启用基本AutoSupport 功能。
3. 将光标悬停在问号上方可查看是否已启用各个AutoSupport 功能。

在 **SANtricity System Manager** 中查看 **AutoSupport** 日志

AutoSupport 日志提供有关状态、派单历史记录以及在交付AutoSupport 派单期间遇到的错误的信息。

关于此任务

可以存在多个日志文件。当当前日志文件达到200 KB时、将对其进行归档并创建新的日志文件。归档的日志文件名称为`ASUPMessages。n`、其中_n_是一个介于1到9之间的整数。如果存在多个日志文件、您可以选择查看最新日志或先前的日志。

- 当前日志-显示最新捕获事件的列表。
- 归档日志-显示早期事件的列表。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择*查看AutoSupport 日志*。

   此时将显示一个对话框、其中列出了当前的AutoSupport 日志。

3. 如果要查看先前的AutoSupport 日志、请选择*已归档*单选按钮、然后从*选择AutoSupport 日志*下拉列表中选择一个日志。

   只有当存储阵列上存在归档日志时、才会显示归档选项。

   选定的AutoSupport 日志将显示在对话框中。

4. 可选：*要搜索**AutoSupport** 日志、请在*查找*框中键入一个术语、然后单击*查找。

再次单击*查找*可搜索此词的其他出现项。

在 **SANtricity System Manager** 中启用 **AutoSupport** 维护窗口

启用AutoSupport 维护窗口以禁止在发生错误事件时自动创建服务单。在正常操作模式下、如果存在问题描述 、存储阵列将使用AutoSupport 向支持部门创建案例。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择*启用AutoSupport 维护窗口*。
3. 输入电子邮件地址、以确认维护窗口请求已处理。

   根据您的配置、您最多可以输入五个电子邮件地址。如果要添加多个地址、请选择*添加其他电子邮件*以打开另一个字段。

4. 指定启用维护窗口的持续时间(以小时为单位)。

   支持的最长持续时间为72小时。

5. 单击 * 是 * 。

   在指定的持续时间窗口中、系统会暂时禁止在错误事件上自动创建AutoSupport 服务单。

完成后

只有在AutoSupport 服务器处理存储阵列的请求之后、维护窗口才会开始。请等待收到确认电子邮件、然后再对存储阵列执行任何维护活动。

在 **SANtricity System Manager** 中禁用 **AutoSupport** 维护窗口

禁用AutoSupport 维护窗口以允许在发生错误事件时自动创建服务单。禁用AutoSupport 维护窗口后、如果存在问题描述 、存储阵列将使用AutoSupport 向支持部门创建案例。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择*禁用AutoSupport 维护窗口*。
3. 输入电子邮件地址、以确认已处理禁用维护窗口请求。

   根据您的配置、您最多可以输入五个电子邮件地址。如果要添加多个地址、请选择*添加其他电子邮件*以打开另一个字段。

4. 单击 * 是 * 。

   已启用错误事件的AutoSupport 自动服务单创建。

完成后

只有在AutoSupport 服务器处理存储阵列的请求之后、维护窗口才会结束。请等待您收到确认电子邮件、然后再继续操作。

查看事件

了解 SANtricity 软件中的事件日志

事件日志提供存储阵列上发生的事件的历史记录、有助于技术支持对导致故障的事件进行故障排除。

您可以使用事件日志作为Recovery Guru的补充诊断工具来跟踪存储阵列事件。在尝试从存储阵列中的组件故障中恢复时、请始终先参考Recovery Guru。

事件类别

事件日志中的事件按不同的状态进行分类。需要对其采取操作的事件具有以下状态：

- 严重
- 警告

以下事件是信息性的、不需要立即采取任何措施：

- 信息性

严重事件

严重事件表示存储阵列存在问题。如果您立即解决此严重事件、则可能会防止数据访问丢失。

发生严重事件时、该事件会记录在事件日志中。所有严重事件都会发送到SNMP管理控制台或您配置为接收警报通知的电子邮件收件人。如果磁盘架ID在事件发生时未知、则磁盘架ID将列为"磁盘架未知"。

收到严重事件后、请参阅Recovery Guru操作步骤 以了解此严重事件的详细问题描述。完成Recovery Guru操作步骤 以更正严重事件。要更正某些关键事件、您可能需要联系技术支持。

使用 SANtricity System Manager 中的事件日志查看事件

您可以查看事件日志、其中提供了存储阵列上发生的事件的历史记录。

步骤

1. 从左侧面板中，选择菜单：Monitoring[Event log]。

   此时将显示"Event Log"页面。

   ▼ 页面详细信息

项目	Description
查看全部字段	在所有事件之间切换、仅在严重事件和警告事件之间切换。
筛选字段	筛选事件。仅用于显示与特定组件相关的事件、特定事件等
选择列图标。	用于选择其他要查看的列。其他列会提供有关事件的追加信息。
复选框	用于选择要保存的事件。表标题中的复选框将选择所有事件。

项目	Description
日期/时间列	事件的日期和时间戳、具体取决于控制器时钟。 事件日志最初会根据序列号对事件进行排序。通常、此序列对应于日期和时间。但是、存储阵列中的两个控制器时钟可能不同步。在这种情况下、事件日志中可能会出现与事件以及显示的日期和时间相关的一些可感知的不一致情况。
优先级列	存在以下优先级值： • 严重—存储阵列存在问题。但是、如果您立即采取措施、则可能会防止丢失对数据的访问。严重事件用于发出警报通知。所有严重事件都将通过SNMP陷阱发送到任何网络管理客户端或您配置的电子邮件收件人。 • 警告—发生错误、导致存储阵列的性能和从其他错误中恢复的能力下降。 • 信息—与存储阵列相关的非关键信息。
组件类型列	受事件影响的组件。组件可以是硬件、例如驱动器或控制器、也可以是软件、例如控制器固件。
组件位置列	组件在存储阵列中的物理位置。
问题描述 列	事件的问题描述。 示例-D写入失败-重试已用尽
序列号列	一个64位编号、用于唯一标识存储阵列的特定日志条目。此数字会随每个新事件日志条目递增一个。要显示此信息、请单击*选择列*图标。
事件类型列	一个4位数的数字、用于标识每种类型的已记录事件。要显示此信息、请单击*选择列*图标。
事件特定代码列	此信息由技术支持使用。要显示此信息、请单击*选择列*图标。
事件类别列	• "故障"—存储阵列中的某个组件出现故障、例如驱动器故障或电池故障。 • 状态更改*—存储阵列中状态发生更改的元素；例如、卷过渡到最佳状态或控制器过渡到脱机状态。 • "内部"–不需要用户操作的内部控制器操作；例如、控制器已完成每日开始。 • "*命令"—已向存储阵列发出的命令；例如、已分配热备用磁盘。 • "#Error*–在存储阵列上检测到错误情况；例如、控制器无法同步和清除缓存、或者在存储阵列上检测到冗余错误。 • 常规—不适合任何其他类别的任何事件。要显示此信息、请单击"**选择列"*图标。
Logged by列	记录事件的控制器的名称。要显示此信息、请单击"**选择列"*图标。

2. 要从存储阵列检索新事件、请单击"刷新"。

   可能需要几分钟的时间、才能记录事件并在事件日志页面中显示。

3. 将事件日志保存到文件：

a. 选中要保存的每个事件旁边的复选框。

b. 单击 * 保存 * 。

此文件将保存在浏览器的"Downloads"文件夹中、名称为`major-event-log-timestamp.log`。

4. 要从事件日志中清除事件、请执行以下操作：

事件日志会先存储大约8、000个事件、然后再将事件替换为新事件。如果要保留事件、可以保存这些事件并从事件日志中清除它们。

a. 首先、保存事件日志。

b. 单击*全部清除*、然后确认您要执行此操作。

管理升级

了解如何升级**SANtricity**软件

使用升级中心下载最新软件和固件，并升级控制器和驱动器。

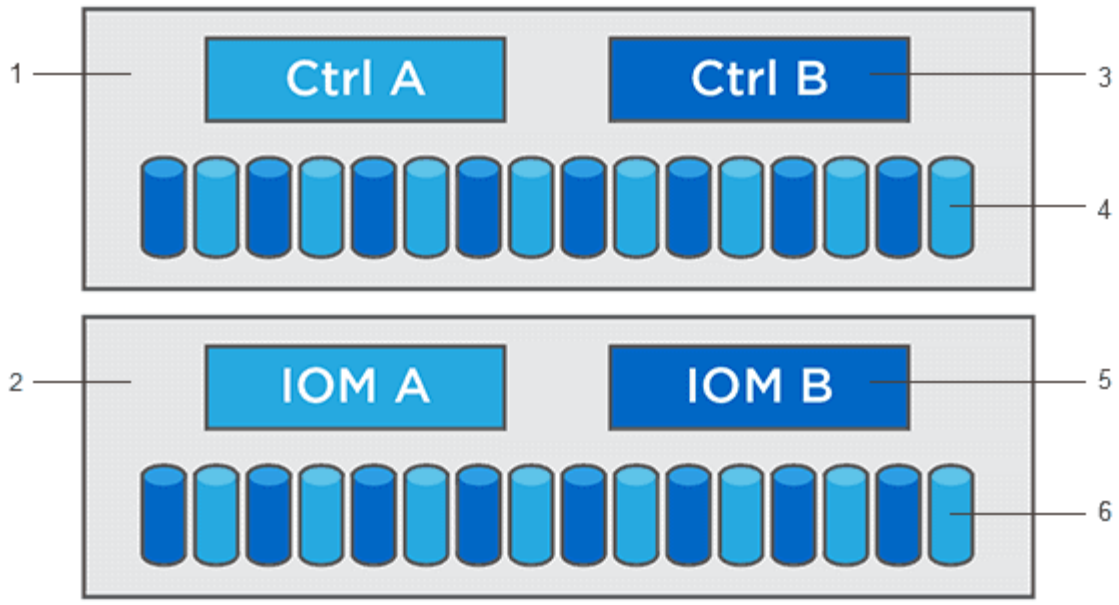
控制器升级概述

您可以升级存储阵列的软件和固件以获得所有最新功能和错误修复。

操作系统控制器升级中包含的组件

多个存储阵列组件包含您可能偶尔需要升级的软件或硬件。

- 管理软件—System Manager是用于管理存储阵列的软件。
- * 控制器固件 * —控制器固件用于管理主机和卷之间的 I/O 。
- * 控制器 NVSRA* - 控制器 NVSRAM 是一个控制器文件，用于指定控制器的默认设置。
- * IOM 固件 * — I/O 模块（ IOM ）固件用于管理控制器与驱动器架之间的连接。它还会监控组件的状态。
- * 监控软件 * —监控软件是运行该软件的控制器上的虚拟机。



[1]控制器架；[2]驱动器架；[3]软件、控制器固件、控制器NVSRAM、 监控软件；[4]驱动器固件；[5] IOM固件；[6]驱动器固件

您可以在软件和固件清单页面上查看当前的软件和固件版本。转到菜单：Support[升级中心]，然后单击*软件和固件清单*的链接。

在升级过程中、可能还需要升级主机的多路径/故障转移驱动程序和/或HBA驱动程序、以便主机可以正确地与控制器进行交互。要确定是否发生这种情况、请参见 "NetApp互操作性表工具"。

何时停止I/O

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、控制器A会将其所有卷故障转移到控制器B、升级、收回其卷和控制器B的所有卷、然后升级控制器B

升级前运行状况检查

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进行。以下情况可能会阻止升级：

- 已分配的驱动器出现故障
- 正在使用热备件
- 卷组不完整
- 正在运行排他操作
- 缺少卷
- 控制器处于非最佳状态
- 事件日志事件数量过多
- 配置数据库验证失败
- 使用旧版 DAC 存储的驱动器

您也可以单独运行升级前运行状况检查，而无需执行升级。

驱动器固件控制驱动器的低级操作特征。驱动器制造商会定期发布驱动器固件更新、以添加新功能、提高性能并修复缺陷。

联机和脱机驱动器固件升级

驱动器固件升级方法有两种：联机和脱机。

联机

在联机升级期间，驱动器会按顺序升级，一次升级一个。升级期间，存储阵列将继续处理 I/O 。您不必停止 I/O 如果驱动器可以执行联机升级，则会自动使用联机方法。

可以执行联机升级的驱动器包括：

- 最佳池中的驱动器
- 最佳冗余卷组（ RAID 1 ， RAID 5 和 RAID 6 ）中的驱动器
- 未分配的驱动器
- 备用热备用驱动器

执行联机驱动器固件升级可能需要几个小时，从而使存储阵列面临潜在的卷故障。在以下情况下，可能会发生卷故障：

- 在 RAID 1 或 RAID 5 卷组中，在升级卷组中的另一个驱动器时，一个驱动器发生故障。
- 在 RAID 6 池或卷组中，升级池或卷组中的另一个驱动器时，两个驱动器发生故障。

脱机(并行)

在脱机升级期间，同一驱动器类型的所有驱动器都会同时升级。此方法需要停止与选定驱动器关联的卷的 I/O 活动。由于多个驱动器可以同时（并行）升级，因此整体停机时间会显著减少。如果驱动器只能执行脱机升级，则会自动使用脱机方法。

以下驱动器必须使用脱机方法：

- 非冗余卷组中的驱动器（ RAID 0 ）
- 非最佳池或卷组中的驱动器
- SSD 缓存中的驱动器

兼容性

每个驱动器固件文件都包含有关运行固件的驱动器类型的信息。您只能将指定的固件文件下载到兼容驱动器。System Manager 会在升级过程中自动检查兼容性。

在 **SANtricity System Manager** 中升级控制器软件和固件

您可以升级存储阵列的软件以及IOM固件和非易失性静态随机存取存储器(NVSRAM)(可选)、以确保您具有所有最新功能并修复了错误。

开始之前

- 您知道是否要升级IOM固件。

  通常，您应同时升级所有组件。但是，如果您不希望在 SANtricity OS 软件升级过程中升级 IOM 固件，或者技术支持已指示您降级 IOM 固件（您只能使用命令行界面降级固件），则可能决定不升级 IOM 固件。

- 您知道是否要升级控制器NVSRAM文件。

  通常，您应同时升级所有组件。但是，如果您的文件已修补或为自定义版本，并且您不想覆盖此文件，则您可能会决定不升级控制器 NVSRAM 文件。

- 您知道是要立即激活操作系统升级还是稍后激活。

  稍后激活的原因可能包括：

  - 当前时间—激活软件和固件可能需要很长时间、因此您可能需要等待I/O负载减轻。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软件和固件，然后再升级其他存储阵列上的文件。

- 您知道是要从不安全的驱动器还是内部安全的驱动器切换、以使用外部密钥管理服务器(KMS)来保护驱动器的安全。
- 您知道是否要在存储阵列中使用基于角色的访问控制。

关于此任务

您可以选择仅升级操作系统软件文件或仅升级控制器NVSRAM文件、也可以选择同时升级这两个文件。

只有在技术支持要求时、才执行此操作。



- 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您未安装多路径驱动程序，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. 从左侧面板中，选择菜单：Support[Upgrade center]。
3. 将新文件从支持站点下载到您的管理客户端。

   a. 单击* NetApp支持*以启动支持网站。
   b. 在支持网站上、单击*下载*选项卡、然后选择*下载*。
   c. 选择* E系列SANtricity 操作系统控制器软件*。
   d. 按照其余说明进行操作。

   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。

4. 如果此时需要更改 IOM 固件行为，请单击*配置 IOM 自动同步*。

   如果存储阵列具有一个控制器，则不会升级 IOM 固件。

5. 在 SANtricity 操作系统软件升级下，单击*开始 SANtricity 操作系统软件升级*。

   此时将显示升级 SANtricity OS 软件页面。

6. 选择一个或多个文件以开始升级过程：

   a. 通过单击 **Browse** 并导航到您从支持网站下载的操作系统软件文件，选择 SANtricity 操作系统软件文件。

   b. 单击 * 浏览 * 并导航到从支持站点下载的 NVSRAM 文件，以选择控制器 NVSRAM 文件。控制器 NVSRAM 文件的文件名类似于 `N2800-830000-000.DLP` 。

      执行以下操作：

      - 默认情况下，仅显示与当前存储阵列配置兼容的文件。
      - 选择要升级的文件时，将显示该文件的名称和大小。

7. 可选： 如果您选择了要升级的 SANtricity 操作系统软件文件，您可以通过选中*立即传输文件，但不启动升级（稍后激活）* 复选框，将文件传输到控制器而无需激活它们。

8. 单击 * 开始 * ，然后确认您要执行此操作。

   您可以在升级前运行状况检查期间取消此操作，但不能在传输或激活期间取消此操作。

9. 可选： 要查看已升级内容的列表，请单击 **Save log**。

   此文件将保存在浏览器的 "Downloads" 文件夹中，名为 `drive_upgrade_log-timestamp.txt` 。

完成后

- 验证所有组件是否均显示在硬件页面上。
- 通过检查软件和固件清单页面来验证新的软件和固件版本（转到菜单：支持[升级中心]，然后单击*软件和固件清单*的链接）。
- 如果您升级了控制器 NVSRAM ，则在激活过程中，应用于现有 NVSRAM 的任何自定义设置都将丢失。激活过程完成后，您需要再次将自定义设置应用于 NVSRAM 。

在 **SANtricity System Manager** 中激活控制器软件和固件

您可以选择立即激活升级文件、也可以等到更方便的时间再激活。

关于此任务

您可以下载和传输这些文件、而无需激活它们。您可以选择稍后激活，原因如下：

- 当前时间—激活软件和固件可能需要很长时间、因此您可能需要等待I/O负载减轻。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软件和固件，然后再升级其他存储阵列上的文件。

当您的软件或固件已传输但未激活时，您可以在通知区域（通过窗口上角的铃铛图标访问）和升级中心页面上看到通知。



激活过程启动后，您无法停止它。

步骤

1. 从左侧面板中，选择菜单：Support[Upgrade center]。
2. 在标记为 SANtricity 操作系统软件升级的区域中，单击 激活分阶段升级，并确认要执行此操作。

   您可以在升级前运行状况检查期间取消此操作、但不能在激活期间取消。

   升级前运行状况检查将开始。如果升级前运行状况检查通过、则升级过程将继续激活文件。如果升级前运行状况检查失败，请使用 Recovery Guru 或联系技术支持以解决此问题。对于某些类型的情况、技术支持可能会建议您通过选中*允许升级*复选框来继续升级、尽管存在错误。

   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： 要查看已升级内容的列表，请单击 **Save log**。

   此文件将保存在浏览器的 "Downloads" 文件夹中，名为 `drive_upgrade_log-timestamp.txt` 。

完成后

- 验证所有组件是否均显示在硬件页面上。
- 通过检查软件和固件清单页面来验证新的软件和固件版本（转到菜单：支持[升级中心]，然后单击*软件和固件清单*的链接）。
- 如果您升级了控制器 NVSRAM ，则在激活过程中，应用于现有 NVSRAM 的任何自定义设置都将丢失。激活过程完成后，您需要再次将自定义设置应用于 NVSRAM 。

在 **SANtricity System Manager** 中升级驱动器固件

您可以升级驱动器固件、以确保具有所有最新功能和错误修复。

开始之前

- 您已使用磁盘到磁盘备份、卷副本(复制到不受计划的固件升级影响的卷组)或远程镜像备份数据。
- 存储阵列处于最佳状态。
- 所有驱动器均处于最佳状态。
- 存储阵列上未运行任何配置更改。
- 如果驱动器只能脱机升级、则与驱动器关联的所有卷的I/O活动将停止。

步骤

1. 从左侧面板中，选择菜单：Support[Upgrade center]。
2. 将新文件从支持站点下载到您的管理客户端。
3. 在驱动器固件升级下，单击 **Begin drive firmware upgrade**。

   此时将显示升级驱动器固件页面，其中列出了当前正在使用的驱动器固件文件。

4. 提取（解压缩）从支持站点下载的文件。
5. 单击 * 浏览 * ，然后选择从支持站点下载的新驱动器固件文件。

   驱动器固件文件的文件名类似于 `D HUC101212CS600_30602291_MS01_2800_0002` ，扩展名为 ` 。 lp` 。

您最多可以选择四个驱动器固件文件，一次一个。如果多个驱动器固件文件与同一驱动器兼容，则会收到文件冲突错误。确定要用于升级的驱动器固件文件，然后删除另一个驱动器固件文件。

6. 单击 * 下一步 * 。

   此时将显示*选择驱动器*步骤，其中列出了可使用选定文件升级的驱动器。

   仅显示兼容的驱动器。

   为驱动器选择的固件将显示在建议的固件信息区域中。如果必须更改固件，请单击 * 返回 * 以返回上一个对话框。

7. 选择要执行的升级类型：

   - **Upgrade all drives online** — 显示可在存储阵列处理 I/O 时支持固件下载的驱动器。选择此升级方法时，无需停止使用这些驱动器对关联卷的 I/O。在存储阵列处理这些驱动器的 I/O 时，这些驱动器会逐个升级。
   - 离线升级所有驱动器（并行） — 仅在使用驱动器的任何卷上停止所有 I/O 活动时显示可以支持固件下载的驱动器。选择此升级方法时，必须停止使用要升级的驱动器的任何卷上的所有 I/O 活动。没有冗余的驱动器必须作为离线操作处理。此要求包括与 SSD 缓存、RAID 0 卷组或任何已降级的池或卷组关联的任何驱动器。离线（并行）升级通常比在线方法更快。

8. 在表的第一列中，选择要升级的一个或多个驱动器。
9. 单击 * 开始 * ，然后确认您要执行此操作。

   如果需要停止升级，请单击 * 停止 * 。当前正在进行的所有固件下载均已完成。已取消所有尚未启动的固件下载。

   停止驱动器固件升级可能会导致数据丢失或驱动器不可用。

10. 可选： 要查看已升级内容的列表，请单击 **Save log**。

    此文件将保存在浏览器的 "Downloads" 文件夹中，名为 `drive_upgrade_log-timestamp.txt` 。

11. 如果在升级操作步骤期间出现以下任何错误，请采取适当的建议操作。

▼ 错误和建议的操作

如果遇到此固件下载错误 ...	然后执行以下操作 ...
已分配的驱动器出现故障	出现此故障的一个原因可能是驱动器没有相应的签名。确保受影响的驱动器为授权驱动器。有关详细信息，请联系技术支持。 更换驱动器时，请确保更换驱动器的容量等于或大于要更换的故障驱动器。 您可以在存储阵列接收 I/O 时更换故障驱动器
检查存储阵列	• 确保已为每个控制器分配 IP 地址。 • 确保连接到控制器的所有缆线均未损坏。 • 确保所有缆线均已紧密连接。

如果遇到此固件下载错误 ...	然后执行以下操作 ...
集成热备用驱动器	必须先更正此错误情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
卷组不完整	如果一个或多个卷组或磁盘池不完整，则必须更正此错误情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
当前在任何卷组上运行的排他操作\(后台介质/奇偶校验扫描除外)	如果正在执行一个或多个独占操作，则必须先完成这些操作，然后才能升级固件。使用 System Manager 监控操作进度。
缺少卷	您必须先更正缺少的卷情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
任一控制器处于非最佳状态	其中一个存储阵列控制器需要注意。必须先更正此情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
控制器对象图形之间的存储分区信息不匹配	验证控制器上的数据时出错。请联系技术支持以解决此问题描述。
SPM 验证数据库控制器检查失败	控制器上发生存储分区映射数据库错误。请联系技术支持以解决此问题描述。
配置数据库验证(如果存储阵列的控制器版本支持)	控制器上发生配置数据库错误。请联系技术支持以解决此问题描述。
与 Mel 相关的检查	请联系技术支持以解决此问题描述。
过去 7 天报告了 10 个以上的 DDN 信息性或严重 MEL 事件	请联系技术支持以解决此问题描述。
过去 7 天报告了超过 2 页 2C 的严重 MEL 事件	请联系技术支持以解决此问题描述。
过去 7 天报告了 2 个以上的 " 降级驱动器通道 " 严重 MEL 事件	请联系技术支持以解决此问题描述。
过去 7 天内超过 4 个关键 MEL 条目	请联系技术支持以解决此问题描述。

完成后

驱动器固件升级已完成。您可以恢复正常操作。

了解 **SANtricity** 软件和固件升级错误

在控制器软件升级或驱动器固件升级期间可能会发生错误。

固件下载错误	**Description**	建议的操作
已分配的驱动器出现故障	无法升级存储阵列中已分配的驱动器。	出现此故障的一个原因可能是驱动器没有相应的签名。确保受影响的驱动器为授权驱动器。有关详细信息，请联系技术支持。 更换驱动器时，请确保更换驱动器的容量等于或大于要更换的故障驱动器。 您可以在存储阵列接收 I/O 时更换故障驱动器
集成热备用驱动器	如果此驱动器标记为热备用磁盘、并且正在用于卷组、则固件升级过程将失败。	必须先更正此错误情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
卷组不完整	如果卷组中的任何驱动器被绕过、删除或无响应、则会将其视为不完整的卷组。不完整的卷组将阻止固件升级。	如果一个或多个卷组或磁盘池不完整，则必须更正此错误情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
当前在任何卷组上运行的独占操作（后台介质 / 奇偶校验扫描除外）	如果正在对卷执行任何独占操作、则无法升级固件。	如果正在执行一个或多个独占操作，则必须先完成这些操作，然后才能升级固件。使用 System Manager 监控操作进度。
缺少卷	如果缺少任何卷、则无法升级固件。	您必须先更正缺少的卷情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
任一控制器处于非最佳状态	如果任一控制器处于非最佳状态、则无法升级固件。	其中一个存储阵列控制器需要注意。必须先更正此情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
SPM 验证数据库控制器检查失败	无法升级固件、因为存储分区映射数据库已损坏。	控制器上发生存储分区映射数据库错误。请联系技术支持以解决此问题描述。
配置数据库验证(如果存储阵列的控制器版本支持)	无法升级固件、因为配置数据库已损坏。	控制器上发生配置数据库错误。请联系技术支持以解决此问题描述。
与 Mel 相关的检查	无法升级固件、因为事件日志包含错误。	请联系技术支持以解决此问题描述。
过去 7 天报告了 10 个以上的 DDN 信息性或严重 MEL 事件	无法升级固件、因为过去七天报告的信息性或严重MEL事件超过10个。	请联系技术支持以解决此问题描述。
过去 7 天报告了超过 2 页 2C 的严重 MEL 事件	无法升级固件、因为过去七天报告的关键MEL事件超过两页2 C。	请联系技术支持以解决此问题描述。
过去 7 天报告了 2 个以上的 " 降级驱动器通道 " 严重 MEL 事件	无法升级固件、因为过去七天报告了两个以上降级驱动器通道严重MEL事件。	请联系技术支持以解决此问题描述。
过去 7 天内超过 4 个关键 MEL 条目	无法升级固件、因为过去七天报告的严重事件日志条目超过四个。	请联系技术支持以解决此问题描述。

固件下载错误	**Description**	建议的操作
需要有效的管理IP地址。	要执行此操作、需要有效的控制器IP地址。	请联系技术支持以解决此问题描述。
此命令要求为每个控制器提供一个活动管理IP地址。	此操作需要为与存储阵列关联的每个控制器提供一个控制器IP地址。	请联系技术支持以解决此问题描述。
返回未处理的下载文件类型。	不支持指定的下载文件。	请联系技术支持以解决此问题描述。
固件下载上传操作步骤 期间发生错误。	固件下载失败、因为控制器无法处理此请求。验证存储阵列是否处于最佳状态、然后重试此操作。	如果验证存储阵列是否为最佳阵列后再次出现此错误、请联系技术支持以解决此问题描述。
固件激活操作步骤 期间发生错误。	固件激活失败、因为控制器无法处理此请求。验证存储阵列是否处于最佳状态、然后重试此操作。	如果验证存储阵列是否为最佳阵列后再次出现此错误、请联系技术支持以解决此问题描述。
等待控制器\ {0} 重新启动时已超时。	重新启动后、管理软件无法重新连接到控制器\ {0} 。验证存储阵列是否具有可操作的连接路径、如果此操作未成功完成、请重试此操作。	如果验证存储阵列是否为最佳阵列后再次出现此错误、请联系技术支持以解决此问题描述。

您可以使用System Manager中的Recovery Guru来更正其中某些情况。但是、在某些情况下、您可能需要联系技术支持。有关最新控制器固件下载的信息、请访问存储阵列。此信息有助于技术支持了解阻止固件升级和下载的错误情况。

使用脚本编辑器

使用 Script 编辑器创建或编辑脚本文件，将脚本文件保存到存储管理站的本地磁盘，或从磁盘加载脚本文件。

开始之前

脚本编辑器与存储阵列通信，以启用脚本语法检查和命令执行。键入到脚本编辑器中的脚本命令通常在存储阵列上运行。

脚本编辑器在窗口中提供两个视图：

- 编辑器窗格 – 提供用于输入或编辑脚本命令的区域。
- 输出窗格 – 显示验证或执行结果。拆分栏在编辑器窗格和输出窗格之间划分窗口。
- 脚本编辑器不支持需要输入文件的命令，例如控制器固件、NVSRAM 或驱动器固件升级。
- 脚本编辑器支持生成输出文件的命令。
- 有一些命令需要在客户端执行（客户端命令）。
  - 此版本唯一支持的客户端命令是 `on error stop` 和 `on error continue`。
  - 如果尝试运行任何其他客户端命令，脚本编辑器会生成错误。

打开脚本编辑器

步骤

1. 从左侧面板中，选择菜单：Support[Script editor]。

   下表列出了脚本编辑器中可用的文件选项：

   ▼ 字段详细信息

任务	Action
打开新脚本	a. 单击 **Load script file** 将现有脚本文件上传到 Script editor。 脚本编辑器在编辑器窗格中打开选定的脚本文件。
验证脚本命令语法	a. 单击 **Syntax check** 以验证编辑器窗格中当前脚本的语法。 Script 编辑器一次一行地解析脚本文件中的语句，并验证它们的语法是否正确。任何语法错误都会出现在输出窗格中，该窗格会报告错误的行号和错误说明。 如果脚本编辑器遇到语法错误，则不会对脚本执行进一步的语法验证。 修复任何语法错误，然后重新运行 **Syntax Check** 以验证错误更正并检查脚本中的其余语句。
执行脚本	a. 单击 **Execute Script** 在编辑器窗格中运行当前脚本。 脚本编辑器启动语法检查操作，然后对输入文件中的每个脚本命令，在存储阵列控制器上运行命令执行。 如果 Script 编辑器遇到语法错误，则会停止执行并显示错误消息。 修复错误，然后重新运行 **Syntax check** 以验证错误更正。 ⓘ 如果发生执行错误，脚本可能无法继续执行，具体取决于包含的 `On Error`脚本语句。 `On Error Stop`语句在遇到执行错误时会停止脚本。 `On Error Continue`语句允许脚本在遇到执行错误后继续运行。此语句是默认设置。
编辑现有脚本	a. 单击 **Load script file** 将现有脚本文件上传到 Script editor。 b. 在编辑器窗格中，对脚本进行任何必要的更改。
将脚本保存到本地文件	a. 单击 **Save script file** 将脚本窗格中的更改下载为新的脚本文件。
清除 Script editor 编辑器窗格中的文本	a. 单击 **Clear editor** 可清除编辑器窗格中的文本。
将输出结果保存到本地文件	a. 单击 **Save results** 将输出窗格的内容下载为新文件。

在脚本编辑器中编写脚本

开始之前

使用脚本编辑器编写脚本命令时，请确保遵循以下准则： * 以分号 (;) 结束所有语句。* 用空格分隔每个基本命令及其相关的主参数和辅助参数。* 在脚本编辑器中输入参数时，不区分大小写。* 将每个语句放在单独的一行。* 向脚本添加注释，以便您和未来的用户更容易理解命令语句的目的。

步骤

1. 用字符 `/*和 `*/`包围多行注释。

   如果脚本引擎未找到开始注释符号和结束注释符号，则会出现错误消息，脚本执行将终止。

2. 以两个正斜杠 (`//` 开始单行注释，并以行尾字符结尾，您可以按 **Enter** 插入行尾字符。

   如果脚本引擎在处理注释后未在脚本中找到行尾字符，则会显示错误消息，并终止脚本执行。

   当注释放置在脚本末尾，而您忘记按 **Enter** 时，通常会出现此错误。

3. 使用 `show` 语句将注释嵌入脚本中，这些注释将在脚本执行期间显示在编辑器窗格中。

   该 `show`语句对于调试脚本非常有用。

   在脚本中包含 `show setting controller mode`语句会导致在脚本执行期间处理此行时输出窗格中出现以下行：

   ```
   setting controller mode
   ```

解读脚本执行结果

在脚本执行期间，消息出现在输出窗格中，开头为：

```
Executing script...
```

如果在解析阶段发生错误，则该错误将显示在输出窗格中，该窗格提供行号和列号以及语法错误的描述。以下是语法错误消息的示例。

如果在脚本中键入以下语句：

```
set controller[a] mod = passive;
```

输出窗格显示生成的语法错误，如下所示：

```
Encountered "mod" at line 2, column 19
Was expecting one of...
"mode"...
"availability"...
"NVSRAMbyte"...
```

如果在脚本执行过程中发生错误，输出窗格中会显示一条消息，指出命令失败并报告错误说明。

例如，如果在脚本中键入以下语句：

```
set volume [three] userLabel="OneOne";
```

由此产生的错误出现在以下输出窗格中。此命令无法发送到存储阵列，因为它处于无响应状态。

```
Unable to change the volume user label using the Set Volume command at
line 1
Error - 1 - Could not communicate with the storage array to complete this
request.
```

某些执行错误，包括无法与存储阵列通信，总是会导致脚本执行停止。在这些情况下，即使使用 `On Error Continue` 语句，执行也会停止。

结果

执行脚本后，请查看输出窗格以检查成功或错误。

SANtricity System Manager 的 AutoSupport 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。

我正在收集哪些数据?

通过AutoSupport 功能和手动支持数据收集功能、可以在客户支持包中收集数据、以便由技术支持进行远程故障排除和问题分析。

客户支持包会将有关存储阵列的所有类型的信息收集到一个压缩文件中。收集的信息包括物理配置、逻辑配置、版本信息、事件、日志文件、 和性能数据。只有技术支持才会使用此信息来解决存储阵列的问题。

无法读取的扇区数据显示了什么?

您可以显示有关在存储阵列中的驱动器上检测到的不可读扇区的详细数据。

不可读扇区日志首先显示最新的不可读扇区。此日志包含有关包含不可读扇区的卷的以下信息。这些字段可排序。

字段	Description
受影响的卷	显示卷的标签。如果缺少的卷包含无法读取的扇区、则会为缺少的卷显示全球通用标识符。
逻辑单元号(LUN)	显示卷的LUN。如果卷没有LUN、则对话框将显示不适用。
已分配给	显示有权访问卷的主机或主机集群。如果主机、主机集群甚至默认集群无法访问此卷、则此对话框将显示不适用。

要查看有关无法读取的扇区的追加信息 、请单击卷旁边的加号(+)。

字段	Description
日期/时间	显示检测到不可读扇区的日期和时间。
卷逻辑块地址	显示了卷的逻辑块地址(LBA)。
驱动器位置	显示了驱动器架、抽盒(如果驱动器架具有抽盒)和托架位置。

字段	Description
驱动器逻辑块地址	显示了驱动器的LBA。
故障类型	显示了以下故障类型之一： • 物理—物理介质错误。 • 逻辑—条带中其他位置出现读取错误、导致数据不可读。例如、由于卷中其他位置出现介质错误而导致的扇区不可读。 • 不一致—冗余数据不一致。 • 数据保证-数据保证错误。

什么是运行状况映像?

运行状况映像是指控制器处理器内存的原始数据转储、技术支持可使用该数据转储来诊断控制器的问题。

固件在检测到某些错误时会自动生成运行状况映像。在某些故障排除情形下、技术支持可能会要求您检索运行状况映像文件并将其发送给它们。

AutoSupport 功能的作用是什么?

AutoSupport 功能由三个单独启用的功能组成。

- *基本AutoSupport *—允许存储阵列自动收集数据并将其发送给技术支持。
- * AutoSupport OnDemand *—允许技术支持在对问题描述 进行故障排除时根据需要请求重新传输先前的AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的重新传输请求并做出相应的响应。
- 远程诊断—允许技术支持在对问题描述 进行故障排除时根据需要请求新的最新AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的新请求并做出相应的响应。

通过**AutoSupport** 功能收集哪种类型的数据?

AutoSupport 功能包含三种标准派单类型：事件派单、计划派单以及按需和远程诊断派单。

AutoSupport 数据不包含任何用户数据。

- 事件派单

  如果系统上发生需要主动通知技术支持的事件、则AutoSupport 功能会自动发送事件触发的派单。

  - 受管存储阵列上发生支持事件时发送。
  - 包括有关事件发生时存储阵列所发生情况的全面快照。
- 计划内派单

  AutoSupport 功能会定期自动发送多个派单。

  - 每日派单—在用户可配置的时间间隔内每天发送一次。包括当前系统事件日志和性能数据。

- 每周派单—在用户可配置的时间间隔和日期内每周发送一次。包括配置和系统状态信息。

- * AutoSupport OnDemand和远程诊断派单*
  - * AutoSupport OnDemand *—允许技术支持在对问题描述 进行故障排除时根据需要请求重新传输先前的AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的重新传输请求并做出相应的响应。
  - 远程诊断—允许技术支持在对问题描述 进行故障排除时根据需要请求新的最新AutoSupport 派单。所有传输均从存储阵列启动、而不是从AutoSupport 服务器启动。存储阵列会定期与AutoSupport 服务器进行检查、以确定是否存在任何待处理的新请求并做出相应的响应。

如何配置**AutoSupport** 功能的交付方法?

AutoSupport功能支持使用HTTPS和SMTP协议将AutoSupport派单发送给技术支持。

开始之前

- 必须启用AutoSupport 功能。您可以在AutoSupport 页面上查看它是否已启用。
- 必须在网络中安装和配置DNS服务器。必须在System Manager中配置DNS服务器地址(此任务可从硬件页面访问)。

关于此任务

查看不同的协议：

- * HTTPS *-允许您使用HTTPS直接连接到目标技术支持服务器。如果要启用AutoSupport OnDemand或远程诊断、则AutoSupport 交付方法必须设置为HTTPS。
- 电子邮件-用于使用电子邮件服务器作为发送AutoSupport 派单的传送方法。



- HTTPS和电子邮件方法之间的差异*。使用SMTP的电子邮件传送方法与HTTPS传送方法有一些重要区别。首先、电子邮件方法的派单大小限制为5 MB、这意味着不会派送某些ASUP数据收集。其次、AutoSupport OnDemand功能仅适用于HTTPS交付方法。

步骤

1. 从左侧面板中，选择菜单：支持[AutoSupport]。
2. 选择 * 配置 AutoSupport 交付方法 * 。

   此时将显示一个对话框、其中列出了派单交付方法。

3. 选择所需的交付方法、然后选择该交付方法的参数。执行以下操作之一：
   - 如果选择HTTPS、请选择以下交付参数之一：
     - 直接—此传送参数为默认选择。通过选择此选项、您可以使用HTTPS协议直接连接到目标技术支持系统。
     - 通过代理服务器-选择此选项可以指定与目标技术支持系统建立连接所需的HTTP代理服务器详细信息。您必须指定主机地址和端口号。但是、如果需要、您只需要输入主机身份验证详细信息(用户名和密码)。
     - 通过代理自动配置脚本**(PAC)**—指定代理自动配置(PAC)脚本文件的位置。通过PAC文件、系统可以自动选择适当的代理服务器、以便与目标技术支持系统建立连接。
   - 如果选择了电子邮件、请输入以下信息：

- 作为完全限定域名、IPv4地址或IPv6地址的邮件服务器地址。
- AutoSupport 派遣电子邮件的发件人字段中显示的电子邮件地址。
- 可选；如果要执行配置测试。 AutoSupport 系统收到测试派单时发送确认的电子邮件地址。
- 如果要对消息进行加密、请选择* SMTPS 或 STARTTLS 作为加密类型、然后选择加密消息的端口号。否则、请选择*无。
- 如果需要、请输入用于向传出发件人和邮件服务器进行身份验证的用户名和密码。

4. 单击*测试配置*、使用指定的传输参数测试与技术支持服务器的连接。如果启用了AutoSupport 按需功能、则系统还会测试AutoSupport 按需派单交付的连接。

   如果配置测试失败、请检查您的配置设置并重新运行测试。如果测试仍失败、请联系技术支持。

5. 单击 * 保存 * 。

什么是配置数据?

选择收集配置数据后、系统将保存RAID配置数据库的当前状态。

RAID配置数据库包含控制器上卷组和磁盘池的所有数据。`s配置数据功能可保存与用于保存storageArray dbmDatabase`的命令行界面命令相同的信息。

在升级**SANtricity OS**软件之前、我需要了解哪些信息?

在升级控制器的软件和固件之前、请注意以下事项。

- 您已阅读此文档和`reADME.txt`文件、并已确定要执行升级。
- 您知道是否要升级IOM固件。

  通常，您应同时升级所有组件。但是、如果您不希望在SANtricity 操作系统控制器软件升级过程中升级IOM固件、或者技术支持已指示您降级IOM固件(您只能使用命令行界面降级固件)、则可能决定不升级IOM固件。

- 您知道是否要升级控制器NVSRAM文件。

  通常，您应同时升级所有组件。但是，如果您的文件已修补或为自定义版本，并且您不想覆盖此文件，则您可能会决定不升级控制器 NVSRAM 文件。

- 您知道是要立即激活还是稍后激活。

  稍后激活的原因可能包括：

  - 当前时间—激活软件和固件可能需要很长时间、因此您可能需要等待I/O负载减轻。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软件和固件，然后再升级其他存储阵列上的文件。

这些组件是SANtricity 操作系统控制器软件升级的一部分：

- 管理软件—System Manager是用于管理存储阵列的软件。

- * 控制器固件 * —控制器固件用于管理主机和卷之间的 I/O 。
- * 控制器 NVSRA* - 控制器 NVSRAM 是一个控制器文件，用于指定控制器的默认设置。
- * IOM 固件 * — I/O 模块（ IOM ）固件用于管理控制器与驱动器架之间的连接。它还会监控组件的状态。
- * 监控软件 * —监控软件是运行该软件的控制器上的虚拟机。

在升级过程中、可能还需要升级主机的多路径/故障转移驱动程序和/或HBA驱动程序、以便主机可以正确地与控制器进行交互。

要确定是否发生这种情况、请参见 "NetApp 互操作性表工具"。

如果存储阵列仅包含一个控制器或您未安装多路径驱动程序，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。

升级期间、请勿更改存储阵列。

暂停IOM自动同步前需要了解哪些信息？

暂停IOM自动同步可防止下次升级SANtricity OS控制器软件时升级IOM固件。

通常、控制器软件和IOM固件会作为捆绑包进行升级。如果要保留在机箱上的特殊IOM固件版本、则可以暂停IOM自动同步。否则、您将在下次升级控制器软件时还原到与控制器软件捆绑在一起的IOM固件。

为什么固件升级进度如此缓慢？

固件升级进度取决于系统的整体负载。

在驱动器固件的联机升级期间、如果在快速重建过程中发生卷传输、系统将对传输的卷启动完全重建。此操作可能需要相当长的时间。实际完整重建时间取决于多个因素、包括重建操作期间发生的I/O活动量、卷组中的驱动器数量、重建优先级设置以及驱动器性能。

升级驱动器固件前需要了解哪些信息？

在升级驱动器固件之前、请注意以下事项。

- 作为预防措施、请使用磁盘到磁盘备份、卷副本(到不受计划的固件升级影响的卷组)或远程镜像备份数据。
- 您可能只需要升级几个驱动器、即可测试新固件的行为、以确保其正常运行。如果新固件运行正常、请升级其余驱动器。
- 如果有任何故障驱动器、请在开始固件升级之前修复它们。
- 如果驱动器可以执行脱机升级、请停止与驱动器关联的所有卷的I/O活动。停止I/O活动后、不会执行与这些卷关联的配置操作。
- 升级驱动器固件时、请勿删除任何驱动器。
- 升级驱动器固件时、请勿对存储阵列进行任何配置更改。

如何选择要执行的升级类型？

您可以根据池或卷组的状态选择要对驱动器执行的升级类型。

- * 联机 *

  如果池或卷组支持冗余并处于最佳状态、则可以使用联机方法升级驱动器固件。联机方法会在存储阵列处理使用这些驱动器的关联卷的I/O时下载firmware _o。您不必停止使用这些驱动器的关联卷的I/O。这些驱动器一次升级一个、并升级到与这些驱动器关联的卷。如果驱动器未分配给池或卷组、则可以使用联机或脱机方法更新其固件。使用联机方法升级驱动器固件时、系统性能可能会受到影响。

- * 脱机 *

  如果池或卷组不支持冗余(RAID 0)或已降级、则必须使用脱机方法升级驱动器固件。脱机方法将在所有I/O活动均已停止时升级固件_only、并使用这些驱动器将其升级到关联卷。您必须停止使用这些驱动器的任何关联卷的所有I/O。如果驱动器未分配给池或卷组、则可以使用联机或脱机方法更新其固件。

使用 SANtricity Unified Manager 8 进行多阵列管理

主接口

了解 SANtricity Unified Manager

SANtricity统一管理器是一个基于Web的界面、可用于在一个视图中管理多个存储阵列。

主页

登录到Unified Manager后、主页将打开*管理-全部*。在此页面中、您可以滚动浏览网络中发现的存储阵列列表、查看其状态、并对单个阵列或一组阵列执行操作。

导航边栏

您可以从导航边栏访问Unified Manager的特性和功能。

区域	Description
管理	发现网络中的存储阵列，为阵列启动 SANtricity System Manager，将设置从一个阵列导入到多个阵列，并管理阵列组。选中阵列名称旁边的复选框以对其执行操作，例如导入设置和创建阵列组。每行末尾的省略号为单个阵列的操作（例如重命名）提供了一个内联菜单。
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。
证书管理	管理证书以在浏览器和客户端之间进行身份验证。
访问管理	为Unified Manager界面建立用户身份验证。
支持	查看技术支持选项、资源和联系人。

接口设置和帮助

在界面的右上角、您可以访问帮助和其他文档。您还可以访问管理选项、这些选项可从您的登录名旁边的下拉列表中找到。

用户登录和密码

当前登录系统的用户将显示在用户设置中。

有关用户和密码的详细信息、请参见：

- "设置管理员密码保护"
- "更改管理员密码"
- "更改本地用户配置文件的密码"

SANtricity Unified Manager 支持的浏览器

SANtricity 统一管理器可从多种类型的浏览器进行访问。

支持以下浏览器和版本。

浏览器	最低版本
Google Chrome	120
Mozilla Firefox	120
Safari	16
Microsoft Edge	120

Web服务代理必须已安装并可供浏览器使用。

了解 SANtricity Unified Manager 中的管理员密码保护

您必须使用管理员密码配置SANtricity Unified Manager、以防止未经授权的访问。

管理员密码和用户配置文件

首次启动Unified Manager时、系统会提示您设置管理员密码。具有管理员密码的任何用户都可以对存储阵列进行配置更改。

除了管理员密码之外、Unified Manager界面还包括预先配置的用户配置文件、其中包含一个或多个映射到这些配置文件的角色。有关详细信息，请参见 "访问管理的工作原理"。

无法更改用户和映射。只能修改密码。要更改密码、请参见：

- "更改管理员密码"
- "更改本地用户配置文件的密码"

会话超时

在单个管理会话期间、软件仅会提示您输入密码一次。默认情况下、会话在30分钟处于非活动状态后超时、此时您必须再次输入密码。如果另一个用户从另一个管理客户端访问软件并在会话期间更改了密码、则在下次尝试配置操作或查看操作时、系统会提示您输入密码。

出于安全原因、您只能在软件进入"锁定"状态之前尝试输入五次密码。在此状态下、软件将拒绝后续的密码尝试。您必须等待10分钟才能重置为"正常"状态、然后才能再次尝试输入密码。

您可以调整会话超时、也可以完全禁用会话超时。有关详细信息，请参见 "管理会话超时"。

在 SANtricity Unified Manager 中更改管理员密码

您可以更改用于访问SANtricity Unified Manager的管理员密码。

开始之前

- 您必须以本地管理员身份登录、其中包括root管理员权限。
- 您必须知道当前的管理员密码。

关于此任务

选择密码时、请记住以下准则：

- 密码区分大小写。
- 设置密码时、不会从密码中删除尾随空格。如果密码中包含空格、请小心操作。
- 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。

步骤

1. 从左侧面板中，选择菜单：Settings[Access Management]。
2. 选择*本地用户角色*选项卡。
3. 从表中选择*管理员*用户。

   更改密码按钮将变为可用。

4. 选择 * 更改密码 * 。

   此时将打开更改密码对话框。

5. 如果未为本地用户密码设置最小密码长度、请选中此复选框以要求用户输入密码以访问系统。
6. 在两个字段中输入新密码。
7. 输入本地管理员密码以确认此操作、然后单击*更改*。

在 SANtricity Unified Manager 中管理会话超时

您可以为SANtricity统一管理器配置超时、以便用户的非活动会话在指定时间后断开连接。

关于此任务

默认情况下、Unified Manager的会话超时为30分钟。您可以调整该时间、也可以完全禁用会话超时。

> 如果使用阵列中嵌入的安全断言标记语言(SAML)功能配置访问管理、则当用户的SSO会话达到其最大限制时、可能会发生会话超时。可能会在System Manager会话超时之前发生这种情况。

步骤

1. 从菜单栏中、选择用户登录名旁边的下拉箭头。
2. 选择*启用/禁用会话超时*。

   此时将打开启用/禁用会话超时对话框。

3. 使用spinner控件以分钟为单位增加或减少时间。

   您可以设置的最小超时时间为15分钟。

要禁用会话超时、请清除*设置时间长度…*复选框。

4. 单击 * 保存 * 。

存储阵列

了解 SANtricity Unified Manager 中的发现

要管理存储资源、您必须先发现网络中的存储阵列。

如何发现阵列?

使用"添加/发现"页面查找并添加要在组织网络中管理的存储阵列。您可以发现多个阵列、也可以发现一个阵列。为此、您需要输入网络IP地址、然后Unified Manager将尝试单独连接到该范围中的每个IP地址。

了解更多信息。

- "发现阵列的注意事项"
- "发现多个存储阵列"
- "发现单个阵列"

如何管理阵列?

发现阵列后、转到*管理-全部*页面。在此页面中、您可以滚动浏览网络中发现的存储阵列列表、查看其状态、并对单个阵列或一组阵列执行操作。

如果要管理单个阵列、可以将其选中并打开System Manager。

了解更多信息。

- "访问System Manager的注意事项"
- "管理单个存储阵列"
- "查看存储阵列状态"

概念

了解如何在 SANtricity Unified Manager 中发现存储阵列

在SANtricity Unified Manager显示和管理存储资源之前、它必须先发现要在组织网络中管理的存储阵列。您可以发现多个阵列、也可以发现一个阵列。

发现多个存储阵列

如果您选择发现多个阵列、请输入一个网络IP地址范围、然后Unified Manager将尝试单独连接到该范围中的每个IP地址。任何已成功访问的存储阵列都会显示在"Discover "页面上、并且可能会添加到您的管理域中。

发现单个存储阵列

如果您选择发现单个阵列、则输入存储阵列中一个控制器的单个IP地址、然后添加单个存储阵列。

Unified Manager只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Unified Manager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

在发现过程中、您必须为要添加的每个存储阵列提供管理员密码。

Web服务证书

在发现过程中、Unified Manager会验证发现的存储阵列是否正在使用受信任源的证书。Unified Manager对与浏览器建立的所有连接使用两种基于证书的身份验证：

- 可信证书

  对于Unified Manager发现的阵列、您可能需要安装证书颁发机构提供的其他受信任证书。

  使用*导入*按钮导入这些证书。如果您之前已连接到此阵列、则一个或两个控制器证书要么已过期、已撤销、要么在其证书链中缺少根证书或中间证书。在管理存储阵列之前、您必须替换已过期或已撤销的证书、或者添加缺少的根证书或中间证书。

- 自签名证书

  也可以使用自签名证书。如果管理员尝试在未导入签名证书的情况下发现阵列、则Unified Manager将显示一个错误对话框、允许管理员接受自签名证书。存储阵列的自签名证书将标记为可信、存储阵列将添加到Unified Manager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Unified Manager。

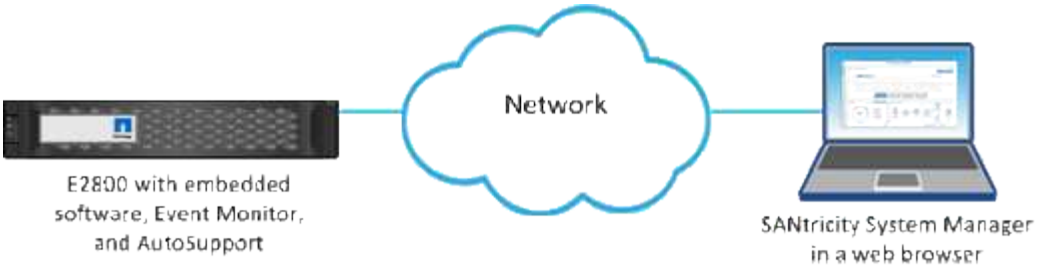
了解如何从 **Unified Manager** 访问 **SANtricity System Manager**

如果要配置和管理存储阵列、请选择一个或多个存储阵列并使用启动选项打开SANtricity系统管理器。

System Manager是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。它包括所有基于阵列的功能。

要访问System Manager、您必须具备：

- 此处列出的阵列型号之一： "E 系列硬件概述"
- 使用Web浏览器与网络管理客户端的带外连接。



发现阵列

在 **SANtricity Unified Manager** 中发现多个存储阵列

您可以发现多个阵列、以检测管理服务器所在子网中的所有存储阵列、并自动将发现的阵列添加到管理域中。

开始之前

- 您必须使用具有安全管理员权限的用户配置文件登录。
- 必须正确设置和配置存储阵列。
- 必须使用 System Manager 的身份验证类别设置存储阵列密码。
- 要解析不可信的证书、您必须拥有证书颁发机构(CA)提供的可信证书文件、并且证书文件可在本地系统上使用。

发现阵列是一种多步骤操作步骤。

第1步：输入网络地址

您可以输入一个网络地址范围、以便在本地子网络中搜索。任何已成功访问的存储阵列都会显示在"Discover "页面上、并且可能会添加到您的管理域中。

如果出于任何原因需要停止发现操作、请单击*停止发现*。

步骤

1. 在 Manage 页面中，选择 * 添加 / 发现 * 。

   此时将显示添加/发现对话框。

2. 选择*发现网络范围内的所有存储阵列*单选按钮。
3. 输入起始网络地址和结束网络地址以在本地子网络中搜索、然后单击*开始发现*。

   发现过程将启动。完成此发现过程可能需要几分钟时间。发现存储阵列时、会填充"发现"页面上的表。

   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. 查看已发现的存储阵列列表。
5. 选中要添加到管理域的任何存储阵列旁边的复选框、然后单击*下一步*。

Unified Manager会对要添加到管理域的每个阵列执行凭据检查。您可能需要解析与该阵列关联的任何自签名证书和不可信证书。

6. 单击 * 下一步 * 继续执行向导中的下一步。

第2步：在发现期间解析自签名证书

在发现过程中、系统会验证存储阵列是否正在使用受信任源的证书。

步骤

1. 执行以下操作之一：
   - 如果您信任与发现的存储阵列的连接、请继续访问向导中的下一个卡。自签名证书将标记为可信证书、存储阵列将添加到Unified Manager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Unified Manager。
2. 单击 * 下一步 * 继续执行向导中的下一步。

第3步：在发现期间解析不可信的证书

如果存储阵列尝试建立与Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。在阵列发现过程中、您可以通过导入可信第三方颁发的证书颁发机构(CA)证书(或CA签名证书)来解析不可信的证书。

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。
- 一个或两个证书均已过期。
- 一个或两个证书均已撤销。
- 一个或两个证书缺少根证书或中间证书。

步骤

1. 选中要为其解析不可信证书的任何存储阵列旁边的复选框、然后选择"*导入"*按钮。

   此时将打开一个对话框、用于导入可信证书文件。

2. 单击*浏览*以选择存储阵列的证书文件。

   文件名显示在对话框中。

3. 单击 * 导入 * 。

   这些文件将上传并进行验证。

   如果任何存储阵列存在未解决的不可信证书问题、则不会添加到Unified Manager中。

4. 单击 * 下一步 * 继续执行向导中的下一步。

第4步：提供密码

您必须输入要添加到管理域的存储阵列的密码。

步骤

1. 输入要添加到Unified Manager的每个存储阵列的密码。
2. *可选：*将存储阵列与组关联：从下拉列表中、选择要与选定存储阵列关联的所需组。
3. 单击 * 完成 * 。

完成后

存储阵列将添加到管理域中并与选定组(如果指定)关联。

Unified Manager连接到指定存储阵列可能需要几分钟的时间。

在 **SANtricity Unified Manager** 中发现单个阵列

使用添加/发现单个存储阵列选项手动发现单个存储阵列并将其添加到组织的网络中。

开始之前

- 必须正确设置和配置存储阵列。
- 必须使用 System Manager 的身份验证类别设置存储阵列密码。

步骤

1. 在 Manage 页面中，选择 * 添加 / 发现 * 。

   此时将显示添加/发现对话框。

2. 选择*发现单个存储阵列*单选按钮。
3. 输入存储阵列中某个控制器的IP地址、然后单击*启动发现*。

   Unified Manager连接到指定存储阵列可能需要几分钟的时间。

   如果无法连接到指定控制器的IP地址、则会显示"Storage Array not accessible"消息。

4. 如果出现提示、请解析任何自签名证书。

   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。如果找不到存储阵列的数字证书、则会提示您通过添加安全异常来解析未由可识别证书颁发机构(CA)签名的证书。

5. 如果出现提示、请解析任何不可信的证书。

   如果存储阵列尝试建立与Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。通过导入可信第三方颁发的证书颁发机构(CA)证书来解析不可信证书。

6. 单击 * 下一步 * 。
7. *可选：*将发现的存储阵列与组相关联：从下拉列表中、选择要与该存储阵列关联的所需组。

   默认情况下、系统会选择"all"组。

8. 输入要添加到管理域的存储阵列的管理员密码、然后单击*确定*。

完成后

存储阵列将添加到Unified Manager中、如果指定此阵列、则还会添加到选定的组中。

如果启用了自动支持数据收集、则会自动收集您添加的存储阵列的支持数据。

管理阵列

在 **SANtricity Unified Manager** 中查看存储阵列状态

SANtricity统一管理器会显示已发现的每个存储阵列的状态。

转到*管理-全部*页面。在此页面中、您可以查看Web服务代理与该存储阵列之间的连接状态。

下表介绍了状态指示灯。

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。
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Web服务代理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Web服务代理启动以来从未进行过联系、则可能会发生这种情况。
脱机	Web服务代理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。

在 **SANtricity Unified Manager** 中管理单个存储阵列

如果要执行管理操作、您可以使用启动选项为一个或多个存储阵列打开基于浏览器的SANtricity 系统管理器。

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 * 。

   系统将打开一个新窗口并显示System Manager登录页面。

3. 输入用户名和密码、然后单击*登录*。

在 **SANtricity Unified Manager** 中更改存储阵列密码

您可以在SANtricity Unified Manager中更新用于查看和访问存储阵列的密码。

开始之前

- 您必须使用包含存储管理员权限的用户配置文件登录。
- 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Unified Manager中访问该密码。如果在System Manager中更改了阵列密码、并且现在还必须在Unified Manager中更改该密码、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*。

从**SANtricity** 统一管理器中删除存储阵列

如果您不想再从SANtricity 统一管理器管理一个或多个存储阵列、则可以将其删除。

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

   存储阵列将从SANtricity Unified Manager的所有视图中删除。

设置导入

了解如何在 **SANtricity Unified Manager** 中导入存储阵列设置

通过导入设置功能、您可以执行批量操作、将设置从一个阵列导入到多个阵列。当您需要在网络中配置多个阵列时、此功能可以节省时间。

可以导入哪些设置?

您可以导入警报方法、AutoSupport 配置、目录服务配置、存储配置(例如卷组和池)和系统设置(例如自动负载平衡)。

了解更多信息。

- "导入设置的工作原理"

- "复制存储配置的要求"

如何执行批量导入?

在要用作源的存储阵列上、打开System Manager并配置所需的设置。然后从Unified Manager中、转到"管理"页面并将设置导入到一个或多个阵列。

了解更多信息。

- "导入警报设置"
- "导入AutoSupport 设置"
- "导入目录服务设置"
- "导入存储配置设置"
- "导入系统设置"

概念

了解如何在 **SANtricity Unified Manager** 中配置多个存储阵列

您可以使用SANtricity 统一管理器将设置从一个存储阵列导入到多个存储阵列。导入设置功能是一个批处理操作、当您需要在网络中配置多个阵列时、可以节省时间。

可用于导入的设置

可以将以下配置导入到多个阵列：

- 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。
- 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
- 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)

配置工作流

要导入设置、请按照以下工作流进行操作：

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Unified Manager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。

在 **SANtricity Unified Manager** 中复制存储阵列配置的要求

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

- 源阵列和目标阵列之间的控制器类型可以不同（例如，从 EF300 导入到 EF80），但 RBOD 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。
- 导入过程不包括精简卷。

使用批量导入

在 **SANtricity Unified Manager** 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

- 在 System Manager 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在 System Manager 中备份（菜单：System[Save storage array configuration]

）。

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。导入的设置包括：

- 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*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Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该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 **SANtricity Unified Manager** 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

- AutoSupport 已在 System Manager 中为要用作源的存储阵列配置（菜单：Support[AutoSupport]）。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：System[Save storage array configuration]）。

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*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Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该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 **SANtricity Unified Manager** 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

- 在 System Manager 中为要用作源的存储阵列配置目录服务（菜单：身份验证[目录服务]）。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：System[Save storage array configuration]）。

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*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Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该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 **SANtricity Unified Manager** 中导入系统设置

您可以将系统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

- 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在 System Manager 中备份（菜单：System[Save storage array configuration]）。

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*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Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该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 **SANtricity Unified Manager** 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

- 已在SANtricity 系统管理器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在 System Manager 中备份（菜单：System[Save storage array configuration]）。
- 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。
  - 导入过程不包括精简卷。

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*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Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该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。

SANtricity Unified Manager 导入设置常见问题解答

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。

将导入哪些设置?

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在SANtricity 系统管理器中配置源存储阵列的方式。

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的存储阵列?

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)。

阵列组

了解 SANtricity Unified Manager 中的组概述

在管理组页面中、您可以创建一组存储阵列组、以便于管理。

什么是阵列组?

您可以通过对一组存储阵列进行分组来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。

组类型有两种：

- 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。

如何配置组?

在管理组页面中、您可以创建一个组、然后向该组添加阵列。

了解更多信息。

- "配置存储阵列组"

在 SANtricity Unified Manager 中配置存储阵列组

您可以创建存储组、然后将存储阵列添加到这些组中。

配置组是一个两步操作步骤。

第1步：创建组

首先创建组。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 * 。

第2步：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。 *

从 SANtricity Unified Manager 中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 **SANtricity Unified Manager** 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 * 。

在 **SANtricity Unified Manager** 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。*

升级

了解 **SANtricity Unified Manager** 中的升级中心

从升级中心、您可以管理多个存储阵列的SANtricity OS软件和NVSRAM升级。

升级如何工作?

下载最新的操作系统软件、然后升级一个或多个阵列。

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软件文件(可从Unified Manager的"支持"页面中找到一个链接)。将此文件保存在管理主机系统(在浏览器中访问Unified Manager的主机)上、然后解压缩此文件。
2. 在Unified Manager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Web服务代理服务器的一个区域)。您可以从菜单：升级中心[升级SANtricity 操作系统软件或从升级中心>管理软件存储库]添加文件。
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(菜单：升级中心[升级SANtricity OS软件])中、选择SANtricity OS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、Unified Manager将执行以下任务：
   a. 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。
   b. 将升级文件传输到每个控制器。
   c. 重新启动控制器并激活新的SANtricity OS软件、一次一个控制器。激活期间、现有SANtricity OS文件将替换为新文件。

   您还可以指定稍后激活此软件。

立即或分阶段升级

您可以立即激活升级，也可以稍后暂存升级。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。根据 I/O 负载和缓存大小，完成控制器升级通常需要 15 到 25 分钟。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 * —您可能需要先在一个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。

要激活暂存软件，请转到菜单：支持[升级中心]，然后在标记为 SANtricity 操作系统控制器软件升级的区域中单击*激活*。

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(转到菜单：升级中心[升级前运行状况检查])。

运行状况检查会评估所有存储系统组件、以确保升级可以继续进行。以下情况可能会阻止升级：

- 已分配的驱动器出现故障
- 正在使用热备件
- 卷组不完整
- 正在运行排他操作
- 缺少卷

- 控制器处于非最佳状态
- 事件日志事件数量过多
- 配置数据库验证失败
- 使用旧版 DAC 存储的驱动器

升级前需要了解哪些信息？

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Unified Manager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 SANtricity OS 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 "NetApp 互操作性表"。另请参见适用于您的操作系统的快速指南中的过程。快速指南可从获取 "E 系列和 SANtricity 文档"。

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。

升级软件和固件

在 **SANtricity Unified Manager** 中执行升级前健康检查

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进行。

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 (...) 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。

升级 **SANtricity** 操作系统

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

- 运行SANtricity Web服务代理和Unified Manager的主机系统上提供了最新的SANtricity 操作系统文件。
- 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。

系统必须运行SANtricity OS 11.70.5才能升级到11.80.x或更高版本。

[NOTE]
====
数据丢失风险或存储阵列损坏风险—升级期间，请勿更改存储阵列。为存储阵列供电。

====
.步骤
. 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。
. 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。
. 选择菜单：升级中心 [升级 SANtricity 操作系统软件] 。
+
此时将显示升级 SANtricity OS 软件页面。

. 从 NetApp 支持站点将最新的 SANtricity OS 软件包下载到您的本地计算机。
+
.. 单击 * 将新文件添加到软件存储库 * 。
.. 单击链接以查找最新的 * SANtricity OS Downloads* 。
.. 单击 * 下载最新版本 * 链接。

.. 按照其余说明将 SANtricity 操作系统文件和 NVSRAM 文件下载到本地计算机。

+
[NOTE]
====
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。

====
. 选择要用于升级控制器的操作系统软件文件和 NVSRAM 文件：
+
.. 从 * 选择 SANtricity OS 软件文件 * 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。

+
[NOTE]
====
软件存储库列出了与 Web 服务代理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。

====
.. 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。

. 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。

. *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。
. 单击 * 开始 * 。
. 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 * 传输 * 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 [激活暂存操作系统软件] 。

** 键入 * 升级 * 确认要在选定升级的阵列上传输并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进行。
** 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。

. *可选：*升级完成后、您可以通过单击省略号(...)并选择*保存日志*来查看为特定存储阵列升级的内容列表。
+
此文件将保存在浏览器的"Downloads"文件夹中、名为`upgrade_log-<date>.json`。

[[IDf6822a065d28b6170c8bd657eb077937]]
= 在 SANtricity Unified Manager 中激活暂存操作系统软件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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 *
—您可能需要先在一个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。

[NOTE]
====
激活过程启动后，您无法停止它。

====
.步骤
. 在主视图中、选择*管理*。如有必要、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。
. 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 [激活暂存操作系统软件] 。
+
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进行。
** 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。

. *可选：*激活完成后、您可以通过单击省略号(...)并选择*保存日志*来查看为特定存储阵列激活的内容列表。
+
此文件将保存在浏览器的 "Downloads" 文件夹中，名称为 `active_log-<date>.json` 。

[[ID294229b168d5e0d19238f70113a94890]]
= 在 Unified Manager 中管理 SANtricity 软件存储库
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
软件存储库列出了与 Web 服务代理关联的所有软件文件。

如果您看不到要使用的文件、可以使用管理软件存储库选项将一个或多个SANtricity操作系统文件导入到运行Web服务代理和Unified

Manager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SANtricity OS文件。

.开始之前
如果要添加SANtricity 操作系统文件、请确保操作系统文件在本地系统上可用。

.步骤
. 在主视图中、选择*管理*、然后选择菜单：升级中心[管理软件存储库]。
+
此时将显示管理软件存储库对话框。

. 执行以下操作之一：
+
[cols="25h,~"]
|===
| 选项 | 执行此操作

a|
导入
a|
.. 单击*导入。*
.. 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`。

.. 选择要添加的一个或多个操作系统文件、然后单击*导入*。

a|
删除
a|
.. 选择要从软件存储库中删除的一个或多个操作系统文件。
.. 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。

[[ID7ed5f1ad003b9ebda9586e0ebaa30279]]
= 清除 SANtricity Unified Manager 中的暂存操作系统软件

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
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
. 在主视图中、选择*管理*、然后选择菜单：升级中心[清除暂存操作系统软件]。
+
此时将打开清除暂存操作系统软件对话框、并列出所有已发现的具有待定软件或NVSRAM的存储系统。

. 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。
. 选中要清除的待定软件存储系统对应的复选框。
. 单击*清除*。
+
此操作的状态将显示在对话框中。

```
:leveloffset: -1


:leveloffset: -1


= 镜像

:leveloffset: +1


[[ID482075d055b7a8169e0ad8a25ead75a2]]
= 了解 SANtricity Unified Manager 中的镜像
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
使用镜像功能可以异步或同步在本地存储阵列和远程存储阵列之间复制数据。

[NOTE]
====
EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

====

[[what-is-mirroring]]
== 什么是镜像?

SANtricity
应用程序包括两种类型的镜像：异步和同步。异步镜像可按需或按计划复制数据卷、从而最大限度地减少或避免因数据损坏或丢失而导致的停机时间。同步镜像可实时复制数据卷、以确保持续可用性。

了解更多信息。

* xref:{relative_path}mirroring-overview.html["镜像的工作原理"]
* xref:{relative_path}mirroring-terminology.html["镜像术语"]

[[how-do-i-configure-mirroring]]
== 如何配置镜像?

您可以在Unified Manager中配置异步或同步镜像、然后使用System Manager管理同步。

了解更多信息。

* xref:{relative_path}mirroring-configuration-workflow.html["镜像配置工作流"]
* xref:{relative_path}requirements-for-using-mirroring.html["使用镜像的要求"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["
创建异步镜像对"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["创建同步镜像对"]

= 概念

:leveloffset: +1

[[ID1282ad037bb0fadf8f5689c111d8bcf5]]
= 了解 SANtricity 镜像
:allow-uri-read:

:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity统一管理器提供了SANtricity镜像功能的配置选项、使管理员能够在两个存储阵列之间复制数据以实现数据保护。

[NOTE]
====
EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

====

[[types-of-mirroring]]
== 镜像类型

SANtricity 应用程序包括两种类型的镜像：异步和同步。

异步镜像可按需或按计划复制数据卷、从而最大限度地减少或避免因数据损坏或丢失而导致的停机时间。异步镜像可捕获主卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。可以立即更新主站点、并在带宽允许的情况下更新二级站点。此信息将在网络资源可用时进行缓存并稍后发送。这种类型的镜像非常适合备份和归档等定期过程。

同步镜像可实时复制数据卷、以确保持续可用性。其目的是、在两个存储阵列之一发生灾难时、提供一份重要数据副本、从而实现零丢失数据的恢复点目标(RPO)。副本与生产数据在每一刻都是相同的、因为每次对主卷执行写入时、都会对二级卷执行写入。在使用主卷上所做的更改更新二级卷之前、主机不会收到写入成功的确认消息。这种类型的镜像非常适合用于灾难恢复等业务连续性目的。

[[differences-between-mirroring-types]]
== 镜像类型之间的差异

下表介绍了这两种镜像类型之间的主要区别。

[cols="1a,1a,1a"]
|===
| 属性 | 异步 | 同步

a|
复制方法
a|
时间点—镜像是按需执行的、也可以根据用户定义的计划自动执行。

a|
持续–镜像会自动持续执行、每次写入主机时都会复制数据。

a|
距离
a|
支持阵列之间的长距离。通常、距离仅受网络功能和通道扩展技术的限制。
a|
限制为阵列之间的距离较短。通常、距离必须在本地存储阵列10公里(6.2英里)以内、才能满足延迟和应用程序性能要求。

a|
通信方法
a|
标准IP或光纤通道网络。
a|
仅限光纤通道网络。

a|
卷类型
a|
标准或精简。
a|
仅限标准配置。

|===

[[IDbe95383692e579b2a83b64cfa2a9c403]]
= 镜像 SANtricity 配置工作流程
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以在SANtricity统一管理器中配置异步或同步镜像、然后使用SANtricity系统管理器管理同步。

[[asynchronous-mirroring-workflow]]
== 异步镜像工作流

异步镜像涉及以下工作流：

. 在Unified Manager中执行初始配置：
+
.. 选择本地存储阵列作为数据传输的源。
..
创建或选择现有镜像一致性组、该组是本地阵列上主卷和远程阵列上二级卷的容器。主卷和二级卷称为"镜像对"。 如果您是首次创建镜像一致性组、则可以指定是要执行手动同步还是计划同步。
.. 从本地存储阵列中选择主卷、然后确定其预留容量。预留容量是为复制操作分配的物理容量。
.. 选择一个远程存储阵列作为传输的目标、一个二级卷、然后确定其预留容量。
.. 开始从主卷到二级卷的初始数据传输。根据卷大小、此初始传输可能需要几小时的时间。

. 检查初始同步的进度：
+
.. 在Unified Manager中、为本地阵列启动System Manager。
.. 在System Manager中、查看镜像操作的状态。镜像完成后、镜像对的状态为"最佳"。

. 您也可以在System
Manager中重新计划或手动执行后续数据传输。只有新的块和更改的块才会从主卷传输到二级卷。
+
[NOTE]
====
由于异步复制是定期进行的、因此系统可以整合更改的块并节省网络带宽。对写入吞吐量和写入延迟的影响最小。

====

[[synchronous-mirroring-workflow]]
== 同步镜像工作流

同步镜像涉及以下工作流：

. 在Unified Manager中执行初始配置：
+
.. 选择一个本地存储阵列作为数据传输的源。
.. 从本地存储阵列中选择主卷。
.. 选择一个远程存储阵列作为数据传输的目标、然后选择一个二级卷。
.. 选择同步和重新同步优先级。

.. 开始从主卷到二级卷的初始数据传输。根据卷大小、此初始传输可能需要几小时的时间。

. 检查初始同步的进度：
+
.. 在Unified Manager中、为本地阵列启动System Manager。
.. 在System Manager中、查看镜像操作的状态。镜像完成后、镜像对的状态为"最佳"。
这两个阵列会尝试通过正常操作保持同步。只有新的块和更改的块才会从主卷传输到二级卷。

. 您也可以在System Manager中更改同步设置。
+
[NOTE]
====
由于同步复制是持续的、因此两个站点之间的复制链路必须提供足够的带宽功能。

====

[[ID1d8cddae0773d663ad6b9fa2965eb3dd]]
= 了解 SANtricity Unified Manager 中的镜像术语
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解镜像术语如何应用于存储阵列。

[cols="25h,~"]
|===
| 期限 | Description

a|
本地存储阵列
a|
本地存储阵列是您要对其执行操作的存储阵列。

a|
镜像一致性组
a|

镜像一致性组是一个或多个镜像对的容器。对于异步镜像操作、必须创建镜像一致性组。组中的所有镜像对会同时重新同步、从而保留一致的恢复点。

同步镜像不使用镜像一致性组。

a|
镜像对

a|
镜像对由两个卷组成、一个是主卷、一个是二级卷。

在异步镜像中、镜像对始终属于镜像一致性组。首先对主卷执行写入操作、然后将其复制到二级卷。镜像一致性组中的每个镜像对共享相同的同步设置。

a|
主卷

a|
镜像对的主卷是要镜像的源卷。

a|
远程存储阵列

a|
远程存储阵列通常指定为二级站点、该站点通常在镜像配置中保存数据的副本。

a|
预留容量

a|
预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

需要这些卷、以便控制器能够持久保存必要的信息、以使镜像保持运行状态。它们包含增量日志和写入时复制数据等信息。

a|
二级卷

a|
镜像对的二级卷通常位于二级站点、并保存数据的副本。

 a|
同步
 a|
在本地存储阵列与远程存储阵列之间进行初始同步时进行同步。如果在通信中断后主卷和二级卷未同步、则也会发生同步。当通信链路重新工作时、任何未复制的数据都会同步到二级卷的存储阵列。

|===

[[IDab76e82fcc5c03359acdd7ad18f0c53e]]
= 在 SANtricity Unified Manager 中使用镜像的要求
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您计划配置镜像、请记住以下要求。

[[unified-manager]]
== Unified Manager

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

[[storage-arrays]]
== 存储阵列

[NOTE]
====
EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储阵列上不提供同步镜像。

====
* 您必须有两个存储阵列。
* 每个存储阵列必须具有两个控制器。
* 必须在Unified Manager中发现这两个存储阵列。

* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
* 您必须知道本地和远程存储阵列的密码。
* 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
* 具有光纤通道(FC)或iSCSI主机端口的控制器支持异步镜像、而只有具有FC主机端口的控制器才支持同步镜像。

[[connectivity-requirements]]
== 连接要求

通过FC接口(异步或同步)进行镜像需要满足以下要求：

* 存储阵列的每个控制器都将其编号最高的FC主机端口专用于镜像操作。
* 如果控制器同时具有基本FC端口和主机接口卡(HIC) FC端口、则编号最高的端口位于HIC上。登录到专用端口的任何主机都将注销、并且不接受任何主机登录请求。只有参与镜像操作的控制器才会接受此端口上的I/O请求。
* 专用镜像端口必须连接到支持目录服务和名称服务接口的FC网络结构环境。特别是、不支持将FC-AL和点对点作为参与镜像关系的控制器之间的连接选项。

通过iSCSI接口(仅限异步)进行镜像需要满足以下要求：

* 与FC不同、iSCSI不需要专用端口。在iSCSI环境中使用异步镜像时、无需将存储阵列的任何前端iSCSI端口专用于异步镜像；这些端口可用于异步镜像流量和主机到阵列I/O连接。
* 控制器会维护一个远程存储系统列表、iSCSI启动程序会尝试与这些系统建立会话。成功建立iSCSI连接的第一个端口将用于此后与该远程存储阵列进行的所有通信。如果通信失败、则会尝试使用所有可用端口进行新会话。
+

NOTE: E4000 控制器不支持 iSCSI 镜像。

*
iSCSI端口在阵列级别逐个端口进行配置。用于配置消息传送和数据传输的控制器间通信使用全局设置、包括以下设置：
+
** VLAN：本地系统和远程系统必须具有相同的VLAN设置才能进行通信
** iSCSI侦听端口
** 巨型帧

[NOTE]

====
建议使用巨型帧以提高 CPU 性能和吞吐量。

====
* 以太网优先级

[NOTE]
====
iSCSI控制器间通信必须使用主机连接端口、而不是管理以太网端口。

====

[[mirrored-volume-candidates]]
== 镜像卷候选项

* 镜像对的主卷和二级卷上的RAID级别、缓存参数和区块大小可能不同。
+

NOTE: 对于EF600和
EF300控制器、异步镜像对中的主卷和二级卷必须匹配相同的协议、托盘级别、区块大小、安全类型和RAID级别。不符合条件的异步镜像对不会显示在可用卷列表中。

* 二级卷必须至少与主卷大小相同。
* 一个卷只能参与一个镜像关系。
* 对于同步镜像对、主卷和二级卷必须是标准卷。它们不能是精简卷或快照卷。
*
对于同步镜像、给定存储阵列上支持的卷数量存在限制。确保存储阵列上已配置的卷数小于支持的限制。当同步镜像处于活动状态时、创建的两个预留容量卷将计入卷限制。
* 对于异步镜像、主卷和二级卷必须具有相同的驱动器安全功能。
+
** 如果主卷支持FIPS、则二级卷必须支持FIPS。
** 如果主卷支持FDE、则二级卷必须支持FDE。
** 如果主卷未使用驱动器安全、则二级卷不得使用驱动器安全。

* 主卷和辅助卷不得启用资源调配。

[[reserved-capacity]]
== 预留容量

异步镜像：

*
主卷和镜像对中的二级卷需要预留容量卷、以便记录写入信息、以便从控制器重置和其他临时中断中恢复。
*
由于镜像对中的主卷和二级卷都需要额外的预留容量、因此您必须确保镜像关系中的两个存储阵列都具有可用容量。

同步镜像：

* 主卷和二级卷需要预留容量、以便记录写入信息、以便从控制器重置和其他临时中断中恢复。
*
激活同步镜像后、系统会自动创建预留容量的卷。由于镜像对中的主卷和二级卷都需要预留容量、因此您必须确保参与同步镜像关系的两个存储阵列上都有足够的可用容量。

[[drive-security-feature]]
== 驱动器安全功能

*
如果您使用的是支持安全的驱动器、则主卷和二级卷必须具有兼容的安全设置。此限制不会强制实施；因此、您必须自行验证。
*
如果使用的是支持安全的驱动器、则主卷和二级卷应使用相同的驱动器类型。此限制不会强制实施；因此、您必须自行验证。
* 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。

:leveloffset: -1

= 配置镜像

:leveloffset: +1

[[IDe0cdb0a8c62d9a4847e459606769b214]]
= 在 SANtricity Unified Manager 中创建异步镜像对
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置异步镜像、请创建一个镜像对、其中包括本地阵列上的主卷和远程阵列上的二级卷。

.开始之前
在创建镜像对之前、请满足Unified Manager的以下要求：

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

此外、对于存储阵列和卷、请确保满足以下要求：

* 每个存储阵列必须具有两个控制器。
* 必须在Unified Manager中发现这两个存储阵列。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
* 您必须知道本地和远程存储阵列的密码。
* 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
* 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。
* 您已创建要在异步镜像关系中使用的主卷和二级卷。
* 二级卷必须至少与主卷大小相同。

.关于此任务
创建异步镜像对的过程包括多步操作步骤。

[[step-1-create-or-select-a-mirror-consistency-group]]
== 第1步：创建或选择镜像一致性组

在此步骤中、您可以创建一个新的镜像一致性组或选择一个现有镜像一致性组。镜像一致性组是主卷和二级卷(镜像对)的容器、并为组中的所有对指定所需的重新同步方法(手动或自动)。

.步骤
. 从*管理*页面中、选择要用于源的本地存储阵列。
. 选择菜单：操作[创建异步镜像对]。
+
此时将打开创建异步镜像对向导。

. 选择现有镜像一致性组或创建新的镜像一致性组。
+
要选择现有组、请确保已选择*现有镜像一致性组*、然后从表中选择该组。一个一致性组可以包含多个镜

像对。

+
要创建新组、请执行以下操作：

+
.. 选择*新的镜像一致性组*、然后单击*下一步*。
..
输入最能描述将在两个存储阵列之间镜像的卷上的数据的唯一名称。名称只能由字母、数字和特殊字符下划线 (_)、短划线 (-) 和哈希符号 (#) 组成。名称不能超过 60 个字符，也不能包含空格。
.. 选择要与本地存储阵列建立镜像关系的远程存储阵列。
+
[NOTE]
====
如果远程存储阵列受密码保护、则系统会提示输入密码。

====
.. 选择是要手动还是自动同步镜像对：
+
*** *手动* --
选择此选项可手动启动此组中所有镜像对的同步。请注意，如果稍后要执行重新同步，则必须为主存储阵列启动 System Manager，然后转到菜单：Mirroring[Asynchronous mirror consistency groups]，选择该组，然后选择菜单：More[Manually resynchronize]。
*** *自动*—从上次更新开始到下次更新开始、选择所需的间隔、以*分钟*、*小时*或*天*为单位。例如、如果同步间隔设置为30分钟、而同步过程在下午4：00开始、则下一个过程将在下午4：30开始

.. 选择所需的警报设置：
+
*** 对于手动同步、请指定接收警报时的阈值(由剩余容量百分比定义)。
*** 对于自动同步、您可以设置三种警报方法：
如果同步未在特定时间长度内完成、远程阵列上的恢复点数据早于特定时间限制、并且预留容量接近特定阈值(由剩余容量百分比定义)。

. 选择*下一步*并转到 <<第2步：选择主卷>>。
+
如果定义了新的镜像一致性组、则Unified Manager会首先在本地存储阵列上创建镜像一致性组、然后在远程存储阵列上创建镜像一致性组。您可以通过为每个阵列启动System Manager来查看和管理镜像一致性组。

+
[NOTE]
====

如果Unified
Manager在本地存储阵列上成功创建镜像一致性组、但无法在远程存储阵列上创建该一致性组、则它会自动从本地存储阵列中删除镜像一致性组。如果在Unified
Manager尝试删除镜像一致性组时发生错误、您必须手动将其删除。

====

[[step-2-select-the-primary-volume]]
== 第2步：选择主卷

在此步骤中、您可以选择要在镜像关系中使用的主卷并分配其预留容量。在本地存储阵列上选择主卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。

添加到本地存储阵列上的镜像一致性组的任何卷都将在镜像关系中发挥主要作用。

.步骤
. 从符合条件的卷列表中、选择要用作主卷的卷、然后单击*下一步*以分配预留容量。
. 从符合条件的候选卷列表中、选择为主卷预留的容量。
+
请记住以下准则：

+
** 预留容量的默认设置为基础卷容量的20%、通常此容量已足够。如果更改百分比、请单击*刷新候选项*。
** 所需容量因向主卷写入I/O的频率和大小以及保留容量所需的时间而异。
** 通常、如果存在以下一种或两种情况、请为预留容量选择更大的容量：
+
*** 您打算将镜像对保留很长时间。
*** 由于
I/O活动繁重、主卷上的数据块会发生很大一部分更改。使用历史性能数据或其他操作系统实用程序帮助您确定主卷的典型I/O活动。

. 选择*下一步*并转到 <<第3步：选择二级卷>>。

[[step-3-select-the-secondary-volume]]
== 第3步：选择二级卷

在此步骤中、您可以选择要在镜像关系中使用的二级卷并分配其预留容量。在远程存储阵列上选择二级卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。

您添加到远程存储阵列上的镜像一致性组的任何卷都将在镜像关系中具有二级角色。

.步骤
. 从符合条件的卷列表中、选择要用作镜像对中二级卷的卷、然后单击*下一步*以分配预留容量。
. 从符合条件的候选卷列表中、选择为二级卷预留的容量。
+
请记住以下准则：

+
** 预留容量的默认设置为基础卷容量的20%、通常此容量已足够。如果更改百分比、请单击*刷新候选项*。
** 所需容量因向主卷写入I/O的频率和大小以及保留容量所需的时间而异。
** 通常、如果存在以下一种或两种情况、请为预留容量选择更大的容量：
+
*** 您打算将镜像对保留很长时间。
*** 由于I/O活动繁重、主卷上的数据块会发生很大一部分更改。使用历史性能数据或其他操作系统实用程序帮助您确定主卷的典型I/O活动。

. 选择*完成*以完成异步镜像序列。

.结果
Unified Manager将执行以下操作：

* 开始在本地存储阵列和远程存储阵列之间进行初始同步。
* 在本地存储阵列和远程存储阵列上为镜像对创建预留容量。

NOTE：如果要镜像的卷是精简卷、则在初始同步期间、只会将配置的块(已分配容量而不是报告的容量)传输到二级卷。这样可以减少完成初始同步所需传输的数据量。

[[ID4bca06f5571da92d04678eb976b3d732]]
= 在 SANtricity Unified Manager 中创建同步镜像对
:allow-uri-read:
:experimental:
:icons: font

:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置同步镜像、请创建一个镜像对、其中包括本地阵列上的主卷和远程阵列上的二级卷。

[NOTE]
====
此功能不适用于 EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统。

====
.开始之前
在创建镜像对之前、请满足Unified Manager的以下要求：

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

此外、对于存储阵列和卷、请确保满足以下要求：

* 您计划用于镜像的两个存储阵列会在Unified Manager中发现。
* 每个存储阵列必须具有两个控制器。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。（它们可以分别运行不同的操作系统版本。）
* 您必须知道本地和远程存储阵列的密码。
* 本地和远程存储阵列通过光纤通道网络结构进行连接。
* 您已创建要在同步镜像关系中使用的主卷和二级卷。
* 主卷必须是标准卷。它不能是精简卷或快照卷。
* 二级卷必须是标准卷。它不能是精简卷或快照卷。
* 二级卷应至少与主卷大小相同。

.关于此任务
创建同步镜像对的过程包括多步操作步骤。

[[step-1-select-the-primary-volume]]
== 第1步：选择主卷

在此步骤中、您可以选择要在同步镜像关系中使用的主卷。在本地存储阵列上选择主卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。您选择的卷在镜像关系中具有主要角色。

.步骤
. 从*管理*页面中、选择要用于源的本地存储阵列。
. 选择菜单：操作[创建同步镜像对]。
+
此时将打开创建同步镜像对向导。

. 从符合条件的卷列表中、选择要用作镜像中主卷的卷。
. 选择*下一步*并转到 <<第2步：选择二级卷>>。

[[step-2-select-the-secondary-volume]]
== 第2步：选择二级卷

在此步骤中、您可以选择要在镜像关系中使用的二级卷。在远程存储阵列上选择二级卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。您选择的卷将在镜像关系中保留二级角色。

.步骤
. 选择要与本地存储阵列建立镜像关系的远程存储阵列。
+
[NOTE]
====
如果远程存储阵列受密码保护、则系统会提示输入密码。

====
+
** 存储阵列按其存储阵列名称列出。如果您尚未为存储阵列命名、则该存储阵列将列为"未命名"。
** 如果要使用的存储阵列不在列表中、请确保已在Unified Manager中发现它。

. 从符合条件的卷列表中、选择要用作镜像中二级卷的卷。
+
[NOTE]
====
如果选择的二级卷的容量大于主卷、则可用容量将限制为主卷的大小。

====
. 单击*下一步*并转到 <<第3步：选择同步设置>>。

[[step-3-select-synchronization-settings]]
== 第3步：选择同步设置

在此步骤中、您可以选择用于确定在通信中断后如何同步数据的设置。您可以设置在通信中断后主卷的控制器所有者与二级卷重新同步数据的优先级。您还必须选择手动或自动重新同步策略。

.步骤
. 使用滑块栏设置同步优先级。
+
同步优先级用于确定在通信中断后、与服务I/O请求相比、用于完成初始同步和重新同步操作的系统资源量。

+
此对话框上设置的优先级适用于主卷和辅助卷。您可以稍后通过转到 System Manager 并选择菜单来修改主卷上的速率：Mirroring[Synchronous mirroring > ellipsis icon > Edit Settings]。

+
同步优先级速率有五种：

+
** 最低
** 低
** 中等
** 高
** 最高
+
如果将同步优先级设置为最低速率、则会优先处理I/O活动、并且重新同步操作所需时间会更长。如果将同步优先级设置为最高比率、则会优先执行重新同步操作、但存储阵列的I/O活动可能会受到影响。

. 选择是手动还是自动重新同步远程存储阵列上的镜像对。
+
** *手动*(建议选项)—选择此选项可要求在恢复与镜像对的通信后手动恢复同步。此选项提供了恢复数据的最佳机会。
** *自动*—选择此选项可在与镜像对的通信恢复后自动开始重新同步。
+
要手动恢复同步，请转到 System Manager 并选择菜单：Mirroring[Synchronous mirroring]，突出显示表中的镜像对，然后选择 *More* 下的 *Resume*。

. 单击*完成*以完成同步镜像序列。

.结果
激活镜像后、系统将执行以下操作：

* 开始在本地存储阵列和远程存储阵列之间进行初始同步。

* 设置同步优先级和重新同步策略。
* 保留控制器HIC编号最高的端口以进行镜像数据传输。
+
只有镜像对中二级卷的远程首选控制器所有者才会接受在此端口上收到的I/O请求。（允许在主卷上进行预留。）

*
创建两个预留容量卷、每个控制器一个、用于记录写入信息、以便从控制器重置和其他临时中断中恢复。
+
每个卷的容量为128 MiB。但是、如果将卷放置在池中、则会为每个卷预留4 GiB。

.完成后
转到 System Manager，然后选择菜单：监控[正在进行的操作
]，以查看同步镜像操作的进度。此操作可能耗时较长，并可能影响系统性能。

:leveloffset: -1

[[ID70ef16e6205e3da6dac3ac575893f79d]]
= SANtricity Unified Manager 存储镜像常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[what-do-i-need-to-know-before-creating-a-mirror-consistency-group]]
== 在创建镜像一致性组之前、我需要了解哪些信息？

在创建镜像一致性组之前、请遵循以下准则。

满足以下Unified Manager要求：

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

此外、请确保满足以下存储阵列要求：

* 必须在Unified Manager中发现这两个存储阵列。
* 每个存储阵列必须具有两个控制器。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。（它们可以分别运行不同的操作系统版本。）
* 您必须知道本地和远程存储阵列的密码。
* 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。

[NOTE]
====
EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

====

[[what-do-i-need-to-know-before-creating-a-mirrored-pair]]
== 在创建镜像对之前、我需要了解哪些信息？

创建镜像对之前、请遵循以下准则。

* 您必须有两个存储阵列。
* 每个存储阵列必须具有两个控制器。
* 必须在Unified Manager中发现这两个存储阵列。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。（它们可以分别运行不同的操作系统版本。）
* 您必须知道本地和远程存储阵列的密码。
* 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
* 具有光纤通道(FC)或iSCSI主机端口的控制器支持异步镜像、而只有具有
FC主机端口的控制器才支持同步镜像。

[NOTE]
====
EF80、EF50、EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

====

[[why-would-i-change-this-percentage]]
== 为什么要更改此百分比？

对于异步镜像操作、预留容量通常为基础卷的20%。通常、此容量足以满足要求。

所需容量因向基础卷写入I/O的频率和大小以及要使用存储对象的副本服务操作的时间而异。通常、如果存在以下一种或两种情况、请选择较大的预留容量百分比：

* 如果特定存储对象的复制服务操作的生命周期很长。
* 如果由于
I/O活动繁重而导致基础卷上的大量数据块发生更改、使用历史性能数据或其他操作系统实用程序帮助您确定基础卷的典型I/O活动。

[[why-do-i-see-more-than-one-reserved-capacity-candidate]]
== 为什么我会看到多个预留容量候选项?

如果一个池或卷组中有多个卷满足您为存储对象选择的容量百分比量、则您将看到多个候选卷。

您可以通过更改要在基础卷上为复制服务操作预留的物理驱动器空间百分比来刷新建议候选对象列表。根据您的选择显示最佳候选对象。

[[why-dont-i-see-all-my-volumes]]
== 为什么我看不到我的所有卷?

为镜像对选择主卷时、列表将显示所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

* 此卷不是最佳卷。
* 此卷已加入镜像关系。
* 对于同步镜像、镜像对中的主卷和二级卷必须是标准卷。它们不能是精简卷或快照卷。
* 对于异步镜像、精简卷必须启用自动扩展。

NOTE：对于EF600和
EF300控制器、异步镜像对中的主卷和二级卷必须匹配相同的协议、托盘级别、区块大小、安全类型和RAID级别。不符合条件的异步镜像对不会显示在可用卷列表中。

[[why-dont-i-see-all-the-volumes-on-the-remote-storage-array]]
== 为什么我看不到远程存储阵列上的所有卷?

在远程存储阵列上选择二级卷时、列表将显示该镜像对的所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

* 此卷是一个非标准卷、例如Snapshot卷。
* 此卷不是最佳卷。
* 此卷已加入镜像关系。
* 对于异步镜像、主卷和二级卷之间的精简卷属性不匹配。
* 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。
+
** 如果主卷已启用DA、则二级卷必须已启用DA。
** 如果主卷未启用DA、则二级卷不能启用DA。

* 对于异步镜像、主卷和二级卷必须具有相同的驱动器安全功能。
+
** 如果主卷支持FIPS、则二级卷必须支持FIPS。
** 如果主卷支持FDE、则二级卷必须支持FDE。
** 如果主卷未使用驱动器安全、则二级卷不得使用驱动器安全。

[[what-impact-does-synchronization-priority-have-on-synchronization-rates]]
== 同步优先级对同步速率有何影响?

同步优先级用于定义为同步活动分配的处理时间与系统性能相关。

主卷的控制器所有者在后台执行此操作。同时、控制器所有者会处理对主卷的本地I/O写入以及对二级卷的相关远程写入。由于重新同步会使控制器处理资源偏离I/O活动、因此重新同步可能会影响主机应用程序的性能。

请牢记以下准则、以帮助您确定同步优先级可能需要多长时间以及同步优先级如何影响系统性能。

可以使用以下优先级：

* 最低
* 低
* 中等
* 高
* 最高

最低优先级速率支持系统性能、但重新同步所需时间较长。最高优先级速率支持重新同步、但系统性能可能会受到影响。

这些准则大致近似于优先级之间的差异。

[cols="45h,~"]
|===
| 完全同步的优先级速率 | 与最高同步速率相比所用时间

a|
最低
a|
约为最高优先级速率的八倍。

a|
低
a|
约为最高优先级速率的六倍。

a|
中等
a|
大约是最高优先级速率的三倍半。

a|
高
a|
大约是最高优先级速率时的两倍。

|===
卷大小和主机I/O速率负载会影响同步时间比较。

[[why-is-it-recommended-to-use-a-manual-synchronization-policy]]
== 为什么建议使用手动同步策略?

建议使用手动重新同步、因为它可以让您以最佳机会恢复数据的方式管理重新同步过程。

如果使用自动重新同步策略、并且在重新同步期间发生间歇性通信问题、则二级卷上的数据可能会暂时损坏。重新同步完成后、数据将得到更正。

:leveloffset: -1

= 证书

:leveloffset: +1

[[ID7eab392eac1efe601af9bb6d57ece6b1]]
= 证书概述
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
通过证书管理、您可以创建证书签名请求(CSR)、导入证书以及管理现有证书。

[[what-are-certificates]]
== 什么是证书?

_Certificates_是数字文件、用于标识网站和服务器等联机实体、以便在互联网上进行安全通信。证书有两种类型：_signed certificate"由证书颁发机构(CA)验证；_self-signed certificate"由实体所有者(而不是第三方)验证。

了解更多信息。

* xref:{relative_path}how-certificates-work-unified.html["证书的工作原理"]
* xref:{relative_path}certificate-terminology-unified.html["证书术语"]

[[how-do-i-configure-certificates]]
== 如何配置证书?

在证书管理中、您可以为托管Unified Manager的管理工作站配置证书、也可以为阵列中的控制器导入证书。

了解更多信息。

* xref:{relative_path}use-ca-signed-certificate-um.html["对管理系统使用CA签名的证书"]
* xref:{relative_path}import-array-certificates-unified.html["导入阵列的证书"]

= 概念

:leveloffset: +1

[[ID810a9ff62c66389face9271afe1939a8]]
= 证书在 SANtricity Unified Manager 中的工作方式
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[signed-certificates]]
== 签名证书

证书可确保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Unified Manager、您可以管理主机管理系统上的浏览器证书以及发现的存储阵列中的控制器证书。

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。

[NOTE]
====
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。

[[self-signed-certificates]]
== 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"`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。

[[certificates-for-unified-manager]]
== Unified Manager的证书

Unified Manager界面随Web服务代理一起安装在主机系统上。打开浏览器并尝试连接到Unified Manager时、浏览器会尝试通过检查数字证书来验证主机是否为可信源。如果浏览器找不到服务器的CA签名证书、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。或者、您也可以从CA获取签名的数字证书、以便不再显示警告消息。

[[certificates-for-controllers]]
== 控制器的证书

在Unified Manager会话期间、当您尝试访问没有CA签名证书的控制器时、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Web服务代理服务器可以对来自这些控制器的传入客户端请求进行身份验证。

[[ID63353279ba7fc64862855103614a8f31]]
= 了解 SANtricity Unified Manager 中的证书术语

```
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
以下术语适用于证书管理。

```
[cols="25h,~"]
|===
| 期限 | Description


 a|
CA
 a|
```
证书颁发机构(Certificate Authority、
CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

```
 a|
CSR
 a|
```
证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述所需的信息。

```
 a|
```
证书
```
 a|
```
出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。

```
 a|
```
证书链
```
 a|
```
一种文件层次结构、用于向证书添加一层安全保护。通常、此链包含一个位于层次结构顶部的根证书、一个或多个中间证书以及用于标识实体的服务器证书。

a|
中间证书

a|
一个或多个中间证书从证书链中的根分支。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。

a|
密钥库

a|
密钥库是主机管理系统上的存储库、其中包含私钥及其对应的公有
密钥和证书。这些密钥和证书用于标识您自己的实体、例如控制器。

a|
根证书

a|
根证书位于证书链中的层次结构顶部、其中包含用于对其他证书签名的专用密钥。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。

a|
签名证书

a|
由证书颁发机构(CA)验证的证书。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。此外、签名证书还包括实体所有者的详细信息(通常为服务器或网站)以及由字母和数字组成的数字签名。签名证书使用信任链、因此最常用于生产环境。也称为"CA签名证书"或"管理证书"。

a|
自签名证书

a|
自签名证书由实体的所有者进行验证。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。它还包括由字母和数字组成的数字签名。自签名证书与CA签名证书使用的信任链不同、因此最常用于测试环境。也称为"预安装"证书。

a|
服务器证书

a|
服务器证书位于证书链的底部。它标识您的特定实体、例如网站或其他设备。存储系统中的每个控制器都

需要一个单独的服务器证书。

 a|
信任存储库
 a|
信任存储库是一个存储库、其中包含来自CA等可信第三方的证书。

|===

:leveloffset: -1

[[IDca005c3401cf12a06add0531a0872d30]]
= 对管理系统使用CA签名的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以获取并导入CA签名的证书、以便安全访问托管SANtricity统一管理器的管理系统。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.关于此任务
使用CA签名证书是一个三步操作步骤。

[[step-1-complete-a-csr-file]]
== 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安装了Web服务代理和Unified Manager的主机系统。

[NOTE]
====
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
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 从管理选项卡中、选择*完成CSR*。
. 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。

. 输入有关安装了Web服务代理的主机系统的以下信息：
+
** *公用名*—安装了Web服务代理的主机系统的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Unified
Manager。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。

. 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。
. 单击 * 完成 * 。
. 转至 <<第2步：提交CSR文件>>。

[[step-2-submit-csr-file]]
== 第2步：提交CSR文件

创建证书签名请求(CSR)文件后、您可以将其发送到证书颁发机构(CA)、以接收托管Unified
Manager和Web服务代理的系统的已签名管理证书。

NOTE: 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
. 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。

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

+
[CAUTION]
====
*将CSR文件提交给CA后、请勿重新生成另一个CSR文件。*每当生成CSR时、系统都会创建一个专用和公有密钥对。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。

====
. 当CA返回签名证书时、转到 <<第3步：导入管理证书>>。

[[step-3-import-management-certificates]]
== 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了Web服务代理和Unified Manager界面的主机系统中。

.开始之前
* 您已从CA收到签名证书。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。
* 您已将证书文件复制到运行Web服务代理的主机系统。

.步骤
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 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。

. 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。

. 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。

[[IDfc72f89d87c9f452be26628745764863]]
= 重置管理证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将管理证书还原到原始出厂自签名状态。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.关于此任务
此任务将从安装了Web服务代理和Unified Manager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
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 选择*阵列管理*选项卡，然后选择*重置*。
+
此时将打开确认重置管理证书对话框。

. 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。

= 使用阵列证书

:leveloffset: +1

[[ID1c2b28bf2ef1095b97bca815ba963bcb]]
= 在 SANtricity Unified Manager 中导入阵列证书
:allow-uri-read:
:experimental:
:icons: font

:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如有必要、您可以导入存储阵列的证书、以便这些证书可以在托管SANtricity Unified Manager的系统中进行身份验证。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
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 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
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 选择*可信*选项卡。
+
此页面显示为存储阵列报告的所有证书。

. 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。
+
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。

. 在对话框中、选择证书、然后单击*导入*。
+
已上传并验证此证书。

[[ID7e9eda7ce03affcb289a7536765d4b9e]]
= 在 SANtricity Unified Manager 中删除受信任的证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[CAUTION]

====
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
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 选择*可信*选项卡。
. 在表中选择一个或多个证书、然后单击*删除*。
+
[NOTE]
====
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。

. 确认删除、然后单击*删除*。
+
此证书将从表中删除。

[[IDa926be8a606eeb97ca5ef945b1d25ece]]
= 解析不可信的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果存储阵列尝试建立与SANtricity Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。

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
* 您必须使用具有安全管理员权限的用户配置文件登录。
* 如果您计划导入CA签名的证书：
+
** 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。
* 一个或两个证书均已过期。
* 一个或两个证书均已撤销。
* 一个或两个证书缺少根证书或中间证书。

.步骤
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 选择*可信*选项卡。
+
此页面显示为存储阵列报告的所有证书。

. 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。
+
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。

. 在对话框中、选择证书、然后单击*导入*。
+
已上传并验证此证书。

:leveloffset: -1

= 管理证书

:leveloffset: +1

[[IDafeabd041eac098a2590d0331cf43230]]
= 查看证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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)。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.步骤
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 选择以下选项卡之一：
+
** *管理*-显示托管Web服务代理的系统的证书。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Unified Manager。
** *可信*-显示Unified Manager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。

. 要查看有关证书的更多信息，请选择其行，选择该行末尾的省略号，然后单击 *View* 或 *Export*。

[[ID152a90368c5a6b513139406d821296df]]
= 在 SANtricity Unified Manager 中导出证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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
. 从左侧面板中，选择菜单：Settings[Certificates]。
. 选择以下选项卡之一：
+
** *管理*-显示托管Web服务代理的系统的证书。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Unified Manager。

** *可信*-显示Unified Manager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。

. 从页面中选择一个证书，然后单击该行末尾的省略号。
. 单击*导出*、然后保存证书文件。
. 在证书查看器应用程序中打开文件。

:leveloffset: -1

:leveloffset: -1

= 访问管理

:leveloffset: +1

[[IDd3eaac57b1b217fa8ce6e32554b76a1b]]
= 了解 SANtricity Unified Manager 访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
访问管理是一种在SANtricity Unified Manager中配置用户身份验证的方法。

[[what-authentication-methods-are-available]]
== 有哪些身份验证方法可用?

可以使用以下身份验证方法：

* *本地用户角色*—身份验证通过RBAC （基于角色的访问控制)功能进行管理。本地用户角色包括预定义的用户配置文件以及具有特定访问权限的角色。
* *目录服务*—身份验证通过LDAP （轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)进行管理。
* * SAML *-身份验证通过使用SAML 2.0的身份提供程序(Identity Provider、IdP)进行管理。

了解更多信息。

* xref:{relative_path}how-access-management-works-unified.html["访问管理的工作原理"]
* xref:{relative_path}access-management-terminology-unified.html["访问管理术语"]
* xref:{relative_path}permissions-for-mapped-roles-unified.html["映射角色的权限"]
* xref:{relative_path}access-management-with-saml.html["SAML"]

[[how-do-i-configure-access-management]]
== 如何配置访问管理?

SANtricity 软件已预先配置为使用本地用户角色。如果要使用LDAP、可以在访问管理页面下对其进行配置。

了解更多信息。

* xref:{relative_path}access-management-with-local-user-roles-unified.html["具有本地用户角色的访问管理"]
* xref:{relative_path}access-management-with-directory-services-unified.html["使用目录服务进行访问管理"]
* xref:{relative_path}configure-saml.html["配置SAML"]

= 概念

:leveloffset: +1

[[IDa1fcd9c3b97921d11548db6d7d471a80]]
= SANtricity Unified Manager 中的访问管理工作原理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
使用访问管理在SANtricity Unified Manager中建立用户身份验证。

[[configuration-workflow]]
== 配置工作流

访问管理配置的工作原理如下：

. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
首次登录时、系统会自动显示用户名`admin`、并且无法更改。`admin`用户可以完全访问系统中的所有功能。必须在首次登录时设置密码。

====
. 管理员可在用户界面中导航到访问管理、其中包括预配置的本地用户角色。这些角色是对RBAC（基于角色的访问控制）功能的实施。
. 管理员配置以下一种或多种身份验证方法：
+
** *本地用户角色*—身份验证通过RBAC功能进行管理。本地用户角色包括具有特定访问权限的预定义用户和角色。管理员可以使用这些本地用户角色作为单一身份验证方法、也可以将其与目录服务结合使用。除了为用户设置密码之外、无需进行任何配置。
** *目录服务*—身份验证通过LDAP （轻型目录访问协议）服务器和目录服务（例如Microsoft的Active Directory）进行管理。管理员连接到LDAP服务器、然后将LDAP用户映射到本地用户角色。
** * SAML *-身份验证通过使用安全断言标记语言（SAML） 2.0的身份提供程序（IdP）进行管理。管理员在IdP系统和存储阵列之间建立通信、然后将IdP用户映射到存储阵列中嵌入的本地用户角色。

. 管理员为用户提供Unified Manager的登录凭据。
. 用户通过输入凭据登录到系统。登录期间、系统将执行以下后台任务：
+
** 根据用户帐户对用户名和密码进行身份验证。
** 根据分配的角色确定用户的权限。
** 使用户能够访问用户界面中的功能。
** 在顶部横幅中显示用户名。

[[functions-available-in-unified-manager]]
== Unified Manager中提供的功能

对功能的访问权限取决于为用户分配的角色、这些角色包括：

* *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。

* *安全管理*—访问访问管理和证书管理中的安全配置。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据和MEL事件。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

不可用的功能将灰显或不显示在用户界面中。

[[ID9ef2d4466621393c0e711c5edade6d93]]
= 了解 SANtricity Unified Manager 访问管理术语
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解访问管理术语如何适用于SANtricity Unified Manager。

[cols="25h,~"]
|===
| 期限 | Description

a|
Active Directory
a|
Active Directory (AD)是一种Microsoft目录服务、使用LDAP进行Windows域网络。

a|
绑定
a|
绑定操作用于向目录服务器对客户端进行身份验证。绑定通常需要帐户和密码凭据、但某些服务器允许匿名绑定操作。

a|
CA
a|
证书颁发机构(Certificate Authority、
CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

a|
证书
a|
出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。

a|
LDAP
a|
轻型目录访问协议(Lightweight Directory Access Protocol、LDAP)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。此协议允许许多不同的应用程序和服务连接到LDAP服务器以验证用户。

a|
RBAC
a|
基于角色的访问控制(Role-Based Access Control、RBAC)是一种根据各个用户的角色来管理对计算机或网络资源的访问的方法。Unified Manager包含预定义角色。

a|
SAML
a|
安全断言标记语言(SAML)是一种基于XML的标准、用于在两个实体之间进行身份验证和授权。SAML支持多因素身份验证、在这种身份验证中、用户必须提供两个或更多项来证明其身份(例如密码和指纹)。存储阵列的嵌入式SAML功能在身份断言、身份验证和授权方面符合SAML2.0标准。

a|
SSO
a|
单点登录(SSO)是一种身份验证服务、允许一组登录凭据访问多个应用程序。

a|
Web服务代理
a|

Web服务代理可通过标准HTTPS机制提供访问、允许管理员为存储阵列配置管理服务。代理可以安装在Windows或Linux主机上。Unified Manager界面可用于Web服务代理。

|===

[[IDcb634e391d03a5455d6064428faab8d6]]
= 映射角色的权限
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
RBAC （基于角色的访问控制）
功能包括已映射一个或多个角色的预定义用户。每个角色都具有访问SANtricity Unified Manager中任务的权限。

这些角色可为用户提供对任务的访问权限、如下所示：

* *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理和证书管理中的安全配置。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据和MEL事件。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

如果用户没有对某个功能的权限、则该功能不可供选择或不会显示在用户界面中。

[[ID9ec4598ff8dc9c3c859879ebe8a70542]]
= SANtricity Unified Manager 中的本地用户角色访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理员可以使用SANtricity 统一管理器中强制实施的RBAC （基于角色的访问控制）
功能。这些功能称为"本地用户角色"。

[[configuration-workflow]]

== 配置工作流

本地用户角色已在系统中预先配置。要使用本地用户角色进行身份验证、管理员可以执行以下操作：

. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
`admin`用户可以完全访问系统中的所有功能。

====
. 管理员会查看用户配置文件、这些配置文件是预定义的、无法修改。
. 管理员也可以为每个用户配置文件分配新密码。
. 用户使用分配的凭据登录到系统。

[[management]]
== 管理

如果仅使用本地用户角色进行身份验证、则管理员可以执行以下管理任务：

* 更改密码。
* 设置密码的最小长度。
* 允许用户在不使用密码的情况下登录。

[[IDeb35b2817601199d61baee0fdface6dc]]
= 使用 SANtricity Unified Manager 中的目录服务进行访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理员可以使用LDAP （轻型目录访问协议）服务器和目录服务、例如Microsoft的Active Directory。

[[configuration-workflow]]
== 配置工作流

如果在网络中使用LDAP服务器和目录服务、则配置的工作原理如下：

. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
`admin`用户可以完全访问系统中的所有功能。

====
. 管理员输入LDAP服务器的配置设置。设置包括域名、URL和绑定帐户信息。
. 如果LDAP服务器使用安全协议(LDAPS)、则管理员将上传证书颁发机构(CA)证书链、以便在LDAP服务器与安装了Web服务代理的主机系统之间进行身份验证。
. 建立服务器连接后、管理员会将用户组映射到本地用户角色。这些角色是预定义的、无法修改。
. 管理员测试LDAP服务器与Web服务代理之间的连接。
. 用户使用其分配的LDAP/Directory服务凭据登录到系统。

[[management]]
== 管理

使用目录服务进行身份验证时、管理员可以执行以下管理任务：

* 添加目录服务器。
* 编辑目录服务器设置。
* 将LDAP用户映射到本地用户角色。
* 删除目录服务器。
* 更改密码。
* 设置密码的最小长度。
* 允许用户在不使用密码的情况下登录。

[[ID610bc27a5a32358fa4e71343b56a2730]]
= 使用 SANtricity Unified Manager 中的 SAML 进行访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于访问管理、管理员可以使用阵列中嵌入的安全断言标记语言(Security Assertion Markup Language、SAML) 2.0功能。

[[configuration-workflow]]
== 配置工作流

SAML配置的工作原理如下：

. 管理员使用包含"安全管理员"权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
`admin`用户可以完全访问System Manager中的所有功能。

====
. 管理员转到访问管理下的* SAML *选项卡。
. 管理员配置与身份提供程序(Identity Provider、IdP)的通信。
IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。要配置与存储阵列的通信、管理员需要从Idp系统下载Idp元数据文件、然后使用Unified Manager将该文件上传到存储阵列。
. 管理员在服务提供商和
IdP之间建立信任关系。服务提供商负责控制用户授权；在这种情况下、存储阵列中的控制器充当服务提供商。要配置通信、管理员可使用Unified
Manager导出控制器的服务提供商元数据文件。然后、管理员会从Idp系统将元数据文件导入到Idp中。
+
[NOTE]
====
管理员还应确保IdP支持在身份验证时返回名称ID。

====
. 管理员会将存储阵列的角色映射到IdP中定义的用户属性。为此、管理员使用Unified
Manager创建映射。
. 管理员测试对IdP URL的SSO登录。此测试可确保存储阵列和IdP能够进行通信。
+
[CAUTION]
====
启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
. 在Unified Manager中、管理员可为存储阵列启用SAML。
. 用户使用其SSO凭据登录到系统。

[[management]]
== 管理

使用SAML进行身份验证时、管理员可以执行以下管理任务：

* 修改或创建新角色映射
* 导出服务提供商文件

[[access-restrictions]]
== 访问限制

启用SAML后、用户无法从原有Storage Manager界面发现或管理该阵列的存储。

此外、以下客户端无法访问存储阵列服务和资源：

* 企业管理窗口(EMW)
* 命令行界面（ CLI ）
* 软件开发人员套件(SDK)客户端
* 带内客户端
* HTTP基本身份验证REST API客户端
* 使用标准REST API端点登录

:leveloffset: -1

= 使用本地用户角色

:leveloffset: +1

[[ID26515b4c6081b504939cad852ec8ae0b]]
= 查看本地用户角色
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在本地用户角色选项卡中、您可以查看用户与默认角色的映射。这些映射是在适用于SANtricity Unified Manager的Web服务代理中强制实施的RBAC （基于角色的访问控制）的一部分。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
无法更改用户和映射。只能修改密码。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择*本地用户角色*选项卡。
+
下表显示了这些用户：

+
** *管理员*—超级管理员、有权访问系统中的所有功能。此用户包括所有角色。
** *存储*—负责所有存储配置的管理员。此用户包括以下角色：存储管理员、支持管理员和监控。
** *安全性
*—负责安全性配置的用户、包括访问管理和证书管理。此用户包括以下角色：安全管理员和监控。
** *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：支持管理员和监控。
** *监控*—对系统具有只读访问权限的用户。此用户仅包含监控角色。
** *读/写*—此用户包括以下角色：存储管理员、支持管理员和监控。
** * ro *(只读)—此用户仅包含监控角色。

[[ID0ff0cd098f41b92170b572e2987769dc]]
= 在 SANtricity Unified Manager 中更改本地用户配置文件的密码
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以在Access Management中更改每个用户的用户密码。

.开始之前
* 您必须以本地管理员身份登录、其中包括root管理员权限。
* 您必须知道本地管理员密码。

.关于此任务
选择密码时、请记住以下准则：

* 任何新的本地用户密码必须满足或超过当前最低密码设置(在"查看/编辑设置"中)。
* 密码区分大小写。
* 设置密码时、不会从密码中删除尾随空格。如果密码中包含空格、请小心操作。

* 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择*本地用户角色*选项卡。
. 从表中选择一个用户。
+
更改密码按钮将变为可用。

. 选择 * 更改密码 * 。
+
此时将打开更改密码对话框。

. 如果未为本地用户密码设置最小密码长度、则可以选中此复选框以要求用户输入密码以访问系统。
. 在两个字段中输入选定用户的新密码。
. 输入本地管理员密码以确认此操作、然后单击*更改*。

.结果
如果用户当前已登录、则更改密码会导致用户的活动会话终止。

[[IDf20c1cd190ce6bd6d460caad23c5c6a4]]
= 在 SANtricity Unified Manager 中更改本地用户密码设置
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以为所有新的或更新的本地用户密码设置所需的最小长度。您还可以允许本地用户访问系统而无需输入密码。

.开始之前
您必须以本地管理员身份登录、其中包括root管理员权限。

.关于此任务
设置本地用户密码的最小长度时、请记住以下准则：

* 设置更改不会影响现有本地用户密码。
* 本地用户密码的最小长度设置必须介于0到30个字符之间。
* 任何新的本地用户密码都必须满足或超过当前的最小长度设置。
* 如果希望本地用户在未输入密码的情况下访问系统、请勿设置密码的最小长度。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择*本地用户角色*选项卡。
. 选择*查看/编辑设置*。
+
此时将打开本地用户密码设置对话框。

. 执行以下操作之一：
+
** 要允许本地用户在不输入密码的情况下访问系统、请清除"至少需要所有本地用户密码"复选框。
** 要为所有本地用户密码设置最小密码长度、请选中"要求所有本地用户密码至少为"
复选框、然后使用spinner框设置所有本地用户密码所需的最小长度。
+
任何新的本地用户密码都必须满足或超过当前设置。

. 单击 * 保存 * 。

:leveloffset: -1

= 使用目录服务

:leveloffset: +1

[[ID2f508c8c73bcee5ed50ec3a4eb926c9c]]
= 在 SANtricity Unified Manager 中添加目录服务器
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要为访问管理配置身份验证、请在LDAP服务器与运行适用于SANtricity Unified Manager的Web服务代理的主机之间建立通信。然后、将LDAP用户组映射到本地用户角色。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 必须在目录服务中定义用户组。
* LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。

* 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

.关于此任务
添加目录服务器分为两步。首先输入域名和URL。如果服务器使用安全协议、则如果CA证书由非标准签名颁发机构签名、则还必须上传此CA证书以进行身份验证。如果您拥有绑定帐户的凭据、则还可以输入您的用户帐户名称和密码。接下来、将LDAP服务器的用户组映射到本地用户角色。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 从*目录服务*选项卡中、选择*添加目录服务器*。
+
此时将打开添加目录服务器对话框。

. 在*服务器设置*选项卡中、输入LDAP服务器的凭据。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

 a|
配置设置

 a|
域
 a|
输入LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(_username_@_domain_)以指定要对其进行身份验证的目录服务器。

 a|
服务器URL
 a|
输入用于访问LDAP服务器的URL、格式为`ldap：//*主机*：*端口*`。

 a|
上传证书(可选)
 a|

NOTE：只有在上述服务器URL字段中指定了LDAPS协议时、才会显示此字段。

单击*浏览*并选择要上传的CA证书。这是用于对LDAP服务器进行身份验证的可信证书或证书链。

a|
绑定帐户（可选）
a|
输入一个只读用户帐户、用于对LDAP服务器进行搜索查询以及在组中进行搜索。以LDAP类型格式输入帐户名称。例如、如果绑定用户名为"bindAcct"、则可以输入一个值、例如`cn=bindAcct、cn=users、DC=cpoc、DC=local`。

a|
绑定密码（可选）
a|

NOTE：输入绑定帐户时会显示此字段。

输入绑定帐户的密码。

a|
添加前测试服务器连接
a|
如果要确保系统可以与您输入的LDAP服务器配置进行通信、请选中此复选框。单击对话框底部的*添加*后、将进行测试。

如果选中此复选框且测试失败、则不会添加配置。您必须解决此错误或取消选中此复选框、才能跳过测试并添加配置。

a|
权限设置

a|
搜索基础DN
a|
输入LDAP环境以搜索用户、通常采用的形式 `CN=Users, DC=cpoc, DC=local`。

a|
username属性
a|
输入绑定到用户ID的属性以进行身份验证。例如：`sAMAccountName`。

a|
组属性
a|
输入用户上的组属性列表、用于组到角色映射。例如：`memberOf、managedObjects`。

|===
====
. 单击*角色映射*选项卡。
. 将LDAP组分配给预定义角色。一个组可以分配多个角色。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

a|
映射

a|
组DN
a|
为要映射的LDAP用户组指定组可分辨名称(DN)。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(\)进行转义：\.[] {} ()<>*+-=！？^$\

a|
角色
a|
单击此字段、然后选择要映射到组DN的本地用户角色之一。您必须单独为此组选择要包含的每个角色。要登录到SANtricity Unified
Manager、需要将监控角色与其他角色结合使用。映射的角色包括以下权限：

** *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理和证书管理中的安全配置。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据和MEL事件。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+

NOTE: 包括管理员在内的所有用户都需要"监控"角色。

. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
. 完成映射后、单击*添加*。
+
系统将执行验证、以确保存储阵列和LDAP服务器可以进行通信。如果显示错误消息、请检查在对话框中输入的凭据、并根据需要重新输入信息。

[[ID253646a21ddd687ce33bf37b6e887bbb]]
= 在 SANtricity Unified Manager 中编辑目录服务器设置和角色映射
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果您之前在Access Management中配置了目录服务器、则可以随时更改其设置。设置包括服务器连接信息和组到角色映射。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 必须定义目录服务器。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择*目录服务*选项卡。
. 如果定义了多个服务器、请从表中选择要编辑的服务器。
. 选择*查看/编辑设置*。
+
此时将打开目录服务器设置对话框。

. 在*服务器设置*选项卡中、更改所需设置。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

a|
配置设置

a|
域
a|
LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(_username_@_domain_)以指定要对其进行身份验证的目录服务器。

a|
服务器URL
a|
用于以形式访问LDAP服务器的URL `ldap[s]://host:port`。

a|
绑定帐户(可选)
a|
用于对LDAP服务器进行搜索查询以及在组内进行搜索的只读用户帐户。

a|
绑定密码(可选)
a|
绑定帐户的密码。(输入绑定帐户时会显示此字段。)

a|
保存前测试服务器连接
a|

检查系统是否可以与LDAP服务器配置进行通信。单击*保存*后会进行测试。如果选中此复选框且测试失败、则不会更改配置。您必须解决此错误或清除此复选框、才能跳过测试并重新编辑配置。

a|
权限设置

a|
搜索基础DN
a|
用于搜索用户的LDAP环境、通常采用的形式 `CN=Users, DC=cpoc, DC=local`。

a|
username属性
a|
绑定到用户ID进行身份验证的属性。例如：`sAMAccountName`。

a|
组属性
a|
用户上的组属性列表、用于组到角色映射。例如：`memberOf、managedObjects`。

|===
====
. 在*角色映射*选项卡中、更改所需的映射。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

a|
映射

a|

组DN

a|
要映射的LDAP用户组的域名。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(\)进行转义：

\.[] {} ()<>*+-=! ? ^$|

a|
角色

a|
要映射到组DN的角色。您必须单独为此组选择要包含的每个角色。要登录到SANtricity Unified Manager、需要将监控角色与其他角色结合使用。这些角色包括：

** *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理和证书管理中的安全配置。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据和MEL事件。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+

NOTE：包括管理员在内的所有用户都需要"监控"角色。

. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
. 单击 * 保存 * 。

.结果
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

[[IDd4b17f5f6490f06265260ce07bf3e358]]
= 删除目录服务器
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要中断目录服务器与Web服务代理之间的连接、您可以从"访问管理"页面中删除服务器信息。如果您配置了新服务器、然后要删除旧服务器、则可能需要执行此任务。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择*目录服务*选项卡。
. 从列表中、选择要删除的目录服务器。
. 单击 * 删除 * 。
+
此时将打开删除目录服务器对话框。

. 在字段中键入`remove`、然后单击*删除*。
+
此时将删除目录服务器配置设置、权限设置和角色映射。用户无法再使用此服务器的凭据登录。

```
:leveloffset: -1
```

```
= 使用SAML
```

```
:leveloffset: +1
```

```
[[ID15a6a1e9e7287e1656cf1cfadffaa4cf]]
= 在 SANtricity Unified Manager 中配置 SAML
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

```
[role="lead"]
```
要为访问管理配置身份验证、您可以使用存储阵列中嵌入的安全断言标记语言(SAML)功能。此配置将在身份提供程序和存储提供程序之间建立连接。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 您必须知道存储阵列中控制器的IP地址或域名。

* IdP管理员已配置IdP系统。
* IdP管理员已确保IdP支持在身份验证时返回名称ID。
* 管理员已确保IdP服务器和控制器时钟同步(通过NTP服务器或通过调整控制器时钟设置)。
* Idp元数据文件将从Idp系统下载、并可在用于访问Unified Manager的本地系统上使用。

.关于此任务
身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。要在IdP和存储阵列之间建立连接、您需要在这两个实体之间共享元数据文件。接下来、将IdP用户实体映射到存储阵列角色。最后、在启用SAML之前、您需要测试连接和SSO登录。

[NOTE]
====
* SAML和目录服务*。如果在将目录服务配置为身份验证方法时启用SAML、则SAML将取代Unified Manager中的目录服务。如果稍后禁用SAML、则目录服务配置将返回到其先前的配置。

====
[CAUTION]
====
*正在编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
配置SAML身份验证是一个多步骤操作步骤。

[[step-1-upload-the-idp-metadata-file]]
== 第1步：上传IdP元数据文件

要为存储阵列提供Idp连接信息、请将Idp元数据导入到Unified Manager中。IdP系统需要使用此元数据将身份验证请求重定向到正确的URL并验证收到的响应。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择* SAML *选项卡。
+
此页面将显示配置步骤的概述。

. 单击*导入身份提供程序(IdP)文件*链接。
+
此时将打开导入身份提供程序文件对话框。

. 单击*浏览*以选择您复制到本地系统的IdP元数据文件并将其上传。

+
选择文件后、将显示IdP实体ID。

. 单击 * 导入 * 。

[[step-2-export-service-provider-files]]
== 第2步：导出服务提供商文件

要在IdP和存储阵列之间建立信任关系、请将服务提供商元数据导入到IdP中。Idp需要此元数据才能与控制器建立信任关系并处理授权请求。此文件包含控制器域名或IP地址等信息、以便IdP可以与服务提供商进行通信。

.步骤
. 单击*导出服务提供商文件*链接。
+
此时将打开导出服务提供商文件对话框。

. 在*控制器A*字段中输入控制器IP地址或DNS名称、然后单击*导出*将元数据文件保存到本地系统。
+
单击*导出*后、服务提供商元数据将下载到本地系统。记下文件的存储位置。

. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
. 从
Idp服务器中、导入服务提供商元数据文件以建立信任关系。您可以直接导入文件、也可以手动输入文件中的控制器信息。

[[step-3-map-roles]]
== 第3步：映射角色

要为用户提供对Unified Manager的授权和访问权限、您必须将
Idp用户属性和组成员资格映射到存储阵列的预定义角色。

.开始之前
* IdP管理员已在IdP系统中配置用户属性和组成员资格。
* Idp元数据文件将导入到Unified Manager中。
* 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

.步骤
. 单击*映射Unified Manager*角色的链接。
+

此时将打开角色映射对话框。

. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

 a|
映射

 a|
用户属性
 a|
指定要映射的SAML组的属性(例如、"member for")。

 a|
属性值
 a|
指定要映射的组的属性值。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(`\`)进行转义：\.[] {} ()<>*+-=! ？ ^$...

 a|
角色
 a|
单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独选择要包括的每个角色。要登录到Unified Manager、需要将"监控"角色与其他角色结合使用。至少一个组还需要安全管理员角色。

映射的角色包括以下权限：

** *存储管理*—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+
[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

====
. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
+
[NOTE]
====
启用SAML后、可以修改角色映射。

====
. 完成映射后、单击*保存*。

[[step-4-test-sso-login]]
== 第4步：测试SSO登录

为了确保IdP系统和存储阵列可以进行通信、您可以选择测试SSO登录。在启用SAML的最后一步中、也会执行此测试。

.开始之前
* Idp元数据文件将导入到Unified Manager中。
* 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

.步骤
. 选择*测试SSO登录*链接。
+
此时将打开一个对话框、用于输入SSO凭据。

. 输入具有安全管理员权限和监控权限的用户的登录凭据。
+
在系统测试登录时、将打开一个对话框。

. 查找Test Successful消息。如果测试成功完成、请转至下一步以启用SAML。
+
如果测试未成功完成、则会显示一条错误消息、其中包含更多信息。请确保：

+

** 该用户属于具有安全管理员和监控权限的组。
** 您为IdP服务器上传的元数据正确无误。
** SP元数据文件中的控制器地址正确。

[[step-5-enable-saml]]
== 第5步：启用SAML

最后一步是完成用户身份验证的SAML配置。在此过程中、系统还会提示您测试SSO登录。上一步介绍了SSO登录测试过程。

.开始之前
* Idp元数据文件将导入到Unified Manager中。
* 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。
* 至少配置了一个监控器和一个安全管理员角色映射。

[CAUTION]
====
*正在编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
.步骤
. 从* SAML *选项卡中、选择*启用SAML *链接。
+
此时将打开确认启用SAML对话框。

. 键入`enable`、然后单击*启用*。
. 输入用于SSO登录测试的用户凭据。

.结果
系统启用SAML后、它将终止所有活动会话并开始通过SAML对用户进行身份验证。

[[ID4e87240aeb5c12986dc462ddab34a62c]]
= 在 SANtricity Unified Manager 中更改 SAML 角色映射
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果先前已为访问管理配置SAML、则可以更改IdP组与存储阵列的预定义角色之间的角色映射。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* IdP管理员已在IdP系统中配置用户属性和组成员资格。
* 已配置并启用SAML。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择* SAML *选项卡。
. 选择*角色映射*。
+
此时将打开角色映射对话框。

. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。
+
[CAUTION]
====
请注意、在启用SAML的情况下、不要删除您的权限、否则您将无法访问Unified Manager。

====
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 正在设置 ... | Description

 a|
映射

 a|
用户属性
 a|
指定要映射的SAML组的属性(例如、"member for")。

a|
属性值
a|
指定要映射的组的属性值。

a|
角色
a|
单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独为此组选择要包含的每个角色。要登录到Unified Manager、需要将"监控
"角色与其他角色结合使用。必须至少将安全管理员角色分配给一个组。映射的角色包括以下权限：

** *存储管理*—对存储对象（例如卷和磁盘池）具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面（符号）的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+

NOTE: 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

. 或者、也可以单击*添加另一个映射*以输入更多组到角色的映射。
. 单击 * 保存 * 。

.结果
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

[[IDcd5d2f3ad225d2805ea88f8f39798fac]]
= 在 SANtricity Unified Manager 中导出 SAML 服务提供商文件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如有必要、您可以导出存储阵列的服务提供程序元数据、然后将该文件重新导入到身份提供程序(Identity Provider、Idp)系统中。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 已配置并启用SAML。

.关于此任务
在此任务中、您将从控制器导出元数据。Idp需要此元数据才能与控制器建立信任关系并处理身份验证请求。此文件包含IdP可用于发送请求的控制器域名或IP地址等信息。

.步骤
. 从左侧面板中，选择菜单：Settings[Access Management]。
. 选择* SAML *选项卡。
. 选择*导出*。
+
此时将打开导出服务提供商文件对话框。

. 单击*Export*将元数据文件保存到本地系统。
+
[NOTE]
====
域名字段为只读。

====
+
记下文件的存储位置。

. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
. 从Idp服务器中、导入服务提供商元数据文件。您可以直接导入文件、也可以手动输入控制器信息。
. 单击 * 关闭 * 。

:leveloffset: -1

[[ID58d80c684bc1a5e0eec3289502a6a2d4]]
= SANtricity Unified Manager 用户访问管理常见问题解答
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
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。

[[why-cant-i-log-in]]
== 为什么我无法登录?

如果在尝试登录时收到错误、请查看这些可能的原因。

出现登录错误的原因可能如下：

* 您输入的用户名或密码不正确。
* 您的权限不足。
* 您尝试多次登录失败、从而触发锁定模式。等待10分钟以重新登录。
* 已启用SAML身份验证。刷新浏览器以登录。

[[what-do-i-need-to-know-before-adding-a-directory-server]]
== 在添加目录服务器之前、我需要了解哪些信息?

在Access Management中添加目录服务器之前、您必须满足特定要求。

* 必须在目录服务中定义用户组。
* LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
* 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

[[what-do-i-need-to-know-about-mapping-to-storage-array-roles]]
== 关于映射到存储阵列角色、我需要了解哪些信息?

在将组映射到角色之前、请查看相关准则。

RBAC （基于角色的访问控制）功能包括以下角色：

* *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理和证书管理中的安全配置。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据和MEL事件。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。

====
如果您使用的是LDAP （轻型目录访问协议）服务器和目录服务、请确保：

* 管理员已在目录服务中定义用户组。
* 您知道LDAP用户组的组域名。

[[saml]]
=== SAML

如果您使用的是存储阵列中嵌入的安全断言标记语言（SAML）功能、请确保：

* 身份提供程序（Identity Provider、IdP）管理员已在IdP系统中配置用户属性和组成员资格。
* 您知道组成员资格名称。
*
您知道要映射的组的属性值。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠（`\`）进行转义：
+
[listing]

\.[]{}()<>*+-=!?^$|
----
* 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

[[what-do-i-need-to-know-before-configuring-and-enabling-saml]]
== 在配置和启用SAML之前、我需要了解哪些信息？

在配置和启用安全断言标记语言（SAML）身份验证功能之前、请确保满足以下要求并了解SAML限制。

[[requirements]]
=== 要求

开始之前、请确保：

* 已在网络中配置身份提供程序（Identity Provider、IdP）。

IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。您的安全团队负责维护IdP。
* IdP管理员已在IdP系统中配置用户属性和组。
* IdP管理员已确保IdP支持在身份验证时返回名称ID。
* 管理员已确保IdP服务器和控制器时钟同步(通过NTP服务器或通过调整控制器时钟设置)。
* Idp元数据文件将从Idp系统下载、并在用于访问Unified Manager的本地系统上可用。
* 您知道存储阵列中控制器的IP地址或域名。

[[restrictions]]
=== 限制

除了上述要求之外、请确保您了解以下限制：

* 启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。建议您先测试SSO登录、然后再在最终配置步骤中启用SAML。（系统还会在启用SAML之前执行SSO登录测试。）
* 如果您将来禁用SAML、则系统会自动还原先前的配置(本地用户角色和/或目录服务)。
* 如果当前已为用户身份验证配置目录服务、则SAML将覆盖此配置。
* 配置SAML后、以下客户端将无法访问存储阵列资源：
+
** 企业管理窗口(EMW)
** 命令行界面（ CLI ）
** 软件开发人员套件(SDK)客户端
** 带内客户端
** HTTP基本身份验证REST API客户端
** 使用标准REST API端点登录

[[what-are-the-local-users]]
== 本地用户有哪些?

本地用户在系统中预定义、并包括特定权限。

本地用户包括：

* *管理员
*—超级管理员、有权访问系统中的所有功能。此用户包括所有角色。必须在首次登录时设置密码。
* *存储
*—负责所有存储配置的管理员。此用户包括以下角色：存储管理员、支持管理员和监控。在设置密码之前，此帐户将被禁用。

* *安全性
*—负责安全性配置的用户、包括访问管理和证书管理。此用户包括以下角色：安全管理员和监控。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：支持管理员和监控。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。此用户仅包含监控角色。在设置密码之前，此帐户将被禁用。
* *读/写*—此用户包括以下角色：存储管理员、支持管理员和监控。在设置密码之前，此帐户将被禁用。
* * ro *(只读)—此用户仅包含监控角色。在设置密码之前，此帐户将被禁用。

:leveloffset: -1

:leveloffset: -1

[[ID8a4a62ac33b992470401bc8e97e3754f]]
= 早期版本
:allow-uri-read:
:icons: font
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/

[role="lead"]
请访问以下链接以访问早期版本 E 系列硬件和 SANtricity
软件的文档。通过这些链接，您可以访问其他文档站点。

[[hardware-documentation-for-earlier-releases]]
== 早期版本的硬件文档

* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484026["安装 E2712 ，E2724 ， E5612 ， E5624 控制器驱动器托盘以及 DE1600 和 DE5600 扩展驱动器托盘"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484072["安装 E2760 和 E5660 控制器驱动器托盘和 DE6600 扩展驱动器托盘"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484108["安装 EF560 闪存阵列和 DE5600 闪存扩展托盘"^]
* https://mysupport.netapp.com/info/web/ECMP11392380.html["安装旧系统"^]
* https://mysupport.netapp.com/info/web/ECMP11751516.html["维护旧系统"^]
* https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1394872["向 E2600 和 E2700 添加第二个控制器"^]

*
https://library.netapp.com/ecm/ecm_download_file/ECMLP2353447["更改或添加主机协议"^]
*
https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1656638["将交流电源转换为直流电源"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2589397["控制器升级指南—传统控制器型号"^]

[[software-documentation-for-earlier-releases]]
== 早期版本的软件文档

[[santricity-release-11-8]]
=== SANtricity 11.8版

* https://docs.netapp.com/us-en/e-series-santricity-118/index.html["System Manager帮助"^]
* https://docs.netapp.com/us-en/e-series-santricity-118/index.html["Unified Manager帮助"^]

[[santricity-release-11-7]]
=== SANtricity 11.7版

* https://docs.netapp.com/us-en/e-series-santricity-117/index.html["System Manager帮助"^]
* https://docs.netapp.com/us-en/e-series-santricity-117/index.html["Unified Manager帮助"^]

[[santricity-release-11-6]]
=== SANtricity 版本 11.6.

* https://docs.netapp.com/us-en/e-series-santricity-116/index.html["System Manager帮助"^]
* https://docs.netapp.com/us-en/e-series-santricity-116/index.html["Unified Manager帮助"^]

[[santricity-release-11-5]]
=== SANtricity 11.5 版

* https://docs.netapp.com/us-en/e-series-santricity-115/index.html["System Manager帮助"^]

[[santricity-release-11-4]]
=== SANtricity 版本 11.4

* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862590["AMW (E2700、E5600/EF560)帮助"^]
* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862588["EMW (E2700、E5600/EF560)帮助"^]

[[ID15b3d2f4adeb598d148e6e78799b5405]]
= 法律声明
:hardbreaks:
:allow-uri-read:
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/

[role="lead lead"]
法律声明提供对版权声明、商标、专利等的访问。

[[copyright]]
== 版权

link:https://www.netapp.com/company/legal/copyright/["https://www.netapp.com/company/legal/copyright/"^]

[[trademarks]]

== 商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

link:https://www.netapp.com/company/legal/trademarks/["https://www.netapp.com/company/legal/trademarks/"^]

[[patents]]
== 专利

有关 NetApp 拥有的专利的最新列表，请访问：

link:https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf["https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf"^]

[[privacy-policy]]
== 隐私政策

link:https://www.netapp.com/company/legal/privacy-policy/["https://www.netapp.com/company/legal/privacy-policy/"^]

[[open-source]]
== 开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

https://library.netapp.com/ecm/ecm_download_file/ECMLP3368671["E 系列 /EF 系列 SANtricity 操作系统注意事项"]

:leveloffset: -1

<<<
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，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进

行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

NetApp、NetApp 标识和 link:http://www.netapp.com/TM[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。