SANtricity 软件 11.9 文档

SANtricity software

NetApp
March 17, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/e-series-santricity-119/index.html on March 17, 2026. Always check docs.netapp.com for the latest.

目录

SANtricity 软件 11.9 文档 1
发行说明 2
SANtricity OS 11.90 中的新增功能 2
版本 11.90R5 中的新增功能 2
版本 11.90R4 中的新增功能 2
版本 11.90R3 中的新增功能 2
版本 11.90R2 中的新增功能 2
版本 11.90R1 中的新增功能 2
版本 11.90 中的新增功能 2
发行说明 3
开始使用 4
了解 SANtricity 软件 4
SANtricity System Manager 4
SANtricity Unified Manager 5
SANtricity 软件浏览器和操作系统支持 7
浏览器 7
操作系统 7
SANtricity System Manager 设置 8
访问 SANtricity System Manager 8
了解 SANtricity System Manager 安装向导 9
SANtricity System Manager 存储系统设置常见问题解答 10
SANtricity Unified Manager 设置 11
安装 SANtricity Unified Manager 11
访问 SANtricity Unified Manager 12
使用 SANtricity System Manager 11.9 进行单阵列管理 13
主界面 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 21
管理界面设置 22
管理通知 25
SANtricity System Manager 管理界面常见问题解答 29
池和卷组 32
了解 SANtricity System Manager 中的池和卷组 33
概念 33
配置存储 40
管理存储 52
修改池和组设置 57
管理 SSD 缓存 63

管理预留容量 68
SANtricity System Manager 的池和卷组常见问题解答 77
卷和工作负载 87
了解 SANtricity System Manager 中的卷和工作负载 87
概念 88
配置存储 102
管理卷 111
管理设置 116
使用复制服务 122
SANtricity System Manager 的卷和工作负载常见问题解答 128
主机和主机集群 131
了解 SANtricity 软件中的主机和主机集群 131
概念 132
配置主机访问 136
管理主机和集群 140
管理设置 142
SANtricity System Manager 的主机系统和主机集群常见问题解答 145
Snapshot 147
了解 SANtricity System Manager 中的快照 147
概念 148
创建快照和快照对象 159
管理 Snapshot 计划 169
管理 snapshot 镜像 171
管理 Snapshot 一致性组 176
管理快照卷 179
SANtricity System Manager 快照常见问题解答 183
镜像 185
概述 185
异步概念 187
同步概念 196
管理异步镜像一致性组 203
管理异步镜像对 208
管理同步镜像对 212
停用镜像 215
SANtricity System Manager 异步镜像常见问题解答 216
SANtricity System Manager 同步镜像常见问题解答 220
远程存储 223
了解 SANtricity System Manager 中的远程存储功能 223
概念 224
管理远程存储 228
SANtricity System Manager 远程存储常见问题解答 231

硬件组件 234
在 SANtricity System Manager 中查看和管理硬件组件 234
相关信息 234
概念 234
管理货架组件 241
管理控制器 246
管理 iSCSI 端口 257
管理 NVMe 端口 266
管理驱动器 269
管理热备盘 281
适用于 SANtricity System Manager 的存储架常见问题解答 284
SANtricity System Manager 存储控制器常见问题解答 286
适用于 SANtricity System Manager 的 iSCSI 协议常见问题解答 288
适用于 SANtricity System Manager 的 NVMe 协议常见问题解答 291
SANtricity System Manager 存储驱动器常见问题解答 293
警报 294
了解 SANtricity System Manager 中的警报 294
概念 294
管理电子邮件提醒 296
管理 SNMP 警报 299
管理 syslog 警报 306
SANtricity System Manager 存储系统警报常见问题解答 308
阵列设置 309
了解 SANtricity System Manager 中的设置概述 309
概念 309
配置数组设置 312
配置附加功能 317
下载 SANtricity 命令行界面 (CLI) 320
SANtricity System Manager 存储阵列设置常见问题解答 321
驱动器安全性 322
了解 SANtricity System Manager 中的驱动器安全性 322
概念 323
配置安全密钥 327
管理安全密钥 330
SANtricity System Manager 存储驱动器安全常见问题解答 337
访问管理 339
了解 SANtricity System Manager 中的访问管理 339
概念 340
使用本地用户角色 346
使用目录服务 348
使用 SAML 356

使用访问令牌 361
管理 syslog 363
SANtricity System Manager 用户访问管理常见问题解答 368
证书 371
了解 SANtricity System Manager 中的证书 371
概念 372
使用证书 374
SANtricity System Manager 的 CA 签名证书和自签名证书常见问题解答 382
支持 383
在 SANtricity System Manager 中获取支持 383
查看信息和诊断 383
收集诊断数据 387
采取恢复操作 390
管理 AutoSupport 392
查看事件 398
管理升级 400
AutoSupport 常见问题解答，适用于 SANtricity System Manager 411
使用 SANtricity Unified Manager 7 进行多阵列管理 417
主界面 417
了解 SANtricity Unified Manager 417
SANtricity Unified Manager 支持的浏览器 418
了解 SANtricity Unified Manager 中的管理员密码保护 418
在 SANtricity Unified Manager 中更改管理员密码 419
在 SANtricity Unified Manager 中管理会话超时 419
存储阵列 420
了解 SANtricity Unified Manager 中的发现 420
概念 420
发现阵列 422
管理阵列 425
设置导入 426
了解如何在 SANtricity Unified Manager 中导入存储阵列设置 426
概念 427
使用批量导入 429
SANtricity Unified Manager 导入设置常见问题 433
阵列组 434
了解 SANtricity Unified Manager 中的组概述 434
在 SANtricity Unified Manager 中配置存储阵列组 434
从 SANtricity Unified Manager 中的组中删除存储阵列 435
在 SANtricity Unified Manager 中删除存储阵列组 435
在 SANtricity Unified Manager 中重命名存储阵列组 435
升级 436

了解 SANtricity Unified Manager 中的升级中心 436
升级软件和固件 438
镜像 442
了解 SANtricity Unified Manager 中的镜像 442
概念 442
配置镜像 447
SANtricity Unified Manager 的存储镜像常见问题 452
证书 455
证书概述 455
概念 456
为管理系统使用 CA 签名的证书 458
重置管理证书 460
使用阵列证书 461
管理证书 463
访问管理 464
了解 SANtricity Unified Manager 访问管理 464
概念 464
使用本地用户角色 469
使用目录服务 471
使用 SAML 478
SANtricity Unified Manager 用户访问管理常见问题 483
早期版本 487
早期版本的硬件文档 487
早期版本的软件文档 487
SANtricity 11.8 版本 487
SANtricity 11.7 版本 487
SANtricity 11.6 版本 487
SANtricity 11.5 版本 487
SANtricity 11.4 版本 487
法律声明 489
版权 489
商标 489
专利 489
隐私政策 489
开源 489

SANtricity 软件 11.9 文档

发行说明

SANtricity OS 11.90 中的新增功能

下表介绍了 SANtricity System Manager 11.9 中的新功能。

版本 11.90R5 中的新增功能

此版本仅包含缺陷修复，不包含新功能。有关此版本中更改的更多信息，请参见 E-Series SANtricity 操作系统 11.90R5 README。

版本 11.90R4 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 11.90R4 README。

版本 11.90R3 中的新增功能

新功能	说明
SANtricity 操作系统支持 IOM12C 和 DCM3	现在，控制器固件 11.90R3 或更高版本可支持 IOM12C 和 DCM3 SAS-3 盘架。IOM12C 和 DCM3 盘架是 IOM12B 和 DCM2 盘架的替代品。

版本 11.90R2 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 11.90 发行说明"。

版本 11.90R1 中的新增功能

新功能	说明
全新存储系统型号 – EF300C 和 EF600C	此版本引入了 EF300C 和 EF600C 全闪存 NVMe 存储系统。EF300C 和 EF600C 是现有 EF300 和 EF600 存储系统的大容量闪存版本。EF300C 和 EF600C 支持 30TB 或 60TB 大小的大容量 NVMe SSD 驱动器。EF300C/EF600C 仅与动态磁盘池兼容，不支持传统 RAID。
EF4000 上支持 12Gb SAS 接口	E4000 控制器现在支持 12Gb SAS 主机接口卡。

版本 11.90 中的新增功能

新功能	说明
新存储系统型号 – E4000	此版本引入了 E4000 低成本存储系统。E4000 每个控制器支持 12 和 60 个驱动器和一个主机接口卡 (HIC)。对于初始版本，支持的主机接口卡包括 iSCSI 和光纤通道。可在 Unified Manager 中查看和管理 E4000 存储系统和其他 E-Series 存储系统。
动态磁盘池容量增加	当池中每个单独驱动器的容量大于 23 TB 时，Dynamic Disk Pools (DDP) 的容量将增加到 12 PB。如果单个驱动器容量小于 23 TB，则 DDP 容量为 6 PB。
默认媒体扫描设置已增加	默认媒体扫描速率已提高到 120 天。
外部密钥管理现已接受私钥	现在可以通过 System Manager 导入通过私钥和公钥对从外部生成的证书签名请求 (CSR) 文件。
登录锁定功能现在可用于 Web Services	现在，仅可通过 REST API 配置的新登录锁定设置可用于嵌入式和代理 Web 服务。

发行说明

发行说明可在本网站之外找到。系统会提示您使用 NetApp Support Site 凭据登录。

- "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"

开始使用

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。

本网站介绍如何使用以下 SANtricity 管理接口：

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

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

SANtricity System Manager

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。安装向导可帮助您开始系统配置。

System Manager 提供各种管理功能，包括：

性能
最多可查看 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、卷复制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一些功能，例如分配热备用驱动器。
警报
通知管理员存储阵列上发生的重要事件。警报可以通过电子邮件、SNMP 陷阱和 syslog 发送。
访问管理
配置用户身份验证，要求用户使用分配的凭据登录系统。
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，以监控存储阵列的运行状况，并将自动调度发送给技术支持。

SANtricity Unified Manager

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 E4000、E2800、EF280、EF300、E5700、EF570、EF600、EF300C 和 EF600C。您还可以在选定的存储阵列上执行批处理操作。

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

Unified Manager 提供多种管理功能，包括：

发现存储阵列

查找并添加要在组织网络中管理的存储阵列。然后，您可以从单个页面查看所有存储阵列的状态。

启动

打开 System Manager 实例以对特定存储阵列执行单个管理操作。

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

在多个存储阵列上升级 SANtricity 操作系统软件。

证书
创建证书签名请求 (CSR)、导入证书以及管理多个存储阵列的现有证书。
访问管理
配置要求用户使用分配的凭据登录到 Unified Manager 的用户身份验证。

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	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

对于 Unified Manager，Web Services Proxy 必须已安装并可供浏览器使用。有关详细信息，请参见 "SANtricity Web Services Proxy 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)	7.x、8.x / 64 位
SuSE Linux Enterprise Server (SLES)	12.x、15.x / 64 位
Oracle Linux (OL)	7.x、8.x / 64 位

操作系统	最低版本/架构
Windows Server	2016、2019、2022 / 64 位
Ubuntu	18.04、20.04 / 64 位

SANtricity System Manager 设置

访问 SANtricity System Manager

要访问 SANtricity System Manager 用户界面，请将浏览器指向控制器的 IP 地址。安装向导可帮助您开始系统配置。

开始之前

- 按照快速配置指南中的说明安装和配置硬件：
  - "Linux Express 配置"
  - "VMware Express 配置"
  - "Windows Express 配置"
- 配置满足以下要求的管理站：
  - 连接到 1 Gbps 或更快的网络。
  - 连接到与存储管理端口相同的子网。
  - 用作单独的工作站，而不是用于数据管理的主机（I/O 附加）。
  - 设置为带外管理，其中存储管理站通过到控制器的 Ethernet 连接向存储系统发送命令。
  - 请使用受支持的浏览器进行设置。请参阅"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` 是其中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 Set Administrator Password 提示。

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*。

   Setup 向导在首次登录时启动。

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的数量。为数组分配一个名称。
   - 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 — 接受快速安装方法的建议池配置。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 Setup Wizard 的更多信息，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，将启动安装向导。安装向导将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（菜单：支持[升级中心]），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"。

如果取消向导，则无法手动重新启动它。打开 System Manager 或刷新浏览器时，向导会自动重新启动，并且满足以下_至少一个_条件：

- 未检测到池和卷组。
- 未检测到工作负载。
- 未配置通知。

Terminology

Setup 向导使用以下术语。

术语	说明
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	警报通知管理员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，并将自动派单发送给技术支持。
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	池是逻辑上分组的一组驱动器。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。）

术语	说明
卷	卷是应用程序、数据库和文件系统存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。 卷是根据池或卷组中的可用容量创建的。卷具有定义的容量。虽然卷可能由多个驱动器组成，但卷在主机上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。卷组具有定义的容量和 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	工作负载是支持应用程序的存储对象。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。这些卷特性是根据工作负载支持的应用程序类型进行优化的。例如，如果创建支持 Microsoft SQL Server 应用程序的工作负载，然后为该工作负载创建卷，则会优化基础卷特征以支持 Microsoft SQL Server。

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

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

如果我没有看到所有硬件组件，该怎么办？

如果在"验证硬件"对话框中未显示所有硬件组件，则可能表示驱动器盘架未正确连接，或者存储阵列中安装了不兼容的盘架。

验证所有驱动器盘架都已正确连接。如果您不确定哪些驱动器盘架是兼容的，请联系技术支持。

如果我没有看到所有主机，该怎么办？

如果未看到已连接的主机，则表示自动检测失败、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。您可以按以下步骤手动创建主机：

- 您可以通过转到菜单：Storage[Hosts] 来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 **Initial Setup** 向导中。
- 目标和主机必须配置为主机端口类型（例如，iSCSI 或 NVMe over RoCE），并且必须在自动检测工作之前建立到存储的会话。

识别应用程序如何帮助我管理存储阵列？

识别应用程序时，SANtricity System Manager 会自动推荐基于应用程序类型优化存储的卷配置。

按应用程序优化卷可以提高数据存储操作的效率。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。此外，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。

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），可以定义优化该应用程序存储的工作负载。

工作负载是支持应用程序的存储对象。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。这些卷特性是根据工作负载支持的应用程序类型进行优化的。例如，如果创建支持 Microsoft SQL Server 应用程序的工作负载，然后为该工作负载创建卷，则会优化基础卷特征以支持 Microsoft SQL Server。

在创建卷期间，系统会提示您回答有关工作负载使用的问题。例如，如果要为 Microsoft Exchange 创建卷，系统会询问您需要多少个邮箱、平均邮箱容量要求以及所需的数据库副本数。系统使用此信息为您创建最佳卷配置，可以根据需要对其进行编辑。

如何配置 **AutoSupport** 的传送方式?

要访问 AutoSupport 交付方式的配置任务，请转到菜单：支持[Support Center]，然后单击 **AutoSupport** 选项卡。

支持以下协议： HTTPS 和 SMTP 。

如何知道我是否应该接受建议的池配置?

是否接受推荐的池配置取决于几个因素。

通过回答以下问题，确定最适合您需求的存储类型：

- 您是否更喜欢多个容量较小的池，而不是尽可能大的池?
- 是否更喜欢 RAID 卷组而不是池?
- 您是否更喜欢手动设置驱动器，而不是建议您进行配置?

如果您对这些问题中的任何一个回答为"是"，请考虑拒绝推荐的池配置。

SANtricity System Manager 未检测到任何主机。我该怎么做?

如果未看到已连接的主机，则表示自动检测失败、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。您可以按以下步骤手动创建主机：

- 您可以通过转到菜单：Storage[Hosts] 来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 **Initial Setup** 向导中。
- 目标和主机必须配置为主机端口类型（例如，iSCSI 或 NVMe over RoCE），并且必须在自动检测工作之前建立到存储的会话。

SANtricity Unified Manager 设置

安装 SANtricity Unified Manager

SANtricity Unified Manager 包含在 Web Services Proxy 中，Web Services Proxy 是单独安装在主机系统上的 RESTful API 服务器，用于管理 NetApp E 系列存储系统。

要安装 Web Services Proxy 和 Unified Manager，请参见 E-Series 和 SANtricity 文档中心中的以下说明：

1. "审核安装和升级要求"
2. "下载并安装 Web Services Proxy 文件"

访问 **SANtricity Unified Manager**

安装 Web Services Proxy 后，您可以访问 SANtricity Unified Manager，在基于 Web 的界面中管理多个存储系统。

有关受支持的浏览器，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[s]://<server>:<port>/um`

   在此 URL 中， `<server>` 表示安装 Web Services Proxy 的服务器的 IP 地址或 FQDN， `<port>` 表示侦听端口号（HTTP 默认为 8080，HTTPS 默认为 8443）。

   此时将打开 Unified Manager 登录页面。

2. 首次登录时，请输入 `admin`用户名，然后为管理员用户设置并确认密码。

   密码最多可包含 30 个字符。

有关用户和密码的更多信息，请参见 "访问管理的工作原理"。

使用 SANtricity System Manager 11.9 进行单阵列管理

主界面

了解 SANtricity System Manager 界面

SANtricity System Manager 是一个基于 Web 的界面，允许您在单个视图中管理存储阵列。

主页

主页为您的存储阵列的日常管理提供了一个仪表板视图。当您登录到 System Manager 时，主页是显示的第一个屏幕。

仪表板视图包括四个摘要区域，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	说明
通知	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 portlet 还会显示自动警报，可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。
性能	性能区域允许您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/s) 和正在使用的处理容量 (CPU) 的性能指标。
容量	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由存储阵列管理的各种硬件组件和存储对象的组织视图。单击下拉箭头，对该硬件组件或存储对象执行特定操作。

接口设置

您可以从主界面更改显示首选项和其他设置。

设置	说明
显示首选项	从界面右上角的首选项下拉菜单中更改容量值和时间范围。
会话超时	配置超时，以便在指定时间后断开用户的非活动会话。
帮助	从界面右上角的下拉菜单中访问帮助文档和其他资源。

用户登录名和密码

当前登录系统的用户显示在界面右上角。

有关用户和密码的更多信息，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

Performance 页面为您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学到什么？

性能图表和表格以近乎实时的方式显示性能数据，可帮助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，并确定问题何时开始或导致问题的原因。

了解详情：

- "性能图表和指南"
- "性能术语"

如何查看性能数据？

可从主页和存储页面获得性能数据。

了解详情：

- "查看图形性能数据"
- "查看和保存表格性能数据"
- "解读性能数据"

了解 **SANtricity System Manager** 中的性能图表和准则

性能页面提供数据图形和表格，可用于评估存储阵列在几个关键领域的性能。

性能函数允许您完成以下任务：

- 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，并确定问题何时开始或导致问题的原因。
- 选择要查看的对象、性能指标和时间范围。
- 比较指标。

您可以以三种格式查看性能数据：

- 实时图形 — 近乎实时地在图形上绘制性能数据。
- 近实时表格 — 在表中近实时列出性能数据。
- 导出的 **CSV** 文件 — 允许您将表格性能数据保存在逗号分隔值的文件中，以便进一步查看和分析。

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	保存数据的能力
实时图形化，实时 实时图形、历史记录	10 秒（直播） 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
近实时表格（表格视图）	10 秒 - 1 小时	最新值	无限制	是
逗号分隔值 (CSV) 文件	取决于所选时间范围	取决于所选时间范围	无限制	是

查看性能数据的指南

- 性能数据收集始终处于开启状态。没有关闭的选项。
- 每次采样间隔过后，都会查询存储数组并更新数据。
- 对于图形数据，5 分钟时间范围支持 10 秒更新，平均时间为 5 分钟。所有其他时间范围每 5 分钟更新一次，在所选时间范围内平均。
- 图形视图中的性能数据会实时更新。表视图中的性能数据近乎实时更新。
- 如果被监控对象在收集数据期间发生变化，则该对象可能没有跨越所选时间范围的完整数据点集。例如，卷集可以在创建、删除、分配或取消分配卷时更改；或者可以添加、删除驱动器或驱动器发生故障。

了解 **SANtricity** 软件中的性能术语

了解性能条款如何适用于您的存储阵列。

术语	说明
应用程序	应用程序是一种软件程序，例如 SQL 或 Exchange。

术语	说明
CPU	CPU 是"中央处理器"的缩写。CPU 表示存储阵列正在使用的处理容量的百分比。
主机	主机是向存储阵列上的卷发送 I/O 的服务器。
IOPS	IOPS 代表每秒的输入/输出操作。
延迟	延迟是请求（例如读取或写入命令）与来自主机或存储阵列的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。此卷以 LUN 的形式作为容量呈现给主机。 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相同的 LUN 来访问不同的卷。
MiB	MiB 是 mebibyte（百万二进制字节）的缩写。1 MiB 为 2，或 1,048,576 字节。与 MB 进行比较，MB 表示基数为 10 的值。1 MB 等于 1,000,000 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	池是逻辑上分组的一组驱动器。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，在主机请求存储阵列中的数据时发生。
卷	卷是应用程序、数据库和文件系统存储数据的容器。它是为主机创建的逻辑组件，用于访问存储阵列上的存储。 卷是根据池或卷组中的可用容量创建的。卷具有定义的容量。虽然卷可能由多个驱动器组成，但卷在主机上显示为一个逻辑组件。
卷名称	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卷中存储的数据类型。
卷组	卷组是具有共享特征的卷的容器。卷组具有定义的容量和 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	工作负载是支持应用程序的存储对象。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。这些卷特性是根据工作负载支持的应用程序类型进行优化的。例如，如果创建支持 Microsoft SQL Server 应用程序的工作负载，然后为该工作负载创建卷，则会优化基础卷特征以支持 Microsoft SQL Server。

术语	说明
写入	写入是"写入操作"的缩写，即数据从主机发送到阵列进行存储时的操作。

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

性能图表显示历史数据以及当前正在捕获的实时数据。图表上标有 Live updating 的垂直线将历史数据与实时数据区分开来。

主页视图

主页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** 以选择所有可用的指标。

详细视图

详细性能视图中提供的图表排列在三个选项卡下：

- **Logical View** — 显示按卷组和池分组的逻辑对象的性能数据。逻辑对象包括卷组、池和卷。
- 物理视图 — 显示控制器、主机通道、驱动器通道和驱动器的性能数据。
- **Applications & Workloads View** — 显示按您定义的应用程序类型和工作负载分组的逻辑对象（卷）列表。

步骤

1. 选择 **Home**。
2. 要选择阵列级视图，请单击 IOPS、MiB/s 或 CPU 按钮。
3. 要查看更多详细信息，请单击 **View Performance Details**。
4. 选择 **Logical View** 选项卡、**Physical View** 选项卡或 **Applications & Workloads View** 选项卡。

   根据对象类型，每个选项卡中都会显示不同的图形。

查看选项卡	为每种对象类型显示的性能数据
逻辑视图	• 存储阵列：IOPS、MiB/s • 池：延迟、IOPS、MiB/s • 卷组：延迟、IOPS、MiB/s • 卷：延迟、IOPS、MiB/s
物理视图	• 控制器：IOPS、MiB/s、CPU、Headroom • 主机通道：延迟、IOPS、MiB/s、净空 • 驱动器通道：延迟、IOPS、MiB/s • 驱动器：延迟、IOPS、MiB/s

查看选项卡	为每种对象类型显示的性能数据
应用程序和工作负载视图	• 存储阵列：IOPS、MiB/s • **Applications**：延迟、IOPS、MiB/s • 工作负载：延迟、IOPS、MiB/s • 卷：延迟、IOPS、MiB/s

5. 使用选项可查看所需的对象和信息。

   选项

查看对象的选项	说明
展开抽屉可查看对象列表。	*Navigation drawers* 包含存储对象，例如池、卷组和驱动器。 单击抽屉可查看抽屉中的对象列表。
选择要查看的对象。	选中每个对象左侧的复选框，以选择要查看的性能数据。
使用 Filter 查找对象名称或部分名称。	在"筛选器"框中，输入对象的名称或部分名称，以仅列出抽屉中的对象。
选择对象后，单击 刷新图形。	从抽屉中选择对象后，选择 刷新图形 以查看选定项目的图形数据。
隐藏或显示图形	选择图形标题以隐藏或显示图形。

6. 根据需要，使用其他选项查看性能数据。

其他选项

选项	说明
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	将光标悬停在图形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可查看较早或较晚的时间跨度。
缩放栏	在图形下方，拖动缩放条手柄以缩小时间范围。缩放条越宽，图形细节的粒度越小。 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

您可以以表格格式查看和保存性能图表数据。这使您可以过滤要显示的数据。

步骤

1. 从任何性能数据图表中，单击 **Launch table view**。

   此时将显示一个表格，其中列出了选定对象的所有性能数据。

2. 根据需要使用对象选择下拉列表和过滤器。
3. 单击 **Show/Hide Columns** 按钮以选择要包含在表中的列。

   您可以单击每个复选框来选择或取消选择一个项目。

4. 选择屏幕底部的 **Export**，将表格视图保存为逗号分隔值 (CSV) 文件。

   此时将显示"导出表"对话框，指示要导出的行数和导出的文件格式（逗号分隔值或 CSV 格式）。

5. 单击 **Export** 以继续下载，或单击 **Cancel**。

   根据您的浏览器设置，系统会保存文件，或者提示您选择文件的名称和位置。

   默认文件名格式为 `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`，其中包括导出文件的日期和时间。

在 **SANtricity System Manager** 中解释性能数据

性能数据可以指导您调整存储阵列的性能。

在解读性能数据时，请记住，有几个因素会影响存储阵列的性能。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 ms）	监控特定对象的 I/O 活动。 识别可能存在瓶颈的对象： • 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，会引入更大的延迟，并且驱动器之间可能存在不均匀的工作负载，从而使延迟值变得不那么有意义，并且通常会更高。 • 驱动器类型和速度会影响延迟。使用随机 I/O，更快的旋转驱动器花费更少的时间在磁盘上的不同位置之间移动。 • 驱动器太少会导致更多的命令排队，并使驱动器处理命令的时间更长，从而增加了系统的一般延迟。 • 较大的 I/O 由于传输数据涉及额外时间而具有更大的延迟。 • 较高的延迟可能表明 I/O 模式本质上是随机的。具有随机 I/O 的驱动器将比具有顺序流的驱动器具有更大的延迟。 • 常见卷组的驱动器或卷之间的延迟差异可能表明驱动器速度较慢。
IOPS	影响每秒输入/输出操作（IOPS 或 IOs/sec）的因素包括以下内容： • 访问模式（随机或顺序） • I/O 大小 • RAID 级别 • 缓存块大小 • 是否启用读缓存 • 是否启用写缓存 • 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 缓存命中率越高，I/O 速率就越高。与禁用相比，启用写缓存会遇到更高的写入 I/O 速率。在决定是否为单个卷启用写缓存时，请查看当前 IOPS 和最大 IOPS。与随机 I/O 模式相比，顺序 I/O 模式的速率应该更高。无论您的 I/O 模式如何，都要启用写缓存，以最大限度地提高 I/O 速率并缩短应用程序响应时间。 您可以在卷的 IOPS 统计信息中查看更改段大小所带来的性能改进。尝试确定最佳段大小，或使用文件系统大小或数据库块大小。

性能数据	对性能调整的影响
MiB/秒	传输或吞吐率由应用程序 I/O 大小和 I/O 速率决定。通常，较小的应用程序 I/O 请求会导致较低的传输速率，但会提供更快的 I/O 速率和更短的响应时间。使用更大的应用程序 I/O 请求，可以实现更高的吞吐率。 了解典型的应用程序 I/O 模式可以帮助您确定特定存储阵列的最大 I/O 传输速率。
CPU	该值是正在使用的处理容量的百分比。 您可能会注意到相同类型对象的 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 使用率较轻或更稳定。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。 您可能需要监控整个存储阵列的 CPU。如果随着时间的推移 CPU 继续增加，而应用程序性能降低，则可能需要添加存储阵列。通过将存储阵列添加到企业，您可以继续以可接受的性能级别满足应用程序需求。
性能余量	净空是指控制器、控制器主机通道和控制器驱动器通道的剩余性能能力。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水平之间的差距。 • 对于控制器，余量是最大可能 IOPS 的百分比。 • 对于通道，净空是最大吞吐量的百分比，即 MiB/s。计算中包括读吞吐量、写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 Storage Hierarchy 提供了由存储阵列管理的各种硬件组件和存储对象的组织视图。

要查看存储层次结构，请转到主页，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

下表描述了存储阵列的物理组件。

组件	说明
控制器	控制器由主板、固件和软件组成。它控制驱动器并实现 System Manager 功能。
磁盘架	搁板是安装在机柜或机架上的外壳。它包含存储阵列的硬件组件。有两种类型的搁板：控制器搁板和驱动器搁板。控制器搁板包括控制器和驱动器。驱动器搁板包括输入/输出模块 (IOM) 和驱动器。 如果您的存储阵列包含不同的介质类型或不同的接口类型，则会显示每个驱动器类型的驱动器架。

组件	说明
驱动器	驱动器是提供数据物理存储介质的电磁机械设备或固态存储设备。
主机	主机是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) 是驻留在主机中的主板，包含一个或多个主机端口。
主机端口	主机端口是主机总线适配器 (HBA) 上的端口，它提供与控制器的物理连接，并用于 I/O 操作。
管理客户端	管理客户端是安装浏览器以访问 System Manager 的计算机。

逻辑组件

存储阵列中的驱动器提供数据的物理存储容量。使用 System Manager 将物理容量配置到逻辑组件中，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。下表描述了存储阵列的逻辑组件。

组件	说明
池	池是逻辑上分组的一组驱动器。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。卷组具有定义的容量和 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。）
卷	卷是应用程序、数据库和文件系统存储数据的容器。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。此卷以 LUN 的形式作为容量呈现给主机。 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相同的 LUN 来访问不同的卷。

管理界面设置

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

必须使用密码配置存储阵列，以保护其免受未经授权的访问。

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。任何拥有管理员密码的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，请参阅 "访问 System Manager"。

出于安全原因，在存储阵列进入"锁定"状态之前，只能尝试输入五次密码。在此状态下，存储阵列将拒绝后续密码尝试。您必须等待 10 分钟，以便存储阵列重置为"正常"状态，然后再次尝试输入密码。

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，其中映射了一个或多个角色。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"。

会话超时后重新输入密码

在单个管理会话期间，系统仅提示您输入一次密码。但是，会话在不活动 30 分钟后超时，此时必须再次输入密码。如果从另一个管理客户端管理同一存储阵列的另一个用户在您的会话正在进行时更改密码，则在下次尝试配置操作或视图操作时将提示您输入密码。

您可以调整会话超时，也可以完全禁用会话超时。请参阅"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，请注意以下几点：

- 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，其密码将不再有效。要纠正这种情况，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 — 如果不想再让命令受密码保护，请输入当前的管理员密码，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导致严重损坏，包括数据丢失。为此，应始终为存储阵列设置管理员密码。请使用至少包含 15 个字母数字字符的长管理员密码，以提高安全性。

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

SANtricity System Manager 可以以 gibibytes (GiB) 或 tebibytes (TiB) 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. 选择菜单：Preferences[Set preferences]。
2. 单击 **Gibibytes** 或 **Tebibytes** 的单选按钮，并确认要执行此操作。

   有关缩写和值，请参见下表。

缩写	值
GiB	$1,024^3$ 字节
TiB	$1,024^4$ 字节

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

您可以更改性能图表显示的默认时间范围。

关于此任务

主页和"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. 选择菜单：Preferences[Set preferences]。
2. 在下拉列表中，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

您可以创建登录横幅，该横幅在用户在 SANtricity System Manager 中建立会话之前向用户显示。横幅可以包括建议通知和同意消息。

关于此任务

创建横幅时，它会显示在对话框中的登录屏幕之前。

步骤

1. 选择菜单：Settings[System]。
2. 在常规部分下，选择 **Configure Login Banner** 。

   此时将打开 Configure Login Banner 对话框。

3. 输入要在登录横幅中显示的文本。

   不要使用 HTML 或其他标记标签进行格式化。

4. 单击 **Save**。

结果

下次用户登录到 System Manager 时，该文本将在对话框中打开。用户必须点击*确定*才能继续到登录屏幕。

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

您可以在 SANtricity System Manager 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。

如果使用嵌入在阵列中的安全断言标记语言 (SAML) 功能配置访问管理，则当用户的 SSO 会话达到最大限制时，可能会发生会话超时。这可能在 System Manager 会话超时之前发生。

步骤

1. 选择菜单：Settings[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. 使用微调器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 15 分钟。

   要禁用会话超时，请取消选中 **Set the length of time…** 复选框。

4. 单击 **Save**。

管理通知

了解 **SANtricity System Manager** 问题通知

SANtricity System Manager 使用图标和其他几种方法通知您存储阵列存在问题。

图标

System Manager 使用这些图标指示存储阵列及其组件的状态。

图标	说明
	最佳
	非最佳或失败
	需要注意或修复
	注意

System Manager 在不同位置显示这些图标。

- 主页上的通知区域显示失败图标和消息。
- 导航区域中的 Home 页面图标显示失败图标。
- 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 还会以其他方式通知您问题。

- System Manager 发送 SNMP 通知或电子邮件错误消息。
- 硬件上的"需要维修操作" LED 指示灯亮起。

当您收到问题通知时，请使用 Recovery Guru 来帮助您解决问题。如有必要，请将硬件文档与恢复步骤一起使用，以更换出现故障的组件。

在 **SANtricity System Manager** 中查看正在进行的操作并对其执行操作

要查看长期运行的操作并对其执行操作，请使用 Operations in Progress 页面。

关于此任务

对于"正在进行的操作"页面上列出的每个操作，都会显示完成百分比和完成操作的预计剩余时间。在某些情况下，您可以停止操作或将其置于更高或更低的优先级。您还可以从列表中清除已完成的 Volume Copy 操作。

步骤

1. 在主页上，选择 **Show operations in progress** 。

   此时将显示正在执行的操作页面。

2. 如果需要，请使用 Actions 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警告文本，特别是在停止操作时。

   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，主页顶端将显示一条信息性消息和黄色扳手图标。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。

在"正在进行的操作"页面上显示的操作包括以下内容：

操作	操作的可能状态	您可以执行的操作
卷副本	已完成	清除
卷副本	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 64TiB 的厚池卷）	进行中	*none*
卷删除（仅限大于 64TiB 的厚池卷）	进行中	*none*
异步镜像组初始同步	进行中	暂停

操作	操作的可能状态	您可以执行的操作
异步镜像组初始同步	已暂停	恢复
同步镜像	进行中	暂停
同步镜像	已暂停	恢复
Snapshot 图像回滚	进行中	取消
Snapshot 图像回滚	待定	取消
Snapshot 图像回滚	已暂停	• 取消 • 恢复
驱动器撤离	进行中	取消（取决于驱动器疏散类型）
向池或卷组添加容量	进行中	*none*
更改卷的 RAID 级别	进行中	*none*
减少池容量	进行中	*none*
精简卷回收	进行中	*none*
检查池卷的即时可用性格式 (IAF) 操作的剩余时间	进行中	*none*
检查卷组的数据冗余	进行中	*none*
对卷组进行碎片整理	进行中	*none*
初始化卷	进行中	*none*
增加卷的容量	进行中	*none*
更改卷的段大小	进行中	*none*
驱动器副本	进行中	*none*
数据重建	进行中	*none*
回拷	进行中	*none*

操作	操作的可能状态	您可以执行的操作
驱动器擦除	进行中	*none*
远程存储导入	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** 从问题中恢复

Recovery Guru 是 SANtricity System Manager 的一个组件，用于诊断存储阵列问题并建议恢复过程以解决问题。

步骤

1. 选择 **Home**。
2. 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，然后按照恢复过程中的说明更正问题。必要时，使用更换说明更换出现故障的部件。对列出的每个问题重复此步骤。

   存储阵列中的多个问题可能相关。在这种情况下，纠正问题的顺序可能会影响结果。按照摘要列表中列出的顺序选择并更正问题。

   电源罐的多个故障被分组，并在摘要列表中列为一个问题。风扇罐的多次故障也被列为一个问题。

4. 要确保恢复过程成功，请单击 **Recheck**。

   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 **Clear** 以从控制器中清除故障，然后单击 **Recheck** 以从 Recovery Guru 中删除事件。

   如果所有问题都已得到纠正，则存储阵列图标最终将从 Needs Attention 过渡到 Optimal。对于某些问题，正在执行操作（如重建）时会显示 Fixing 图标。

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

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`。

6. 要打印 Recovery Guru 信息，请单击 **Print** 图标。

SANtricity System Manager 管理界面常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

支持哪些浏览器?

SANtricity System Manager 支持这些浏览器版本。

浏览器	最低版本
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

键盘快捷键有哪些?

您可以单独使用键盘在 SANtricity System Manager 中导航。

整体导航

操作	键盘快捷方式
移至下一项。	选项卡
移至上一项。	Shift + Tab
选择一个项目。	Enter
下拉列表—移至下一项或上一项。	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
可展开文本—展开或收起项目。	Enter

表格导航

操作	键盘快捷方式
选择一行。	Tab 选择一行，然后按 Enter
向上或向下滚动。	向下箭头/向上箭头或 Page Down/Page Up
更改列的排序顺序。	按 Tab 选择一个列标题，然后按 Enter

日历导航

操作	键盘快捷方式
移至上月。	向上翻页
移至下个月。	向下翻页
移至上一年。	Ctrl + Page Up
移至下一年。	Ctrl + Page Down
打开日期选择器（如果已关闭）。	Ctrl + Home
移至当前月份。	Control / Command + Home
移至前一天。	Control / Command + 左
移至下一天。	Control / Command + 右
移至上周。	Control / Command + 上
移至下周。	Control / Command + 下
选择焦点日期。	Enter
关闭日期选择器并清除日期。	Control / Command + End
关闭日期选择器而不进行选择。	退出

单个卷的性能统计与总量有何关系？

通过聚合所有卷（包括保留容量卷）来计算池和卷组的统计信息。

保留容量由存储系统内部使用，以支持精简卷、快照和异步镜像，并且对 I/O 主机不可见。因此，池、控制器和存储阵列统计信息加起来可能不是可查看卷的总和。

但是，对于应用程序和工作负载统计信息，仅聚合可见卷。

为什么数据在图形和表格中显示为零？

当图形和表格中的数据点显示零时，表示该时间点的对象没有 I/O 活动。发生这种情况的原因可能是主机未启动对该对象的 I/O，也可能是该对象本身存在问题。

对象的历史数据仍可供查看。一旦对象的 I/O 活动开始发生，图形和表格将显示非零数据。

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。

数组级对象类型	原因数据显示为零
卷	• 卷无主机分配。
卷组	• 正在导入卷组。 • 卷组不包含分配给主机的卷，***and*** 卷组不包含任何保留容量。
驱动器	• 驱动器出现故障。 • 驱动器已被删除。 • 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。 • 控制器已被移除。 • 控制器处于未知状态。
存储阵列	• 存储阵列不包含卷。

延迟图表显示了什么？

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。

延迟是指在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，以毫秒 (ms) 为单位查看该时间点的以下值：

- 阅读时间。
- 写入时间。
- 平均 I/O 大小。

IOPS 图形显示了什么？

IOPS 图表显示每秒输入/输出操作的统计信息。在主页上，此图表显示存储阵列的统计信息。在性能图块的 Logical View、Physical View 和 Applications & Workloads View 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_每秒输入/输出 (I/O) 操作_的缩写。将光标悬停在图形上的某个点上，以查看该时间点的以下值：

- 读取操作数。
- 写入操作数。
- 读取和写入操作总数。

MiB/s 图表显示了什么？

MiB/s 图表以每秒 mebibyte 为单位显示传输速度统计信息。在主页上，此图表显示存储阵列的统计信息。在性能图块的 Logical View、Physical View 和 Applications & Workloads View 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/s 是 *mebibytes per second* 或 1,048,576 bytes per second 的缩写。将光标悬停在图形上的某个点上，以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。在主页上，此图表显示存储阵列的统计信息。在性能图块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 图形显示针对阵列上的操作使用的 CPU 处理容量的百分比。即使没有发生外部 I/O，CPU 利用率百分比也可以非零，因为存储操作系统可能正在执行后台操作和监视。将光标悬停在图形上的某个点上，以查看该时间点正在使用的处理功能的百分比。

净空图表显示了什么？

净空图与存储阵列控制器的剩余性能功能相关。此图形在主页和 Performance 磁贴的 Physical View 选项卡上可见。

净空图表显示存储系统中物理对象的剩余性能能力。将光标悬停在图形上的某个点上，以查看控制器 A 和控制器 B 的 IOPS 和 MiB/s 剩余能力的百分比。

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：

- 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"。
- 有关显示性能图的默认时间范围的详细信息，请参见 "为性能图表设置默认时间范围"。

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驱动器的子集创建逻辑存储容量。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要。

什么是池和卷组?

pool 是一组逻辑分组的驱动器。*volume group* 是具有共享特征的卷的容器。您可以使用池或卷组来创建主机可访问的卷。

了解详情：

- "池和卷组的工作原理"
- "容量术语"
- "决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，您可以从菜单手动创建池：Storage[Pools & Volume Groups]。

了解详情：

- "自动与手动池创建"
- "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 & Volume Groups] 创建卷组。

了解详情：

- "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：

- "预留容量的运作方式"
- "SSD 缓存的工作原理"

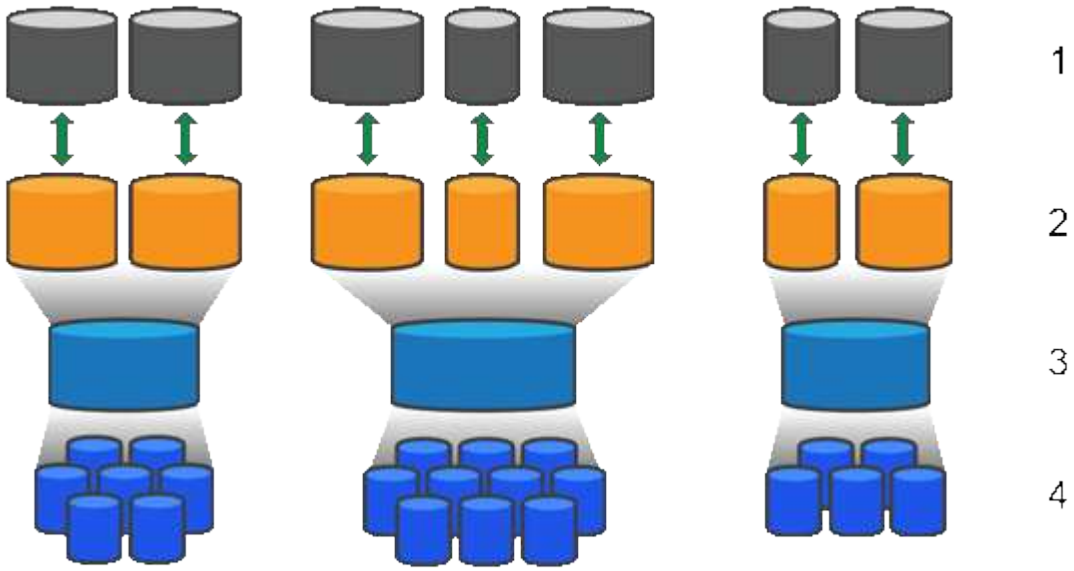
概念

要配置存储，请创建一个池或卷组，其中将包含要在存储阵列中使用的硬盘驱动器 (HDD) 或固态硬盘 (SSD) 驱动器。

物理硬件配置到逻辑组件中，以便可以组织并轻松检索数据。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部分。在这些逻辑分区内是存储数据的单个卷或 LUN。下图说明了这个概念。



[1] 主机 LUN；[2] 卷；[3] 卷组或池；[4] HDD 或 SSD 驱动器

部署存储系统时，第一步是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）以满足特定的业务要求

您可以在同一存储系统上拥有池或卷组，但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呈现给主机用于 I/O 的卷。

池

池旨在将物理硬盘驱动器聚合到大型存储空间中，并为其提供增强的 RAID 保护。池根据分配给池的驱动器总数创建多个虚拟 RAID 集，并在所有参与的驱动器之间均匀分布数据。如果驱动器丢失或添加，System Manager 会在所有活动驱动器上动态重新平衡数据。

池充当另一个 RAID 级别，虚拟化底层 RAID 架构，以在执行重建、驱动器扩展和处理驱动器丢失等任务时优化性能和灵活性。System Manager 在 8+2 配置（八个数据磁盘加两个奇偶校验磁盘）中自动将 RAID 级别设置为 6。

驱动器匹配

您可以从 HDD 或 SSD 中选择在池中使用；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，因此您必须确保您有足够数量的驱动器用于您选择的技术。

管理故障驱动器

池的最小容量为 11 个驱动器；但是，在发生驱动器故障时，会为备用容量保留一个驱动器的容量。这种备用容量称为"`preservation capacity`"。

创建池时，会保留一定的容量以备紧急使用。此容量以 System Manager 中的多个驱动器表示，但实际实施分布在整个驱动器池中。保留的默认容量量基于池中的驱动器数量。

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

卷组

卷组定义如何在存储系统中将容量分配给卷。磁盘驱动器被组织成 RAID 组，卷驻留在 RAID 组中的驱动器上。因此，卷组配置设置确定哪些驱动器属于该组以及使用什么 RAID 级别。

创建卷组时，控制器会自动选择要包含在该组中的驱动器。您必须手动选择该组的 RAID 级别。卷组的容量是您选择的驱动器总数乘以其容量。

驱动器匹配

您必须匹配卷组中驱动器的大小和性能。如果卷组中有较小和较大的驱动器，则所有驱动器都将被识别为最小容量大小。如果卷组中有较慢和较快的驱动器，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）。RAID 3、5 和 6 限制为最多 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

卷组使用热备盘驱动器作为备用，以防卷组中包含的 RAID 1/10、RAID 3、RAID 5 或 RAID 6 卷中的驱动器出现故障。热备盘驱动器不包含任何数据，并为存储阵列添加另一个级别的冗余。

如果存储阵列中的驱动器出现故障，热备盘驱动器将自动替换出现故障的驱动器，而无需进行物理交换。如果热备盘驱动器在驱动器发生故障时可用，则控制器使用冗余数据将数据从发生故障的驱动器重建到热备盘驱动器。

了解 **SANtricity** 软件中的容量术语

了解容量术语如何适用于您的存储阵列。

存储对象

以下术语描述了可以与存储阵列交互的不同类型的存储对象。

存储对象	说明
主机	主机是向存储阵列上的卷发送 I/O 的服务器。

存储对象	说明
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。此卷以 LUN 的形式作为容量呈现给主机。 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相同的 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，一个主卷和一个辅助卷。
池	池是逻辑上分组的一组驱动器。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。）
快照一致性组	快照一致性组是创建快照映像时被视为单个实体的卷集合。每个卷都有自己的快照映像，但所有映像都是在相同的时间点创建的。
Snapshot 组	快照组是来自单个基本卷的快照图像的集合。
Snapshot 卷	快照卷允许主机访问快照映像中的数据。快照卷包含其自己的保留容量，该容量可保存对基本卷的任何修改，而不会影响原始快照映像。
卷	卷是应用程序、数据库和文件系统存储数据的容器。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。卷组具有定义的容量和 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

以下术语描述了您的存储阵列上使用的不同类型的容量。

容量类型	说明
已分配容量	分配的容量是从池或卷组中的驱动器分配的物理容量。 您可以使用分配的容量来创建卷和进行复制服务操作。
可用容量	可用容量是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、卷或卷组容量是指已分配给池或卷组的存储阵列中的容量。此容量用于创建卷并为复制服务操作和存储对象的各种容量需求提供服务。
池不可用容量	池不可用容量是指由于驱动器大小不匹配而无法使用的池中空间。

容量类型	说明
保存容量	保留容量是在池中保留的容量（驱动器数量），用于支持潜在的驱动器故障。
已报告容量	报告容量是报告给主机并可由主机访问的容量。
预留容量	保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。
SSD 缓存	SSD Cache 是一组固态硬盘 (SSD) 驱动器，您可以在存储阵列中将它们逻辑地组合在一起。SSD Cache 功能将最常访问的数据（"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。
未分配容量	未分配容量是存储阵列中 未 分配给池或卷组的空间。
写入容量	写入容量是从为精简卷分配的预留容量中已写入的容量大小。

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，例如预期的 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到组成池的一组驱动器上。

  您无法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。可以在创建卷组时指定 RAID 级别。
- 如果要跨构成卷组的驱动器集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。

用途	池	卷组
工作负载随机	更好	较好

用途	池	卷组
工作负载顺序	较好	更好
驱动器重建时间	更快	较慢
性能（最佳模式）	良好：最适合小块、随机工作负载。	良好：最适合大块、顺序工作负载
性能（驱动器重建模式）	更好：通常比 RAID 6 更好	降级：性能下降高达 40%
多个驱动器故障	更好的数据保护：更快、优先的重建	数据保护较少：重建速度缓慢，数据丢失风险更大
添加驱动器	更快：即时添加到池中	较慢：需要 Dynamic Capacity Expansion 操作
精简卷支持	是	否
固态硬盘 (SSD) 支持	是	是
简化管理	是：没有要配置的热备盘或 RAID 设置	否：必须分配热备用，配置 RAID
可调性能	否	是

池和卷组的功能比较

池和卷组的功能和目的是相同的。这两个对象都是在存储阵列中逻辑分组在一起的一组驱动器，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。	可以。提供 RAID 0、1、10、5 和 6。
支持精简卷	是	否
支持全磁盘加密 (FDE)	是	是
支持数据保障 (DA)	是	是
支持磁盘架丢失保护	是	是

功能	池	卷组
支持抽屉丢失保护	是	是
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。最小驱动器决定所有驱动器的容量。
最小驱动器数量	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 的最小值为 3。RAID 6 的最小值为 5。
最大驱动器数量	不超过存储阵列的最大限制	RAID 1 和 10——最多达到存储阵列的最大限制 RAID 5、6——30 个驱动器
在创建卷时可以选择单个驱动器	否	是
可以在创建卷时指定段大小	是的。支持 128K。	是
可以在创建卷时指定 I/O 特性	否	是。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，使重建更快。	使用热备盘驱动器。重建受到驱动器 IOPS 的限制。
达到容量限制时的警告	是的。当使用的容量达到最大容量的百分比时，可以设置警报。	否
支持迁移到其他存储阵列	否。要求您首先迁移到卷组。	是
动态区块大小 (DSS)	否	是
可以更改 RAID 级别	否	是
卷扩展（增加容量）	是	是
容量扩展（增加容量）	是	是
容量减少	是	否

池或卷组均不支持混合驱动器类型（HDD、SSD）。

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

您可以自动或手动创建池以允许对物理存储进行分组，然后根据需要进行动态分配。创建池后，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。检测到未分配容量时，System Manager 会自动提示您创建一个或多个池，或将未分配容量添加到现有池，或两者兼而有之。

当以下条件之一为真时，将自动创建池：

- 池不存在于存储阵列中，并且有足够的类似驱动器来创建新池。
- 新驱动器被添加到至少有一个池的存储阵列。

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。System Manager 将提示您完成以下任务：

- 如果这些类型的驱动器数量足够，则创建单个池。
- 如果未分配的容量由不同的驱动器类型组成，则创建多个池。
- 如果已在存储阵列中定义了池，则将驱动器添加到现有池中，并将相同驱动器类型的新驱动器添加到池中。
- 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。

手动创建

当自动创建无法确定最佳配置时，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。
- 一个或多个新的候选池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者无法保持其货架丢失保护或抽屉丢失保护状态。

如果您的存储阵列上有多个应用程序，并且不希望它们竞争相同的驱动器资源，则可能还需要手动创建池。在这种情况下，您可以考虑手动为一个或多个应用程序创建一个较小的池。您可以只分配一个或两个卷，而不是将工作负载分配给具有多个卷的大型池来分配数据。手动创建一个专用于特定应用程序工作负载的单独池，可以使存储阵列操作更快地执行，争用更少。

配置存储

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

当 SANtricity System Manager 检测到存储阵列中未分配的驱动器时，系统会自动启动池创建。您可以使用自动池创建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

当以下条件之一成立时，可以启动 Pool Auto-Configuration 对话框：

- 至少检测到一个未分配的驱动器，该驱动器可以添加到具有相似驱动器类型的现有池中。
- 检测到十一（11）个或更多未分配的驱动器，可用于创建新池（如果由于驱动器类型不同而无法将其添加到现有池）。

关于此任务

请注意以下几点：

- 将驱动器添加到存储阵列时，System Manager 会自动检测驱动器，并提示您根据驱动器类型和当前配置创建单个池或多个池。
- 如果之前定义了池，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时，System Manager 会自动将数据重新分配到新容量中，该容量现在包括您添加的新驱动器。
- 配置 EF600 或 EF300 存储阵列时，确保每个控制器可以访问前 12 个插槽中的数量相等的驱动器，以及最后 12 个插槽中的数量相等的驱动器。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 Pool Auto-Configuration 对话框：

- 检测到未分配的容量时，池自动配置建议将显示在通知区域的主页上。单击 **View Pool Auto-Configuration** 以启动此对话框。
- 您还可以从 Pools and Volume Groups 页面启动 Pool Auto-Configuration 对话框，如以下任务中所述。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择菜单：更多 [Launch pool auto-configuration]。

   结果表列出了新的池、添加了驱动器的现有池，或两者兼而有之。默认情况下，新池使用序列号命名。

   System Manager 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）并具有相似的容量，则创建单个池。
   - 如果未分配的容量由不同的驱动器类型组成，则创建多个池。
   - 如果已在存储阵列中定义了池，则将驱动器添加到现有池中，并将相同驱动器类型的新驱动器添加到池中。
   - 将相同驱动器类型的驱动器添加到现有池中，如果新驱动器具有不同的驱动器类型，则使用其他驱动器类型创建不同的池。
3. 要更改新池的名称，请单击 **Edit** 图标（铅笔）。
4. 要查看池的其他特征，请将光标悬停或触摸 **Details** 图标（页面）。

   此时将显示有关驱动器类型、安全功能、Data Assurance (DA) 功能、货架丢失保护和抽屉丢失保护的信息。

   对于 EF600 和 EF300 存储阵列，还会显示资源调配和卷块大小的设置。

5. 单击 **Accept**。

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

如果池自动配置功能未提供满足您需求的池，您可以手动（从一组候选项中）创建池。

池提供必要的逻辑存储容量，您可以从中创建单个卷，然后可用于托管应用程序。

开始之前

- 必须至少有 11 个驱动器具有相同的驱动器类型（HDD 或 SSD）。
- 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盘架中，并且一个驱动器盘架中不超过两个驱动器。
- 抽屉丢失保护要求构成存储池的驱动器位于至少五个不同的抽屉中，并且存储池包括来自每个抽屉的同等数量的驱动器架。
- 配置 EF600 或 EF300 存储阵列时，确保每个控制器可以访问前 12 个插槽中的数量相等的驱动器，以及最后 12 个插槽中的数量相等的驱动器。此配置有助于控制器更有效地使用驱动器端 PCIe 总线。当前 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. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击菜单：创建 [Pool]。

   此时将显示"创建池"对话框。

3. 输入池的名称。
4. *可选：*如果您的存储阵列中有多个类型的驱动器，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的池。

5. 根据以下特征选择要使用的池候选，然后单击 创建。

特征	用途
空闲容量	显示池候选的空闲容量（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候选池。 保护（备用）容量也分布在整个池中，不属于可用容量。
驱动器总数	显示池候选项中可用的驱动器数量。 System Manager 会自动为保留容量保留尽可能多的驱动器（对于池中的每六个驱动器，System Manager 会为保留容量保留一个驱动器）。 当发生驱动器故障时，保留容量用于保存重建的数据。
驱动器块尺寸（仅限 EF300 和 EF600）	显示池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。

特征	用途
支持安全功能	指示此候选池是否完全由支持安全的驱动器组成，这些驱动器可以是 Full Disk Encryption (FDE) 驱动器或 Federal Information Processing Standard (FIPS) 驱动器。 • 您可以使用 Drive Security 保护池，但所有驱动器必须具有安全功能才能使用此功能。 • 如果要创建仅限 FDE 的池，请在"支持安全"列中查找 **Yes - FDE**。如果要创建仅限 FIPS 的池，请查找 **Yes - FIPS** 或 **Yes - FIPS (Mixed)**。"Mixed" 表示 140-2 和 140-3 级别驱动器的混合。如果您使用这些级别的混合，请注意，池将在较低的安全级别 (140-2) 运行。 • 您可以创建一个由驱动器组成的池，这些驱动器可能具有安全功能，也可能不具有安全功能，或者是安全级别的混合。如果池中的驱动器包括不具备安全功能的驱动器，则无法确保池安全。
启用安全？	提供使用具有安全功能的驱动器启用 Drive Security 功能的选项。如果池具有安全功能，并且您已创建安全密钥，则可以通过选中复选框来启用安全性。 启用 Drive Security 后删除它的唯一方法是删除池并擦除驱动器。
支持 DA	指示此池候选项是否可用 Data Assurance (DA)。DA 检查并更正数据通过控制器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：存储[卷 > 查看/编辑设置 > 高级 > 永久禁用 Data Assurance] 来禁用 DA。如果在卷上禁用 DA，则无法重新启用它。
支持资源调配（仅限 EF300 和 EF600）	显示资源调配是否可用于此池候选。资源调配是 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。 如果使用单个驱动器盘架完全失去通信，盘架丢失保护可保证对池中卷上的数据的可访问性。
抽屉丢失保护	显示抽屉丢失保护是否可用，仅当您使用包含抽屉的驱动器架时才提供。 如果与驱动器架中的单个抽屉发生完全通信中断，抽屉丢失保护可保证对池中卷上的数据的可访问性。
支持的卷块大小（仅限 EF300 和 EF600）	显示可以为池中的卷创建的块大小： • 512n — 原生 512 字节。 • 512e — 模拟 512 字节。 • 4K — 4,096 字节。

在 **SANtricity System Manager** 中创建卷组

使用卷组创建一个或多个可供主机访问的卷。卷组是具有 RAID 级别和容量等共享特性的卷的容器。

凭借更大容量的驱动器和跨控制器分配卷的能力，为每个卷组创建多个卷是利用存储容量和保护数据的好方法。

开始之前

在创建卷组之前，请查看以下指导原则：

- 您至少需要一个未分配的驱动器。
- 单个卷组中可以拥有的驱动器数量存在限制。这些限制会根据 RAID 级别而有所不同。
- 要启用货架/抽屉丢失保护，您必须创建一个使用至少位于三个货架或抽屉中的驱动器的卷组，除非您使用 RAID 1，其中两个货架/抽屉是最低要求。
- 如果您有 EF600 或 EF300 存储阵列，并且您计划手动创建卷组，请确保每个控制器可以访问前 12 个插槽中的相同数量的驱动器以及最后 12 个插槽中的相同数量的驱动器。此配置可帮助控制器更有效地使用驱动器端 PCIe 总线。当前 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生成容量：
  - 如果选择 RAID 1，则必须一次添加两个驱动器，以确保选择了镜像对。镜像和条带化（称为 RAID 10 或 RAID 1+0）是在选择四个或更多驱动器时实现的。
  - 如果选择 RAID 5，则必须添加至少三个驱动器才能创建卷组。
  - 如果选择 RAID 6，则必须添加至少五个驱动器才能创建卷组。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击菜单：Create[Volume group]。

   此时将显示创建卷组对话框。

3. 键入此卷组的名称。
4. 选择最能满足数据存储和保护要求的 RAID 级别。

   此时将显示卷组候选项表，并仅显示支持选定 RAID 级别的候选项。

5. *可选：*如果您的存储阵列中有多个类型的驱动器，请选择要使用的驱动器类型。

   此时将显示卷组候选项表，并仅显示支持选定驱动器类型和 RAID 级别的候选项。

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。自动方法是默认选择。

   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，它会变为*自动选择驱动器（高级）。

   Manual 方法允许您选择哪些特定驱动器构成卷组。您可以选择特定的未分配驱动器来获得所需的容量。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能使用 Manual 方法。

7. 根据显示的驱动器特性，选择要在卷组中使用的驱动器，然后单击 创建。

   显示的驱动器特性取决于您选择的是自动方法还是手动方法。

自动方法驱动特性

特征	用途
空闲容量	以 GiB 为单位显示可用容量。选择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	显示此卷组可用的驱动器数量。请选择具有所需驱动器数量的卷组候选项。
驱动器块尺寸（仅限 EF300 和 EF600）	显示组中的驱动器可写入的块大小（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。
支持安全功能	指示此卷组候选项是否完全由支持安全的驱动器组成，这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。 • 您可以使用 Drive Security 保护卷组，但所有驱动器必须具有安全功能才能使用此功能。 • 如果要创建仅限 FDE 的卷组，请在"支持安全"列中查找 **Yes - FDE**。如果要创建仅限 FIPS 的卷组，请查找 **Yes - FIPS** 或 **Yes - FIPS (Mixed)**。"Mixed" 表示 140-2 和 140-3 级别驱动器的混合。如果使用这些级别的混合，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，这些驱动器可能具有安全功能，也可能不具有安全功能，或者是安全级别的混合。如果卷组中的驱动器包括不支持安全功能的驱动器，则无法使卷组安全。
启用安全？	提供使用具有安全功能的驱动器启用 Drive Security 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，则可以通过选中复选框来启用 Drive Security。 启用 Drive Security 后，将其删除的唯一方法是删除卷组并擦除驱动器。
支持 DA	指示此组是否可用 Data Assurance (DA)。Data Assurance (DA) 检查并更正数据通过控制器传输到驱动器时可能发生的错误。 如果要使用 DA，请选择支持 DA 的卷组。（对于支持 DA 的驱动器，会在池中创建的卷上自动启用 DA。） 卷组可以包含支持 DA 或不支持 DA 的驱动器，但所有驱动器都必须支持 DA 才能使用此功能。
支持资源调配（仅限 EF300 和 EF600）	显示资源调配是否可用于此组。资源调配是 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。

特征	用途
磁盘架丢失保护	显示盘架丢失保护是否可用。盘架丢失保护可保证在发生与盘架的完全通信丢失时可访问卷组中的卷上的数据。
抽屉丢失保护	显示抽屉丢失保护是否可用，仅当您使用包含抽屉的驱动器架时提供。抽屉丢失保护可保证在与驱动器架中的单个抽屉完全失去通信时对卷组中卷上的数据的可访问性。
支持的卷块大小（仅限 EF300 和 EF600）	显示可以为组中的卷创建的块大小： • 512n — 原生 512 字节。 • 512e — 模拟 512 字节。 • 4K — 4,096 字节。

手动方法驱动器特性

特征	用途
介质类型	指示媒体类型。支持以下媒体类型： • 硬盘驱动器 • 固态硬盘 (SSD) 卷组中的所有驱动器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。
驱动器块尺寸（仅限 EF300 和 EF600）	显示组中的驱动器可写入的块大小（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	表示驱动器容量。 • 尽可能选择容量等于卷组中当前驱动器容量的驱动器。 • 如果必须添加容量较小的未分配驱动器，请注意当前卷组中每个驱动器的可用容量会降低。因此，整个卷组中的驱动器容量是相同的。 • 如果您必须添加容量较大的未分配驱动器，请注意，您添加的未分配驱动器的可用容量会减少，以便它们与卷组中驱动器的当前容量相匹配。
托盘	指示驱动器的托盘位置。
插槽	指示驱动器的插槽位置。
速度 (rpm)	指示驱动器的速度。
逻辑扇区大小	指示扇区大小和格式。
支持安全功能	指示此卷组候选项是否完全由支持安全的驱动器组成，这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。 • 您可以使用 Drive Security 保护卷组，但所有驱动器必须具有安全功能才能使用此功能。 • 如果要创建仅限 FDE 的卷组，请在"支持安全"列中查找 **Yes - FDE**。如果要创建仅限 FIPS 的卷组，请查找 **Yes - FIPS** 或 **Yes - FIPS (Mixed)**。"Mixed" 表示 140-2 和 140-3 级别驱动器的混合。如果使用这些级别的混合，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，这些驱动器可能具有安全功能，也可能不具有安全功能，或者是安全级别的混合。如果卷组中的驱动器包括不支持安全功能的驱动器，则无法使卷组安全。

特征	用途
支持 DA	指示此组是否可用 Data Assurance (DA)。Data Assurance (DA) 检查并更正数据通过控制器传输到驱动器时可能发生的错误。 如果要使用 DA，请选择支持 DA 的卷组。（对于支持 DA 的驱动器，会在池中创建的卷上自动启用 DA。） 卷组可以包含支持 DA 或不支持 DA 的驱动器，但所有驱动器都必须支持 DA 才能使用此功能。
支持的卷块大小（仅限 EF300 和 EF600）	显示可以为组中的卷创建的块大小： • 512n — 原生 512 字节。 • 512e — 模拟 512 字节。 • 4K — 4,096 字节。
支持资源调配（仅限 EF300 和 EF600）	显示资源调配是否可用于此组。资源调配是 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。

此扩展将导致池或卷组中包括额外的可用容量。您可以使用此可用容量创建额外的卷。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）。
- 池或卷组必须处于 Optimal 状态。
- 卷组中允许的最大卷数为 256 个。
- 池中允许的最大卷数取决于存储系统型号：
  - 2,048 卷（EF600 和 E5700 系列）
  - 1,024 卷 (EF300)
  - 512 卷（E4000 和 E2800 系列）
- 如果池或卷组包含所有支持安全的驱动器，则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 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。

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。如果需要添加超过最大数

量的驱动器，请重复此过程。（池包含的驱动器数不能超过存储系统的最大限制。）

添加驱动器后，可能需要增加您的保存容量。您应该考虑在扩展操作后增加您的预留容量。

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

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要将驱动器添加到的池或卷组，然后单击 **Add Capacity**。

   此时将显示"添加容量"对话框。仅显示与池或卷组兼容的未分配驱动器。

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*的列表下方。

字段详细信息

字段	说明
磁盘架	指示驱动器的盘架位置。
托架	指示驱动器的托架位置。
容量 (GiB)	表示驱动器容量。 • 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都会降低。因此，整个池或卷组的驱动器容量相同。 • 如果您必须添加容量较大的未分配驱动器，请注意，您添加的未分配驱动器的可用容量会减少，以便它们与池或卷组中驱动器的当前容量相匹配。
支持安全功能	指示驱动器是否具有安全功能。 • 要使用 Drive Security 功能保护您的池或卷组，所有驱动器必须具有安全功能。 • 可以使用支持安全的驱动器和不支持安全的驱动器混合创建池或卷组，但无法启用 Drive Security 功能。 • 即使未使用加密功能，具有所有支持安全的驱动器的池或卷组也不能接受不支持安全的驱动器进行备用或扩展。 • 报告为具有安全功能的驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。 • FIPS 驱动器可以是 140-2 级或 140-3 级，140-3 级为更高级别的安全级别。如果选择 140-2 和 140-3 级别驱动器的混合，则池或卷组将在较低的安全级别（140-2）运行。
支持 DA	指示驱动器是否支持 Data Assurance (DA)。 • 不建议使用不支持数据保障 (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。 • 不建议使用支持数据保障 (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。
DULBE 功能	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 EF300 或 EF600 存储阵列支持资源调配的卷。

4. 单击 **Add**。

   如果要将驱动器添加到池或卷组，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，则会显示确认对话框：

   - 货架损失保护 *
   - 抽屉丢失保护 *
   - 全磁盘加密功能
   - 数据保证能力
   - DULBE 功能

   * 目前，将驱动器添加到具有货架丢失保护或抽屉丢失保护的池时，不会显示确认对话框。

1. 要继续，请单击 **Yes**；否则，请单击 **Cancel**。

结果

将未分配的驱动器添加到池或卷组后，将重新分配池或卷组中每个卷中的数据，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根据 Recovery Guru 的指示，您可以检查池或卷组中卷上的冗余，以确定该卷上的数据是否一致。

冗余数据用于在池或卷组中的一个驱动器发生故障时快速重建替换驱动器上的信息。

开始之前

- 此池或卷组的状态必须为 Optimal。
- 池或卷组必须没有正在进行的卷修改操作。
- 您可以在除 RAID 0 以外的任何 RAID 级别上检查冗余，因为 RAID 0 没有数据冗余。

仅在 Recovery Guru 指示并在技术支持指导下检查卷冗余。

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导致错误。要避免此问题，请等待一到两分钟，然后再对同一个池或卷组运行另一个冗余检查。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择菜单：Uncommon Tasks[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` 以确认要执行此操作。
4. 单击 **Check**。

   检查卷冗余操作开始。从对话框中的表顶端开始，按顺序扫描池或卷组中的卷。在扫描每个卷时，将执行以下操作：

   - 卷在卷表中被选中。
   - 冗余检查的状态显示在 **Status** 列中。
   - 检查在遇到任何介质或奇偶校验错误时停止，然后报告该错误。

     有关冗余检查状态的更多信息

状态	说明
待定	这是第一个要扫描的卷，您尚未单击 Start 开始冗余检查。 或 正在池或卷组中的其他卷上执行冗余检查操作。
正在检查	卷正在进行冗余检查。
已通过	此卷通过了冗余检查。在冗余信息中未检测到不一致。
失败	此卷未通过冗余检查。在冗余信息中检测到不一致。
媒体错误	驱动器介质有缺陷且不可读。按照 Recovery Guru 中显示的说明进行操作。
奇偶校验错误	奇偶校验不是数据给定部分的应有结果。奇偶校验错误可能很严重，并可能导致数据永久丢失。

5. 检查池或卷组中的最后一个卷后，单击 **Done**。

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的容量，您可以重新配置以满足您的应用程序存储需求。

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)。
- 必须卸载卷上的任何文件系统。
- 您必须已删除池或卷组中的任何镜像关系。
- 您必须已停止池或卷组正在进行的任何卷复制操作。
- 池或卷组不得参与异步镜像操作。
- 卷组中的驱动器不得具有永久保留。

步骤

1. 选择菜单：Storage[Pools & 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：Uncommon Tasks[Delete] 并确认。

结果

System Manager 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，允许您在新的或现有的池或卷组中重复使用它们。

在 **SANtricity System Manager** 中整合卷组的可用容量

使用 Consolidate Free Capacity 选项可合并选定卷组上的现有可用盘区。通过执行此操作，您可以从卷组中的最大可用容量创建其他卷。

开始之前

- 卷组必须至少包含一个可用容量区域。
- 卷组中的所有卷必须联机且处于"最佳"状态。
- 卷修改操作不得正在进行中，例如更改卷的段大小。

关于此任务

操作开始后无法取消。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 Consolidate Free Capacity 对话框：

- 当至少检测到一个卷组的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的主页上。单击 合并可用容量 链接以启动对话框。
- 您还可以从 Pools & Volume Groups 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

可用容量区域是删除卷或在卷创建过程中未使用所有可用容量而产生的可用容量。在具有一个或多个可用容量区域的卷组中创建卷时，卷的容量仅限于该卷组中最大的可用容量区域。例如，如果一个卷组总共有 15 GiB 的可用容量，并且最大的可用容量区域为 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。随着时间的推移，随着主机写入、修改和删除文件，卷组的可用容量将变得碎片化。最终，可用容量将不会位于单个连续块中，而是分散在整个卷组中的小碎片中。这会导致进一步的文件碎片化，因为主机必须将新文件作为碎片写入，以适应可用簇的可用范围。

通过整合所选卷组的可用容量，每当主机写入新文件时，您都会注意到文件系统性能的提高。合并过程还有助于防止将来新文件碎片化。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要合并的具有可用容量的卷组，然后选择菜单：Uncommon Tasks[Consolidate volume group free capacity]。

   此时将显示合并可用容量对话框。
3. 输入 `consolidate` 以确认要执行此操作。
4. 单击 **Consolidate**。

   System Manager 开始将卷组的可用容量区域整合（碎片整理）为一个连续量，用于后续存储配置任务。

完成后

选择菜单：Home[View Operations in Progress] 以查看 Consolidate Free Capacity 操作的进度。此操作可能很长，并可能影响系统性能。

在 **SANtricity CLI** 中导出/导入卷组

卷组迁移允许您导出卷组，以便将该卷组导入其他存储阵列。

SANtricity System Manager 用户界面不支持导出/导入功能。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 Cache** 中的定位器指示灯

您可以定位驱动器以物理标识包含选定池、卷组或 SSD Cache 的所有驱动器。所选池、卷组或 SSD Cache 中的每个驱动器上的 LED 指示灯都会亮起。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要查找的池、卷组或 SSD Cache，然后单击菜单：更多[打开定位器指示灯]。

   此时将显示一个对话框，指示包含所选池、卷组或 SSD Cache 的驱动器上的指示灯已打开。
3. 成功定位驱动器后，单击 关闭。

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

您可以删除驱动器以减少现有池或 SSD Cache 的容量。

删除驱动器后，池或 SSD Cache 的每个卷中的数据将重新分配给剩余的驱动器。拆除的驱动器将被取消分配，其容量将成为存储阵列总可用容量的一部分。

关于此任务

移除容量时，请遵循以下准则：

- 如果不先删除 SSD Cache，则无法删除 SSD Cache 中的最后一个驱动器。
- 您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。如果需要拆除超过 12 个驱动器，请重复此过程。
- 如果池或 SSD Cache 中没有足够的可用容量来包含数据，则无法删除驱动器，当该数据被重新分配到池或 SSD Cache 中的剩余驱动器时。

了解潜在的性能影响

- 从池或 SSD 缓存中删除驱动器可能会导致卷性能降低。
- 从池或 SSD Cache 中删除容量时，不会消耗保留容量。但是，根据池或 SSD Cache 中剩余的驱动器数量，保留容量可能会减少。

了解对具有安全功能的驱动器的影响

- 如果删除最后一个不支持安全功能的驱动器，则池中将保留所有支持安全功能的驱动器。在这种情况下，您可以选择启用池的安全性。
- 如果删除最后一个不支持 Data Assurance (DA) 的驱动器，则池中将保留所有支持 DA 的驱动器。

在池中创建的任何新卷都将支持 DA。如果希望现有卷具有 DA 功能，则需要删除该卷，然后重新创建该卷。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择池或 SSD Cache，然后单击菜单：更多[删除容量]。

   此时将显示"删除容量"对话框。

3. 在列表中选择一个或多个驱动器。

   当您在列表中选择或取消选择驱动器时，选定的总容量 字段会更新。此字段显示删除选定驱动器后产生的池或 SSD Cache 的总容量。

4. 单击 **Remove**，然后确认要删除驱动器。

   池或 SSD Cache 的新减少容量反映在池和卷组视图中。

修改池和组设置

更改 **SANtricity System Manager** 中池的配置设置

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

此任务描述如何更改池的配置设置。

> 无法使用 System Manager 界面更改池的 RAID 级别。System Manager 自动将池配置为 RAID 6。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要编辑的池，然后单击 **View/Edit Settings**。

   此时将显示池设置对话框。

3. 选择 **Settings** 选项卡，然后根据需要编辑池设置。

字段详细信息

设置	说明
名称	您可以更改用户提供的池名称。需要指定池的名称。
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 将发送一条消息，允许您有时间添加更多存储空间或删除不必要的对象。 警报显示在仪表板的通知区域，可以通过电子邮件和 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，此严重警报会通知您。使用微调器控件调整阈值百分比。选中复选框以禁用此通知。 • 早期警报 — 当池中的可用容量达到指定阈值时，此早期警报会通知您。使用微调器控件调整阈值百分比。选中复选框以禁用此通知。
修改优先级	您可以相对于系统性能指定池中修改操作的优先级。池中修改操作的优先级越高，操作完成速度越快，但会降低主机 I/O 性能。优先级较低会导致操作耗时较长，但主机 I/O 性能影响较小。 您可以选择五个优先级：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 — 当多个驱动器故障导致某些数据没有冗余且额外的驱动器故障可能导致数据丢失时，此滑块确定数据重建操作的优先级。 • 降级的重建优先级 — 此滑动条确定驱动器发生故障时数据重建操作的优先级，但数据仍具有冗余，并且额外的驱动器故障不会导致数据丢失。 • 后台操作优先级 — 此滑动条确定池处于最佳状态时发生的池后台操作的优先级。这些操作包括 Dynamic Volume Expansion (DVE)、Instant Availability Format (IAF) 以及将数据迁移到更换或添加的驱动器。

设置	说明
保存容量（EF600 或 EF300 的"优化容量"）	保留容量 — 您可以定义驱动器数量，以确定池上保留的容量，以支持潜在的驱动器故障。当发生驱动器故障时，保留容量用于保存重建的数据。池在数据重建过程中使用保留容量，而不是在卷组中使用的热备用驱动器。 使用微调器控制来调整驱动器数量。根据驱动器数量，池中的保留容量显示在微调器框旁边。 请记住以下有关保存容量的信息。 • 由于从池的总可用容量中减去保留容量，因此保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。 • 如果减少保存容量，则会增加可用于池卷的容量。 额外的优化容量（仅限 EF600 和 EF300 阵列）-- 创建池时，将生成推荐的优化容量，以提供可用容量与性能和驱动器磨损寿命之间的平衡。您可以通过向右移动滑块来调整此平衡，以获得更好的性能和驱动器磨损寿命，但会减少可用容量，或者向左移动滑块以增加可用容量，但会降低性能和驱动器磨损寿命。 当未分配部分容量时，SSD 驱动器将具有更长的使用寿命和更好的最大写入性能。对于与池相关联的驱动器，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预留的可用容量的一部分。额外的优化容量通过减少可用容量来确保最低限度的优化容量，因此无法用于卷创建。

4. 单击 **Save**。

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 级别以适应访问卷组的应用程序的性能需求，请务必满足以下先决条件：

- 卷组必须处于最佳状态。
- 您必须在卷组中具有足够的容量才能转换到新的 RAID 级别。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要编辑的卷组，然后单击 **View/Edit Settings**。

   此时将显示卷组设置对话框。

3. 选择 **Settings** 选项卡，然后根据需要编辑卷组设置。

字段详细信息

设置	说明
名称	您可以更改用户提供的卷组的名称。需要指定卷组的名称。
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。如果卷组中的单个驱动器出现故障，则所有关联的卷都会出现故障，并且所有数据都会丢失。条带化 RAID 组将两个或多个驱动器合并为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。通过将一个驱动器的内容自动镜像到镜像对中的第二个驱动器来保护您的数据。在发生单个驱动器故障时，它可以提供保护。 • **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的大容量事务应用程序，例如数据库。 • **RAID 5** — 最适合多用户环境（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** — 适用于需要超出 RAID 5 的冗余保护但不需要高写入性能的环境。 只能使用命令行界面 (CLI) 将 RAID 3 分配给卷组。 更改 RAID 级别时，无法在操作开始后取消此操作。在更改期间，您的数据仍然可用。
优化容量（仅限 EF600 阵列）	创建卷组时，将生成推荐的优化容量，以提供可用容量与性能和驱动器磨损寿命之间的平衡。您可以通过将滑块向右移动来调整此平衡，以获得更好的性能和驱动器磨损寿命，但会减少可用容量，或者将滑块向左移动以增加可用容量，但会降低性能和驱动器磨损寿命。 当未分配部分容量时，SSD 驱动器将具有更长的使用寿命和更好的最大写入性能。对于与卷组相关联的驱动器，未分配的容量由组的可用容量（卷未使用的容量）和作为额外优化容量预留的可用容量的一部分组成。额外的优化容量通过减少可用容量来确保最低限度的优化容量，因此无法用于卷创建。

4. 单击 **Save**。

   如果由于 RAID 级别更改而导致容量减少、卷冗余丢失或架子/抽屉丢失保护丢失，则会出现一个确认对话框。选择 **Yes** 继续；否则单击 **No**。

结果

如果更改卷组的 RAID 级别，System Manager 将更改构成卷组的每个卷的 RAID 级别。操作过程中可能会轻微影响性能。

在 **SANtricity System Manager** 中启用或禁用现有卷组和池上的资源配置

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调配。

资源调配是 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。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 的系统上启用资源调配。除非之前已禁用资源调配，否则无需启用它。

开始之前

- 您必须具有 EF300 或 EF600 存储阵列。

  目前 EF300C 或 EF600C 存储阵列不支持 DULBE。

- 您必须具有 SSD 卷组或池，其中所有驱动器都支持 NVMe Deallocated 或 Unwritten Logical Block Error Enable (DULBE) 错误恢复功能。否则，资源调配选项不可用。

关于此任务

为现有卷组和池启用资源调配时，将更改选定卷组或池中的所有卷，以允许取消分配块。此过程可能涉及后台操作，以确保在 unmap 粒度上的一致分配。此操作不会取消任何空间的映射。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。

为现有卷组或池禁用资源调配时，后台操作会重写每个卷中的所有逻辑块。现有数据保持不变。写入操作将映射或设置与卷组或池关联的驱动器上的块。

对于新的卷组和池，您可以从菜单：Settings[System > Additional Settings > Enable/Disable Resource-Provisioned Volumes] 启用或禁用资源调配。

步骤

1. 选择菜单：Storage[Pools & 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 **Uncommon Tasks**，然后选择 **Enable resource provisioning** 或 **Disable resource provisioning**。
4. 在对话框中，确认此操作。

如果重新启用 **DULBE** — 后台操作完成后，可能需要重新启动主机，以便它检测到 DULBE 配置更改，然后重新装载所有文件系统。

在 **SANtricity System Manager** 中为新卷组或池启用或禁用资源配置

如果以前禁用了资源调配的默认功能，则可以为创建的任何新 SSD 卷组或池重新启用它。您也可以再次禁用此设置。

资源调配是 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。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，将在驱动器支持 DULBE 的系统上启用资源调配。

开始之前

- 您必须具有 EF300 或 EF600 存储阵列。
- 您必须具有 SSD 卷组或池，其中所有驱动器都支持 NVMe Deallocated 或 Unwritten Logical Block Error Enable (DULBE) 错误恢复功能。

  目前 EF300C 或 EF600C 存储阵列不支持 DULBE。

关于此任务

为新卷组或池重新启用资源调配时，只会影响新创建的卷组和池。启用资源调配的任何现有卷组和池将保持不变。

步骤

1. 选择菜单：Settings[System]。
2. 向下滚动到 **Additional Settings**，然后单击 **Enable/Disable Resource-Provisioned Volumes**。

   设置描述指示当前是启用还是禁用资源配置。

3. 在对话框中，确认此操作。

结果

启用或禁用资源调配仅影响您创建的新 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

可以为池或卷组启用驱动器安全，以防止对池或卷组中包含的驱动器上的数据进行未经授权的访问。只有通过配置了安全密钥的控制器才能对驱动器进行读取和写入访问。

开始之前

- 必须启用驱动器安全功能。
- 必须创建安全密钥。
- 该池或卷组必须处于 Optimal 状态。
- 池或卷组中的所有驱动器都必须是具有安全功能的驱动器。

关于此任务

如果要使用 Drive Security，请选择具有安全功能的池或卷组。池或卷组可以同时包含具有安全功能和不具有安全功能的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。

启用安全后，只能通过删除池或卷组，然后擦除驱动器来将其删除。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要启用安全性的池或卷组，然后单击菜单：More[Enable security]。

此时将显示"确认启用安全"对话框。

3. 确认您要为所选池或卷组启用安全性，然后单击 **Enable**。

管理 SSD 缓存

SSD 缓存在 SANtricity 软件中的工作原理

SSD Cache 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硬盘（SSD）上，以动态提高系统性能。SSD Cache 仅用于主机读取。

SSD 缓存与主缓存

SSD Cache 是与控制器的动态随机存取内存 (DRAM) 中的主缓存一起使用的辅助缓存。

SSD 缓存的运行方式与主缓存不同：

- 对于主缓存，每个 I/O 操作必须通过缓存暂存数据以执行此操作。

  在主缓存中，数据在主机读取后存储在 DRAM 中。

- 仅当将数据放置在缓存中有利于提高整体系统性能时，才使用 SSD 缓存。

  在 SSD 缓存中，数据从卷复制并存储在两个内部 RAID 卷上（每个控制器一个），这些卷在创建 SSD 缓存时自动创建。

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，这两个卷确实计算在存储阵列中允许的卷总数中。

SSD 缓存的使用方式

智能缓存将数据置于较低延迟的驱动器中，因此可以更快地响应对该数据的未来请求。如果程序请求缓存中的数据（称为"`cache hit`"），则较低延迟的驱动器可以为该事务提供服务。否则，会发生"`cache miss`"，必须从原始较慢的驱动器访问数据。随着更多的缓存命中，整体性能会得到改善。

当主机程序访问存储阵列的驱动器时，数据将存储在 SSD Cache 中。当主机程序再次访问相同的数据时，它会从 SSD Cache 而不是硬盘驱动器中读取。常用的数据存储在 SSD Cache 中。只有在无法从 SSD Cache 读取数据时才会访问硬盘驱动器。

只有在有利于将数据放入缓存以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，它遵循以下步骤：

1. 检查 DRAM 缓存。
2. 如果在 DRAM 缓存中未找到，则检查 SSD 缓存。
3. 如果在 SSD 缓存中未找到，则从硬盘获取。如果数据被认为值得缓存，则复制到 SSD 缓存。

性能提升

将访问量最大的数据（热点）复制到 SSD Cache 可以实现更高效的硬盘操作、降低延迟并加快读写速度。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。

简单的卷 I/O 机制用于将数据移动到 SSD Cache 和从 SSD Cache 移动数据。在 SSD 上缓存和存储数据后，在 SSD Cache 上执行该数据的后续读取，从而无需访问 HDD 卷。

SSD 缓存和驱动器安全功能

要在也使用驱动器安全（已启用安全）的卷上使用 SSD Cache，卷的驱动器安全功能和 SSD Cache 必须匹配。如果不匹配，则卷将不会启用安全。

实施 SSD 缓存

要实现 SSD Cache，请执行以下操作：

1. 创建 SSD 缓存。
2. 将 SSD Cache 与要为其实施 SSD 读缓存的卷关联。

> 分配给使用控制器 SSD Cache 的任何卷都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

了解在您的存储阵列上使用 SSD Cache 时的限制。

限制

- 分配给使用控制器 SSD Cache 的任何卷都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 Cache。
- 存储阵列上的最大可用 SSD Cache 容量为 10 TB。
- 快照映像不支持 SSD 缓存。
- 如果导入或导出已启用或禁用 SSD Cache 的卷，则不会导入或导出缓存数据。
- 如果不先删除 SSD Cache，则无法删除 SSD Cache 中的最后一个驱动器。

驱动器安全的限制

- 只有在创建 SSD Cache 时，才能在 SSD Cache 上启用安全性。您以后无法启用安全性，就像您可以在卷上启用安全性一样。
- 如果将支持安全的驱动器与 SSD Cache 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 Drive Security。
- 已启用安全的卷必须具有已启用安全的 SSD Cache。

在 SANtricity System Manager 中创建 SSD 缓存

您可以使用 SSD Cache 功能将最常访问的数据（"热"数据）缓存到延迟较低的固态硬盘（SSD）上，从而动态提高系统性能。SSD Cache 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 Cache 时，您可以使用单个驱动器或多个驱动器。由于读缓存位于存储阵列中，因此在使用存储阵列的所有应用程序之间共享缓存。您选择要缓存的卷，然后缓存是自动和动态的。

创建新 SSD 缓存时，请遵循以下准则。

- 只有在创建 SSD Cache 时，您才可以启用安全性，而不是以后。
- 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 缓存将分配给拥有该卷的控制器。
- 存储阵列上的最大可用 SSD Cache 容量取决于控制器的主缓存容量。
- 快照映像不支持 SSD 缓存。
- 如果导入或导出已启用或禁用 SSD Cache 的卷，则不会导入或导出缓存数据。
- 分配给使用控制器 SSD Cache 的任何卷都不符合自动负载平衡传输的条件。
- 如果关联的卷已启用安全，请创建一个启用安全的 SSD Cache。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击菜单：创建 [SSD Cache]。

   此时将显示创建 SSD 缓存对话框。

3. 输入 SSD Cache 的名称。
4. 根据以下特征选择要使用的 SSD Cache 候选项。

特征	用途
容量	以 GiB 为单位显示可用容量。为应用程序的存储需求选择容量。 SSD Cache 的最大容量取决于控制器的主缓存容量。如果分配给 SSD Cache 的容量超过最大值，则任何额外容量都无法使用。 SSD Cache 容量计入您的总分配容量。
驱动器总数	显示此 SSD 缓存可用的驱动器数量。选择具有所需驱动器数量的 SSD 候选。
支持安全功能	指示 SSD Cache 候选项是否完全由支持安全的驱动器组成，这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。 如果要创建启用安全的 SSD Cache，请在支持安全的列中查找 **Yes - FDE** 或 **Yes - FIPS**。
启用安全?	提供使用具有安全功能的驱动器启用驱动器安全功能的选项。如果要创建启用安全的 SSD Cache，请选中启用安全复选框。 一旦启用，就不能禁用安全性。您只能在创建 SSD Cache 时启用 SSD Cache 的安全性，而不能稍后启用。

特征	用途
支持 DA	指示此 SSD Cache 候选项是否可用 Data Assurance (DA)。Data Assurance (DA) 检查并更正数据通过控制器传输到驱动器时可能发生的错误。 如果要使用 DA，请选择支持 DA 的 SSD Cache 候选项。此选项仅在已启用 DA 功能时可用。 SSD Cache 可以包含支持 DA 和不支持 DA 的驱动器，但所有驱动器都必须支持 DA 才能使用 DA。

5. 将 SSD Cache 与要为其实施 SSD 读缓存的卷关联。要立即在兼容卷上启用 SSD Cache，请选中*在映射到主机的现有兼容卷上启用 SSD Cache*复选框。

   如果卷共享相同的驱动器安全和 DA 功能，则它们是兼容的。

6. 单击 **Create**。

在 **SANtricity System Manager** 中更改 **SSD Cache** 设置

您可以编辑 SSD Cache 的名称，并查看其状态、最大和当前容量、Drive Security 和 Data Assurance 状态及其关联的卷和驱动器。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要编辑的 SSD Cache，然后单击 **View/Edit Settings**。

   此时将显示 SSD 缓存设置对话框。

3. 根据需要查看或编辑 SSD Cache 设置。

字段详细信息

设置	说明
名称	显示 SSD Cache 的名称，您可以更改该名称。SSD Cache 的名称是必需的。
特点	显示 SSD Cache 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
容量	显示 SSD Cache 的当前容量和允许的最大容量。 SSD Cache 允许的最大容量取决于控制器的主缓存大小： • 高达 1 GiB • 1 GiB 至 2 GiB • 2 GiB 至 4 GiB • 超过 4 GiB
安全与 DA	显示 SSD Cache 的驱动器安全和 Data Assurance 状态。 • 支持安全 — 指示 SSD Cache 是否完全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 — 指示是否在 SSD Cache 上启用安全功能。 • 支持 **DA** — 指示 SSD Cache 是否完全由支持 DA 的驱动器组成。支持 DA 的驱动器可以检查并纠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	显示与 SSD Cache 关联的卷和驱动器。

4. 单击 **Save**。

在 **SANtricity System Manager** 中查看 **SSD** 缓存统计信息

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

标称统计数据是详细统计数据的子集，显示在"查看 SSD 缓存统计数据"对话框中。仅当将所有 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。

在查看和解释统计数据时，请记住，某些解释是通过查看统计数据的组合得出的。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择要查看其统计信息的 SSD Cache，然后单击菜单：更多[查看 SSD Cache 统计信息]。

   此时将显示 View SSD Cache Statistics（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	说明
读取	显示从启用 SSD Cache 的卷中读取的主机总数。读取与写入比率越大，缓存的操作就越好。
写入	对启用了 SSD Cache 的卷的主机写入总数。读取与写入的比率越大，缓存的操作就越好。
缓存命中数	显示缓存命中次数。
缓存命中率 %	显示缓存命中的百分比。此数字源自 Cache Hits /（读取 + 写入）。要进行有效的 SSD Cache 操作，缓存命中率应大于 50%。
缓存分配 %	显示已分配的 SSD Cache 存储百分比，以此控制器可用的 SSD Cache 存储百分比表示，并从已分配字节数/可用字节数得出。
缓存利用率 %	显示包含来自已启用卷的数据的 SSD Cache 存储百分比，以分配的 SSD Cache 存储百分比表示。此金额表示 SSD Cache 的使用率或密度。从分配的字节/可用字节派生。
全部导出	将所有 SSD Cache 统计信息导出为 CSV 格式。导出的文件包含 SSD Cache 的所有可用统计信息（标称和详细）。

3. 单击 **Cancel** 以关闭此对话框。

管理预留容量

SANtricity 软件中保留容量的工作原理

为卷提供复制服务操作（如快照或异步镜像操作）时，将自动创建保留容量。

保留容量的目的是在出现问题时存储这些卷上的数据更改。与卷一样，保留容量是从池或卷组创建的。

复制使用预留容量的服务对象

保留容量是这些复制服务对象使用的底层存储机制：

- Snapshot 组
- 读/写快照卷
- 一致性组成员卷
- 镜像对卷

创建或扩展这些复制服务对象时，必须从池或卷组创建新的保留容量。保留容量通常是快照操作的基本卷的 40% 和异步镜像操作的基本卷的 20%。但是，保留容量会根据对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 256 TiB 的最大报告容量，则无法增加其容量。确保将精简卷的预留容量设置为大于最大报告容量的大小。（精简卷始终是精简配置的，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保留容量，请查看有关保留容量的以下操作和结果：

- 如果精简卷的保留容量失败，则精简卷本身不会自动转换为"失败"状态。但是，由于精简卷上的所有 I/O 操作都需要访问保留容量卷，因此 I/O 操作将始终导致将检查条件返回给请求主机。如果保留容量卷的根本问题可以解决，则保留容量卷将返回到"最佳"状态，并且精简卷将再次发挥作用。
- 如果使用现有精简卷来完成异步镜像对，则会使用新的保留容量卷重新初始化该精简卷。在初始同步过程中，只有在主端调配的块才会被传输。

容量警报

复制服务对象具有可配置的容量警告和警报阈值，以及保留容量已满时的可配置响应。

当复制服务对象卷的保留容量接近填充点时，向用户发出警报。默认情况下，当保留容量卷已满 75% 时会发出此警报；但是，您可以根据需要向上或向下调整此警报点。如果您收到此警报，则可以增加当时保留容量卷的容量。在这方面，每个复制服务对象都可以独立配置。

孤立的预留容量卷

孤立的保留容量卷是一个不再存储用于复制服务操作的数据的卷，因为其关联的复制服务对象已被删除。当复制服务对象被删除时，其保留容量卷也应该被删除。但是，保留容量卷无法删除。

由于孤立的保留容量卷未被任何主机访问，因此它们是回收的候选卷。手动删除孤立的保留容量卷，以便您可以将其容量用于其他操作。

System Manager 会在主页的通知区域显示"回收未使用的容量"消息，提醒您孤立的保留容量卷。您可以单击*回收未使用的容量*以显示"回收未使用的容量"对话框，您可以在其中删除孤立的保留容量卷。

预留容量的特点

- 在卷创建期间，需要考虑分配给保留容量的容量，以保留足够的可用容量。
- 保留容量可以小于基本卷（最小大小为 8 MiB）。
- 一些空间由元数据消耗，但它非常小（192 KiB），因此在确定保留容量卷的大小时不需要考虑它。

- 保留容量不能从主机直接读取或写入。
- 每个读/写快照卷、快照组、一致性组成员卷和镜像对卷都存在保留容量。

在 **SANtricity System Manager** 中增加预留容量

您可以增加保留容量，这是用于存储对象上的任何复制服务操作的物理分配容量。

对于快照操作，它通常是基本卷的 40%；对于异步镜像操作，它通常是基本卷的 20%。通常，当您收到存储对象的保留容量正在变满的警告时，您会增加保留容量。

开始之前

- 池或卷组中的卷必须具有"最佳"状态，并且不得处于任何修改状态。
- 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不存在可用容量，则可以将未分配的容量以未使用的驱动器的形式添加到池或卷组中。

关于此任务

对于以下存储对象，只能以 8 GiB 的增量增加保留容量：

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

如果您认为主卷将经历许多更改或特定复制服务操作的寿命将非常长，请使用较高的百分比。

> 您不能增加只读快照卷的保留容量。只有读写快照卷需要保留容量。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择 **Reserved Capacity** 选项卡。
3. 选择要为其增加保留容量的存储对象，然后单击 增加容量。

   此时将显示"增加保留容量"对话框。

4. 使用微调框调整容量百分比。

   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。

5. 单击 **Increase**。

结果

System Manager 执行以下操作：

- 增加存储对象的保留容量。

- 显示新增的保留容量。

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

您可以使用"减少容量"选项来减少以下存储对象的保留容量：快照组、快照卷和一致性组成员卷。您只能按用于增加保留容量的数量来减少保留容量。

开始之前

- 存储对象必须包含多个保留容量卷。
- 存储对象不得为镜像对卷。
- 如果存储对象是快照卷，则它必须是已禁用的快照卷。
- 如果存储对象是快照组，则它不得包含任何关联的快照映像。

关于此任务

查看以下指南：

- 您只能按照与添加时相反的顺序删除保留容量卷。
- 无法减少只读快照卷的保留容量，因为它没有任何关联的保留容量。仅读写快照卷需要保留容量。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击 **Reserved Capacity** 选项卡。
3. 选择要降低其预留容量的存储对象，然后单击 降低容量。

   此时将显示减少保留容量对话框。
4. 选择要减少预留容量的容量大小，然后单击 **Decrease**。

结果

System Manager 执行以下操作：

- 更新存储对象的容量。
- 显示存储对象的新更新保留容量。
- 当您降低快照卷的容量时，System Manager 会自动将快照卷转换为"已禁用"状态。已禁用意味着快照卷当前未与快照映像关联，因此无法分配给主机进行 I/O。

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 System Manager 发送保留容量警报通知的百分比点或保留容量达到其最大定义百分比时要使用的策略。

在创建 Snapshot 组期间，将创建保留容量以存储组中包含的所有 Snapshot 映像的数据。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击 **Reserved Capacity** 选项卡。
3. 选择要编辑的 snapshot 组，然后单击*查看/编辑设置*。

   此时将显示 Snapshot 组设置对话框。

4. 根据需要更改 Snapshot 组的设置。

字段详细信息

设置	说明
Snapshot 组设置	名称
快照组的名称。需要指定快照组的名称。	自动删除
将组中的快照图像总数保持在或低于用户定义的最大值的设置。启用此选项时，System Manager 会在创建新快照时自动删除组中最旧的快照图像，以符合组允许的最大快照图像数。	Snapshot 图像限制
一个可配置的值，指定 Snapshot 组允许的最大 Snapshot 映像数。	Snapshot 计划
如果是，则设置自动创建 Snapshot 的计划。	保留容量设置
在…时提醒我	使用微调框可调整 System Manager 在 Snapshot 组保留容量接近满时发送警报通知的百分比点。 当 Snapshot 组的保留容量超过指定阈值时，System Manager 会发送警报，允许您有时间增加保留容量或删除不必要的对象。
完全保留容量的政策	您可以从以下策略中选择一项： • 清除最旧的 **snapshot** 映像 — System Manager 会自动清除 snapshot 组中最旧的 snapshot 映像，从而释放 snapshot 映像保留容量，以便在组内重复使用。 • 拒绝对基本卷的写入 — 当保留容量达到其最大定义百分比时，System Manager 会拒绝对触发保留容量访问的基本卷的任何 I/O 写入请求。
关联对象	基础卷

设置	说明
用于组的基本卷的名称。基本卷是创建 Snapshot 映像的源。它可以是厚卷或精简卷，通常分配给主机。基本卷可以驻留在卷组或磁盘池中。	Snapshot 图像

5. 单击 保存 以将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，以调整系统在快照卷的保留容量接近满时发送警报通知的百分比点。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击 **Reserved Capacity** 选项卡。
3. 选择要编辑的快照卷，然后单击 查看/编辑设置。

   此时将显示 Snapshot Volume Reserved Capacity Settings 对话框。

4. 根据需要更改快照卷的保留容量设置。

   字段详细信息

设置	说明
在…时提醒我	使用旋转框可调整当成员卷的保留容量接近满时系统发送警报通知的百分比点。 当快照卷的保留容量超过指定阈值时，系统会发送警报，让您有时间增加保留容量或删除不必要的对象。

5. 单击 保存 以将更改应用于快照卷保留容量设置。

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，以调整成员卷的保留容量接近满时 SANtricity System Manager 发送警报通知的百分比点，并更改策略以在保留容量达到其最大定义百分比时使用。

关于此任务

更改单个成员卷的保留容量设置也会更改与一致性组关联的所有成员卷的保留容量设置。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击 **Reserved Capacity** 选项卡。
3. 选择要编辑的一致性组成员卷，然后单击 **View/Edit Settings**。

   此时将显示"成员卷保留容量设置"对话框。

4. 根据需要更改成员卷的预留容量设置。

   字段详细信息

设置	说明
在…时提醒我	使用微调框可调整 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。 当成员卷的保留容量超过指定阈值时，System Manager 会发送警报，允许您有时间增加保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相同一致性组的 *all* 成员卷的警报设置。
完全保留容量的政策	您可以从以下策略中选择一项： • 清除最旧的 **snapshot** 映像 — System Manager 会自动清除一致性组中最旧的 snapshot 映像，从而释放成员的保留容量，以便在组内重用。 • 拒绝对基本卷的写入 — 当保留容量达到其最大定义百分比时，System Manager 会拒绝对触发保留容量访问的基本卷的任何 I/O 写入请求。

5. 单击 **Save** 以应用更改。

结果

System Manager 更改成员卷的保留容量设置，以及一致性组中所有成员卷的保留容量设置。

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 System Manager 发送警报通知的百分比点，即当镜像对卷的预留容量接近满时。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择 **Reserved Capacity** 选项卡。
3. 选择要编辑的镜像对卷，然后单击 **View/Edit Settings**。

   此时将显示镜像配对卷保留容量设置对话框。

4. 根据需要更改镜像对卷的预留容量设置。

   字段详细信息

设置	说明
在…时提醒我	使用微调框可调整在镜像对的保留容量接近满时 System Manager 发送警报通知的百分比点。 当镜像对的保留容量超过指定阈值时，System Manager 会发送警报，让您有时间增加保留容量。 更改一个镜像对的 Alert 设置会更改属于同一镜像一致性组的所有镜像对的 Alert 设置。

5. 单击 **Save** 以应用更改。

在 SANtricity System Manager 中取消待处理的快照映像

您可以在完成之前取消挂起的快照图像。快照异步发生，快照的状态处于挂起状态，直到快照完成。快照图像在同步操作完成后立即完成。

关于此任务

由于以下并发条件，快照映像处于 Pending 状态：

- 包含此快照映像的快照组或一致性组的一个或多个成员卷的基本卷是异步镜像组的成员。
- 此卷或多个卷当前处于异步镜像同步操作中。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击 **Reserved Capacity** 选项卡。
3. 选择要取消挂起快照映像的快照组，然后单击菜单：Uncommon Tasks[Cancel pending snapshot image]。
4. 单击 **Yes** 以确认要取消挂起的快照映像。

在 SANtricity System Manager 中删除快照组

当要永久删除快照组的数据并将其从系统中删除时，可以删除该快照组。删除快照组将回收池或卷组中可重用的保留容量。

关于此任务

如果删除某个快照组，则此组中的所有快照映像也将被删除。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 单击 **Reserved Capacity** 选项卡。

3. 选择要删除的快照组，然后单击 **Uncommon Tasks › Delete snapshot group**。

   此时将显示确认删除快照组对话框。

4. 键入 `delete` 以确认。

结果

System Manager 执行以下操作：

- 删除与快照组关联的所有快照映像。
- 禁用与快照组映像关联的任何快照卷。
- 删除快照组的保留容量。

SANtricity System Manager 的池和卷组常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是卷组?

卷组是具有共享特征的卷的容器。卷组具有定义的容量和 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?

池是逻辑上分组的一组驱动器。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。）

池可以消除管理员监视每个主机上的使用情况以确定它们何时可能耗尽存储空间并避免传统磁盘大小调整中断的需要。当池接近耗尽时，可以无中断地将其他驱动器添加到池中，并且容量增长对主机是透明的。

使用池，数据会自动重新分配以保持平衡。通过在整个池中分配奇偶校验信息和备用容量，池中的每个驱动器都可用于重建出现故障的驱动器。这种方法不使用专用热备盘驱动器，而是在整个池中保留保存（备用）容量。驱动器出现故障时，读取其他驱动器上的段以重新创建数据。然后选择一个新的驱动器来写入故障驱动器上的每个段，以便保持驱动器之间的数据分布。

什么是预留容量?

保留容量是物理分配的容量，用于存储快照映像、一致性组成员卷和镜像对卷等复制服务对象的数据。

与复制服务操作关联的保留容量卷驻留在池或卷组中。您可以从池或卷组创建保留容量。

什么是 **FDE/FIPS** 安全?

FDE/FIPS 安全是指在写入期间加密数据并在读取期间使用唯一加密密钥解密数据的具有安全功能的驱动器。这些具有安全功能的驱动器可防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。

支持安全的驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。FIPS 驱动器已通过认证测试。

对于需要 FIPS 支持的卷，仅使用 FIPS 驱动器。在卷组或池中混合 FIPS 和 FDE 驱动器将导致所有驱动器被视为 FDE 驱动器。此外，FDE 驱动器不能添加到全 FIPS 卷组或池中或用作备件。

什么是冗余检查?

冗余检查确定池或卷组中的卷上的数据是否一致。冗余数据用于在池或卷组中的一个驱动器发生故障时快速重建替换驱动器上的信息。

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导致错误。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。

池和卷组之间有什么区别?

池类似于卷组，具有以下差异。

- 池中的数据随机存储在池中的所有驱动器上，而卷组中的数据存储在同一组驱动器上。
- 在驱动器发生故障时，池具有较少的性能降级，并且重建所需的时间较短。
- 池具有内置的保存容量，因此不需要专用的热备盘驱动器。
- 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?

以下示例说明了为什么要手动配置池。

- 如果存储阵列上有多个应用程序，并且不希望它们竞争相同的驱动器资源，则可以考虑为一个或多个应用程序手动创建一个较小的池。

  您可以只分配一个或两个卷，而不是将工作负载分配给具有多个卷的大型池来分发数据。手动创建一个专用于特定应用程序工作负载的单独池，可以使存储阵列操作执行得更快，争用更少。

  要手动创建池：选择 **Storage**，然后选择 **Pools & Volume Groups**。在 All Capacity 选项卡中，单击菜单：Create[Pool]。

- 如果存在相同驱动器类型的多个池，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中。

  要手动将驱动器添加到现有池：从 Pools & Volume Groups 页面，选择池，然后单击 **Add Capacity**。

为什么容量警报很重要？

容量警报指示何时将驱动器添加到池中。池需要足够的可用容量才能成功执行存储阵列操作。您可以通过配置 SANtricity System Manager 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 **Pool auto-configuration** 选项或 **Create pool** 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提醒通知。如果选择手动创建池，则可以确定提醒通知设置；如果愿意，则可以接受默认设置。您可以稍后在 **Settings › Alerts** 中调整这些设置。

当池中的可用容量达到指定的百分比时，将使用您在警报配置中指定的方法发送警报通知。

为什么我无法增加保存容量？

如果已在所有可用的可用容量上创建了卷，则可能无法增加保留容量。

保留容量是在池上保留以支持潜在驱动器故障的容量（驱动器数量）。创建池时，系统会根据池中的驱动器数量自动保留默认的保留容量。如果已为所有可用容量创建了卷，则如果不通过添加驱动器或删除卷向池中添加容量，则无法增加保留容量。

您可以从 **Pools & Volume Groups** 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。

保留容量指定为驱动器数量，即使实际保留容量分布在池中的驱动器之间。

我可以从池中删除的驱动器数量是否有限制？

SANtricity System Manager 为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少于 11 个驱动器。
- 如果在将数据重新分配给池中的剩余驱动器时，池中的可用容量不足以包含已删除驱动器中的数据，则无法删除驱动器。
- 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。如果需要删除超过 60 个驱动器，请重复"删除驱动器"操作。

驱动器支持哪些媒体类型？

支持以下媒体类型：硬盘驱动器 (HDD) 和固态硬盘 (SSD)。

为什么有些驱动器没有显示？

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。

由于以下任何原因，驱动器不符合条件：

- 驱动器必须取消分配且未启用安全功能。已成为另一个池、另一个卷组一部分或配置为热备盘的驱动器不符合条件。如果驱动器未分配但已启用安全功能，您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。
- 如果驱动器的容量太小，则不符合条件。

- 驱动器介质类型必须在池或卷组内匹配。您不能混合以下内容：
  - 带固态硬盘 (SSD) 的硬盘驱动器 (HDD)
  - 使用 SAS 驱动器的 NVMe
  - 具有 512 字节和 4KiB 卷块大小的驱动器
- 如果池或卷组包含所有支持安全的驱动器，则不会列出不支持安全的驱动器。
- 如果池或卷组包含所有联邦信息处理标准 (FIPS) 驱动器，则不列出非 FIPS 驱动器。
- 如果池或卷组包含所有支持 Data Assurance (DA) 的驱动器，并且池或卷组中至少有一个启用 DA 的卷，则不支持 DA 的驱动器不符合条件，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 DA 的卷，则可以将不支持 DA 的驱动器添加到该池或卷组。如果您决定混合使用这些驱动器，请记住您无法创建任何启用 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的容量。

如何维护货架/抽屉丢失保护?

要为池或卷组维护货架/抽屉丢失保护，请使用下表中指定的标准。

级别	货架/抽屉损失保护标准	所需的最少货架/抽屉数量
池	对于磁盘架，池在单个磁盘架中包含的驱动器不得超过两个。 对于抽屉，池必须包含来自每个抽屉的相等数量的驱动器。	6 个用于机架 5 个用于抽屉
RAID 6	该卷组在单个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单独的架子或抽屉中。	3
RAID 1	镜像对中的每个驱动器必须位于单独的架子或抽屉中。	2
RAID 0	无法实现货架/抽屉丢失保护。	不适用

如果池或卷组中的驱动器已出现故障，则不维护盘架/抽屉丢失保护。在这种情况下，失去对驱动器盘架或抽屉的访问权限，从而导致池或卷组中的另一个驱动器丢失数据。

池和卷组的最佳驱动器定位是什么?

创建池和卷组时，请确保在上驱动器插槽和下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 连接到不同的 PCI 网桥。为了获得最佳性能，您应该平衡驱动器选择，以包括来自上下插槽的大致相等数量的驱动器。这种定位可确保您的卷不会在必要时提前达到带宽限制。

哪个 **RAID** 级别最适合我的应用程序?

要最大限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取和写入百分比来确定适当的 RAID 级别。使用"性能"页面获取这些百分比。

RAID 级别和应用程序性能

RAID 依赖于一系列名为 *levels* 的配置，以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 配置的出色读取性能，具有高读取百分比的应用程序在使用 RAID 5 卷或 RAID 6 卷时将表现良好。

读取百分比较低（写入密集型）的应用程序在 RAID 5 卷或 RAID 6 卷上的性能不佳。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

- 说明
  - 非冗余、条带化模式。
- 工作原理
  - RAID 0 在卷组中的所有驱动器上对数据进行条带化。
- 数据保护功能
  - 对于高可用性需求，不建议使用 RAID 0。RAID 0 更适合非关键数据。
  - 如果卷组中的单个驱动器出现故障，则所有关联的卷都会出现故障，并且所有数据都会丢失。
- 驱动器数量要求
  - RAID 级别 0 至少需要一个驱动器。
  - RAID 0 卷组可以有 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**

- 说明
  - 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 使用驱动器条带化对一组镜像驱动器对中的数据进行条带化。
- 数据保护功能
  - RAID 1 和 RAID 10 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拷贝到另一个驱动器。
  - 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相关卷降级。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的卷发生故障，并可能发生数据丢失。

- 驱动器数量要求
  - 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，则会在整个卷组中自动配置 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 **Pools & Volume Groups** 以向卷组添加其他驱动器，然后重试该操作。
  - RAID 1 和 RAID 10 卷组可以有 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

- 说明
  - 高 I/O 模式。
- 工作原理
  - 用户数据和冗余信息（奇偶校验）在驱动器上进行条带化。
  - 一个驱动器的等效容量用于冗余信息。
- 数据保护功能
  - 如果 RAID 5 卷组中的单个驱动器发生故障，则所有关联的卷都将降级。冗余信息仍然允许访问数据。
  - 如果 RAID 5 卷组中有两个或多个驱动器发生故障，则所有关联的卷都会出现故障，并且所有数据都会丢失。
- 驱动器数量要求
  - 卷组中必须至少有三个驱动器。
  - 通常，卷组中最多只能有 30 个驱动器。

RAID 6

- 说明
  - 高 I/O 模式。
- 工作原理
  - 用户数据和冗余信息（双奇偶校验）在驱动器上进行条带化。
  - 两个驱动器的等效容量用于冗余信息。
- 数据保护功能
  - 如果 RAID 6 卷组中有一个或两个驱动器发生故障，则所有关联的卷都会降级，但冗余信息仍允许访问数据。
  - 如果 RAID 6 卷组中有三个或更多驱动器发生故障，则所有关联的卷都会出现故障，并且所有数据都会丢失。
- 驱动器数量要求
  - 卷组中必须至少有五个驱动器。
  - 通常，卷组中最多只能有 30 个驱动器。

不能更改池的 RAID 级别。用户界面自动将池配置为 RAID 6。

RAID 级别和数据保护

RAID 1、RAID 5 和 RAID 6 将冗余数据写入驱动器介质以实现容错。冗余数据可以是数据的副本（镜像）或从数据导出的纠错代码。如果驱动器发生故障，您可以使用冗余数据快速重建替换驱动器上的信息。

您可以在单个卷组中配置单个 RAID 级别。该卷组的所有冗余数据都存储在卷组内。卷组的容量是成员驱动器的总容量减去为冗余数据保留的容量。冗余所需的容量取决于所使用的 RAID 级别。

什么是数据保障?

数据保障 (DA) 实施 T10 Protection Information (PI) 标准，该标准通过检查和纠正沿 I/O 路径传输数据时可能发生的错误来提高数据完整性。

Data Assurance 功能的典型使用将检查控制器和驱动器之间的 I/O 路径部分。DA 功能在池和卷组级别呈现。

启用此功能后，存储阵列会将错误检查代码（也称为循环冗余检查或 CRC）附加到卷中的每个数据块。移动数据块后，存储阵列使用这些 CRC 代码来确定在传输过程中是否发生任何错误。潜在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支持 DA 的池或卷组（在池和卷组候选表中的"DA"旁边查找"是"）。

确保使用支持 DA 的 I/O 接口将这些启用 DA 的卷分配给主机。支持 DA 的 I/O 接口包括光纤通道、SAS、TCP/IP 上的 iSCSI、NVMe/FC、NVMe/IB、NVME/RoCE 和 iSER over InfiniBand（用于 RDMA/IB 的 iSCSI 扩展）。SRP over InfiniBand 不支持 DA。

什么是安全功能 **(Drive Security)**?

驱动器安全是一项功能，可防止在从存储阵列中移除启用安全功能的驱动器时对其上的数据进行未经授权的访问。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。

关于增加预留容量，我需要知道什么?

通常，当您收到预留容量可能已满的警告时，您应该增加容量。您只能以 8 GiB 的增量增加预留容量。

- 您必须在池或卷组中具有足够的可用容量，以便在必要时可以对其进行扩展。

  如果任何池或卷组上不存在可用容量，则可以将未分配的容量以未使用的驱动器的形式添加到池或卷组中。

- 池或卷组中的卷必须具有"最佳"状态，并且不得处于任何修改状态。
- 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保留容量。只有读写快照卷需要保留容量。

对于快照操作，保留容量通常为基本卷的 40%。对于异步镜像操作，保留容量通常为基本卷的 20%。如果您认为基本卷将发生许多变化，或者存储对象的复制服务操作的估计预期寿命将非常长，请使用更高的百分比。

为什么我不能选择其他减少金额?

您只能按照之前增加预留容量的数量来减少预留容量。成员卷的预留容量只能按照添加时的相反顺序进行删除。

如果存在以下条件之一，则无法降低存储对象的保留容量：

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

您只能按照与添加时相反的顺序删除保留容量的卷。

无法减少只读快照卷的保留容量，因为它没有任何关联的保留容量。仅读写快照卷需要保留容量。

为什么我需要为每个成员卷保留容量？

快照一致性组中的每个成员卷必须具有自己的保留容量，以保存主机应用程序对基本卷所做的任何修改，而不会影响引用的一致性组快照映像。保留容量为主机应用程序提供对指定为读写的成员卷中包含的数据副本的写入访问权限。

主机无法直接读取或写入一致性组快照映像。相反，快照映像仅用于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 为一致性组中的每个成员卷创建保留容量。此保留容量为主机应用程序提供了对一致性组快照映像中包含的数据副本的写入权限。

如何查看和解释所有 **SSD Cache** 统计信息？

您可以查看 SSD Cache 的名义统计数据和详细统计数据。名义统计数据是详细统计数据的子集。

只有将所有 SSD 统计信息导出到 `.csv` 文件时，才能查看详细统计信息。在查看和解释统计数据时，请记住，一些解释是通过查看统计数据的组合得出的。

名义统计

要查看 SSD Cache 统计信息，请选择菜单：Storage[Pools & Volume Groups]。选择要查看其统计信息的 SSD Cache，然后选择菜单：More[View Statistics]。标称统计信息显示在"View SSD Cache Statistics"对话框中。

以下列表包括名义统计数据，这些统计数据是详细统计数据的子集。

标称统计量	说明
读取/写入	从启用 SSD Cache 的卷读取或向其写入的主机读取和主机写入总数。比较读取相对于写入的情况。读取需要大于写入才能有效执行 SSD Cache 操作。读取与写入的比例越大，缓存的操作就越好。
缓存命中数	缓存命中次数的计数。
缓存命中率 (%)	派生自 Cache Hits / (读取 + 写入)。要进行有效的 SSD Cache 操作，Cache Hit 百分比应大于 50%。一个小数字可以表示几件事： • 读取与写入比率太小 • 不重复读取 • 缓存容量太小

标称统计量	说明
缓存分配 (%)	分配的 SSD Cache 存储量，以此控制器可用的 SSD Cache 存储的百分比表示。从分配的字节/可用字节派生。Cache Allocation 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，或者 SSD Cache 容量大于所有正在访问的数据。在后一种情况下，较小的 SSD Cache 容量可以提供相同的性能水平。请注意，这并不表示缓存数据已放入 SSD Cache；这只是将数据放入 SSD Cache 之前的一个准备步骤。
缓存利用率 (%)	包含来自启用卷的数据的 SSD Cache 存储量，以分配的 SSD Cache 存储的百分比表示。此值表示从用户数据字节/分配字节派生的 SSD Cache 的利用率或密度。Cache Utilization 百分比通常低于 100%，可能要低得多。此数字显示 SSD Cache 容量中充满缓存数据的百分比。此数字低于 100% 是因为 SSD Cache 的每个分配单元（SSD Cache 块）被划分为称为子块的较小单元，这些子块在某种程度上是独立填充的。数字越高通常越好，但即使数字较小，性能提升也可能很显著。

详细统计信息

详细统计数据由名义统计数据加上其他统计数据组成。这些其他统计数据与名义统计数据一起保存，但与名义统计数据不同，它们不会显示在"查看 SSD 缓存统计数据"对话框中。您只能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	说明
读取块	主机读取中的块数。
写入块	主机写入中的块数。
完全命中块	缓存命中中的块数。完全命中块表示已完全从 SSD Cache 读取的块数。SSD Cache 仅对完全缓存命中的操作有益于性能。
部分命中	SSD Cache 中至少有一个块（但不是所有块）的主机读取数。部分命中是 SSD Cache 未命中，其中读取从基本卷得到满足。
部分命中 - 块	Partial Hits 中的块数。部分缓存命中和部分缓存命中块源于 SSD Cache 中只有部分数据的操作。在这种情况下，操作必须从缓存硬盘驱动器 (HDD) 卷获取数据。SSD Cache 对这种类型的命中不提供性能优势。如果部分缓存命中块计数高于完全缓存命中块，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。与 Cache Hits 相比，当 SSD Cache 预热时，预计会有更多的 Partial Hits 和 Misses。
未命中	SSD Cache 中没有任何块的主机读取数。当从基本卷满足读取时，会出现 SSD Cache 未命中。预计在 SSD Cache 预热时，部分命中和未命中的数量会比 Cache 命中更多。
未命中 - 块	Misses 中的块数。

详细统计信息	说明
填充操作（主机读取）	将数据从基本卷复制到 SSD Cache 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）	将数据从基本卷复制到 SSD Cache 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。
使操作无效	数据被无效或从 SSD Cache 中删除的次数。对于每个主机写入请求、具有强制单元访问 (FUA) 的每个主机读取请求、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 Cache 块已重复用于另一个基本卷和/或不同逻辑块寻址 (LBA) 范围的次数。为了有效的缓存操作，与读取和写入操作的组合数量相比，回收次数必须较少。如果回收操作数接近读取和写入总数，则 SSD Cache 发生颠簸。缓存容量需要增加或工作负载不适合与 SSD Cache 一起使用。
可用字节	SSD Cache 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 缓存分配的字节可能为空，或者它们可能包含来自基本卷的数据。
用户数据字节	SSD 缓存中包含来自基本卷的数据的已分配字节数。可用字节、已分配字节和用户数据字节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？

当未分配部分容量时，SSD 驱动器将具有更长的使用寿命和更好的最大写入性能。

对于与池相关联的驱动器，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）和作为额外优化容量预留的可用容量的一部分。额外的优化容量通过减少可用容量来确保最低限度的优化容量，因此无法用于卷创建。

创建池时，将生成推荐的优化容量，以提供性能、驱动器磨损寿命和可用容量的平衡。位于池设置对话框中的其他优化容量滑块允许调整池的优化容量。调整滑块以牺牲可用容量为代价，提供更好的性能和驱动器磨损寿命，或以牺牲性能和驱动器磨损寿命为代价，提供额外的可用容量。

附加优化容量滑块仅适用于 EF600 和 EF300 存储系统。

什么是卷组的优化容量？

当未分配部分容量时，SSD 驱动器将具有更长的使用寿命和更好的最大写入性能。

对于与卷组关联的驱动器，未分配容量由卷组的可用容量（卷未使用的容量）和可用容量的一部分作为优化容量

组成。额外的优化容量通过减少可用容量来确保最低限度的优化容量，因此无法用于卷创建。

创建卷组时，将生成推荐的优化容量，以提供性能、驱动器磨损寿命和可用容量的平衡。卷组设置对话框中的附加优化容量滑块允许调整卷组的优化容量。调整滑块以牺牲可用容量为代价来提供更好的性能和驱动器磨损寿命，或以牺牲性能和驱动器磨损寿命为代价来增加可用容量。

附加优化容量滑块仅适用于 EF600 和 EF300 存储系统。

资源配置功能是什么?

资源调配是 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。

资源调配的卷是 SSD 卷组或池中的厚卷，其中在创建卷时分配（分配给卷）驱动器容量，但取消分配（未映射）驱动器块。相比之下，在传统的厚卷中，所有驱动器块在后台卷初始化操作期间进行映射或分配，以初始化 Data Assurance 保护信息字段，并使每个 RAID 条带中的数据和 RAID 奇偶校验一致。使用资源调配的卷，没有时间限制的后台初始化。相反，每个 RAID 条带在第一次写入条带中的卷块时进行初始化。

资源调配的卷仅在 SSD 卷组和池上受支持，其中组或池中的所有驱动器都支持 NVMe Deallocated 或 Unwritten Logical Block Error Enable (DULBE) 错误恢复功能。创建资源调配的卷时，分配给该卷的所有驱动器块都将被取消分配（未映射）。此外，主机可以使用 NVMe Dataset Management 命令或 SCSI Unmap 命令取消分配卷中的逻辑块。取消分配块可以提高 SSD 磨损寿命并提高最大写入性能。每种驱动器型号和容量的改进程度各不相同。

目前 EF300C 或 EF600C 存储阵列不支持 DULBE。

关于资源调配的卷功能，我需要了解哪些信息?

资源调配是 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。

资源调配的卷是 SSD 卷组或池中的厚卷，其中在创建卷时分配（分配给卷）驱动器容量，但取消分配（未映射）驱动器块。相比之下，在传统的厚卷中，所有驱动器块在后台卷初始化操作期间进行映射或分配，以初始化 Data Assurance 保护信息字段，并使每个 RAID 条带中的数据和 RAID 奇偶校验一致。使用资源调配的卷，没有时间限制的后台初始化。相反，每个 RAID 条带在第一次写入条带中的卷块时进行初始化。

资源调配的卷仅在 SSD 卷组和池上受支持，其中组或池中的所有驱动器都支持 NVMe Deallocated 或 Unwritten Logical Block Error Enable (DULBE) 错误恢复功能。创建资源调配的卷时，分配给该卷的所有驱动器块都将被取消分配（未映射）。此外，主机可以使用 NVMe Dataset Management 命令或 SCSI Unmap 命令取消分配卷中的逻辑块。取消分配块可以提高 SSD 磨损寿命并提高最大写入性能。每种驱动器型号和容量的改进程度各不相同。

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。

目前 EF300C 或 EF600C 存储阵列不支持 DULBE。

卷和工作负载

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

您可以将卷创建为应用程序、数据库和文件系统存储数据的容器。创建卷时，还可以选择一个工作负载，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?

volume 是创建的逻辑组件，具有供主机访问的特定容量。尽管卷可能由多个驱动器组成，但对主机而言，卷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。*workload* 是支持应用程序（如 SQL Server 或 Exchange）的存储对象，可用于优化该应用程序的存储。

了解详情：

- "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"
- "可以对卷执行的操作"

如何创建卷和工作负载?

首先，您要创建一个工作负载。转到菜单：Storage[Volumes]，然后打开一个向导，引导您完成这些步骤。接下来，从池或卷组中的可用容量创建卷，然后分配创建的工作负载。

了解详情：

- "创建卷的工作流程"
- "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 软件中卷的工作原理

卷是管理和组织存储阵列上存储空间的数据容器。

您可以从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。这个概念类似于使用计算机上的文件夹/目录来组织文件，以便轻松快速地访问。

卷是主机唯一可见的数据层。在 SAN 环境中，卷映射到逻辑单元编号 (LUN)，这些逻辑单元编号对主机可见。LUN 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其容量。您可以从存储阵列上存在的池或卷组创建以下类型的卷。

- 从池 — 您可以从池中创建卷，作为_完全置备的（厚）卷_或_精简置备的（薄）卷_。

> 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 — 您只能将卷组中的卷创建为_完全置备（厚）卷_。

胖卷和瘦卷以不同的方式从存储阵列中获取容量：

- 在创建卷时分配厚卷的容量。
- 精简卷的容量在写入卷时作为数据进行分配。

精简配置有助于避免浪费分配的容量，并可以为企业节省前期存储成本。但是，完全配置的优点是延迟更少，因为在创建厚卷时会一次分配所有存储。

> 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其中存储的数据类型具有其各自的特征。其中一些特征包括：

- 段大小 — 段是在存储阵列移动到条带中的下一个驱动器（RAID 组）之前以千字节 (KiB) 为单位存储在驱动器上的数据量。段大小等于或小于卷组的容量。池的段大小是固定的，无法更改。
- 容量 — 您可以从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才能创建卷。
- 控制器所有权 — 所有存储阵列都可以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"`拥有`"卷的首选控制器（A 或 B）。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，以便在工作负载跨控制器转移时纠正任何负载平衡问题。自动负载平衡提供自动 I/O 工作负载平衡，并确保来自主机的传入 I/O 流量在两个控制器之间进行动态管理和平衡。
- 卷分配 — 您可以在创建卷时或稍后向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。主机检测到分配给卷的 LUN。如果要将卷分配给多个主机，请使用群集软件确保卷对所有主机可用。

  主机类型可以对主机可以访问的卷数进行特定限制。在创建供特定主机使用的卷时，请记住此限制。

- 描述性名称 — 您可以随心所欲地命名卷，但我们建议您使名称具有描述性。

在创建卷期间，为每个卷分配容量，并为其分配名称、段大小（仅限卷组）、控制器所有权和卷到主机的分配。根据需要，卷数据会自动在控制器之间进行负载平衡。

工作负载在 **SANtricity** 软件中的工作原理

创建卷时，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。

工作负载是支持应用程序的存储对象。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。这些卷特性是根据工作负载支持的应用程序类型进行优

化的。例如，如果创建支持 Microsoft SQL Server 应用程序的工作负载，然后为该工作负载创建卷，则会优化基础卷特征以支持 Microsoft SQL Server。

在创建卷期间，系统会提示您回答有关工作负载使用的问题。例如，如果要为 Microsoft Exchange 创建卷，系统会询问您需要多少个邮箱、平均邮箱容量要求以及所需的数据库副本数。系统使用此信息为您创建最佳卷配置，可以根据需要对其进行编辑。或者，您可以在卷创建顺序中跳过此步骤。

工作负载类型

您可以创建两种类型的工作负载：Application-specific 和 Other。

- 特定于应用程序。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。对于为以下应用程序类型创建的工作负载，会自动推荐和优化 I/O 类型、段大小、控制器所有权以及读取和写入缓存等卷特征。
  - Microsoft® SQL Server™
  - Microsoft® Exchange Server™
  - 视频监控应用程序
  - VMware ESXi™（用于与 Virtual Machine File System 配合使用的卷）

    您可以使用 Add/Edit Volumes 对话框查看推荐的卷配置并编辑、添加或删除系统推荐的卷和特征。
- 其他 （或不支持特定卷创建的应用程序）。其他工作负载使用的卷配置必须在您要创建未与特定应用程序关联的工作负载时手动指定，或者如果系统未针对您要在存储阵列上使用的应用程序进行内置优化。您必须使用"添加/编辑卷"对话框手动指定卷配置。

应用程序和工作负载视图

要查看应用程序和工作负载，请启动 SANtricity System Manager。从该界面，您可以通过几种不同的方式查看与特定于应用程序的工作负载相关的信息：

- 您可以选择卷图块中的 **Applications & 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。
- 您可以选择性能图块中的*应用程序和工作负载*选项卡，以查看逻辑对象的性能指标（延迟、IOPS 和 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

了解卷术语如何适用于您的存储阵列。

所有卷类型

术语	说明
已分配容量	您可以使用分配的容量来创建卷和进行复制服务操作。 对于厚卷，分配的容量和报告的容量是相同的，但对于精简卷，分配的容量和报告的容量是不同的。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，报告的容量是报告给主机的容量，而分配的容量是当前分配用于写入数据的驱动器空间量。

术语	说明
应用程序	应用程序是 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，系统会自动推荐优化存储的卷配置。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。
容量	容量是可以存储在卷中的数据量。
控制器所有权	控制器所有权定义了被指定为卷的所有者或主控制器的控制器。卷可以具有"`拥有`"卷的首选控制器（A 或 B）。使用 Automatic Load Balancing 功能自动调整卷所有权，以便在工作负载跨控制器转移时纠正任何负载平衡问题。Automatic Load Balancing 提供自动 I/O 工作负载平衡，并确保来自主机的传入 I/O 流量在两个控制器之间进行动态管理和平衡。
动态缓存读取预取	动态缓存读取预取允许控制器在将数据块从驱动器读取到缓存时将额外的顺序数据块复制到缓存中。这种缓存增加了将来从缓存中填充数据请求的可能性。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。预取到缓存的数据速率和数量是根据主机读取的速率和请求大小自行调整的。随机访问不会导致数据被预取到缓存中。禁用读缓存时，此功能不适用。 对于精简卷，动态缓存读取预取始终被禁用且无法更改。
可用容量区域	可用容量区域是删除卷或在卷创建过程中未使用所有可用容量而产生的可用容量。在具有一个或多个可用容量区域的卷组中创建卷时，卷的容量仅限于该卷组中最大的可用容量区域。例如，如果一个卷组总共有 15 GiB 的可用容量，并且最大的可用容量区域为 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其他卷。
主机	主机是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	仅卷组支持热备盘驱动器。热备盘驱动器不包含任何数据，并在卷组中 RAID 1、RAID 3、RAID 5 或 RAID 6 卷中的驱动器出现故障时充当备用驱动器。热备盘驱动器为您的存储阵列增加了另一个级别的冗余。
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。此卷以 LUN 的形式作为容量呈现给主机。 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相同的 LUN 来访问不同的卷。
媒体扫描	介质扫描提供了一种在从驱动器正常读取或写入驱动器期间发现驱动器介质错误之前检测驱动器介质错误的方法。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。

术语	说明
命名空间	命名空间是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	池是逻辑上分组的一组驱动器。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、卷或卷组容量是指已分配给池或卷组的存储阵列中的容量。此容量用于创建卷并为复制服务操作和存储对象的各种容量需求提供服务。
读取缓存	读缓存是存储已从驱动器读取的数据的缓冲区。读取操作的数据可能已经存在于先前操作的缓存中，因此无需访问驱动器。数据保留在读缓存中，直到刷新为止。
已报告容量	报告容量是报告给主机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是相同的，但对于精简卷则不同。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，报告的容量是报告给主机的容量，而分配的容量是当前分配用于写入数据的驱动器空间量。
区块大小	段是在存储阵列移动到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。段大小等于或小于卷组的容量。池的段大小是固定的，不能更改。
条带化	条带化是在存储阵列上存储数据的方式。条带化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上分发和存储数据。条带化是 RAID 0 的同义词，它将数据分散到 RAID 组中的所有驱动器上而不进行奇偶校验。
卷	卷是应用程序、数据库和文件系统存储数据的容器。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 分配给一个卷的方式。
卷名称	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卷中存储的数据类型。
卷组	卷组是具有共享特征的卷的容器。卷组具有定义的容量和 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	工作负载是支持应用程序的存储对象。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。这些卷特性是根据工作负载支持的应用程序类型进行优化的。例如，如果创建支持 Microsoft SQL Server 应用程序的工作负载，然后为该工作负载创建卷，则会优化基础卷特征以支持 Microsoft SQL Server。

术语	说明
写入缓存	写缓存是存储来自主机尚未写入驱动器的数据的缓冲区。数据将保留在写缓存中，直到写入驱动器。写缓存可以提高 I/O 性能。
使用镜像写入缓存	当写入一个控制器的缓存内存的数据也写入另一个控制器的缓存内存时，将发生镜像写入缓存。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。仅当写缓存已启用且存在两个控制器时，写缓存镜像才可用。使用镜像进行写缓存是创建卷时的默认设置。
不使用电池的写入缓存	没有电池的写缓存设置允许写缓存继续，即使电池丢失、故障、完全放电或未完全充电。通常不建议选择没有电池的写缓存，因为如果断电，数据可能会丢失。通常，控制器会暂时关闭写缓存，直到电池充电或更换故障电池。

特定于精简卷

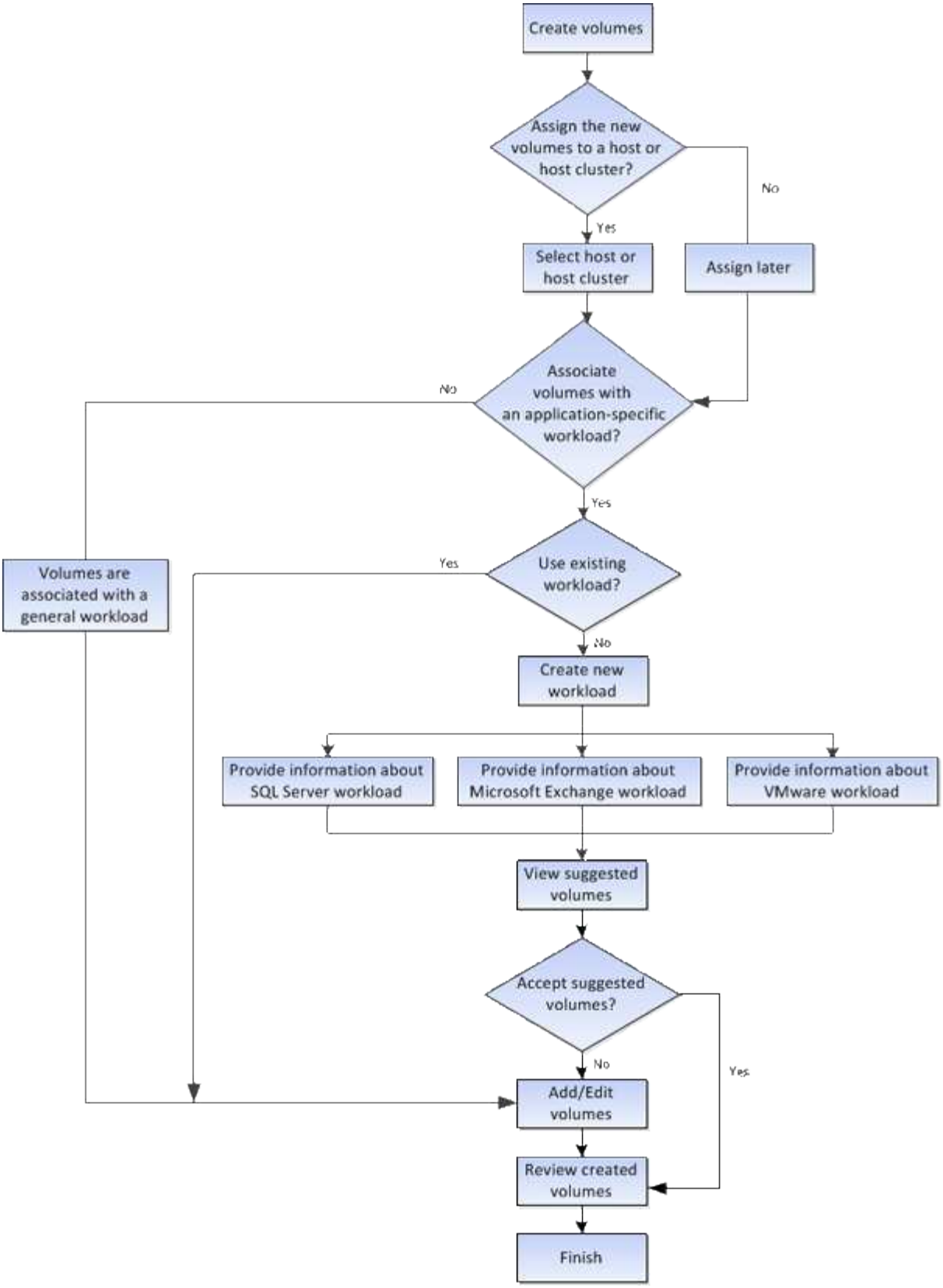
System Manager 不提供创建精简卷的选项。如果要创建精简卷，请使用命令行界面 (CLI)。

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

术语	说明
已分配容量限制	分配容量限制是精简卷分配的物理容量可以增长的上限。
写入容量	写入容量是从为精简卷分配的预留容量中已写入的容量大小。
警告阈值	您可以设置警告阈值警报，以便在精简卷的分配容量达到已满百分比（警告阈值）时发出。

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

在 SANtricity System Manager 中，您可以按照以下步骤创建卷。



了解 **SANtricity** 软件中卷的数据完整性和数据安全性

您可以启用卷以使用 Data Assurance (DA) 功能和 Drive Security 功能。这些功能在池和卷组级别呈现。

数据保障

数据保障 (DA) 实施 T10 Protection Information (PI) 标准，该标准通过检查和纠正沿 I/O 路径传输数据时可能发生的错误来提高数据完整性。数据保障功能的典型使用将检查控制器和驱动器之间的 I/O 路径部分。DA 功能在池和卷组级别呈现。

启用此功能后，存储阵列会将错误检查代码（也称为循环冗余检查或 CRC）附加到卷中的每个数据块。移动数据块后，存储阵列使用这些 CRC 代码来确定在传输过程中是否发生任何错误。潜在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支持 DA 的池或卷组（在池和卷组候选表中的"DA"旁边查找"是"）。

驱动器安全

驱动器安全是一项功能，可防止在从存储阵列中移除时对启用安全功能的驱动器上的数据进行未经授权的访问。这些驱动器可以是全磁盘加密 (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。

Drive Security 在驱动器级别的工作原理

具有安全功能的驱动器（FDE 或 FIPS）在写入期间对数据进行加密，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程。每个驱动器都有自己独特的加密密钥，永远无法从驱动器传输。

Drive Security 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，还可以为这些池或卷组启用驱动器安全。驱动器安全选项使驱动器以及关联的卷组和池安全-已启用。池或卷组可以同时包含具有安全功能和不具有安全功能的驱动器，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

要实现驱动器安全，请执行以下步骤。

1. 为您的存储阵列配备支持安全的驱动器，无论是 FDE 驱动器还是 FIPS 驱动器。（对于需要 FIPS 支持的卷，仅使用 FIPS 驱动器。在卷组或池中混合 FIPS 和 FDE 驱动器将导致所有驱动器被视为 FDE 驱动器。此外，FDE 驱动器不能添加到全 FIPS 卷组或池中或用作备用驱动器。）
2. 创建一个安全密钥，它是控制器和驱动器共享的字符串，用于读/写访问。您可以从控制器的持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。对于外部密钥管理，必须与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：
   - 创建池或卷组（在 Candidates 表中的 **Secure-capable** 列中查找 **Yes**）。
   - 在创建新卷时选择池或卷组（在池和卷组候选项表中的 **Secure-capable** 旁边查找 **Yes**）。

     使用 Drive Security 功能，您可以创建在存储阵列中启用安全的驱动器和控制器之间共享的安全密钥。每当关闭和打开驱动器的电源时，启用安全的驱动器都会变为 Security Locked 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 Cache，以提高只读性能。SSD Cache 由一组固态磁盘 (SSD) 驱动器组成，您可以在存储阵列中将它们逻辑地分组在一起。

卷

简单的卷 I/O 机制用于将数据移动到 SSD Cache 和从 SSD Cache 移动数据。在 SSD 上缓存和存储数据后，在 SSD Cache 上执行该数据的后续读取，从而无需访问 HDD 卷。

SSD Cache 是与控制器的动态随机存取内存 (DRAM) 中的主缓存一起使用的辅助缓存。

- 在主缓存中，数据在主机读取后存储在 DRAM 中。
- 在 SSD 缓存中，数据从卷复制并存储在两个内部 RAID 卷上（每个控制器一个），这些卷在创建 SSD 缓存时自动创建。

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，这两个卷确实计算在存储阵列中允许的卷总数中。

分配给使用控制器 SSD Cache 的任何卷都不符合自动负载平衡传输的条件。

驱动器安全功能

要在也使用驱动器安全（已启用安全）的卷上使用 SSD Cache，卷的驱动器安全功能和 SSD Cache 必须匹配。如果不匹配，则卷将不会启用安全。

可以对 **SANtricity System Manager** 中的卷执行的操作

您可以在卷上执行许多不同的操作：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媒体扫描设置。

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。

  您可以通过选择菜单：Storage[Pools and Volume Groups > Add Capacity] 向卷添加容量。

- 将未分配的容量（以未使用驱动器的形式）添加到卷的池或卷组。池或卷组中不存在可用容量时使用此选项。

  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。必须首先增加池或卷组的大小或删除未使用的卷。

扩展卷容量后，您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您正在使用的文件系统。有关详细信息，请参阅您的主机操作系统文档。

删除

通常，如果卷是使用错误的参数或容量创建的，不再满足存储配置需求，或者是备份或应用程序测试不再需要的快照映像，则会删除卷。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。删除卷还将删除所有关联的快照映像、计划和快照卷，并删除所有镜像

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来复制卷：Storage[Volumes > Copy Services > Copy volume]。

初始化

初始化卷会擦除卷中的所有数据。卷在首次创建时会自动初始化。但是，Recovery Guru 可能会建议您手动初始化卷以从某些故障状态中恢复。初始化卷时，该卷将保留其 WWN、主机分配、分配的容量和保留的容量设置。它还保留相同的 Data Assurance (DA) 设置和安全设置。

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

重新分配

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处移动卷。

大多数主机多路径驱动程序会尝试访问其首选控制器所有者路径上的每个卷。但是，如果此首选路径不可用，主机上的多路径驱动程序会故障转移到备用路径。此故障转移可能会导致卷所有权更改为备用控制器。解决导致故障转移的条件后，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，可能需要手动重新分配卷。

您可以通过选择菜单：Storage[Volumes > More > 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下：Storage[Volumes > View/Edit Settings > Advanced tab]。

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

镜像和卷所有权

如果镜像对的主卷由控制器 A 所有，则辅助卷也将由远程存储阵列的控制器 A 所有。更改主卷的所有者将自动更改辅助卷的所有者，以确保两个卷由同一个控制器所有。主端的当前所有权变更会自动传播到辅助端的相应当前所有权变更。

如果镜像一致性组包含本地辅助卷，并且控制器所有权发生更改，则辅助卷会在第一次写入操作时自动传输回其原始控制器所有者。您无法使用 **Change ownership** 选项更改辅助卷的控制器所有权。

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，当复制卷操作启动时，两个卷没有相同的首选控制器。因此，目标卷的所有权将自动转移到源卷的首选控制器。当卷副本完成或停止时，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，则还会更改目标卷的所有权。在某些操作系统环境中，可能需要在使用 I/O 路径之前重新配置多路径主机驱动程序。（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，请参阅您的驱动程序文档。）

更改缓存设置

缓存内存是控制器上临时易失性存储 (RAM) 的区域，其访问时间快于驱动器介质。如果使用缓存内存，由于以下原因，您可以提高整体 I/O 性能：

- 从主机请求读取的数据可能已经存在于先前操作的缓存中，因此无需驱动器访问。
- 写入数据最初会写入缓存，从而使应用程序可以继续，而不是等待数据写入驱动器。

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

- 读写缓存 — 读缓存是存储已从驱动器读取的数据的缓冲区。读取操作的数据可能已经存在于先前操作的缓存中，因此无需访问驱动器。数据保留在读缓存中，直到刷新为止。

  写缓存是存储来自主机尚未写入驱动器的数据的缓冲区。数据将保留在写缓存中，直到写入驱动器。写缓存可以提高 I/O 性能。

- 带镜像的写缓存 — 当写入一个控制器的缓存内存的数据也写入另一个控制器的缓存内存时，将发生带镜像的写缓存。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。仅当写缓存已启用且存在两个控制器时，写缓存镜像才可用。使用镜像进行写缓存是创建卷时的默认设置。
- 不带电池的写缓存 — 不带电池的写缓存设置允许写缓存继续，即使电池丢失、故障、完全放电或未完全充电。通常不建议选择没有电池的写缓存，因为如果断电，数据可能会丢失。通常，控制器会暂时关闭写缓存，直到电池充电或更换故障电池。

  此设置仅在启用写缓存时可用。此设置不适用于精简卷。

- 动态读缓存预取 — 动态缓存读取预取允许控制器在将数据块从驱动器读取到缓存时将额外的顺序数据块复制到缓存中。这种缓存增加了将来从缓存中填充数据请求的可能性。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。预取到缓存的数据速率和数量是根据主机读取的速率和请求大小自行调整的。随机访问不会导致数据被预取到缓存中。禁用读缓存时，此功能不适用。

  对于精简卷，动态缓存读取预取始终被禁用且无法更改。

更改媒体扫描设置

介质扫描检测并修复应用程序不经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，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冗余信息和池或卷组中其他驱动器的数据重建的。

介质扫描根据要扫描的容量和扫描持续时间以恒定速率连续运行。后台扫描可能会被更高优先级的后台任务（例如重建）暂时挂起，但将以相同的恒定速率恢复。

您可以通过选择菜单：Storage[Volumes > More > Change media scan settings] 来启用和设置介质扫描运行的持续时间。

仅当为存储阵列和该卷启用了媒体扫描选项时，才会扫描卷。如果该卷也启用了冗余检查，则将检查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，默认情况下会启用带冗余检查的媒体扫描。

如果在扫描过程中遇到不可恢复的介质错误，则将使用冗余信息（如果可用）修复数据。例如，冗余信息在最佳 RAID 5 卷中可用，或者在最佳 RAID 6 卷中可用，或者仅有一个驱动器发生故障。如果无法使用冗余信息修复不可恢复的错误，数据块将被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，则将其报告给事件日志。

如何在 **SANtricity System Manager** 中为卷分配容量

存储阵列中的驱动器为数据提供物理存储容量。在开始存储数据之前，必须将分配的容量配置为称为池或卷组的逻辑组件。您可以使用这些存储对象在存储阵列上配置、存储、维护和保留数据。

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，可以同时创建池或卷组和卷。
- 从可用容量创建卷时，您是在现有池或卷组上创建一个附加卷。

扩展卷容量后，您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您正在使用的文件系统。有关详细信息，请参阅您的主机操作系统文档。

厚卷和薄卷的容量类型

您可以创建厚卷或精简卷。对于厚卷，报告容量和分配容量相同，但对于精简卷则不同。

- 对于厚卷，报告的卷容量等于分配的物理存储容量。必须存在整个物理存储容量。物理分配的空间等于向主机报告的空间。

  您通常会将厚卷的报告容量设置为您认为该卷将增长到的最大容量。厚卷为您的应用程序提供高性能和可预测的性能，主要是因为所有用户容量都是在创建时保留和分配的。

- 对于精简卷，报告的容量是报告给主机的容量，而分配的容量是当前分配用于写入数据的驱动器空间量。

  报告的容量可能大于存储阵列上分配的容量。可以调整瘦卷大小以适应增长，而无需考虑当前可用的资产。

> 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。

在增加厚卷的报告容量时，请记住以下准则：

- 最多可以指定三个小数位（例如 65.375 GiB）。
- 容量需要小于（或等于）卷组中的最大可用容量。

  创建卷时，会为动态段大小 (DSS) 迁移预分配一些额外容量。DSS 迁移是软件的一项功能，允许您更改卷的段大小。

- 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确定）。实际上，某些主机操作系统支持高达 128 TiB 的卷。请参见主机操作系统文档了解其他详细信息。

您可以创建具有较大报告容量和相对较小分配容量的精简卷，这有利于提高存储利用率和效率。精简卷可以帮助简化存储管理，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，从而实现更好的存储利用率。

除了报告的容量和分配的容量外，精简卷还包含已写入容量。已写入容量是从为精简卷分配的保留容量中已写入的容量量。

下表列出了精简卷的容量限制。

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

对于精简卷，如果已达到 256 TiB 的最大报告容量，则无法增加其容量。确保将精简卷的预留容量设置为大于最大报告容量的大小。

系统会根据分配的容量限制自动扩展分配的容量。分配的容量限制允许您将精简卷的自动增长限制在报告的容量以下。当写入数据量接近分配容量时，可以更改分配容量限制。

要更改分配的容量限制，请选择菜单：Storage[Volumes > Thin Volume Monitoring tab > Change Limit]。

由于 System Manager 在创建精简卷时未分配全部容量，因此池中可能存在可用容量不足的情况。空间不足可能会阻止对池的写入，这不仅适用于精简卷，也适用于需要池容量的其他操作（例如快照映像或快照卷）。但是，您仍然可以从池中执行读取操作。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容量不足情况。

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：Storage[Volumes > Thin Volume Monitoring] 选项卡，以监控精简卷在达到分配容量最大限制之前的增长量。

您可以使用 Thin Monitoring 视图执行以下操作：

- 定义限制精简卷可以自动扩展到的已分配容量的限制。
- 设置当精简卷接近最大分配容量限制时将警报（超过警告阈值）发送到 Home 页面上的 Notifications 区域的百分比点。

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)。

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

厚卷始终是完全配置的，这意味着在创建卷时将分配所有容量。精简卷始终是精简配置的，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)。

卷类型	说明
厚卷	• 厚卷是从池或卷组创建的。 • 对于厚卷，会预先提供大量存储空间，以满足未来的存储需求。 • 密集卷是在创建卷时在物理存储上预分配卷的整个大小而创建的。这种预分配意味着创建 100 GiB 的卷实际上会消耗驱动器上 100 GiB 的已分配容量。但是，空间可能仍未使用，导致存储容量利用不足。 • 创建厚卷时，请确保不要过度分配单个卷的容量。过度分配单个卷的容量会迅速消耗系统中的所有物理存储。 • 请记住，拷贝服务（快照映像、快照卷、卷拷贝和异步镜像）也需要存储容量，因此不要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，您将收到空闲容量警报阈值警告。
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。 • EF600/EF600C 或 EF300/EF300C 存储系统上没有可用的精简卷。 • 您必须使用 CLI 创建精简卷。 • 与厚卷不同，精简卷所需的空间不会在创建过程中分配，而是在以后按需提供。 • 精简卷可让您过度分配其大小。也就是说，您可以分配大于卷大小的 LUN 大小。然后，您可以根据需要扩展卷（如果需要，在此过程中添加驱动器），而无需扩展 LUN 的大小，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调整回收空间的用途，以满足同一存储阵列中其他精简配置卷的分配请求，从而更好地报告磁盘空间消耗情况并更有效地利用资源。

精简卷限制

精简卷支持与厚卷相同的所有操作，但以下情况除外：

- 您无法更改精简卷的段大小。
- 无法对精简卷启用预读冗余检查。
- 在 Copy Volume 操作中，不能使用精简卷作为目标卷。
- 只能在异步镜像对的主端更改精简卷的分配容量限制和警告阈值。主端对这些参数的任何更改都会自动传播到辅助端。

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. 选择菜单：Storage[Volumes]。
2. 选择菜单：创建 [Workload]。

   此时将显示"创建应用程序工作负载"对话框。

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 **Create**。

完成后

您已准备好将存储容量添加到您创建的工作负载。使用 **Create Volume** 选项为应用程序创建一个或多个卷，并为每个卷分配特定数量的容量。

在 **SANtricity System Manager** 中创建卷

创建卷是为了向特定于应用程序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群集可见。此外，卷创建顺序还提供了为要创建的每个卷分配特定容量的选项。

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个邮箱、平均邮箱容量要求以及所需的数据库副本数。System Manager 使用此信息为您创建最佳卷配置，可以根据需要对其进行编辑。

创建卷的过程是一个多步骤过程。

步骤 **1**：选择卷的主机

创建卷是为了向特定于应用程序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群集可见。此外，卷创建顺序还提供了为要创建的每个卷分配特定容量的选项。

开始之前

- Hosts 图块下方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 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，则关联的主机无法访问启用了 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量进行特定限制。在创建供特定主机使用的卷时，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。
- 主机或主机群集不能使用相同的逻辑单元号 (LUN) 两次访问卷。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，以便离线初始化新创建的卷。

> 如果尝试将卷分配给与主机群集中已建立的主机分配冲突的主机群集，则将卷分配给主机将失败。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择菜单：Create[Volume]。

   此时将显示"创建卷"对话框。

3. 从下拉列表中，选择要向其分配卷的特定主机或主机群集，或选择稍后分配主机或主机群集。
4. 若要继续选定主机或主机群集的卷创建顺序，请单击 **Next**，然后转到 步骤 2：为卷选择工作负载。

   此时将显示"选择工作负载"对话框。

步骤 2：为卷选择工作负载

选择工作负载以自定义特定应用程序（如 Microsoft SQL Server、Microsoft Exchange、视频监控应用程序或 VMware）的存储阵列配置。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

此任务描述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/编辑卷"对话框查看推荐的卷配置，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/编辑卷"对话框手动指定卷配置。

步骤

1. 执行以下操作之一：
   - 选择 **Create volumes for an existing workload** 选项，为现有工作负载创建卷。
   - 选择 **Create a new workload** 选项，为受支持的应用程序或"其他"应用程序定义新工作负载。
     - 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，请从"其他"条目中选择一项。

     - 输入要创建的工作负载的名称。
2. 单击 **Next**。

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：添加或编辑卷。

步骤 3：添加或编辑卷

System Manager 可能会根据您选择的应用程序或工作负载建议卷配置。此卷配置根据工作负载支持的应用程序类型进行优化。您可以接受推荐的卷配置，也可以根据需要进行编辑。如果选择了其中一个"其他"应用程序，则必须手动指定要创建的卷和特征。

开始之前

- 池或卷组必须具有足够的可用容量。
- 卷组中允许的最大卷数为 256 个。
- 池中允许的最大卷数取决于存储系统型号：
  - 2,048 卷（EF600、EF600C 和 E5700 系列）
  - 1,024 卷（EF300 和 EF300C）
  - 512 卷（E4000 和 E2800 系列）
- 要创建启用 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 DA 的卷，请选择支持 DA 的池或卷组（在池和卷组候选表中的"DA"旁边查找 **Yes**）。
  >
  > DA 功能在 System Manager 中的池和卷组级别呈现。DA 保护会检查并更正数据通过控制器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，则关联的主机无法访问启用 DA 的卷上的数据。

- 要创建启用安全的卷，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

  > 如果要创建启用安全的卷，请选择支持安全的池或卷组（在池和卷组候选项表中的"支持安全"旁边查找是）。
  >
  > 驱动器安全功能在 System Manager 中的池和卷组级别呈现。具有安全功能的驱动器可防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。启用安全的驱动器在写入期间对数据进行加密，并在读取期间使用唯一的_加密密钥_对数据进行解密。
  >
  > 池或卷组可以同时包含具有安全功能和不具有安全功能的驱动器，但所有驱动器都必须具有安全功能才能使用其加密功能。

- 要创建资源调配的卷，所有驱动器都必须是具有 Deallocated or Unwritten Logical Block Error (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/编辑卷对话框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。

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

步骤

1. 根据您是选择了"其他"还是特定于应用程序的工作负载，选择以下操作之一：
   - 其他 — 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	说明
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，也可以提供一个更具描述性的名称来指示卷中存储的数据类型。
已报告容量	定义新卷的容量和要使用的容量单位（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。 请记住，复制服务（快照映像、快照卷、卷副本和远程镜像）也需要存储容量；因此，不要将所有容量分配给标准卷。 池中的容量以 4-GiB 或 8-GiB 的增量分配，具体取决于您的驱动器类型。任何不是 4-GiB 或 8-GiB 的倍数的容量都已分配，但不可用。为确保整个容量可用，请以 4-GiB 或 8-GiB 增量指定容量。如果存在不可用的容量，则重新获得它的唯一方法是增加卷的容量。
卷块大小（仅限 EF300 和 EF600）	显示可以为卷创建的块大小： • 512 — 512 字节 • 4K — 4,096 字节
区块大小	显示区段大小设置，该设置仅对卷组中的卷显示。您可以更改区段大小以优化性能。 允许的段大小转换 — System Manager 确定允许的段大小转换。从当前段大小进行不适当转换的段大小在下拉列表中不可用。允许的转换通常是当前段大小的两倍或一半。例如，如果当前卷段大小为 32 KiB，则允许 16 KiB 或 64 KiB 的新卷段大小。 启用 **SSD Cache** 的卷 — 您可以为启用 SSD Cache 的卷指定 4-KiB 段大小。确保仅为处理小块 I/O 操作的启用 SSD Cache 的卷选择 4-KiB 段大小（例如，16 KiB I/O 块大小或更小）。如果为处理大块顺序操作的启用 SSD Cache 的卷选择 4 KiB 作为段大小，性能可能会受到影响。 更改段大小的时间量 — 更改卷的段大小的时间量取决于以下变量： • 来自主机的 I/O 负载 • 卷的修改优先级 • 卷组中的驱动器数 • 驱动器通道数 • 存储阵列控制器的处理能力 当您更改卷的段大小时，I/O 性能会受到影响，但您的数据仍然可用。

字段	说明
支持安全功能	只有当池或卷组中的驱动器具有安全功能时，是 才会显示在 "Secure-capable" 旁边。 驱动器安全性可防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。仅当启用了驱动器安全功能并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具有安全功能和不具有安全功能的驱动器，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	是 仅在池或卷组中的驱动器支持数据保障 (DA) 时显示在 "DA" 旁边。 DA 提高了整个存储系统的数据完整性。DA 使存储阵列能够检查数据通过控制器传输到驱动器时可能发生的错误。对新卷使用 DA 可确保检测到任何错误。
已配置资源（仅限 EF300 和 EF600）	只有当驱动器支持此选项时，*是*才会显示在"资源调配"旁边。资源调配是 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 下一步 接受选定工作负载的系统推荐卷和特性，或单击 编辑卷 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	说明
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，也可以提供一个更具描述性的名称来指示卷中存储的数据类型。
已报告容量	定义新卷的容量和要使用的容量单位（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。 请记住，复制服务（快照映像、快照卷、卷副本和远程镜像）也需要存储容量；因此，不要将所有容量分配给标准卷。 池中的容量以 4-GiB 或 8-GiB 的增量分配，具体取决于您的驱动器类型。任何不是 4-GiB 或 8-GiB 的倍数的容量都已分配，但不可用。为确保整个容量可用，请以 4-GiB 或 8-GiB 增量指定容量。如果存在不可用的容量，则重新获得它的唯一方法是增加卷的容量。
卷类型	卷类型指明为特定于应用程序的工作负载创建的卷的类型。
卷块大小（仅限 EF300 和 EF600）	显示可以为卷创建的块大小： • 512 — 512 字节 • 4K — 4,096 字节

字段	说明
区块大小	显示区段大小设置，该设置仅对卷组中的卷显示。您可以更改区段大小以优化性能。 允许的段大小转换 — System Manager 确定允许的段大小转换。从当前段大小进行不适当转换的段大小在下拉列表中不可用。允许的转换通常是当前段大小的两倍或一半。例如，如果当前卷段大小为 32 KiB，则允许 16 KiB 或 64 KiB 的新卷段大小。 启用 **SSD Cache** 的卷 — 您可以为启用 SSD Cache 的卷指定 4-KiB 段大小。确保仅为处理小块 I/O 操作的启用 SSD Cache 的卷选择 4-KiB 段大小（例如，16 KiB I/O 块大小或更小）。如果为处理大块顺序操作的启用 SSD Cache 的卷选择 4 KiB 作为段大小，性能可能会受到影响。 更改段大小的时间量 — 更改卷的段大小的时间量取决于以下变量： • 来自主机的 I/O 负载 • 卷的修改优先级 • 卷组中的驱动器数 • 驱动器通道数 • 存储阵列控制器的处理能力 当您更改卷的段大小时，I/O 性能会受到影响，但您的数据仍然可用。
支持安全功能	只有当池或卷组中的驱动器具有安全功能时，是才会显示在 "Secure-capable" 旁边。 驱动器安全性可防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。此选项仅在已启用驱动器安全功能并为存储阵列设置安全密钥时可用。 池或卷组可以同时包含具有安全功能和不具有安全功能的驱动器，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	是 仅在池或卷组中的驱动器支持数据保障 (DA) 时显示在 "DA" 旁边。 DA 提高了整个存储系统的数据完整性。DA 使存储阵列能够检查数据通过控制器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。

字段	说明
已配置资源（仅限 EF300 和 EF600）	只有当驱动器支持此选项时，"资源调配"旁边才会显示 是。资源调配是 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. 要继续选定应用程序的卷创建顺序，请单击 **Next**，然后转到 步骤 4：检查卷配置。

步骤 **4**：检查卷配置

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 在选定的池和卷组中创建新卷，然后在 All Volumes 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此卷。
- 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`以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 获得。此可下载版本的 SMcli 可在 E4000、EF600、EF600C、EF300、EF300C、E5700、EF570、E2800 和 EF280 控制器上使用。要在 SANtricity System Manager 中下载 SMcli，请选择*设置* > 系统*和*附加组件 > 命令行界面。

向 **SANtricity System Manager** 中的工作负载添加卷

您可以向现有或新工作负载添加一个或多个当前未与工作负载关联的卷。

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），则不与工作负载关联。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择 **Applications & Workloads** 选项卡。

   此时将显示 Applications & Workloads 视图。

3. 选择 **Add to Workload**。

   此时将显示"选择工作负载"对话框。

4. 请执行以下操作之一：

- 向现有工作负载添加卷 — 选择此选项可向现有工作负载添加卷。

  使用下拉列表选择工作负载。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。

- 向新工作负载添加卷 — 选择此选项可为应用程序类型定义新工作负载，并向新工作负载添加卷。

5. 选择 **Next** 继续添加到工作负载序列。

   此时将显示"选择卷"对话框。

6. 选择要添加到工作负载的卷。
7. 查看要添加到所选工作负载的卷。
8. 对工作负载配置感到满意后，单击 完成。

管理卷

在 **SANtricity System Manager** 中增加卷的容量

您可以使用池或卷组中的可用容量来增加卷的报告容量（报告给主机的容量）。

开始之前

- 卷的关联池或卷组中有足够的可用容量。
- 此卷为 Optimal，未处于任何修改状态。
- 对于薄卷，尚未达到 256 TiB 的最大报告容量。
- 卷中没有正在使用的热备盘驱动器。（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，您将来可能对此池或卷组中的其他卷有任何容量要求。确保您有足够的可用容量来创建快照映像、快照卷或远程镜像。

> 仅在某些操作系统上支持增加卷的容量。如果在不受支持的主机操作系统上增加卷容量，则扩展的容量将无法使用，并且无法恢复原始卷容量。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择要增加容量的卷，然后选择 增加容量。

   此时将显示确认增加容量对话框。

3. 选择 是 以继续。

   此时将显示"增加报告容量"对话框。

   此对话框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*框以向当前可用报告容量添加容量。您可以更改以 mebibytes (MiB)、gibibytes (GiB) 或 tebibytes (TiB) 显示的容量值。
5. 单击 **Increase**。

结果

- System Manager 根据您的选择增加卷的容量。
- 选择菜单：Home[View Operations in Progress] 以查看当前为所选卷运行的增加容量操作的进度。此操作可能很长，并可能影响系统性能。

完成后

扩展卷容量后，您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您正在使用的文件系统。有关详细信息，请参阅您的主机操作系统文档。

在 **SANtricity System Manager** 中初始化卷

卷在首次创建时会自动初始化。但是，Recovery Guru 可能会建议您手动初始化卷以从某些故障条件下恢复。仅在技术支持指导下使用此选项。您可以选择一个或多个要初始化的卷。

开始之前

- 所有 I/O 操作已停止。
- 必须卸载要初始化的卷上的任何设备或文件系统。
- 卷处于 Optimal 状态，卷上没有正在进行的修改操作。

> 操作开始后无法取消。所有卷数据都被擦除。请勿尝试此操作，除非 Recovery Guru 建议您这样做。在开始此过程之前，请联系技术支持。

关于此任务

初始化卷时，卷将保留其 WWN、主机分配、分配的容量和保留的容量设置。它还保留相同的数据保障 (DA) 设置和安全设置。

以下类型的卷_无法_初始化：

- 快照卷的基本卷
- 镜像关系中的主卷
- 镜像关系中的辅助卷
- 卷副本中的源卷
- 卷副本中的目标卷
- 正在执行初始化的卷

本主题仅适用于从池或卷组创建的标准卷。

步骤

1. 选择菜单：Storage[Volumes]。

2. 选择任何卷，然后选择菜单：More[Initialize volumes]。

   此时将显示"初始化卷"对话框。此对话框中将显示存储阵列上的所有卷。

3. 选择要初始化的一个或多个卷，并确认要执行此操作。

结果

System Manager 执行以下操作：

- 擦除已初始化卷的所有数据。
- 清除块索引，这会导致未写入的块被读取，就好像它们是零填充的（卷看起来完全为空）。

选择菜单：Home[View Operations in Progress] 以查看当前为所选卷运行的初始化操作的进度。此操作可能很长，并可能影响系统性能。

在 **SANtricity System Manager** 中重新分布卷

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

开始之前

- 要重新分发的卷未使用，否则将发生 I/O 错误。
- 在使用要重新分发的卷的所有主机上安装多路径驱动程序，否则将发生 I/O 错误。

  如果要在主机上没有多路径驱动程序的情况下重新分配卷，则必须停止_重新分配操作进行期间_对卷的所有 I/O 活动，以防止应用程序错误。

关于此任务

大多数主机多路径驱动程序会尝试访问其首选控制器所有者路径上的每个卷。但是，如果此首选路径不可用，主机上的多路径驱动程序会故障转移到备用路径。此故障转移可能会导致卷所有权更改为备用控制器。解决导致故障转移的条件后，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，可能需要手动重新分配卷。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择菜单：More[重新分配卷]。

   此时将显示"重新分配卷"对话框。此对话框中将显示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。

3. 选择要重新分发的一个或多个卷，并确认要执行此操作。

结果

System Manager 将选定卷移动到其首选控制器所有者，或者您可能会看到"重新分配卷不必要"对话框。

更改 **SANtricity System Manager** 中卷的控制器所有权

您可以更改卷的首选控制器所有权，以便主机应用程序的 I/O 通过新路径进行定向。

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该卷的所有主机应用程序。此操作可防止 I/O 路径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. 选择菜单：Storage[Volumes]。
2. 选择任何卷，然后选择菜单：更多[更改所有权]。

   此时将显示更改卷所有权对话框。此对话框中将显示存储阵列上的所有卷。

3. 使用 **Preferred Owner** 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 更改卷的控制器所有权。卷的 I/O 现在通过此 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 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，如果卷是使用错误的参数或容量创建的，不再满足存储配置需求，或者是备份或应用程序测试不再需要的快照映像，则会删除卷。

删除卷会增加池或卷组中的可用容量。您可以选择要删除的一个或多个卷。

开始之前

在计划删除的卷上，确保以下内容：

- 所有数据都已备份。
- 所有输入/输出 (I/O) 均已停止。
- 任何设备和文件系统均已卸载。

关于此任务

无法删除具有以下条件之一的卷：

- 此卷正在初始化。
- 正在重建此卷。
- 此卷是包含正在执行回写操作的驱动器的卷组的一部分。
- 卷正在进行修改操作，例如更改段大小，除非卷现在处于 Failed 状态。
- 此卷包含任何类型的永久预留。
- 此卷是 Copy Volume 中状态为"待定"、"正在进行"或"失败"的源卷或目标卷。

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，正在后台执行删除，释放的空间可能无法立即使用。

步骤

1. 选择菜单：Storage[Volumes]。
2. 单击 **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，并确认要执行此操作。
4. 单击 **Delete**。

结果

System Manager 执行以下操作：

- 删除所有关联的快照映像、计划和快照卷。
- 删除所有镜像关系。
- 增加池或卷组中的可用容量。

更改 **SANtricity System Manager** 中精简卷的已分配容量限制

对于能够按需分配空间的精简卷，您可以更改限制分配容量的限制，精简卷可以自动扩展到该容量。

当精简卷接近分配的容量限制时，您还可以更改将警报（超过警告阈值）发送到 Home 页面上 Notifications 区域的百分比点。您可以选择启用或禁用此警报通知。

此功能在 EF600/EF600C 或 EF300/EF300C 存储系统中不可用。

系统会根据分配的容量限制自动扩展分配的容量。分配的容量限制允许您将精简卷的自动增长限制在报告的容量以下。当写入数据量接近分配容量时，可以更改分配容量限制。

更改精简卷的分配容量限制和警告阈值时，必须考虑卷的用户数据和复制服务数据要消耗的空间。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择 **Thin Volume Monitoring** 选项卡。

   此时将显示精简卷监控视图。

3. 选择要更改的精简卷，然后选择 **Change Limit**。

   此时将显示"更改限制"对话框。此对话框中将显示所选精简卷的已分配容量限制和警告阈值设置。

4. 根据需要更改分配的容量限制和警告阈值。

字段详细信息

设置	说明
将分配的容量限制更改为…	写入失败的阈值，防止精简卷消耗额外资源。此阈值是卷的报告容量大小的百分比。
在…时提醒我（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。警报将发送到主页上的"通知"区域。此阈值是卷的报告容量大小的百分比。 清除复选框以禁用警告阈值警报通知。

5. 单击 **Save**。

管理设置

更改 **SANtricity System Manager** 中卷的设置

您可以更改卷的设置，例如其名称、主机分配、段大小、修改优先级、缓存等。

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. 选择菜单：Storage[Volumes]。
2. 选择要更改的卷，然后选择 **View/Edit Settings**。

   此时将显示"卷设置"对话框。此对话框中将显示所选卷的配置设置。

3. 选择 **Basic** 选项卡以更改卷的名称和主机分配。

字段详细信息

设置	说明
名称	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。
容量	显示选定卷的已报告和已分配容量。 对于厚卷，报告的容量和分配的容量是相同的，但对于精简卷则不同。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，报告的容量是报告给主机的容量，而分配的容量是当前分配用于写入数据的驱动器空间量。
池 / 卷组	显示池或卷组的名称和 RAID 级别。指示池或卷组是否具有安全功能并启用了安全功能。
主机	显示卷分配。将卷分配给主机或主机群集，以便可以访问该卷进行 I/O 操作。此分配授予主机或主机群集对特定卷或存储阵列中的多个卷的访问权限。 • 分配给 — 标识可以访问所选卷的主机或主机群集。 • **LUN** — 逻辑单元编号 (LUN) 是分配给主机用于访问卷的地址空间的编号。卷以 LUN 的形式作为容量呈现给主机。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相同的 LUN 来访问不同的卷。 对于 NVMe 接口，此列显示命名空间 ID。命名空间是为块访问而格式化的 NVM 存储。它类似于 SCSI 中的逻辑单元，与存储阵列中的卷相关。命名空间 ID 是 NVMe 控制器的命名空间唯一标识符，可以设置为 1 到 255 之间的值。它类似于 SCSI 中的逻辑单元号 (LUN)。
标识符	显示选定卷的标识符。 • 全球标识符 **(WWID)** — 卷的唯一十六进制标识符。 • 扩展唯一标识符 **(EUI)** — 卷的 EUI-64 标识符。 • 子系统标识符 **(SSID)** — 卷的存储阵列子系统标识符。

4. 选择 **Advanced** 选项卡以更改池或卷组中卷的其他配置设置。

字段详细信息

设置	说明
应用程序和工作负载信息	在创建卷期间，您可以创建特定于应用程序的工作负载或其他工作负载。如果适用，将显示选定卷的工作负载名称、应用程序类型和卷类型。 您可以根据需要更改工作负荷名称。
服务质量设置	永久禁用 **Data Assurance** — 仅当卷启用了 Data Assurance (DA) 时才会显示此设置。DA 检查并更正数据通过控制器传输到驱动器时可能发生的错误。使用此选项可永久禁用所选卷上的 DA。禁用时，无法在此卷上重新启用 DA。 启用预读冗余检查 — 仅当卷为厚卷时才会显示此设置。预读冗余检查确定每次执行读取时卷上的数据是否一致。如果控制器固件确定数据不一致，启用此功能的卷将返回读取错误。
控制器所有权	定义被指定为卷的拥有者或主控制器的控制器。 控制器所有权非常重要，应仔细规划。控制器应尽可能紧密地平衡总 I/O。
区段大小调整	显示区段大小设置，该设置仅对卷组中的卷显示。您可以更改区段大小以优化性能。 允许的段大小转换 — System Manager 确定允许的段大小转换。从当前段大小进行不适当转换的段大小在下拉列表中不可用。允许的转换通常是当前段大小的两倍或一半。例如，如果当前卷段大小为 32 KiB，则允许 16 KiB 或 64 KiB 的新卷段大小。 启用 **SSD Cache** 的卷 — 您可以为启用 SSD Cache 的卷指定 4-KiB 段大小。确保仅为处理小块 I/O 操作的启用 SSD Cache 的卷选择 4-KiB 段大小（例如，16 KiB I/O 块大小或更小）。如果为处理大块顺序操作的启用 SSD Cache 的卷选择 4 KiB 作为段大小，性能可能会受到影响。 更改段大小的时间量 — 更改卷的段大小的时间量取决于以下变量： • 来自主机的 I/O 负载 • 卷的修改优先级 • 卷组中的驱动器数 • 驱动器通道数 • 存储阵列控制器的处理能力 当您更改卷的段大小时，I/O 性能会受到影响，但您的数据仍然可用。

设置	说明
修改优先级	显示修改优先级的设置，该设置仅对卷组中的卷显示。 修改优先级定义相对于系统性能为卷修改操作分配多少处理时间。您可以提高卷修改优先级，尽管这可能会影响系统性能。 移动滑块栏以选择优先级。 修改优先级比率 — 最低优先级比率有利于系统性能，但修改操作需要更长时间。最高优先级比率有利于修改操作，但系统性能可能会受到影响。
缓存	显示缓存设置，您可以更改该设置以影响卷的整体 I/O 性能。
SSD 缓存	显示 SSD Cache 设置，您可以在兼容卷上启用该设置，以提高只读性能。如果卷共享相同的驱动器安全和 Data Assurance 功能，则它们是兼容的。 **SSD Cache** 功能使用单个或多个固态硬盘 **(SSD)** 来实现读缓存。由于 SSD 的读取时间更快，因此提高了应用程序性能。由于读缓存在存储阵列中，因此缓存在使用存储阵列的所有应用程序之间共享。只需选择要缓存的卷，即可实现自动和动态缓存。

5. 单击 **Save**。

   System Manager 根据您的选择更改卷的设置。

完成后

选择菜单：Home[View Operations in Progress] 以查看当前为所选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。当当前名称不再有意义或不再适用时，更改工作负载的名称。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择 **Applications & Workloads** 选项卡。

   此时将显示 Applications & Workloads 视图。

3. 选择要更改的工作负载，然后选择 **View/Edit Settings**。

   此时将显示"Applications & Workloads 设置"对话框。

4. *可选：*更改用户提供的工作负载名称。
5. 单击 **Save**。

更改 **SANtricity System Manager** 中卷的缓存设置

您可以更改读缓存和写缓存设置，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。此图标指示控制器已暂时暂停缓存操作。

  当新电池正在充电、控制器已被移除或控制器检测到缓存大小不匹配时，可能会发生此操作。条件清除后，对话框中选择的缓存属性将变为活动状态。如果所选缓存属性未处于活动状态，请联系技术支持。

- 您可以更改存储阵列上单个卷或多个卷的缓存设置。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. 选择菜单：Storage[Volumes]。
2. 选择任何卷，然后选择菜单：更多[更改缓存设置]。

   此时将显示"更改缓存设置"对话框。此对话框中将显示存储阵列上的所有卷。

3. 选择 **Basic** 选项卡以更改读缓存和写缓存的设置。

   字段详细信息

缓存设置	说明
读取缓存	读缓存是存储已从驱动器读取的数据的缓冲区。读取操作的数据可能已经存在于先前操作的缓存中，因此无需访问驱动器。数据保留在读缓存中，直到刷新为止。
写缓存	写缓存是存储来自主机尚未写入驱动器的数据的缓冲区。数据将保留在写缓存中，直到写入驱动器。写缓存可以提高 I/O 性能。 禁用卷的 **Write caching** 后，缓存会自动刷新。

4. 选择 **Advanced** 选项卡以更改厚卷的高级设置。高级缓存设置仅适用于厚卷。

字段详细信息

缓存设置	说明
动态读缓存预取	动态缓存读取预取允许控制器在将数据块从驱动器读取到缓存时将额外的顺序数据块复制到缓存中。这种缓存增加了将来从缓存中填充数据请求的可能性。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。预取到缓存的数据速率和数量是根据主机读取的速率和请求大小自行调整的。随机访问不会导致数据被预取到缓存中。禁用读缓存时，此功能不适用。 对于精简卷，动态缓存读取预取始终被禁用且无法更改。
不使用电池的写缓存	没有电池的写缓存设置允许写缓存继续，即使电池丢失、故障、完全放电或未完全充电。通常不建议选择没有电池的写缓存，因为如果断电，数据可能会丢失。通常，控制器会暂时关闭写缓存，直到电池充电或更换故障电池。 可能丢失数据 — 如果选择此选项并且没有通用电源进行保护，则可能会丢失数据。此外，如果您没有控制器电池并启用 **Write caching without batteries** 选项，则可能会丢失数据。 此设置仅在启用写缓存时可用。此设置不适用于精简卷。
使用镜像写入缓存	当写入一个控制器的缓存内存的数据也写入另一个控制器的缓存内存时，将发生镜像写入缓存。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。仅当写缓存已启用且存在两个控制器时，写缓存镜像才可用。使用镜像进行写缓存是创建卷时的默认设置。 此设置仅在启用写缓存时可用。此设置不适用于精简卷。

5. 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，用于扫描卷中的所有数据和冗余信息。使用此选项可启用或禁用一个或多个卷的介质扫描设置，或更改扫描持续时间。

开始之前

了解以下内容：

- 介质扫描根据要扫描的容量和扫描持续时间以恒定速率连续运行。后台扫描可能会被更高优先级的后台任务（例如重建）暂时挂起，但将以相同的恒定速率恢复。
- 仅当为存储阵列和该卷启用了媒体扫描选项时，才会扫描卷。如果该卷也启用了冗余检查，则将检查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，默认情况下会启用带冗余检查的媒体扫描。
- 如果在扫描过程中遇到不可恢复的介质错误，将使用冗余信息（如果可用）修复数据。

  例如，冗余信息在最佳 RAID 5 卷中可用，或者在最佳 RAID 6 卷中可用，或者仅有一个驱动器发生故障。

如果无法使用冗余信息修复不可恢复的错误，数据块将被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，则将其报告给事件日志。

默认介质扫描周期设置为 120 天。

关于此任务

介质扫描会检测并修复应用程序不经常读取的磁盘块上的介质错误。这可以在发生驱动器故障时防止数据丢失，因为故障驱动器的数据是使用冗余信息和卷组或池中其他驱动器的数据重建的。

您可以执行以下操作：

- 启用或禁用整个存储阵列的后台媒体扫描
- 更改整个存储阵列的扫描持续时间
- 启用或禁用一个或多个卷的媒体扫描
- 启用或禁用一个或多个卷的冗余检查

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择任何卷，然后选择菜单：更多[更改介质扫描设置]。

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

3. 要启用介质扫描，请选中 **Scan media over the course of…** 复选框。

   禁用介质扫描复选框将暂停所有介质扫描设置。

4. 指定希望运行媒体扫描的天数。
5. 选中要执行介质扫描的每个卷的 **Media Scan** 复选框。

   System Manager 为您选择运行媒体扫描的每个卷启用冗余检查选项。如果存在不希望执行冗余检查的单个卷，请取消选中 **Redundancy Check** 复选框。

6. 单击 **Save**。

   System Manager 根据您的选择将更改应用于后台媒体扫描。

使用复制服务

了解 **SANtricity System Manager** 中的 **Copy Volume**

Copy Volume 功能可通过在同一存储阵列上创建两个单独的卷（源卷和目标卷）来创建卷的时间点副本。

此函数执行从源卷到目标卷的逐字节复制，使目标卷上的数据与源卷上的数据相同。

数据复制以获得更大的访问权限

当您对卷的存储要求发生变化时，您可以使用 Copy Volume 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 Copy Volume 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更高的驱动器。
- 改用采用新技术的驱动器，以获得更高的性能。
- 将薄卷更改为厚卷。

复制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：

- **Native block size** – 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 4K，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 Copy Volume 操作创建精简卷的副本。Copy Volume 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

复制卷功能允许您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。您可以将目标卷用作源卷的备份、用于系统测试或备份到其他设备（如磁带驱动器）。

将快照卷数据还原到基本卷

如果需要将数据从其关联的快照卷还原到基本卷，可以使用 Copy Volume 功能将数据从快照卷复制到基本卷。您可以在快照卷上创建数据的卷副本，然后将数据复制到基本卷。

源卷和目标卷

下表指定了可用于 Copy Volume 功能的源卷和目标卷的卷类型。

卷类型	脱机卷复制源卷	联机卷复制源卷	联机和脱机目标卷
池中的厚卷	是	是	是
卷组中的厚卷	是	是	是
精简卷	是[1]	是	否
Snapshot 卷	是[2]	否	否

卷类型	脱机卷复制源卷	联机卷复制源卷	联机和脱机目标卷
Snapshot 基本卷	是	是	否
远程镜像主卷	是[3]	是	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，无法使用快照卷副本。

[3] 如果源卷是主卷，则目标卷的容量必须大于或等于源卷的可用容量。

了解 **SANtricity** 软件中拷贝卷操作的类型

您可以执行 *offline* Copy Volume 操作或 *online* Copy Volume 操作。脱机操作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，并将其数据复制到目标卷。

为了确保数据完整性，在任何一种类型的拷贝卷操作期间，目标卷的所有 I/O 活动都将暂停。此暂停是因为在过程完成之前，目标卷上的数据状态不一致。

下面将介绍离线和在线 Copy Volume 操作。

离线拷贝卷操作

脱机拷贝卷关系位于源卷和目标卷之间。脱机副本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复制的源卷的所有更新。将暂停对源卷的所有更新，以防止在目标卷上创建按时间顺序排列的不一致。

有关离线复制操作的注意事项	
读取和写入请求	• 参与脱机拷贝的源卷可用于只读 I/O 活动，而 Copy Volume 操作的状态为"正在进行"或"待处理"。 • 允许在脱机复制完成后写入请求。 • 为防止出现写保护错误消息，请勿访问状态为"正在进行"的参与 Copy Volume 操作的源卷。
日志文件系统	• 如果已使用日志文件系统格式化源卷，则任何向源卷发出读取请求的尝试都可能被存储阵列控制器拒绝，并可能出现错误消息。 • 日志文件系统驱动程序在尝试发出读取请求之前发出写入请求。控制器拒绝写入请求，并且由于被拒绝的写入请求，可能无法发出读取请求。此情况可能导致出现错误消息，指示源卷受写保护。 • 为防止出现此问题，请勿尝试在 Copy Volume 操作的状态为 In Progress 时访问参与脱机副本的源卷。

联机复制卷操作

联机 Copy Volume 关系是快照卷和目标卷之间的关系。您可以在源卷联机并可用于数据写入时启动 Copy Volume 操作。此功能通过创建卷的快照并将快照用作副本的实际源卷来实现。

当您启动源卷的复制卷操作时，System Manager 会创建基本卷的快照映像以及基本卷的快照映像与目标卷之间的复制关系。将快照映像用作源卷允许存储阵列在复制过程中继续写入源卷。

在联机复制操作期间，由于写入时复制过程，会遇到性能影响。在线复制完成后，将恢复基本卷性能。

有关在线复制操作的注意事项	
可以使用什么类型的卷？	• 为其创建时间点映像的卷称为基本卷，并且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。目标卷不能是快照组中的精简卷或基本卷。 • 您可以使用联机复制卷功能将数据从精简卷复制到驻留在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	• 如果用作复制源的快照卷处于活动状态，则由于写入时复制操作，基本卷性能会降低。复制完成后，将禁用快照，并恢复基本卷性能。虽然快照被禁用，但保留的容量卷和复制关系保持不变。
已创建卷的类型	• 快照卷和保留容量卷是在联机复制操作期间创建的。 • 快照卷不是包含数据的实际卷；相反，它是对特定时间卷上包含的数据的引用。 • 对于拍摄的每个快照，都会创建一个保留容量卷来保存快照的数据。保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，要修改的块的内容将被复制到保留容量卷以供保存。 • 由于保留容量卷将原始数据的副本存储在这些数据块中，因此对这些数据块的进一步更改仅写入源卷。 • 联机复制操作使用的磁盘空间少于完整物理副本，因为存储在保留容量卷中的唯一数据块是自 snapshot 时间以来已更改的数据块。

在 **SANtricity System Manager** 中复制卷

您可以将数据从同一存储阵列中的一个卷复制到另一个卷，并创建源卷的物理时间点副本（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。
- 如果以前在 Copy Volume 操作中使用过目标卷，则不再需要该数据或已备份该数据。

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 Copy Volume 时，源卷中的数据将完整拷贝到目标卷。

目标卷是维护源卷数据副本的标准卷。Copy Volume 操作完成后，目标卷与源卷完全相同。目标卷必须具有与源卷相同或更大的容量；但是，它可以具有不同的 RAID 级别。

有关联机和脱机副本的详细信息

在线副本

在线拷贝会创建存储阵列中任何卷的时间点拷贝，同时仍然可以在拷贝正在进行的情况下写入卷。此功能通过创建卷的快照并将快照用作副本的实际源卷来实现。创建时间点映像的卷称为基本卷，它可以是存储阵列中的标准卷或精简卷。

离线副本

脱机副本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复制的源卷的所有更新。将暂停对源卷的所有更新，以防止在目标卷上创建按时间顺序排列的不一致。脱机卷复制关系在源卷和目标卷之间。

拷贝卷操作会覆盖目标卷上的数据，并会使与目标卷关联的所有快照卷（如果存在）出现故障。

步骤

1. 选择菜单：Storage[Volumes]。
2. 选择要用作 Copy Volume 操作的源的卷，然后选择菜单：Copy Services[Copy volume]。

   此时将显示"复制卷-选择目标"对话框。

3. 选择要将数据复制到的目标卷。

   此对话框中显示的表格列出了所有符合条件的目标卷。

4. 使用滑块栏设置 Copy Volume 操作的复制优先级。

   与服务 I/O 请求相比，复制优先级确定用于完成复制卷操作的系统资源量。

   有关复制优先级费率的更多信息

   复制优先级有五种：

   - 最低
   - 低
   - 中
   - 高
   - 最高

   如果将拷贝优先级设置为最低等级，则会优先处理 I/O 活动，而 Copy Volume 操作则需要更长的时间。如果将拷贝优先级设置为最高等级，则会优先处理 Copy Volume 操作，而存储阵列的 I/O 活动可能受到影响。

5. 选择要创建联机副本还是脱机副本。要创建联机副本，请选中 **Keep source volume online during copy operation** 复选框。
6. 执行以下操作之一：

- 要执行_在线_复制操作，请单击*下一步*继续到*保留容量*对话框。
- 要执行 *offline* 复制操作，请单击 **Finish** 以启动离线复制。

7. 如果您选择创建在线副本，请设置存储在线副本的数据和其他信息所需的保留容量，然后单击 完成 以启动在线副本。

   卷候选表仅显示支持指定保留容量的候选。保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。

   使用以下指南分配预留容量：

   - 保留容量的默认设置为基本卷容量的 40%，通常此容量就足够了。
   - 但是，保留的容量会根据对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，保留的容量就应该越大。

结果

System Manager 将所有数据从源卷复制到目标卷。Copy Volume 操作完成后，目标卷将自动对主机变为只读。

完成后

选择菜单：Home[View Operations in Progress] 以查看 Copy Volume 操作的进度。此操作可能很长，并可能影响系统性能。

在 **SANtricity System Manager** 中对复制卷操作执行操作

您可以查看正在执行的 Copy Volume 操作以及停止、更改优先级、重新拷贝或清除 Copy Volume 操作。

步骤

1. 选择菜单：Home[View Operations in Progress]。

   此时将显示"正在进行的操作"对话框。

2. 找到要对其执行操作的 Copy Volume 操作，然后单击 **Actions** 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警告文本，特别是在停止操作时。

操作	说明
停止	当操作处于"进行中"、"待定"或"失败"状态时，可以停止 Copy Volume 操作。 当 Copy Volume 停止时，所有映射的主机都具有对源卷的写入权限。如果将数据写入源卷，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	您可以在操作状态为"正在进行"时更改 Copy Volume 操作的优先级，以选择 Copy Volume 操作完成的速率。

操作	说明
重新复制	停止拷贝卷操作并希望重新启动时，或拷贝卷操作失败或停止时，可以重新拷贝卷。拷贝卷操作从头开始。 重新复制操作会覆盖目标卷上的现有数据，并会使与目标卷关联的所有快照卷（如果有）出现故障。
清除	您可以在操作处于"正在进行"、"待定"或"失败"状态时删除 Copy Volume 操作。 请确保在选择 **Clear** 之前要执行此操作。没有确认对话框。

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

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是卷?

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

卷是根据池或卷组中的可用容量创建的。卷具有定义的容量。虽然卷可能由多个驱动器组成，但卷在主机上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?

所选卷组可能有一个或多个可用容量区域。可用容量区域是删除卷或在卷创建期间未使用所有可用容量而产生的可用容量。

在具有一个或多个可用容量区域的卷组中创建卷时，卷的容量仅限于该卷组中最大的可用容量区域。例如，如果一个卷组总共有 15 GiB 的可用容量，并且最大的可用容量区域为 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，则卷组图表包含指示现有可用容量区域数量的链接。选择链接以显示一个弹出窗口，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其他卷。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：

- 当至少检测到一个卷组的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的主页上。单击 合并可用容量 链接以启动对话框。
- 您还可以选择菜单：池和卷组[Uncommon Tasks > Consolidate volume group free capacity] 以启动此对话框。

如果要使用特定的可用容量区域而非最大的可用容量区域，请使用命令行界面 (CLI)。

我选择的工作负载如何影响卷的创建?

在创建卷期间，系统会提示您输入有关工作负载使用情况的信息。系统使用此信息为您创建最佳卷配置，可根据需要对其进行编辑。您也可以在卷创建顺序中跳过此步骤。

工作负载是支持应用程序的存储对象。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。这些卷特性是根据工作负载支持的应用程序类型进行优化的。例如，如果创建支持 Microsoft SQL Server 应用程序的工作负载，然后为该工作负载创建卷，则会优化基础卷特征以支持 Microsoft SQL Server。

- 特定于应用程序 — 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。对于为以下应用程序类型创建的工作负载，会自动推荐和优化 I/O 类型、段大小、控制器所有权以及读取和写入缓存等卷特征。
  - Microsoft® SQL Server™
  - Microsoft® Exchange Server™
  - 视频监控应用程序
  - VMware ESXi™（用于与 Virtual Machine File System 配合使用的卷）

    您可以使用 Add/Edit Volumes 对话框查看推荐的卷配置并编辑、添加或删除系统推荐的卷和特征。
- 其他（或不支持特定卷创建的应用程序）-- 其他工作负载使用卷配置，当您要创建未与特定应用程序关联的工作负载时，或者如果没有针对您打算在存储阵列上使用的应用程序的内置优化时，您必须手动指定此配置。您必须使用 Add/Edit Volumes 对话框手动指定卷配置。

为什么这些卷不与工作负载关联？

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

为什么无法删除选定的工作负载？

此工作负载由使用命令行界面 (CLI) 创建或从不同存储阵列迁移（导入/导出）的一组卷组成。因此，此工作负载中的卷与特定于应用程序的工作负载无关，因此无法删除该工作负载。

特定于应用程序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工作负载与存储阵列组件的交互方式，并有助于确定给定配置下环境的性能。

应用程序是 SQL Server 或 Exchange 等软件。您定义一个或多个工作负载以支持每个应用程序。

提供此信息如何帮助创建存储？

工作负载信息用于优化所选工作负载的卷特征，例如 I/O 类型、段大小和读/写缓存。这些优化的特性决定了您的工作负载如何与存储阵列组件交互。

根据您提供的工作负载信息，System Manager 会创建适当的卷，并将其放置在系统上当前存在的可用池或卷组中。系统会根据您选择的工作负载的当前最佳实践创建卷并优化其特征。

在完成为给定工作负载创建卷之前，您可以使用"添加/编辑卷"对话框查看建议的卷配置并编辑、添加或删除系统建议的卷和特征。

请参见特定于应用程序的文档以了解最佳实践信息。

我需要做些什么来识别扩展的容量？

如果增加卷的容量，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的卷容量，并在启动卷扩展后自动扩展。但是，有些可能不会。如果您的 OS 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，您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您正在使用的文件系统。

有关更多详细信息，请参见主机操作系统文档。

为什么我没有看到所有的池和/或卷组？

无法将卷移动到的任何池或卷组都不会显示在列表中。

由于以下任何原因，池或卷组不符合条件：

- 池或卷组池的 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。

什么是段大小？

段是以千字节 (KiB) 为单位存储在驱动器上的数据量，存储阵列会在此之后移动到条带中的下一个驱动器（RAID 组）。段大小仅适用于卷组，而不适用于池。

段大小由其包含的数据块数量定义。在确定段大小时，您必须知道将存储在卷中的数据类型。如果应用程序通常使用较小的随机读写 (IOPS)，则较小的段大小通常工作得更好。或者，如果应用程序具有较大的顺序读写（吞吐量），则较大的段大小通常更好。

无论应用程序使用的是小的随机读取和写入，还是大的顺序读取和写入，如果段大小大于典型的数据块区块大小，则存储阵列的性能会更好。这通常使驱动器更容易和更快地访问数据，这对于提高存储阵列性能非常重要。

IOPS 性能很重要的环境

在每秒 I/O 操作数 (IOPS) 环境中，如果使用的段大小大于读/写到驱动器的典型数据块大小（“chunk”），则存储阵列的性能会更好。这可确保每个 chunk 都写入单个驱动器。

吞吐量很重要的环境

在吞吐量环境中，段大小应为数据总驱动器数和典型数据块大小（I/O 大小）的偶数分数。这会将数据作为单个条带分布在卷组中的驱动器上，从而实现更快的读取和写入。

什么是首选控制器所有权？

首选控制器所有权定义了被指定为卷的拥有者或主控制器的控制器。

控制器所有权非常重要，应仔细规划。控制器应尽可能紧密地平衡总 I/O。

例如，如果一个控制器主要读取大型顺序数据块，而另一个控制器具有频繁读写的小数据块，则负载非常不同。了解哪些卷包含哪些类型的数据，可以在两个控制器上均衡 I/O 传输。

我什么时候想使用"稍后分配主机"选项？

如果要加快创建卷的过程，可以跳过主机分配步骤，以便离线初始化新创建的卷。

必须初始化新创建的卷。系统可以使用两种模式之一对其进行初始化：即时可用格式 (IAF) 后台初始化过程或离线过程。

当您将卷映射到主机时，它会强制该组中的任何初始化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，这有时会很耗时。

当未映射卷组中的任何卷时，将执行脱机初始化。脱机流程比后台流程快得多。

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"）。您必须在卷创建过程中设置正确的值。如果可能，系统会建议适当的默认值。

在设置卷块大小之前，请阅读以下限制和指南。

- 某些操作系统和虚拟机（尤其是目前的 VMware）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呈现 4KiB 块大小来实现最佳性能；但是，请确保您的主机允许 4KiB（或"`4Kn`"）块。
- 为池或卷组选择的驱动器类型也决定了支持的卷块大小，如下所示：
  - 如果您使用写入 512 字节块的驱动器创建卷组，则只能创建具有 512 字节块的卷。
  - 如果您使用写入 4KiB 块的驱动器创建卷组，则可以使用 512 字节或 4KiB 块创建卷。
- 如果阵列具有 iSCSI 主机接口卡，则所有卷都限制为 512 字节块（无论卷组块大小如何）。这是由于特定的硬件实现所致。
- 一旦设置了块大小，则无法对其进行更改。如果需要更改块大小，则必须删除该卷并重新创建它。

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群集，它们定义了存储阵列和数据服务器之间的连接。

什么是主机和主机集群？

host 是向存储阵列上的卷发送 I/O 的服务器。*host cluster* 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。

了解详情：

- "主机术语"
- "访问卷"
- "LUN 的最大数量"

如何配置主机和主机群集？

要定义主机连接，您可以转到菜单：Storage[Hosts] 手动配置主机。如果您希望两个或多个主机共享对同一卷集的访问权限，则可以定义一个群集并将该卷分配给该群集。

了解详情：

- "手动创建主机"
- "如何将卷分配给主机和主机群集"
- "主机创建和卷分配的工作流程"
- "手动创建主机"
- "创建主机集群"
- "将卷分配给主机"

相关信息

了解更多与主机相关的任务：

- "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

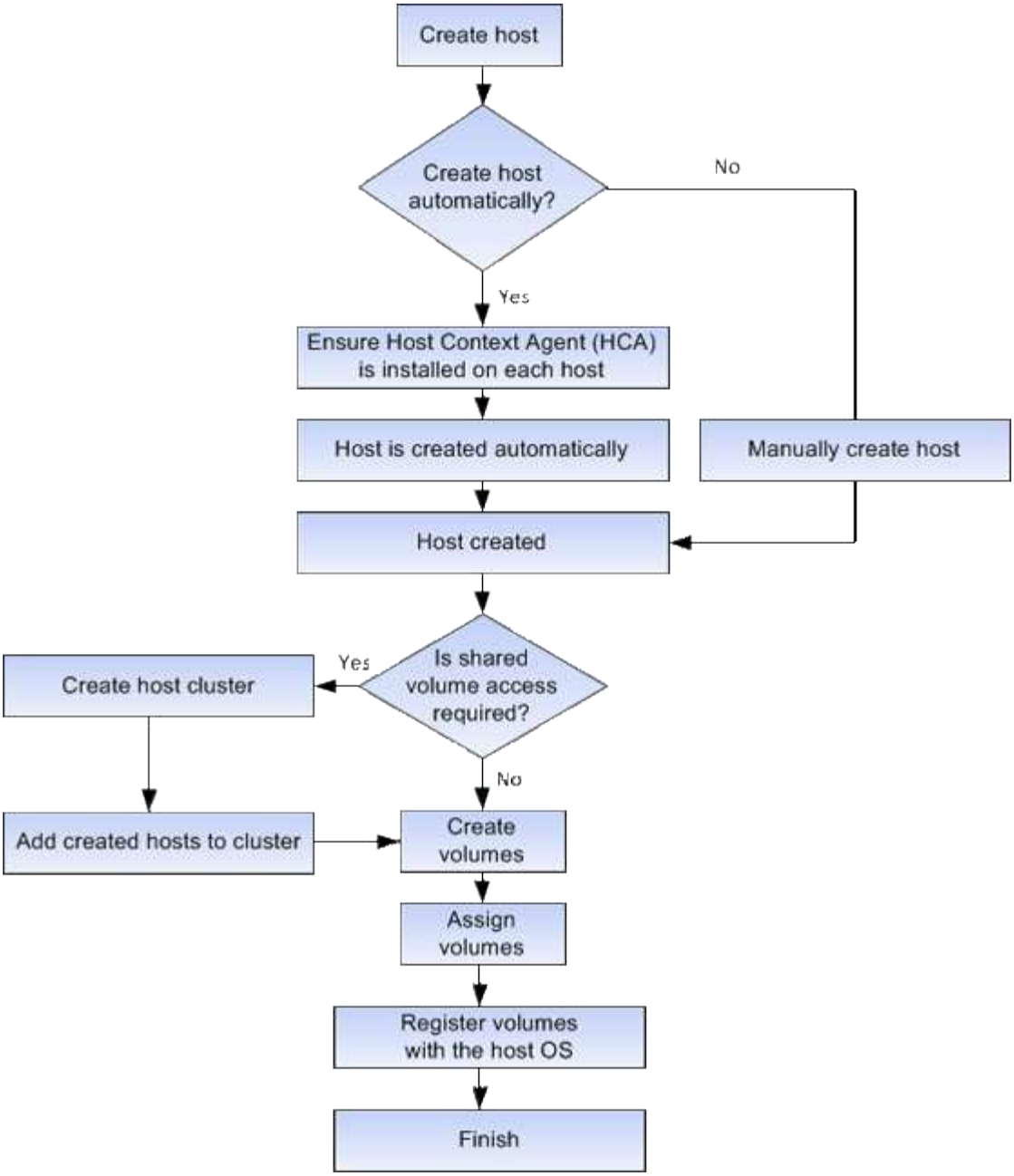
了解主机术语如何适用于您的存储阵列。

组件	定义
主机	主机是向存储阵列上的卷发送 I/O 的服务器。
主机名	主机名应等同于主机的系统名称。
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) 是驻留在主机中的主板，包含一个或多个主机端口。
主机端口	主机端口是主机总线适配器 (HBA) 上的端口，它提供与控制器的物理连接，并用于 I/O 操作。

组件	定义
主机端口标识符	主机端口标识符是与主机总线适配器 (HBA) 上的每个主机端口相关联的唯一全球名称。 • Internet Small Computer System Interface (iSCSI) 主机端口标识符必须介于 1 到 233 个字符之间。iSCSI 主机端口标识符以标准 IQN 格式显示（例如，`iqn.xxx.com.xxx:8b3ad`）。 • 非 iSCSI 主机端口标识符（如光纤通道和串行连接 SCSI (SAS)）在每两个字符后显示为冒号分隔（例如， `xx:yy:zz`）。光纤通道主机端口标识符必须有 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对 I/O 的反应方式，具体取决于主机的操作系统（或变体）。这有时也简称为 *host type*。
控制器主机端口	控制器主机端口是控制器上的一个端口，用于提供与主机的物理连接，并用于 I/O 操作。
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。此卷以 LUN 的形式作为容量呈现给主机。 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相同的 LUN 来访问不同的卷。

SANtricity System Manager 中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。



了解如何在 **SANtricity System Manager** 中手动创建主机

创建主机是让存储阵列知道哪些主机连接到它并允许对卷进行 I/O 访问所需的步骤之一。您只能手动创建主机。

手动创建

手动创建主机允许您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或手动输入主机端口标识符来关联主机端口标识符。创建主机后，如果计划共享对卷的访问权限，则可以为其分配卷或将其添加到主机群集中。

如何在 **SANtricity** 软件中将卷分配给主机和主机群集

要使主机或主机群集向卷发送 I/O，必须将该卷分配给主机或主机群集。

您可以在创建卷时选择主机或主机群集，也可以稍后将卷分配给主机或主机群集。主机群集是一组主机。您可以创建主机群集，以便轻松地将相同的卷分配给多个主机。

您可以灵活地为主机分配卷，从而满足特定的存储需求。

- 独立主机，不属于主机群集 — 您可以将卷分配给单个主机。该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都可以访问该卷。
- 主机群集中的主机 — 您可以将卷分配给作为主机群集一部分的单个主机。即使主机是主机群集的一部分，卷只能由单个主机访问，而不能由主机群集中的任何其他主机访问。

创建卷时，将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"。可以在创建卷后更改 LUN。

在 **SANtricity System Manager** 中访问卷

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 (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。仅当您使用命令行界面 (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 E4000、EF600/EF600C 或 EF300/EF300C 存储系统。

首次将卷分配给主机时会自动创建访问卷。例如，如果您将 Volume_1 和 Volume_2 分配给主机，当您查看该分配的结果时，您会看到三个卷（Volume_1、Volume_2 和 Access）。

如果您没有使用 CLI 自动创建主机或在带内管理存储阵列，则不需要访问卷，并且可以通过删除访问卷来释放 LUN。此操作将删除卷到 LUN 的分配以及到主机的所有带内管理连接。

了解 **SANtricity** 软件中 **LUN** 的最大数量

存储阵列具有可用于每个主机的逻辑单元号 (LUN) 的最大数量。

最大数量取决于主机的操作系统。存储阵列跟踪使用的 LUN 数。如果尝试将卷分配给超出最大 LUN 数的主机，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

初始连接主机时，存储阵列使用默认主机类型。它定义了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。

如果需要相对于连接到存储阵列的主机更改存储阵列的运行方式，则可以更改主机类型。通常，在将主机连接到存储阵列之前或连接其他主机时，都会更改默认主机类型。

请记住以下准则：

- 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），请更改主机类型以匹配操作系统。
- 如果您计划连接到存储阵列的主机具有不同的操作系统（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，并且其中六个主机正在运行 Windows 操作系统，则必须选择 Windows 作为默认主机操作系统类型。

- 如果大多数连接的主机混合使用不同的操作系统，请将主机类型更改为 Factory Default。

  例如，如果要将八台不同的主机连接到存储阵列，其中两台主机运行的是 Windows 操作系统，三台主机运行的是 VMware 操作系统，另外三台主机运行的是 Linux 操作系统，则必须选择 Factory Default 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。创建主机是让存储阵列知道哪些主机连接到它并允许对卷进行 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：

- 您必须定义与该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，此操作将不会成功。
- 名称长度不能超过 30 个字符。

步骤

1. 选择菜单：Storage[Hosts]。
2. 单击菜单：Create[Host]。

   此时将显示创建主机对话框。

3. 根据需要选择主机的设置。

字段详细信息

设置	说明
名称	输入新主机的名称。
主机操作系统类型	从下拉列表中选择正在新主机上运行的操作系统。
主机接口类型	（可选）如果存储阵列上支持多种类型的主机接口，请选择要使用的主机接口类型。
主机端口	执行以下操作之一： • 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。HBA 实用程序或 iSCSI 启动程序实用程序可用于查找主机端口标识符并将其与主机相关联。 您可以手动输入主机端口标识符，或将它们从实用程序（一次一个）复制/粘贴到 **Host ports** 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多个标识符。每个标识符都显示在*主机端口*字段中。如有必要，您也可以选择旁边的*X*来删除标识符。
CHAP 启动程序	（可选）如果选择或手动输入带有 iSCSI IQN 的主机端口，并且如果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 密码。如果要使用双方 CHAP 身份验证（双向身份验证，使主机能够向存储阵列验证自身，并使存储阵列能够向主机验证自身），还必须在初始设置或更改设置时为存储阵列设置 CHAP 密码。 • 如果您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。

4. 单击 **Create**。

结果

成功创建主机后，系统会为该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 host IPT is IPT_1 创建的第一个端口的默认别名。

在 SANtricity System Manager 中创建主机集群

当两个或多个主机需要对同一卷进行 I/O 访问时，可以创建主机群集。

关于此任务

创建主机集群时，请记住以下准则：

- 除非有两个或多个主机可用于创建集群，否则此操作不会启动。
- 主机群集中的主机可以使用不同的操作系统（异构）。
- 主机集群中的 NVMe 主机无法与非 NVMe 主机混合。
- 要创建启用 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，则关联的主机无法访问启用 DA 的卷上的数据。

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

步骤

1. 选择菜单：Storage[Hosts]。
2. 选择菜单：Create[Host Cluster]。

   此时将显示"创建主机群集"对话框。

3. 根据需要选择主机集群的设置。

   字段详细信息

设置	说明
名称	键入新主机集群的名称。
选择要共享卷访问权限的主机	从下拉列表中选择两个或多个主机。只有那些尚未成为主机集群一部分的主机才会显示在列表中。

4. 单击 **Create**。

   如果所选主机连接到具有不同 Data Assurance (DA) 功能的接口类型，则会出现一个对话框，其中显示 DA 在主机群集上不可用。此不可用性可防止将启用了 DA 的卷添加到主机群集中。选择 **Yes** 继续，或选择 **No** 取消。

   DA 提高了整个存储系统的数据完整性。DA 使存储阵列能够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

新主机群集显示在表中，分配的主机位于下方的行中。

在 **SANtricity System Manager** 中将卷分配给主机

必须将卷分配给主机或主机群集，以便将其用于 I/O 操作。此分配授予主机或主机群集对存储阵列中一个或多个卷的访问权限。

关于此任务

将卷分配给主机时，请记住以下准则：

- 一次只能将一个卷分配给一个主机或主机群集。
- 分配的卷在存储阵列中的控制器之间共享。
- 主机或主机群集不能使用相同的逻辑单元号 (LUN) 两次访问卷。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，所有 卷都将恢复到较慢的初始化。您可以从菜单：主页 [正在进行的操作] 中检查初始化进度。

在以下情况下分配卷失败：

- 已分配所有卷。
- 此卷已分配给另一个主机或主机群集。

在以下情况下无法分配卷：

- 不存在有效的主机或主机群集。
- 未为该主机定义任何主机端口标识符。
- 已定义所有卷分配。

在此任务期间，将显示所有未分配的卷，但具有或不具有数据保障 (DA) 的主机的功能适用如下：

- 对于支持 DA 的主机，您可以选择启用 DA 或未启用 DA 的卷。
- 对于不支持 DA 的主机，如果选择启用了 DA 的卷，则会显示一条警告，指出系统必须在将卷分配给主机之前自动关闭卷上的 DA。

步骤

1. 选择菜单：Storage[Hosts]。
2. 选择要向其分配卷的主机或主机群集，然后单击 **Assign Volumes**。

   此时将显示一个对话框，其中列出可以分配的所有卷。您可以对任意列进行排序，或在 **Filter** 框中输入内容，以便更轻松地查找特定卷。

3. 选中要分配的每个卷旁边的复选框，或选中表头中的复选框以选择所有卷。
4. 单击 分配 完成此操作。

结果

成功将一个或多个卷分配给主机或主机群集后，系统将执行以下操作：

- 分配的卷接收下一个可用的 LUN 编号。主机使用 LUN 编号访问此卷。
- 用户提供的卷名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可在存储阵列级别更改默认主机类型。通常，在将主机连接到存储阵列之前或连接其他主机时，都会更改默认主机类型。

关于此任务

请记住以下准则：

- 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），请更改主机类型以匹配操作系统。
- 如果您计划连接到存储阵列的主机具有不同的操作系统（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，并且其中六个主机正在运行 Windows 操作系统，则必须选择 Windows 作为默认主机操作系统类型。

- 如果大多数连接的主机混合使用不同的操作系统，请将主机类型更改为 Factory Default。

  例如，如果要将八台不同的主机连接到存储阵列，其中两台主机运行的是 Windows 操作系统，三台主机运行的是 VMware 操作系统，另外三台主机运行的是 Linux 操作系统，则必须选择 Factory Default 作为默认主机操作系统类型。

步骤

1. 选择菜单：Settings[System]。
2. 向下滚动到 **Additional Settings**，然后单击 **Change Default Host Operating System Type**。
3. 选择要用作默认值的主机操作系统类型。
4. 单击 **Change**。

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

如果不再需要从主机或主机群集对该卷进行 I/O 访问，请取消分配主机或主机群集的卷。

关于此任务

取消分配卷时，请记住以下准则：

- 如果您要从主机群集中删除最后分配的卷，并且主机群集还具有分配了特定卷的主机，请确保在删除主机群集的最后一个分配之前删除或移动这些分配。
- 如果将主机群集、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. 选择菜单：Storage[Hosts]。
2. 选择要编辑的主机或主机群集，然后单击 取消分配卷。

   此时将显示一个对话框，其中显示当前分配的所有卷。

3. 选中要取消分配的每个卷旁边的复选框，或选中表头中的复选框以选择所有卷。
4. 单击 **Unassign**。

结果

- 未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群集。

关于此任务

删除主机或主机群集时，请记住以下准则：

- 任何特定卷分配都将被删除，并且关联的卷可用于新分配。
- 如果主机是具有其自身特定分配的主机群集的一部分，则主机群集不受影响。但是，如果主机是没有任何其他分配的主机群集的一部分，则主机群集和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。
- 任何与该主机关联的主机端口标识符都将变为未定义。

步骤

1. 选择菜单：Storage[Hosts]。
2. 选择要删除的主机或主机群集，然后单击 **Delete**。

   此时将显示确认对话框。

3. 确认您要执行此操作，然后单击 **Delete**。

结果

如果您删除了主机，系统将执行以下操作：

- 删除主机，并在适用的情况下将其从主机集群中删除。
- 删除对任何已分配卷的访问。
- 将关联的卷返回到未分配的状态。
- 将与主机关联的任何主机端口标识符返回到未关联状态。

如果删除了主机群集，系统将执行以下操作：

- 删除主机群集及其关联主机（如果有）。
- 删除对任何已分配卷的访问。
- 将关联的卷返回到未分配的状态。

- 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配置的主机之间的连接，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，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，自动负载平衡监控和平衡控制器资源利用率。

步骤

1. 选择菜单：Settings[System]。
2. 向下滚动至 **Additional Settings**，然后单击 **Enable/Disable Host Connectivity Reporting**。

   此选项下方的文本指示当前是已启用还是已禁用。

   此时将打开一个确认对话框。

3. 单击 **Yes** 继续。

   通过选择此选项，您可以在启用/禁用之间切换功能。

管理设置

在 **SANtricity System Manager** 中更改主机设置

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群集。

步骤

1. 选择菜单：Storage[Hosts]。
2. 选择要编辑的主机，然后单击 **View/Edit Settings**。

   此时将显示一个对话框，显示当前主机设置。

3. 如果尚未选择，请单击 **Properties** 选项卡。
4. 根据需要更改设置。

字段详细信息

设置	说明
名称	您可以更改用户提供的主机名称。必须指定主机的名称。
关联的主机集群	您可以从以下选项中进行选择： • 无 — 主机仍然是独立主机。如果主机与主机集群相关联，则系统会从集群中删除主机。 • **<Host Cluster>** — 系统将主机与选定集群关联。
主机操作系统类型	您可以更改在您定义的主机上运行的操作系统类型。

5. 单击 **Save**。

在 **SANtricity System Manager** 中更改主机集群的设置

您可以更改主机集群名称，或在主机集群中添加或删除主机。

步骤

1. 选择菜单：Storage[Hosts]。
2. 选择要编辑的主机群集，然后单击 **View/Edit Settings**。

   此时将显示一个对话框，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

设置	说明
名称	您可以指定用户提供的主机集群名称。必须为集群指定名称。
关联主机	要添加主机，请单击 **Associated Hosts** 框，然后从下拉列表中选择主机名。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 **Save**。

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

当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删除主机端口标识符时，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，您正在将主机端口标识符关联到为连接到存储阵列而创建的主机。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，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. 选择菜单：Storage[Hosts]。
2. 选择端口将关联的主机，然后单击 **View/Edit Settings**。

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

   此时将显示一个对话框，显示当前主机设置。

3. 单击 **Host Ports** 选项卡。

   此对话框显示当前主机端口标识符。

4. 根据需要更改主机端口标识符设置。

设置	说明
主机端口	您可以从以下选项中进行选择： • 添加 — 使用添加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。 • **Delete** — 使用 Delete 删除（取消关联）主机端口标识符。Delete 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。
标签	要更改端口标签名称，请单击*编辑*图标（铅笔）。端口标签名称必须是唯一的。不允许使用已配置的标签名称。
CHAP 密钥	仅对 iSCSI 主机显示。您可以设置或更改启动器（iSCSI 主机）的 CHAP 密码。 System Manager 使用质询握手身份验证协议 (CHAP) 方法，该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 密钥的共享安全密钥。

5. 单击 **Save**。

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

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是主机和主机集群?

主机是向存储阵列上的卷发送 I/O 的服务器。主机群集是一组主机。您可以创建主机群集，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。它可以是独立实体，也可以添加到主机群集中。可以将卷分配给单个主机，或者主机可以是与主机群集中的其他主机共享一个或多个卷的访问权限的主机群集的一部分。

主机群集是在 SANtricity System Manager 中创建的逻辑实体。必须先将主机添加到主机群集中，然后才能分配卷。

为什么需要创建主机集群?

如果要让两个或多个主机共享对同一卷集的访问权限，则需要创建主机群集。通常，单个主机上安装了群集软件来协调卷访问。

如何知道哪种主机操作系统类型是正确的?

"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推荐的主机类型。

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。最新版本首先显示最常见的选项，这些选项最有可能是合适的。此列表中的外观并不意味着完全支持该选项。

有关主机支持的详细信息，请参阅 "NetApp 互操作性表工具"。

以下主机类型可能会出现在列表中：

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 Device Mapper 多路径故障转移解决方案且内核版本为 3.10 或更高版本的 Linux 操作系统。
VMware ESXi	支持运行 Native Multipathing Plug-in (NMP) 架构的 VMware ESXi 操作系统，使用 VMware 内置存储阵列类型策略模块 SATP_ALUA。
Windows（集群或非集群）	支持未运行 ATTO 多路径驱动程序的 Windows 群集或非群集配置。
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 SVC	支持 IBM SAN Volume Controller 配置。
出厂默认值	保留用于存储阵列的初始启动。如果您的主机操作系统类型设置为 Factory Default，请将其更改为与连接主机上运行的主机操作系统和多路径驱动程序相匹配。
Linux DM-MP（内核 3.9 或更早版本）	支持使用 Device Mapper 多路径故障转移解决方案且内核版本为 3.9 或更早版本的 Linux 操作系统。
窗口聚集（已弃用）	如果主机操作系统类型设置为该值，请改用 Windows（群集或非群集）设置。

什么是 **HBA** 和适配器端口?

主机总线适配器 (HBA) 是驻留在主机中的主板，包含一个或多个主机端口。主机端口是主机总线适配器 (HBA) 上的端口，用于提供与控制器的物理连接，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 有一个唯一的全球标识符 (WWID)，每个 HBA 主机端口都有一个唯一的 WWID。当您通过 SANtricity System Manager 手动创建主机时，主机端口标识符用于将相应的 HBA 与物理主机关联。

如何将主机端口与主机匹配?

如果要手动创建主机，首先必须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，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。如果您关联了错误的主机端口标识符，则可能会导致其他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 Challenge Handshake Authentication Protocol (CHAP) 身份验证，则必须为每个 iSCSI 主机重新输入该启动器 CHAP 密码。

为此，您可以将 System Manager 用作 Create Host（创建主机）操作的一部分或通过 View/Edit Settings（查看/编辑设置）选项使用。

如果您使用 CHAP 相互身份验证，还必须在 Settings 页中定义存储阵列的目标 CHAP 密码，然后在每个 iSCSI 主机上重新输入该目标 CHAP 密码。

什么是默认集群？

默认集群是一个系统定义的实体，它允许已登录到存储阵列的任何未关联的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一个主机端口，它在逻辑上不与特定主机关联，而是物理安装在主机中并登录到存储阵列。

> 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_不_使用默认群集。相反，您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 Create Host 操作期间手动完成。然后，您将卷分配给单个主机或主机群集。

您应该_仅_在外部存储环境有利于允许所有主机和连接到存储阵列的所有登录主机端口标识符访问所有卷（全访问模式）而无需特别使存储阵列或用户界面了解主机的特殊情况下使用默认集群。

最初，只能通过命令行界面 (CLI) 将卷分配给默认群集。但是，将至少一个卷分配给默认群集后，此实体（称为 Default Cluster）将显示在用户界面中，然后您可以在其中管理此实体。

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。

如果电缆松动、损坏或丢失，或者主机出现其他问题，可能会导致连接中断。在这些情况下，系统可能会打开 Recovery Guru 消息：

- 主机冗余丢失 — 如果任何一个控制器无法与主机通信，则打开。
- 主机类型不正确 — 如果主机类型在存储阵列上指定不正确，则打开，这可能导致故障转移问题。

在重新启动控制器可能需要比连接超时更长的时间的情况下，您可能需要禁用主机连接报告。禁用此功能将抑制 Recovery Gurus 消息。

> 禁用主机连接报告还会禁用自动负载平衡，该功能用于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。

Snapshot

了解 SANtricity System Manager 中的快照

通过 Snapshot 功能，您可以创建用于备份或测试的存储阵列卷的时间点映像。

什么是快照映像？

_快照映像_是在特定时间点捕获的卷数据的逻辑副本。像还原点一样，快照映像允许您回滚到已知良好的数据集。虽然主机可以访问快照映像，但不能直接读写。

了解详情：

- "快照存储的工作原理"
- "Snapshot 术语"
- "基本卷、保留容量和快照组"

- "快照计划和一致性组"
- "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：Storage[Snapshots] 中获得。

了解详情：

- "快照的要求和准则"
- "用于创建快照映像和卷的工作流程"
- "创建快照映像"
- "计划 snapshot 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。您可以从菜单：Storage[Snapshots] 中回滚快照数据。

了解详情：

- "Snapshot 回滚"
- "启动基本卷的快照映像回滚"
- "为一致性组成员启动快照映像回滚"

相关信息

详细了解与快照相关的任务：

- "更改快照卷的保留容量"
- "更改快照组的保留容量"

概念

快照存储在 **SANtricity** 软件中的工作原理

快照功能使用写时复制技术来存储快照映像并使用分配的预留容量。

如何使用快照映像

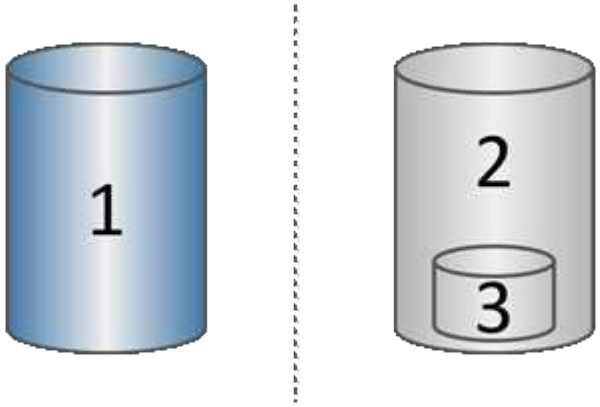
快照映像是在特定时间点捕获的卷内容的逻辑只读副本。您可以使用快照来防止数据丢失。

快照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权限，因此快照始终是安全的备份资源。

Snapshot 创建

创建快照时， Snapshots 功能按如下方式存储图像数据：

- 创建快照映像时，它与基本卷完全匹配。快照功能使用写时复制技术。拍摄快照后，对基本卷上的任何块或块集的第一次写入会导致在将新数据写入基本卷之前将原始数据复制到保留容量。
- 后续快照仅包括已更改的数据块。在基本卷上覆盖数据之前，Snapshots 功能使用其写入时复制技术将受影响扇区的所需映像保存到快照保留容量。



[1] 基本卷（物理磁盘容量）；[2] 快照（逻辑磁盘容量）；[3] 保留容量（物理磁盘容量）

- 保留容量存储拍摄快照后已更改的基本卷部分的原始数据块，并包括用于跟踪更改的索引。通常，保留容量的大小默认为基本卷的 40%。（如果您需要更多保留容量，可以增加保留容量。）
- 快照映像根据其时间戳按特定顺序存储。只有基本卷的最旧快照映像可用于手动删除。

Snapshot 恢复

要将数据还原到基本卷，您可以使用快照卷或快照映像：

- 快照卷 — 如果需要检索已删除的文件，请从已知良好的快照映像创建快照卷，然后将其分配给主机。
- **Snapshot** 映像 — 如果需要将基本卷还原到特定的时间点，请使用先前的 snapshot 映像将数据回滚到基本卷。

了解 **SANtricity** 软件中的快照术语

了解 Snapshot 术语如何适用于您的存储阵列。

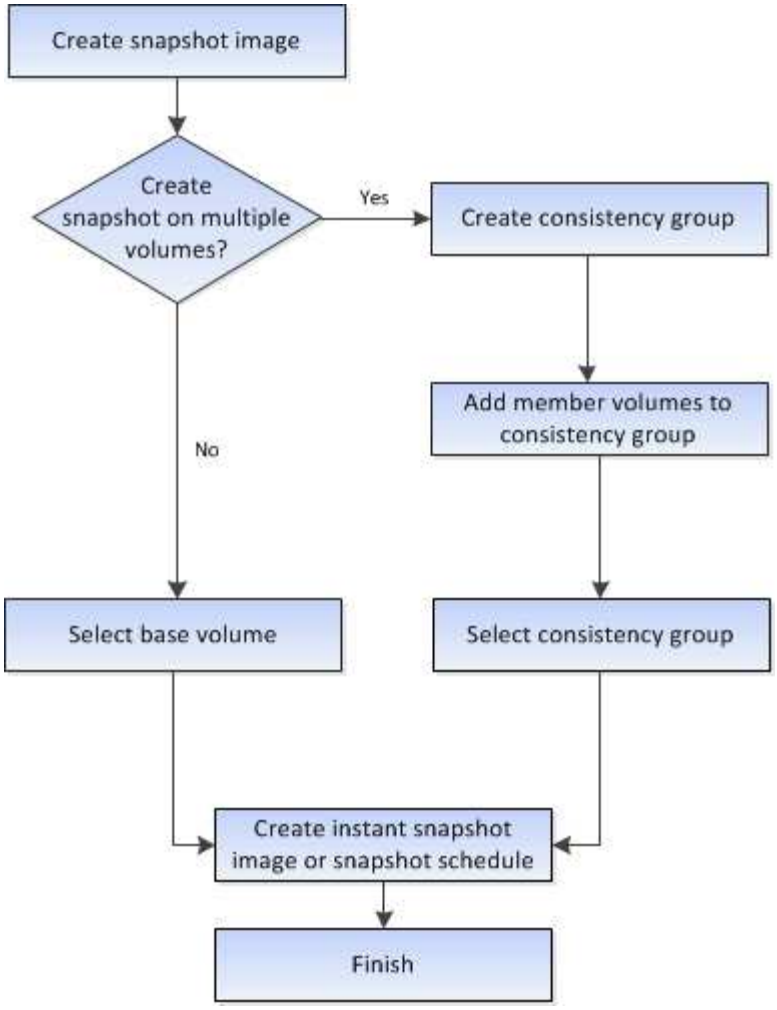
术语	说明
Snapshot 功能	Snapshots 功能用于创建和管理卷的映像。
Snapshot 图像	快照映像是在特定时间点捕获的卷数据的逻辑副本。像还原点一样，快照映像允许您回滚到已知良好的数据集。虽然主机可以访问快照映像，但不能直接读写。

术语	说明
基础卷	基本卷是创建快照映像的源。它可以是厚卷或精简卷，通常分配给主机。基本卷可以驻留在卷组或磁盘池中。
Snapshot 卷	快照卷允许主机访问快照映像中的数据。快照卷包含其自己的保留容量，该容量可保存对基本卷的任何修改，而不会影响原始快照映像。
Snapshot 组	快照组是来自单个基本卷的快照图像的集合。
预留容量卷	保留容量卷跟踪基本卷的哪些数据块被覆盖以及这些块的保留内容。
Snapshot 计划	Snapshot 计划是用于创建自动快照映像的时间表。通过该计划，您可以控制映像创建的频率。
快照一致性组	快照一致性组是创建快照映像时被视为单个实体的卷集合。每个卷都有自己的快照映像，但所有映像都是在相同的时间点创建的。
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	回滚是将基本卷中的数据返回到上一个时间点的过程。
预留容量	保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。

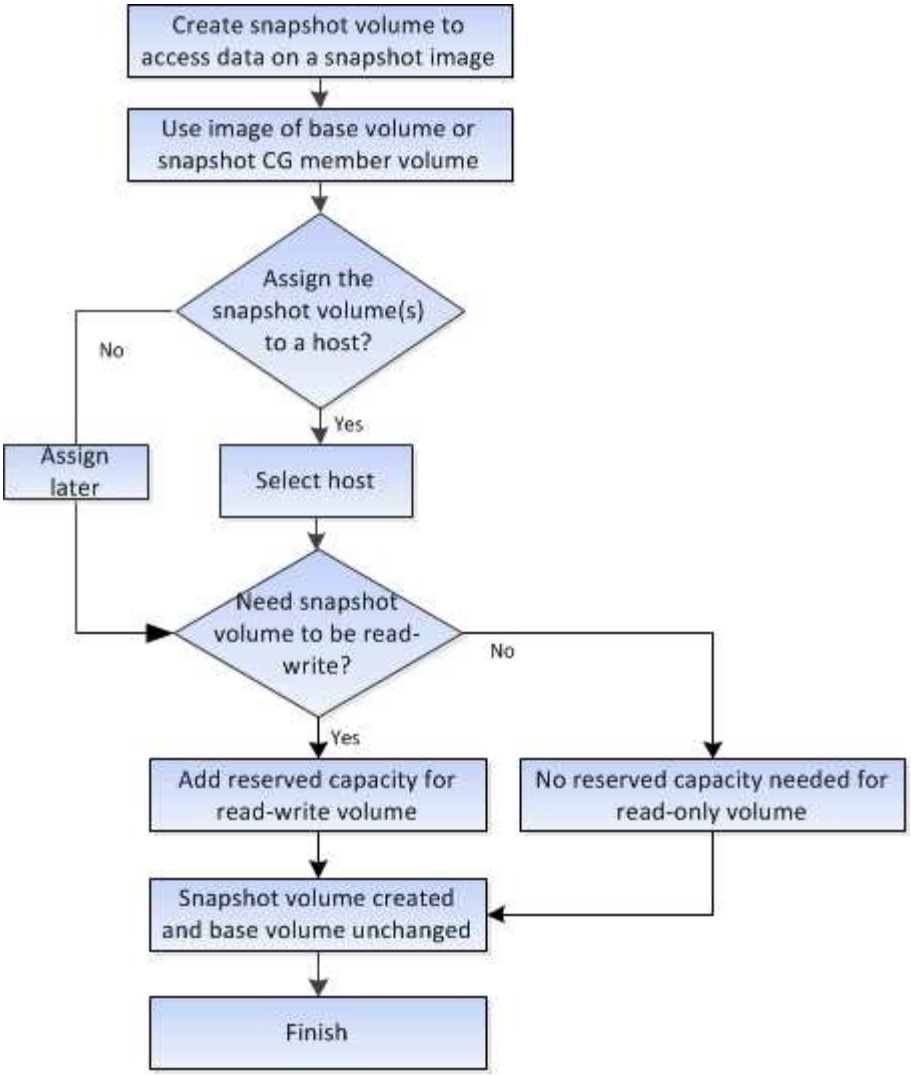
如何在 **SANtricity System Manager** 中创建快照映像和快照卷

在 SANtricity System Manager 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程


Create snapshot image
Create snapshot on multiple volumes?
Yes
Create consistency group
Add member volumes to consistency group
No
Select base volume
Select consistency group
Create instant snapshot image or snapshot schedule
Finish

创建快照卷的工作流程



SANtricity System Manager 中快照的要求和准则

创建和使用快照时，请查看以下要求和准则。

快照映像和快照组

- 每个快照映像仅与一个快照组关联。
- 第一次为关联对象创建计划或即时快照映像时，即会创建快照组。这将创建保留容量。

  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，也会删除快照计划。
- 如果您有一个不再需要的快照卷，则可以重复使用它以及任何关联的保留容量，而不是将其删除。这会创建相同基本卷的不同快照卷。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，只要快照映像位于相同的基本卷中即可。

快照一致性组

- 快照一致性组包含作为快照一致性组成员的每个卷的一个快照组。
- 一个快照一致性组只能与一个计划相关联。
- 如果删除具有快照计划的快照一致性组，也会删除快照计划。
- 不能单独管理与快照一致性组关联的快照组。相反，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

- 快照卷必须具有与关联的基本卷相同的数据保证 (DA) 和安全设置。
- 无法为出现故障的基本卷创建快照卷。
- 如果基本卷驻留在卷组中，则任何关联的快照一致性组的成员卷都可以驻留在池或卷组中。
- 如果基本卷驻留在池中，则任何关联的快照一致性组的所有成员卷都必须驻留在与基本卷相同的池中。

预留容量

- 保留容量仅与一个基本卷相关联。
- 使用计划可能会产生大量快照图像。确保您有足够的保留容量用于计划的快照。
- 快照一致性组的保留容量卷必须与快照一致性组成员卷的相关基本卷具有相同的数据保证 (DA) 和安全设置。

挂起的 **Snapshot** 映像

在以下情况下，快照映像创建可能保持"待处理"状态：

- 包含此快照映像的基本卷是异步镜像组的成员。
- 基本卷当前处于同步操作中。快照映像创建在同步操作完成后立即完成。

快照图像的最大数量

- 如果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本卷允许的最大快照组数。
- 如果尝试在快照组或快照一致性组上创建快照映像，但关联的组已达到其快照映像的最大数量，您有两种选择：
  - 为快照组或快照一致性组启用自动删除。
  - 从快照组或快照一致性组中手动删除一个或多个快照图像并重试此操作。

自动删除

如果快照组或快照一致性组已启用自动删除，则当系统为该组创建新快照映像时，System Manager 会删除最旧的快照映像。

回滚操作

- 正在执行回滚操作时，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本卷创建新的快照映像。
- 更改关联快照组的 Repository-Full 策略。

- 当以下任一操作正在进行时，您无法启动回滚操作：
  - 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
  - 卷的段大小更改
- 如果基本卷参与卷副本，则无法启动回滚操作。
- 如果基本卷是远程镜像中的辅助卷，则无法启动回滚操作。
- 如果关联快照存储库卷中的任何已用容量具有不可读扇区，则回滚操作将失败。

了解 **SANtricity System Manager** 中的基础卷、预留容量和快照组

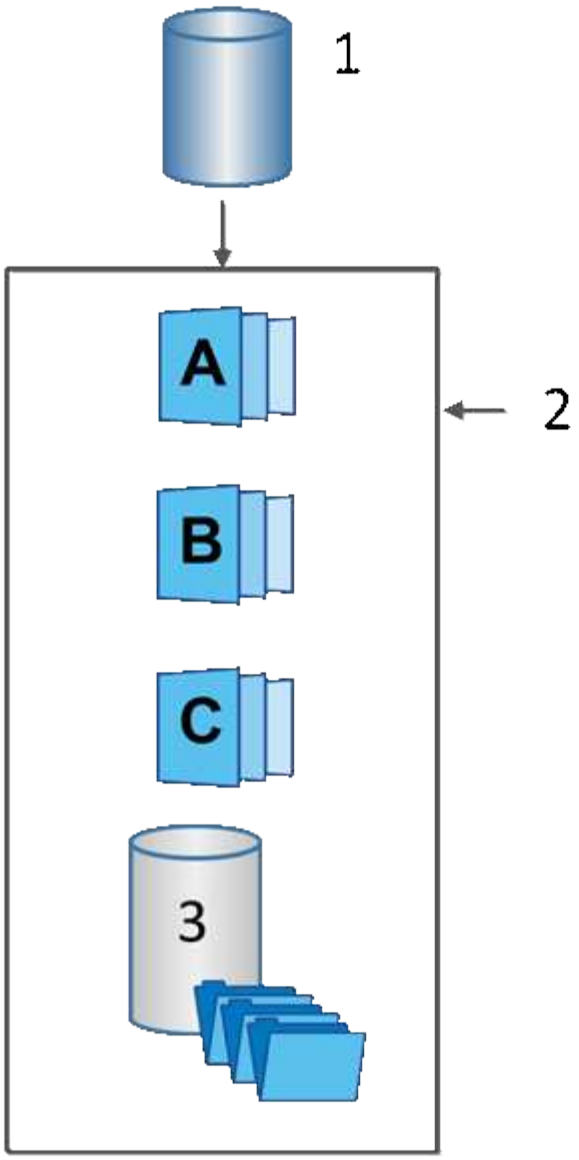
快照功能利用基本卷、保留容量和快照组。

基础卷

_基本卷_是用作快照映像源的卷。基本卷可以是厚卷或精简卷，并且可以位于池或卷组中。

要拍摄基本卷的快照，您可以随时创建即时映像，也可以通过定义快照的常规计划来自动执行此过程。

下图显示了快照对象和基本卷之间的关系。



[1] 基本卷；[2] 组中的快照对象（映像和预留容量）；[3] 为快照组预留容量。

预留容量和快照组

System Manager 将快照映像组织到_快照组_中。当 System Manager 建立快照组时，它会自动创建关联的_预留容量_来保存该组的快照映像，并跟踪对其他快照的后续更改。

如果基本卷位于卷组中，则保留容量可以位于池或卷组中。如果基本卷位于池中，则保留容量必须位于与基本卷相同的池中。

快照组无需用户操作，但您可以随时调整快照组上的保留容量。此外，当满足以下条件时，可能会提示您创建保留容量：

- 每当您拍摄尚未具有快照组的基本卷的快照时，System Manager 都会自动创建快照组。此操作还为用于存储后续快照映像的基本卷创建保留容量。
- 每当您为基本卷创建快照计划时，System Manager 都会自动创建快照组。

自动删除

使用快照时，使用默认选项启用自动删除。当快照组达到 32 个图像的快照组限制时，自动删除会自动删除最旧的快照图像。如果关闭自动删除，则最终会超出快照组限制，您必须采取手动操作来配置快照组设置和管理保留容量。

了解 **SANtricity System Manager** 中的 **Snapshot** 计划和 **Snapshot** 一致性组

使用计划收集 Snapshot 映像，并使用 Snapshot 一致性组来管理多个基本卷。

要轻松管理基本卷的 snapshot 操作，可以使用以下功能：

- **Snapshot** 计划 — 为单个基本卷自动执行快照。
- **Snapshot** 一致性组 — 作为一个实体管理多个基本卷。

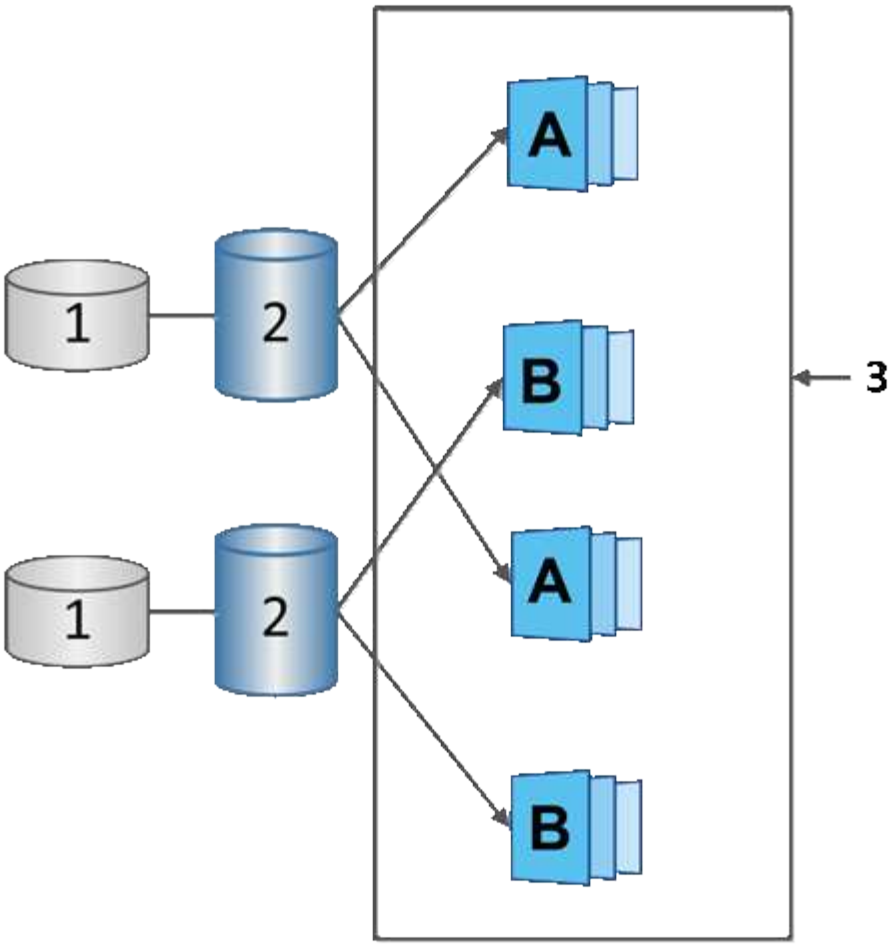
Snapshot 计划

如果要自动为基本卷拍摄 Snapshot，可以创建 Snapshot 计划。例如，您可以定义一个 Snapshot 计划，每周六午夜、每月 1 日或您决定的任何日期和时间拍摄 Snapshot 映像。在单个 Snapshot 计划最多达到 32 个 Snapshot 后，您可以挂起计划的 Snapshot，创建更多保留容量，也可以删除 Snapshot。Snapshot 可以手动删除，也可以通过自动删除过程删除。删除 Snapshot 映像后，额外的保留容量可供重复使用。

快照一致性组

如果要确保同时在多个卷上拍摄 Snapshot 映像，请创建 Snapshot 一致性组。对整个 Snapshot 一致性组执行 Snapshot 映像操作。例如，您可以计划具有相同时间戳的所有卷的同步 Snapshot。Snapshot 一致性组非常适合跨多个卷的应用程序，例如将日志存储在一个卷上而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保留容量。您可以定义一个计划来自动创建每个成员卷的快照映像。



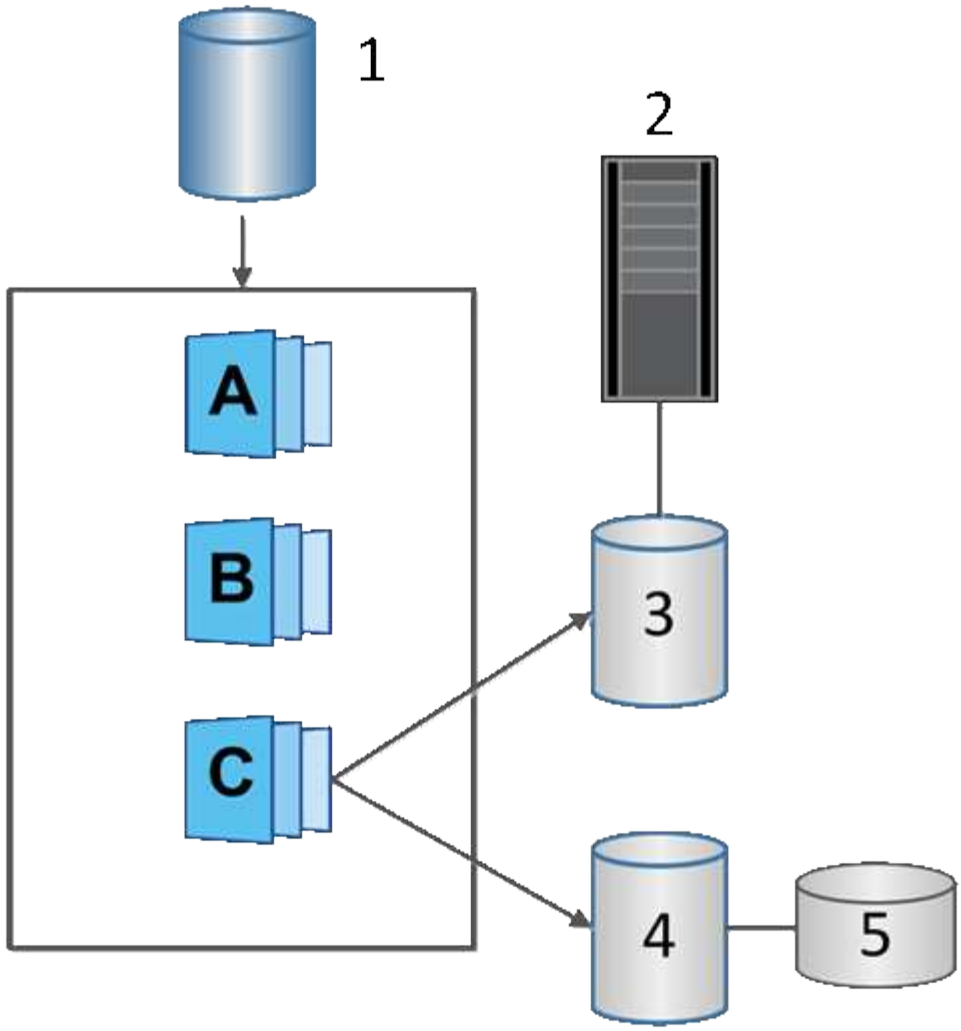
[1] 预留容量；[2] 成员卷；[3] 一致性组 Snapshot 映像

了解 **SANtricity** 软件中的快照卷

如果要读取或写入 snapshot 数据，可以创建 snapshot 卷并将其分配给主机。snapshot 卷与基本卷具有相同的特性（RAID 级别、I/O 特性等）。

创建快照卷时，可以将其指定为只读或_读写访问_。

创建只读快照卷时，无需添加保留容量。创建读写快照卷时，必须添加保留容量以提供写入访问。



[1] 基本卷；[2] 主机；[3] 只读 Snapshot 卷；[4] 读写 Snapshot 卷；[5] 预留容量

了解 **SANtricity** 软件中的快照回滚

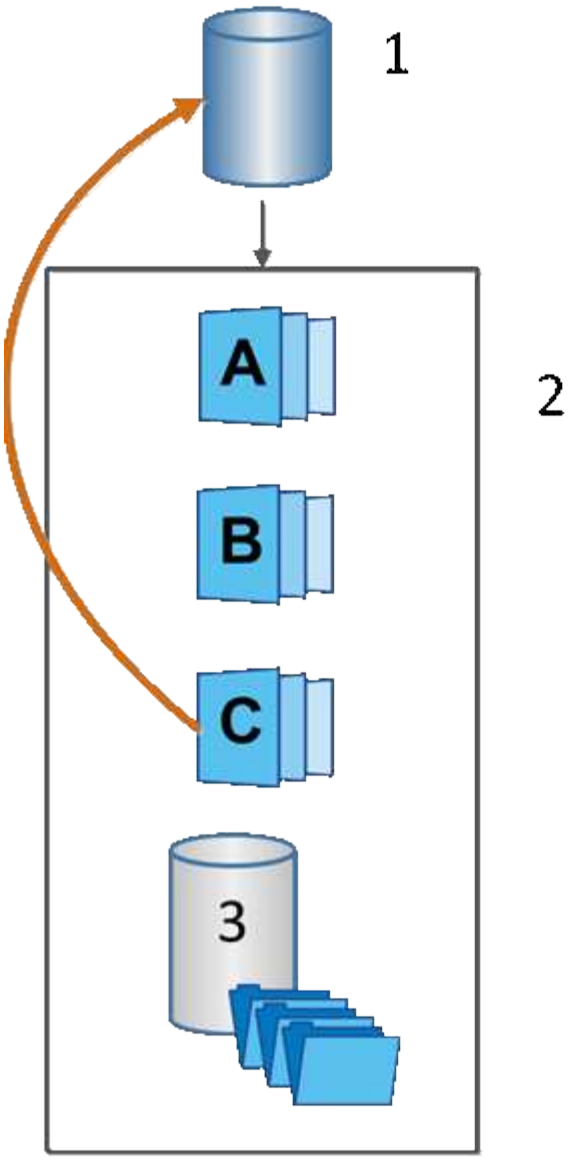
回滚操作将基本卷返回到选定 Snapshot 确定的先前状态。

对于回滚，您可以从以下任意源中选择 Snapshot 映像：

- **Snapshot** 映像回滚，用于基本卷的完全恢复。
- **Snapshot** 一致性组回滚，可用于回滚一个或多个卷。

在回滚过程中，Snapshots 功能将保留组中的所有快照图像。如果 I/O 操作需要，它还允许主机在此过程中访问基本卷。

启动回滚时，后台进程扫描基本卷的逻辑块地址 (LBA)，然后在要还原的回滚快照映像中查找写入时复制数据。由于基本卷可供主机访问以进行读取和写入，并且所有以前写入的数据都可以立即使用，因此保留的容量卷必须足够大，以便在处理回滚时包含所有更改。数据传输继续作为后台操作，直到回滚完成。



[1] 基本卷；[2] 组中的 Snapshot 对象；[3] Snapshot 组保留容量

创建快照和快照对象

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

您可以从基本卷或快照一致性组手动创建快照映像。这也称为 即时快照 或 即时映像。

开始之前

- 基础卷必须是最佳的。
- 驱动器必须处于最佳状态。
- 无法将快照组指定为"`reserved.`"
- 保留容量卷必须具有与快照组的关联基本卷相同的 Data Assurance (DA) 设置。

步骤

1. 请执行以下操作之一以创建快照映像：

   - 选择菜单：Storage[Volumes]。选择对象（基本卷或快照一致性组），然后选择菜单：Copy Services[Create instant snapshot]。
   - 选择菜单：Storage[Snapshots]。选择 **Snapshot Images** 选项卡，然后选择菜单：Create[Instant snapshot]。

     此时将显示创建快照图像对话框。选择对象（基本卷或快照一致性组），然后单击 下一步。如果为卷或快照一致性组创建了以前的快照图像，则系统会立即创建即时快照。否则，如果这是第一次为卷或快照一致性组创建快照图像，则将显示确认创建快照图像对话框。

2. 单击 **Create** 以接受需要保留容量的通知，并继续执行 Reserve Capacity 步骤。

   此时将显示"保留容量"对话框。

3. 使用微调框调整容量百分比，然后单击 **Next** 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，并确认要执行此操作。

   字段详细信息

设置	说明
Snapshot 图像设置	Snapshot 图像限制
如果要在指定限制后自动删除快照图像，请选中此复选框；使用旋转框更改限制。如果清除此复选框，快照图像创建将在 32 个图像后停止。	保留容量设置
在…时提醒我	使用微调框可调整系统在快照组的保留容量接近满时发送警报通知的百分比点。 当快照组的保留容量超过指定阈值时，请使用提前通知来增加保留容量或在剩余空间用完之前删除不必要的对象。
完全保留容量的政策	从下列策略中选择一项： • 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，从而释放快照映像保留容量，以便在组内重复使用。 • 拒绝对基本卷的写入 — 当保留容量达到其最大定义百分比时，系统会拒绝对触发保留容量访问的基本卷的任何 I/O 写入请求。

结果

- System Manager 在"快照图像"表中显示新的快照图像。该表按时间戳和关联的基本卷或快照一致性组列出了新映像。
- 由于以下条件，快照创建可能保持"挂起"状态：
  - 包含此快照映像的基本卷是异步镜像组的成员。
  - 基本卷当前处于同步操作中。快照映像创建在同步操作完成后立即完成。

在 **SANtricity System Manager** 中计划快照映像

您可以创建快照计划，以便在基本卷出现问题时启用恢复并执行计划备份。基本卷或快照一致性组的快照可以在一天中的任何时间按每日、每周或每月计划创建。

开始之前

基本卷必须为 Optimal。

关于此任务

此任务描述如何为现有 Snapshot 一致性组或基本卷创建 Snapshot 计划。

> 您还可以在创建基本卷或 Snapshot 一致性组的 Snapshot 映像的同时创建 Snapshot 计划。

步骤

1. 请执行以下操作之一来创建 Snapshot 计划：
   - 选择菜单：Storage[Volumes]。

     为此 Snapshot 计划选择对象（卷或 Snapshot 一致性组），然后选择菜单：复制服务[创建 Snapshot 计划]。

   - 选择菜单：Storage[Snapshots]。

     选择 **Schedules** 选项卡，然后单击 **Create**。
2. 选择此 Snapshot 计划的对象（卷或 Snapshot 一致性组），然后单击 **Next**。

   此时将显示"创建 Snapshot 计划"对话框。
3. 请执行以下操作之一：
   - 使用另一个 **Snapshot** 对象中先前定义的计划。

     确保显示高级选项。单击*显示更多选项*。单击*Import Schedule*，选择要导入的带有计划的对象，然后单击*Import*。

   - 修改基本或高级选项。

     在对话框右上角，单击 **Show more options** 以显示所有选项，然后参阅下表。

字段详细信息

字段	说明
基本设置	选择天数
为快照图像选择一周中的各个日期。	开始时间
从下拉列表中，为每日 Snapshot 选择新的开始时间（以半小时为间隔提供选择）。默认情况下，开始时间比当前时间提前半小时。	Time zone
从下拉列表中，选择阵列的时区。	高级设置
日 / 月	从下列选项中选择一项： • 每日/每周 — 为同步快照选择单个日期。如果您想要每日计划，也可以选择右上角的 选择所有日期 复选框。 • 每月/每年 — 选择用于同步快照的个别月份。在 **On day(s)** 字段中，输入每月进行同步的日期。有效输入为 **1** 至 **31** 和 **Last**。您可以使用逗号或分号分隔多天。对于包含的日期，请使用连字符。例如：1,3,4,10-15,Last。如果您需要每月计划，也可以选择右上角的 **Select all months** 复选框。
开始时间	从下拉列表中，为每日 Snapshot 选择新的开始时间（以半小时为间隔提供选择）。默认情况下，开始时间比当前时间提前半小时。
Time zone	从下拉列表中，选择阵列的时区。
每天 Snapshot 数 / Snapshot 之间的时间	选择每天要创建的 snapshot 映像数。如果选择多个，请同时选择 snapshot 映像之间的时间间隔。对于多个 snapshot 映像，请确保您有足够的保留容量。
是否立即创建快照映像？	选中此复选框可以创建即时映像，这是在您正在计划的自动映像之外额外创建的。
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. 请执行以下操作之一：
   ◦ 如果对象是 Snapshot 一致性组，请单击*创建*以接受设置并创建 Snapshot 计划。

- 如果对象是卷，请单击 下一步 为 Snapshot 映像分配预留容量。

  卷候选表仅显示支持指定保留容量的候选。保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。

5. 使用微调框为 snapshot 图像分配预留容量。执行以下操作之一：
   - 接受默认设置。

     使用此推荐选项为具有默认设置的 snapshot 图像分配保留容量。

   - 分配您自己的预留容量设置，以满足您的数据存储需求。

     如果更改默认保留容量设置，请单击 **Refresh Candidates** 以刷新您指定的保留容量的候选列表。

     使用以下指南分配预留容量：

     - 保留容量的默认设置为基本卷容量的 40%。通常这个容量就足够了。
     - 所需的容量因 I/O 写入卷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 **Next**。

   此时将显示"编辑设置"对话框。

7. 根据需要编辑 Snapshot 计划的设置，然后单击 完成 。

字段详细信息

设置	说明
Snapshot 映像限制	启用自动删除快照映像时…
如果要在指定限制后自动删除快照图像，请选中此复选框；使用旋转框更改限制。如果清除此复选框，快照图像创建将在 32 个图像后停止。	保留容量设置
在…时提醒我	使用微调框调整当 Snapshot 计划的预留容量接近满时系统发送警报通知的百分比点。 当计划的保留容量超过指定阈值时，请使用提前通知来增加保留容量或在剩余空间用完之前删除不必要的对象。
完全保留容量的政策	从下列策略中选择一项： • 清除最旧的 **snapshot** 映像 — 系统会自动清除最旧的 snapshot 映像，从而释放 snapshot 映像保留容量，以便在 snapshot 组内重复使用。 • 拒绝对基本卷的写入 — 当保留容量达到其最大定义百分比时，系统会拒绝对触发保留容量访问的基本卷的任何 I/O 写入请求。

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

为确保您拥有一致的副本，您可以创建一组名为 *snapshot consistency group* 的多个卷。

此组允许您同时制作所有卷的快照映像，以实现一致性。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，系统会自动创建与此成员卷对应的新快照组。

关于此任务

快照一致性组创建顺序允许您为该组选择成员卷，并为成员卷分配容量。

创建快照一致性组的过程是一个多步骤过程。

步骤 **1**：将成员添加到快照一致性组

选择成员以指定构成快照一致性组的卷集合。您在快照一致性组上执行的任何操作均统一扩展到选定的成员卷。

开始之前

成员卷必须为 Optimal。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Consistency Groups** 选项卡。
3. 选择菜单：Create[Snapshot consistency group]。

   此时将显示"创建快照一致性组"对话框。

4. 选择要作为成员卷添加到快照一致性组的卷。
5. 单击 **Next**，然后转到 步骤 2：为快照一致性组保留容量。

步骤 2：为快照一致性组保留容量

将保留容量关联到快照一致性组。System Manager 根据快照一致性组的属性建议卷和容量。您可以接受建议的保留容量配置或自定义分配的存储。

关于此任务

在"保留容量"对话框中，卷候选表仅显示支持指定保留容量的候选。保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。

步骤

1. 使用微调框为快照一致性组分配保留容量。执行以下操作之一：
   - 接受默认设置。

     使用此推荐选项为具有默认设置的每个成员卷分配保留容量。

   - 分配您自己的预留容量设置，以满足您的数据存储需求。

     使用以下指南分配预留容量。

     - 保留容量的默认设置为基本卷容量的 40%。通常这个容量就足够了。
     - 所需的容量因 I/O 写入卷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： 如果更改默认保留容量设置，请单击 **Refresh Candidates** 以刷新指定保留容量的候选列表。
3. 单击 **Next**，然后转到 步骤 3：编辑快照一致性组的设置。

步骤 3：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

快照一致性组创建顺序允许您为该组选择成员卷，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

设置	说明
Snapshot 一致性组设置	名称
指定快照一致性组的名称。	启用自动删除快照映像时…
如果要在指定限制后自动删除快照图像，请选中此复选框；使用旋转框更改限制。如果清除此复选框，快照图像创建将在 32 个图像后停止。	保留容量设置
在…时提醒我	使用微调框可调整系统在快照一致性组的保留容量接近满时发送警报通知的百分比点。 当快照一致性组的保留容量超过指定阈值时，请使用提前通知来增加保留容量或在剩余空间用完之前删除不必要的对象。
完全保留容量的政策	从下列策略中选择一项： • 清除最旧的快照映像 — 系统会自动清除快照一致性组中最旧的快照映像，从而释放快照映像保留容量，以便在组内重复使用。 • 拒绝对基本卷的写入 — 当保留容量达到其最大定义百分比时，系统会拒绝对触发保留容量访问的基本卷的任何 I/O 写入请求。

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，以提供对卷或快照一致性组的快照映像的主机访问权限。您可以将快照卷指定为只读或读写。

关于此任务

快照卷创建顺序允许您从快照映像创建快照卷，并提供在卷为读/写时分配保留容量的选项。快照卷可以指定为以下卷之一：

- 只读快照卷为主机应用程序提供了对快照映像中包含的数据副本的读取访问权限，但不能修改快照映像。只读快照卷没有关联的保留容量。
- 读写快照卷为主机应用程序提供了对快照映像中包含的数据副本的写入权限。它具有自己的保留容量，用于保存主机应用程序对基本卷所做的任何后续修改，而不会影响引用的快照映像。

创建快照卷的过程是一个多步骤过程。

步骤 1：检查快照卷的成员

选择基本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. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Volumes** 选项卡。
3. 选择 **Create**。

   此时将显示创建快照卷对话框。

4. 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 **Next**。在 **Filter** 字段中使用文本条目以缩小列表范围。

   如果选择的是快照一致性组快照映像，将显示"审阅成员"对话框。

   在查看成员对话框中，查看选定要转换为快照卷的卷列表，然后单击 **Next**。

5. 转至 步骤 2：将快照卷分配给主机。

步骤 2：将快照卷分配给主机

选择特定主机或主机群集以将其分配给快照卷。此分配授予主机或主机群集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

- 有效的主机或主机群集存在于 Hosts 页面下。
- 必须为主机定义主机端口标识符。
- 在创建启用 DA 的卷之前，请验证计划的主机连接是否支持 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，则关联的主机无法访问启用 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量进行特定限制。
- 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。
- 主机或主机群集不能两次使用相同的逻辑单元号 (LUN) 来访问快照卷。您必须使用唯一的 LUN。

如果尝试将卷分配给与主机群集中已建立的主机分配冲突的主机群集，则将卷分配给主机失败。

步骤

1. 在 **Assign to Host** 对话框中，选择要分配给新卷的主机或主机群集。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 **Assign later**。
2. 选择访问模式。请从以下选项中选择一项：

- 读/写 — 此选项为主机提供对快照卷的读/写访问权限，并且需要保留容量。
- 只读 — 此选项为主机提供对快照卷的只读访问权限，并且不需要保留容量。

3. 单击 **Next**，然后执行以下操作之一：
   - 如果快照卷为读/写，将显示"查看容量"对话框。转到 步骤 3：为快照卷保留容量。
   - 如果快照卷为只读，将显示"编辑优先级"对话框。转到 步骤 4：编辑快照卷的设置。

步骤 3：为快照卷保留容量

将保留容量关联到读/写快照卷。System Manager 根据基本卷或快照一致性组的属性建议卷和容量。您可以接受建议的保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快照卷的保留容量。如果您发现快照保留容量大于您需要的容量，则可以减少其大小以释放其他逻辑卷所需的空间。

步骤

1. 使用微调器框为快照卷分配保留容量。

   Volume Candidate 表仅显示支持指定预留容量的候选卷。

   请执行以下操作之一：

   - 接受默认设置。

     使用此推荐选项为具有默认设置的快照卷分配保留容量。

   - 分配您自己的预留容量设置，以满足您的数据存储需求。

     如果更改默认保留容量设置，请单击 **Refresh Candidates** 以刷新您指定的保留容量的候选列表。

     使用以下指南分配预留容量。

     - 保留容量的默认设置为基本卷容量的 40%，通常此容量就足够了。
     - 所需的容量因 I/O 写入卷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"选项将显示在保留容量候选表中。单击 更改候选 以选择备用保留容量候选。
3. 单击 **Next**，然后转到 步骤 4：编辑快照卷的设置。

步骤 4：编辑快照卷的设置

更改快照卷的设置，例如其名称、缓存、保留容量警报阈值等。

关于此任务

您可以将卷添加到固态磁盘 (SSD) 缓存，以提高只读性能。SSD 缓存由一组 SSD 驱动器组成，您可以在存储阵列中将它们逻辑地分组在一起。

步骤

1. 根据需要接受或更改快照卷的设置。

字段详细信息

设置	说明
快照卷设置	名称
指定快照卷的名称。	启用 SSD 缓存
选择此选项可在 SSD 上启用只读缓存。	保留容量设置
在…时提醒我	仅适用于读/写快照卷。 使用微调框可调整系统在快照组的保留容量接近满时发送警报通知的百分比点。 当快照组的保留容量超过指定阈值时，请使用提前通知来增加保留容量或在剩余空间用完之前删除不必要的对象。

2. 查看快照卷配置。单击 返回 进行任何更改。
3. 当您满意快照卷配置后，单击 完成。

管理 Snapshot 计划

在 SANtricity System Manager 中更改快照计划的设置

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相关联，因此预留容量可能会受到计划设置更改的影响。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Schedules** 选项卡。
3. 选择要更改的快照计划，然后单击 **Edit**。

   此时将显示"编辑快照计划"对话框。

4. 执行以下操作之一：
   - 使用另一个快照对象中先前定义的计划 — 单击 导入计划，选择要导入的带有计划的对象，然后单击 导入。
   - 编辑计划设置 — 请参阅下面的字段详细信息。

字段详细信息

设置	说明
日 / 月	从下列选项中选择一项： • 每日/每周 — 为同步快照选择单个日期。如果您想要每日计划，也可以选择右上角的 选择所有日期 复选框。 • 每月/每年 — 选择用于同步快照的个别月份。在 **On day(s)** 字段中，输入每月进行同步的日期。有效输入为 **1** 至 **31** 和 **Last**。您可以使用逗号或分号分隔多天。对于包含的日期，请使用连字符。例如：1,3,4,10-15,Last。如果您需要每月计划，也可以选择右上角的 **Select all months** 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。选择以半小时为增量提供。默认情况下，开始时间比当前时间提前半小时。
Time zone	从下拉列表中，选择存储阵列的时区。
每天快照数 快照之间的时间间隔	选择每天要创建的快照映像数。 如果选择多个，请同时选择还原点之间的时间。对于多个还原点，请确保您有足够的保留容量。
开始日期 结束日期 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。

5. 单击 **Save**。

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

当需要节省存储空间时，可以暂时暂停快照图像的计划收集。此方法比删除和稍后重新创建快照计划更有效。

关于此任务

快照计划的状态保持暂停状态，直到您使用 **Activate** 选项恢复计划的快照活动。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 如果尚未显示，请单击 **Schedules** 选项卡。

   时间表列在页面上。

3. 选择要挂起的活动快照计划，然后单击 **Activate / Suspend**。

状态列状态变为 挂起，快照计划停止收集所有快照图像。

4. 要恢复收集快照映像，请选择要恢复的挂起快照计划，然后单击 激活/挂起。

   状态列状态更改为 **Active**。

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

如果不想再收集快照图像，则可以删除现有的快照计划。

关于此任务

删除快照计划时，不会随之删除关联的快照图像。如果您认为快照图像的集合可能会在某个时候恢复，则应暂停快照计划，而不是将其删除。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Schedules** 选项卡。
3. 选择要删除的快照计划，并确认此操作。

结果

系统从基本卷或快照一致性组中删除所有计划属性。

管理 **snapshot** 镜像

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、保留容量和关联对象。

关于此任务

快照映像的关联对象包括此快照映像是其还原点的基本卷或快照一致性组、关联的快照组以及从快照映像创建的任何快照卷。使用快照设置来确定是否要复制或转换快照映像。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Images** 选项卡。
3. 选择要查看的快照映像，然后单击 **View Settings**。

   此时将显示"快照图像设置"对话框。

4. 查看快照映像的设置。

在 **SANtricity System Manager** 中启动基础卷的快照映像回滚

可以执行回滚操作，以更改基本卷的内容，使其与 Snapshot 映像中保存的内容相匹配。

回滚操作不会改变与基本卷相关联的 snapshot 映像的内容。

开始之前

- 有足够的保留容量可用于启动回滚操作。
- 选定的快照映像为最佳，选定的卷为最佳。
- 所选卷没有正在进行的回滚操作。

关于此任务

回滚启动顺序允许您在基本卷的快照映像上开始回滚，同时提供添加存储容量的选项。一次不能为基本卷启动多个回滚操作。

主机可以立即访问新的回滚基本卷，但在回滚开始后，现有的基本卷不允许主机读写访问。您可以在开始回滚之前创建基本卷的 Snapshot，以保留用于恢复的预回滚基本卷。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Images** 选项卡。
3. 选择 Snapshot 映像，然后选择菜单：Rollback[Start]。

   此时将显示"确认开始回滚"对话框。

4. 可选： 如有必要，选择 **Increase Capacity** 选项。

   此时将显示"增加保留容量"对话框。

   a. 使用微调框调整容量百分比。

      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 **Increase**。
5. 确认您要执行此操作，然后单击 **Rollback**。

结果

System Manager 执行以下操作：

- 使用选定快照映像上保存的内容还原卷。
- 使回滚卷立即可用于主机访问。无需等待回滚操作完成。

完成后

选择菜单：Home[View Operations in Progress] 以查看回滚操作的进度。

如果回滚操作不成功，则操作暂停。您可以恢复暂停的操作，如果仍然不成功，请按照 Recovery Guru 程序更正问题或联系技术支持。

在 **SANtricity System Manager** 中为 **Snapshot** 一致性组成员卷启动 **Snapshot** 映像回滚

可以执行回滚操作，以更改 snapshot 一致性组成员卷的内容，使其与 snapshot 映像中保存的内容相匹配。

回滚操作不会更改与 Snapshot 一致性组相关联的 Snapshot 映像的内容。

开始之前

- 有足够的保留容量可用于启动回滚操作。
- 选定的快照映像为最佳，选定的卷为最佳。
- 所选卷没有正在进行的回滚操作。

关于此任务

回滚启动序列允许您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。一次不能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，但在回滚启动后，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，以保留用于恢复目的的预回滚基本卷。

开始回滚快照一致性组的快照映像的过程是一个多步骤过程。

步骤 1：选择成员

必须选择要回滚的成员卷。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Images** 选项卡。
3. 选择快照一致性组快照映像，然后选择菜单：Rollback[Start]。

   此时将显示"开始回滚"对话框。

4. 选择成员卷。
5. 单击 **Next**，然后执行以下操作之一：
   - 如果任何所选成员卷与存储快照图像的多个保留容量对象相关联，将显示"查看容量"对话框。转到 步骤 2：审查容量。
   - 如果所选成员卷均未与存储快照图像的多个保留容量对象相关联，则将显示"编辑优先级"对话框。转到 步骤 3：编辑优先级。

步骤 2：审查容量

如果选择了与多个保留容量对象相关联的成员卷，例如快照组和保留容量卷，则可以查看并增加回滚卷的保留容量。

步骤

1. 在保留容量非常低（或为零）的任何成员卷旁边，单击 **Edit** 列中的 **Increase capacity** 链接。

   此时将显示"增加保留容量"对话框。

2. 使用微调框调整容量百分比，然后单击 **Increase**。

   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 **Next**，然后转到 步骤 3：编辑优先级。

   此时将显示"编辑优先级"对话框。

步骤 3：编辑优先级

如果需要，您可以编辑回滚操作的优先级。

关于此任务

回滚优先级确定以牺牲系统性能为代价将多少系统资源专用于回滚操作。

步骤

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

结果

System Manager 执行以下操作：

- 使用选定快照映像上保存的内容还原快照一致性组成员卷。
- 使回滚卷立即可用于主机访问。无需等待回滚操作完成。

完成后

选择菜单：Home[View Operations in Progress] 以查看回滚操作的进度。

如果回滚操作不成功，则操作暂停。您可以恢复暂停的操作，如果仍然不成功，请按照 Recovery Guru 程序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，则该操作将自动暂停。您可以恢复处于暂停状态的回滚操作。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Images** 选项卡。
3. 突出显示已暂停的回滚，然后选择菜单：Rollback[Resume]。

   操作恢复。

结果

System Manager 执行以下操作：

- 如果回滚操作成功恢复，您可以在"正在进行的操作"窗口中查看回滚操作的进度。
- 如果回滚操作不成功，则操作再次暂停。您可以按照 Recovery Guru 程序更正问题或联系技术支持。

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（正在复制数据）、挂起的回滚（在等待启动资源的挂起队列中）或由于错误而暂停的回滚。

关于此任务

当您取消正在执行的回滚操作时，基本卷将恢复到不可用状态并显示为失败。因此，仅当存在恢复基本卷内容的恢复选项时，才考虑取消回滚操作。

> 如果快照映像所在的快照组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. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Images** 选项卡。
3. 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。
4. 单击 是 确认。

结果

System Manager 停止回滚操作。基本卷可用，但可能存在不一致或不完整的数据。

完成后

取消回滚操作后，必须采取以下操作之一：

- 重新初始化基本卷的内容。
- 执行新的回滚操作，使用在取消回滚操作中使用的相同快照映像或不同的快照映像来还原基本卷。

在 SANtricity System Manager 中删除快照映像

您可以删除快照映像以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图像，也可以从具有相同创建时间戳的快照一致性组中删除快照图像。您还可以从快照组中删除快照图像。

如果快照映像不是关联的基本卷或快照一致性组的最旧快照映像，则无法删除该快照映像。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Images** 选项卡。
3. 选择要删除的快照映像，并确认要执行此操作。

   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，并确认要执行此操作。

4. 单击 **Delete**。

结果

System Manager 执行以下操作：

- 从存储阵列中删除快照图像。
- 释放保留容量，以便在快照组或快照一致性组内重用。
- 禁用已删除快照映像存在的所有关联快照卷。
- 从快照一致性组删除中，将与已删除快照映像关联的任何成员卷移动到 Stopped 状态。

管理 Snapshot 一致性组

将成员卷添加到 **SANtricity System Manager** 中的快照一致性组

可以向现有快照一致性组添加新成员卷。添加新成员卷时，还必须为成员卷保留容量。

开始之前

- 成员卷必须为 Optimal。
- 快照一致性组的卷数必须小于允许的最大数量（由您的配置定义）。
- 每个保留容量卷必须具有与关联成员卷相同的数据保证 (DA) 和安全设置。

关于此任务

您可以将标准卷或精简卷添加到快照一致性组。基本卷可以驻留在池或卷组中。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Consistency Groups** 选项卡。

   该表显示与存储阵列关联的所有快照一致性组。

3. 选择要修改的快照一致性组，然后单击 **Add Members**。

   此时将显示"添加成员"对话框。

4. 选择要添加的成员卷，然后单击 **Next**。

   此时将显示 Reserve Capacity（保留容量）步骤。Volume Candidate（候选卷）表仅显示支持指定保留容量的候选卷。

5. 使用微调器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。

     使用此推荐选项为具有默认设置的成员卷分配保留容量。

   - 分配您自己的预留容量设置，以满足您的数据存储需求。

     如果更改默认保留容量设置，请单击 **Refresh Candidates** 以刷新您指定的保留容量的候选列表。

使用以下指南分配预留容量。

- 保留容量的默认设置为基本卷容量的 40%，通常此容量就足够了。
- 所需的容量因 I/O 写入卷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 **Finish** 以添加成员卷。

从 **SANtricity System Manager** 中的快照一致性组中删除成员卷

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. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Consistency Groups** 选项卡。
3. 通过选择要修改的快照一致性组旁边的加号 (+) 展开。
4. 选择要删除的成员卷，然后单击 **Remove**。
5. 确认您要执行此操作，然后单击 **Remove**。

结果

System Manager 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。

更改 **SANtricity System Manager** 中快照一致性组的设置

当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时，请更改快照一致性组的设置。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Consistency Groups** 选项卡。
3. 选择要编辑的快照一致性组，然后单击 **View/Edit Settings** 。

   此时将显示 Snapshot Consistency Group Setting 对话框。

4. 根据需要更改快照一致性组的设置。

字段详细信息

设置	说明
Snapshot 一致性组设置	名称
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图像，请选中此复选框；使用旋转框更改限制。如果清除此复选框，快照图像创建将在 32 个图像后停止。	Snapshot 图像限制
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
成员卷	您可以查看与快照一致性组关联的成员卷的数量。

5. 单击 **Save**。

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

确认所有成员卷的映像不再需要用于备份或测试目的。

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. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Consistency Groups** 选项卡。
3. 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快照一致性组对话框。

4. 确认您要执行此操作，然后单击 **Delete**。

结果

System Manager 执行以下操作：

- 从快照一致性组中删除所有现有的快照映像和快照卷。
- 删除快照一致性组中每个成员卷存在的所有关联快照映像。
- 删除快照一致性组中每个成员卷存在的所有关联快照卷。
- 删除快照一致性组中每个成员卷的所有关联保留容量（如果选择）。

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，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。

转换为可读写访问的快照卷包含其自己的保留容量。此容量用于保存主机应用程序对基本卷所做的任何后续修改，而不影响引用的快照映像。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Volumes** 选项卡。

   此时会显示 Snapshot Volumes 表，并显示与存储阵列关联的所有快照卷。

3. 选择要转换的只读快照卷，然后单击 **Convert to Read/Write**。

   此时将显示转换为读/写对话框，并激活 **Reserve Capacity** 步骤。Volume Candidate 表仅显示支持指定保留容量的候选项。

4. 要为读写快照卷分配保留容量，请执行以下操作之一：
   - 接受默认设置 — 使用此推荐选项为具有默认设置的快照卷分配保留容量。
   - 分配您自己的预留容量设置以满足您的数据存储需求 — 使用以下指南分配预留容量。
     - 保留容量的默认设置为基本卷容量的 40%，通常此容量就足够了。
     - 所需的容量因 I/O 写入卷的频率和大小而异。
5. 选择 **Next** 以查看或编辑设置。

   此时将显示"编辑设置"对话框。

6. 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

设置	说明
保留容量设置	在…时提醒我

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重命名它，启用或禁用 SSD 缓存，或更改主机、主机群集或逻辑单元号 (LUN) 分配。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 单击 **Snapshot Volumes** 选项卡。
3. 选择要更改的快照卷，然后单击 **View/Edit Settings**。

   此时将显示"快照卷设置"对话框。

4. 根据需要查看或编辑快照卷的设置。

   字段详细信息

设置	说明
Snapshot 卷	名称
您可以更改快照卷的名称。	已分配给
您可以更改快照卷的主机或主机集群分配。	LUN
可以更改快照卷的 LUN 分配。	SSD 缓存
您可以启用/禁用固态硬盘 (SSD) 上的只读缓存。	关联对象
Snapshot 图像	您可以查看与快照卷关联的快照映像。快照映像是在特定时间点捕获的卷数据的逻辑副本。像还原点一样，快照映像允许您回滚到已知良好的数据集。虽然主机可以访问快照映像，但它不能直接读取或写入快照映像。
基础卷	您可以查看与快照卷关联的基本卷。基本卷是创建快照映像的源。它可以是厚卷或精简卷，通常分配给主机。基本卷可以驻留在卷组或磁盘池中。
Snapshot 组	您可以查看与快照卷关联的快照组。快照组是来自单个基本卷的快照图像的集合。

在 **SANtricity System Manager** 中复制快照卷

您可以在快照卷或快照一致性组快照卷上执行 Copy Volume 过程。

关于此任务

您可以将快照卷复制到目标卷，就像在正常的 Copy Volume 操作中一样。但是，在复制卷过程中，快照卷不能保持联机状态。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Volumes** 选项卡。

   此时会显示 Snapshot Volumes 表，并显示与存储阵列关联的所有快照卷。

3. 选择要复制的快照卷，然后选择 **Copy Volume**。

   此时将显示"复制卷"对话框，提示您选择目标。

4. 选择要用作复制目标的目标卷，然后单击 **Finish**。

在 **SANtricity System Manager** 中重新创建快照卷

您可以重新创建以前禁用的快照卷或快照一致性组快照卷。重新创建快照卷所用的时间要少于创建新卷所用的时间。

开始之前

- 快照卷必须处于"最佳"或"已禁用"状态。
- 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禁用状态。

关于此任务

无法重新创建单个成员快照卷；只能重新创建整个快照一致性组快照卷。

> 如果快照卷或快照一致性组快照卷是联机复制关系的一部分，则无法在该卷上执行重新创建选项。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Volumes** 选项卡。

   此时会显示 Snapshot Volumes 表，并显示与存储阵列关联的所有快照卷。

3. 选择要重新创建的快照卷，然后选择菜单：Uncommon Tasks[Recreate]。

   此时将显示"重新创建快照卷"对话框。

4. 从下列选项中选择一项：
   - 从卷 **<name>** 创建的现有快照映像

     选择此选项以指示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

选择此选项以创建要从中重新创建快照卷的新快照映像。

5. 单击 **Recreate**。

结果

System Manager 执行以下操作：

- 删除任何关联快照存储库卷上的所有 `write` 数据。
- 快照卷或快照一致性组快照卷参数与先前禁用的卷参数保持相同。
- 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

当您不再需要快照卷或想要暂时停止使用快照一致性组中的快照卷时，可以禁用快照卷或快照一致性组中的快照卷。

关于此任务

如果满足以下条件之一，请使用禁用选项：

- 您暂时已完成快照卷或快照一致性组快照卷。
- 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），并希望保留相关的保留容量，因此无需再次创建它。
- 您希望通过停止对读写快照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被指定为读写，则此选项还允许您停止对其关联的保留容量卷的任何进一步写入活动。如果决定重新创建快照卷或快照一致性组快照卷，则必须从相同的基本卷中选择快照映像。

如果快照卷或快照一致性组快照卷是联机复制关系的一部分，则无法在该卷上执行 Disable 选项。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Volumes** 选项卡。

   System Manager 会显示与存储阵列关联的所有快照卷。

3. 选择要禁用的快照卷，然后选择菜单：Uncommon Tasks[Disable]。
4. 确认您要执行此操作，然后单击 **Disable**。

结果

- 快照卷与其基本卷保持关联。
- 快照卷保留其全球通用名称 (WWN)。
- 如果为读写，快照卷将保留其关联的预留容量。
- 快照卷保留所有主机分配和访问权限。但是，读写请求失败。
- 快照卷与其快照映像失去关联。

在 **SANtricity System Manager** 中删除快照卷

您可以删除不再需要用于备份或软件应用程序测试目的的快照卷或快照一致性组快照卷。

还可以指定是删除与 `read-write`快照卷关联的快照保留容量卷，还是将快照保留容量卷保留为未分配的卷。

关于此任务

删除基本卷会自动删除任何关联的快照卷或一致性组快照卷。您无法删除处于 **In Progress** 状态的卷副本中的快照卷。

步骤

1. 选择菜单：Storage[Snapshots]。
2. 选择 **Snapshot Volumes** 选项卡。

   System Manager 会显示与存储阵列关联的所有快照卷。
3. 选择要删除的快照卷，然后选择菜单：Uncommon Tasks[Delete]。
4. 确认您要执行此操作，然后单击 **Delete**。

结果

System Manager 执行以下操作：

- 删除所有成员快照卷（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

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

为什么我没有看到所有的卷、主机或主机集群?

具有启用 DA 的基本卷的快照卷没有资格分配给不支持数据保障 (DA) 的主机。必须先在基本卷上禁用 DA，然后才能将快照卷分配给不支持 DA 的主机。

对于要向其分配快照卷的主机，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，则主机不支持 DA。
- 如果主机群集至少有一个主机成员不具备 DA 功能，则该主机群集不具备 DA 功能。

> 无法在与快照（一致性组、快照组、快照映像和快照卷）、卷副本和镜像关联的卷上禁用 DA。在基本卷上禁用 DA 之前，必须删除所有关联的保留容量和快照对象。

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。快照映像使用最少的存储空间。

快照图像数据的存储方式如下：

- 创建快照映像时，它与基本卷完全匹配。拍摄快照后，当基本卷上的任何块或块集发生第一次写入请求时，原始数据将在新数据写入到基本卷之前复制到快照保留容量。
- 后续快照仅包括自创建第一个快照映像以来已更改的数据块。每次后续的写入时复制操作都会将即将在基本卷上覆盖的原始数据保存到快照保留容量，然后再将新数据写入到基本卷。

为什么要使用快照映像？

您可以使用快照来防止意外或恶意的数据丢失或损坏，并允许从中恢复。

选择一个基本卷或一组基本卷（称为快照一致性组），然后通过以下一种或多种方式捕获快照映像：

- 您可以创建单个基本卷的快照映像或由多个基本卷组成的快照一致性组。
- 您可以手动拍摄快照，也可以为基本卷或快照一致性组创建计划，以自动捕获定期快照映像。
- 您可以创建快照映像的主机可访问快照卷。
- 您可以执行回滚操作以还原快照图像。

系统保留多个快照图像作为还原点，您可以使用它们在特定时间点回滚到已知良好的数据集。回滚功能可防止意外删除数据和数据损坏。

可以使用哪些类型的卷进行快照？

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。基本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拍摄快照映像，请创建一个快照一致性组。

例如，由多个卷组成的数据库需要保持一致以进行恢复，因此需要快照一致性组来收集所有卷的协调快照，并使用它们来还原整个数据库。

快照一致性组中包含的卷称为 成员卷。

可以在快照一致性组上执行以下快照操作：

- 创建快照一致性组的快照映像以获取成员卷的同时映像。
- 为快照一致性组创建一个计划，以自动捕获成员卷的定期同时映像。
- 创建快照一致性组映像的主机可访问快照卷。
- 对快照一致性组执行回滚操作。

什么是快照卷？什么时候需要保留容量？

快照卷允许主机访问快照映像中的数据。快照卷包含其自己的保留容量，该容量可保存对基本卷的任何修改，而不会影响原始快照映像。主机无法读取或写入快照映像。如果要读取或写入快照数据，请创建快照卷并将其分配给主机。

您可以创建两种类型的快照卷。快照卷的类型决定它是否使用保留容量。

- 只读 — 创建为只读的快照卷为主机应用程序提供了对快照映像中包含的数据副本的读取访问权限。只读快照卷不使用保留容量。

- 读写 — 创建为读写的快照卷允许您对快照卷进行更改，而不会影响引用的快照映像。读写快照卷使用保留容量来存储这些更改。您可以随时将只读快照卷转换为读写卷。

什么是快照组?

快照组是单个关联基本卷的时间点快照映像的集合。

System Manager 将快照映像组织成_快照组_。快照组无需用户操作，但您可以随时调整快照组上的保留容量。此外，当满足以下条件时，可能会提示您创建保留容量：

- 每当您拍摄尚未具有快照组的基本卷的快照时，System Manager 都会自动创建快照组。这将为用于存储后续快照映像的基本卷创建保留容量。
- 每当您为基本卷创建快照计划时，System Manager 都会自动创建快照组。

为什么要禁用快照卷?

如果要将不同的快照卷分配给快照映像，请禁用快照卷。可以保留禁用的快照卷供以后使用。

如果您不再需要快照卷或一致性组快照卷，并且不打算在以后重新创建它，则应删除该卷，而不是禁用它。

什么是禁用状态?

处于禁用状态的快照卷当前未分配给快照映像。要启用快照卷，必须使用重新创建操作将新的快照映像分配给禁用的快照卷。

快照卷特性由分配给它的快照映像定义。处于已禁用状态的快照卷上的读写活动已挂起。

为什么要暂停快照计划?

当计划被暂停时，计划的快照映像创建不会发生。您可以暂停快照计划以节省存储空间，然后在以后恢复计划的快照。

如果不需要快照计划，则应删除该计划，而不是将其挂起。

镜像

概述

了解 **SANtricity** 软件中的异步镜像

异步镜像功能为本地存储阵列和远程存储阵列之间的数据复制提供了控制器级、基于固件的机制。

什么是异步镜像?

Asynchronous mirroring 捕获特定时间点的主卷的状态，并仅复制自上次图像捕获以来已更改的数据。可以立即更新主站点，并在带宽允许的情况下更新辅助站点。当网络资源可用时，信息将被缓存并稍后发送。

异步镜像是基于每个卷创建的，但在组级别进行管理，允许您将不同的远程镜像卷与给定存储阵列上的任何主卷相关联。这种类型的镜像非常适合满足不间断操作的需求，并且一般来说，对于周期性流程来说，网络效率要高

得多。

了解详情：

- "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。

了解详情：

- "使用异步镜像的要求"
- "异步镜像卷的工作流程"
- "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内容"
- "创建镜像对之前需要了解的内容"
- "异步镜像与同步镜像的区别"

了解 **SANtricity** 软件中的同步镜像

同步镜像功能提供远程存储阵列之间的在线实时数据复制。

此功能在 EF600/EF600C 或 EF300/EF300C 存储系统中不可用。

什么是同步镜像？

同步镜像 实时复制数据卷，以确保连续可用性。存储阵列控制器管理镜像操作，对主机和软件应用程序透明。

这种类型的镜像非常适合业务连续性目的，例如灾难恢复。

了解详情：

- "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。

了解详情：

- "使用同步镜像的要求"
- "同步镜像卷的工作流程"
- "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内容"
- "异步镜像与同步镜像的区别"

异步概念

异步镜像在 **SANtricity System Manager** 中的工作原理

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可能因数据损坏或丢失而导致的停机时间。

异步镜像捕获特定时间点的主卷的状态，并仅复制自上次图像捕获以来发生变化的数据。可以立即更新主站点，并在带宽允许的情况下更新辅助站点。当网络资源可用时，信息将被缓存并稍后发送。

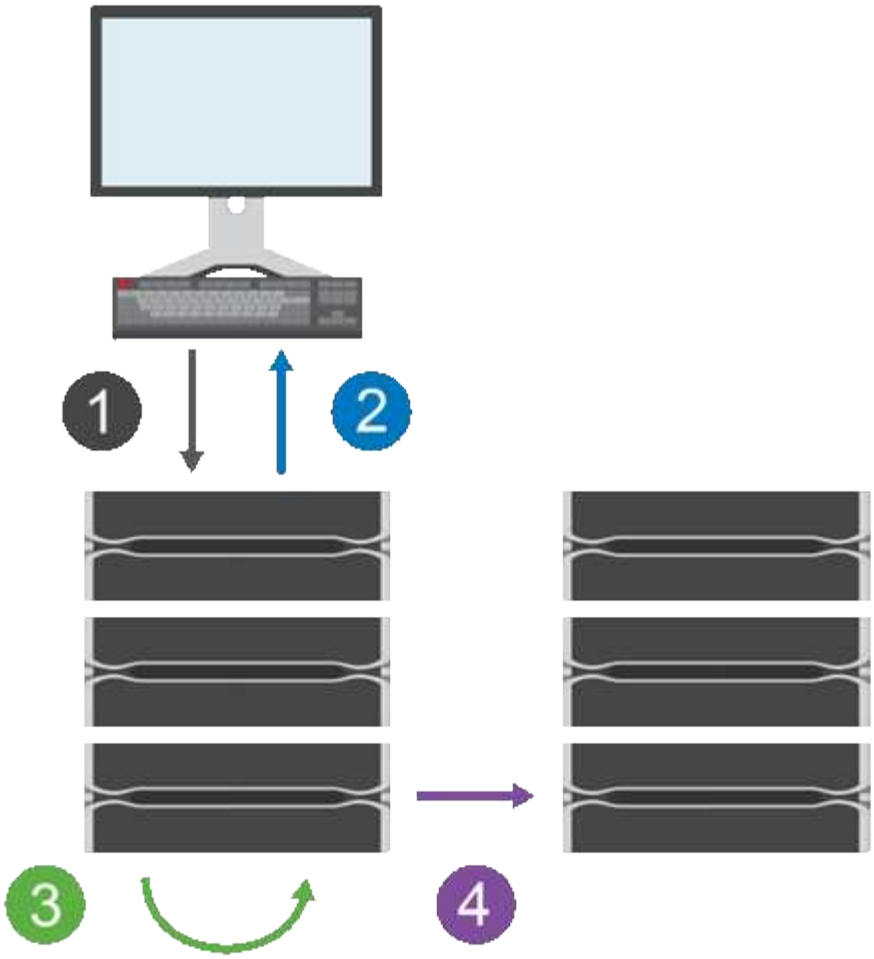
这种类型的镜像非常适合满足不间断操作的需求，一般来说，对于定期流程（如备份和存档），其网络效率要高得多。使用异步镜像的原因包括：

- 远程备份整合。
- 防范局部或广域灾害。
- 对实时数据的时间点映像进行应用程序开发和测试。

异步镜像会话

异步镜像捕获特定时间点的主卷的状态，并仅复制自上次图像捕获以来发生变化的数据。异步镜像允许立即更新主站点，并在带宽允许的情况下更新辅助站点。信息将被缓存并在网络资源可用时稍后发送。

活动异步镜像会话中有四个主要步骤。



1. 写入操作首先发生在主卷的存储阵列上。
2. 此操作的状态将返回给主机。
3. 记录并跟踪主卷上的所有更改。
4. 所有更改都作为后台进程发送到辅助卷的存储阵列。

根据定义的同步间隔重复这些步骤，或者如果没有定义间隔，则可以手动重复这些步骤。

异步镜像仅以设置的时间间隔将数据传输到远程站点，因此本地 I/O 不会受到慢速网络连接的影响。由于此传输未绑定到本地 I/O，因此不会影响应用程序性能。因此，异步镜像可以使用较慢的连接（如 iSCSI），并在本地和远程存储系统之间运行较长的距离。

存储阵列必须具有 7.84 的最低固件版本。（它们可以各自运行不同的 OS 版本。）

镜像一致性组和镜像对

您创建镜像一致性组，以建立本地存储阵列和远程存储阵列之间的镜像关系。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辅助卷。

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。包含辅助卷的存储阵列通常位于辅助站点，并保存数据的副本。辅助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，还可以定义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。

创建镜像一致性组时，还要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。

当主卷的存储阵列无法将数据写入辅助卷时，镜像对中的主卷和辅助卷可能会变得不同步。这种情况可能是由以下问题引起的：

- 本地和远程存储阵列之间的网络问题。
- 出现故障的辅助卷。
- 正在镜像对上手动挂起同步。
- 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。

保留容量和异步镜像

当未发生同步时，保留容量用于跟踪主卷和辅助卷之间的差异。它还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其自己的保留容量。

配置和管理

要启用和配置两个阵列之间的镜像，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适用于您的存储阵列。

术语	说明
本地存储阵列	本地存储阵列是您要执行操作的存储阵列。 当您在本地角色列中看到 **Primary** 时，它指示存储阵列包含在镜像关系中占有主要角色的卷。当您在本地角色列中看到 **Secondary** 时，它指示存储阵列包含在镜像关系中具有辅助角色的卷。
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，一个主卷和一个辅助卷。 在异步镜像中，镜像对始终属于镜像一致性组。写入操作首先执行到主卷，然后复制到辅助卷。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。

术语	说明
远程存储阵列	远程存储阵列通常被指定为辅助站点，它通常在镜像配置中保存数据的副本。
预留容量	保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。
角色更改	角色变更是指将主要角色分配给辅助卷，反之亦然。
二级卷	镜像对的辅助卷通常位于辅助站点，并保存数据的副本。
同步	在本地存储阵列和远程存储阵列之间的初始同步时进行同步。当通信中断后主卷和辅助卷不同步时，也会发生同步。当通信链路再次工作时，任何未复制的数据都将同步到辅助卷的存储阵列。

在 **SANtricity** 软件中异步镜像卷

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，该组是本地阵列上的主卷和远程阵列上的辅助卷的容器。主卷和辅助卷称为"镜像对"。如果是首次创建镜像一致性组，请指定要执行手动同步还是计划同步。
   c. 从本地存储阵列中选择一个主卷，然后确定其保留容量。保留容量是用于复制操作的物理分配容量。
   d. 选择远程存储阵列作为传输的目标、辅助卷，然后确定其保留容量。
   e. 开始从主卷到辅助卷的初始数据传输。根据卷的大小，此初始传输可能需要几个小时。
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。完成镜像后，镜像对的状态为"最佳"。
3. *可选：*您可以在 System Manager 中重新安排或手动执行后续数据传输。仅新的和更改的数据块从主卷传输到辅助卷。

> 由于异步复制是周期性的，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

要启用和配置两个阵列之间的镜像，必须使用 Unified Manager 界面。Unified Manager 与 Web Services Proxy 一起安装在主机系统上。

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

存储阵列

- 您必须有两个存储阵列。
- 每个存储阵列必须有两个控制器。
- 必须在 Unified Manager 中发现两个存储阵列。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。
- 您的本地和远程存储阵列通过光纤通道结构或 iSCSI 接口连接。

支持的连接

异步镜像可以使用 FC 或 iSCSI 连接，或者同时使用两者进行本地和远程存储系统之间的通信。在创建镜像一致性组时，如果 FC 和 iSCSI 都连接到远程存储阵列，管理员可以为该组选择 FC 或 iSCSI。不存在从一种通道类型到另一种通道类型的故障转移。

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辅助端。

- 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，则编号最高的端口在 HIC 上。登录到专用端口的任何主机都已注销，并且不接受任何主机登录请求。此端口上的 I/O 请求仅接受来自参与镜像操作的控制器。

  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 结构环境。特别是，不支持 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** 接口进行镜像

  与 FC 不同，iSCSI 不需要专用端口。在 iSCSI 环境中使用异步镜像时，不必将存储阵列的任何前端 iSCSI 端口专用于异步镜像；这些端口为异步镜像流量和主机到阵列 I/O 连接共享。

  控制器维护 iSCSI 启动程序尝试与之建立会话的远程存储系统列表。成功建立 iSCSI 连接的第一个端口用于与该远程存储阵列的所有后续通信。如果通信失败，将尝试使用所有可用端口进行新会话。

  iSCSI 端口是逐个端口在阵列级别配置的。用于配置消息传递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
- 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辅助端。由于异步镜像适用于延迟更高、成本更低的网络，因此 iSCSI（因此基于 TCP/IP）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；这些端口为异步镜像流量和主机到阵列 I/O 连接共享

> 使用 iSCSI 协议时，E4000 不支持异步镜像。

镜像卷候选项

- 在异步镜像对的主卷和辅助卷上，RAID 级别、缓存参数和段大小可以不同。

> 对于 EF600 和 EF300 控制器，异步镜像对的主卷和辅助卷必须匹配相同的协议、托盘级别、段大小、安全类型和 RAID 级别。不符合条件的异步镜像对将不会出现在可用卷列表中。

- 辅助卷必须至少与主卷一样大。
- 一个卷只能参与一个镜像关系。
- 候选卷必须共享相同的数据安全功能。
  - 如果主卷支持 FIPS，则辅助卷必须支持 FIPS。
  - 如果主卷具有 FDE 功能，则辅助卷必须具有 FDE 功能。
  - 如果主卷未使用 Drive Security，则辅助卷不得使用 Drive Security。
- 主卷和辅助卷必须共享相同的驱动器类型。不支持在主卷和辅助卷之间混合使用 NVMe 和 SAS 驱动器。
- 主卷和辅助卷不得启用 Resource Partitioning。

预留容量

- 镜像对中的主卷和辅助卷需要保留容量卷来记录写入信息，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辅助卷都需要额外的保留容量，因此您必须确保镜像关系中的两个存储阵列都有可用的空闲容量。
- 保留容量卷必须与其关联的镜像卷共享相同的驱动器类型。
  - 如果在 NVMe 驱动器上创建保留容量卷，则还必须在 NVMe 驱动器上创建其镜像卷。
  - 如果在 SAS 驱动器上创建保留容量卷，则还必须在 SAS 驱动器上创建其镜像卷。

驱动器安全功能

- 如果使用具有安全功能的驱动器，则主卷和辅助卷必须具有兼容的安全设置。此限制未强制执行；因此，您必须自己验证。
- 如果使用具有安全功能的驱动器，则主卷和辅助卷应使用相同的驱动器类型。此限制未强制执行；因此，您

必须自己验证。

- 如果使用数据保障 (DA)，则主卷和辅助卷必须具有相同的 DA 设置。

在 **SANtricity System Manager** 中查看异步镜像状态

镜像状态定义了镜像一致性组和镜像卷对的状态。

镜像一致性组的状态

状态	说明
正在同步（初始同步）	镜像卷对之间已完成的初始数据同步进度。 在初始同步期间，卷可以转换为以下状态：降级/失败/最佳/未知。
正在同步（间隔同步）	已在镜像卷对之间完成的定期数据同步的进度。
系统已挂起	存储系统在镜像一致性组级别暂停所有镜像对上的数据同步。 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	用户在镜像一致性组级别暂停所有镜像对上的数据同步。 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，数据同步过程已暂停。
孤立	当一致性镜像组中的成员卷已在一致性镜像组的一侧（主侧或辅助侧）被删除但未在另一侧删除时，就会存在孤立的镜像对卷。 当恢复阵列间通信且镜像配置的两侧协调镜像参数时，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。
角色变更待定/正在进行中	镜像一致性组之间的角色更改处于待处理状态或正在进行中。 角色反转更改（更改为主要角色或次要角色）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。

状态	说明
角色冲突	由于角色更改操作期间本地存储阵列和远程存储阵列之间的通信问题，镜像一致性组之间发生角色冲突。 当通信问题得到解决时，会发生角色冲突。使用 Recovery Guru 从此错误中恢复。 解决角色冲突时不允许强制提升。

镜像对的状态

镜像对的状态指示主卷和辅助卷上的数据是否已同步。

状态	说明
正在同步	镜像对之间已完成的初始或定期数据同步的进度。 有两种类型的同步：初始同步和定期同步。初始同步进度也会显示在"长期运行操作"对话框中。
最佳	镜像对中的卷是同步的，这表明存储阵列之间的连接是可操作的，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，并且镜像对尚未在辅助阵列上完成。 当卷添加到远程存储阵列上的镜像一致性组时，镜像对创建过程即完成。此卷将成为异步镜像对中的辅助卷。 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、辅助卷或镜像保留容量出现故障，异步镜像操作无法正常运行。
孤立	当一致性镜像组中的成员卷已在一致性镜像组的一侧（主侧或辅助侧）被删除但未在另一侧删除时，就会存在孤立的镜像对卷。 当两个存储阵列之间恢复通信且镜像配置的两侧协调镜像参数时，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	镜像对处于停止状态，因为镜像一致性组处于系统挂起状态。

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。

如果镜像对的主卷由控制器 A 所有，则辅助卷也将由远程存储阵列的控制器 A 所有。更改主卷的所有者将自动

更改辅助卷的所有者，以确保两个卷由同一个控制器所有。主端的当前所有权变更会自动传播到辅助端的相应当前所有权变更。

例如，主卷由控制器 A 所有，然后将控制器所有者更改为控制器 B。在这种情况下，下一次远程写入会将辅助卷的控制器所有者从控制器 A 更改为控制器 B。由于辅助端的控制器所有权更改由主端控制，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，在远程写入可以写入辅助卷之前，控制器重置或存储阵列电源循环会中断远程写入。在这种情况下，控制器不需要执行镜像对的完全同步。

当控制器重置期间远程写入被中断时，主端的新控制器所有者读取存储在首选控制器所有者保留容量卷中的日志文件中的信息。然后，新的控制器所有者将受影响的数据块从主卷复制到辅助卷，无需完全同步镜像卷。

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，可以将主镜像一致性组降级为辅助角色，或将辅助镜像一致性组升级为主角色。

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辅助角色时，该镜像一致性组中的所有镜像对也会降级到辅助角色，反之亦然。
- 当主镜像一致性组降级为辅助角色时，已分配给该组中成员卷的主机不再具有对它们的写入权限。
- 当镜像一致性组被提升为主角色时，访问该组中成员卷的任何主机现在都可以对其进行写入。
- 如果本地存储阵列无法与远程存储阵列通信，则可以在本地存储阵列上强制更改角色。

强制角色更改

当本地存储阵列和远程存储阵列之间的通信问题导致次镜像一致性组中的成员卷无法升级或主镜像一致性组中的成员卷无法降级时，可以强制在镜像一致性组之间更改角色。

您可以强制二级侧的镜像一致性组过渡到主角色。然后，恢复主机能够访问该镜像一致性组中新提升的成员卷，并且业务运营可以继续。

什么时候允许和不允许强制提升？

仅当镜像一致性组的所有成员卷都已同步并且具有一致的恢复点时，才允许强制升级镜像一致性组。

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处于初始同步过程中。
- 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，由于完全保留的容量错误）。
- 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，或者任何关联的成员卷或保留容量卷出现故障。

镜像组角色冲突

当本地和远程存储阵列之间的通信问题得到解决时，会出现镜像组角色冲突情况。使用 Recovery Guru 从此错误中恢复。在解决双重角色冲突时，不允许强制提升。

要避免镜像组角色冲突情况和后续恢复步骤，请等待存储阵列之间的连接正常运行以强制角色更改。

角色更改进行中状态

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被强制降级为辅助角色，并且镜像一致性组的辅助端被强制提升为主角色，则在恢复通信时，两个存储阵列上的镜像一致性组都将处于 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并继续定期同步来完成角色更改过程。

同步概念

SANtricity System Manager 中同步镜像的工作原理

同步镜像实时复制数据卷，以确保连续可用性。

EF600/EF600C 或 EF300/EF300C 存储阵列上不提供同步镜像。

同步镜像通过在两个存储阵列之一发生灾难时提供重要数据的副本，实现零丢失数据的恢复点目标 (RPO)。副本在任何时刻都与生产数据相同，因为每次对主卷执行写入操作时，都会对辅助卷执行写入操作。在使用在主卷上所做的更改成功更新辅助卷之前，主机不会收到写入成功确认。

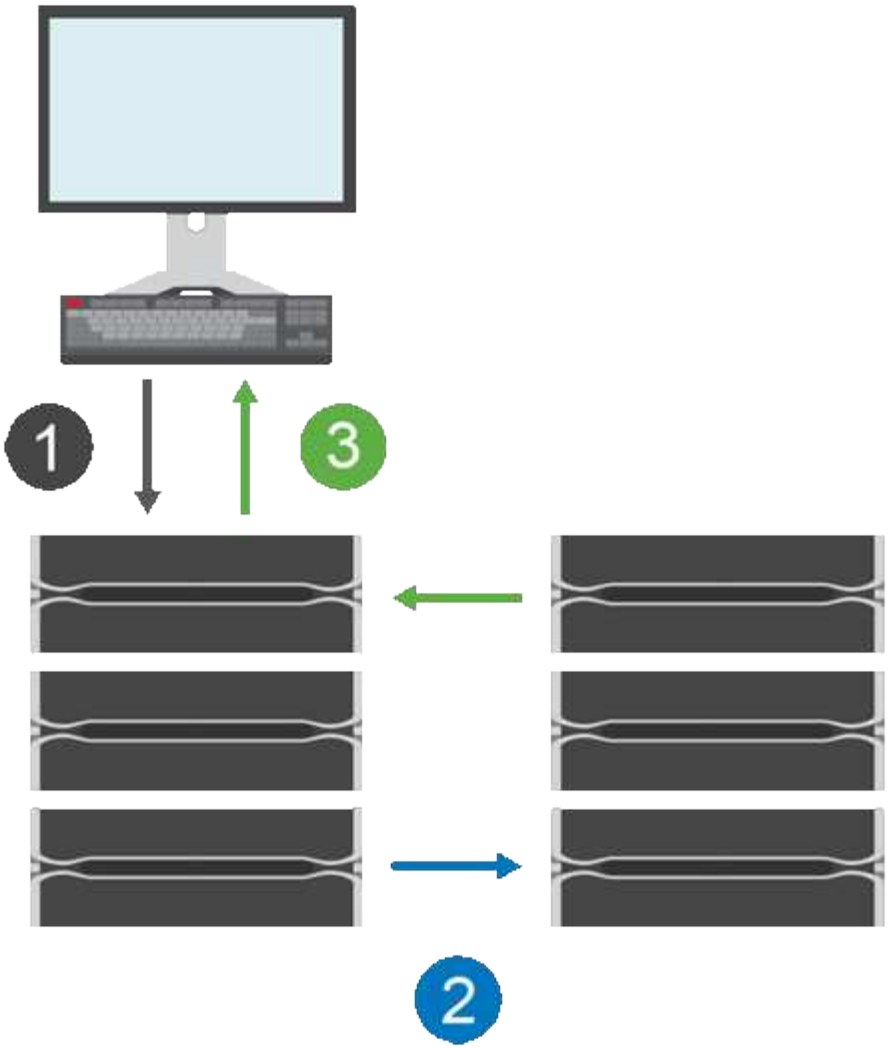
这种类型的镜像非常适合业务连续性目的，例如灾难恢复。

同步镜像关系

同步镜像关系由不同存储阵列上的主卷和辅助卷组成。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。包含辅助卷的存储阵列通常位于辅助站点，并保存数据的副本。如果主卷的存储阵列不可用，则使用辅助卷，例如，由于主站点完全停电、火灾或硬件故障。

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（由一个存储阵列上的主卷和另一个存储阵列上的辅助卷组成）后，可以开始同步镜像。同步镜像的步骤如下所示。



1. 主机发出写入请求。
2. 写入被提交到主卷，传播到远程系统，然后提交到辅助卷。
3. 主卷的存储阵列在两个写入操作都成功完成后，向主机系统发送 I/O 完成消息。

保留容量用于记录有关来自主机的传入写入请求的信息。

当主卷的当前控制器所有者收到来自主机的写入请求时，控制器首先将有关写入的信息记录到主卷的保留容量中。然后，它将数据写入主卷。接下来，控制器启动远程写入操作，将受影响的数据块复制到远程存储阵列的辅助卷。

由于主机应用程序必须等待在本地存储阵列上以及通过网络在远程存储阵列上进行写入，因此需要在本地存储阵列和远程存储阵列之间建立非常快速的连接，以保持镜像关系，而不会过度降低本地 I/O 性能。

灾难恢复

同步镜像会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，例如停电或洪水，则可以从辅助站点快速访问数据。

正在执行同步镜像操作时，辅助卷不可用于主机应用程序，因此，在本地存储阵列发生灾难时，可以故障转移到远程存储阵列。要进行故障切换，请将辅助卷提升为主角色。然后，恢复主机能够访问新提升的卷，并且业务运营可以继续。

同步设置

创建镜像对时，还可以定义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。

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。当通信链路再次工作时，可以将任何未复制的数据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接再次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。手动重新同步是推荐的策略。

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

当主卷的存储阵列无法将数据写入辅助卷时，主卷和辅助卷将不同步。这可能是由于以下问题造成的：

- 本地和远程存储阵列之间的网络问题
- 出现故障的辅助卷
- 正在镜像对上手动挂起同步

孤立的镜像对

当一侧（主侧或辅助侧）的成员卷已被移除但另一侧未被移除时，存在孤立的镜像对卷。

当恢复阵列间通信且镜像配置的两侧协调镜像参数时，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

要启用和配置两个阵列之间的镜像，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适用于您的存储阵列。

术语	说明
本地存储阵列	本地存储阵列是您要执行操作的存储阵列。 当您在本地角色列中看到 **Primary** 时，它指示存储阵列包含在镜像关系中占有主要角色的卷。当您在本地角色列中看到 **Secondary** 时，它指示存储阵列包含在镜像关系中具有辅助角色的卷。
镜像对	镜像对由两个卷组成，一个主卷和一个辅助卷。
主卷	镜像对的主卷是要镜像的源卷。

术语	说明
恢复点目标 (RPO)	恢复点目标 (RPO) 表示一个目标，指示镜像对中主卷和辅助卷之间被认为可接受的差异。RPO 为零表示不能容忍主卷和辅助卷之间的任何差异。RPO 大于零表示辅助卷不够新或落后于主卷。
远程存储阵列	远程存储阵列通常被指定为辅助站点，它通常在镜像配置中保存数据的副本。
预留容量	保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。
角色更改	角色变更是指将主要角色分配给辅助卷，反之亦然。
二级卷	镜像对的辅助卷通常位于辅助站点，并保存数据的副本。
同步	在本地存储阵列和远程存储阵列之间的初始同步时进行同步。当通信中断后主卷和辅助卷不同步时，也会发生同步。当通信链路再次工作时，任何未复制的数据都将同步到辅助卷的存储阵列。

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。

此功能在 EF600/EF600C 或 EF300/EF300C 存储系统中不可用。

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. 从本地存储阵列中选择主卷。
   c. 选择远程存储阵列作为数据传输的目标，然后选择辅助卷。
   d. 选择同步和重新同步优先级。
   e. 开始从主卷到辅助卷的初始数据传输。根据卷的大小，此初始传输可能需要几个小时。
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。完成镜像后，镜像对的状态为"最佳"。这两个阵列试图通过正常操作保持同步。仅将新的和更改的块从主卷传输到辅助卷。
3. *可选：*您可以在 System Manager 中更改同步设置。

由于同步复制是连续的，因此两个站点之间的复制链路必须提供足够的带宽容量。

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

要启用和配置两个阵列之间的镜像，必须使用 Unified Manager 界面。Unified Manager 与 Web Services Proxy 一起安装在主机系统上。

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

存储阵列

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。
- 每个存储阵列必须有两个控制器。
- 必须在 Unified Manager 中发现两个存储阵列。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。
- 您的本地和远程存储阵列通过 Fibre Channel 结构连接。

支持的连接

仅在具有光纤通道 (FC) 主机端口的控制器上支持同步镜像的通信。

同步镜像在本地存储阵列和远程存储阵列上的每个控制器上使用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 通常保留用于镜像数据传输。

镜像卷候选项

- RAID 级别、缓存参数和段大小在同步镜像对的主卷和辅助卷上可以不同。
- 同步镜像对中的主卷和辅助卷必须是标准卷。它们不能是精简卷或快照卷。
- 辅助卷必须至少与主卷一样大。
- 只有主卷可以具有与其关联的快照和/或是卷复制操作中的源卷或目标卷。
- 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有限制。确保存储阵列上配置的卷数小于支持的限制。当同步镜像处于活动状态时，创建的两个保留容量卷将计入卷限制。

预留容量

- 主卷和辅助卷需要保留容量来记录写入信息，以便从控制器重置和其他临时中断中恢复。
- 激活同步镜像时，将自动创建保留容量卷。由于镜像对中的主卷和辅助卷都需要保留容量，因此您必须确保在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。

- 如果使用具有安全功能的驱动器，则主卷和辅助卷必须具有兼容的安全设置。此限制未强制执行；因此，您必须自己验证。
- 如果使用具有安全功能的驱动器，则主卷和辅助卷应使用相同的驱动器类型。此限制未强制执行；因此，您必须自己验证。
  - 如果主卷使用 Full Disk Encryption (FDE) 驱动器，则辅助卷应使用 FDE 驱动器。
  - 如果主卷使用 Federal Information Processing Standards 140-2 (FIPS) 验证的驱动器，则辅助卷应使用 FIPS 140-2 验证的驱动器。
- 如果使用数据保障 (DA)，则主卷和辅助卷必须具有相同的 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辅助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。

此功能在 EF600/EF600C 或 EF300/EF300C 存储系统中不可用。

同步镜像对可具有以下状态之一：

- 最佳

  指示镜像对中的卷是同步的，这意味着存储阵列之间的结构连接是可操作的，并且每个卷都处于所需的工作状态。

- 正在同步

  显示镜像对之间的数据同步进度。此状态也将在初始同步期间显示。

  通信链路中断后，仅将链路中断期间主卷上已更改的数据块复制到辅助卷。

- 未同步

  指示主卷的存储阵列无法将传入数据写入远程阵列。本地主机可以继续写入主卷，但远程写入不会发生。不同的条件可能会阻止主卷的存储阵列将传入数据写入辅助卷，例如：

  - 辅助卷不可访问。
  - 远程存储数组不可访问。
  - 存储阵列之间的结构连接不可访问。
  - 无法使用新的全球标识符 (WWID) 更新辅助卷。

- 已暂停

  指示同步镜像操作已被用户挂起。当镜像对被挂起时，不会尝试接触辅助卷。对主卷的任何写入都会持续记录在镜像保留容量卷中。

- 失败

  表示由于主卷、辅助卷或镜像保留容量出现故障，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 EF600/EF600C 或 EF300/EF300C 存储系统上的同步镜像。

如果镜像对的主卷由控制器 A 所有，则辅助卷也将由远程存储阵列的控制器 A 所有。更改主卷的所有者将自动更改辅助卷的所有者，以确保两个卷由同一个控制器所有。主端的当前所有权变更会自动传播到辅助端的相应当前所有权变更。

例如，主卷由控制器 A 所有，然后将控制器所有者更改为控制器 B。在这种情况下，下一次远程写入会将辅助卷的控制器所有者从控制器 A 更改为控制器 B。由于辅助端的控制器所有权更改由主端控制，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，在远程写入可以写入辅助卷之前，控制器重置或存储阵列电源循环会中断远程写入。在这种情况下，控制器不需要执行镜像对的完全同步。

当控制器重置期间远程写入被中断时，主端的新控制器所有者读取存储在首选控制器所有者保留容量卷中的日志文件中的信息。然后，新的控制器所有者将受影响的数据块从主卷复制到辅助卷，无需完全同步镜像卷。

了解 SANtricity 软件中镜像对中的卷角色更改

您可以在镜像对中的卷之间更改角色。您可以通过将主卷降级为辅助角色或将辅助卷升级为主角色来执行此操作。

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：

- 当主卷降级为辅助角色时，该镜像对中的辅助卷将提升为主角色，反之亦然。
- 当主卷降级为辅助角色时，已分配给该卷的主机不再具有对该卷的写入权限。
- 当辅助卷升级为主卷时，正在访问该卷的任何主机现在都可以对其进行写入。
- 如果本地存储阵列无法与远程存储阵列通信，则可以在本地存储阵列上强制更改角色。

强制角色更改

当本地存储阵列和远程存储阵列之间的通信问题阻止了辅助卷的升级或主卷的降级时，可以强制在镜像对中的卷之间进行角色更改。

您可以强制辅助端的卷过渡到主要角色。然后，恢复主机可以访问新升级的卷，业务运营可以继续。

当远程存储阵列已恢复且任何通信问题都已解决时，将出现同步镜像 - 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。

什么时候允许和不允许强制提升？

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处于初始同步过程中。
- 镜像对处于"失败"、"角色更改挂起"或"角色更改正在进行"状态，或者任何关联的保留容量卷出现故障。

角色更改进行中状态

如果镜像配置中的两个存储阵列断开连接，并且镜像对的主卷被强制降级为辅助角色，并且镜像对的辅助卷被强制提升为主角色，则在恢复通信时，两个存储阵列上的卷都将处于 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操作状态并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和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存在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有通信路径。连接测试在存储阵列之间发送阵列间消息，然后验证远程存储阵列上是否存在对应的镜像一致性组。它还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 Test Unit 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的端口的最小、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. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡，然后选择要测试的镜像一致性组。
3. 选择 **Test Communication**。

   此时将显示"测试通信"对话框。

4. 选择要在与所选镜像一致性组关联的本地和远程存储阵列之间执行的一个或多个通信测试，然后单击 **Test**。
5. 查看 Results 窗口中显示的信息。

通信测试状态	说明
正常且无错误	镜像一致性组正在正确通信。
通过状态（但不正常）	检查可能的网络或连接问题并重试测试。
失败状态	说明了故障原因。请参见 Recovery Guru 以纠正此问题。
端口连接错误	原因可能是本地存储阵列未连接或无法连接到远程存储阵列。请参阅 Recovery Guru 以纠正问题。

结果

通信测试完成后，此对话框显示"正常"状态、"通过"状态或"失败"状态。

如果通信测试返回 Failed 状态，则在关闭此对话框后测试会继续运行，直到恢复镜像一致性组之间的通信。

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，这比在单个镜像对上暂停或恢复同步更有效。

关于此任务

在组上暂停和恢复同步有助于减少对主机应用程序的任何性能影响，这可能会在本地存储阵列上的任何更改数据复制到远程存储阵列时发生。

在使用"恢复"选项恢复同步活动之前，镜像一致性组及其镜像对的状态将保持为挂起状态。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   将显示 Mirrored Consistency Group（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 **More › Suspend** 或 **More › Resume**。

   系统显示确认信息。
4. 选择 是 确认。

结果

System Manager 执行以下操作：

- 在不删除镜像关系的情况下，暂停或恢复镜像一致性组中所有镜像对之间的数据传输。
- 记录在镜像组暂停时写入镜像一致性组的主侧的任何数据，并在镜像组恢复时自动将数据写入镜像一致性组的辅助侧。无需完全同步。
- 对于 *suspended* 镜像一致性组，在 Mirror Consistency Groups 表中显示 **user-suspended**。

- 对于 *resumed* 镜像一致性组，在镜像一致性组暂停时写入主卷的数据会立即写入辅助卷。如果设置了自动同步间隔，则恢复定期同步。

更改 **SANtricity System Manager** 中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最初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. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   将显示 Mirrored Consistency Group（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：More[Edit Settings]。

   系统显示"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 **Save**。

   字段详细信息

字段	说明
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，每隔 – 选择此选项可通过指定从上一次更新开始到下一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。默认时间间隔为 10 分钟。
提醒我…	如果将同步方法设置为自动执行，请设置以下警报： • 同步 – 设置 System Manager 发送同步未完成警报的时间长度。 • 远程恢复点 – 设置一个时间限制，在此时间限制之后，System Manager 将发送警报，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。定义从上一次更新结束起的时间限制。 • 保留容量阈值 – 定义保留容量数量，当达到该数量时，System Manager 会发送警报，提示您接近保留容量阈值。按剩余容量的百分比定义阈值。

结果

System Manager 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

您可以手动启动镜像一致性组中所有镜像对的重新同步。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   将显示 Mirror Consistency Group（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：More[Manually resynchronize]。

   系统显示确认信息。

4. 选择 是 确认。

结果

系统执行以下操作：

- 在所选镜像一致性组内的所有镜像对上启动数据的重新同步。
- 将修改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的未同步数据量

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的非同步数据量。当镜像一致性组处于未同步状态时，不会发生镜像活动。

关于此任务

当选定的镜像一致性组包含镜像对且同步当前未在进行时，您可以执行此任务。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   将显示 Mirror Consistency Group（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：More[查看未同步的数据量]。

   如果存在未同步的数据，则表格值会反映这一点。数据量列以 MiB 为单位列出未同步的数据量。

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，以重新建立与本地存储阵列的连接。

开始之前

必须将本地存储阵列和远程存储阵列配置为使用 iSCSI 连接进行异步镜像。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   Mirror Consistency Group 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]。

   系统显示更新远程 IP 地址对话框。

4. 选择 **Update** 以更新远程存储阵列的 iSCSI IP 地址。

结果

系统重置远程存储阵列的 IP 地址，以重新建立与本地存储阵列的连接。

在 **SANtricity System Manager** 中将镜像一致性组角色更改为主要或次要

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角色。在远程存储阵列上创建的镜像一致性组具有辅助角色。可以将本地镜像一致性组降级为辅助角色，也可以将远程镜像一致性组升级为主角色。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   将显示 Mirror Consistency Group（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. 选择要更改其角色的镜像一致性组，然后选择菜单：More[Change role to <Primary | Secondary>]**>**。

   系统显示确认信息。

4. 确认您要更改镜像一致性组的角色，然后单击 **Change Role**。

   当请求角色更改时，系统显示"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 执行以下操作：

- Mirror Consistency Group 表在进行角色更改的镜像一致性组旁边显示状态"挂起"或"正在进行"。您可以通过单击表格单元格中的 **Cancel** 链接来取消挂起的 Role Change 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 将次镜像一致性组提升为主角色或将主镜像一致性组降级为次角色（取决于您的选择）。角色更改会影响所选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. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirror Consistency Groups** 选项卡。

   将显示 Mirror Consistency Group（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 **Uncommon Tasks › Delete**。

   系统显示确认信息。

4. 选择 是 删除镜像一致性组。

结果

System Manager 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 Mirror Consistency Group 表中删除镜像一致性组。

完成后

有时，可能会出现从本地存储阵列中成功删除镜像一致性组的情况，但通信错误会阻止从远程存储阵列中删除镜像一致性组。在此情况下，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

删除镜像对可从本地存储阵列上的主卷和远程存储阵列上的辅助卷中删除镜像关系。

关于此任务

查看有关孤立镜像对的以下信息：

- 当一致性镜像组中的成员卷在一侧（本地存储阵列侧或远程存储阵列侧）已被删除但在另一侧未被删除时，就会存在孤立的镜像对。
- 当恢复阵列间通信且镜像配置的两侧协调镜像参数时，会检测到孤立的镜像对。
- 您可以删除镜像对以更正孤立的镜像对状态。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirrored Pair** 选项卡。

将显示 Mirrored Pairs（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 **Remove**。

结果

System Manager 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，并删除保留容量。
- 将主卷和辅助卷返回到主机可访问的非镜像卷。
- 通过删除异步镜像对来更新 Asynchronous Mirroring 磁贴。

在 **SANtricity System Manager** 中增加预留容量

您可以增加保留容量，这是用于存储对象上的任何复制服务操作的物理分配容量。

对于快照操作，它通常是基本卷的 40%；对于异步镜像操作，它通常是基本卷的 20%。通常，当您收到存储对象的保留容量正在变满的警告时，您会增加保留容量。

开始之前

- 池或卷组中的卷必须具有"最佳"状态，并且不得处于任何修改状态。
- 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不存在可用容量，则可以将未分配的容量以未使用的驱动器的形式添加到池或卷组中。

关于此任务

对于以下存储对象，只能以 8 GiB 的增量增加保留容量：

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

如果您认为主卷将经历许多更改或特定复制服务操作的寿命将非常长，请使用较高的百分比。

您不能增加只读快照卷的保留容量。只有读写快照卷需要保留容量。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择 **Reserved Capacity** 选项卡。
3. 选择要为其增加保留容量的存储对象，然后单击 增加容量。

   此时将显示"增加保留容量"对话框。

4. 使用微调框调整容量百分比。

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。

5. 单击 **Increase**。

结果

System Manager 执行以下操作：

- 增加存储对象的保留容量。
- 显示新增的保留容量。

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 System Manager 发送警报通知的百分比点，即当镜像对卷的预留容量接近满时。

步骤

1. 选择菜单：Storage[Pools & Volume Groups]。
2. 选择 **Reserved Capacity** 选项卡。
3. 选择要编辑的镜像对卷，然后单击 **View/Edit Settings**。

   此时将显示镜像配对卷保留容量设置对话框。

4. 根据需要更改镜像对卷的预留容量设置。

   字段详细信息

设置	说明
在…时提醒我	使用微调框可调整在镜像对的保留容量接近满时 System Manager 发送警报通知的百分比点。 当镜像对的保留容量超过指定阈值时，System Manager 会发送警报，让您有时间增加保留容量。 更改一个镜像对的 Alert 设置会更改属于同一镜像一致性组的所有镜像对的 Alert 设置。

5. 单击 **Save** 以应用更改。

在 **SANtricity System Manager** 中为在旧系统上创建的主卷完成镜像对

如果您在无法由 SANtricity System Manager 管理的旧存储阵列上创建了主卷，则可以使用 SANtricity System Manager 在此阵列上创建辅助卷。

关于此任务

您可以在使用不同接口的传统阵列和可由 System Manager 管理的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，因为您已经完成了镜像对创建序列中的镜像对。
- 在远程存储阵列上执行此任务。

步骤

1. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择 **Mirrored Pair** 选项卡。

   将显示 Mirrored Pairs（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 Incomplete 的镜像对卷，然后单击镜像对列中显示的 **Complete mirrored pair** 链接。
4. 通过选择以下单选按钮之一，选择是自动还是手动完成镜像对创建序列：
   - 自动 — 创建新的辅助卷。

     通过选择要在其中创建辅助卷的现有池或卷组，接受镜像对远程端的默认设置。使用此推荐选项可使用默认设置为辅助卷分配保留容量。

   - **Manual** — 选择现有卷。

     为辅助卷定义自己的参数。

     i. 单击 **Next** 选择辅助卷。

     ii. 选择要用作辅助卷的现有卷，然后单击 **Next** 以分配保留容量。

     iii. 分配预留容量。执行以下操作之一：

     - 接受默认设置。

       保留容量的默认设置为基本卷容量的 20%，通常此容量就足够了。

     - 分配您自己的保留容量设置，以满足与异步镜像相关的数据存储需求。

       所需的容量因向主卷写入 I/O 的频率和大小以及保留容量所需的时间而异。一般来说，如果存在以下一种或两种情况，请为保留容量选择更大的容量：

       - 您打算将镜像对保留很长一段时间。
       - 由于繁重的 I/O 活动，主卷上的大部分数据块将发生变化。使用历史性能数据或其他操作系统实用程序来帮助您确定主卷的典型 I/O 活动。
5. 选择 **Complete**。

结果

System Manager 执行以下操作：

- 在远程存储阵列上创建辅助卷，并为镜像对的远程端分配保留容量。
- 开始本地存储阵列和远程存储阵列之间的初始同步。
- 如果正在镜像的卷是精简卷，则在初始同步期间仅将分配的块传输到辅助卷。这种传输会减少必须传输才能

完成初始同步的数据量。

- 在本地存储阵列和远程存储阵列上为镜像对创建保留容量。

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和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出现的通信问题。

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。通信测试验证本地存储阵列可以与远程存储阵列通信，并且与镜像对关联的辅助卷存在于远程存储阵列上。
- 延迟 — 向与镜像对关联的远程存储阵列上的辅助卷发送 SCSI 测试单元命令，以测试最小、平均和最大延迟。

步骤

1. 选择菜单：Storage[Synchronous Mirroring]。
2. 选择要测试的镜像对，然后选择 **Test Communication**。
3. 查看"结果"窗口中显示的信息，并在必要时按照指示的纠正措施进行操作。

> 如果通信测试失败，则在关闭此对话框后测试继续运行，直到恢复镜像对之间的通信。

在 **SANtricity System Manager** 中暂停和恢复镜像对的同步

您可以使用 Suspend 选项和 Resume 选项来控制何时同步镜像对中主卷和辅助卷上的数据。

关于此任务

如果手动挂起镜像对，则该镜像对在手动恢复之前不会同步。

步骤

1. 选择菜单：Storage[Synchronous Mirroring]。
2. 选择要暂停或恢复的镜像对，然后选择 **More › Suspend** 或 **More › Resume**。

   系统显示确认信息。

3. 选择 是 确认。

结果

System Manager 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* 镜像对：

- 在镜像配对表中显示 已挂起。
- 记录在同步挂起时写入镜像对主卷的任何数据。

- 对于 *resumed* 镜像对，在恢复同步时，将数据自动写入镜像对的辅助卷。无需完全同步。

在 **SANtricity System Manager** 中更改镜像对中卷之间的角色

您可以在参与同步镜像的镜像对中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，此任务可能是必要的。

关于此任务

您可以将主卷降级为辅助卷，也可以将辅助卷升级为主卷。任何正在访问主卷的主机都具有对该卷的读/写访问权限。当主卷成为辅助卷时，只有由主控制器启动的远程写入才会写入到卷中。

步骤

1. 选择菜单：Storage[Synchronous Mirroring]。
2. 选择包含要更改角色的卷的镜像对，然后选择菜单：More[Change Role]。

   系统显示确认信息。

3. 确认您要更改卷的角色，然后选择 **Change Role**。

   如果本地存储阵列无法与远程存储阵列通信，则当请求角色更改时，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 **Yes** 以强制更改角色。

结果

System Manager 执行以下操作：

- 如果可以联系镜像对中的关联卷，则卷之间的角色会发生变化。System Manager 将镜像对中的辅助卷提升为主角色，或将镜像对中的主卷降级为辅助角色（取决于您的选择）。

更改 **SANtricity System Manager** 中镜像对的同步设置

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

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. 选择菜单：Storage[Synchronous Mirroring]。
2. 选择要编辑的镜像对，然后选择菜单：More[Edit settings]。

   系统显示查看/编辑设置对话框。

3. 使用滑动条编辑同步优先级。

   与服务 I/O 请求相比，同步优先级确定通信中断后有多少系统资源用于完成重新同步操作。

有关同步速率的详细信息

有五个同步优先级：

- 最低
- 低
- 中
- 高
- 最高

如果将同步优先级设置为最低等级，则会优先处理 I/O 活动，而重新同步操作则需要更长的时间。如果将同步优先级设置为最高等级，则会优先处理重新同步操作，而存储阵列的 I/O 活动可能受到影响。

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。

   - **Manual**（推荐选项）-- 选择此选项可要求在通信恢复到镜像对后手动恢复同步。此选项为恢复数据提供了最佳机会。
   - 自动 — 选择此选项可在通信恢复到镜像对后自动开始重新同步。

5. 选择 **Save**。

删除 **SANtricity System Manager** 中的同步镜像关系

删除镜像对可从本地存储阵列上的主卷和远程存储阵列上的辅助卷中删除镜像关系。

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：

- 当一侧（本地/远程）的成员卷已被删除，但另一侧未被删除时，存在孤立的镜像对。
- 在恢复阵列间通信时会检测到孤立的镜像对。

步骤

1. 选择菜单：Storage[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 **Remove**。

结果

System Manager 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。
- 将主卷和辅助卷返回到主机可访问的非镜像卷。

- 使用删除同步镜像对来更新同步镜像磁贴。

停用镜像

在 **SANtricity System Manager** 中停用异步镜像

您可以停用本地和远程存储阵列上的异步镜像，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 Fibre Channel 结构或 iSCSI 接口连接。

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. 选择菜单：Storage[Asynchronous Mirroring]。
2. 选择菜单：Uncommon Tasks[Deactivate]。

   系统显示确认信息。

3. 选择 是 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取和写入请求。
- 此存储阵列中的任何卷都不能作为主卷或辅助卷参与镜像关系。

在 **SANtricity System Manager** 中停用同步镜像

您可以停用存储阵列上的同步镜像功能，以重新建立主机总线适配器 (HBA) 主机端口 4 的正常使用，该端口保留用于镜像数据传输。

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. 选择菜单：Storage[Synchronous Mirroring]。
2. 选择菜单：Uncommon Tasks[Deactivate]。

   系统显示确认信息。

3. 选择 是 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取和写入请求。

- 存储阵列上的保留容量卷将被删除。

SANtricity System Manager 异步镜像常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

异步镜像与同步镜像有何不同?

Asynchronous Mirroring 功能与 Synchronous Mirroring 功能在一个基本方面有所不同：它捕获特定时间点的源卷状态，并仅复制自上次图像捕获以来发生变化的数据。

使用同步镜像，主卷的状态不会在某个时间点捕获，而是将主卷上所做的所有更改反映到辅助卷上。辅助卷每时每刻都与主卷相同，因为使用这种类型的镜像，每次对主卷执行写入操作时，都会对辅助卷执行写入操作。在使用主卷上所做的更改成功更新辅助卷之前，主机不会收到写入成功确认。

使用异步镜像，远程存储阵列未与本地存储阵列完全同步，因此，如果应用程序由于本地存储阵列丢失而需要转换到远程存储阵列，则可能会丢失一些事务。

镜像功能之间的比较：

异步镜像	同步镜像
复制方法	• 时间点 镜像按需完成或根据用户定义的时间表自动完成。时间表可以以分钟为单位进行定义。两次同步之间的最短时间为 10 分钟。
• 连续 镜像会自动连续执行，从每次主机写入中复制数据。	预留容量
• 多个 每个镜像对都需要一个预留容量卷。	• 单个 所有镜像卷都需要单个保留容量卷。
沟通	• **iSCSI** 和光纤通道 支持存储阵列之间的 iSCSI 和 Fibre Channel 接口。
• **Fibre Channel** 仅支持存储阵列之间的 Fibre Channel 接口。	距离

异步镜像	同步镜像
• 无限制 支持本地存储阵列和远程存储阵列之间几乎无限的距离，距离通常仅受网络功能和通道扩展技术的限制。	• 受限 通常必须在距离本地存储阵列约 10 km（6.2 miles）的范围内，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？

镜像在 SANtricity Unified Manager 界面中配置。

EF600/EF600C 或 EF300/EF300C 存储阵列上不提供同步镜像。

要启用和配置两个阵列之间的镜像，请验证以下内容：

- Web Services Proxy 服务必须正在运行。(Unified Manager 与 Web Services Proxy 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 必须具有存储阵列的有效 SSL 证书。您可以接受自签名证书或从 Unified Manager 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，我需要知道什么？

在创建镜像一致性组之前，请遵循这些指南。

EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

您可以在 Unified Manager 的"创建镜像对"向导中创建一致性组。

满足 Unified Manager 的以下要求：

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

此外，请务必满足存储阵列的以下要求：

- 必须在 Unified Manager 中发现两个存储阵列。

- 每个存储阵列必须有两个控制器。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 您的本地和远程存储阵列通过光纤通道结构或 iSCSI 接口连接。

异步镜像 - 在创建镜像对之前，我需要知道什么？

您可以在 SANtricity Unified Manager 界面中配置镜像对，然后在 SANtricity System Manager 中管理这些对。

在创建镜像对之前，请遵循以下指南。

- 您必须有两个存储阵列。
- 每个存储阵列必须有两个控制器。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，并且必须连接到您的网络。
- 您的本地和远程存储阵列通过光纤通道结构或 iSCSI 接口连接。
- 存储阵列的最低固件版本为 7.84。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。
- 您已安装 Web Services Proxy 和 Unified Manager。镜像对在 Unified Manager 界面中配置。
- 在 Unified Manager 中发现两个存储阵列。
- 您的存储阵列必须至少包含一个镜像一致性组。您可以在 Unified Manager 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，我需要知道什么？

通常，当您收到镜像对的保留容量已满的警告时，应增加保留容量。您只能以 8 GiB 的增量增加保留容量。

对于异步镜像操作，保留容量通常为基本卷的 20%。如果存在以下一种或两种情况，请为保留容量选择更大的容量：

- 您打算将镜像对保留很长一段时间。
- 由于繁重的 I/O 活动，主卷上的大部分数据块将发生变化。使用历史性能数据或其他操作系统实用程序来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保留容量：

- 通过选择菜单：Storage[Pools and Volumes Groups] 来调整镜像对卷的容量百分比，然后单击 **Reserved Capacity** 选项卡。
- 使用池或卷组上可用的可用容量创建新卷。

  如果任何池或卷组上不存在可用容量，则可以将未配置的容量以未使用的驱动器的形式添加到池或卷组中。

为什么我无法按请求的数量增加预留容量?

您只能以 4 GiB 的增量增加保留容量。

查看以下指南：

- 您必须在池或卷组中具有足够的可用容量，以便在必要时可以对其进行扩展。

  如果任何池或卷组上不存在可用容量，则可以将未分配的容量以未使用的驱动器的形式添加到池或卷组中。

- 池或卷组中的卷必须具有"最佳"状态，并且不得处于任何修改状态。
- 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，保留容量通常为基本卷的 20%。如果您认为基本卷将发生许多变化，或者存储对象的复制服务操作的估计预期寿命将非常长，请使用更高的百分比。

为什么要更改此百分比?

保留容量通常为快照操作的基本卷的 40%，异步镜像操作的基本卷的 20%。

通常这个容量就足够了。所需的容量因向基本卷写入 I/O 的频率和大小以及您打算使用存储对象的复制服务操作的时长而异。

一般来说，如果存在以下一种或两种情况，请为保留容量选择更大的百分比：

- 如果特定存储对象的复制服务操作的生命周期非常长。
- 如果由于大量 I/O 活动，基本卷上的大量数据块将发生变化。使用历史性能数据或其他操作系统实用程序来帮助您确定基本卷的典型 I/O 活动。

为什么我看到多个预留容量候选项?

如果池或卷组中有多个卷符合您为存储对象选择的容量百分比量，您将看到多个候选项。

您可以通过更改要在基本卷上保留用于复制服务操作的物理驱动器空间百分比来刷新推荐候选列表。根据您的选择显示最佳候选。

为什么在表中显示 **Not Available** 值?

当位于远程存储阵列上的数据不可显示时，该表列出了 Not Available 值。

要显示远程存储阵列数据，请从 Unified Manager 启动 System Manager。

为什么我没有看到所有的池和卷组?

为异步镜像对创建辅助卷时，系统将显示该异步镜像对的所有符合条件的池和卷组的列表。任何不符合使用条件的池或卷组都不会显示在该列表中。

池或卷组可能因以下任何原因而不符合条件。

- 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，列表会显示所有符合条件的卷。

不符合使用条件的任何卷都不会显示在该列表中。卷可能因以下任何原因不符合条件：

- 卷不是最佳的。
- 此卷已参与镜像关系。
- 对于精简卷，必须启用自动扩展。

> 对于 EF600 和 EF300 控制器，异步镜像对的主卷和辅助卷必须匹配相同的协议、托盘级别、段大小、安全类型和 RAID 级别。不符合条件的异步镜像对将不会出现在可用卷列表中。

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辅助卷时，列表会显示该镜像对的所有合格卷。

任何不符合使用条件的卷都不会显示在该列表中。由于以下任何原因，卷可能不符合条件：

- 卷不是最佳的。
- 此卷已参与镜像关系。
- 主卷和辅助卷之间的精简卷属性不匹配。
- 如果使用数据保障 (DA)，则主卷和辅助卷必须具有相同的 DA 设置。
  - 如果主卷启用了 DA，则辅助卷必须启用 DA。
  - 如果主卷未启用 DA，则辅助卷不得启用 DA。

为什么要更新远程存储阵列的 **IP** 地址？

当 iSCSI 端口的 IP 地址更改且本地存储阵列无法与远程存储阵列通信时，可以更新远程存储阵列的 IP 地址。

当与 iSCSI 连接建立异步镜像关系时，本地和远程存储阵列都会在异步镜像配置中存储远程存储阵列的 IP 地址的记录。如果 iSCSI 端口的 IP 地址发生变化，则尝试使用该端口的远程存储阵列将遇到通信错误。

具有更改的 IP 地址的存储阵列向与镜像一致性组关联的每个远程存储阵列发送一条消息，这些镜像一致性组被配置为通过 iSCSI 连接进行镜像。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将其阵列间消息发送到远程存储阵列，则系统会向您发送连接问题警报。使用"更新远程 IP 地址"选项与本地存储阵列重新建立连接。

SANtricity System Manager 同步镜像常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

异步镜像与同步镜像有何不同?

Asynchronous Mirroring 功能与 Synchronous Mirroring 功能在一个基本方面有所不同：它捕获特定时间点的源卷状态，并仅复制自上次图像捕获以来发生变化的数据。

使用同步镜像，主卷的状态不会在某个时间点捕获，而是将主卷上所做的所有更改反映到辅助卷上。辅助卷每时每刻都与主卷相同，因为使用这种类型的镜像，每次对主卷执行写入操作时，都会对辅助卷执行写入操作。在使用主卷上所做的更改成功更新辅助卷之前，主机不会收到写入成功确认。

使用异步镜像，远程存储阵列未与本地存储阵列完全同步，因此，如果应用程序由于本地存储阵列丢失而需要转换到远程存储阵列，则可能会丢失一些事务。

镜像功能之间的比较：

异步镜像	同步镜像
复制方法	• 时间点 镜像按需完成或根据用户定义的时间表自动完成。时间表可以以分钟为单位进行定义。两次同步之间的最短时间为 10 分钟。
• 连续 镜像会自动连续执行，从每次主机写入中复制数据。	预留容量
• 多个 每个镜像对都需要一个预留容量卷。	• 单个 所有镜像卷都需要单个保留容量卷。
沟通	• **iSCSI** 和光纤通道 支持存储阵列之间的 iSCSI 和 Fibre Channel 接口。
• **Fibre Channel** 仅支持存储阵列之间的 Fibre Channel 接口。	距离
• 无限制 支持本地存储阵列和远程存储阵列之间几乎无限的距离，距离通常仅受网络功能和通道扩展技术的限制。	• 受限 通常必须在距离本地存储阵列约 10 km（6.2 miles）的范围内，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，列表会显示所有符合条件的卷。

不符合使用条件的任何卷都不会显示在该列表中。由于以下任何原因，卷可能不符合条件：

- 此卷是非标准卷，例如快照卷或精简卷。
- 卷不是最佳的。
- 此卷已参与镜像关系。

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辅助卷时，列表会显示该镜像对的所有合格卷。

任何不符合使用条件的卷都不会显示在该列表中。由于以下任何原因，卷可能不符合条件：

- 此卷是非标准卷，例如快照卷或精简卷。
- 卷不是最佳的。
- 此卷已参与镜像关系。
- 如果使用数据保障 (DA)，则主卷和辅助卷必须具有相同的 DA 设置。
  - 如果主卷启用了 DA，则辅助卷必须启用 DA。
  - 如果主卷未启用 DA，则辅助卷不得启用 DA。

同步镜像 - 在创建镜像对之前，我需要知道什么？

您可以在 SANtricity Unified Manager 界面中配置镜像对，然后在 SANtricity System Manager 中管理这些对。

在创建镜像对之前，请遵循以下指南：

- 您必须有两个存储阵列。
- 每个存储阵列必须有两个控制器。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，并且必须连接到您的网络。
- 您的本地和远程存储阵列通过 Fibre Channel 结构连接。
- 存储阵列的最低固件版本为 7.84。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。
- 您已安装 Web Services Proxy 和 Unified Manager。镜像对在 Unified Manager 界面中配置。
- 在 Unified Manager 中发现两个存储阵列。

同步优先级对同步速率有何影响？

同步优先级定义了相对于系统性能为同步活动分配的处理时间。

主卷的控制器所有者在后台执行此操作。同时，控制器所有者处理对主卷的本地 I/O 写入和对辅助卷的相关远程

写入。由于重新同步会从 I/O 活动中转移控制器处理资源，因此重新同步可能会对主机应用程序产生性能影响。

请记住这些准则，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

可提供以下优先级费率：

- 最低
- 低
- 中
- 高
- 最高

最低优先级速率支持系统性能，但重新同步需要更长的时间。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。

这些指南大致反映了优先级之间的差异。

完全同步的优先级	与最高同步速率相比所用时间
最低	大约是最高优先级速率的八倍长。
低	大约是最高优先级速率的六倍长。
中	长度约为最高优先级速率的三倍半。
高	长度约为最高优先级速率的两倍。

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？

建议手动重新同步，因为它允许您以一种为恢复数据提供最佳机会的方式管理重新同步过程。

如果使用自动重新同步策略，并且在重新同步过程中发生间歇性通信问题，则辅助卷上的数据可能会暂时损坏。当重新同步完成时，数据将被更正。

远程存储

了解 **SANtricity System Manager** 中的远程存储功能

如果您具有 Remote Storage 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?

_远程存储_功能允许您将数据从远程存储系统导入到本地 E 系列存储系统。远程系统可以是另一个 E 系列系统或来自另一个供应商的系统。当您希望以最短的停机时间（例如在设备升级期间）简化数据迁移时，此功能非常有用。

要使用远程存储，必须在子模型 ID (SMID) 中启用此功能。

了解详情：

- "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。此向导可从菜单中获得：Storage[Remote storage]。

了解详情：

- "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

远程存储功能允许您将数据从远程存储系统导入到本地 E 系列存储系统。当您希望以最短的停机时间（例如在设备升级期间）简化数据迁移时，此功能非常有用。

要配置远程存储功能，必须设置硬件，然后使用 System Manager 创建远程存储对象。此配置完成后，导入过程开始。

硬件设置

使用以下工作流程准备硬件连接。

这些步骤在远程存储功能的用户指南中进一步描述，该指南可从 E 系列和 SANtricity 文档中心获得 "远程存储卷概述"，以及在 "远程存储技术报告"中。

E4000 系统当前不支持 SANtricity Remote Storage Volumes。

在本地 E 系列存储系统上：

1. 确保每个控制器都有到远程存储系统的 iSCSI 连接。通过此连接，本地 E 系列系统充当 iSCSI 启动程序，可以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，具有匹配的块大小，并且未映射。请参阅 "创建卷"。
3. 从 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：**Settings › System › iSCSI settings › Target IQN**。

在远程存储系统上：

1. 使用其 IQN 将本地 E 系列系统设置为远程系统上的主机。请务必设置相应的主机类型，如下所示：
   - 如果远程系统是 E 系列型号，请参见"主机和主机集群概述"。使用"Factory Default"的主机类型。
   - 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. 对于所选的源卷，从远程存储系统中收集以下信息，以便可以创建导入：
   - 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 系列存储系统上的目标卷。当您选择*完成*时，导入过程开始。
2. 从"查看操作"对话框或"正在进行的操作"面板监视导入。如有必要，您也可以暂停和恢复流程。
3. 可选地，在导入完成时断开源卷和目标卷之间的连接，或保留连接以供将来导入。

了解 **SANtricity** 软件中的远程存储术语

了解远程存储术语如何适用于您的存储阵列。

术语	说明
IQN	iSCSI 限定名称 (IQN) 标识符，它是 iSCSI 启动程序或目标的唯一名称。
LUN	逻辑单元编号，用于标识可以呈现给主机进行访问的逻辑单元。
远程存储系统	最初驻留数据的存储系统。远程存储系统可以是 E 系列型号，也可以是其他供应商的系统。
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，这称为"卷"。

术语	说明
远程存储对象	包含允许 E 系列系统识别并连接到远程存储系统的信息的对象。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 系列系统上的标准卷，允许对远程存储设备进行数据访问。
卷	存储数据的容器。它是为主机创建的用于访问数据的逻辑组件。

了解 **SANtricity** 软件中的远程存储功能要求

在使用 Remote Storage 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）
- 用于两个 E 系列控制器的 iSCSI 连接，以通过一个或多个 iSCSI 连接与远程存储系统进行通信
- SANtricity 操作系统 11.71 或更高版本
- 在子模型 ID (SMID) 中启用的远程存储功能

远程系统可以是 E 系列存储系统或其他供应商的系统。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得有快照。
- 在开始导入之前，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禁用资源调配。
- 不支持将远程存储卷直接映射到主机或多个主机。
- 不支持 Web Services Proxy。

- 不支持 iSCSI CHAP 机密。
- 不支持 SMcli。
- 不支持 VMware 数据存储区。
- 当存在导入对时，关系/导入对中只能同时升级一个存储系统。

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"。此卷必须符合以下标准：

- 不能是另一个导入的一部分
- 必须具有在线状态

开始导入后，控制器固件会在后台创建一个远程存储卷。由于该后台进程，远程存储卷无法在 System Manager 中管理，只能用于导入操作。

创建后，远程存储卷将被视为 E 系列系统上的任何其他标准卷，但以下情况除外：

- 可以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。
- 正在执行导入时，无法更改 Data Assurance 设置。
- 无法映射到任何主机，因为它们是严格为导入操作保留的。

每个远程存储卷仅与一个远程存储对象相关联；但是，一个远程存储对象可以与多个远程存储卷相关联。使用以下组合唯一标识远程存储卷：

- 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。目标卷必须符合以下标准：

- 必须为 RAID/DDP 卷。
- 必须具有等于或大于远程存储卷的容量。
- 块大小必须与远程存储卷大小相同。
- 必须具有有效状态（最佳）。
- 不能具有以下任何关系：卷副本、快照副本、异步或同步镜像。
- 无法执行任何重新配置操作：Dynamic Volume Expansion、Dynamic Capacity Expansion、Dynamic Segment Size、Dynamic RAID Migration、Dynamic Capacity Reduction 或 Defragmentation。
- 在导入开始之前无法映射到主机（但是，可以在导入完成后映射它）。

- 无法启用闪存读取缓存 (FRC)。

System Manager 会在导入远程存储向导中自动检查这些要求。仅显示满足所有要求的卷以进行目标卷选择。

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通信。

> 硬件配置在远程存储功能的用户指南中进行了描述，该指南可从 E 系列和 SANtricity 文档中心获取，网址为 "配置硬件"，以及在 "远程存储技术报告"中。

- 对于远程存储系统，收集以下信息：
  - iSCSI IQN
  - iSCSI IP 地址
  - 远程存储设备的 LUN 编号（源卷）
- 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。请参阅 "创建卷"。目标卷必须满足以下要求：
  - 匹配远程存储设备的块大小（源卷）。
  - 容量等于或大于远程存储设备。
  - 状态为 Optimal 且可用。

有关要求的完整列表，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和本地 E 系列存储系统上的卷之间创建映射。完成配置后，导入开始。

> 由于许多变量会影响导入操作及其完成时间，因此我们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按预期工作，并确保导入操作在适当的时间内完成。

步骤

1. 选择菜单：Storage[Remote storage]。
2. 单击 **Import Remote Storage** 。

   此时将显示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。如果要添加其他 iSCSI 连接，请单击 添加其他 **IP** 地址 以包括远程存储的其他 IP 地址。完成后，单击 下一步。

字段详细信息

设置	说明
名称	输入远程存储设备的名称，以便在 System Manager 界面中对其进行标识。 一个名称最多可包含 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。 • **Port**：输入要用于源和目标设备之间通信的端口号。默认情况下，端口号为 3260。

单击 **Next**（下一步）后，将显示 Configure Source（配置源）面板的 **Step 1b**（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 **Next**。

   Configure Target（配置目标）面板打开并显示要作为导入目标的卷候选项。由于块大小、容量或卷可用性，某些卷不会显示在候选项列表中。

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

   如果目标卷的容量大于源卷，则不会将该附加容量报告给连接到 E 系列系统的主机。要使用新容量，必须在导入操作完成并断开连接后在主机上执行文件系统扩展操作。

   在对话框中确认配置后，将显示 Review 面板。

6. 在 Review 面板中，验证设置是否准确，然后单击 **Finish** 以启动导入。

   将打开另一个对话框，询问您是否要启动另一个导入。

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

   导入过程开始后，整个目标卷将被复制的数据覆盖。如果主机在此过程中将任何新数据写入目标卷，则该新数据将传播回远程设备（源卷）。

8. 在 Remote Storage 面板下的 View Operations 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，本地卷将成为远程存储设备的副本。

完成后

当您准备好中断两个卷之间的关系时，从"正在进行的操作"视图中选择导入对象上的*断开连接*。关系断开后，本地卷的性能将恢复正常，并且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，Operations in Progress 对话框将显示完成百分比和预计剩余时间。操作包括更改导入优先级、停止和恢复操作以及断开与操作的连接。

您还可以从主页查看正在进行的操作（菜单：Home[Show operations in progress]）。

步骤

1. 在远程存储页面中，选择 查看操作。

   此时将显示正在执行的操作对话框。

2. 如果需要，请使用 **Actions** 列中的链接来停止和恢复、更改优先级或断开与操作的连接。

   - **Change Priority** — 选择 **Change Priority** 以更改正在进行或待定的操作的处理优先级。将优先级应用于操作，然后单击 **OK**。
   - 停止 — 选择 停止 以暂停从远程存储设备复制数据。导入对之间的关系仍然完好无损，当您准备好继续导入操作时，可以选择 恢复。
   - **Resume** — 选择 **Resume** 以从中断的地方开始已停止或失败的过程。接下来，将优先级应用于 Resume 操作，然后单击 **OK**。此操作 不会 从头开始重新启动导入。如果要从头重新启动该过程，则必须选择 **Disconnect**，然后通过 Import Remote Storage 向导重新创建导入。
   - 断开 — 选择 断开 以断开已停止、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 View/Edit Settings 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[Remote storage]。
2. 从列表中，选择要修改的远程存储对象。
3. 单击 **View/Edit Settings**。

   此时将显示远程存储设置对话框。

4. 单击 **Connection Properties** 选项卡。

   此时将显示远程存储导入的已配置 IP 地址和端口设置。

5. 请执行以下操作之一：
   - 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。
   - **Add** — 单击 **Add**，然后在提供的字段中输入新的 IP 地址和端口信息。单击 **Add** 以确认，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。通过在提供的字段中键入 `delete`来确认操作，然后单击 删除。连接将从远程存储对象列表中删除。
6. 单击 **Save**。

   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，如果您不再希望在本地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

确保没有导入与您计划删除的远程存储对象关联。

关于此任务

删除远程存储对象时，将删除本地和远程设备之间的连接。

步骤

1. 选择菜单：Storage[Remote storage]。
2. 从列表中选择要删除的远程存储对象。
3. 单击 **Remove**。

   此时将显示确认删除远程存储连接对话框。
4. 键入 `remove`确认操作，然后单击*删除*。

   已删除所选远程存储对象。

SANtricity System Manager 远程存储常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

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，请参阅：

- "配置 iSCSI 端口"
- "远程存储技术报告"

为什么系统提示我删除远程卷？

当它达到远程卷的最大数量时，存储系统会自动检测任何未使用的远程卷，并提示您删除它们。

在某些情况下，在创建过程中未清理未使用的远程卷。在开始任何其他导入操作之前，请验证您的系统是否处于最佳状态并且网络连接是否稳定。

为什么我在目标阵列上看不到所有卷？

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，某些卷未出现在目标候选列表中。

要出现在列表中，候选卷必须具有：

- 容量等于或大于远程卷。
- 与远程卷大小相同的块大小。
- Optimal 的当前状态。

如果卷候选项具有以下情况，则将从列表中排除：

- 以下任何关系：卷复制、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。

关于导入中的远程卷，我需要了解什么？

使用远程存储功能时，请注意远程卷是数据的来源。

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。

开始远程存储导入之前，我需要了解哪些信息？

远程存储功能允许您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，请查看以下指南。

配置

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具有到远程存储系统的 iSCSI 连接。
- 在本地 E 系列存储系统上，为导入操作创建目标卷。确保卷的容量等于或大于源卷，块大小与源卷匹配，并且未映射。请参阅 "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：设置[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到新创建的本地 E 系列存储系统主机。

- 从远程存储系统收集以下信息，以便可以创建导入：
  - iSCSI 限定名称 (IQN)
  - iSCSI IP 地址
  - 源数据来源的远程存储设备的 LUN 编号
- 一旦导入过程开始，整个本地目标卷将被复制的数据覆盖。在创建导入后，写入到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，我们建议您在开始导入过程之前备份远程存储系统上的卷。

导入流程

以下步骤概述了导入过程。

1. 访问 System Manager 界面，然后转到 **Remote Storage** 页面。选择 **Import** 以开始新的导入创建。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。

   一旦导入开始，就可以映射目标卷。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. 当您准备中断映射关系时，从 正在进行的操作 面板中对导入对象执行 断开连接。

一旦断开导入连接，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得有快照。
- 在开始导入之前，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禁用资源调配。
- 不支持将远程存储卷直接映射到主机或多个主机。
- 不支持 Web Services Proxy。
- 不支持 iSCSI CHAP 机密。
- 不支持 SMcli。
- 不支持 VMware 数据存储区。
- 当存在导入对时，关系/导入对中只能同时升级一个存储系统。

追加信息

有关远程存储功能的更多信息，请参阅 "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 Hardware 页面上检查组件状态，并执行与这些组件相关的一些功能。

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一些功能：

- 机架 — _机架_是包含存储阵列硬件（控制器、电源/风扇模块和驱动器）的组件。机架有三种尺寸，最多可容纳 12、24 或 60 个驱动器。
- 控制器 — _控制器_是实现存储阵列和管理功能的组合硬件和固件。它包括缓存、驱动器支持和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)。根据托架的大小，托架上最多可安装 12 个、24 个或 60 个驱动器。

了解详情：

- "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。您可以通过选择架子视图右上角的 驱动器 或 控制器 选项卡，在阵列架子的前视图和后视图之间切换。

了解详情：

- "查看货架组件状态和设置"
- "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"
- "货架丢失保护和抽屉丢失保护"

概念

SANtricity System Manager 硬件页面和组件

硬件页面提供存储阵列的物理组件的图形描述。在这里，您可以检查组件状态并执行与这

些组件相关的一些功能。

磁盘架

机架是包含存储阵列硬件的组件（控制器、电源/风扇罐和驱动器）。有两种类型的机架：

- 控制器架 — 包含驱动器、电源/风扇罐和控制器。
- 驱动器架（或*扩展架*）-- 包含驱动器、电源/风扇罐和两个输入/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。

货架有三种尺寸，最多可容纳 12、24 或 60 个驱动器。每个货架都包含一个 ID 号，该 ID 号由控制器固件分配。ID 显示在货架视图的左上角。

硬件页面上的货架视图显示正面或背面的组件。您可以通过从货架视图右上角选择 驱动器 或 控制器 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：

- 前部组件 — 驱动器和空驱动器托架。
- 背面组件 — 控制器和电源/风扇罐（用于控制器架）或 IOM 和电源/风扇罐（用于驱动器架）。

您可以执行以下与货架相关的功能：

- 打开货架的定位灯，以便在机柜或机架中找到货架的物理位置。
- 更改货架视图左上角显示的 ID 号。
- 查看盘架设置，例如安装的驱动器类型和序列号。
- 上下移动货架视图，以匹配存储阵列中的物理布局。

控制器

控制器是实现存储阵列和管理功能的组合硬件和固件。它包括缓存内存、驱动器支持和主机接口支持。

您可以执行以下与控制器相关的功能：

- 配置管理端口的 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。
- 允许局域网外的用户启动 SSH 会话并更改控制器上的设置。
- 将控制器置于离线、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)。根据托架的大小，托架上最多可以安装 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，以便在盘架中找到驱动器的物理位置。

- 查看驱动器状态和设置。
- 重新分配驱动器（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。
- 手动使驱动器发生故障，以便更换。（使驱动器发生故障可让您在更换驱动器之前复制驱动器的内容。）
- 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。

一般硬件术语：

组件	说明
托架	托架是架子上安装驱动器或其他组件的插槽。
控制器	控制器由主板、固件和软件组成。它控制驱动器并实现 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罐。控制器罐装有控制器、主机接口卡 (HIC) 和电池。
驱动器	驱动器是提供数据物理存储介质的电磁机械设备或固态存储设备。
驱动器架	驱动器架也称为扩展架，包含一组驱动器和两个输入/输出模块 (IOM)。IOM 包含将驱动器架连接到控制器架或其他驱动器架的 SAS 端口。
IOM（ESM）	IOM 是一个输入/输出模块，包括用于将驱动器架连接到控制器架的 SAS 端口。在以前的控制器模型中，IOM 被称为环境服务模块（ESM）。
电源/风扇盒	电源/风扇罐是滑入架子的组件。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	搁板是安装在机柜或机架上的外壳。它包含存储阵列的硬件组件。有两种类型的搁板：控制器搁板和驱动器搁板。控制器搁板包括控制器和驱动器。驱动器搁板包括输入/输出模块 (IOM) 和驱动器。
存储阵列	存储阵列包括盘架、控制器、驱动器、软件和固件。

控制器条款：

组件	说明
控制器	控制器由主板、固件和软件组成。它控制驱动器并实现 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罐。控制器罐装有控制器、主机接口卡 (HIC) 和电池。
DHCP	动态主机配置协议 (DHCP) 是在 Internet Protocol (IP) 网络上用于动态分发网络配置参数（例如 IP 地址）的协议。
DNS	域名系统 (DNS) 是连接到互联网或专用网络的设备的命名系统。DNS 服务器维护域名目录并将其转换为互联网协议 (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，另一个控制器会接管其 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，两个设备可以同时在两个方向上进行通信。在半双工模式下，设备一次可以在一个方向上通信（一个设备发送消息，而另一个设备接收消息）。
HIC	主机接口卡（HIC）可以可选地安装在控制器罐内。内置在控制器中的主机端口称为基板主机端口。内置在 HIC 中的主机端口称为 HIC 端口。
ICMP PING 响应	互联网控制消息协议 (ICMP) 是联网计算机的操作系统用于发送消息的协议。ICMP 消息确定主机是否可达以及往返该主机传输数据包需要多长时间。
MAC 地址	以太网使用媒体访问控制标识符（MAC 地址）来区分连接同一物理传输网络接口上两个端口的单独逻辑通道。
管理客户端	管理客户端是安装浏览器以访问 System Manager 的计算机。
MTU	最大传输单元 (MTU) 是可以在网络中发送的最大大小的数据包或帧。
NTP	网络时间协议 (NTP) 是一种用于数据网络中计算机系统之间时钟同步的网络协议。
单工配置	Simplex 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，其行为就像与同一设备（交换机、路由器等）支持的其他网络在物理上分离一样。

驱动器术语：

组件	说明
DA	数据保障 (DA) 是一项检查和纠正数据通过控制器传输到驱动器时可能发生的错误的功能。数据保障可以在池或卷组级别启用，主机使用支持 DA 的 I/O 接口，如 Fibre Channel。
驱动器安全功能	驱动器安全是一种存储阵列功能，可通过全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器提供额外的安全层。当这些驱动器与驱动器安全功能一起使用时，它们需要安全密钥才能访问其数据。当驱动器从阵列中物理卸下时，它们必须安装在另一个阵列中才能运行，此时，它们将处于安全锁定状态，直到提供正确的安全密钥。
驱动器架	驱动器架也称为扩展架，包含一组驱动器和两个输入/输出模块 (IOM)。IOM 包含将驱动器架连接到控制器架或其他驱动器架的 SAS 端口。
DULBE	Deallocated or Unwritten Logical Block Error (DULBE) 是 NVMe 驱动器上的一个选项，允许 EF300 或 EF600 存储阵列支持资源调配的卷。
FDE 驱动器	全磁盘加密 (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，该芯片在写入过程中对数据进行加密，然后在读取过程中对数据进行解密。
FIPS 驱动器	FIPS 驱动器使用联邦信息处理标准 (FIPS) 140-2 level 2。它们本质上是 FDE 驱动器，符合美国政府确保强大加密算法和方法的标准。FIPS 驱动器具有比 FDE 驱动器更高的安全标准。
HDD	硬盘驱动器 (HDD) 是使用具有磁性涂层的旋转金属盘片的数据存储设备。
热备盘驱动器	热备盘在 RAID 1、RAID 5 或 RAID 6 卷组中充当备用驱动器。它们是功能齐全的驱动器，不包含任何数据。如果卷组中的驱动器出现故障，控制器会自动将故障驱动器的数据重建到热备盘。
NVMe	Non-Volatile Memory Express (NVMe) 是专为基于闪存的存储设备（如 SSD 驱动器）设计的接口。与以前的逻辑设备接口相比，NVMe 减少了 I/O 开销，并包括性能改进。
SAS	串行连接 SCSI (SAS) 是一种点对点串行协议，它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 (FDE) 驱动器，也可以是联邦信息处理标准 (FIPS) 驱动器，它们在写入期间加密数据，在读取期间解密数据。这些驱动器被认为是安全_有能力_的，因为它们可以使用 Drive Security 功能用于额外的安全性。如果为与这些驱动器一起使用的卷组和池启用了 Drive Security 功能，则驱动器将变得安全_已启用_。

组件	说明
启用安全功能的驱动器	启用安全的驱动器与 Drive Security 功能一起使用。当您启用 Drive Security 功能，然后将 Drive Security 应用于支持安全的驱动器上的池或卷组时，驱动器将变为启用安全。只能通过配置了正确安全密钥的控制器进行读写访问。这种额外的安全性可以防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。
SSD	固态硬盘（SSD）是使用固态内存（闪存）永久存储数据的数据存储设备。SSD 模拟传统硬盘驱动器，并提供与硬盘驱动器相同的接口。

iSCSI 术语：

术语	说明
CHAP	质询握手身份验证协议 (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。
控制器	控制器由主板、固件和软件组成。它控制驱动器并实现 System Manager 功能。
DHCP	动态主机配置协议 (DHCP) 是在 Internet Protocol (IP) 网络上用于动态分发网络配置参数（例如 IP 地址）的协议。
IB	InfiniBand (IB) 是高性能服务器和存储系统之间数据传输的通信标准。
ICMP PING 响应	互联网控制消息协议 (ICMP) 是联网计算机的操作系统用于发送消息的协议。ICMP 消息确定主机是否可达以及往返该主机传输数据包需要多长时间。
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	用于 RDMA 的 iSCSI 扩展（iSER）是一种协议，它扩展了 iSCSI 协议以便通过 RDMA 传输（例如 InfiniBand 或以太网）进行操作。
iSNS	Internet Storage Name Service (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 Fibre Channel 设备。
MAC 地址	以太网使用媒体访问控制标识符（MAC 地址）来区分连接同一物理传输网络接口上两个端口的单独逻辑通道。
管理客户端	管理客户端是安装浏览器以访问 System Manager 的计算机。
MTU	最大传输单元 (MTU) 是可以在网络中发送的最大大小的数据包或帧。
RDMA	远程直接内存访问 (RDMA) 是一种技术，允许网络计算机在不涉及任何一台计算机的操作系统的情况下交换主内存中的数据。
未命名发现会话	启用未命名发现会话的选项后，iSCSI 启动程序无需指定目标 IQN 即可检索控制器的信息。

NVMe 术语：

术语	说明
InfiniBand	InfiniBand (IB) 是高性能服务器和存储系统之间数据传输的通信标准。
命名空间	命名空间是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 控制器的命名空间唯一标识符，可以设置为 1 到 255 之间的值。它类似于 SCSI 中的逻辑单元号 (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持久性内存。
NVMe	Non-Volatile Memory Express (NVMe) 是专为基于闪存的存储设备（如 SSD 驱动器）设计的接口。与以前的逻辑设备接口相比，NVMe 减少了 I/O 开销，并包括性能改进。
NVMe-oF	Non-Volatile Memory Express over Fabrics (NVMe-oF) 是一种规范，使 NVMe 命令和数据能够在主机和存储之间通过网络传输。
NVMe 控制器	在主机连接过程中创建 NVMe 控制器。它提供了主机和存储阵列中的命名空间之间的访问路径。
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	远程直接内存访问 (RDMA) 通过在网络接口卡 (NIC) 硬件中实现传输协议，实现更直接的数据进出服务器。
RoCE	RDMA over Converged Ethernet (RoCE) 是一种网络协议，允许通过以太网进行远程直接内存访问 (RDMA)。
SSD	固态硬盘（SSD）是使用固态内存（闪存）永久存储数据的数据存储设备。SSD 模拟传统硬盘驱动器，并提供与硬盘驱动器相同的接口。

管理货架组件

在 **SANtricity System Manager** 中查看硬件组件

硬件页面提供排序和过滤功能，可以更轻松地查找组件。

步骤

1. 选择 **Hardware**。
2. 使用下表中描述的函数查看硬件组件。

功能	说明
驱动器、控制器和组件视图	要在正面和背面货架视图之间切换，请从最右侧选择 **Drives** 或 **Controllers & Components**（显示的链接取决于当前视图）。**Drives** 视图显示驱动器和任何空驱动器托架。**Controllers & Components** 视图显示控制器以及任何 IOM (ESM) 模块、电源/风扇罐或空控制器托架。在页面底部，您还可以选择 **Show all drives**。
驱动器视图筛选器	如果存储阵列包含具有不同类型物理和逻辑属性的驱动器，则 **Hardware** 页面包括驱动器视图筛选器。这些筛选字段通过限制页面上显示的驱动器类型，帮助您快速定位特定驱动器。在 **Show drives that are…** 下，单击左侧的筛选字段（默认情况下，显示 **Any drive type**）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 **Anywhere in the storage array**）以查看逻辑属性（例如，卷组分配）的下拉列表。您可以同时或单独使用这些筛选条件。 如果存储阵列包含的驱动器都具有相同的物理属性，则不会显示左侧的 **Any drive type** 字段。如果驱动器都位于同一个逻辑位置，则不会显示右侧的 **Anywhere in the storage array** 字段。
图例	组件以特定颜色显示，以描绘其角色状态。要展开和折叠这些状态的描述，请单击 **Legend**。
显示状态图标详细信息	状态指示器可以包括可用性状态的文本描述。单击 **Show status icon details** 以显示或隐藏此状态文本。
机架/机架图标	每个盘架视图提供相关命令的列表，以及属性和状态。单击 **Shelf** 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。
上架顺序	货架可以在硬件页面上重新排列。使用每个货架视图右上角的上下箭头更改货架的顶部/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、风扇和电源的状态描述。

步骤

1. 选择 **Hardware**。
2. 要查看后部或前部组件：
   - 如果要查看控制器和电源/风扇罐组件，但显示的是驱动器，请单击 **Controllers & Components** 选项卡。
   - 如果要查看驱动器，但显示的是控制器和电源/风扇罐组件，请单击 **Drives** 选项卡。

3. 要查看或隐藏弹出式状态描述：
   - 如果要查看状态图标的弹出式描述，请单击货架视图右上角的 **Show status icon details**（选中复选框）。
   - 要隐藏弹出式描述，请再次单击 **Show status icon details** （清除复选框）。
4. 如果要查看完整的状态详细信息，请在货架视图中选择组件，然后选择 **View settings**。
5. 如果要查看彩色组件的描述，请选择 **Legend**。

在 **SANtricity System Manager** 中显示正面和背面视图

硬件页面可以显示货架的前视图或后视图。

关于此任务

后视图显示控制器/IOM 和电源风扇罐。前视图显示驱动器。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。
4. 您也可以选择位于页面底部的 **Show all front** 或 **Show all back**。

更改 **SANtricity System Manager** 中磁盘架的查看顺序

您可以更改 Hardware 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. 选择 **Hardware**。
2. 从货架视图的右上角，选择向上或向下箭头以重新排列 Hardware 页面上显示的货架顺序。

在 **SANtricity System Manager** 中打开磁盘架定位灯

要查找 Hardware 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. 选择 **Hardware**。
2. 选择 Controller Shelf 或 Drive Shelf 的下拉列表，然后选择 **Turn on locator light**。

   货架的定位灯打开。
3. 物理定位货架后，返回对话框并选择 **Turn off**。

在 **SANtricity System Manager** 中更改磁盘架 **ID**

货架 ID 是唯一标识存储阵列中货架的数字。货架在每个货架视图的左上角连续编号，从 00 或 01 开始。

关于此任务

控制器固件会自动分配货架 ID，但如果要创建不同的订购方案，您可以更改该编号。

步骤

1. 选择 **Hardware**。
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。

   此对话框不显示当前分配给活动磁盘架的 ID。

4. 选择一个可用号码，然后单击 保存。

   根据您选择的编号，可以在"硬件"页面上重新排列货架顺序。如果需要，您可以使用每个货架右上角的向上/向下箭头重新调整顺序。

在 **SANtricity System Manager** 中查看磁盘架组件状态和设置

硬件页面提供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

可用组件取决于机架类型：

- 驱动器架 — 在一个架子中包含一组驱动器、电源/风扇罐、输入/输出模块 (IOM) 和其他支持组件。
- **Controller shelf** — 在一个架子中包含一组驱动器、一个或两个 controller 罐、电源/风扇罐和其他支持组件。

步骤

1. 选择 **Hardware**。
2. 选择 Controller Shelf 或 Drive Shelf 的下拉列表，然后选择 **View Settings**。

   此时将打开"Shelf Components Settings"对话框，其中包含显示与货架组件相关的状态和设置的选项卡。根据所选货架类型，表格中描述的某些选项卡可能不会显示。

选项卡	说明
磁盘架	**Shelf** 选项卡显示以下属性： • **Shelf ID** — 唯一标识存储阵列中的货架。控制器固件分配此编号，但您可以通过选择菜单：Shelf[Change ID] 进行更改。 • **Shelf path redundancy** — 指定货架和控制器之间的连接是否具有备用方法 (是) 或没有 (否)。 • 当前驱动器类型 — 显示内置于驱动器中的技术类型（例如，具有安全功能的 SAS 驱动器）。如果有多种驱动器类型，则显示两种技术。 • 序列号 — 显示货架的序列号。
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 Optimal、Failed、Optimal (Miswire) 或 Uncertified。其他信息包括固件版本和配置设置版本。 选择 **Show more settings** 以查看最大和当前数据速率，以及卡通信的状态（是或否）。 您还可以通过选择 IOM 图标 （位于 Shelf 下拉列表旁边）来查看此状态。
电源	**Power Supplies** 选项卡显示电源盒和电源本身的状态。状态可以是 Optimal、Failed、Removed 或 Unknown。它还显示了电源的部件号。 您还可以通过选择 Shelf 下拉列表旁边的电源图标 来查看此状态。
风扇	**Fans** 选项卡显示风扇罐和风扇本身的状态。状态可以是 Optimal、Failed、Removed 或 Unknown。 您还可以通过选择 Shelf 下拉列表旁边的 Fan 图标 来查看此状态。
温度	**Temperature** 选项卡显示货架组件的温度状态，例如传感器、控制器和电源/风扇罐。状态可以是 Optimal、Nominal temperature exceeded、Maximum temperature exceeded 或 Unknown。 您还可以通过选择 Shelf 下拉列表旁边的温度图标 来查看此状态。

选项卡	说明
电池	**Batteries** 选项卡显示控制器电池的状态。状态可以是 Optimal、Failed 、Removed 或 Unknown。其他信息包括电池寿命、更换前天数、学习周期以及学习周期之间的周数。 您还可以通过选择 Shelf 下拉列表旁边的 Batteries 图标 来查看此状态。
SFP	**SFPs** 选项卡显示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 **Show more settings** 以查看 SFP 的部件号、序列号和供应商。 您还可以通过选择 Shelf 下拉列表旁边的 SFP 图标 来查看此状态。

3. 单击 **Close**。

在 **SANtricity System Manager** 中更新电池学习周期

学习周期是用于校准智能电池仪表的自动周期。周期计划在同一天和同一时间以 8 周的间隔自动启动（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

更新学习周期会影响两个控制器电池。

步骤

1. 选择 **Hardware**。
2. 选择 Controller Shelf 的下拉列表，然后选择 **View settings**。
3. 选择 **Batteries** 选项卡。
4. 选择 **Update battery learn cycles** 。

   此时将打开更新电池学习周期对话框。

5. 从下拉列表中选择一个新的日期和时间。
6. 单击 **Save**。

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：在线、离线和服务模式。

在线状态

在线状态是控制器的正常工作状态。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，其状态设置为最佳。

离线状态

当存储阵列中有两个控制器时，离线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离线状态：发出显式命令或控制器失败。控制器只能通过发出另一个显式命令或替换出现故障的控制器来退出离线状态。仅当存储阵列中有两个控制器时，才能将控制器置于离线状态。

当控制器处于离线状态时，满足以下条件：

- 控制器不可用于 I/O。
- 您无法通过该控制器管理存储阵列。
- 该控制器当前拥有的任何卷都将移动到另一个控制器。
- 已禁用缓存镜像，所有卷都已更改为通过缓存模式写入。

服务模式

服务模式通常仅由技术支持人员用于将所有存储阵列卷移动到一个控制器，以便可以诊断另一个控制器。控制器必须手动置于服务模式，且必须在服务操作完成后手动恢复联机。

当控制器处于服务模式时，满足以下条件：

- 控制器不可用于 I/O。
- 技术支持人员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。
- 该控制器当前拥有的任何卷都将移动到另一个控制器。
- 已禁用缓存镜像，所有卷都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，控制器在两个网络端口上都启用了 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。您还可以使用 IPv6 无状态自动配置。

默认情况下，在新控制器上禁用 IPv6 ，但您可以使用替代方法配置管理端口 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"link down"状态，即与 LAN 断开连接时，系统将其配置报告为静态，显示 IP 地址为 0.0.0.0（早期版本），或启用 DHCP 但未报告 IP 地址（晚期版本）。网络端口处于"link up"状态（即连接到 LAN）后，尝试通过 DHCP 获取 IP 地址。

如果控制器无法在给定的网络端口上获取 DHCP 地址，它将恢复为默认 IP 地址，这可能需要长达 3 分钟。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：

- 在控制器上保留端口 2 以供客户支持使用。请勿更改默认网络设置（启用 DHCP）。
- 要为 E4000、E2800 和 E5700 控制器设置静态 IP 地址，请使用 SANtricity System Manager。要为 E2700 和 E5600 控制器设置静态 IP 地址，请使用 SANtricity Storage Manager。配置静态 IP 地址后，它将在所有链路断开/启动事件中保持设置。
- 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。使用永久的 DHCP 租约。

> 默认地址不会在链路关闭事件中保留。当控制器上的网络端口设置为使用 DHCP 时，控制器会尝试在每个链路启动事件（包括电缆插入、重新启动和电源循环）上获取 DHCP 地址。每次 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

控制器包括一个用于系统管理的 Ethernet 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

在此过程中，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以访问控制器和 System Manager 的网络。

> 不要在任何一个控制器上使用端口 2。端口 2 保留给技术支持人员使用。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 单击具有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。
4. 选择 **Configure management ports**。

   此时将打开配置管理端口对话框。

5. 确保显示端口 1，然后单击 **Next**。
6. 选择配置端口设置，然后单击 **Next**。

   字段详细信息

字段	说明
速度和双工模式	如果您希望 System Manager 确定存储阵列和网络之间的传输参数，请保留自动协商设置；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。只有有效的速度和双工组合显示在列表中。
启用 IPv4 / 启用 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*，点击*下一步*后将打开一个对话框，用于选择 IPv4 设置。如果您选择*启用 IPv6*，点击*下一步*后将打开一个对话框，用于选择 IPv6 设置。如果您选择这两个选项，则首先打开 IPv4 设置的对话框，然后单击*下一步*后，将打开 IPv6 设置的对话框。

7. 自动或手动配置 IPv4 和/或 IPv6 设置。

   字段详细信息

字段	说明
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，您可以剪切地址并将其粘贴到字段中。）对于 IPv4，包括网络子网掩码和网关。对于 IPv6，包括可路由 IP 地址和路由器 IP 地址。 如果更改 IP 地址配置，则会丢失到存储阵列的管理路径。如果您使用 SANtricity Unified Manager 全局管理网络中的阵列，请打开用户界面并转到菜单：Manage[Discover]。如果使用 SANtricity Storage Manager，则必须从企业管理窗口（EMW）中删除设备，通过选择菜单将其添加回 EMW：Edit[Add Storage Array]，然后输入新的 IP 地址。

8. 单击 **Finish**。

结果

管理端口配置显示在控制器设置的 Management Ports 选项卡中。

在 **SANtricity System Manager** 中配置 **NTP** 服务器地址

您可以配置到网络时间协议 (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的域名、IPv4 地址或 IPv6 地址。

> 如果为 NTP 服务器输入一个或多个域名，还必须配置 DNS 服务器以解析 NTP 服务器地址。仅需在配置了 NTP 并提供了域名的控制器上配置 DNS 服务器。

关于此任务

NTP 使存储阵列能够使用简单网络时间协议 (SNTP) 自动将控制器的时钟与外部主机同步。控制器定期查询配置的 NTP 服务器，然后使用结果更新其内部时钟。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。如果两个控制器都未启用 NTP，则控制器定期彼此同步其时钟。

> 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硬件或通信故障期间保持同步的能力。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 单击要配置的控制器。

   此时将显示控制器的上下文菜单。
4. 选择 **Configure NTP server**。

   配置网络时间协议 (NTP) 服务器对话框打开。
5. 选择 **I want to enable NTP on Controller** (**A** 或 **B**)。

   此时此对话框中将显示其他选择。
6. 从下列选项中选择一项：
   - 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。（这些地址字段在您选择单选按钮后出现。）服务器地址可以是完全限定域名、IPv4 地址或 IPv6 地址。
7. 可选： 输入备份 NTP 服务器的服务器信息和身份验证凭据。
8. 单击 **Save**。

结果

NTP 服务器配置显示在控制器设置的 **DNS / NTP** 选项卡中。

在 **SANtricity System Manager** 中配置 **DNS** 服务器地址

域名系统 (DNS) 用于解析控制器和网络时间协议 (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 服务器和可选备份 DNS 服务器的地址。这些地址可以是 IPv4 地址或 IPv6 地址。

关于此任务

此过程描述了如何指定主 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) 配置了存储阵列的管理端口，并且有一个或多个与 DHCP 设置相关联的 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. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 选择要配置的控制器。

   此时将显示控制器的上下文菜单。

4. 选择 **Configure DNS server**。

   配置域名系统 (DNS) 服务器对话框打开。

5. 从下列选项中选择一项：
   - 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 DNS 服务器。

   - 手动指定 **DNS** 服务器地址 — 输入主 DNS 服务器地址和备份 DNS 服务器地址。备份服务器是可选的。（这些地址字段在您选择单选按钮后显示。）这些地址可以是 IPv4 地址或 IPv6 地址。
6. 单击 **Save**。
7. 对另一个控制器重复这些步骤。

结果

DNS 配置显示在控制器设置的 **DNS / NTP** 选项卡中。

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. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 请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 **View settings**。
   - 选择控制器图标（**Shelf** 下拉列表旁边）。对于双工配置，请从对话框中选择 **Controller A** 或 **Controller B**，然后单击*下一步*。

     此时将打开 Controller Settings 对话框。

4. 选择选项卡以在属性设置之间移动。

   有些选项卡的右上角有 **Show more settings** 的链接。

字段详细信息

选项卡	说明
基础	显示控制器状态、型号名称、替换部件号、当前固件版本和非易失性静态随机存取存储器 (NVSRAM) 版本。
缓存	显示控制器的缓存设置，包括数据缓存、处理器缓存和缓存备份设备。缓存备份设备用于在控制器断电时备份缓存中的数据。状态可以是 Optimal 、Failed、Removed、Unknown、Write Protected 或 Incompatible。
主机接口	显示主机接口信息和每个端口的链路状态。主机接口是控制器和主机之间的连接，例如 Fibre Channel 或 iSCSI。 主机接口卡 (HIC) 位置位于基板或插槽（托架）中。"基板"表示 HIC 端口内置于控制器中。"插槽"端口位于可选 HIC 上。
驱动器接口	显示驱动器接口信息和每个端口的链路状态。驱动器接口是控制器与驱动器（例如 SAS）之间的连接。
管理端口	显示管理端口详细信息，例如用于访问控制器的主机名以及是否已启用远程登录。管理端口连接控制器和管理客户端，这是安装浏览器以访问 System Manager 的地方。
DNS / NTP 服务器	如果已在 System Manager 中配置 DNS 服务器和 NTP 服务器，则显示这些服务器的寻址方法和 IP 地址。 域名系统 (DNS) 是连接到互联网或专用网络的设备的命名系统。DNS 服务器维护域名目录并将其转换为互联网协议 (IP) 地址。 网络时间协议 (NTP) 是一种用于数据网络中计算机系统之间时钟同步的网络协议。

5. 单击 **Close**。

在 **SANtricity System Manager** 中配置远程登录 **(SSH)**

通过启用远程登录，您可以允许来自局域网外的用户启动 SSH 会话并访问控制器上的设置。

对于 SANtricity 版本 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 (MFA)。对于 SANtricity 版本 11.73 及更早版本，此功能_不_包括使用 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，只有技术支持人员应使用远程登录功能。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 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。

4. 选择 **Configure remote login (SSH)**。（对于 SANtricity 版本 11.73 及更早版本，此菜单项为 **Change remote login**。）

   此时将打开对话框以启用远程登录。

5. 选中 启用远程登录 复选框。

   此设置为远程登录提供了三个授权选项：

   - 仅限密码。对于此选项，您已完成操作，可以单击 **Save**。如果您有双工系统，则可以按照前面的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，请继续下一步。
   - 密码和 **SSH** 密钥。对于此选项，选中 **Require authorized public key and password for remote login** 复选框，然后继续下一步。

6. 填写 **Authorized public key** 字段。此字段包含授权公钥列表，格式为 OpenSSH **authorized_keys** 文件。

   填写 授权公钥 字段时，请注意以下准则：

   - **Authorized public key** 字段适用于两个控制器，并且只需要在第一个控制器上配置。
   - **authorized_keys** 文件每行应仅包含一个密钥。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 "配置 OpenSSH 的授权密钥"。
   - **authorized_keys** 文件应与以下示例类似：

     ```
     ssh-rsa
     AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
     9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
     j1tHymwtbdhPuipd2wIDAQAB
     ```

7. 完成后，单击 保存 。
8. 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。如果您同时配置密码和 SSH 密钥的选项，请务必再次选中 **Require authorized public key and password for remote login** 复选框。
9. 技术支持完成故障排除后，您可以通过返回配置远程登录对话框并取消选中*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的 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处于服务模式，则可以将其重新联机。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 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。

4. 选择 **Place online**，并确认要执行此操作。

结果

多路径驱动程序检测恢复的首选路径可能需要长达 10 分钟的时间。

当收到每个卷的 I/O 请求时，此控制器最初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 **Redistribute volumes** 命令手动重新分配卷。

在 **SANtricity System Manager** 中使控制器脱机

如果系统指示您执行此操作，则可以将控制器置于离线状态。

开始之前

- 存储阵列必须有两个控制器。未脱机的控制器必须处于联机状态（处于最佳状态）。
- 确保没有正在使用的卷，或者在使用这些卷的所有主机上都安装了多路径驱动程序。

关于此任务

除非 Recovery Guru 或技术支持人员指示，否则请勿将控制器置于离线状态。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 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。

4. 选择 **Place offline**，并确认要执行此操作。

结果

System Manager 可能需要几分钟才能将控制器的状态更新为脱机。在更新状态之前，请勿开始任何其他操作。

在 **SANtricity System Manager** 中将控制器置于服务模式

如果系统指示您执行此操作，则可以将控制器置于服务模式。

开始之前

- 存储阵列必须有两个控制器。未处于维修模式的控制器必须处于联机状态（处于最佳状态）。
- 确保没有正在使用的卷，或者在使用这些卷的所有主机上都安装了多路径驱动程序。

> 将控制器置于服务模式可能会显著降低性能。除非技术支持人员指示，否则请勿将控制器置于服务模式。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 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。
4. 选择 **Place in service mode**，并确认要执行此操作。

在 **SANtricity System Manager** 中重置（重新启动）控制器

某些问题需要重置（重新启动）控制器。即使您没有物理访问权限，也可以重置控制器。

开始之前

- 存储阵列必须有两个控制器。未重置的控制器必须处于联机状态（处于最佳状态）。
- 确保没有正在使用的卷，或者在使用这些卷的所有主机上都安装了多路径驱动程序。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 单击要重置的控制器。

   此时将显示控制器的上下文菜单。
4. 选择 **Reset**，并确认要执行此操作。

管理 iSCSI 端口

在 SANtricity System Manager 中配置 iSCSI 端口

如果您的控制器包含 iSCSI 主机连接，则可以从"硬件"页面配置 iSCSI 端口设置。

开始之前

- 您的控制器必须包含 iSCSI 端口；否则，iSCSI 设置不可用。
- 您必须知道网络速度（端口和主机之间的数据传输速率）。

> 仅当您的存储阵列支持 iSCSI 时，才会显示 iSCSI 设置和功能。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 单击具有要配置的 iSCSI 端口的控制器。

   此时将显示控制器的上下文菜单。
4. 选择 **Configure iSCSI ports**。

   > 仅当 System Manager 检测到控制器上的 iSCSI 端口时，才会显示 **Configure iSCSI ports** 选项。

   此时将打开配置 iSCSI 端口对话框。
5. 在下拉列表中，选择要配置的端口，然后单击 **Next**。
6. 选择配置端口设置，然后单击 **Next**。

   要查看所有端口设置，请单击对话框右侧的 **Show more port settings** 链接。

字段详细信息

端口设置	说明
配置的以太网端口速度（仅适用于某些类型的 Host Interface Card）	选择与端口上 SFP 的速度能力相匹配的速度。
前向纠错 (FEC) 模式（仅适用于某些类型的主机接口卡）	如果需要，请为指定的主机端口选择一种 FEC 模式。 Reed Solomon 模式不支持 25 Gbps 端口速度。
启用 IPv4 / 启用 IPv6	选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。 如果要禁用端口访问，请取消选中两个复选框。
TCP 侦听端口（点击 显示更多端口设置 即可使用。）	如有必要，请输入新的端口号。 侦听端口是控制器用于侦听来自主机 iSCSI 启动器的 iSCSI 登录的 TCP 端口号。默认侦听端口为 3260。您必须输入 3260 或介于 49152 和 65535 之间的值。
MTU 大小（可通过单击*显示更多端口设置*获得。）	如有必要，请输入最大传输单元 (MTU) 的新大小（以字节为单位）。 默认最大传输单元 (MTU) 大小为每帧 1500 字节。必须输入介于 1500 和 9000 之间的值。
启用 ICMP PING 响应	选择此选项以启用互联网控制消息协议 (ICMP)。联网计算机的操作系统使用此协议发送消息。这些 ICMP 消息确定主机是否可达以及往返该主机传输数据包所需的时间。

如果您选择了*启用 IPv4*，点击*下一步*后将打开一个对话框，用于选择 IPv4 设置。如果您选择了*启用 IPv6*，点击*下一步*后将打开一个对话框，用于选择 IPv6 设置。如果您选择了这两个选项，则首先打开 IPv4 设置的对话框，然后单击*下一步*后，将打开 IPv6 设置的对话框。

7. 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

端口设置	说明
自动获取配置	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，然后在字段中输入静态地址。（如果需要，您可以将地址剪切并粘贴到字段中。）对于 IPv4，包括网络子网掩码和网关。对于 IPv6，包括可路由 IP 地址和路由器 IP 地址。
启用 VLAN 支持（通过单击*显示更多设置*可用。）	选择此选项以启用 VLAN 并输入其 ID。VLAN 是一种逻辑网络，其行为就像与相同交换机、相同路由器或两者都支持的其他物理和虚拟局域网 (LAN) 在物理上分离一样。
启用以太网优先级（通过单击 **Show more settings** 可用。）	选择此选项可启用确定访问网络的优先级的参数。使用滑块选择 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，许多站点可能会争夺对网络的访问权限。访问采用先到先得的方式。两个站点可能会同时尝试访问网络，这会导致两个站点后退并等待重试。对于交换式以太网，此过程被最小化，其中只有一个站点连接到交换机端口。

8. 单击 **Finish**。

在 **SANtricity System Manager** 中配置 **iSCSI** 身份验证

为了在 iSCSI 网络中提供额外的安全性，您可以在控制器（目标）和主机（启动器）之间设置身份验证。

System Manager 使用质询握手身份验证协议 (CHAP) 方法，该方法在初始链接期间验证目标和启动器的身份。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 密码之前或之后为启动器（iSCSI 主机）设置 CHAP 密码。在执行此任务中的说明之前，应等待主机先建立 iSCSI 连接，然后在单个主机上设置 CHAP 密码。建立连接后，主机的 IQN 名称及其 CHAP 密码将列在 iSCSI 身份验证的对话框中（在此任务中进行了描述），您无需手动输入它们。

关于此任务

您可以选择以下身份验证方法之一：

- 单向身份验证 — 使用此设置可允许控制器对 iSCSI 主机的标识进行身份验证（单向身份验证）。
- 双向身份验证 — 使用此设置允许控制器和 iSCSI 主机执行身份验证（双向身份验证）。此设置通过使控制器能够对 iSCSI 主机的身份进行身份验证来提供第二级安全性；进而使 iSCSI 主机能够对控制器的身份进行身份验证。

只有当您的存储阵列支持 iSCSI 时，iSCSI 设置和功能才会显示在"设置"页面上。

步骤

1. 选择菜单：Settings[System]。
2. 在 iSCSI 设置下，单击 配置身份验证。

   此时将显示"配置身份验证"对话框，其中显示当前设置的方法。它还显示是否有任何主机配置了 CHAP 密码。

3. 选择以下选项之一：
   - 无身份验证 — 如果您不希望控制器对 iSCSI 主机的身份进行身份验证，请选择此选项并单击*完成*。对话框关闭，完成配置。
   - 单向身份验证 — 要允许控制器验证 iSCSI 主机的身份，请选择此选项并单击 **Next** 以显示 Configure Target CHAP 对话框。
   - 双向身份验证 — 要允许控制器和 iSCSI 主机执行身份验证，请选择此选项，然后单击*下一步*以显示"配置目标 CHAP"对话框。
4. 对于单向或双向身份验证，输入或确认控制器（目标）的 CHAP 密钥。CHAP 密码必须介于 12 到 57 个可打印的 ASCII 字符之间。

   如果之前配置了控制器的 CHAP 密码，则字段中的字符将被屏蔽。如有必要，您可以替换现有字符（新字符不会被屏蔽）。

5. 执行以下操作之一：
   - 如果您正在配置 *one-way* 身份验证，请点击 **Finish**。对话框关闭，配置完成。
   - 如果要配置_双向_身份验证，请单击 下一步 以显示配置启动器 CHAP 对话框。
6. 对于双向身份验证，请输入或确认任何 iSCSI 主机（启动器）的 CHAP 密码，该密码可以为 12 到 57 个可打印 ASCII 字符。如果不想为特定主机配置双向身份验证，请将 Initiator CHAP Secret 字段留空。

   如果之前配置了主机的 CHAP 密码，则该字段中的字符将被屏蔽。如有必要，您可以替换现有字符（新字符不会被屏蔽）。

7. 单击 **Finish**。

结果

除非您未指定身份验证，否则在控制器和 iSCSI 主机之间的 iSCSI 登录序列期间进行身份验证。

在 **SANtricity System Manager** 中启用 **iSCSI** 发现设置

您可以启用与 iSCSI 网络中存储设备发现相关的设置。

目标发现设置允许您使用 Internet Storage Name Service (iSNS) 协议注册存储阵列的 iSCSI 信息，并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

您可以启用以下与 iSCSI 发现相关的设置：

- 启用 **iSNS** 服务器以注册目标 — 启用后，存储阵列将其 iSCSI Qualified Name (IQN) 和端口信息注册到 iSNS 服务器。此设置允许 iSNS 发现，以便启动器可以从 iSNS 服务器检索 IQN 和端口信息。
- 启用未命名发现会话 — 启用未命名发现会话后，发起方（iSCSI 主机）无需在登录序列期间为发现类型连接提供目标（控制器）的 IQN。禁用时，主机确实需要提供 IQN 以建立对控制器的发现会话。但是，正常（I/O 承载）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。

只有当您的存储阵列支持 iSCSI 时，iSCSI 设置和功能才会显示在"设置"页面上。

步骤

1. 选择菜单：Settings[System]。
2. 在 **iSCSI** 设置*下，单击*查看/编辑目标发现设置。

   此时将显示"目标发现设置"对话框。在 **Enable iSNS server**… 字段下方，该对话框指示控制器是否已经注册。

3. 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** 服务器自动获取配置 — 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。

     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.” 此选项需要在数据字节 0xa-0xd (10-13) 中包含 iSNS 服务器 IPv4 地址。

   - 手动指定静态配置 — 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）。
4. 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，iSCSI 启动程序无需指定目标 IQN 即可检索控制器的信息。
   - 禁用时，除非启动器提供目标 IQN，否则将阻止发现会话。禁用未命名的发现会话可提高安全性。
5. 单击 **Save**。

结果

当 System Manager 尝试向 iSNS 服务器注册控制器时，将出现一个进度条。此过程可能需要长达五分钟时间。

在 **SANtricity System Manager** 中查看 **iSCSI** 统计信息包

您可以查看有关 iSCSI 连接到存储阵列的数据。

关于此任务

System Manager 显示这些类型的 iSCSI 统计信息。所有统计信息都是只读的，无法设置。

System Manager 中显示的统计数据类型基于您的存储阵列可用的统计数据。

- 以太网 **MAC** 统计信息 — 提供媒体访问控制 (MAC) 的统计数据。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发送到子网内的目的地。

- 以太网 **TCP/IP** 统计信息 — 提供 TCP/IP 的统计数据，即 iSCSI 设备的传输控制协议 (TCP) 和互联网协议 (IP)。使用 TCP，网络主机上的应用程序可以相互创建连接，从而可以在数据包中交换数据。IP 是一种面向数据的协议，可在分组交换的互联网络中传输数据。IPv4 统计数据和 IPv6 统计数据分别显示。
- 以太网内核统计 — 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 统计信息选项相似。但是，内核统计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/启动器（协议）统计信息 — 显示 iSCSI 目标的统计信息，该目标提供对其存储介质的块级访问，并显示存储阵列在异步镜像操作中用作启动器时的 iSCSI 统计信息。
- **DCBX** 运行状态统计 — 显示各种数据中心桥接交换 (DCBX) 功能的运行状态。
- **LLDP TLV** 统计数据 — 显示链路层发现协议 (LLDP) 类型长度值 (TLV) 统计数据。
- **DCBX TLV** 统计信息 — 显示标识数据中心桥接 (DCB) 环境中存储阵列主机端口的信息。此信息将与网络对等设备共享，用于识别和功能目的。

您可以将这些统计数据中的每一个查看为原始统计数据或基线统计数据。原始统计数据是自控制器启动以来收集的所有统计数据。基线统计数据是自您设置基线时间以来收集的时间点统计数据。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **View iSCSI Statistics Packages**。
3. 单击选项卡可查看不同的统计信息集。
4. 要设置基线，请单击 **Set new baseline**。

   设置基线为统计数据的收集设置了一个新的起点。相同的基线用于所有 iSCSI 统计信息。

在 **SANtricity System Manager** 中查看 **iSCSI** 会话

您可以查看有关到存储阵列的 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一起进行。

步骤

1. 选择菜单：Settings[System]。
2. 选择 **View/End iSCSI Sessions**。

   此时将显示当前 iSCSI 会话的列表。

3. 可选： 要查看有关特定 iSCSI 会话的其他信息，请选择一个会话，然后单击 查看详细信息。

字段详细信息

项目	说明
会话标识符 (SSID)	标识 iSCSI 启动程序和 iSCSI 目标之间会话的十六进制字符串。SSID 由 ISID 和 TPGT 组成。
启动程序 Session ID (ISID)	会话标识符的启动程序部分。启动程序在登录期间指定 ISID。
目标门户组	iSCSI 目标。
目标门户组标记 (TPGT)	会话标识符的目标部分。iSCSI 目标门户组的 16 位数字标识符。
启动程序 iSCSI 名称	启动器的全球唯一名称。
启动程序 iSCSI 标签	在 System Manager 中设置的用户标签。
启动程序 iSCSI 别名	也可以与 iSCSI 节点关联的名称。该别名允许组织将用户友好的字符串与 iSCSI 名称关联。但是，别名不能替代 iSCSI 名称。iSCSI 启动程序别名只能在主机上设置，不能在 System Manager 中设置
主机	向存储阵列发送输入和输出的服务器。
连接 ID (CID)	启动程序和目标之间的会话内连接的唯一名称。启动程序生成此 ID 并在登录请求期间将其提供给目标。在关闭连接的注销过程中也会提供连接 ID。
端口标识符	与连接关联的控制器端口。
启动程序 IP 地址	启动程序的 IP 地址。
协商登录参数	在 iSCSI 会话登录期间处理的参数。
身份验证方法	对希望访问 iSCSI 网络的用户进行身份验证的技术。有效值为 **CHAP** 和 **None**。
标头摘要方法	显示 iSCSI 会话可能的报头值的技术。HeaderDigest 和 DataDigest 可以是 **None** 或 **CRC32C**。两者的默认值均为 **None**。
数据摘要方法	显示 iSCSI 会话的可能数据值的技术。HeaderDigest 和 DataDigest 可以是 **None** 或 **CRC32C**。两者的默认值均为 **None**。
最大连接数	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 **1**。
目标别名	与目标关联的标签。

项目	说明
启动程序别名	与启动程序关联的标签。
目标 IP 地址	iSCSI 会话目标的 IP 地址。不支持 DNS 名称。
初始 R2T	初始传输准备就绪状态。状态可以是 是 或 否。
最大突发长度	此 iSCSI 会话的最大 SCSI 负载（以字节为单位）。最大突发长度可以为 512 到 262,144 (256 KB)。默认值为 **262,144 (256 KB)**。
首个突发长度	此 iSCSI 会话未经请求的数据的 SCSI 负载（以字节为单位）。第一个突发长度可以是 512 到 131,072 (128 KB)。默认值为 **65,536 (64 KB)**。
默认等待时间	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是 0 到 3600。默认值为 **2**。
默认保留时间	在连接终止或连接重置后，仍然可以进行连接的最大秒数。默认保留时间为 0 至 3600。默认值为 **20**。
最大未结 R2T	此 iSCSI 会话的"准备好传输"未完成的最大数量。最大未完成准备传输值可以为 1 到 16。默认值为 **1**。
错误恢复级别	此 iSCSI 会话的错误恢复级别。错误恢复级别值始终设置为 **0**。
最大接收数据段长度	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。
目标名称	目标的正式名称（而不是别名）。具有 *iqn* 格式的目标名称。
启动程序名称	启动程序的正式名称（不是别名）。使用 *iqn* 或 *eui* 格式的启动程序名称。

4. 可选：*要将报告保存到文件，请单击 ***Save**。

   文件以文件名 `iscsi-session-connections.txt` 保存在浏览器的 Downloads 文件夹中。

在 **SANtricity System Manager** 中结束 **iSCSI** 会话

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一起发生。

关于此任务

出于以下原因，您可能需要结束 iSCSI 会话：

- 未经授权的访问 — 如果 iSCSI 启动程序已登录且不应具有访问权限，则可以结束 iSCSI 会话以强制 iSCSI

启动程序离开存储阵列。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 — 如果您需要关闭存储阵列，并且发现 iSCSI 启动程序仍处于登录状态，则可以结束 iSCSI 会话以使 iSCSI 启动程序从存储阵列中注销。

步骤

1. 选择菜单：Settings[System]。
2. 选择 **View/End iSCSI Sessions**。

   此时将显示当前 iSCSI 会话的列表。

3. 选择要结束的会话。
4. 单击 **End Session**，并确认要执行此操作。

在 SANtricity System Manager 中通过 InfiniBand 端口配置 iSER

如果您的控制器包含通过 InfiniBand 端口的 iSER，您可以配置与主机的网络连接。

开始之前

- 您的控制器必须包含 iSER over InfiniBand 端口；否则，iSER over InfiniBand 设置在 System Manager 中不可用。
- 您必须知道主机连接的 IP 地址。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 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。

4. 选择 通过 **InfiniBand** 端口配置 **iSER**。

   此时将打开通过 InfiniBand 端口配置 iSER 对话框。

5. 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。
6. 单击 **Configure**。
7. 完成配置，然后单击 是 重置 iSER over InfiniBand 端口。

在 SANtricity System Manager 中查看基于 InfiniBand 的 iSER 统计信息

如果存储阵列的控制器包含 iSER over InfiniBand 端口，则可以查看有关主机连接的数据。

关于此任务

System Manager 显示以下类型的 iSER over InfiniBand 统计信息。所有统计信息都是只读的，无法设置。

- 本地目标（协议）统计信息 — 提供 iSER over InfiniBand 目标的统计信息，显示对其存储介质的块级访问。
- **iSER over InfiniBand Interface statistics** — 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。

您可以将这些统计数据中的每一个查看为原始统计数据或基线统计数据。原始统计数据是自控制器启动以来收集的所有统计数据。基线统计数据是自您设置基线时间以来收集的时间点统计数据。

步骤

1. 选择菜单：Settings[System]。
2. 选择 **View iSER over InfiniBand Statistics**。
3. 单击选项卡可查看不同的统计信息集。
4. 可选：*要设置基线，请单击*设置新基线。

   设置基线为统计数据的收集设置了一个新的起点。相同的基线用于所有 iSER over InfiniBand 统计。

管理 NVMe 端口

了解 NVMe 和 SANtricity 软件

某些控制器包括用于在结构上实施 NVMe（Non-Volatile Memory Express）的端口。NVMe 允许在主机和存储阵列之间进行高性能通信。

什么是 NVMe?

NVM 代表"非易失性内存"，是许多类型的存储设备中使用的持久性内存。*NVMe* (NVM Express) 是专为与 NVM 设备进行高性能多队列通信而设计的标准化接口或协议。

什么是 NVMe over Fabrics?

NVMe over Fabrics (NVMe-oF) 是一种技术规范，使基于 NVMe 消息的命令和数据能够在主机计算机和存储之间通过网络传输。主机可以使用结构访问 NVMe 存储阵列（称为 *subsystem*）。NVMe 命令被启用并封装在主机端和子系统端的传输抽象层中。这可以将高性能 NVMe 接口从主机端到端扩展到存储，并标准化和简化命令集。

NVMe-oF 存储作为本地块存储设备呈现给主机。该卷（称为 *namespace*）可以与任何其他块存储设备一样装载到文件系统。您可以使用 REST API、SMcli 或 SANtricity System Manager 根据需要配置存储。

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，不得修改。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。

什么是命名空间和命名空间 ID?

命名空间相当于 SCSI 中的一个逻辑单元，它与数组中的一个卷相关。命名空间 ID (NSID) 等同于 SCSI 中的逻辑单元号 (LUN)。您可以在命名空间创建时创建 NSID，并且可以将其设置为介于 1 到 255 之间的值。

什么是 **NVMe** 控制器?

与表示从主机的启动器到存储系统目标的路径的 SCSI I_T nexus 类似，在主机连接过程中创建的 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。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。

您可以配置哪些主机可以访问哪些命名空间，并使用 SANtricity System Manager 为主机设置命名空间 ID。然后，在创建 NVMe 控制器时，将创建 NVMe 控制器可访问的命名空间 ID 列表，并用于配置允许的连接。

在 **SANtricity System Manager** 中配置基于 **InfiniBand** 的 **NVMe** 端口

如果您的控制器包含 NVMe over InfiniBand 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 NVMe over InfiniBand 主机端口；否则，NVMe over InfiniBand 设置在 System Manager 中不可用。
- 您必须知道主机连接的 IP 地址。

> 仅当存储阵列的控制器包含 NVMe over InfiniBand 端口时，才会显示 NVMe over InfiniBand 设置和功能。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。
3. 单击具有要配置的 NVMe over InfiniBand 端口的控制器。

   此时将显示控制器的上下文菜单。
4. 选择 通过 **InfiniBand** 端口配置 **NVMe**。

   此时将打开通过 InfiniBand 端口配置 NVMe 对话框。
5. 从下拉列表中选择要配置的 HIC 端口，然后输入 IP 地址。

   如果要使用支持 200Gb 的 HIC 配置 EF600 存储阵列，则此对话框将显示两个 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）。您应该为两个端口分配唯一的 IP 地址。这些设置允许主机在每个端口之间建立路径，并使 HIC 实现最大性能。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。
6. 单击 **Configure**。
7. 完成配置，然后单击 **Yes** 通过 InfiniBand 端口重置 NVMe。

在 **SANtricity System Manager** 中配置基于 **RoCE** 的 **NVMe** 端口

如果您的控制器包含 NVMe over RoCE（RDMA over Converged Ethernet）的连接，则可

以从"硬件"页面配置 NVMe 端口设置。

开始之前

- 控制器必须包含基于 RoCE 的 NVMe 主机端口；否则，System Manager 中无法使用基于 RoCE 的 NVMe 设置。
- 您必须知道主机连接的 IP 地址。

步骤

1. 选择 **Hardware**。
2. 如果图形显示驱动器，请单击 **Controllers & Components** 选项卡。

   图形会更改为显示控制器而不是驱动器。

3. 单击具有要配置的 NVMe over RoCE 端口的控制器。

   此时将显示控制器的上下文菜单。

4. 选择 **Configure NVMe over RoCE ports**。

   此时将打开通过 RoCE 端口配置 NVMe 对话框。

5. 在下拉列表中，选择要配置的 HIC 端口。
6. 单击 **Next**。

   要查看所有端口设置，请单击对话框右侧的 **Show more port settings** 链接。

   字段详细信息

端口设置	说明
配置的以太网端口速度	选择与端口上 SFP 的速度能力相匹配的速度。
启用 IPv4 / 启用 IPv6	选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。 如果要禁用端口访问，请取消选中两个复选框。
MTU 大小（可通过单击*显示更多端口设置*获得。）	如有必要，请输入最大传输单元 (MTU) 的新大小（以字节为单位）。 默认最大传输单元 (MTU) 大小为每帧 1500 字节。必须输入介于 1500 和 9000 之间的值。

   如果您选择了*启用 IPv4*，点击*下一步*后将打开一个对话框，用于选择 IPv4 设置。如果您选择了*启用 IPv6*，点击*下一步*后将打开一个对话框，用于选择 IPv6 设置。如果您选择了这两个选项，则首先打开 IPv4 设置的对话框，然后单击*下一步*后，将打开 IPv6 设置的对话框。

7. 自动或手动配置 IPv4 和/或 IPv6 设置。

字段详细信息

端口设置	说明
自动获取配置	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，然后在字段中输入静态地址。（如果需要，您可以将地址剪切并粘贴到字段中。）对于 IPv4，包括网络子网掩码和网关。对于 IPv6，包括可路由 IP 地址和路由器 IP 地址。如果要使用支持 200Gb 的 HIC 配置 EF600 存储阵列，则此对话框将显示两组网络参数字段，一组用于物理端口（外部），另一组用于虚拟端口（内部）。您应该为两个端口分配唯一参数。这些设置允许主机在每个端口之间建立路径，并使 HIC 实现最大性能。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。

8. 单击 **Finish**。

在 **SANtricity System Manager** 中查看 **NVMe over Fabrics** 统计信息

您可以查看有关 NVMe over Fabrics 连接到存储阵列的数据。

关于此任务

System Manager 显示这些类型的 NVMe over Fabrics 统计信息。所有统计信息都是只读的，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** 接口统计 — 提供 RDMA 接口上所有 NVMe over Fabrics 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。此选项卡仅在 NVMe over Fabrics 端口可用时显示。

您可以将这些统计数据中的每一个查看为原始统计数据或基线统计数据。原始统计数据是自控制器启动以来收集的所有统计数据。基线统计数据是自您设置基线时间以来收集的时间点统计数据。

步骤

1. 选择菜单：Settings[System]。
2. 选择 **View NVMe over Fabrics Statistics**。
3. 可选：*要设置基线，请单击*设置新基线。

   设置基线为统计数据的收集设置了一个新的起点。所有 NVMe 统计信息都使用相同的基线。

管理驱动器

了解 **SANtricity System Manager** 中的驱动器状态

SANtricity System Manager 报告驱动器的各种状态。

辅助功能状态

状态	定义
已绕过	驱动器实际存在，但控制器无法在任何端口上与其通信。
不兼容	存在以下条件之一： • 该驱动器未经认证，无法在存储阵列中使用。 • 此驱动器具有不同的扇区大小。 • 驱动器包含来自较旧或较新固件版本的无法使用的配置数据。
已删除	驱动器已从存储阵列中被不当移除。
现有	控制器可以在两个端口上与驱动器通信。
无响应	驱动器未响应命令。

角色状态

状态	定义
已分配	该驱动器是池或卷组的成员。
使用中的热备盘	此驱动器当前正被用作出现故障的驱动器的替代品。热备盘仅用于卷组，而不用于池。
备用热备盘	驱动器已准备好用作发生故障的驱动器的替代品。热备盘仅用于卷组，而不用于池。
未分配	驱动器不是池或卷组的成员。

可用性状态

状态	定义
失败	驱动器无法工作。驱动器上的数据不可用。
即将发生的故障	已检测到驱动器可能很快出现故障。驱动器上的数据仍然可用。
脱机	驱动器通常无法用于存储数据，因为它是正在导出的卷组的一部分或正在进行固件升级。
最佳	驱动器运行正常。

了解 SANtricity System Manager 中的固态硬盘 (SSD)

固态硬盘（SSD）是使用固态内存（闪存）永久存储数据的数据存储设备。SSD 模拟传统硬盘驱动器，并提供与硬盘驱动器相同的接口。

SSD 的优势

SSD 相对于硬盘的优势包括：

- 启动速度更快（无旋转）
- 更低的延迟
- 更高的每秒 I/O 操作数 (IOPS)
- 更少的运动部件，更高的可靠性
- 更低的功耗
- 产生的热量更少，所需冷却更少

识别 SSD

从"硬件"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。

卷组

卷组中的所有驱动器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。

缓存

控制器的写缓存始终为 SSD 启用。写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，还可以实现 SSD 缓存功能，以提高整体系统性能。在 SSD 缓存中，数据从卷复制并存储在两个内部 RAID 卷上（每个控制器一个）。

在 SANtricity System Manager 中筛选驱动器视图

如果存储阵列包括具有不同类型物理和逻辑属性的驱动器，则 Hardware 页面会提供过滤器字段，帮助您限制驱动器视图并定位特定驱动器。

关于此任务

驱动器过滤器可以将视图仅限于某些类型的物理驱动器（例如，所有 SAS），具有某些安全属性（例如，具有安全功能），在某些逻辑位置（例如，卷组 1）。您可以同时或单独使用这些筛选条件。

> 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，则不会出现 **Anywhere in the storage array** 筛选器字段。

步骤

1. 选择 **Hardware**。
2. 在第一个筛选字段中（在 **Show drives that are…** 下），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（从高到低）
- 驱动器速度（从最高到最低）安全属性可能包括：
- 支持安全功能
- 已启用安全保护
- 具备 DA (Data Assurance) 功能
- 符合 FIPS
- 符合 FIPS 标准（FIPS 140-2）
- 符合 FIPS 标准（FIPS 140-3）

  如果所有驱动器的这些属性都相同，则不会显示在下拉列表中。例如，如果存储阵列包括所有具有 SAS 接口和 15000 RPM 速度的 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。

当您从字段中选择一个选项时，与您的筛选条件不匹配的驱动器在图形视图中将变为灰色。

3. 在第二个过滤器框中，单击下拉箭头以显示驱动器的可用逻辑位置。

   如果您需要清除筛选条件，请选择筛选框最右侧的 **Clear**。

   逻辑位置可能包括：

   - 池
   - 卷组
   - 热备用磁盘
   - SSD 缓存
   - 未分配

     当您从字段中选择一个选项时，与您的筛选条件不匹配的驱动器在图形视图中将变为灰色。

4. 或者，您可以在过滤器字段最右侧选择 **Turn on locator lights**，以打开显示驱动器的定位灯。

   此操作可帮助您实际定位存储阵列中的驱动器。

在 **SANtricity System Manager** 中打开驱动器定位灯

从 Hardware 页面，您可以打开定位器指示灯，以查找存储阵列中驱动器的物理位置。

关于此任务

您可以找到 Hardware 页面上显示的单个驱动器或多个驱动器。

步骤

1. 选择 **Hardware**。
2. 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。（如果图形显示控制器，请单击 驱动器 选项卡。）单击驱动器以显示其上下文菜单，然后选择 打开定位灯。

     驱动器的定位指示灯亮起。实际定位驱动器后，返回对话框并选择 关闭。
   - 多个驱动器 — 在筛选器字段中，从左侧下拉列表中选择物理驱动器类型，从右侧下拉列表中选择逻辑驱动器类型。符合条件的驱动器数量显示在字段的最右侧。接下来，您可以单击 打开定位灯 或从上下文菜单中选择 查找所有已过滤的驱动器。物理定位驱动器后，返回对话框并选择 关闭。

在 **SANtricity System Manager** 中查看驱动器状态和设置

您可以查看驱动器的状态和设置，例如媒体类型、接口类型和容量。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。
3. 选择要查看其状态和设置的驱动器。

   驱动器的上下文菜单打开。
4. 选择 **View settings**。

   此时将打开驱动器设置对话框。
5. 要查看所有设置，请单击对话框右上角的 **Show more settings**。

字段详细信息

设置	说明
状态	显示 Optimal、Offline、Non-critical fault 和 Failed。Optimal 状态指示所需的工作条件。
模式	显示已分配、未分配、热备盘待机或正在使用的热备盘。
位置	显示驱动器所在的货架和托架编号。
分配给/可以保护/保护	如果驱动器分配给池、卷组或 SSD 缓存，此字段将显示"分配给"。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盘，且其模式为待机，则此字段显示"可以保护"。如果热备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盘，且其模式为"正在使用中"，则此字段将显示"保护"。该值是受影响的卷组的名称。 如果驱动器未分配，则不会显示此字段。
介质类型	显示驱动器使用的记录媒体类型，可以是硬盘驱动器 (HDD) 或固态硬盘 (SSD)。
使用的续航时间百分比（仅当 SSD 驱动器存在时显示）	到目前为止写入驱动器的数据量，除以总理论写入限制。
接口类型	显示驱动器使用的接口类型，例如 SAS。
驱动器路径冗余	显示驱动器和控制器之间的连接是否冗余（是）或不冗余（否）。
容量 (GiB)	显示驱动器的可用容量（配置的总容量）。
速度 (RPM)	以 RPM 为单位显示速度（对于 SSD 不显示）。
当前数据速率	显示驱动器和存储阵列之间的数据传输速率。
逻辑扇区大小（字节）	显示驱动器使用的逻辑扇区大小。
物理扇区大小 (字节)	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。
驱动器固件版本	显示驱动器固件的修订级别。
全球标识符	显示驱动器的唯一十六进制标识符。

设置	说明
产品 ID	显示由制造商分配的产品标识符。
序列号	显示驱动器的序列号。
制造商	显示驱动器的供应商。
制造日期	显示驱动器的构建日期。 不适用于 NVMe 驱动器。
支持安全功能	显示驱动器是否具有安全功能（是）或不具有（否）。支持安全的驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器（级别 140-2 或 140-3），它们在写入期间加密数据，在读取期间解密数据。这些驱动器被认为是安全_有能力_的，因为它们可以使用 Drive Security 功能用于额外的安全性。如果为与这些驱动器一起使用的卷组和池启用了 Drive Security 功能，则驱动器将变得安全_已启用_。
已启用安全保护	显示驱动器是否已安全启用（是）或未启用（否）。启用安全的驱动器与 Drive Security 功能一起使用。当您启用 Drive Security 功能，然后将 Drive Security 应用于具有安全_功能_的驱动器上的池或卷组时，驱动器将变为安全_启用_状态。只能通过配置了正确安全密钥的控制器进行读写访问。这种额外的安全性可防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。
可读/写访问	显示驱动器是否可读/写访问（是）或不可访问（否）。
驱动器安全密钥标识符	显示启用安全功能的驱动器的安全密钥。Drive Security 是一种存储阵列功能，可通过全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器提供额外的安全层。当这些驱动器与 Drive Security 功能一起使用时，它们需要安全密钥才能访问其数据。当驱动器从阵列中物理卸下时，它们必须安装在另一个阵列中才能运行，此时，它们将处于 Security Locked 状态，直到提供正确的安全密钥。
具备数据保障 (DA) 能力	显示数据保障 (DA) 功能是否已启用（是）或未启用（否）。数据保障 (DA) 是一项检查和纠正数据通过控制器传输到驱动器时可能发生的错误的功能。数据保障可以在池或卷组级别启用，主机使用支持 DA 的 I/O 接口，如 Fibre Channel。
DULBE 功能	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 EF300 或 EF600 存储阵列支持资源调配的卷。

6. 单击 **Close**。

在 **SANtricity System Manager** 中逻辑替换驱动器

如果驱动器出现故障或由于任何其他原因要替换它，则可以从逻辑上使用未分配的驱动器或完全集成的热备盘替换出现故障的驱动器。

关于此任务

在逻辑上更换驱动器时，驱动器将被分配，然后成为关联池或卷组的永久成员。

您使用逻辑替换选项来替换以下类型的驱动器：

- 故障驱动器
- 缺少驱动器
- Recovery Guru 已通知您即将到达使用寿命终点的 SSD 驱动器
- Recovery Guru 已通知您即将发生驱动器故障的硬盘驱动器
- 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

替换驱动器必须具有以下特性：

- 处于"最佳"状态
- 处于未分配状态
- 与要更换的驱动器相同的属性（媒体类型、接口类型等）
- 相同的 FDE 功能（推荐，但不是必需的）
- 相同的 DA 功能（推荐，但不是必需的）

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 单击要逻辑更换的驱动器。

   此时将显示驱动器的上下文菜单。

4. 单击 **Logically replace**。
5. 可选： 选择 **Fail drive after it is replaced** 复选框，以在更换原始驱动器后使其失效。

   只有当原始分配的驱动器未出现故障或丢失时，才会启用此复选框。

6. 从 **Select a replacement drive** 表中，选择要使用的替换驱动器。

   该表仅列出与要更换的驱动器兼容的驱动器。如果可能，请选择能够保持货架丢失保护和抽屉丢失保护的驱动器。

7. 单击 **Replace**。

如果原始驱动器出现故障或丢失，则使用奇偶校验信息在替换驱动器上重建数据。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，其数据将复制到替换驱动器。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转换为未分配状态，或者如果选中该复选框，则转换为失败状态。

在 **SANtricity System Manager** 中手动重建驱动器

驱动器重建通常在更换驱动器后自动开始。如果驱动器重建未自动开始，您可以手动开始重建。

仅在技术支持或 Recovery Guru 的指示下执行此操作。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 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。

4. 选择 **Reconstruct**，并确认要执行此操作。

在 **SANtricity System Manager** 中初始化（格式化）驱动器

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）这些驱动器，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以前的配置信息并将其返回到未分配状态。此时驱动器可用于添加到新存储阵列中的新池或卷组。

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。

可能丢失数据 — 初始化驱动器时，驱动器上的所有数据都会丢失。仅在技术支持人员的指示下执行此操作。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 单击要初始化的驱动器。

此时将显示驱动器的上下文菜单。

4. 选择 **Initialize**，并确认要执行此操作。

在 **SANtricity System Manager** 中手动使驱动器故障

如果有指示，您可以手动使驱动器出现故障。

关于此任务

System Manager 监视存储阵列中的驱动器。当检测到驱动器产生大量错误时，Recovery Guru 会通知您即将发生的驱动器故障。如果发生这种情况，并且您有可用的替换驱动器，则可能需要使该驱动器出现故障，以便采取先发制人的操作。如果没有可用的替换驱动器，则可以等待该驱动器自行发生故障。

> 可能丢失数据访问权限 — 此操作可能会导致数据丢失或数据冗余丢失。仅在技术支持或 Recovery Guru 的指示下执行此操作。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 单击要使其失效的驱动器。

   此时将显示驱动器的上下文菜单。

4. 选择 **Fail**。
5. 保持 **Copy contents of drive before failing** 复选框处于选中状态。

   仅为分配的驱动器和非 RAID 0 卷组显示复制选项。

   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，如果不首先复制驱动器的内容，则可能会丢失关联的池或卷组上的所有数据或数据冗余。

   复制选项允许比重建更快的驱动器恢复，并减少在复制操作期间如果另一个驱动器发生故障时卷发生故障的可能性。

6. 确认要使驱动器出现故障。

   驱动器出现故障后，请至少等待 60 秒，然后再将其移除。

在 **SANtricity System Manager** 中擦除驱动器

您可以使用 Erase 选项准备要从系统中删除的未分配驱动器。此过程将永久删除数据，确保数据无法再次读取。

开始之前

该驱动器必须处于未分配状态。

关于此任务

仅当您想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功能，擦除选项将执行加密擦除，并将驱动器的安全属性重置为支持安全功能。

擦除功能不支持某些较旧的驱动器型号。如果您尝试擦除其中一个旧型号，则会显示一条错误消息。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 您也可以使用筛选器字段查看盘架中所有未分配的驱动器。从 **Show drives that are…** 下拉列表中，选择 **Unassigned**。

   盘架视图仅显示未分配的驱动器；所有其他驱动器均呈灰色。

4. 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 Erase Drives 对话框中执行此操作。）

   可能丢失数据 — Erase 操作无法撤消。确保在操作过程中选择正确的驱动器。

5. 从上下文菜单中，选择 **Erase**。

   此时将打开 Erase Drives 对话框，其中显示擦除操作的所有符合条件的驱动器。

6. 如果需要，从表中选择其他驱动器。您不能选择 *all* 驱动器；请确保有一个驱动器保持未选择状态。
7. 通过键入 `erase`确认操作，然后单击 **Erase**。

   请确保要继续此操作。单击下一个对话框中的"是"后，操作将无法中止。

8. 在估计完成时间对话框中，单击 是 继续进行擦除操作。

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：Home[View Operations in Progress]。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，必须首先对其进行初始化。为此，请从驱动器的上下文菜单中选择 **Initialize**。

在 **SANtricity System Manager** 中解锁或重置锁定的 **NVMe** 或 **FIPS** 驱动器

如果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，则可以通过输入其 Physical Security ID (PSID) 来对每个锁定驱动器执行重置，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，请确保在管理客户端（使用浏览器访问 System Manager 的系统）上提供安全密钥文件（扩展名为 `.slk`）。您还必须知道与密钥相关的密码短语。
- 对于重置选项，您必须在要重置的每个驱动器上找到 PSID。要查找 PSID，请实际移除驱动器，并在驱动器标签上找到 PSID 字符串（最多 32 个字符），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存储阵列来解锁 NVMe 或 FIPS 驱动器中的数据。对于安全密钥不可用的情况，此任务还描述了如何对锁定的驱动器执行重置。

> 如果使用外部密钥管理服务器锁定驱动器，请在 System Manager 中选择菜单：Settings[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菜单访问解锁功能：Settings[System > Security key management]。下面的任务提供了硬件页面的说明。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 选择要解锁或重置的 NVMe 或 FIPS 驱动器。

   驱动器的上下文菜单打开。

4. 选择 **Unlock** 应用安全密钥文件，如果没有安全密钥文件，则选择 **Reset**。

   仅当您选择锁定的 NVMe 或 FIPS 驱动器时，才会显示这些选项。

   > 在重置操作期间，所有数据都将被擦除。仅当您没有安全密钥时才执行重置。重置锁定的驱动器将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。

5. 执行以下操作之一：

   a. 解锁：在 解锁安全驱动器 对话框中，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。接下来，输入密码，然后单击 解锁。

   b. 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，必须单独选择要重置的每个驱动器。

结果

驱动器现在可以在另一个卷组或磁盘池或另一个存储阵列中使用。

管理热备盘

了解 **SANtricity System Manager** 中的热备用驱动器

热备盘在 SANtricity System Manager 中充当 RAID 1、RAID 5 或 RAID 6 卷组的备用驱动器。

它们是功能齐全的驱动器，不包含任何数据。如果卷组中的驱动器出现故障，控制器会自动将故障驱动器的数据重建到分配为热备盘的驱动器。

热备盘不专用于特定的卷组。它们可用于存储阵列中的任何故障驱动器，只要热备盘和驱动器共享以下属性：

- 相等的容量（或热备盘的更大容量）
- 相同的介质类型（例如 HDD 或 SSD）
- 相同的接口类型（例如 SAS）

如何识别热备盘

您可以通过 Initial Setup Wizard 或从 Hardware 页面分配热备件。要确定是否分配了热备件，请转到 Hardware 页面并查找以粉红色显示的任何驱动器托架。

热备件覆盖范围的工作原理

热备件覆盖范围的工作原理如下：

- 将未分配的驱动器保留为 RAID 1、RAID 5 或 RAID 6 卷组的热备盘。

> 热备盘不能用于池，池具有不同的数据保护方法。池不会预留额外的驱动器，而是在池的每个驱动器内预留备用容量（称为 *preservation capacity*）。如果池中的驱动器出现故障，控制器将在该备用容量中重建数据。

- 如果 RAID 1、RAID 5 或 RAID 6 卷组中的驱动器出现故障，控制器会自动使用冗余数据从出现故障的驱动器重建数据。热备盘会自动替换出现故障的驱动器，而无需进行物理交换。
- 物理更换故障驱动器后，将执行从热备盘驱动器到更换驱动器的复制操作。如果您已将热备盘驱动器指定为卷组的永久成员，则不需要执行复制操作。
- 卷组的托盘丢失保护和抽屉丢失保护的可用性取决于构成卷组的驱动器的位置。由于驱动器故障和热备盘驱动器的位置，托盘丢失保护和抽屉丢失保护可能会丢失。为确保托盘丢失保护和抽屉丢失保护不受影响，您必须更换出现故障的驱动器以启动复制过程。
- 在更换故障驱动器时，存储阵列卷保持联机并可访问，因为热备用驱动器会自动替换故障驱动器。

热备盘容量注意事项

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 9 GiB 或更大的驱动器作为热备盘。通常，请勿将驱动器分配为热备盘，除非其容量等于或大于存储阵列中最大驱动器的容量。

> 如果没有具有相同物理容量的热备盘，则如果驱动器的"已用容量"等于或小于热备驱动器的容量，则可以将容量较低的驱动器用作热备盘。

介质和接口类型的注意事项

用作热备盘的驱动器必须与其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 驱动器的热备盘。

具有安全功能的驱动器的注意事项

具有安全功能的驱动器（如 FDE 或 FIPS）可以用作具有或不具有安全功能的驱动器的热备盘。但是，不具备安全功能的驱动器不能用作具有安全功能的驱动器的热备盘。

当您选择要用于热备盘的启用了安全的驱动器时，System Manager 会提示您执行安全擦除，然后才能继续。安全擦除将驱动器的安全属性重置为支持安全，但不启用安全。

> 当您启用驱动器安全功能，然后从具有安全功能的驱动器创建池或卷组时，驱动器将变为_安全启用_。只能通过配置了正确安全密钥的控制器进行读写访问。这种增加的安全性可防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。

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盘。否则，您可以在存储阵列中的卷组之间手动创建热备盘驱动器。

在 **SANtricity System Manager** 中分配热备用磁盘

您可以将热备盘分配为备用驱动器，以便在 RAID 1、RAID 5 或 RAID 6 卷组中进行额外的数据保护。如果驱动器在其中一个卷组中发生故障，则控制器将数据从发生故障的驱动器重新构建到热备盘。

开始之前

- 必须创建 RAID 1、RAID 5 或 RAID 6 卷组。（热备盘不能用于池。相反，池会在每个驱动器内使用备用容量来进行数据保护。）
- 必须提供符合以下条件的驱动器：
  - 未分配，状态为最佳。
  - 与卷组中的驱动器相同的介质类型（例如 SSD）。
  - 与卷组中的驱动器相同的接口类型（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 Hardware 页面手动分配热备盘。建议的覆盖范围是每个驱动器集两个热备盘。

> 热备盘也可以通过初始设置向导进行分配。您可以通过在 Hardware 页面上查找以粉红色显示的驱动器托架来确定是否已分配热备盘。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

图形更改为显示驱动器而不是控制器。

3. 选择要用作热备盘的未分配驱动器（以灰色显示）。

   驱动器的上下文菜单打开。

4. 选择 **Assign hot spare**。

   如果驱动器已启用安全功能，则会打开 Secure Erase Drive? 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 Secure Erase 操作以删除其所有数据并重置其安全属性。

   ⚠ 可能丢失数据 — 确保选择了正确的驱动器。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，则将打开"确认分配热备盘驱动器"对话框。

5. 查看对话框中的文本，然后确认操作。

   驱动器在"硬件"页面上以粉红色显示，这表明它现在是热备盘。

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的数据重建到热备盘。

在 **SANtricity System Manager** 中取消分配热备盘

您可以将热备盘更改回未分配的驱动器。

开始之前

热备盘必须处于最佳、待机状态。

关于此任务

您无法取消分配当前正在接管故障驱动器的热备盘。如果热备盘未处于最佳状态，请按照 Recovery Guru 程序更正任何问题，然后再尝试取消分配驱动器。

步骤

1. 选择 **Hardware**。
2. 如果图形显示控制器，请单击 **Drives** 选项卡。

   图形更改为显示驱动器而不是控制器。

3. 选择要取消分配的热备盘驱动器（以粉红色显示）。

   如果粉红色驱动器托架上有对角线，则热备盘当前正在使用中，无法取消分配。

   驱动器的上下文菜单打开。

4. 从驱动器的下拉列表中，选择 **Unassign hot spare**。

   该对话框显示受删除此热备盘影响的任何卷组，以及是否有任何其他热备盘正在保护它们。

5. 确认取消分配操作。

结果

驱动器返回到未分配（以灰色显示）。

适用于 SANtricity System Manager 的存储架常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是货架丢失保护和抽屉丢失保护?

磁盘架丢失保护和抽屉丢失保护是池和卷组的属性，允许您在发生单个磁盘架或抽屉故障时保持数据访问。

磁盘架丢失保护

盘架是包含驱动器或驱动器和控制器的盘柜。盘架丢失保护可保证在单个驱动器盘架发生完全通信中断时对池或卷组中卷上的数据的可访问性。完全失去通信的一个例子可能是驱动器架断电或两个 I/O 模块 (IOM) 出现故障。

如果驱动器已在池或卷组中出现故障，则无法保证提供盘架丢失保护。在这种情况下，失去对驱动器盘架的访问权限，从而导致池或卷组中的另一个驱动器导致数据丢失。

货架丢失保护的标准取决于保护方法，如下表所述：

级别	货架丢失保护标准	所需的最少磁盘架数量
池	池必须包含至少五个盘架上的驱动器，并且每个盘架上的驱动器数量必须相等。盘架丢失保护不适用于大容量盘架；如果您的系统包含大容量盘架，请参阅抽屉丢失保护。	5
RAID 6	此卷组在一个盘架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单独的托架中。	3
RAID 1	RAID 1 对中的每个驱动器必须位于单独的机架中。	2
RAID 0	无法实现 Shelf Loss Protection。	不适用

抽屉丢失保护

抽屉是货架的一个隔间，您可以拉出它来访问驱动器。只有大容量的货架才有抽屉。抽屉丢失保护可确保在单个抽屉完全失去通信的情况下，可以访问池或卷组中的卷上的数据。完全失去通信的一个例子可能是抽屉断电或抽屉内部组件故障。

如果驱动器已在池或卷组中出现故障，则无法保证提供抽屉丢失保护。在这种情况下，失去对抽屉（以及池或卷组中的另一个驱动器）的访问权限会导致数据丢失。

抽屉损失保护的标准取决于保护方法，如下表所述：

级别	抽屉损失保护标准	所需的最少抽屉数量
池	池候选项必须包括来自所有抽屉的驱动器，并且每个抽屉中必须有数量相等的驱动器。 池必须包括至少五个抽屉中的驱动器，并且每个抽屉中的驱动器数量必须相等。 当池中包含 15、20、25、30、35、40、45、50、55 或 60 个驱动器时，60 驱动器磁盘架可以实现抽屉丢失保护。初始创建后，可以将 5 的倍数增量添加到池中。	5
RAID 6	此卷组在一个抽屉中包含的驱动器不超过两个。	3
RAID 3 或 RAID 5	卷组中的每个驱动器都位于单独的抽屉中。	3
RAID 1	镜像对中的每个驱动器必须位于单独的抽屉中。	2
RAID 0	无法实现抽屉丢失保护。	不适用

什么是电池学习周期?

学习周期是用于校准智能电池仪表的自动周期。

学习周期包括以下几个阶段：

- 受控电池放电
- 休息期间
- 收费

将电池放电至预定阈值。在此阶段，电池仪表被校准。

学习周期需要以下参数：

- 充满电的电池
- 无电池过热

双工控制器系统的学习周期同时发生。对于具有来自多个电池或电池组的备用电源的控制器，学习周期按顺序进行。

学习周期计划在一周中的同一时间和同一天定期自动启动。周期间隔以周为单位描述。

一个学习周期可能需要几个小时才能完成。

SANtricity System Manager 存储控制器常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是自动协商？

自动协商是网络接口与另一个网络接口自动协调其自身连接参数（速度和双工）的能力。

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，则应手动将网络接口设置设置为正确的配置。自动协商由控制器的以太网管理端口执行。iSCSI 主机总线适配器不执行自动协商。

如果自动协商失败，控制器将尝试在 10BASE-T 半双工模式下建立连接，这是最低的公分母。

什么是 **IPv6** 无状态地址自动配置？

使用无状态自动配置，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具有链路本地地址、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。

无状态自动配置和有状态自动配置相辅相成。例如，主机可以使用无状态自动配置来配置自己的地址，但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。互联网协议第 6 版（IPv6）还定义了一种方法，通过该方法，可以一次对网络上的所有 IP 地址进行重新编号。IPv6 定义了一种方法，让网络上的设备自动配置其 IP 地址和其他参数，而无需服务器。

设备在使用无状态自动配置时执行以下步骤：

1. 生成链路本地地址 — 设备生成一个链路本地地址，该地址有 10 位，后跟 54 个零，后跟 64 位接口 ID。
2. 测试链路本地地址的唯一性 — 节点进行测试，以确保其生成的链路本地地址尚未在本地网络上使用。节点使用 ND 协议发送邻居请求消息。作为响应，本地网络侦听邻居通告消息，这表明另一个设备已经在使用链路本地地址。如果是这样，则必须生成新的链路本地地址或自动配置失败，并且必须使用其他方法。
3. 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本地网络上的通信，但不能通过 Internet 进行通信。
4. 联系路由器 — 节点尝试联系本地路由器，了解有关继续配置的详细信息。此联系是通过侦听路由器定期发送的路由器通告消息，或通过发送特定的路由器请求消息向路由器询问有关下一步操作的信息来执行的。
5. 为节点提供方向 — 路由器为节点提供有关如何进行自动配置的方向。或者，路由器告诉主机如何确定全局 Internet 地址。
6. 配置全局地址 — 主机使用其全局唯一的 Internet 地址配置自己。此地址通常由路由器提供给主机的网络前缀形成。

我应该选择哪一个— DHCP 或手动配置?

网络配置的默认方法是 Dynamic Host Configuration Protocol (DHCP)。除非您的网络没有 DHCP 服务器，否则始终使用此选项。

什么是 DHCP 服务器?

动态主机配置协议 (DHCP) 是一种自动分配互联网协议 (IP) 地址的协议。

必须为连接到 TCP/IP 网络的每个设备分配唯一的 IP 地址。这些设备包括存储阵列中的控制器。

如果没有 DHCP，网络管理员将手动输入这些 IP 地址。使用 DHCP，当客户端需要启动 TCP/IP 操作时，客户端会广播对地址信息的请求。DHCP 服务器接收请求，在称为租用期的指定时间内分配新地址，并将该地址发送到客户端。使用 DHCP，设备每次连接到网络时都可以使用不同的 IP 地址。在某些系统中，即使设备仍处于连接状态，设备的 IP 地址也可能发生变化。

如何配置我的 DHCP 服务器?

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，并且可以更改，因为它们有一个到期的租用期。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。

为什么需要更改控制器网络配置?

使用带外管理时，必须为每个控制器设置网络配置（其 Internet Protocol (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。如果您未使用 DHCP 服务器，则必须手动输入网络配置。

从何处获取网络配置?

您可以从网络管理员处获取 Internet Protocol (IP) 地址、子网掩码 (subnet mask) 和网关信息。

在控制器上配置端口时需要此信息。

什么是 ICMP PING 响应?

互联网控制消息协议 (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` 是系统管理员用于手动测试网络设备之间的连接以及测试网络延迟和数据包丢失的故障排除工具。 `ping` 命令向网络上的设备发送 `ICMP echo request`，设备立即响应 (`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它们。

何时应刷新端口配置？

在修改或升级服务器时刷新 DHCP 服务器，并且与要使用的当前存储阵列和存储阵列相关的 DHCP 信息已更改。

具体来说，当您知道 DHCP 服务器将分配不同的地址时，请从 DHCP 服务器刷新端口配置或 iSNS 服务器。

刷新端口配置会对该端口上的所有 iSCSI 连接造成破坏。

配置管理端口后我该怎么做？

如果更改了存储阵列的 IP 地址，则可能需要在 SANtricity Unified Manager 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[Discover]。

如果仍在使用 SANtricity Storage Manager，请转到企业管理窗口 (EMW)，在此必须删除并重新添加新 IP 地址。

为什么存储系统处于非优化模式？

处于非最佳模式的存储系统是由于系统配置状态无效所致。尽管存在此状态，但完全支持对现有卷的正常 I/O 访问；但是，SANtricity System Manager 将禁止某些操作。

由于以下原因之一，存储系统可能会转换为无效系统配置：

- 控制器不合规，可能是因为它的子型号 ID (SMID) 代码不正确，或者它已超过高级功能的限制。
- 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。
- 发生一般锁定情况。

适用于 **SANtricity System Manager** 的 **iSCSI** 协议常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

使用 **iSNS** 服务器进行注册时会发生什么？

使用 Internet Storage Name Service (iSNS) 服务器信息时，可以将主机（启动器）配置为查询 iSNS 服务器以从目标（控制器）检索信息。

此注册为 iSNS 服务器提供控制器的 iSCSI 限定名称 (IQN) 和端口信息，并允许在启动器（iSCSI 主机）和目标（控制器）之间进行查询。

iSCSI 自动支持哪些注册方法？

iSCSI 实现支持 Internet Storage Name Service (iSNS) 发现方法或使用 Send Targets 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。您需要注册目标控制器，为 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 Send Targets 命令。作为响应，控制器返回

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 iSCSI 启动程序可以从 iSNS 服务器检索目标 IP。

如何解释基于 **InfiniBand** 的 **iSER** 统计数据?

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 iSER over InfiniBand 目标的统计信息，显示对其存储介质的块级访问。
- **iSER over InfiniBand Interface** 统计信息 — 提供 InfiniBand 接口上所有 iSER over InfiniBand 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。

您可以将这些统计数据中的每一个查看为原始统计数据或基线统计数据。原始统计数据是自控制器启动以来收集的所有统计数据。基线统计数据是自您设置基线时间以来收集的时间点统计数据。

我还需要做些什么来配置或诊断基于 **InfiniBand** 的 **iSER**?

下表列出了可用于在 InfiniBand 会话中配置和管理 iSER 的 SANtricity System Manager 功能。

> 仅当存储阵列的控制器包含 iSER over InfiniBand 主机管理端口时，iSER over InfiniBand 设置才可用。

操作	位置
通过 InfiniBand 端口配置 iSER	1. 选择 **Hardware**。 2. 选择 **Controllers & Components** 选项卡。 3. 选择控制器。 4. 选择 通过 **InfiniBand** 端口配置 **iSER**。 或 1. 选择菜单：Settings[System]。 2. 向下滚动到 **iSER over InfiniBand settings**，然后选择 **Configure iSER over InfiniBand Ports**。
查看基于 InfiniBand 的 iSER 统计信息	1. 选择菜单：Settings[System]。 2. 向下滚动到 **iSER over InfiniBand settings**，然后选择 **View iSER over InfiniBand Statistics**。

我还需要执行哪些操作来配置或诊断 **iSCSI**?

iSCSI 会话可与异步镜像关系中的主机或远程存储阵列一起进行。下表列出了可用于配置和管理这些 iSCSI 会话的 SANtricity System Manager 功能。

> 只有当您的存储阵列支持 iSCSI 时，iSCSI 设置才可用。

配置 **iSCSI**

操作	位置
管理 iSCSI 设置	1. 选择菜单：Settings[System]。 2. 向下滚动到 **iSCSI** 设置 以查看所有管理功能。
配置 iSCSI 端口	1. 选择 **Hardware**。 2. 选择 **Controllers & Components** 选项卡。 3. 选择控制器。 4. 选择 **Configure iSCSI ports**。
设置主机 CHAP 密码	1. 选择菜单：Settings[System]。 2. 向下滚动到 **iSCSI** 设置，然后选择*配置身份验证*。 或 1. 选择菜单：Storage[Hosts]。 2. 选择一个主机成员。 3. 单击菜单：View/Edit Settings[Host Ports] 选项卡。

诊断 **iSCSI**

操作	位置
查看或结束 iSCSI 会话	1. 选择菜单：Settings[System]。 2. 向下滚动到 **iSCSI** 设置，然后选择*查看/结束 iSCSI 会话*。 或 1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。 2. 选择 **View/End iSCSI Sessions**。

操作	位置
查看 iSCSI 统计信息	1. 选择菜单：Settings[System]。 2. 向下滚动到 **iSCSI** 设置，然后选择*查看 iSCSI 统计数据包*。 或 1. 选择菜单：Support[Support Center > Diagnostics]选项卡。 2. 选择 **View iSCSI Statistics Packages**。

适用于 **SANtricity System Manager** 的 **NVMe** 协议常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

如何解释 **NVMe over Fabrics** 统计信息？

View NVMe over Fabrics Statistics 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。有关这些统计信息的详细信息，请单击*查看表格标题的图例*。
- **RDMA** 接口统计 — 提供 RDMA 接口上所有 NVMe over Fabrics 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。此选项卡仅在 NVMe over Fabrics 端口可用时显示。有关统计信息的详细信息，请单击*查看表格标题的图例*。

您可以将这些统计数据中的每一个查看为原始统计数据或基线统计数据。原始统计数据是自控制器启动以来收集的所有统计数据。基线统计数据是自您设置基线时间以来收集的时间点统计数据。

我还需要执行哪些操作来配置或诊断基于 **InfiniBand** 的 **NVMe**？

下表列出了可用于通过 InfiniBand 会话配置和管理 NVMe 的 SANtricity System Manager 功能。

仅当存储阵列的控制器包含 NVMe over InfiniBand 端口时，NVMe over InfiniBand 设置才可用。

操作	位置
通过 InfiniBand 端口配置 NVMe	1. 选择 **Hardware**。 2. 选择 **Controllers & Components** 选项卡。 3. 选择控制器。 4. 选择 通过 **InfiniBand** 端口配置 **NVMe**。 或 1. 选择菜单：Settings[System]。 2. 向下滚动到 **NVMe over InfiniBand settings**，然后选择 **Configure NVMe over InfiniBand Ports**。
查看 NVMe over InfiniBand 统计信息	1. 选择菜单：Settings[System]。 2. 向下滚动到 **NVMe over InfiniBand settings**，然后选择 **View NVMe over Fabrics Statistics**。

我还需要执行哪些操作来配置或诊断基于 **RoCE** 的 **NVMe**?

您可以从硬件和设置页面配置和管理 NVMe over RoCE。

仅当存储阵列的控制器包含 NVMe over RoCE 端口时，NVMe over RoCE 设置才可用。

操作	位置
通过 RoCE 端口配置 NVMe	1. 选择 **Hardware**。 2. 选择 **Controllers & Components** 选项卡。 3. 选择控制器。 4. 选择 **Configure NVMe over RoCE ports**。 或 1. 选择菜单：Settings[System]。 2. 向下滚动到 **NVMe over RoCE settings**，然后选择 **Configure NVMe over RoCE Ports**。
查看基于网络结构的 NVMe 统计信息	1. 选择菜单：Settings[System]。 2. 向下滚动到 **NVMe over RoCE** 设置，然后选择 **View NVMe over Fabrics Statistics**。

为什么一个物理端口有两个 **IP** 地址?

EF600 存储阵列可以包括两个 HIC — 一个外部和一个内部。

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。

为了实现最大的 200Gb 性能，您必须为物理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，则 HIC 将以大约一半的速度运行。

为什么一个物理端口有两组参数？

EF600 存储阵列可以包括两个 HIC — 一个外部和一个内部。

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。

要实现最大 200Gb 性能，必须为物理端口和虚拟端口分配参数，以便主机可以建立与每个端口的连接。如果不为虚拟端口分配参数，则 HIC 将以大约一半的速度运行。

SANtricity System Manager 存储驱动器常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是热备盘驱动器？

热备盘在 RAID 1、RAID 5 或 RAID 6 卷组中充当备用驱动器。它们是功能齐全的驱动器，不包含任何数据。如果卷组中的驱动器出现故障，控制器会自动将故障驱动器的数据重建到热备盘。

如果存储阵列中的驱动器出现故障，热备盘驱动器将自动替换出现故障的驱动器，而无需进行物理交换。如果热备盘驱动器在驱动器发生故障时可用，则控制器使用冗余数据将数据从发生故障的驱动器重建到热备盘驱动器。

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）。

池不支持热备盘驱动器。池使用包含池的每个驱动器中的保留容量，而不是热备盘驱动器。

什么是保存容量？

保留容量是在池中保留的容量（驱动器数量），用于支持潜在的驱动器故障。

创建池后，系统会根据池中的驱动器数量自动保留默认的保留容量。

池在重建期间使用保留容量，而卷组使用热备盘驱动器用于相同的目的。与热备盘驱动器相比，保留容量方法是一种改进，因为它可以更快地进行重建。保留容量分布在池中的多个驱动器上，而不是热备盘驱动器的一个驱动器上，因此您不受一个驱动器的速度或可用性的限制。

我为什么要在逻辑上更换驱动器？

如果驱动器出现故障或由于任何其他原因要更换它，并且存储阵列中存在未分配的驱动器，则可以从逻辑上将出现故障的驱动器替换为未分配的驱动器。如果没有未分配的驱动器，则可以改为实际更换驱动器。

来自原始驱动器的数据被复制或重建至替换驱动器。

在哪里可以查看正在重建的驱动器的状态?

您可以从"正在进行的操作"仪表板查看驱动器重建状态。

在主页中，单击右上角的 查看正在进行的操作 链接。

根据驱动器的不同，完整的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。

警报

了解 SANtricity System Manager 中的警报

您可以配置 SANtricity System Manager 通过电子邮件、SNMP 陷阱和 syslog 消息发送存储阵列警报。

什么是警报?

Alerts 通知管理员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 Optimal 到 Offline 或控制器中的冗余错误等问题。所有 Critical 事件以及一些 Warning 和 Informational 事件都被视为"可警报"事件。

了解详情：

- "提醒的运作方式"
- "警报术语"

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 **Settings › Alerts** 获得。

了解详情：

- "为警报配置邮件服务器和收件人"
- "为警报配置 syslog 服务器"
- "配置 SNMP 警报"

相关信息

详细了解与警报相关的概念：

- "事件日志概述"
- "时间戳不一致"

概念

SANtricity System Manager 中警报的工作原理

警报通知管理员存储阵列上发生的重要事件。警报可以通过电子邮件、SNMP 陷阱和 syslog 发送。

警报流程的工作原理如下：

1. 管理员在 System Manager 中配置以下一种或多种警报方法：
   - 电子邮件 — 消息将发送到电子邮件地址。
   - **SNMP** — SNMP 陷阱被发送到 SNMP 服务器。
   - **Syslog** — 消息发送到 syslog 服务器。
2. 当存储阵列的事件监视器检测到问题时，它会将有关该问题的信息写入事件日志（可从菜单：Support[Event Log] 获取）。例如，问题可能包括电池故障、组件从 Optimal 移动到 Offline 或控制器中的冗余错误等事件。
3. 如果事件监视器确定该事件是"可警报的"，则使用配置的警报方法（电子邮件、SNMP 和/或 syslog）发送通知。所有关键事件以及一些警告和信息事件都被认为是"可警报的"。

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。要检查当前配置，请转到菜单：Settings[Alerts]。

警报图块显示警报配置，可为以下选项之一：

- 未配置。
- 已配置；至少设置了一个警报方法。要确定配置了哪些警报方法，请将光标指向图块。

警报信息

警报可能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。
- 事件的简要描述。

系统日志警报遵循 RFC 5424 消息传递标准。

了解 SANtricity 软件中的警报术语

了解警报条款如何适用于您的存储阵列。

组件	说明
事件监控器	事件监视器驻留在存储阵列上，并作为后台任务运行。当事件监视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 Optimal 到 Offline 或控制器中的冗余错误等事件。如果事件监视器确定事件是"可警报的"，则使用配置的警报方法（电子邮件、SNMP 和/或 syslog）发送通知。所有 Critical 事件以及一些 Warning 和 Informational 事件都被视为"可警报"事件。
邮件服务器	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)。
SNMP	简单网络管理协议 (SNMP) 是一种互联网标准协议，用于在 IP 网络上的设备之间管理和共享信息。
SNMP 陷阱	SNMP 陷阱是发送到 SNMP 服务器的通知。陷阱包含有关存储阵列重大问题的信息。
SNMP 陷阱目标	SNMP 陷阱目标是运行 SNMP 服务的服务器的 IPv4 或 IPv6 地址。
社区名称	社区名称是一个字符串，其作用类似于 SNMP 环境中网络服务器的密码。
MIB 文件	管理信息库 (MIB) 文件定义了存储阵列中被监控和管理的数据。必须在具有 SNMP 服务应用程序的服务器上复制和编译该文件。此 MIB 文件可在支持站点上与 System Manager 软件一起获取。
MIB 变量	Management Information Base (MIB) 变量可以返回值，例如存储阵列名称、阵列位置和联系人，以响应 SNMP GetRequests。
系统日志	Syslog 是网络设备用于将事件消息发送到日志记录服务器的协议。
UDP	用户数据报协议 (UDP) 是一种传输层协议，在其数据包标头中指定源和目标端口号。

管理电子邮件提醒

在 **SANtricity System Manager** 中配置邮件服务器和警报收件人

要配置电子邮件警报，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。地址可以是 IPv4 或 IPv6 地址，也可以是完全限定域名。

> 要使用完全限定的域名，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。这是警报消息"发件人"字段中显示的地址。SMTP 协议中需要发件人地址；如果没有它，将导致错误。
- 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 Alerts 页面输入的所有电子邮件地址。

电子邮件警报也可以通过 Initial Setup 向导进行配置。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Email** 选项卡。

   如果尚未配置电子邮件服务器，Email 选项卡将显示"Configure Mail Server"。

3. 选择 **Configure Mail Server**。

   此时将打开 Configure Mail Server 对话框。

4. 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。

     要使用完全限定的域名，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 — 请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 — 如果要加密邮件，请选择 **SMTPS** 或 **STARTTLS** 作为加密类型，然后选择加密邮件的端口号。否则，请选择 **None**。
   - 用户名和密码 — 如果需要，请输入用户名和密码，以便与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 — 要将发件人的联系信息包含在警报消息中，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"提醒"页面的"电子邮件"选项卡中。

5. 选择 **Add Emails**。

   此时将打开添加电子邮件对话框。

6. 输入警报收件人的一个或多个电子邮件地址，然后单击 **Add**。

   电子邮件地址将显示在"提醒"页面上。

7. 如果要确保电子邮件地址有效，请单击 **Test All Emails** 以向收件人发送测试消息。

结果

配置电子邮件警报后，每当发生可警报事件时，事件监视器都会向指定的收件人发送电子邮件。

在 **SANtricity System Manager** 中编辑警报的电子邮件地址

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 Alerts 页面的 Email 选项卡中定义。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Email** 选项卡。
3. 在 **Email Address** 表中，选择您要更改的地址，然后单击最右侧的 **Edit**（铅笔）图标。

   该行成为可编辑字段。

4. 输入新地址，然后单击 **Save**（复选标记）图标。

   如果要取消更改，请选择 **Cancel** (X) 图标。

结果

警报页面的电子邮件选项卡显示更新后的电子邮件地址。

在 **SANtricity System Manager** 中添加警报电子邮件地址

您最多可以为电子邮件提醒添加 20 个收件人。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Email** 选项卡。
3. 选择 **Add Emails**。

   此时将打开添加电子邮件对话框。

4. 在空白字段中，输入新电子邮件地址。如果要添加多个地址，请选择 **Add another email** 以打开其他字段。
5. 单击 **Add**。

结果

Alerts 页面的 Email 选项卡显示新的电子邮件地址。

删除 **SANtricity System Manager** 中用于警报的邮件服务器或电子邮件地址

您可以删除先前定义的邮件服务器，以便不再将警报发送到电子邮件地址，也可以删除单个电子邮件地址。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Email** 选项卡。
3. 从表中，执行以下操作之一：
   - 要删除邮件服务器，以便不再将警报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，以便不再将警报发送到此地址，请选择要删除的电子邮件地址的行。表格右上角的 **Delete** 按钮可供选择。
4. 点击 **Delete**，并确认操作。

在 **SANtricity System Manager** 中编辑警报的邮件服务器

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。地址可以是 IPv4 或 IPv6 地址，也可以是完全限定域名。

> 要使用完全限定的域名，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

1. 选择菜单：Settings[Alerts]。
2. 选择 **Email** 选项卡。
3. 选择 **Configure Mail Server**。

   此时将打开 Configure Mail Server 对话框。

4. 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。

     > 要使用完全限定的域名，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。
   - 在电子邮件中包含联系信息 — 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。
5. 单击 **Save**。

管理 **SNMP** 警报

在 **SANtricity System Manager** 中配置 **SNMP** 警报

要配置简单网络管理协议 (SNMP) 警报，必须至少标识一个存储阵列的事件监视器可以发送 SNMP 陷阱的服务器。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

- 必须使用 SNMP 服务应用程序配置网络服务器。您需要此服务器的网络地址（IPv4 或 IPv6 地址），以便事件监视器可以向该地址发送陷阱消息。您可以使用多台服务器（最多允许 10 台服务器）。
- 管理信息库 (MIB) 文件已使用 SNMP 服务应用程序复制并编译到服务器上。此 MIB 文件定义了被监控和管理的数据。

  如果没有 MIB 文件，则可以从 NetApp 支持站点获取该文件：

  - 转至 "NetApp 支持"。
  - 单击 **Downloads** 选项卡，然后选择 **Downloads**。
  - 单击 **E-Series SANtricity OS Controller Software**。
  - 选择 **Download Latest Release**。
  - 登录。
  - 接受警告声明和许可协议。
  - 向下滚动，直到看到控制器类型的 MIB 文件，然后单击链接下载文件。

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

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   首次设置时， SNMP 选项卡显示"配置社区/用户"。

3. 选择 **Configure Communities/Users**。

   此时将打开选择 SNMP 版本对话框。

4. 选择警报的 SNMP 版本，**SNMPv2c** 或 **SNMPv3**。

   根据您的选择，"配置社区"对话框或"配置 SNMPv3 用户"对话框将打开。

5. 请按照 SNMPv2c（社区）或 SNMPv3（用户）的相应说明进行操作：

   - **SNMPv2c (communities)** — 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。社区名称是标识一组已知管理站的字符串，通常由网络管理员创建。它仅由可打印的 ASCII 字符组成。您最多可以添加 256 个社区。完成后，单击 **Save**。
   - **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，该引擎 ID 用于为消息生成身份验证和加密密钥，并且在管理域中必须是唯一的。在大多数情况下，您应该选择 **Local**。如果您有非标准配置，请选择 **Custom**；另一个字段出现，您必须以十六进制字符串的形式输入权威引擎 ID，偶数个字符的长度在 10 到 32 个字符之间。
     - 身份验证凭据 — 选择身份验证协议，以确保用户的身份。接下来，输入身份验证密码，这是设置或更改身份验证协议时所需的密码。密码长度必须介于 8 到 128 个字符之间。
     - **Privacy credentials** — 选择用于加密消息内容的隐私协议。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 **Add**，然后单击

Close。

6. 在选中 SNMP 选项卡的警报页面中，单击 添加陷阱目标。

   此时将打开添加陷阱目标对话框。

7. 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 **Add**。
   - **Trap Destination** — 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)。（如果您只定义了一个，则该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*警报*页面的 **SNMP** 选项卡中。
8. 要确保陷阱有效，请从表中选择一个陷阱目标，然后单击 **Test Trap Destination** 以将测试陷阱发送到配置的地址。

结果

每当发生可警报事件时，事件监视器都会向服务器发送 SNMP 陷阱。

在 **SANtricity System Manager** 中添加 **SNMP** 警报的陷阱目标

您最多可以添加 10 个用于发送 SNMP 陷阱的服务器。

开始之前

- 必须使用 SNMP 服务应用程序配置要添加的网络服务器。您需要此服务器的网络地址（IPv4 或 IPv6 地址），以便事件监视器可以向该地址发送陷阱消息。您可以使用多台服务器（最多允许使用 10 台服务器）。
- 管理信息库 (MIB) 文件已使用 SNMP 服务应用程序复制并编译到服务器上。此 MIB 文件定义了被监控和管理的数据。

  如果没有 MIB 文件，则可以从 NetApp 支持站点获取该文件：

  - 转至 "NetApp 支持"。
  - 单击 **Downloads**，然后选择 **Downloads**。
  - 单击 **E-Series SANtricity OS Controller Software**。
  - 选择 **Download Latest Release**。
  - 登录。
  - 接受警告声明和许可协议。
  - 向下滚动，直到看到控制器类型的 MIB 文件，然后单击链接下载文件。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   当前定义的陷阱目标显示在表中。

3. 选择 **Add Trap Destinations**。

   此时将打开添加陷阱目标对话框。

4. 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 **Add**。
   - **Trap Destination** — 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)。（如果您只定义了一个，则该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，陷阱目标和关联的社区名称或用户名将显示在表中。
5. 要确保陷阱有效，请从表中选择一个陷阱目标，然后单击 **Test Trap Destination** 以将测试陷阱发送到配置的地址。

结果

每当发生可警报事件时，事件监视器都会向服务器发送 SNMP 陷阱。

在 **SANtricity System Manager** 中配置 **SNMP MIB** 变量

对于 SNMP 警报，您可以选择配置出现在 SNMP 陷阱中的 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。

如果没有 MIB 文件，则可以按以下方式获取：

- 转至 "NetApp 支持"。
- 单击 **Downloads**，然后选择 **Downloads**。
- 单击 **E-Series SANtricity OS Controller Software**。
- 选择 **Download Latest Release**。
- 登录。
- 接受警告声明和许可协议。
- 向下滚动，直到看到控制器类型的 MIB 文件，然后单击链接下载文件。

关于此任务

本任务介绍如何为 SNMP 陷阱定义 MIB 变量。这些变量可以响应 SNMP GetRequests 返回以下值：

- `sysName` （存储阵列的名称）
- `sysLocation` （存储阵列的位置）
- `sysContact` （管理员姓名）

步骤

1. 选择菜单：Settings[Alerts]。

2. 选择 **SNMP** 选项卡。
3. 选择 **Configure SNMP MIB Variables** 。

   此时将打开配置 SNMP MIB 变量对话框。

4. 输入以下一个或多个值，然后单击 保存。
   - **Name** — MIB 变量的值 `sysName`。例如，输入存储阵列的名称。
   - 位置 — MIB 变量的值 `sysLocation`。例如，输入存储阵列的位置。
   - **Contact** — MIB 变量的值 `sysContact`。例如，请输入负责存储阵列的管理员。

结果

这些值出现在存储阵列警报的 SNMP 陷阱消息中。

在 **SANtricity System Manager** 中编辑 **SNMPv2c** 陷阱的社区

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

1. 选择菜单：Setting[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目标和社区名称显示在表中。

3. 选择 **Configure Communities** 。
4. 输入新的社区名称，然后单击 **Save**。社区名称只能由可打印的 ASCII 字符组成。

结果

警报页面的 SNMP 选项卡显示更新的社区名称。

在 **SANtricity System Manager** 中编辑 **SNMPv3** 陷阱的用户设置

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

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目标和用户名显示在表中。

3. 要编辑用户定义，请在表中选择用户，然后单击 **Configure Users**。

4. 在对话框中，单击 **View/Edit Settings**。
5. 编辑以下信息：
   - 用户名 — 更改标识用户的名称，最长可达 31 个字符。
   - 引擎 **ID** — 选择引擎 ID，该引擎 ID 用于为消息生成身份验证和加密密钥，并且在管理域中必须是唯一的。在大多数情况下，您应该选择 **Local**。如果您有非标准配置，请选择 **Custom**；另一个字段出现，您必须以十六进制字符串的形式输入权威引擎 ID，偶数个字符的长度在 10 到 32 个字符之间。
   - 身份验证凭据 — 选择身份验证协议，以确保用户的身份。接下来，输入身份验证密码，这是设置或更改身份验证协议时所需的密码。密码长度必须介于 8 到 128 个字符之间。
   - 隐私凭据 — 选择用于加密消息内容的隐私协议。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

警报页面的 SNMP 选项卡显示更新的设置。

在 **SANtricity System Manager** 中为 **SNMPv2c** 陷阱添加社区

您最多可以为 SNMPv2c 陷阱添加 256 个社区名称。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目标和社区名称显示在表中。

3. 选择 **Configure Communities** 。

   此时将打开"配置社区"对话框。

4. 选择 **Add another community** 。
5. 输入新的社区名称，然后单击 **Save**。

结果

新的社区名称将显示在警报页面的 SNMP 选项卡中。

在 **SANtricity System Manager** 中为 **SNMPv3** 陷阱添加用户

您最多可以为 SNMPv3 陷阱添加 256 个用户。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目标和用户名显示在表中。

3. 选择 **Configure Users**。

此时将打开配置 SNMPv3 用户对话框。

4. 选择 **Add**。
5. 输入以下信息，然后单击 **Add**。
   - 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，该引擎 ID 用于为消息生成身份验证和加密密钥，并且在管理域中必须是唯一的。在大多数情况下，您应该选择 **Local**。如果您有非标准配置，请选择 **Custom**；另一个字段出现，您必须以十六进制字符串的形式输入权威引擎 ID，偶数个字符的长度在 10 到 32 个字符之间。
   - 身份验证凭据 — 选择身份验证协议，以确保用户的身份。接下来，输入身份验证密码，这是设置或更改身份验证协议时所需的密码。密码长度必须介于 8 到 128 个字符之间。
   - 隐私凭据 — 选择用于加密消息内容的隐私协议。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。

在 **SANtricity System Manager** 中删除 **SNMPv2c** 陷阱的社区

您可以删除 SNMPv2c 陷阱的社区名称。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目的地和社区名称显示在 **Alerts** 页面上。

3. 选择 **Configure Communities** 。

   此时将打开"配置社区"对话框。

4. 选择要删除的社区名称，然后单击最右侧的 **Remove** (X) 图标。

   如果陷阱目标与此团体名称关联，Confirm Remove Community 对话框将显示受影响的陷阱目标地址。

5. 确认操作，然后单击 **Remove**。

结果

社区名称及其关联的陷阱目标将从警报页面中删除。

在 **SANtricity System Manager** 中删除 **SNMPv3** 陷阱的用户

您可以删除 SNMPv3 陷阱的用户。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目标和用户名显示在"警报"页面上。

3. 选择 **Configure Users**。

此时将打开配置 SNMPv3 用户对话框。

4. 选择要删除的用户名，然后单击 **Delete**。
5. 确认操作，然后单击 **Delete**。

结果

用户名及其关联的陷阱目标将从"警报"页面中删除。

在 **SANtricity System Manager** 中删除陷阱目标

您可以删除陷阱目标地址，以便存储阵列的事件监视器不再向该地址发送 SNMP 陷阱。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **SNMP** 选项卡。

   陷阱目标地址显示在表中。

3. 选择一个陷阱目标，然后单击页面右上角的 **Delete**。
4. 确认操作，然后单击 **Delete**。

   目标地址不再显示在"提醒"页面上。

结果

已删除的陷阱目标不再从存储阵列的事件监视器接收 SNMP 陷阱。

管理 **syslog** 警报

在 **SANtricity System Manager** 中为警报配置系统日志服务器

要配置 syslog 警报，您必须输入 syslog 服务器地址和 UDP 端口。最多允许五个 syslog 服务器。

开始之前

- syslog 服务器地址必须可用。此地址可以是完全限定的域名、IPv4 地址或 IPv6 地址。
- syslog 服务器的 UDP 端口号必须可用。此端口通常为 514。

关于此任务

此任务描述如何输入 syslog 服务器的地址和端口，然后测试您输入的地址。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Syslog** 选项卡。

   如果尚未定义 syslog 服务器，警报页面将显示"添加 Syslog 服务器"。

3. 单击 **Add Syslog Servers**。

   此时将打开添加 Syslog 服务器对话框。

4. 输入一个或多个 syslog 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 Port** — 通常，syslog 的 UDP 端口为 514。该表显示了已配置的 syslog 服务器。
5. 要向服务器地址发送测试警报，请选择 **Test All Syslog Servers**。

结果

每当发生可警报事件时，事件监视器都会向 syslog 服务器发送警报。要进一步配置审核日志的 syslog 设置，请参见 "为审核日志配置 syslog 服务器"。

> 如果配置了多个 syslog 服务器，则所有配置的 syslog 服务器都将收到审核日志。

在 **SANtricity System Manager** 中编辑警报的系统日志服务器

您可以编辑用于接收 syslog 警报的服务器地址。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Syslog** 选项卡。
3. 从表中选择一个 syslog 服务器地址，然后单击最右侧的*编辑*（铅笔）图标。

   该行成为可编辑字段。

4. 编辑服务器地址和 UDP 端口号，然后单击 **Save**（复选标记）图标。

结果

已更新的服务器地址将显示在表中。

在 **SANtricity System Manager** 中为警报添加系统日志服务器

您最多可为 syslog 警报添加五台服务器。

开始之前

- syslog 服务器地址必须可用。此地址可以是完全限定的域名、IPv4 地址或 IPv6 地址。
- syslog 服务器的 UDP 端口号必须可用。此端口通常为 514。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Syslog** 选项卡。
3. 选择 **Add Syslog Servers**。

   此时将打开添加 Syslog 服务器对话框。

4. 选择 **Add another syslog server**。
5. 输入 syslog 服务器的信息，然后单击 **Add**。
   - **Syslog** 服务器地址 — 输入完全限定的域名、IPv4 地址或 IPv6 地址。
   - **UDP** 端口 — 通常，syslog 的 UDP 端口为 514。

   您最多可以配置五个 syslog 服务器。

结果

syslog 服务器地址显示在表中。

删除 **SANtricity System Manager** 中用于警报的系统日志服务器

您可以删除 syslog 服务器，使其不再接收警报。

步骤

1. 选择菜单：Settings[Alerts]。
2. 选择 **Syslog** 选项卡。
3. 选择一个 syslog 服务器地址，然后单击右上角的 **Remove**。

   此时将打开确认删除 Syslog 服务器对话框。

4. 确认操作，然后单击 **Delete**。

结果

您删除的服务器不再接收来自事件监视器的警报。

SANtricity System Manager 存储系统警报常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

如果已禁用警报，该怎么办？

如果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。警报通知可以通过电子邮件、SNMP 陷阱或 syslog 消息发送。此外，可以从初始设置向导配置电子邮件警报。

如何配置 **SNMP** 或 **syslog** 警报？

除了电子邮件警报外，您还可以将警报配置为通过简单网络管理协议 (SNMP) 陷阱或 syslog 消息发送。

要配置 SNMP 或 syslog 警报，请转到菜单：设置[警报]。

为什么数组和警报之间的时间戳不一致？

当存储阵列发送警报时，它不会更正接收警报的目标服务器或主机的时区。相反，存储阵列使用本地时间 (GMT) 来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

存在不一致。

由于存储阵列在发送警报时未针对时区进行校正，因此警报上的时间戳是 GMT 相关的，其时区偏移量为零。要计算适合您当地时区的时间戳，您应该从 GMT 确定小时偏移量，然后从时间戳中添加或减去该值。

阵列设置

了解 **SANtricity System Manager** 中的设置概述

您可以为某些常规阵列设置和附加功能配置 SANtricity System Manager。

我可以配置哪些设置?

阵列设置包括：

- "缓存设置和性能"
- "自动负载平衡"
- "附加功能"
- "驱动器安全性"

相关任务

详细了解与 System Settings 相关的任务：

- "下载命令行界面 (CLI)"
- "创建内部安全密钥"
- "创建外部安全密钥"
- "配置 iSCSI 端口"
- "通过 IB 端口配置 NVME"
- "通过 RoCE 端口配置 NVMe"

概念

了解 **SANtricity** 软件中的缓存设置和性能

高速缓存内存是控制器上的临时易失性存储区域，其访问时间快于驱动器介质。

使用缓存，可以通过以下方式提高整体 I/O 性能：

- 从主机请求读取的数据可能已经存在于先前操作的缓存中，因此无需驱动器访问。
- 写入数据最初会写入缓存，从而使应用程序可以继续，而不是等待数据写入驱动器。

默认缓存设置满足大多数环境的要求，但您可以根据需要进行更改。

存储阵列缓存设置

对于存储阵列中的所有卷，您可以从系统页面指定以下值：

- 刷新的起始值 — 缓存中触发缓存刷新（写入磁盘）的未写入数据的百分比。当缓存保存指定的未写入数据的启动百分比时，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，它是缓存管理的组织单位。缓存块大小默认为 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，而较大的大小适合需要大量数据传输或顺序 I/O 的应用程序。

卷缓存设置

对于存储阵列中的各个卷，您可以从 Volumes 页面（菜单：Storage[Volumes]）指定以下值：

- 读缓存 — 读缓存是存储已从驱动器读取的数据的缓冲区。读取操作的数据可能已经存在于先前操作的缓存中，因此无需访问驱动器。数据保留在读缓存中，直到刷新为止。
  - 动态读缓存预取 — 动态缓存读取预取允许控制器在将数据块从驱动器读取到缓存时将额外的顺序数据块复制到缓存中。这种缓存增加了将来从缓存中填充数据请求的可能性。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。预取到缓存的数据速率和数量是根据主机读取的速率和请求大小自行调整的。随机访问不会导致数据被预取到缓存中。禁用读缓存时，此功能不适用。
- 写缓存 — 写缓存是一个缓冲区，用于存储来自主机但尚未写入驱动器的数据。数据将保留在写缓存中，直到写入驱动器。写缓存可以提高 I/O 性能。

  可能丢失数据 — 如果启用 无电池写缓存 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启用 无电池写缓存 选项，则可能会丢失数据。

  - 不带电池的写缓存 — 不带电池的写缓存设置允许写缓存继续，即使电池丢失、故障、完全放电或未完全充电。通常不建议选择没有电池的写缓存，因为如果断电，数据可能会丢失。通常，控制器会暂时关闭写缓存，直到电池充电或更换故障电池。
  - 带镜像的写缓存 — 当写入一个控制器的缓存内存的数据也写入另一个控制器的缓存内存时，将发生带镜像的写缓存。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。仅当写缓存已启用且存在两个控制器时，写缓存镜像才可用。使用镜像进行写缓存是创建卷时的默认设置。

了解 **SANtricity** 软件中的自动负载平衡

自动负载平衡通过对负载随时间的变化做出动态反应，并自动调整卷控制器所有权，在工作负载跨控制器转移时纠正任何负载不平衡问题，从而改善 I/O 资源管理。

每个控制器的工作负载都会被持续监控，并且在安装在主机上的多路径驱动程序的协助下，可以在必要时自动实现平衡。当工作负载在控制器之间自动重新平衡时，存储管理员将免除手动调整卷控制器所有权的负担，以适应存储阵列上的负载变化。

启用自动负载平衡后，它执行以下功能：

- 自动监控和平衡控制器资源利用率。
- 在需要时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。

启用和禁用 **Automatic Load Balancing**

所有存储阵列上的自动负载平衡默认处于启用状态。

您可能希望在存储阵列上禁用 Automatic Load Balancing，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。
- 您正在高度调节的环境中运行，其中有目的地设置负载分布，以实现控制器之间的特定分布。

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，您为主机或主机群集选择的主机类型也会对该功能的运行方式产生直接影响。

在跨控制器平衡存储阵列的工作负载时，Automatic Load Balancing 功能会尝试移动两个控制器都可访问且仅映射到能够支持 Automatic Load Balancing 功能的主机或主机群集的卷。

此行为可防止主机由于负载平衡过程而失去对卷的访问权限；但是，映射到不支持 Automatic Load Balancing 的主机的卷的存在会影响存储阵列平衡工作负载的能力。为了实现 Automatic Load Balancing 以平衡工作负载，多路径驱动程序必须支持 TPGS，并且下表中必须包含主机类型。

要将主机集群视为能够 Automatic Load Balancing，该组中的所有主机必须能够支持 Automatic Load Balancing。

支持自动负载平衡的主机类型	使用此多路径驱动程序
Windows 或 Windows 集群	MPIO 与 NetApp E 系列 DSM
Linux DM-MP（内核 3.10 或更高版本）	带有 `scsi_dh_alua`设备处理程序的 DM-MP
VMware	带有 `VMW_SATP_ALUA Storage Array Type`插件的本机多路径插件 (NMP)

除少数例外情况外，不支持 Automatic Load Balancing 的主机类型可继续正常运行，无论该功能是否已启用。一个例外是，如果系统有故障转移，存储阵列会在数据路径返回时将未映射或未分配的卷移回拥有的控制器。映射或分配给非 Automatic Load Balancing 主机的任何卷都不会移动。

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，请参见 "互操作性表工具"。

验证操作系统与 **Automatic Load Balancing** 功能的兼容性

在设置新的（或迁移现有）系统之前，验证操作系统与 Automatic Load Balancing 功能的兼容性。

1. 转到 "互操作性表工具" 以查找您的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。

2. 更新并配置 `/etc/multipath.conf file`。

3. 确保为适用的供应商和产品同时将 `retain_attached_device_handler`和 `detect_prio`设置为 `yes`，或使用默认设置。

配置数组设置

在 **SANtricity System Manager** 中编辑存储阵列名称

您可以更改在 SANtricity System Manager 标题栏中显示的存储阵列名称。

步骤

1. 选择菜单：Settings[System]。
2. 在 **General** 下，查找 **Name:** 字段。

   如果尚未定义存储阵列名称，则此字段显示"Unknown"。

3. 单击存储阵列名称旁边的 **Edit**（铅笔）图标。

   该字段变为可编辑。

4. 输入新名称。

   名称可以包含字母、数字和特殊字符下划线 (_)、短划线 (-) 和哈希符号 (#)。名称不能包含空格。名称最长可为 30 个字符。此名称必须唯一。

5. 单击 **Save**（复选标记）图标。

   如果要关闭可编辑字段而不进行更改，请单击 取消 (X) 图标。

结果

新名称显示在 SANtricity System Manager 的标题栏中。

在 **SANtricity System Manager** 中打开存储阵列定位器指示灯

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

1. 选择菜单：Settings[System]。
2. 在 常规 下，单击 打开存储阵列定位器指示灯。

   打开"打开存储阵列定位器指示灯"对话框，相应存储阵列的定位器指示灯打开。

3. 物理定位存储阵列后，返回对话框并选择 **Turn Off**。

结果

定位器灯关闭，对话框关闭。

在 **SANtricity System Manager** 中同步存储阵列时钟

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，以便它们与管理客户端（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，控制器保持可用和可操作。

> 如果在 System Manager 中启用了 NTP，请不要使用此选项来同步时钟。相反，NTP 使用 SNTP（Simple Network Time Protocol）自动将时钟与外部主机同步。

> 同步后，您可能会注意到性能统计数据丢失或偏斜，时间表受到影响（ASUP、快照等），日志数据中的时间戳偏斜。使用 NTP 可以避免此问题。

步骤

1. 选择菜单：Settings[System]。
2. 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。

   > 对于单工存储阵列，仅显示一个控制器。

3. 如果对话框中显示的时间不匹配，请单击 **Synchronize**。

结果

同步成功后，事件日志和主机日志的事件时间戳相同。

在 **SANtricity System Manager** 中保存存储阵列配置

您可以将存储阵列的配置信息保存在脚本文件中，以节省使用相同配置设置其他存储阵列的时间。

开始之前

存储阵列不得进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、分配或修改热备盘驱动器或向卷组添加容量（驱动器）。

关于此任务

保存存储阵列配置将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 CLI 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，不应使用此生成的 CLI 脚本进行灾难恢复。相反，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联系技术支持以从最新的 Auto-Support 数据中获取此数据。

此操作 不 保存这些设置：

- 电池的使用寿命

- 控制器时间
- 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（Optimal 除外）和状态
- 复制服务，例如镜像和卷复制

应用程序错误的风险 — 如果存储阵列正在进行将更改任何逻辑配置设置的操作，请不要使用此选项。这些操作的示例包括创建或删除卷、下载控制器固件、分配或修改热备盘驱动器或向卷组添加容量（驱动器）。

步骤

1. 选择菜单：Settings[System]。
2. 选择 **Save Storage Array Configuration**。
3. 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

   如果选择 **Host-to-volume assignments** 项目，则会默认选择 **Volume configuration** 项目和 **Host configuration** 项目。不同时保存 "Volume configuration" 和 "Host configuration"，则无法保存 "Host-to-volume assignments"。
4. 单击 **Save**。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `storage-array-configuration.cfg`。

完成后

要将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) 来应用 `.cfg` 文件。

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：Manage[Import Settings]）。

在 **SANtricity System Manager** 中清除存储阵列配置

当要从存储阵列中删除所有池、卷组、卷、主机定义和主机分配时，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 Clear Storage Array Configuration 选项：

- **Volume** — 通常，您可以使用 Volume 选项将测试存储阵列重新配置为生产存储阵列。例如，您可以配置用于测试的存储阵列，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 Engineering 中使用存储阵列，而现在 Engineering 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 Administration，以便重新配置它。

  Storage Array 选项会删除一些其他设置。

	卷	存储阵列
停用 ARVM	X	X
删除池和卷组	X	X
删除卷	X	X
删除主机和主机集群	X	X
删除主机分配	X	X
删除存储阵列名称		X
将存储阵列缓存设置重置为默认值		X

数据丢失风险 — 此操作将从存储阵列中删除所有数据。（不执行安全擦除。）此操作启动后无法取消。仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Settings[System]。
2. 选择 **Clear Storage Array Configuration** 。
3. 在下拉列表中，选择 **Volume** 或 **Storage Array**。
4. *可选：*如果要保存配置（而不是数据），请使用对话框中的链接。
5. 确认要执行此操作。

结果

- 当前配置被删除，将销毁存储阵列上的所有现有数据。
- 所有驱动器均未分配。

存储阵列将在恢复模式下启动。使用存储阵列前必须清除恢复模式。有关详细信息，请参见 "清除恢复模式"。

在 **SANtricity System Manager** 中更改存储阵列缓存设置

对于存储阵列中的所有卷，您可以调整刷新和块大小的缓存内存设置。

关于此任务

缓存内存是控制器上的临时易失性存储区域，具有比驱动器介质更快的访问时间。要调整缓存性能，您可以调整以下设置：

缓存设置	说明
启动按需缓存刷新	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，当未写入数据达到 80% 容量时，缓存刷新开始。对于主要进行写入操作的环境，较高的百分比是一个不错的选择，因此可以通过缓存处理新的写入请求，而无需访问磁盘。在 I/O 不稳定（具有数据突发）的环境中，较低的设置更好，因此系统会在数据突发之间频繁刷新缓存。但是，低于 80% 的启动百分比可能会导致性能下降。
缓存块大小	缓存块大小确定每个缓存块的最大大小，这是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 KiBs。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，较小的大小是一个不错的选择。较大的尺寸非常适合生成顺序 I/O 的应用程序，例如多媒体。

步骤

1. 选择菜单：Settings[System]。
2. 向下滚动到 **Additional Settings**，然后单击 **Change Cache Settings**。

   此时将打开更改缓存设置对话框。

3. 调整以下值：
   - 启动需求缓存刷新 — 选择适合环境中使用的 I/O 的百分比。如果选择低于 80% 的值，您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。
4. 单击 **Save**。

在 **SANtricity System Manager** 中设置自动负载平衡

自动负载平衡功能可确保来自主机的传入 I/O 流量在两个控制器之间进行动态管理和平衡。默认情况下，此功能处于启用状态，但您可以从 SANtricity System Manager 中禁用它。

关于此任务

启用自动负载平衡后，它执行以下功能：

- 自动监控和平衡控制器资源利用率。
- 在需要时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。

您可能希望在存储阵列上禁用 Automatic Load Balancing，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。
- 您正在高度调节的环境中运行，其中有目的地设置负载分布，以实现控制器之间的特定分布。

步骤

1. 选择菜单：Settings[System]。
2. 向下滚动到 **Additional Settings**，然后单击 **Enable/Disable Automatic Load Balancing**。

   此选项下方的文本指示该功能当前是已启用还是已禁用。

   此时将打开一个确认对话框。

3. 单击 是 确认以继续。

   通过选择此选项，您可以在启用/禁用之间切换功能。

   如果此功能从已禁用移至已启用，则也会自动启用 Host Connectivity Reporting 功能。

在 **SANtricity System Manager** 中启用或禁用旧版管理界面

您可以启用或禁用旧式管理界面 (SYMbol)，这是存储阵列与管理客户端之间的通信方法。

关于此任务

默认情况下，旧版管理界面处于打开状态。如果禁用它，存储阵列和管理客户端将使用更安全的通信方法（通过 https 的 REST API）；但是，如果禁用它，某些工具和任务可能会受到影响。

对于 EF600 存储系统，默认情况下此功能处于禁用状态。

此设置会影响以下操作：

- **On**（默认）-- 使用 CLI 和一些其他工具（例如 OCI 适配器）配置镜像所需的设置。
- **Off** — 在存储阵列和管理客户端之间的通信中强制保密以及访问外部工具的必要设置。配置 Directory Server (LDAP) 时的推荐设置。

步骤

1. 选择菜单：Settings[System]。
2. 向下滚动到 **Additional Settings**，然后单击 **Change Management Interface**。
3. 在对话框中，单击 **Yes** 以继续。

配置附加功能

SANtricity System Manager 中附加功能的工作原理

附加组件是 SANtricity System Manager 标准配置中未包含的功能，可能需要密钥才能启用。附加功能可以是单个高级功能或捆绑功能包。

以下步骤概述了如何启用高级功能或功能包：

1. 获取以下信息：
   - 机箱序列号和功能启用标识符，用于标识要安装功能的存储阵列。这些项目在 System Manager 中可用。
   - 功能激活码，可在购买功能时从 Support 站点获得。
2. 通过联系存储提供商或访问 Premium Feature Activation 网站获取功能密钥。提供用于激活的机箱序列号、启用标识符和功能代码。
3. 使用 System Manager，使用功能密钥文件启用高级功能或功能包。

了解 **SANtricity** 软件中的附加功能术语

了解附加功能条款如何适用于您的存储阵列。

术语	说明
功能启用标识符	功能启用标识符是标识特定存储阵列的唯一字符串。此标识符可确保在获取高级功能时，它仅与该特定存储阵列相关联。此字符串显示在"系统"页面上的"附加组件"下。
功能密钥文件	功能密钥文件是您收到的用于解锁和启用高级功能或功能包的文件。
功能包	功能包是更改存储阵列属性的捆绑包（例如，将协议从 Fibre Channel 更改为 iSCSI）。功能包需要特殊密钥才能启用。
高级功能	高级功能是需要密钥才能启用的额外选项。它不包含在 System Manager 的标准配置中。

在 **SANtricity System Manager** 中获取功能密钥文件

要在存储阵列上启用高级功能或功能包，必须首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。必填信息包括：

- 机箱序列号
- 功能启用标识符
- 功能激活码

步骤

1. 在 System Manager 中，找到并记录机箱序列号。您可以将鼠标悬停在 Support Center 图块上来查看此序列号。
2. 在 System Manager 中，找到功能启用标识符。转到菜单：Settings[System]，然后向下滚动到*附加组件*。寻找*功能启用标识符*。记录功能启用标识符的编号。
3. 找到并记录用于功能激活的代码。对于功能包，此代码在执行转换的相应说明中提供。

对于高级功能，您可以从 Support 站点访问激活码，如下所示：

a. 登录到 "NetApp 支持"。

b. 转至产品的 **Software Licenses**。

c. 输入存储阵列机箱的序列号，然后单击 **Go**。

d. 在*许可证密钥*列中查找功能激活码。

e. 记录所需功能的功能激活码。

4. 通过向您的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。

   您还可以转到 "NetApp 许可证激活：存储阵列高级功能激活"并输入所需的信息，以获取功能或功能包。（本网站上的说明适用于高级功能，而不是功能包。）

完成后

当您有功能密钥文件时，您可以启用高级功能或功能包。

在 **SANtricity System Manager** 中启用高级功能

高级功能是需要密钥才能启用的额外选项。

开始之前

- 您已获得功能密钥。如果需要，请联系技术支持以获得密钥。
- 您已将密钥文件加载到管理客户端（具有用于访问 System Manager 的浏览器的系统）。

关于此任务

此任务介绍如何使用 System Manager 启用高级功能。

> 如果要禁用高级功能，必须在命令行界面 (CLI) 中使用 Disable Storage Array Feature 命令 (`disable storageArray (featurePack | feature=featureAttributeList`。

步骤

1. 选择菜单：Settings[System]。
2. 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。

3. 单击 **Browse**，然后选择密钥文件。

   文件名显示在对话框中。

4. 单击 启用。

在 **SANtricity System Manager** 中启用功能包

功能包是更改存储阵列属性的捆绑包（例如，将协议从 Fibre Channel 更改为 iSCSI）。功能包需要特殊密钥才能启用。

开始之前

- 您已经遵循了描述新存储阵列属性的转换和准备的相应说明。有关主机协议转换说明，请参见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。
- 所有数据都已备份。
- 您已获得功能包文件。

  功能包文件加载到管理客户端（具有用于访问 System Manager 的浏览器的系统）。

必须安排停机维护时段，并停止主机与控制器之间的所有 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

1. 选择菜单：Settings[System]。
2. 在 **Add-ons** 下，选择 **Change Feature Pack**。
3. 单击 **Browse**，然后选择密钥文件。

   文件名显示在对话框中。
4. 在字段中键入 `change`。
5. 单击 **Change**。

   功能包迁移开始，控制器重新启动。会删除未写入的缓存数据，从而确保没有 I/O 活动。要使新功能包生效，两个控制器都会自动重新启动。重启完成后，存储阵列返回到响应状态。

下载 **SANtricity** 命令行界面 **(CLI)**

从 SANtricity System Manager，您可以下载命令行界面 (CLI) 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，并使用与外部安装的管理软件包中可用的 CLI 相同的语法。下载 CLI 无需密钥。

开始之前

Java Runtime Environment (JRE) 8 及更高版本必须在计划运行 CLI 命令的管理系统上可用。

步骤

1. 选择菜单：Settings[System]。
2. 在 附加组件 下，选择 命令行界面。

   ZIP 包将下载到浏览器。
3. 将 ZIP 文件保存到计划在其中为存储阵列运行 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 CLI 命令，例如 DOS C: 提示符。System Manager 用户界面右上角的"帮助"菜单提供了 CLI 命令参考。

SANtricity System Manager 存储阵列设置常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

什么是自动负载平衡?

自动负载平衡功能提供自动 I/O 平衡，并确保来自主机的传入 I/O 流量在两个控制器之间进行动态管理和平衡。

自动负载平衡功能通过对负载随时间变化的动态响应和自动调整卷控制器所有权来提供改进的 I/O 资源管理，以便在工作负载跨控制器转移时纠正任何负载不平衡问题。

每个控制器的工作负载都会被持续监控，并且在安装在主机上的多路径驱动程序的协助下，可以在必要时自动实现平衡。当工作负载在控制器之间自动重新平衡时，存储管理员将免除手动调整卷控制器所有权的负担，以适应存储阵列上的负载变化。

启用自动负载平衡后，它执行以下功能：

- 自动监控和平衡控制器资源利用率。
- 在需要时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。

分配给使用控制器 SSD Cache 的任何卷都不符合自动负载平衡传输的条件。

什么是控制器缓存?

控制器缓存是一个物理内存空间，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。

对于读取和写入数据传输，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。

当控制器缓存接收到数据时，控制器会向主机应用程序确认它现在正在保存数据。这样，主机应用程序无需等待 I/O 写入磁盘。相反，应用程序可以继续操作。服务器应用程序也可以轻松访问缓存的数据，无需额外的磁盘读取即可访问数据。

控制器缓存以多种方式影响存储阵列的整体性能：

- 缓存充当缓冲区，因此无需同步主机和磁盘数据传输。
- 来自主机的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。
- 如果使用写缓存，则主机可以在将来自先前写操作的数据写入磁盘之前发送后续写命令。
- 如果启用缓存预取，则优化顺序读取访问。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。

可能丢失数据 — 如果启用 无电池写缓存 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启用 无电池写缓存 选项，则可能会丢失数据。

什么是缓存刷新？

当缓存中的未写入数据量达到一定水平时，控制器会定期将缓存数据写入驱动器。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，直到缓存数据量低于缓存刷新阈值。默认情况下，当 80% 的缓存正在使用时，就会开始刷新。

在 System Manager 中，您可以设置"`Start demand cache flushing`"阈值，以最好地支持环境中使用的 I/O 类型。在主要是写入操作的环境中，应将"`Start demand cache flushing`"百分比设置为高，以增加缓存无需转到磁盘即可处理任何新写入请求的可能性。高百分比设置会限制缓存刷新的次数，以便缓存中保留更多数据，从而增加更多缓存命中的机会。

在 I/O 不稳定（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刷新缓存。在处理各种负载的多样化 I/O 环境中，或当负载类型未知时，将阈值设置为 50% 作为良好的中间地带。请注意，如果选择低于 80% 的起始百分比，您可能会看到性能下降，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维持缓存级别所需的磁盘写入次数，从而增加系统开销。

基于年龄的算法指定写入数据可以保留在缓存中的时间段，然后才有资格刷新到磁盘。控制器使用基于年龄的算法，直到达到缓存刷新阈值。默认值为 10 秒，但此时间段仅在不活动期间计算。您无法在 System Manager 中修改刷新计时；相反，您必须在命令行界面 (CLI) 中使用 **Set Storage Array** 命令。

> 可能丢失数据 — 如果启用 无电池写缓存 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启用 无电池写缓存 选项，则可能会丢失数据。

什么是缓存块大小？

存储阵列的控制器将其缓存组织成"块"，这些块可以是大小为 8、16、32 KiB 的内存块。存储系统上的所有卷都共享相同的缓存空间；因此，卷只能有一个缓存块大小。

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 KiBs。较小的大小是文件系统或数据库应用程序的理想选择。对于需要大数据传输、顺序 I/O 或高带宽（如多媒体）的应用程序，较大尺寸是一个不错的选择。

何时应同步存储阵列时钟？

如果您注意到 SANtricity System Manager 中显示的时间戳与管理客户端（通过浏览器访问 SANtricity System Manager 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。仅当未在 SANtricity System Manager 中启用 NTP（网络时间协议）时，才需要执行此任务。

> 我们强烈建议您使用 NTP 服务器而不是手动同步时钟。NTP 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"系统"页面的"同步存储阵列时钟"对话框中检查同步状态。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，该对话框指示控制器时钟的时间显示是否已偏移且不再同步。

驱动器安全性

了解 **SANtricity System Manager** 中的驱动器安全性

您可以从 Security Key Management 页面配置 Drive Security 和密钥管理。

什么是 **Drive Security**?

Drive Security 是一项功能，可防止在从存储阵列中删除时对启用安全功能的驱动器上的数据进行未经授权的访问。这些驱动器可以是全磁盘加密 (FDE) 驱动器，也可以是联邦信息处理标准 (FIPS) 驱动器。当 FDE 或 FIPS 驱动器从阵列中物理移除时，它们必须安装在另一个阵列中才能运行，此时，驱动器将处于安全锁定状态，直到提供正确的安全密钥。_安全密钥_是在这些类型的驱动器和存储阵列中的控制器之间共享的字符串。

了解详情：

- "Drive Security 功能的工作方式"
- "安全密钥管理的工作原理"
- "驱动器安全术语"

如何配置密钥管理?

要实现 Drive Security，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，请转到菜单：Settings[System > Security key management]，您可以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 Drive Security。

了解详情：

- "创建内部安全密钥"
- "创建外部安全密钥"
- "手动创建池"
- "创建卷组"

如何解锁驱动器?

如果您配置了密钥管理，然后将启用安全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。

了解详情：

- "使用内部密钥管理时解锁驱动器"
- "使用外部密钥管理时解锁驱动器"

相关信息

详细了解与密钥管理相关的任务：

- "使用 CA 签名的证书对密钥管理服务器进行身份验证"
- "备份安全密钥"

概念

SANtricity System Manager 中驱动器安全功能的工作原理

Drive Security 是一种存储阵列功能，通过全磁盘加密 (FDE) 驱动器或联邦信息处理标准

(FIPS) 驱动器提供额外的安全层。

当这些驱动器与 Drive Security 功能一起使用时，它们需要安全密钥才能访问其数据。当驱动器从阵列中物理卸下时，它们必须安装在另一个阵列中才能运行，此时，它们将处于 Security Locked 状态，直到提供正确的安全密钥。

如何实施驱动器安全

要实现驱动器安全，请执行以下步骤。

1. 为您的存储阵列配备支持安全的驱动器，无论是 FDE 驱动器还是 FIPS 驱动器。（对于需要 FIPS 支持的卷，仅使用 FIPS 驱动器。在卷组或池中混合 FIPS 和 FDE 驱动器将导致所有驱动器被视为 FDE 驱动器。此外，FDE 驱动器不能添加到全 FIPS 卷组或池中或用作备用驱动器。）
2. 创建一个安全密钥，它是控制器和驱动器共享的字符串，用于读/写访问。您可以从控制器的持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。对于外部密钥管理，必须与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：
   - 创建池或卷组（在 Candidates 表中的 **Secure-capable** 列中查找 **Yes**）。
   - 在创建新卷时选择池或卷组（在池和卷组候选项表中的 **Secure-capable** 旁边查找 **Yes**）。

Drive Security 在驱动器级别的工作原理

具有安全功能的驱动器（FDE 或 FIPS）在写入期间对数据进行加密，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程。每个驱动器都有自己独特的加密密钥，永远无法从驱动器传输。

驱动器安全功能通过具有安全功能的驱动器提供额外的保护层。当这些驱动器上的卷组或池被选择用于 Drive Security 时，驱动器在允许访问数据之前会查找安全密钥。您可以随时为池和卷组启用 Drive Security，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 Drive Security。

Drive Security 在存储阵列级别的工作原理

使用 Drive Security 功能，您可以创建在存储阵列中启用安全的驱动器和控制器之间共享的安全密钥。每当关闭和打开驱动器的电源时，启用安全的驱动器都会变为 Security Locked 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安全的驱动器，并将其重新安装到其他存储阵列中，则该驱动器将处于安全锁定状态。重新定位的驱动器在重新访问数据之前会查找安全密钥。要解锁数据，请从源存储阵列应用安全密钥。成功解锁后，重新定位的驱动器将使用目标存储阵列中已存储的安全密钥，不再需要导入的安全密钥文件。

> 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。它不是人类可读的格式，用户也无法访问。

Drive Security 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，还可以为这些池或卷组启用驱动器安全。驱动器安全选项使驱动器和关联的卷组和池安全-已启用。

在创建启用安全的卷组和池之前，请记住以下准则：

- 卷组和池必须完全由具有安全功能的驱动器组成。（对于需要 FIPS 支持的卷，仅使用 FIPS 驱动器。在卷组或池中混合 FIPS 和 FDE 驱动器将导致所有驱动器被视为 FDE 驱动器。此外，FDE 驱动器不能添加到全 FIPS 卷组或池中或用作备用驱动器。）

- 卷组和池必须处于最佳状态。

SANtricity System Manager 中安全密钥管理的工作原理

当您实施驱动器安全功能时，启用安全的驱动器（FIPS 或 FDE）需要安全密钥才能访问数据。安全密钥是在这些类型的驱动器和存储阵列中的控制器之间共享的一串字符。

每当关闭和打开驱动器的电源时，启用安全的驱动器将变为安全锁定状态，直到控制器应用安全密钥。如果从存储阵列中删除了启用安全的驱动器，则该驱动器的数据将被锁定。当驱动器重新安装在不同的存储阵列中时，它会在重新访问数据之前查找安全密钥。要解锁数据，您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：

- 控制器持久内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

内部密钥管理

内部密钥被维护并"`hidden`"在控制器永久内存上的不可访问位置。要实施内部密钥管理，请执行以下步骤：

1. 在存储阵列中安装具有安全功能的驱动器。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。
2. 确保已启用 Drive Security 功能。如有必要，请联系您的存储供应商，以获取有关启用 Drive Security 功能的说明。
3. 创建内部安全密钥，其中包括定义标识符和通行短语。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：设置[系统 > 安全密钥管理 > 创建内部密钥]。

安全密钥存储在控制器上的隐藏且不可访问的位置。然后，您可以创建启用安全的卷组或池，也可以在现有卷组和池上启用安全性。

外部密钥管理

外部密钥使用密钥管理互操作性协议 (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：

1. 在存储阵列中安装具有安全功能的驱动器。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。
2. 确保已启用 Drive Security 功能。如有必要，请联系您的存储供应商，以获取有关启用 Drive Security 功能的说明。
3. 获取已签名的客户端证书文件。客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 KMIP 请求。
   a. 首先，完成并下载客户端证书签名请求 (CSR)。进入菜单：Settings[Certificates > Key Management > Complete CSR]。
   b. 接下来，向受密钥管理服务器信任的 CA 请求签名的客户端证书。（您还可以使用 CSR 文件从密钥管理服务器创建和下载客户端证书。）
   c. 获得客户端证书文件后，将该文件复制到访问 System Manager 的主机。

d. 或者，您可以使用私钥和公钥对在外部生成证书签名请求。

4. 从密钥管理服务器检索证书文件，然后将该文件复制到您正在访问 System Manager 的主机。密钥管理服务器证书验证密钥管理服务器，因此存储阵列可以信任其 IP 地址。您可以为密钥管理服务器使用根证书、中间证书或服务器证书。

5. 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：Settings[System > Security key management > Create External Key]。

系统使用您输入的凭据连接到密钥管理服务器。然后，您可以创建启用安全的卷组或池，也可以对现有卷组和池启用安全性。

了解 **SANtricity** 软件中的驱动器安全术语

了解 Drive Security 术语如何适用于您的存储阵列。

术语	说明
驱动器安全功能	驱动器安全是一种存储阵列功能，可通过全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器提供额外的安全层。当这些驱动器与驱动器安全功能一起使用时，它们需要安全密钥才能访问其数据。当驱动器从阵列中物理卸下时，它们必须安装在另一个阵列中才能运行，此时，它们将处于安全锁定状态，直到提供正确的安全密钥。
FDE 驱动器	全磁盘加密 (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，该芯片在写入过程中对数据进行加密，然后在读取过程中对数据进行解密。
FIPS 驱动器	FIPS 驱动器使用联邦信息处理标准 (FIPS) 140-2 level 2。它们本质上是 FDE 驱动器，符合美国政府确保强大加密算法和方法的标准。FIPS 驱动器具有比 FDE 驱动器更高的安全标准。
管理客户端	本地系统（计算机、平板电脑等），包括用于访问 System Manager 的浏览器。
密码短语	密码短语用于加密安全密钥以进行备份。由于驱动器迁移或磁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。 Drive Security 的通行短语与存储阵列的管理员密码无关。
支持安全的驱动器	支持安全的驱动器可以是全磁盘加密 (FDE) 驱动器，也可以是联邦信息处理标准 (FIPS) 驱动器，它们在写入期间加密数据，在读取期间解密数据。这些驱动器被认为是安全_有能力_的，因为它们可以使用 Drive Security 功能用于额外的安全性。如果为与这些驱动器一起使用的卷组和池启用了 Drive Security 功能，则驱动器将变得安全_已启用_。

术语	说明
启用安全功能的驱动器	启用安全的驱动器与 Drive Security 功能一起使用。当您启用 Drive Security 功能，然后将 Drive Security 应用于支持安全的驱动器上的池或卷组时，驱动器将变为启用安全。只能通过配置了正确安全密钥的控制器进行读写访问。这种额外的安全性可以防止对从存储阵列中物理移除的驱动器上的数据进行未经授权的访问。
安全密钥	安全密钥是在存储阵列中启用安全的驱动器和控制器之间共享的一串字符。每当关闭和打开驱动器的电源时，启用安全的驱动器将变为安全锁定状态，直到控制器应用安全密钥。如果从存储阵列中删除了启用安全的驱动器，则该驱动器的数据将被锁定。当驱动器重新安装在不同的存储阵列中时，它会在重新访问数据之前查找安全密钥。要解锁数据，您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 — 在控制器的持久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。
安全密钥标识符	安全密钥标识符是在密钥创建过程中与安全密钥关联的字符串。标识符存储在控制器和与安全密钥关联的所有驱动器上。

配置安全密钥

在 **SANtricity System Manager** 中创建内部安全密钥

要使用 Drive Security 功能，您可以创建由存储阵列中的控制器和具有安全功能的驱动器共享的内部安全密钥。内部密钥保留在控制器的永久内存中。

开始之前

- 必须在存储阵列中安装具有安全功能的驱动器。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。
- 必须启用驱动器安全功能。否则，在此任务期间将打开"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以获取有关启用驱动器安全功能的说明。

如果 FDE 和 FIPS 驱动器都安装在存储阵列中，则它们都共享相同的安全密钥。

关于此任务

在此任务中，您定义与内部安全密钥关联的标识符和密码短语。

Drive Security 的通行短语与存储阵列的管理员密码无关。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Create Internal Key**。

   如果尚未生成安全密钥，则会打开"创建安全密钥"对话框。

3. 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，由控制器固件生成）或输入您自己的值。您最多可以输入 189 个字母数字字符，无需空格、标点符号或符号。

     其他字符将自动生成，并附加到您输入的字符串的两端。生成的字符确保标识符是唯一的。

   - **Define a pass phrase/Re-enter pass phrase** — 输入并确认密码短语。该值可以包含 8 到 32 个字符，并且必须包含以下每个字符：
     - 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）。

     请务必记录您的输入以供以后使用。如果需要从存储阵列中移动启用安全的驱动器，则必须知道标识符和密码短语才能解锁驱动器数据。

4. 单击 **Create**。

   安全密钥存储在控制器上不可访问的位置。除了实际的密钥外，还有一个从浏览器下载的加密密钥文件。

   下载文件的路径可能取决于浏览器的默认下载位置。

5. 记录您的密钥标识符、密码以及下载的密钥文件的位置，然后单击 **Close**。

结果

现在，您可以创建启用安全的卷组或池，也可以对现有卷组和池启用安全性。

每当驱动器的电源关闭然后再次打开时，所有启用安全的驱动器都会变为安全锁定状态。在此状态下，在控制器在驱动器初始化期间应用正确的安全密钥之前，数据不可访问。如果有人物理移除锁定的驱动器并将其安装在另一个系统中，安全锁定状态可防止对其数据进行未经授权的访问。

完成后

您应该验证安全密钥，以确保密钥文件未损坏。

在 **SANtricity System Manager** 中创建外部安全密钥

要将 Drive Security 功能与密钥管理服务器一起使用，必须创建由密钥管理服务器和存储阵列中具有安全功能的驱动器共享的外部密钥。

开始之前

- 必须在阵列中安装具有安全功能的驱动器。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。

  如果 FDE 和 FIPS 驱动器都安装在存储阵列中，则它们都共享相同的安全密钥。

- 必须启用驱动器安全功能。否则，在此任务期间将打开"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以获取有关启用驱动器安全功能的说明。
- 您拥有存储阵列控制器的签名客户端证书文件，并且已将该文件复制到访问 System Manager 的主机。客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 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您正在访问 System Manager 的主机。密钥管理服务器证书验证密钥管理服务器，因此存储阵列可以信任其 IP 地址。您可以为密钥管理服务器使用根证书、中间证书或服务器证书。

> 有关服务器证书的详细信息，请参阅密钥管理服务器的文档。

关于此任务

在此任务中，您需要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

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Create External Key**。

> 如果当前配置了内部密钥管理，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。

3. 在 **Connect to Key Server** 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，将使用第二个密钥服务器。确保每个密钥服务器都可以访问相同的密钥数据库；否则，数组将发布错误，无法使用备份服务器。

> 一次仅使用一个密钥服务器。如果存储阵列无法到达主密钥服务器，则阵列将联系备份密钥服务器。请注意，必须保持两台服务器之间的奇偶校验；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，为存储阵列的控制器选择证书文件。
   - 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 按钮为密钥管理服务器选择证书文件。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。
4. 单击 **Next**。
5. 在 **Create/Backup Key** 下，您可以出于安全目的创建备份密钥。
   - （推荐）要创建备份密钥，请选中复选框，然后输入并确认密码短语。该值可以包含 8 到 32 个字符，并且必须包含以下每个字符：
     - 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）。

请务必记录您的输入以供以后使用。如果需要从存储阵列中移动启用安全的驱动器，则必须知道密码短语才能解锁驱动器数据。

+

- 如果不想创建备份密钥，请取消选中该复选框。

请注意，如果您失去了对外部密钥服务器的访问权限，并且您没有备份密钥，则如果它们迁移到其他存储阵列，您将失去对驱动器上数据的访问权限。此选项是在 System Manager 中创建备份密钥的唯一方法。

6. 单击 **Finish**。

   系统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您的本地系统上。

   下载文件的路径可能取决于浏览器的默认下载位置。

7. 记录您的密码短语和下载的密钥文件的位置，然后单击 关闭。

   页面将显示以下消息以及用于外部密钥管理的其他链接：

   ```
   Current key management method: External
   ```

8. 通过选择 测试通信 来测试存储阵列和密钥管理服务器之间的连接。

   测试结果显示在对话框中。

结果

启用外部密钥管理后，可以创建启用安全的卷组或池，也可以启用现有卷组和池的安全性。

每当驱动器的电源关闭然后再次打开时，所有启用安全的驱动器都会变为安全锁定状态。在此状态下，在控制器在驱动器初始化期间应用正确的安全密钥之前，数据不可访问。如果有人物理移除锁定的驱动器并将其安装在另一个系统中，安全锁定状态可防止对其数据进行未经授权的访问。

完成后

您应该验证安全密钥，以确保密钥文件未损坏。

管理安全密钥

在 **SANtricity System Manager** 中更改安全密钥

您可以随时用新密钥替换安全密钥。如果您的公司存在潜在的安全漏洞，并且希望确保未经授权的人员无法访问驱动器数据，则可能需要更改安全密钥。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Change Key**。

   此时将打开更改安全密钥对话框。

3. 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（存储阵列名称和时间戳，由控制器固件生成）或输入您自己的值。您最多可以输入 189 个字母数字字符，无需空格、标点符号或符号。

     其他字符将自动生成，并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。

   - **Define a pass phrase/Re-enter pass phrase** — 在这些字段中，输入您的通行短语。该值可以包含 8 到 32 个字符，并且必须包含以下每个字符：
     - 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）。
4. 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"Delete current security key…"复选框。

   请务必记录您的条目以供以后使用 — 如果您需要从存储阵列中移动启用安全的驱动器，则必须知道标识符和密码短语才能解锁驱动器数据。

5. 单击 **Change**。

   新的安全密钥将覆盖上一个不再有效的密钥。

   下载文件的路径可能取决于浏览器的默认下载位置。

6. 记录您的密钥标识符、密码以及下载的密钥文件的位置，然后单击 **Close**。

完成后

您应该验证安全密钥，以确保密钥文件未损坏。

在 **SANtricity System Manager** 中从外部密钥管理切换到内部密钥管理

您可以将 Drive Security 的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。先前为外部密钥管理定义的安全密钥然后用于内部密钥管理。

关于此任务

在此任务中，您将禁用外部密钥管理，并将新的备份副本下载到本地主机。现有密钥仍用于 Drive Security，但将在存储阵列中进行内部管理。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Disable External Key Management**。

此时将打开禁用外部密钥管理对话框。

3. 在 **Define a pass phrase/Re-enter pass phrase** 中，输入并确认密钥备份的密码短语。该值可以包含 8 到 32 个字符，并且必须包含以下每个字符：

   - 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）。

   > 请务必记录您的条目以供以后使用。如果需要从存储阵列中移动启用安全的驱动器，则必须知道标识符和密码短语才能解锁驱动器数据。

4. 单击 **Disable**。

   备份密钥已下载到本地主机。

5. 记录您的密钥标识符、密码以及下载的密钥文件的位置，然后单击 **Close**。

结果

驱动器安全性现在通过存储阵列进行内部管理。

完成后

您应该验证安全密钥，以确保密钥文件未损坏。

在 **SANtricity System Manager** 中编辑密钥管理服务器设置

如果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

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **View/Edit Key Management Server Settings**。
3. 在以下字段中编辑信息：
   - 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 (KMIP) 通信的端口号。

     可选： 您可以通过单击 添加密钥服务器 添加另一个密钥服务器。

4. 单击 **Save**。

在 **SANtricity System Manager** 中备份安全密钥

创建或更改安全密钥后，您可以创建密钥文件的备份副本，以防原始文件损坏。

关于此任务

此任务介绍如何备份之前创建的安全密钥。在此过程中，为备份创建新的密码短语。此密码短语不需要与创建或上次更改原始密钥时使用的密码短语相匹配。密码短语仅适用于正在创建的备份。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Back Up Key**。

   此时将打开备份安全密钥对话框。

3. 在 **Define a pass phrase/Re-enter pass phrase** 字段中，输入并确认此备份的密码短语。

   该值可以包含 8 到 32 个字符，并且必须包含以下每个字符：

   - 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）

   请务必记录您的条目以供日后使用。您需要密码短语才能访问此安全密钥的备份。

4. 单击 **Back Up**。

   将安全密钥的备份下载到本地主机，然后打开 **Confirm/Record Security Key Backup** 对话框。

   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。

5. 在安全的位置记录您的密码短语，然后单击 关闭。

完成后

您应验证备份安全密钥。

在 **SANtricity System Manager** 中验证安全密钥

您可以验证安全密钥以确保其未损坏，并验证您的密码短语是否正确。

关于此任务

此任务介绍如何验证您之前创建的安全密钥。这是一个重要的步骤，可以确保密钥文件未损坏，并且密码短语正确，这样可以确保在将启用了安全功能的驱动器从一个存储阵列移动到另一个存储阵列时，您以后可以访问驱动器数据。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Validate Key**。

   此时将打开验证安全密钥对话框。

3. 单击 **Browse**，然后选择密钥文件（例如， `drivesecurity.slk`）。
4. 输入与所选密钥关联的密码短语。

   当您选择有效的密钥文件和密码短语时，**Validate** 按钮将变为可用。

5. 单击 **Validate**。

验证结果显示在对话框中。

6. 如果结果显示"安全密钥已成功验证"，请单击 **Close**。如果出现错误消息，请按照对话框中显示的建议说明进行操作。

在 **SANtricity System Manager** 中使用内部密钥管理时解锁驱动器

如果您配置了内部密钥管理，然后将启用安全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，以访问驱动器上的加密数据。

开始之前

- 在源阵列（要卸下驱动器的阵列）上，您已导出卷组并卸下驱动器。在目标阵列上，您已重新安装驱动器。

> System Manager 用户界面不支持导出/导入功能；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，请参阅 "NetApp 知识库"。对于由 System Manager 管理的新阵列或旧系统，请务必遵循相应的说明。

- 必须启用驱动器安全功能。否则，在此任务期间将打开"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以获取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。
- 安全密钥文件在管理客户端（具有用于访问 System Manager 的浏览器的系统）上可用。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，安全密钥将本地存储在存储阵列上。安全密钥是由控制器和驱动器共享的一串字符，用于读/写访问。当驱动器从阵列中物理卸下并安装在另一个阵列中时，除非您提供正确的安全密钥，否则驱动器无法运行。

> 您可以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。本主题介绍在使用 *internal* 密钥管理时解锁数据。如果您使用 *external* 密钥管理，请参阅 "使用外部密钥管理时解锁驱动器"。如果您正在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 E-Series 和 SANtricity 文档中心中 "解锁驱动器" 所述的不同步骤进行操作。

在另一个阵列中重新安装启用安全的驱动器后，该阵列将发现驱动器并显示"需要注意"条件以及"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。（此密码与存储阵列的管理员密码不同。）

如果在新存储阵列中安装了其他启用安全的驱动器，则它们可能使用与您导入的安全密钥不同的安全密钥。在导入过程中，旧的安全密钥仅用于解锁要安装的驱动器的数据。当解锁过程成功时，新安装的驱动器将重新设置为目标存储阵列的安全密钥。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Unlock Secure Drives**。

   解锁安全驱动器对话框打开。任何需要安全密钥的驱动器都会显示在表中。

3. *可选：*将鼠标悬停在驱动器编号上，以查看驱动器的位置（盘架编号和托架编号）。

4. 单击 **Browse**，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。

5. 输入与此密钥文件关联的密码短语。

   您输入的字符将被屏蔽。

6. 单击 **Unlock**。

   如果解锁操作成功，此对话框将显示："关联的安全驱动器已解锁。"

结果

当所有驱动器都被锁定然后解锁时，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，则控制器将不会重新启动。

完成后

在目标阵列（具有新安装驱动器的阵列）上，现在可以导入卷组。

> System Manager 用户界面不支持导出/导入功能；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，请参阅 "NetApp 知识库"。

在 **SANtricity System Manager** 中使用外部密钥管理时解锁驱动器

如果您配置了外部密钥管理，然后将启用安全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，以访问驱动器上的加密数据。

开始之前

- 在源阵列（要卸下驱动器的阵列）上，您已导出卷组并卸下驱动器。在目标阵列上，您已重新安装驱动器。

  > System Manager 用户界面不支持导出/导入功能；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，请参阅 "NetApp 知识库"。对于由 System Manager 管理的新阵列或旧系统，请务必遵循相应的说明。

- 必须启用驱动器安全功能。否则，在此任务期间将打开"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以获取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。
- 您拥有存储阵列控制器的签名客户端证书文件，并且已将该文件复制到访问 System Manager 的主机。客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 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您正在访问 System Manager 的主机。密钥管理服务器证书验证密钥管理服务器，因此存储阵列可以信任其 IP 地址。您可以为密钥管理服务器使用根证书、中间证书或服务器证书。

有关服务器证书的详细信息，请参阅密钥管理服务器的文档。

关于此任务

当您使用外部密钥管理时，安全密钥将外部存储在旨在保护安全密钥的服务器上。安全密钥是由控制器和驱动器共享的字符串，用于读/写访问。当驱动器从阵列中物理卸下并安装在另一个阵列中时，在您提供正确的安全密钥之前，它们无法运行。

您可以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。本主题介绍在使用 *external* 密钥管理时解锁数据。如果您使用 *internal* 密钥管理，请参阅 "使用内部密钥管理时解锁驱动器"。如果您正在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 E-Series 和 SANtricity 文档中心中 "解锁驱动器" 所述的不同步骤进行操作。

在另一个阵列中重新安装启用安全的驱动器后，该阵列将发现驱动器并显示"需要注意"条件以及"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。（此密码与存储阵列的 Administrator 密码不同。）在此过程中，将存储阵列配置为使用外部密钥管理服务器，然后即可访问安全密钥。您需要提供存储阵列的服务器的联系信息，以连接和检索安全密钥。

如果在新存储阵列中安装了其他启用安全的驱动器，则它们可能使用与您导入的安全密钥不同的安全密钥。在导入过程中，旧的安全密钥仅用于解锁要安装的驱动器的数据。当解锁过程成功时，新安装的驱动器将重新设置为目标存储阵列的安全密钥。

步骤

1. 选择菜单：Settings[System]。
2. 在 **Security key management** 下，选择 **Create External Key**。
3. 使用先决条件连接信息和证书完成向导。
4. 单击 **Test Communication** 以确保访问外部密钥管理服务器。
5. 选择 **Unlock Secure Drives**。

   解锁安全驱动器对话框打开。任何需要安全密钥的驱动器都会显示在表中。
6. *可选：*将鼠标悬停在驱动器编号上，以查看驱动器的位置（盘架编号和托架编号）。
7. 单击 **Browse**，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。
8. 输入与此密钥文件关联的密码短语。

   您输入的字符将被屏蔽。
9. 单击 **Unlock**。

   如果解锁操作成功，此对话框将显示："关联的安全驱动器已解锁。"

结果

当所有驱动器都被锁定然后解锁时，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，则控制器将不会重新启动。

完成后

在目标阵列（具有新安装驱动器的阵列）上，现在可以导入卷组。

> System Manager 用户界面不支持导出/导入功能；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，请参阅 "NetApp 知识库"。

SANtricity System Manager 存储驱动器安全常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

在创建安全密钥之前，我需要知道什么？

安全密钥由存储阵列中的控制器和启用安全功能的驱动器共享。如果从存储阵列中删除了启用安全的驱动器，安全密钥将保护数据免受未经授权的访问。

您可以使用以下方法之一创建和管理安全密钥：

- 控制器持久内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

内部密钥管理

内部密钥得到维护，并"隐藏"在控制器永久内存上的不可访问位置。在创建内部安全密钥之前，您必须执行以下操作：

1. 在存储阵列中安装具有安全功能的驱动器。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。
2. 确保已启用 Drive Security 功能。如有必要，请联系您的存储供应商，以获取有关启用 Drive Security 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。完成后，安全密钥将存储在控制器上不可访问的位置。然后，您可以创建启用安全的卷组或池，也可以在现有卷组和池上启用安全性。

外部密钥管理

外部密钥使用密钥管理互操作性协议 (KMIP) 维护在单独的密钥管理服务器上。在创建外部安全密钥之前，必须执行以下操作：

1. 在存储阵列中安装具有安全功能的驱动器。这些驱动器可以是全磁盘加密 (FDE) 驱动器或联邦信息处理标准 (FIPS) 驱动器。
2. 确保已启用 Drive Security 功能。如有必要，请联系您的存储供应商，以获取有关启用 Drive Security 功能的说明。
3. 获取已签名的客户端证书文件。客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 KMIP 请求。
   a. 首先，完成并下载客户端证书签名请求 (CSR)。进入菜单：Settings[Certificates > Key Management > Complete CSR]。

b. 接下来，向受密钥管理服务器信任的 CA 请求签名的客户端证书。（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。）

c. 获得客户端证书文件后，将该文件复制到访问 System Manager 的主机。

4. 从密钥管理服务器检索证书文件，然后将该文件复制到您正在访问 System Manager 的主机。密钥管理服务器证书验证密钥管理服务器，因此存储阵列可以信任其 IP 地址。您可以为密钥管理服务器使用根证书、中间证书或服务器证书。

然后，您可以创建一个外部密钥，其中包括定义密钥管理服务器的 IP 地址和用于 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，您可以创建启用安全的卷组或池，也可以在现有卷组和池上启用安全性。

为什么需要定义密码短语？

密码短语用于对存储在本地管理客户端上的安全密钥文件进行加密和解密。如果没有密码短语，安全密钥将无法解密，并且在重新安装到另一个存储阵列中时无法用于从启用安全的驱动器解锁数据。

为什么记录安全密钥信息很重要？

如果丢失安全密钥信息且没有备份，则可能会在重新定位启用安全的驱动器或升级控制器时丢失数据。您需要安全密钥才能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保存安全密钥文件的本地主机上的位置。

在备份安全密钥之前，我需要知道什么？

如果您的原始安全密钥已损坏，并且您没有备份，则如果驱动器从一个存储阵列迁移到另一个存储阵列，您将失去对驱动器上数据的访问权限。

在备份安全密钥之前，请记住以下准则：

- 请确保您知道原始密钥文件的安全密钥标识符和密码。

  仅内部密钥使用标识符。创建标识符时，会自动生成附加字符并将其附加到标识符字符串的两端。生成的字符确保标识符是唯一的。

- 您为备份创建新的密码短语。此密码短语不需要与创建或上次更改原始密钥时使用的密码短语相匹配。密码短语仅适用于您要创建的备份。

  不应将驱动器安全的密码短语与存储阵列的管理员密码混淆。驱动器安全的密码短语保护安全密钥的备份。管理员密码可保护整个存储阵列免受未经授权的访问。

- 备份安全密钥文件将下载到您的管理客户端。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。

解锁安全驱动器之前，我需要了解哪些信息？

要从启用安全的驱动器解锁数据，您必须导入其安全密钥。

在解锁启用安全功能的驱动器之前，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键入到目标存储阵列。
- 对于要迁移的驱动器，您必须知道安全密钥标识符和对应于安全密钥文件的密码短语。
- 安全密钥文件必须在管理客户端（具有用于访问 System Manager 的浏览器的系统）上可用。
- 如果要重置锁定的 NVMe 驱动器，则必须输入驱动器的安全 ID。要查找安全 ID，您必须以物理方式移除驱动器，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。

什么是读/写可访问性？

Drive Settings 窗口包含有关 Drive Security 属性的信息。"Read/Write Accessible"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（转到菜单：Settings[System > Unlock Secure Drives]）。

关于验证安全密钥，我需要了解哪些信息？

创建安全密钥后，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。
- 如果控制器无法解密安全密钥进行验证，则可能是输入了错误的密码短语。请仔细检查密码短语，如有必要请重新输入，然后重试验证。如果错误消息再次出现，请选择密钥文件的备份（如果可用）并重试验证。
- 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。

内部安全密钥和外部安全密钥管理有什么区别？

当您实施 Drive Security 功能时，可以使用内部安全密钥或外部安全密钥在从存储阵列中移除启用安全的驱动器时锁定数据。

安全密钥是一串字符，在存储阵列中启用安全的驱动器和控制器之间共享。内部密钥保留在控制器的永久内存中。外部密钥使用密钥管理互操作性协议 (KMIP) 维护在单独的密钥管理服务器上。

访问管理

了解 **SANtricity System Manager** 中的访问管理

访问管理是在 SANtricity System Manager 中建立用户身份验证的方法。

有哪些可用的身份验证方法？

身份验证方法包括 RBAC（基于角色的访问控制）、Directory Services 和 Security Assertion Markup Language (SAML)：

- **RBAC/**本地用户角色 — 身份验证通过存储阵列中实施的 RBAC 功能进行管理。本地用户角色包括预定义的

用户配置文件和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 (IdP) 进行管理。

了解详情：

- "访问管理的工作原理"
- "访问管理术语"
- "映射角色的权限"
- "本地用户角色"
- "目录服务"
- "SAML"

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：Settings[Access Management]。

了解详情：

- "添加 LDAP 目录服务器"
- "配置 SAML"

相关信息

详细了解与访问管理相关的任务：

- "更改密码"
- "查看审核日志活动"
- "为审核日志配置 syslog 服务器"

概念

访问管理在 **SANtricity System Manager** 中的工作原理

访问管理是在 SANtricity System Manager 中建立用户身份验证的方法。

配置和用户身份验证的工作原理如下：

1. 管理员使用包含安全管理员权限的用户配置文件登录到 System Manager。

   首次登录时，用户名 `admin`会自动显示且无法更改。 `admin`用户可以完全访问系统中的所有功能。

2. 管理员导航到用户界面中的访问管理。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。

3. 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和具有特定访问权限的角色。管理员可以将这些本地用户角色用作单一身份验证方法，也可以将其与目录服务结合使用。除了为用户设置密码外，无需进行其他配置。
   - 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 用户映射到嵌入在存储阵列中的本地用户角色。
   - **SAML** — 身份验证通过身份提供程序 (IdP) 使用安全断言标记语言 (SAML) 2.0 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 用户映射到嵌入在存储阵列中的本地用户角色。
4. 管理员为用户提供 System Manager 的登录凭据。
5. 用户通过输入其凭据登录到系统。

> 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。

在登录过程中，系统会执行以下后台任务：

- 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。
- 在界面右上角显示用户名。

System Manager 中的可用任务

对任务的访问取决于用户分配的角色，包括以下内容：

- **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。
- 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。
- **Support admin** — 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。
- **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

不可用的任务要么变为灰色，要么不显示在用户界面中。例如，具有 Monitor 角色的用户可以查看有关卷的所有信息，但不能访问修改该卷的功能。**Copy Services** 和 **Add to Workload** 等功能的选项卡将变为灰色；仅 **View/Edit Settings** 可用。

Unified Manager 和 Storage Manager 中的限制

如果为存储阵列配置了 SAML，则用户无法从 Unified Manager 或旧版 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时，用户必须在执行以下任一功能之前输入凭据：

- 重命名存储阵列

- 升级控制器固件
- 加载存储阵列配置
- 执行脚本
- 尝试在未使用的会话超时时执行活动操作

了解 **SANtricity** 软件中的访问管理术语

了解 Access Management 条款如何适用于您的存储阵列。

术语	说明
访问令牌	访问令牌用于使用 REST API 或命令行界面 (CLI) 代替用户名和密码进行身份验证。令牌与特定用户（包括 LDAP 用户）相关联，并包括一组权限和过期时间。
Active Directory	Active Directory (AD) 是一种 Microsoft 目录服务，它将 LDAP 用于 Windows 域网络。
绑定	绑定操作用于向目录服务器验证客户端。绑定通常需要帐户和密码凭据，但有些服务器允许匿名绑定操作。
CA	证书颁发机构 (CA) 是颁发电子文档（称为数字证书）以实现 Internet 安全的受信任实体。这些证书可以识别网站所有者，从而实现客户端和服务器之间的安全连接。
证书	出于安全目的，证书可识别站点的所有者，从而防止攻击者模拟站点。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）的受信任实体的身份。
IdP	身份提供程序 (IdP) 是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的外部系统。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。
LDAP	轻型目录访问协议（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。
RBAC	基于角色的访问控制 (RBAC) 是一种根据单个用户的角色来调节对计算机或网络资源的访问的方法。RBAC 控件在存储阵列上实施，并包括预定义角色。
SAML	Security Assertion Markup Language (SAML) 是用于两个实体之间的身份验证和授权的基于 XML 的标准。SAML 允许多因素身份验证，其中用户必须提供两个或多个项目来证明其身份（例如密码和指纹）。存储阵列的嵌入式 SAML 功能符合 SAML2.0 的身份断言、身份验证和授权。
SP	服务提供商 (SP) 是控制用户身份验证和访问的系统。使用 SAML 配置访问管理时，存储阵列充当向身份提供程序请求身份验证的服务提供程序。
SSO	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。

了解 SANtricity System Manager 中映射角色的权限

存储阵列上实施的 RBAC（基于角色的访问控制）功能包括预定义的用户配置文件，其中映射了一个或多个角色。每个角色都包含访问 SANtricity System Manager 中任务的权限。

用户配置文件和映射角色可从菜单：Settings[Access Management > Local User Roles] 在任一 System Manager 的用户界面中访问。

这些角色为用户提供对任务的访问权限，如下所示：

- **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。
- 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。
- **Support admin** — 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。
- **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

如果用户没有某个任务的权限，则该任务将以灰色显示或不显示在用户界面中。

在 SANtricity System Manager 中使用本地用户角色配置访问管理

对于访问管理，管理员可以使用在存储阵列中实施的 RBAC（基于角色的访问控制）功能。这些功能称为"本地用户角色"。

配置工作流

已为存储阵列预配置本地用户角色。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：

1. 管理员使用包含安全管理员权限的用户配置文件登录到 System Manager。

> `admin` 用户可以完全访问系统中的所有功能。

2. 管理员审阅用户配置文件，这些配置文件是预定义的，无法修改。
3. 可选地，管理员为每个用户配置文件分配新密码。
4. 用户使用其分配的凭据登录到系统。

管理

当仅使用本地用户角色进行身份验证时，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。
- 允许用户无需密码即可登录。

在 SANtricity System Manager 中使用目录服务配置访问管理

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。

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：

1. 管理员使用包含安全管理员权限的用户配置文件登录到 System Manager。

> `admin` 用户可以完全访问系统中的所有功能。

2. 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。
3. 如果 LDAP 服务器使用安全协议 (LDAPS)，管理员将上传证书颁发机构 (CA) 证书链，用于 LDAP 服务器和存储阵列之间的身份验证。
4. 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。
5. 管理员测试 LDAP 服务器与存储阵列之间的连接。
6. 用户使用其分配的 LDAP/目录服务凭据登录到系统。

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。

在 SANtricity System Manager 中使用 SAML 配置访问管理

对于访问管理，管理员可以使用嵌入在数组中的安全断言标记语言 (SAML) 2.0 功能。

配置工作流

SAML 配置的工作原理如下：

1. 管理员使用包含安全管理员权限的用户配置文件登录到 System Manager。

> 此 `admin`用户具有对 System Manager 中所有功能的完全访问权限。

2. 管理员转到 Access Management 下的 **SAML** 选项卡。
3. 管理员配置与身份提供商 (IdP) 的通信。IdP 是用于向用户请求凭据并确定用户是否成功通过身份验证的外部系统。要配置与存储阵列的通信，管理员从 IdP 系统下载 IdP 元数据文件，然后使用 System Manager 将文件上传到存储阵列。

4. 管理员在服务提供商和 IdP 之间建立信任关系。服务提供商控制用户授权；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 IdP。

   管理员还应确保 IdP 支持在身份验证时返回名称 ID 的功能。

5. 管理员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 System Manager 创建映射。
6. 管理员测试 IdP URL 的 SSO 登录。此测试确保存储阵列和 IdP 可以通信。

   启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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。

7. 在 System Manager 中，管理员为存储阵列启用 SAML。
8. 用户使用其 SSO 凭据登录到系统。

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：

- 修改或创建新的角色映射
- 导出 Service Provider 文件

访问限制

启用 SAML 后，用户无法从 Unified Manager 或旧版 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)
- 软件开发工具包 (SDK) 客户端
- 带内客户端
- 使用标准 REST API 端点登录

启用 **SAML** 时的有限连接

启用 SAML 时，以下存储阵列功能与 JSON Web Token 身份验证的连接受限。

- 命令行界面 (CLI)
- HTTP 基本身份验证 REST API 客户端

了解访问令牌和 **SANtricity** 软件

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，而不会暴露用户名和密码。令牌与特定用户（包括 LDAP 用户）相关联，并包括一组权限和过期。

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 实际上变得不可操作，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，该令牌要求用户通过 MFA 进行身份验证。

> 无需启用 SAML 即可使用 web 令牌，但建议使用 SAML 以获得最高级别的安全性。

创建和使用令牌的工作流程

1. 在 System Manager 中创建令牌并确定其过期时间。
2. 将令牌文本复制到剪贴板或将其下载到文件，然后将令牌文本保存在安全位置。
3. 按如下方式使用令牌：
   - **REST API**：要在 REST API 请求中使用令牌，请向请求添加 HTTP 标头。例如：
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI**：要在 CLI 中使用令牌，请在命令行上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`

了解详情：

- "创建访问令牌"
- "编辑访问令牌"
- "撤销访问令牌"

使用本地用户角色

在 SANtricity System Manager 中查看本地用户角色

从本地用户角色选项卡，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 RBAC（基于角色的访问控制）的一部分。

开始之前

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 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

1. 选择菜单：Settings[Access Management]。
2. 选择 **Local User Roles** 选项卡。

   用户配置文件显示在表中：

   - **Root admin** (admin) — 有权访问系统中所有功能的超级管理员。此用户配置文件包括所有角色。

- **Storage admin** （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：Storage Admin、Support Admin 和 Monitor。
- **Security admin** （安全） — 负责安全配置的用户，包括访问管理、证书管理和启用安全的驱动器功能。此用户配置文件包括以下角色：Security Admin 和 Monitor。
- **Support admin**（support）-- 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。
- **Monitor**（monitor）-- 对系统具有只读访问权限的用户。此用户配置文件仅包括 Monitor 角色。

在 **SANtricity System Manager** 中更改密码

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都必须满足或超过当前设置的最低密码要求（在 View/Edit Settings 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，请务必包含空格。
- 为提高安全性，请至少使用 15 个字母数字字符，并经常更改密码。

> 在 System Manager 中更改密码也会在命令行界面 (CLI) 中更改密码。此外，密码更改会导致用户的活动会话终止。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Local User Roles** 选项卡。
3. 从表中选择一个用户。

   "更改密码"按钮变为可用。

4. 选择 **Change Password**。

   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，则可以选中该复选框，要求所选用户输入密码以访问存储阵列，然后可以为所选用户键入新密码。
6. 输入您的本地管理员密码，然后单击 **Change**。

结果

如果用户当前已登录，密码更改将导致用户的活动会话终止。

在 **SANtricity System Manager** 中更改本地用户密码设置

您可以为存储阵列上的所有新用户密码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存储阵列，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的本地用户密码。
- 本地用户密码所需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。
- 如果您希望本地用户在不输入密码的情况下访问存储阵列，请不要设置密码的最小长度。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Local User Roles** 选项卡。
3. 选择 **View/Edit Settings** 按钮。

   此时将打开本地用户密码设置对话框。

4. 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"要求所有本地用户密码至少为"复选框。
   - 要为所有本地用户密码设置最小密码长度，请选中"Require all local user passwords to be at least"复选框，然后使用微调框为所有本地用户密码设置所需的最小长度。

     任何新的本地用户密码必须满足或超过当前设置。

5. 单击 **Save**。

使用目录服务

在 **SANtricity System Manager** 中添加 **LDAP** 目录服务器

要为访问管理配置身份验证，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

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 必须在您的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

添加目录服务器是一个两步的过程。首先，输入域名和 URL。如果服务器使用安全协议，则如果 CA 证书由非标准签名机构签名，则还必须上传该证书进行身份验证。如果您有绑定帐户的凭据，还可以输入您的用户帐户名和密码。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。

> 在添加 LDAP 服务器的过程中，旧版管理界面将被禁用。旧版管理界面 (SYMbol) 是存储阵列与管理客户端之间的通信方法。禁用时，存储阵列和管理客户端使用更安全的通信方法 (基于 https 的 REST API)。

步骤

1. 选择菜单：Settings[Access Management]。
2. 在 Directory Services 选项卡中，选择 **Add Directory Server**。

   此时将打开添加目录服务器对话框。
3. 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

设置	说明
配置设置	域
输入 LDAP 服务器的域名。对于多个域，请在逗号分隔的列表中输入域。登录名（ *username@domain* ）中使用域名来指定要进行身份验证的目录服务器。	服务器 URL
以 `ldap[s]://` **`host:`**`*port*` 的格式输入用于访问 LDAP 服务器的 URL。	上传证书（可选）
仅当在上面的服务器 URL 字段中指定了 LDAPS 协议时，才会显示此字段。 单击 **Browse** 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受信任证书或证书链。	绑定帐户（可选）
输入只读用户帐户，以便对 LDAP 服务器进行搜索查询并在组内进行搜索。以 LDAP 类型的格式输入帐户名称。例如，如果绑定用户名为 "bindacct"，则可以输入诸如 "CN=bindacct,CN=Users,DC=cpoc,DC=local" 之类的值。	绑定密码（可选）

设置	说明
在上面输入绑定帐户时，将显示此字段。 输入绑定帐户的密码。	添加前测试服务器连接
如果要确保存储阵列可以与您输入的 LDAP 服务器配置通信，请选中此复选框。单击对话框底部的*添加*后进行测试。如果选中此复选框且测试失败，则不会添加配置。您必须解决错误或取消选中复选框才能跳过测试并添加配置。	权限设置
搜索基本 DN	输入 LDAP 上下文以搜索用户，通常采用的形式为 `CN=Users, DC=cpoc, DC=local`。
用户名属性	输入绑定到用户 ID 进行身份验证的属性。例如： `sAMAccountName`。
组属性	输入用户的组属性列表，用于组到角色的映射。例如： `memberOf, managedObjects`。

4. 单击 **Role Mapping** 选项卡。
5. 将 LDAP 组分配给预定义的角色。一个组可以有多个分配的角色。

字段详细信息

设置	说明
映射	组 DN
指定要映射的 LDAP 用户组的组可分辨名称 (DN)。支持正则表达式。如果这些特殊正则表达式字符不是正则表达式模式的一部分，则必须使用反斜杠(`\`转义：\.[]{}()<>*+-=!?^$	
角色	在字段中单击，然后选择要映射到组 DN 的存储阵列的一个角色。您必须单独选择要包含到此组的每个角色。Monitor 角色与其他角色结合使用是登录到 SANtricity System Manager 所必需的。映射的角色包括以下权限： • **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。 • 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。 • **Support admin** — 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。 • **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

所有用户（包括管理员）都需要 Monitor 角色。如果没有 Monitor 角色，System Manager 将无法为任何用户正常运行。

6. 如果需要，单击 **Add another mapping** 以输入更多组到角色的映射。
7. 完成映射后，单击 **Add**。

   系统执行验证，确保存储阵列和 LDAP 服务器可以通信。如果出现错误消息，请检查在对话框中输入的凭据，并在必要时重新输入信息。

在 **SANtricity System Manager** 中编辑目录服务器设置和角色映射

如果以前在 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的映射。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 必须定义目录服务器。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Directory Services** 选项卡。
3. 如果定义了多个服务器，请从表中选择要编辑的服务器。
4. 选择 **View/Edit Settings**。

   此时将打开目录服务器设置对话框。

5. 在 Server Settings 选项卡中，更改所需的设置。

字段详细信息

设置	说明
配置设置	域
LDAP 服务器的域名。对于多个域，请在逗号分隔的列表中输入域。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。	服务器 URL
用于以 `ldap[s]://host:port` 形式访问 LDAP 服务器的 URL。	绑定帐户（可选）
只读用户帐户，用于针对 LDAP 服务器进行搜索查询以及在组内进行搜索。	绑定密码（可选）
bind 帐户的密码。（输入 bind 帐户时将显示此字段。）	保存前测试服务器连接
检查存储阵列是否可以与 LDAP 服务器配置通信。测试在您单击对话框底部的*保存*后进行。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以跳过测试并重新编辑配置。	权限设置
搜索基本 DN	用于搜索用户的 LDAP 上下文，通常采用的形式为 `CN=Users, DC=cpoc, DC=local`。
用户名属性	绑定到用户 ID 进行身份验证的属性。例如： `sAMAccountName`。
组属性	用户的组属性列表，用于组到角色的映射。例如： `memberOf, managedObjects`。

6. 在角色映射选项卡中，更改所需的映射。

字段详细信息

设置	说明
映射	组 DN
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是正则表达式模式的一部分，则必须使用反斜杠(`\`转义：\.[]{}()<>*+-=!?^$	
角色	要映射到组 DN 的存储阵列的角色。您必须单独选择要包含到此组的每个角色。Monitor 角色需要与其他角色结合使用才能登录到 SANtricity System Manager。存储阵列的角色包括以下内容： • **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。 • 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。 • **Support admin** — 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。 • **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

所有用户（包括管理员）都需要 Monitor 角色。如果没有 Monitor 角色，System Manager 将无法为任何用户正常运行。

7. 如果需要，单击 **Add another mapping** 以输入更多组到角色的映射。
8. 单击 **Save**。

结果

完成此任务后，将终止所有活动的用户会话。仅保留当前用户会话。

在 **SANtricity System Manager** 中删除目录服务器

要断开目录服务器和存储阵列之间的连接，可以从"访问管理"页删除服务器信息。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

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。

关于此任务

完成此任务后，将终止所有活动的用户会话。仅保留当前用户会话。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Directory Services** 选项卡。
3. 从列表中选择要删除的目录服务器。
4. 单击 **Remove**。

   此时将打开删除目录服务器对话框。

5. 在字段中键入 `remove`，然后单击*删除*。

   目录服务器配置设置、权限设置和角色映射将被删除。用户无法再使用此服务器的凭据登录。

使用 SAML

在 SANtricity System Manager 中配置 SAML

要为 Access Management 配置身份验证，可以使用存储阵列中嵌入的 Security Assertion Markup Language (SAML) 功能。此配置在 Identity Provider 和 Storage Provider 之间建立连接。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 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 的功能。
- 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 元数据文件从 IdP 系统下载，可在用于访问 System Manager 的本地系统上使用。

关于此任务

标识提供程序 (IdP) 是一个外部系统，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。IdP 可以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 (SP) 是控制用户身份验证和访问的系统。使用 SAML 配置访问管理时，存储阵列充当向身份提供程序请求身份验证的服务提供程序。要在 IdP 和存储阵列之间建立连接，请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 之前测试连接和 SSO 登录。

SAML 和 **Directory Services**。如果在将 Directory Services 配置为身份验证方法时启用 SAML，则 SAML 将取代 System Manager 中的 Directory Services。如果稍后禁用 SAML，Directory Services 配置将返回到以前的配置。

*编辑和禁用。*启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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过程。

步骤 1：上传 IdP 元数据文件

要向存储阵列提供 IdP 连接信息，请将 IdP 元数据导入 System Manager。IdP 系统需要此元数据才能将身份验证请求重定向到正确的 URL 并验证收到的响应。您只需要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

1. 选择菜单：Settings[Access Management]。
2. 选择 **SAML** 选项卡。

   该页面显示了配置步骤的概述。

3. 单击 **Import Identity Provider (IdP) file** 链接。

   此时将打开导入身份提供程序文件对话框。

4. 单击 **Browse** 以选择并上传您复制到本地系统的 IdP 元数据文件。

   选择文件后，将显示 IdP 实体 ID。

5. 单击 **Import**。

步骤 2：导出服务提供程序文件

若要在 IdP 和存储阵列之间建立信任关系，请将 Service Provider 元数据导入 IdP。IdP 需要此元数据来与控制器建立信任关系并处理授权请求。该文件包括控制器域名或 IP 地址等信息，以便 IdP 可以与 Service Provider 进行通信。

步骤

1. 单击 **Export Service Provider files** 链接。

   此时将打开 Export Service Provider Files 对话框。

2. 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 以将元数据文件保存到本地系统。如果存储阵列包括两个控制器，请在 控制器 **B** 字段中对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您的本地系统。记下文件的存储位置。

3. 从本地系统中，找到您导出的 Service Provider 元数据文件。

   每个控制器都有一个 XML 格式的文件。

4. 从 IdP 服务器导入 Service Provider 元数据文件以建立信任关系。您可以直接导入文件，也可以从文件中手动输入控制器信息。

步骤 3：映射角色

要向用户提供对 System Manager 的授权和访问权限，必须将 IdP 用户属性和组成员身份映射到存储阵列的预定义角色。

开始之前

- IdP 管理员在 IdP 系统中配置了用户属性和组成员身份。

- IdP 元数据文件导入到 System Manager 中。
- 为信任关系将每个控制器的 Service Provider 元数据文件导入 IdP 系统中。

步骤

1. 单击*映射 System Manager* 角色的链接。

   此时将打开角色映射对话框。

2. 将 IdP 用户属性和组分配给预定义的角色。一个组可以有多个分配的角色。

   字段详细信息

设置	说明
映射	用户属性
为要映射的 SAML 组指定属性（例如"成员"）。	属性值
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是正则表达式模式的一部分，则必须使用反斜杠(`\`转义：\.[]{}()<>*+-=!?^$	
角色	在字段中单击，然后选择要映射到属性的存储阵列角色之一。您必须单独选择要包含的每个角色。要登录到 System Manager，需要将监视器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： • **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。 • 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。 • **Support admin** — 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。 • **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

   所有用户（包括管理员）都需要 Monitor 角色。如果没有 Monitor 角色，System Manager 将无法为任何用户正常运行。

3. 如果需要，单击 **Add another mapping** 以输入更多组到角色的映射。

启用 SAML 后，可以修改角色映射。

4. 完成映射后，单击 **Save**。

步骤 4：测试 SSO 登录

为了确保 IdP 系统和存储阵列可以通信，您可以选择测试 SSO 登录。此测试也在启用 SAML 的最后一步中执行。

开始之前

- IdP 元数据文件导入到 System Manager 中。
- 为信任关系将每个控制器的 Service Provider 元数据文件导入 IdP 系统中。

步骤

1. 选择 **Test SSO Login** 链接。

   此时将打开一个用于输入 SSO 凭据的对话框。

2. 输入具有 Security Admin 权限和 Monitor 权限的用户的登录凭据。

   系统测试登录时将打开一个对话框。

3. 查找"测试成功"消息。如果测试成功完成，请转到下一步以启用 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 Security Admin 和 Monitor 权限的组。
   - 您为 IdP 服务器上传的元数据正确。
   - SP 元数据文件中的控制器地址正确。

步骤 5：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。上一步描述了 SSO 登录测试流程。

开始之前

- IdP 元数据文件导入到 System Manager 中。
- 为信任关系将每个控制器的 Service Provider 元数据文件导入 IdP 系统中。
- 至少配置了一个 Monitor 和一个 Security Admin 角色映射。

*编辑和禁用。*启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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

1. 从 **SAML** 选项卡中，选择 **Enable SAML** 链接。

   此时将打开确认启用 SAML 对话框。

2. 键入 `enable`，然后单击 **Enable**。
3. 输入 SSO 登录测试的用户凭据。

结果

系统启用 SAML 后，将终止所有活动会话，并开始通过 SAML 对用户进行身份验证。

在 **SANtricity System Manager** 中更改 **SAML** 角色映射

如果之前为访问管理配置了 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

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- IdP 管理员在 IdP 系统中配置了用户属性和组成员身份。
- 已配置并启用 SAML。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **SAML** 选项卡。
3. 选择 **Role Mapping**。

   此时将打开角色映射对话框。

4. 将 IdP 用户属性和组分配给预定义的角色。一个组可以有多个分配的角色。

   请小心，不要在启用 SAML 时删除权限，否则您将失去对 System Manager 的访问权限。

   字段详细信息

设置	说明
映射	用户属性
为要映射的 SAML 组指定属性（例如"成员"）。	属性值
指定要映射的组的属性值。	角色

   所有用户（包括管理员）都需要 Monitor 角色。如果没有 Monitor 角色，System Manager 将无法为任何用户正常运行。

5. （可选）单击 **Add another mapping** 以输入更多组到角色的映射。

6. 单击 **Save**。

结果

完成此任务后，将终止所有活动的用户会话。仅保留当前用户会话。

在 **SANtricity System Manager** 中导出 **SAML** 服务提供程序文件

如有必要，您可以导出存储阵列的 Service Provider 元数据，然后将文件重新导入 Identity Provider (IdP) 系统。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 已配置并启用 SAML。

关于此任务

在此任务中，您可以从控制器导出元数据（每个控制器一个文件）。IdP 需要此元数据来与控制器建立信任关系并处理身份验证请求。此文件包括 IdP 可用于发送请求的控制器域名或 IP 地址等信息。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **SAML** 选项卡。
3. 选择 **Export**。

   此时将打开 Export Service Provider Files 对话框。

4. 对于每个控制器，单击 导出 将元数据文件保存到本地系统。

   每个控制器的域名字段都是只读的。

   记下文件的存储位置。

5. 从本地系统中，找到您导出的 Service Provider 元数据文件。

   每个控制器都有一个 XML 格式的文件。

6. 从 IdP 服务器导入 Service Provider 元数据文件。您可以直接导入文件，也可以从中手动输入控制器信息。
7. 单击 **Close**。

使用访问令牌

在 **SANtricity System Manager** 中创建访问令牌

您可以创建访问令牌以通过 REST API 或命令行界面 (CLI) 进行身份验证，而不是用户名和密码。

令牌没有密码，因此您必须仔细管理它们。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Access Tokens** 选项卡。
3. 选择 **View/Edit Access Token Settings**。在对话框中，确保选中 **Enable access tokens** 复选框。单击 **Save** 关闭对话框。
4. 选择 **Create Access Token**。
5. 在对话框中，选择令牌有效的持续时间。

   令牌过期后，用户的身份验证尝试将失败。

6. 单击 **Create** 。
7. 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。

     请务必保存令牌文本。这是您在关闭对话框之前查看文本的唯一机会。

8. 单击 **Close**。
9. 按如下方式使用令牌：
   - **REST API**：要在 REST API 请求中使用令牌，请向请求添加 HTTP 标头。例如：
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI**：要在 CLI 中使用令牌，请在命令行上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`

       如果未指定用户名、密码或令牌，CLI 将在命令行上提示用户输入访问令牌值。

在 **SANtricity System Manager** 中编辑访问令牌设置

您可以编辑访问令牌的设置，其中包括到期时间和创建新令牌的功能。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Access Tokens** 选项卡。
3. 选择 **View/Edit Access Token Settings**。
4. 在该对话框中，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。

当您取消选择 启用访问令牌 设置时，它会阻止令牌创建和令牌身份验证。如果稍后重新启用此设置，则可以重复使用未到期的令牌。如果要永久吊销所有现有令牌，请参阅 "撤销访问令牌"。

5. 单击 **Save**。

在 **SANtricity System Manager** 中撤销访问令牌

如果您确定令牌已被泄露，或者您希望对用于签名和验证访问令牌的加密密钥执行手动密钥轮换，则可以吊销所有访问令牌。

此操作重新生成用于签名令牌的密钥。密钥重置后，所有 已颁发的令牌将立即失效。由于存储阵列不跟踪令牌，因此无法吊销单个令牌。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Access Tokens** 选项卡。
3. 选择 **Revoke All Access Tokens**。
4. 在对话框中，单击 **Yes**。

撤销所有令牌后，您可以创建新令牌并立即使用它们。

管理 syslog

在 **SANtricity System Manager** 中查看审核日志活动

通过查看审核日志，具有 Security Admin 权限的用户可以监视用户操作、身份验证失败、无效登录尝试和用户会话生存期。

开始之前

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Audit Log** 选项卡。

   审核日志活动以表格格式显示，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（格林威治标准时间）。
   - **Username** — 与事件关联的用户名。对于存储阵列上的所有未经身份验证的操作，"N/A" 将显示为用户名。未经身份验证的操作可能由内部代理或某些其他机制触发。
   - 状态代码 — 操作的 HTTP 状态代码（200、400 等）和与事件关联的描述性文本。
   - 访问的 **URL** — 完整 URL（包括主机）和查询字符串。
   - **Client IP Address** — 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 Services 或 Support Shell。

◦ 描述 — 有关事件的其他信息（如适用）。

3. 使用 Audit Log 页面上的选择来查看和管理事件。

选择详细信息

选择	说明
显示来自…的事件	限制按日期范围显示的事件（过去 24 小时、过去 7 天、过去 30 天或自定义日期范围）。
筛选器	限制字段中输入的字符所显示的事件。对于完全匹配的单词，请使用引号(")，输入 `OR`可返回一个或多个单词，输入破折号(--)可省略单词。
刷新	选择 **Refresh** 以将页面更新为最新事件。
查看/编辑设置	选择 **View/Edit Settings** 以打开一个对话框，该对话框允许您指定要记录的完整日志策略和操作级别。
删除事件	选择 **Delete** 以打开一个对话框，用于从页面中删除旧事件。
显示/隐藏列	单击 **Show/Hide** 列图标 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）。 • **CLI** 命令已执行 — 为 Secure CLI 请求执行的 CLI 命令（语法）。 • **CLI** 返回状态 — CLI 状态代码或对来自客户端的输入文件的请求。 • **SYMbol** 过程 — 执行的 SYMbol 过程。 • **SSH** 事件类型 — Secure Shell (SSH) 事件类型，例如登录、注销和 login_fail。 • **SSH** 会话 **PID** — SSH 会话的进程 ID 编号。 • **SSH** 会话持续时间（秒） — 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。 • **Authentication ID** — 经过身份验证的会话的 ID。
切换列筛选器	单击 **Toggle** 图标 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。
撤消更改	单击 **Undo** 图标 将表返回到默认配置。
导出	单击 **Export** 将表格数据保存为逗号分隔值 (CSV) 文件。

在 **SANtricity System Manager** 中定义审核日志策略

您可以更改覆盖策略和记录在审核日志中的事件类型。

开始之前

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 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和用于记录事件类型的策略。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Audit Log** 选项卡。
3. 选择 **View/Edit Settings**。

   此时将打开审核日志设置对话框。

4. 更改覆盖策略或记录的事件类型。

   字段详细信息

设置	说明
覆盖策略	确定在达到最大容量时覆盖旧事件的策略： • 允许在审核日志已满时覆盖审核日志中最旧的事件 — 在审核日志达到 50,000 条记录时覆盖旧事件。 • 要求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。 如果禁用覆盖策略并且审核日志条目达到最大限制，则拒绝没有 Security Admin 权限的用户访问 System Manager。若要将系统访问权限还原到没有 Security Admin 权限的用户，分配给 Security Admin 角色的用户必须删除旧事件记录。 如果为存档审核日志配置了 syslog 服务器，则覆盖策略不适用。
要记录的操作级别	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。

5. 单击 **Save**。

从 **SANtricity System Manager** 中删除审核日志中的事件

您可以清除旧事件的审核日志，这使得对事件的搜索更易于管理。删除时，您可以选择将旧事件保存为 CSV（逗号分隔值）文件。

开始之前

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Audit Log** 选项卡。
3. 选择 **Delete**。

   此时将打开删除审核日志对话框。
4. 选择或输入要删除的最早事件数。
5. 如果要将已删除的事件导出到 CSV 文件（推荐），请选中此复选框。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，如果不想将事件保存到 CSV 文件，请单击该复选框以取消选中该复选框。
6. 单击 **Delete**。

   此时将打开一个确认对话框。
7. 在字段中键入 `delete`，然后单击*删除*。

   最早的事件将从 Audit Log 页面中删除。

在 **SANtricity System Manager** 中为审核日志配置 **syslog** 服务器

如果要将审核日志存档到外部 syslog 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，审核日志将自动保存到 syslog 服务器。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- syslog 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的域名、IPv4 地址或 IPv6 地址。
- 如果您的服务器使用安全协议（例如 TLS），则必须在本地系统上提供证书颁发机构 (CA) 证书。CA 证书用于识别网站所有者，以确保服务器和客户端之间的安全连接。

步骤

1. 选择菜单：Settings[Access Management]。
2. 在 Audit Log（审计日志）选项卡中，选择 **Configure Syslog Servers**。

   此时将打开配置 Syslog 服务器对话框。
3. 单击 **Add**。

   此时将打开添加 Syslog 服务器对话框。

4. 输入服务器的信息，然后单击 **Add**。
   - 服务器地址 — 输入完全限定的域名、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 协议但尚未上传已签名的 CA 证书，请单击*浏览*以上传证书文件。没有受信任的证书，审核日志不会存档到 syslog 服务器。

     如果证书稍后变得无效，则 TLS 握手将失败。因此，将错误消息发布到审核日志，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：Settings[Audit Log > Configure Syslog Servers > Test All]。

   - **Port** — 输入 syslog 接收器的端口号。单击 **Add** 后，Configure Syslog Servers 对话框打开，并在页面上显示您配置的 syslog 服务器。
5. 要测试服务器与存储阵列的连接，请选择 **Test All**。

结果

配置后，所有新的审核日志都将发送到 syslog 服务器。不会传输以前的日志。要进一步配置警报的 syslog 设置，请参见 "为警报配置 syslog 服务器"。

```
NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.
```

在 **SANtricity System Manager** 中编辑审核日志记录的系统日志服务器设置

您可以更改用于存档审核日志的 syslog 服务器的设置，还可以上传服务器的新证书颁发机构 (CA) 证书。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- syslog 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的域名、IPv4 地址或 IPv6 地址。
- 如果要上传新的 CA 证书，则证书必须在本地系统上可用。

步骤

1. 选择菜单：Settings[Access Management]。
2. 在 Audit Log（审计日志）选项卡中，选择 **Configure Syslog Servers**。

   配置的 syslog 服务器显示在页面上。

3. 要编辑服务器信息，请选择服务器名称右侧的 **Edit**（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 syslog 接收器的端口号。
4. 如果您将协议更改为安全 TLS 协议（从 UDP 或 TCP），请单击*导入受信任的证书*以上传 CA 证书。

5. 要测试与存储阵列的新连接，请选择 **Test All**。

结果

配置完成后，所有新的审核日志都将发送到 syslog 服务器。不会传输以前的日志。

SANtricity System Manager 用户访问管理常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

为什么我无法登录？

如果在尝试登录到 SANtricity System Manager 时收到错误，请查看这些可能的原因。

由于以下原因之一，可能会发生到 System Manager 的登录错误：

- 您输入了错误的用户名或密码。
- 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。
- 您多次尝试登录失败，这触发了锁定模式。请等待 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 Access Management 并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。

用于镜像任务的远程存储阵列的登录错误可能出于以下原因之一：

- 您输入的密码不正确。
- 您多次尝试登录失败，这触发了锁定模式。请等待 10 分钟后重新登录。
- 已达到控制器上使用的客户端连接数上限。检查是否有多个用户或客户端。

在添加目录服务器之前，我需要知道什么？

在 Access Management 中添加目录服务器之前，请确保满足下列要求。

- 必须在您的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，请查看以下指南。

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：

- **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。
- 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。

- **Support admin** — 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。
- **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

目录服务

如果使用 LDAP（轻型目录访问协议）服务器和目录服务，请确保：

- 管理员在目录服务中定义了用户组。
- 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是正则表达式模式的一部分，则必须使用反斜杠(`\`转义：

```
\.[]{}()<>*+-=!?^$|
```

- 所有用户（包括管理员）都需要 Monitor 角色。如果没有 Monitor 角色，System Manager 将无法为任何用户正常运行。

SAML

如果您使用存储阵列中嵌入的 Security Assertion Markup Language (SAML) 功能，请确保：

- 身份提供程序 (IdP) 管理员在 IdP 系统中配置了用户属性和组成员身份。
- 您知道组成员身份名称。
- 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是正则表达式模式的一部分，则必须使用反斜杠 (\ 转义它们：

```
\.[]{}()<>*+-=!?^$|
```

- 所有用户（包括管理员）都需要 Monitor 角色。如果没有 Monitor 角色，System Manager 将无法为任何用户正常运行。

哪些外部管理工具可能会受到此变更的影响?

当您在 SANtricity System Manager 中进行某些更改时（例如切换管理接口或使用 SAML 作为身份验证方法），某些外部工具和功能可能会被限制使用。

管理界面

除非启用了"旧版管理界面"设置，否则直接与旧版管理界面 (SYMbol) 进行通信的工具（例如 SANtricity SMI-S Provider 或 OnCommand Insight (OCI)）将不起作用。此外，如果禁用此设置，则无法使用旧版 CLI 命令或执行镜像操作。

有关详细信息，请与技术支持联系。

SAML 身份验证

启用 SAML 后，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)
- 软件开发工具包 (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，请与技术支持联系。

在配置和启用 **SAML** 之前，我需要了解什么？

在配置和启用安全断言标记语言 (SAML) 身份验证功能之前，请确保满足下列要求并了解 SAML 限制。

要求

在开始之前，请确保：

- 在网络中配置了标识提供程序 (IdP)。IdP 是用于向用户请求凭据并确定用户是否成功通过身份验证的外部系统。您的安全团队负责维护 IdP。
- IdP 管理员在 IdP 系统中配置了用户属性和组。
- IdP 管理员已确保 IdP 支持在身份验证时返回名称 ID 的功能。
- 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 元数据文件是从 IdP 系统下载的，可在用于访问 System Manager 的本地系统上使用。
- 您知道存储阵列中每个控制器的 IP 地址或域名。

限制

除了上述要求之外，请务必了解以下限制：

- 启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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。我们建议您在最终配置步骤中启用 SAML 之前测试 SSO 登录。（系统在启用 SAML 之前还会执行 SSO 登录测试。）
- 如果以后禁用 SAML，系统会自动恢复以前的配置（本地用户角色和/或目录服务）。
- 如果当前为用户身份验证配置了 Directory Services，则 SAML 将覆盖该配置。
- 配置 SAML 时，以下客户端无法访问存储阵列资源：
  - 企业管理窗口 (EMW)
  - 命令行界面 (CLI)
  - 软件开发工具包 (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

审计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 — 来自 System Manager 中的用户操作，涉及对系统的更改，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。

在配置 **syslog** 服务器之前，我需要知道什么？

您可以将审核日志存档到外部 syslog 服务器上。

在配置 syslog 服务器之前，请记住以下指导原则。

- 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的域名、IPv4 地址或 IPv6 地址。
- 如果您的服务器使用安全协议（例如 TLS），则必须在本地系统上提供证书颁发机构 (CA) 证书。CA 证书用于识别网站所有者，以确保服务器和客户端之间的安全连接。
- 配置完成后，所有新的审核日志都将发送到 syslog 服务器。不会传输以前的日志。
- 覆盖策略设置（可从 查看/编辑设置 获得）不影响使用 syslog 服务器配置管理日志的方式。
- 审核日志遵循 RFC 5424 消息格式。

syslog 服务器不再接收审核日志。我该怎么办？

如果使用 TLS 协议配置了 syslog 服务器，则如果证书因任何原因无效，服务器将无法接收消息。有关无效证书的错误消息被发布到审核日志中。

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：设置[审核日志 > 配置 Syslog 服务器 > 全部测试]。

证书

了解 SANtricity System Manager 中的证书

您可以使用 SANtricity System Manager 创建证书签名请求 (CSR)、导入证书和管理现有证书。

什么是证书？

Certificates 是用于识别网站和服务器等在线实体的数字文件，用于在互联网上进行安全通信。有两种类型的证书：*signed certificate* 由证书颁发机构 (CA) 进行验证，*self-signed certificate* 由实体的所有者而不是第三方进行验证。

了解详情：

- "证书的工作原理"
- "证书术语"

如何配置已签名的证书?

您可以从 System Manager 或外部使用私钥和公钥对生成签名请求。签名请求被发送到 CA 以生成证书文件。CA 返回证书文件后，您可以使用 System Manager 导入它们。

了解详情：

- "对控制器使用 CA 签名的证书"
- "使用 CA 签名的证书对密钥管理服务器进行身份验证"

相关信息

详细了解与证书相关的任务：

- "查看导入的证书信息"
- "启用证书吊销检查"

概念

证书在 **SANtricity System Manager** 中的工作原理

证书是数字文件，用于识别在线实体（如网站和服务器），以便在互联网上进行安全通信。

证书确保 Web 通信仅在指定的服务器和客户端之间以加密形式私下传输且不被更改。使用 System Manager，可以管理主机管理系统上的浏览器（作为客户端）和存储系统中的控制器（作为服务器）之间的证书。

证书可以由受信任的颁发机构签名，也可以是自签名的。"签名"仅仅意味着有人验证了所有者的身份，并确定他们的设备可以被信任。存储阵列在每个控制器上都附带自动生成的自签名证书。您可以继续使用自签名证书，也可以获取 CA 签名证书，以便在控制器和主机系统之间建立更安全的连接。

> 虽然 CA 签名的证书可以提供更好的安全保护（例如，防止中间人攻击），但如果您拥有大型网络，它们也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，而不是在生产环境中。

已签名证书

签名的证书由证书颁发机构 (CA) 进行验证，CA 是受信任的第三方组织。签名证书包括有关实体所有者（通常是服务器或网站）、证书颁发日期和到期日期、实体的有效域以及由字母和数字组成的数字签名的详细信息。

当您打开浏览器并输入网址时，系统会在后台执行证书检查过程，以确定您连接的网站是否包含有效的 CA 签名证书。通常，使用签名证书保护的站点在地址中包含挂锁图标和 https 标识。如果您尝试连接到不包含 CA 签名证书的网站，浏览器将显示该网站不安全的警告。

CA 在申请过程中会采取步骤验证您的身份。他们可能会向您注册的公司发送电子邮件，验证您的公司地址，并执行 HTTP 或 DNS 验证。申请流程完成后，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：

- **Root** — 层次结构的顶端是根证书，其中包含用于对其他证书进行签名的私钥。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。

- 中级 — 从根分支出来的是中级证书。CA 颁发一个或多个中级证书，以充当受保护的根证书和服务器证书之间的中间人。
- 服务器 — 链条底部是服务器证书，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单独的服务器证书。

自签名证书

存储阵列中的每个控制器都包含一个预安装的自签名证书。自签名证书类似于 CA 签名的证书，但它由实体的所有者而不是第三方进行验证。与 CA 签名证书一样，自签名证书包含自己的私钥，并确保数据经过加密并通过服务器和客户端之间的 HTTPS 连接发送。但是，自签名证书不使用与 CA 签名证书相同的信任链。

浏览器不"信任"自签名证书。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的链接，以便继续访问网站；通过这样做，您基本上接受了自签名证书。

用于密钥管理服务器的证书

如果使用带有 Drive Security 功能的外部密钥管理服务器，还可以管理该服务器与控制器之间的身份验证证书。

了解 **SANtricity** 软件中的证书术语

以下术语适用于证书管理。

术语	说明
CA	证书颁发机构 (CA) 是颁发电子文档（称为数字证书）以实现 Internet 安全的受信任实体。这些证书可以识别网站所有者，从而实现客户端和服务器之间的安全连接。
CSR	证书签名请求 (CSR) 是从申请人发送到证书颁发机构 (CA) 的消息。CSR 验证 CA 颁发证书所需的信息。
证书	出于安全目的，证书可识别站点的所有者，从而防止攻击者模拟站点。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）的受信任实体的身份。
证书链	为证书添加安全层的文件层次结构。通常，链包括层次结构顶端的一个根证书、一个或多个中间证书以及标识实体的服务器证书。
客户端证书	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。
中间证书	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，以充当受保护的根证书和服务器证书之间的中间人。
密钥管理服务器证书	对于安全密钥管理，密钥管理服务器证书会验证服务器，因此存储阵列可以信任其 IP 地址。
密钥库	密钥库是主机管理系统上的存储库，其中包含私钥以及相应的公钥和证书。这些密钥和证书标识您自己的实体，例如控制器。

术语	说明
OCSP 服务器	联机证书状态协议 (OCSP) 服务器确定证书颁发机构 (CA) 是否在计划到期日期之前吊销了任何证书，然后在证书被吊销时阻止用户访问服务器。
根证书	根证书位于证书链中层次结构的顶端，并包含用于对其他证书进行签名的私钥。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。
已签名证书	由证书颁发机构 (CA) 验证的证书。此数据文件包含一个私钥，并确保通过 HTTPS 连接在服务器和客户端之间以加密形式发送数据。此外，签名证书包括有关实体所有者（通常是服务器或网站）的详细信息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中。也称为"CA 签名证书"或"管理证书"。
自签名证书	自签名证书由实体的所有者验证。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。自签名证书不使用与 CA 签名证书相同的信任链，因此最常用于测试环境。也称为"预安装"证书。
服务器证书	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单独的服务器证书。

使用证书

在 **SANtricity System Manager** 中为控制器使用 **CA** 签名证书

您可以获取 CA 签名的证书，以便在控制器和用于访问 SANtricity System Manager 的浏览器之间进行安全通信。

开始之前

- 必须使用包含 Security admin 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 签名的证书是一个三步过程。

步骤 **1**：完成控制器的 **CSR**

您必须首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 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，则生成一个 CSR 文件，如果存储阵列具有两个控制器，则生成两个 CSR 文件。

或者，您可以使用 OpenSSL 等工具生成 CSR 文件，并跳至 步骤 2：提交 CSR 文件。

步骤

1. 选择菜单：Settings[Certificates]。
2. 从阵列管理选项卡中，选择 **Complete CSR**。

   如果您看到提示您接受第二个控制器的自签名证书的对话框，请单击 **Accept Self-Signed Certificate** 以继续。

3. 输入以下信息，然后单击 **Next**：
   - 组织 — 贵公司或组织的完整法定名称。包括后缀，例如 Inc. 或 Corp.。
   - 组织单位（可选） — 处理证书的组织部门。
   - 城市/地区 — 您的存储阵列或业务所在的城市。
   - 州/地区（可选） — 您的存储阵列或业务所在的州或地区。
   - 国家/地区 **ISO** 代码 — 您所在国家/地区的两位数 ISO（International Organization for Standardization）代码，例如 US。

   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。除非您确定预先填充的值不正确，否则请勿更改。例如，如果您尚未完成 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。

4. 验证或输入有关存储阵列中控制器 A 的以下信息：
   - **Controller A common name** — 默认显示控制器 A 的 IP 地址或 DNS 名称。请确保此地址正确；它必须与您在浏览器中访问 System Manager 时输入的内容完全匹配。DNS 名称不能以通配符开头。
   - **Controller A** 备用 **IP** 地址 — 如果公用名称是 IP 地址，您可以选择输入 controller A 的任何其他 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 — 如果公用名称是 DNS 名称，请输入控制器 A 的任何其他 DNS 名称。对于多个条目，请使用逗号分隔格式。如果没有其他 DNS 名称，但您在第一个字段中输入了 DNS 名称，请将该名称复制到此处。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*完成*按钮可用。

     如果存储阵列有两个控制器，则 **Next** 按钮可用。

   最初创建 CSR 请求时，请勿单击 跳过此步骤 链接。此链接在错误恢复情况下提供。在极少数情况下，CSR 请求可能会在一个控制器上失败，但不会在另一个控制器上失败。此链接允许您跳过在控制器 A 上创建 CSR 请求的步骤（如果已定义），并继续下一步在控制器 B 上重新创建 CSR 请求。

5. 如果只有一个控制器，请单击 **Finish**。如果有两个控制器，请单击 **Next** 输入控制器 B 的信息（同上），然后单击 **Finish**。

   对于单个控制器，将一个 CSR 文件下载到您的本地系统。对于双控制器，下载两个 CSR 文件。下载的文件夹位置取决于您的浏览器。

6. 转至 步骤 2：提交 CSR 文件。

步骤 **2**：提交 **CSR** 文件

创建证书签名请求 (CSR) 文件后，将文件发送到证书颁发机构 (CA)。E-Series 系统要求签名证书采用 PEM 格

式 (Base64 ASCII 编码)，其中包括以下文件类型：.pem、.crt、.cer 或 .key。

步骤

1. 找到下载的 CSR 文件。
2. 将 CSR 文件提交给 CA（例如，Verisign 或 DigiCert），并以 PEM 格式请求已签名的证书。

> *向 CA 提交 CSR 文件后，请勿重新生成其他 CSR 文件。*每当您生成 CSR 时，系统都会创建私钥和公钥对。公钥是 CSR 的一部分，而私钥则保存在系统的密钥库中。当您收到签名的证书并导入它们时，系统将确保私钥和公钥都是原始对。如果密钥不匹配，则签名的证书将不起作用，您必须向 CA 请求新证书。

3. 当 CA 返回已签名的证书时，请转到 步骤 3：导入控制器的签名证书。

步骤 **3**：导入控制器的签名证书

收到来自证书颁发机构 (CA) 的签名证书后，导入控制器的文件。

开始之前

- CA 返回了签名的证书文件。这些文件包括根证书、一个或多个中间证书和服务器证书。
- 如果 CA 提供了一个链接的证书文件（例如 .p7b 文件），则必须将链接的文件解压缩为单个文件：根证书、一个或多个中间证书以及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 Base-64 编码。导出完成后，将显示链中每个证书文件的 CER 文件。
- 已将证书文件复制到访问 System Manager 的主机系统。

步骤

1. 选择菜单：Settings[Certificates]
2. 从 Array Management 选项卡中，选择 **Import**。

   此时会打开一个对话框以导入证书文件。

3. 单击 浏览 按钮，首先选择根证书文件和中间证书文件，然后为控制器选择每个服务器证书。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。如果您从外部工具生成了 CSR，则还必须导入与 CSR 一起创建的私钥文件。

   文件名显示在对话框中。

4. 单击 **Import**。

   文件已上传并验证。

结果

会话会自动终止。要使此证书生效，必须重新登录。当您再次登录时，新的 CA 签名的证书将用于您的会话。

在 **SANtricity System Manager** 中重置管理证书

您可以将控制器上的证书从使用 CA 签名的证书还原回出厂设置的自签名证书。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。
- 必须先导入 CA 签名的证书。

关于此任务

Reset 函数从每个控制器中删除当前 CA 签名的证书文件。然后，控制器将恢复使用自签名证书。

步骤

1. 选择菜单：Settings[Certificates]。
2. 从 Array Management 选项卡中，选择 **Reset**。

   此时将打开确认重置管理证书对话框。

3. 在字段中键入 `reset`，然后单击*重置*。

   刷新浏览器后，浏览器可能会阻止对目标站点的访问，并报告该站点正在使用 HTTP Strict Transport Security。当您切换回自签名证书时会出现这种情况。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

控制器恢复使用自签名证书。因此，系统会提示用户手动接受其会话的自签名证书。

在 **SANtricity System Manager** 中查看导入的证书信息

从"证书"页面，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

必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。

步骤

1. 选择菜单：Settings[Certificates]。
2. 选择其中一个选项卡以查看有关证书的信息。

选项卡	说明
阵列管理	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。
值得信赖	查看有关为控制器导入的所有其他类型证书的信息。使用 **Show certificates that are…** 下的筛选字段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，当控制器充当客户端（而不是服务器）时，可以包括受信任的证书、LDAPS 证书和 Identity Federation 证书。 • 预安装 — 存储阵列随附的自签名证书。

选项卡	说明
密钥管理	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。

在 **SANtricity System Manager** 中充当客户端时为控制器导入证书

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"选项卡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

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。
- 证书文件已安装在本地系统上。

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"选项卡导入证书。

步骤

1. 选择菜单：Settings[Certificates]。
2. 在"受信任"选项卡中，选择 导入。

   此时将打开一个对话框，用于导入受信任的证书文件。

3. 单击 **Browse** 为控制器选择证书文件。

   文件名显示在对话框中。

4. 单击 **Import**。

结果

文件已上传并验证。

在 **SANtricity System Manager** 中启用证书吊销检查

您可以启用已吊销证书的自动检查，以便 Online Certificate Status Protocol (OCSP) 服务器阻止用户进行非安全连接。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。
- 两个控制器上都配置了 DNS 服务器，这使得 OCSP 服务器可以使用完全限定的域名。此任务可从硬件页面获得。
- 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

在 CA 颁发证书不当或私钥泄露的情况下，自动吊销检查非常有用。

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 服务器确定 CA 是否在其计划到期日期之前吊销了任何证书，然后如果证书被吊销，则阻止用户访问站点。

步骤

1. 选择菜单：Settings[Certificates]。
2. 选择 **Trusted** 选项卡。

   您还可以从 **Key Management** 选项卡启用吊销检查。

3. 单击 **Uncommon Tasks**，然后从下拉菜单中选择 **Enable Revocation Checking**。
4. 选择 **I want to enable revocation checking**，以便在复选框中显示复选标记，并在对话框中显示其他字段。
5. 在 **OCSP responder address** 字段中，您可以选择输入 OCSP responder 服务器的 URL。如果您不输入地址，系统将使用证书文件中 OCSP 服务器的 URL。
6. 单击 **Test Address** 以确保系统可以打开与指定 URL 的连接。
7. 单击 **Save**。

结果

如果存储阵列尝试连接到具有已吊销证书的服务器，则连接将被拒绝并记录事件。

在 **SANtricity System Manager** 中删除受信任的证书

您可以删除以前从 Trusted 选项卡导入的用户安装的证书。

开始之前

- 必须使用包含 Security admin 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的证书，则必须先导入更新的证书，然后才能删除旧证书。

如果在导入替换证书之前删除用于对控制器和其他服务器（如 LDAP 服务器）进行身份验证的证书，则可能会失去对系统的访问权限。

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

1. 选择菜单：Settings[Certificates]。
2. 选择 **Trusted** 选项卡。

   下表显示了存储阵列的可信证书。

3. 从表中选择要删除的证书。
4. 单击菜单：Uncommon Tasks[Delete]。

   将打开确认删除受信任证书对话框。

5. 在字段中键入 `delete`，然后单击*删除*。

使用 **CA** 签名的证书在 **SANtricity System Manager** 中与密钥管理服务器进行身份验证

为了在密钥管理服务器和存储阵列控制器之间进行安全通信，必须配置相应的证书集。

开始之前

必须使用包含 Security admin 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

控制器和密钥管理服务器之间的身份验证是一个两步过程。

步骤 **1**：完成并提交 **CSR** 以通过密钥管理服务器进行身份验证

您必须首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) 请求签名的客户端证书。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。客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 Key Management Interoperability Protocol (KMIP) 请求。

通过私钥和公钥对从外部生成的 CSR 文件可以通过"创建外部安全密钥"对话框导入。有关导入外部生成的 CSR 文件的更多信息，请参见 "步骤 2：导入密钥管理服务器的证书"。

步骤

1. 选择菜单：Settings[Certificates]。
2. 从密钥管理选项卡中，选择 **Complete CSR**。
3. 输入以下信息：
   - 通用名称 — 标识客户端的名称。通常的做法是将通用名称中的内容与 KMS 服务器对客户端证书命名约定的要求相匹配。通用名称通常有助于 KMS 在握手过程中出示证书时识别客户端的证书。
   - 组织 — 贵公司或组织的完整法定名称。包括后缀，例如 Inc. 或 Corp.。
   - 组织单位（可选） — 处理证书的组织部门。
   - 城市/地区 — 您的组织所在的城市或地区。
   - 州/地区（可选） — 您的组织所在的州或地区。
   - 国家/地区 **ISO** 代码 — 两位数的 ISO（国际标准化组织）代码，例如 US，即您的组织所在的位置。
4. 单击 **Download**。

   CSR 文件已保存到您的本地系统。

5. 从受密钥管理服务器信任的 CA 请求签名的客户端证书。

   密钥管理服务器通常具有直接生成签名证书的设施，因为它作为自己的 CA 运行。

6. 拥有客户端证书时，请转到 步骤 2：导入密钥管理服务器的证书。

步骤 **2**：导入密钥管理服务器的证书

下一步是导入证书，以便在存储阵列和密钥管理服务器之间进行身份验证。有两种类型的证书：客户端证书验证

存储阵列的控制器，而密钥管理服务器证书验证服务器。必须同时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

- 您有一个已签名的客户端证书文件（请参阅 步骤 1：完成并提交 CSR 以通过密钥管理服务器进行身份验证），并且您已将该文件复制到访问 System Manager 的主机。客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 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您正在访问 System Manager 的主机。密钥管理服务器证书验证密钥管理服务器，因此存储阵列可以信任其 IP 地址。您可以为密钥管理服务器使用根证书、中间证书或服务器证书。

> 有关服务器证书的详细信息，请参阅密钥管理服务器的文档。

步骤

1. 选择菜单：Settings[Certificates]。
2. 从密钥管理选项卡中，选择 导入。

   此时将打开一个用于导入证书文件的对话框。

3. 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。

   文件名显示在对话框中。

4. 如果您使用私钥和公钥对在外部生成证书文件，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。

   文件名显示在对话框中。

5. 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。

   文件名显示在对话框中。

6. 单击 **Import**。

   文件已上传并验证。

在 **SANtricity System Manager** 中导出密钥管理服务器证书

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

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。
- 必须先导入证书。

步骤

1. 选择菜单：Settings[Certificates]。
2. 选择 **Key Management** 选项卡。

3. 从表中选择要导出的证书，然后单击 **Export**。

   此时将打开保存对话框。

4. 输入文件名并单击 保存。

SANtricity System Manager 的 CA 签名证书和自签名证书常见问题解答

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

为什么会出现"无法访问其他控制器"对话框？

执行与 CA 证书相关的某些操作（例如，导入证书）时，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（双工配置）的存储阵列中，如果 SANtricity System Manager 无法与第二个控制器通信，或者如果您的浏览器在操作中的某个点无法接受证书，则有时会出现此对话框。

如果打开此对话框，请单击 **Accept Self-Signed Certificate** 以继续。如果其他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。
- 访问第二个控制器 withSystem Manager，接受自签名证书，然后返回第一个控制器并继续。

如何知道需要将哪些证书上传到 **SANtricity System Manager** 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，从而使两个实体可以相互信任。

客户端证书验证存储阵列的控制器，以便密钥管理服务器可以信任其 Key Management Interoperability Protocol (KMIP) 请求。

要获取客户端证书，请使用 System Manager 完成存储阵列的 CSR。您还可以使用私钥和公钥对在外部生成 CSR。

然后，您可以将 CSR 上传到密钥管理服务器并从中生成客户端证书。获得客户端证书后，将该文件复制到访问 System Manager 的主机。

密钥管理服务器证书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正在访问 System Manager 的主机。

关于证书吊销检查，我需要了解哪些信息？

SANtricity System Manager 允许您通过使用在线证书状态协议 (OCSP) 服务器来检查吊销的证书，而不是上传证书吊销列表 (CRL)。

已吊销的证书不应再受信任。证书可能出于多种原因而被吊销；例如，如果 Certificate Authority (CA) 不正确地颁发了证书、私钥被泄露或被识别的实体不符合策略要求。

在 System Manager 中建立到 OCSP 服务器的连接后，存储阵列在连接到 AutoSupport 服务器、外部密钥管理服务器 (EKMS)、基于 SSL 的轻型目录访问协议 (LDAPS) 服务器或 Syslog 服务器时执行吊销检查。存储阵列尝试验证这些服务器的证书，以确保它们未被吊销。然后，服务器返回该证书的 "good"、"revoked" 或 "unknown" 值。如果证书被吊销或阵列无法联系 OCSP 服务器，则连接被拒绝。

在 System Manager 或命令行界面 (CLI) 中指定 OCSP 响应程序地址将覆盖在证书文件中找到的 OCSP 地址。

将为哪些类型的服务器启用吊销检查?

每当连接到 AutoSupport 服务器、外部密钥管理服务器 (EKMS)、基于 SSL 的轻型目录访问协议 (LDAPS) 服务器或 Syslog 服务器时，存储阵列都会执行吊销检查。

支持

在 **SANtricity System Manager** 中获取支持

通过"支持"页面可以访问技术支持资源。

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、查看事件日志和执行软件升级。

了解详情：

- "AutoSupport 功能概述"
- "事件日志概述"
- "升级中心概述"

如何联系技术支持?

在主页，单击菜单：支持[支持中心 > 支持资源选项卡]。技术支持联系信息列在界面右上角。

查看信息和诊断

在 **SANtricity System Manager** 中查看存储阵列的配置文件

存储阵列配置文件提供了存储阵列的所有组件和属性的描述。

关于此任务

您可以使用存储阵列配置文件作为恢复过程中的辅助功能，或作为存储阵列当前配置的概述。您可能需要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拷贝。如果配置发生更改，请创建存储阵列配置文件的新副本。

步骤

1. 选择菜单：Support[Support Center > Support Resources] 选项卡。
2. 向下滚动到 **Launch detailed storage array information**，然后选择 **Storage Array Profile**。

此报告会显示在您的屏幕上。

字段详细信息

板块	说明
存储阵列	显示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、驱动器盘架、驱动器、磁盘池、卷组、卷和热备盘驱动器的数量；允许的驱动器盘架、驱动器、固态硬盘 (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；有关功能的信息；有关固件版本的信息；有关机箱序列号的信息；AutoSupport 状态和 AutoSupport 计划信息；自动支持数据收集和计划支持数据收集的设置；存储阵列全球标识符 (WWID)；以及媒体扫描和缓存设置。
存储	显示存储阵列中所有存储设备的列表。根据您的存储阵列配置，Storage 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、卷状态、容量、RAID 级别、卷组或磁盘池、驱动器类型和其他详细信息。 • 缺少卷 — 显示存储阵列中当前具有缺少状态的所有卷的列表。列出的信息包括每个缺失卷的全球标识符 (WWID)。
复制服务	显示用于存储阵列的所有复制服务的列表。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： • **Volume Copies** — 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、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。 • 快照卷 — 显示存储阵列中所有快照卷的列表。 • 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。 • 保留容量 — 显示存储阵列中所有保留容量卷的列表。
主机分配	显示存储阵列中主机分配的列表。列出的信息包括卷名、逻辑单元号 (LUN)、控制器 ID、主机名或主机群集名以及卷状态。列出的其他信息包括拓扑定义和主机类型定义。

板块	说明
硬件	显示存储阵列中所有硬件的列表。根据您的存储阵列配置，Hardware 部分可能会显示这些子部分。 • **Controllers** — 显示存储阵列中所有控制器的列表，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。驱动器按机架 ID、抽屉 ID、插槽 ID 顺序列出。列出的信息包括每个驱动器的机架 ID、抽屉 ID、插槽 ID、状态、原始容量、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、热备盘覆盖信息和磨损寿命信息（仅适用于 SSD 驱动器）。磨损寿命信息包括已使用的耐久性百分比，即迄今为止写入 SSD 驱动器的数据量除以驱动器的总理论写入限制。 • 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、链接状态（如适用）、驱动器计数和累计错误计数。 • 机架 — 显示存储阵列中所有机架的信息。列出的信息包括驱动器类型和机架每个组件的状态信息。机架组件可能包括电池组、小型可插拔 (SFP) 收发器、电源风扇罐或输入/输出模块 (IOM) 罐。如果存储阵列使用安全密钥，"硬件"部分还会显示安全密钥标识符。
功能	显示已安装功能包的列表以及每个主机或主机群集允许的最大快照组数、快照（旧版）和卷数。功能部分中的信息还包括驱动器安全；即存储阵列是启用安全还是禁用安全。

3. 要搜索存储阵列配置文件，请在 **Find** 文本框中键入搜索词，然后单击 **Find** 。

   所有匹配的术语都会突出显示。要一次滚动浏览所有结果，请继续单击 **Find**。

4. 要保存存储阵列配置文件，请单击 **Save**。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `storage-array-profile.txt`。

在 **SANtricity System Manager** 中查看软件和固件清单

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

存储阵列由许多组件组成，其中可能包括控制器、驱动器、抽屉和输入/输出模块 (IOM)。这些组件中的每一个都包含固件。某些版本的固件依赖于其他版本的固件。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

1. 选择菜单：Support[Support Center > Support Resources] 选项卡。
2. 向下滚动到 **Launch detailed storage array information**，然后选择 **Software and Firmware Inventory**。

软件和固件清单报告将显示在屏幕上。

3. 要保存软件和固件清单，请单击 **Save** 。

   文件以文件名 `firmware-inventory.txt` 保存在浏览器的"下载"文件夹中。

4. 按照技术支持提供的说明将文件发送给他们。

收集诊断数据

在 **SANtricity System Manager** 中手动收集支持数据

您可以在单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，您也可以转到 **AutoSupport** 选项卡并选择 发送 **AutoSupport** 派单 来收集此数据。

一次只能运行一个集合操作。如果尝试启动其他操作，则会收到错误消息。

仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Collect Support Data**。
3. 单击 **Collect**。

   该文件保存在浏览器的"下载"文件夹中，名称为 `support-data.7z`。如果您的货架包含抽屉，则该货架的诊断数据将存档在名为 `tray-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

此任务描述如何保存 RAID 配置数据库的当前状态。此数据从控制器的 RPA 内存位置检索。

收集配置数据功能将保存与 CLI 命令相同的信息 `save storageArray dbmDatabase`。

只能在 Recovery Guru 操作或技术支持人员的指示下执行此任务。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Collect Configuration Data**。
3. 在对话框中，单击 **Collect**。

   文件 `configurationData-<arrayName>-<dateTime>.7z`保存在浏览器的"下载"文件夹中。

4. 请与技术支持联系，了解有关向其发送文件以及将数据加载回系统的详细信息。

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来解决问题。SANtricity System Manager 会自动保存这些文件。

开始之前

技术支持要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. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Retrieve Recovery Support Files**。

   对话框会列出存储阵列收集的所有恢复支持文件。要查找特定文件，您可以对任何列进行排序或在 **Filter** 框中键入字符。

3. 选择一个文件，然后单击 **Download**。

   文件保存在浏览器的下载文件夹中。

4. 如果需要保存其他文件，请重复上一步。
5. 单击 **Close**。
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

您可以从控制器检索跟踪缓冲区，并将文件发送到技术支持进行分析。

关于此任务

固件使用跟踪缓冲区来记录处理，特别是可能对调试有用的异常条件。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。

仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Retrieve Trace Buffers**。
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 Failed 或 Disabled，则禁用该复选框。

4. 单击 **Yes**。

   文件以文件名 `trace-buffers.7z` 保存在浏览器的"下载"文件夹中。

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 路径统计文件并将其发送到技术支持进行分析。

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使用率、CPU 使用率、网络延迟、I/O 延迟或其他问题引起的。I/O 路径统计信息在支持数据收集期间自动收集，或者您可以手动收集它们。此外，如果您已打开 AutoSupport，则会自动收集 I/O 路径统计信息并发送给技术支持人员。

在确认要收集 I/O 路径统计信息后，将重置 I/O 路径统计信息的计数器。即使您随后取消操作，计数器也会重置。当控制器重置（重新启动）时，计数器也会重置。

仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Collect I/O Path Statistics**。
3. 通过键入 `collect`确认您要执行此操作，然后单击 **Collect**。

   文件以文件名 `io-path-statistics.7z` 保存在浏览器的 Downloads 文件夹中。

4. 按照技术支持提供的说明将文件发送给他们。

在 **SANtricity System Manager** 中检索运行状况映像

您可以查看控制器的运行状况映像。运行状况映像是控制器处理器内存的原始数据转储，技术支持可以使用它来诊断控制器问题。

关于此任务

固件在检测到某些错误时会自动生成健康图像。生成运行状况映像后，发生错误的控制器将重新启动并在事件日志中记录事件。

如果已开启 AutoSupport，则会自动将运行状况图像发送给技术支持。如果尚未打开 AutoSupport，则需要联系技术支持以获取有关检索运行状况图像并将其发送给他们进行分析的说明。

仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Retrieve Health Image**。

   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 **Collect**。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `health-image.7z`。

4. 按照技术支持提供的说明将文件发送给他们。

采取恢复操作

在 **SANtricity System Manager** 中查看不可读扇区日志

您可以保存不可读扇区日志并将文件发送给技术支持进行分析。

关于此任务

不可读扇区日志包含由报告不可恢复媒体错误的驱动器引起的不可读扇区的详细记录。在正常 I/O 期间和修改操作（例如重建）期间检测到不可读扇区。当在存储阵列上检测到不可读扇区时，将显示存储阵列的"需要注意"警报。Recovery Guru 会区分哪些不可读扇区状况需要注意。不可读扇区中包含的任何数据都无法恢复，应被视为丢失。

无法读取的扇区日志可存储多达 1,000 个无法读取的扇区。当无法读取的扇区日志达到 1,000 个条目时，适用以下条件：

- 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 期间检测到的新的不可读扇区，I/O 会出现故障，并且不会记录任何条目。

这些操作包括在溢出之前本应成功的 RAID 5 写入和 RAID 6 写入。

可能丢失数据 — 从不可读扇区恢复是一个复杂的过程，可能涉及几种不同的方法。仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **View/Clear Unreadable Sectors**。

3. 要保存不可读扇区日志：

   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）或选择所有卷（选择表标题中的复选框）。

      要查找特定卷，您可以对任何列进行排序或在 **Filter** 框中键入字符。

   b. 单击 **Save**。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `unreadable-sectors.txt`。

4. 如果技术支持指示您清除不可读扇区日志，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）或选择所有卷（选择表标题中的复选框）。

   b. 单击 **Clear**，并确认要执行此操作。

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纠正措施从错误接线状态中恢复。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 重新启用驱动器端口，并确认要执行此操作。

   仅当存储阵列禁用了驱动器端口时，才会显示此选项。

   控制器重新启用检测到接线错误时禁用的所有 SAS 端口。

清除 **SANtricity** 软件中的恢复模式

恢复存储阵列配置后，使用清除恢复模式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以前的配置，则必须在清除恢复模式之前从备份还原配置。
- 您必须执行验证检查或咨询技术支持，以确保恢复成功。确定恢复成功后，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，或者配置数据库已损坏，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，从而让您有时间执行以下操作之一：

- 从控制器闪存设备中存储的自动备份中恢复配置。您必须联系技术支持才能执行此操作。
- 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通过命令行界面 (CLI) 执行。
- 从头开始重新配置存储阵列。

在恢复或重新定义存储阵列配置并验证一切正常后，您必须手动清除恢复模式。

清除恢复模式操作启动后无法取消。清除恢复模式可能需要很长时间。仅在技术支持人员指示时执行此操作。

步骤

1. 选择菜单：Support[Support Center > Diagnostics] 选项卡。
2. 选择 **Clear Recovery Mode**，并确认要执行此操作。

   仅当存储阵列处于恢复模式时才会显示此选项。

管理 AutoSupport

了解有关 E 系列 AutoSupport 的信息

AutoSupport 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。

技术支持以被动方式使用 AutoSupport 数据来加快客户问题的诊断和解决，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。调度可以立即发送或按计划发送（每日和每周）。

主要优势

AutoSupport 功能的一些主要优势包括：

- 加快案例解决时间
- 先进的监控，实现更快的事件管理
- 根据时间表自动报告，并自动报告关键事件
- 所选组件（如驱动器）的自动硬件更换请求
- 非侵入式警报，通知您出现问题并为技术支持提供信息以采取纠正措施
- 监控派遣中已知配置问题的 AutoSupport 分析工具

各个 AutoSupport 功能

该 AutoSupport 功能由三个单独的功能组成，您可以分别启用这些功能。

- 基本 **AutoSupport** — 允许您的存储阵列自动收集数据并将其发送给技术支持。
- **AutoSupport OnDemand** — 允许技术支持在需要解决问题时请求重新传输以前的 AutoSupport 派单。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器进行检查，以确定是否存在任何挂起的重传请求，并做出相应的响应。
- 远程诊断 — 允许技术支持在需要解决问题时请求新的最新 AutoSupport 派遣。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器签入，以确定是否存在任何挂起的新请求，并做出相应的响应。

AutoSupport 与收集支持数据之间的差异

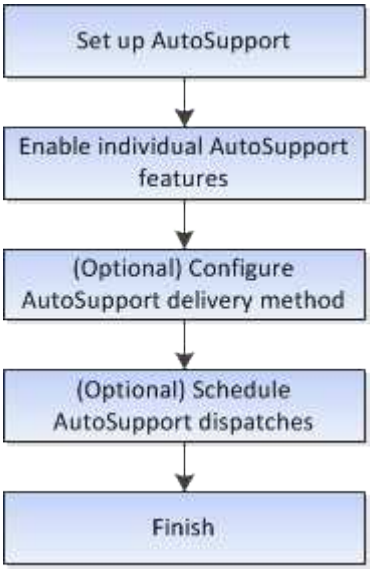
存储阵列中存在两种收集支持数据的方法：

- **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，因为数据是自动收集和发送的。可以主动使用 AutoSupport 数据来防止问题发生。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。出于这些原因，AutoSupport 功能是首选的数据收集方法。

在 **SANtricity System Manager** 中配置 **AutoSupport**

在 SANtricity System Manager 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 功能和单个 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，必须将 AutoSupport 传递方法设置为 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。启用 AutoSupport 功能可以大大加快问题确定和解决的速度，如果存储阵列上出现问题。

该 AutoSupport 功能由三个单独的功能组成，您可以分别启用这些功能。

- 基本 **AutoSupport** — 允许您的存储阵列自动收集数据并将其发送给技术支持。
- **AutoSupport OnDemand** — 允许技术支持在需要解决问题时请求重新传输以前的 AutoSupport 派单。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器进行检查，以确定是否存在任何挂起的重传请求，并做出相应的响应。
- 远程诊断 — 允许技术支持在需要解决问题时请求新的最新 AutoSupport 派遣。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器签入，以确定是否存在任何挂起的新请求，并做出相应的响应。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
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。

   这些特征相互依赖，如对话框中项目的缩进所示。例如，您必须先启用 AutoSupport OnDemand，然后才能启用远程诊断。

4. 单击 **Save**。

   如果禁用 AutoSupport，主页上将显示通知。您可以通过点击*忽略*来关闭通知。

在 **SANtricity System Manager** 中配置 **AutoSupport** 交付方法

AutoSupport 功能支持 HTTPS 和 SMTP 协议，用于将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 页面上查看是否已启用此功能。
- 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获得）。

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，必须将 AutoSupport 传递方法设置为 HTTPS。
- 电子邮件 — 允许您使用电子邮件服务器作为发送 AutoSupport 派单的传递方法。

> **HTTPS** 和电子邮件方法之间的差异。使用 SMTP 的电子邮件传递方法与 HTTPS 传递方法有一些重要区别。首先，电子邮件方法的调度大小限制为 5MB，这意味着某些 ASUP 数据集将不会被调度。其次，AutoSupport OnDemand 功能仅在 HTTPS 传递方法上可用。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 配置 **AutoSupport** 交付方式。

   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，然后为该交付方法选择参数。执行以下操作之一：
   - 如果选择了 HTTPS，请选择以下交付参数之一：
     - 直接 — 此交付参数是默认选择。选择此选项后，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。必须指定主机地址和端口号。但是，如果需要，只需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。PAC 文件允许系统自动选择适当的代理服务器，以建立与目标技术支持系统的连接。

◦ 如果选择"电子邮件"，请输入以下信息：

- 邮件服务器地址作为完全限定域名、IPv4 地址或 IPv6 地址。
- AutoSupport 调度电子邮件"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。
- 如果要加密邮件，请选择 **SMTPS** 或 **STARTTLS** 作为加密类型，然后选择加密邮件的端口号。否则，请选择 **None**。
- 如果需要，请输入用户名和密码，以便与传出发件人和邮件服务器进行身份验证。

4. 如果您的防火墙阻止了这些 ASUP 派单的传递，请将以下 URL 添加到白名单中：
`https://support.netapp.com/put/AsupPut/`
5. 单击 测试配置 以使用指定的交付参数测试与技术支持服务器的连接。如果您启用了 AutoSupport 按需功能，系统还将测试 AutoSupport OnDemand 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再次运行测试。如果测试继续失败，请联系技术支持。

6. 单击 **Save**。

在 **SANtricity System Manager** 中安排 **AutoSupport** 派发

SANtricity System Manager 会自动为 AutoSupport 派遣创建默认计划。如果您愿意，可以指定自己的时间表。

开始之前

必须启用 AutoSupport 功能。您可以在 AutoSupport 页面上查看是否已启用此功能。

关于此任务

- 每日时间 — 在您指定的时间范围内，每天收集和发送每日派单。System Manager 在范围中随机选择时间。所有时间均为协调世界时 (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。
- 每周一天 — 每周派单每周收集和发送一次。System Manager 从您指定的日期中随机选择一天。取消选择您不希望进行每周派单的任何日期。System Manager 从您允许的日期中随机选择一天。
- 每周时间 — 每周派单在您指定的时间范围内每周收集和发送一次。System Manager 在范围内随机选择时间。所有时间均为协调世界时 (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。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 **Schedule AutoSupport Dispatches**。

   此时将显示计划 AutoSupport 快件向导。

3. 按照向导中的步骤操作。

在 **SANtricity System Manager** 中发送 **AutoSupport** 派单

SANtricity System Manager 允许您向技术支持发送 AutoSupport 派单，而无需等待预定的派单。

开始之前

必须启用 AutoSupport 功能。您可以在 AutoSupport 页面上查看是否已启用此功能。

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，以便他们对问题进行故障排除。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 **Send AutoSupport Dispatch**。

   此时将显示"发送 AutoSupport 派单"对话框。

3. 选择 发送 以确认操作。

在 **SANtricity System Manager** 中查看 **AutoSupport** 状态

AutoSupport 页面显示当前是否已启用 AutoSupport 功能和各个 AutoSupport 功能。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 查看选项卡下方的页面右侧，了解基本 AutoSupport 功能是否已启用。
3. 将光标悬停在问号上，以查看是否已启用单个 AutoSupport 功能。

在 **AutoSupport System Manager** 中查看 **SANtricity** 日志

AutoSupport 日志提供有关 AutoSupport 派单交付过程中遇到的状态、派单历史记录和错误的信息。

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，它将被存档并创建一个新的日志文件。存档的日志文件名为 `ASUPMessages.n`，其中 *n* 是 1 到 9 之间的整数。如果存在多个日志文件，则可以选择查看最新日志或以前的日志。

- 当前日志 — 显示最新捕获事件的列表。
- 已存档日志 — 显示早期事件列表。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 查看 **AutoSupport** 日志。

   此时将显示一个对话框，其中列出当前 AutoSupport 日志。

3. 如果要查看以前的 AutoSupport 日志，请选择 已存档 单选按钮，然后从 选择 **AutoSupport** 日志 下拉列表中选择一个日志。

   仅当存储阵列上存在已存档日志时，才会显示 Archived 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 框中输入术语，然后单击 查找。

   再次单击 查找 以搜索该术语的其他匹配项。

在 **SANtricity System Manager** 中启用 **AutoSupport** 维护窗口

启用 AutoSupport 维护窗口以禁止在错误事件时自动创建票证。在正常操作模式下，如果出现问题，存储阵列使用 AutoSupport 打开支持案例。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 启用 **AutoSupport** 维护窗口。
3. 输入电子邮件地址以接收已处理维护窗口请求的确认。

   根据您的配置，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 **Add another email** 以打开其他字段。

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 **Yes**。

   在指定的持续时间窗口内，错误事件的 AutoSupport 自动票证创建功能被暂时禁止。

完成后

在 AutoSupport 服务器处理存储阵列的请求之前，维护窗口不会开始。请等待收到确认电子邮件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 维护窗口以允许在错误事件时自动创建票证。当 AutoSupport 维护窗口被禁用时，如果出现问题，存储阵列将使用 AutoSupport 打开支持案例。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 禁用 **AutoSupport** 维护窗口。
3. 输入电子邮件地址以接收已处理禁用维护窗口请求的确认。

   根据您的配置，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 **Add another email** 以打开其他字段。

4. 单击 **Yes**。

   已启用错误事件上的 AutoSupport 自动票证创建。

完成后

在 AutoSupport 服务器处理存储阵列的请求之前，维护窗口不会结束。请等到收到确认电子邮件后再继续。

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。

您可以将事件日志用作 Recovery Guru 的补充诊断工具，以跟踪存储阵列事件。当您尝试从存储阵列中的组件故障中恢复时，请始终首先参考 Recovery Guru。

事件类别

事件日志中的事件按不同状态进行分类。需要执行操作的事件具有以下状态：

- 严重
- 警告

以下事件仅供参考，无需立即采取行动：

- 信息

严重事件

关键事件表示存储阵列存在问题。如果立即解决关键事件，可能会防止数据访问丢失。

当发生关键事件时，它将记录在事件日志中。所有关键事件都将发送到 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。如果事件发生时货架 ID 未知，货架 ID 将列为"货架未知"。

当您收到关键事件时，请参阅 Recovery Guru 程序，了解关键事件的详细说明。完成 Recovery Guru 程序以更正关键事件。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. 选择菜单：Support[Event Log]。

   此时将显示事件日志页面。

页面详细信息

项目	说明
查看所有字段	在所有事件和仅关键事件和警告事件之间切换。
筛选字段	筛选事件。用于仅显示与特定组件、特定事件等相关的事件。
选择列图标。	允许您选择要查看的其他列。其他列可为您提供有关事件的其他信息。
复选框	允许您选择要保存的事件。表格标题中的复选框会选择所有事件。
日期/时间列	事件的日期和时间戳，根据控制器时钟。 事件日志最初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。在此情况下，相对于事件以及显示的日期和时间，一些感知到的不一致可能会出现在事件日志中。
优先级列	存在以下优先级值： • 严重 — 存储阵列存在问题。但是，如果您立即采取行动，您可能会防止失去对数据的访问权限。关键事件用于警报通知。所有关键事件都将发送到任何网络管理客户端（通过 SNMP 陷阱）或您配置的电子邮件收件人。 • 警告 — 发生错误，降低了存储阵列的性能和从另一个错误恢复的能力。 • 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，如驱动器或控制器，也可以是软件，如控制器固件。
组件位置列	组件在存储阵列中的物理位置。
说明列	对事件的描述。 示例 — `Drive write failure - retries exhausted`
Sequence Number 列	唯一标识存储阵列的特定日志条目的 64 位数字。此数字随着每个新事件日志条目增加一。要显示此信息，请单击*选择列*图标。
事件类型列	标识每种记录事件类型的 4 位数字。要显示此信息，请单击 **Select columns** 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 **Select columns** 图标。

项目	说明
事件类别列	• 故障 – 存储阵列中的组件出现故障；例如，驱动器故障或电池故障。 • 状态更改 – 存储阵列中已更改状态的元素；例如，卷转换为最佳状态，或控制器转换为离线状态。 • 内部 – 不需要用户操作的内部控制器操作；例如，控制器已完成一天的开始。 • 命令 – 已向存储阵列发出的命令；例如，已分配热备盘。 • 错误 – 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。 • 一般 – 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	记录事件的控制器名称。要显示此信息，请单击 选择列 图标。

2. 要从存储阵列中检索新事件，请单击 刷新。

   记录事件并在 Event Log 页面中显示可能需要几分钟的时间。

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 **Save**。

      此文件将以此名称保存在浏览器的 Downloads 文件夹中 `major-event-log-timestamp.log`。

4. 从事件日志中清除事件：

   事件日志存储大约 8,000 个事件，然后将事件替换为新事件。如果要保留事件，可以将其保存并从事件日志中清除。

   a. 首先，保存事件日志。
   b. 单击 **Clear All**，并确认要执行此操作。

管理升级

了解有关升级 **SANtricity** 软件的信息

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。

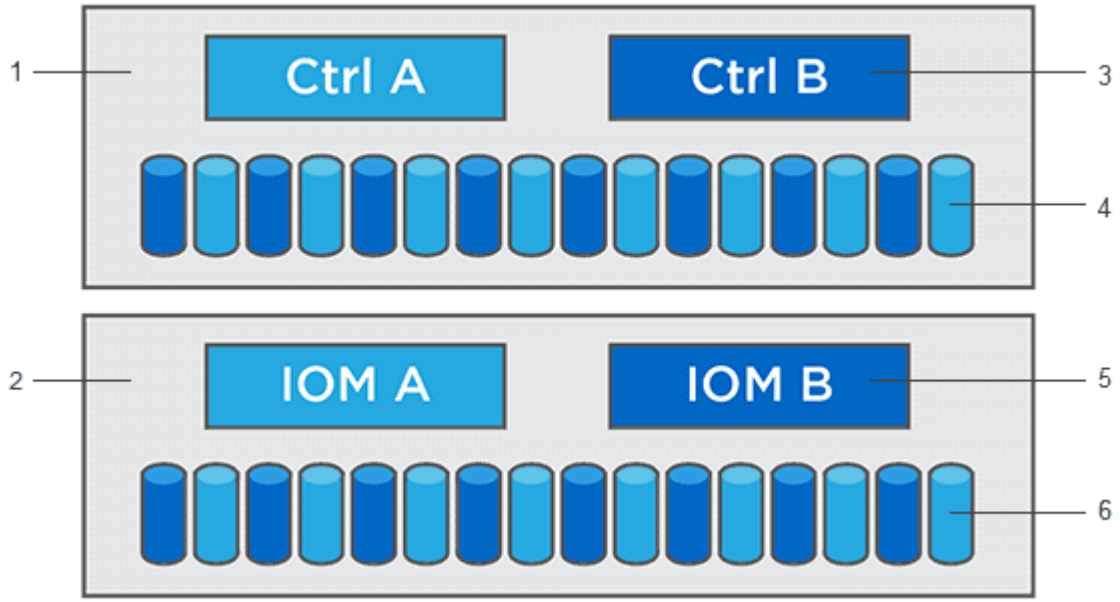
控制器升级概述

您可以升级存储阵列的软件和固件，以获取所有最新功能和错误修复。

OS 控制器升级中包含的组件

几个存储阵列组件包含您可能需要偶尔升级的软件或硬件。

- 管理软件 — System Manager 是管理存储阵列的软件。
- 控制器固件 — 控制器固件管理主机和卷之间的 I/O。
- 控制器 **NVSRAM** — 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) 固件管理控制器和驱动器架之间的连接。它还监控组件的状态。
- **Supervisor** 软件 — Supervisor 软件是运行该软件的控制器上的虚拟机。



[1] 控制器盘架；[2] 驱动器盘架；[3] 软件、控制器固件、控制器 NVSRAM、主管软件；[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"对话框中查看当前的软件和固件版本。转到菜单：Support[Upgrade Center]，然后单击 **Software and Firmware Inventory** 的链接。

作为升级过程的一部分，主机的多路径/故障转移驱动程序和/或 HBA 驱动程序也可能需要升级，以便主机可以与控制器正确交互。要确定是否属于这种情况，请参见 "NetApp Interoperability Matrix Tool"。

何时停止 I/O

如果您的存储阵列包含两个控制器，并且您安装了多路径驱动程序，则在升级过程中，存储阵列可以继续处理 I/O。在升级期间，控制器 A 将其所有卷故障转移到控制器 B，升级，取回其卷和控制器 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。以下情况可能会阻止升级：

- 分配的驱动器出现故障

- 正在使用的热备件
- 不完整的卷组
- 正在运行独占操作
- 缺失卷
- 处于非最佳状态的控制器
- 事件日志事件数过多
- 配置数据库验证失败
- 带有旧版本 DACstore 的驱动器

您还可以单独运行升级前运行状况检查，而无需进行升级。

驱动器升级概述

驱动器固件控制驱动器的低级操作特性。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。

在线和离线驱动器固件升级

有两种类型的驱动器固件升级方法：在线和离线。

联机

在线升级期间，驱动器按顺序逐个升级。升级过程中，存储阵列继续处理 I/O。无需停止 I/O。如果驱动器可以执行在线升级，则会自动使用在线方法。

可以执行在线升级的驱动器包括：

- 优化池中的驱动器
- 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
- 备用热备盘驱动器

执行在线驱动器固件升级可能需要几个小时，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，在升级卷组中的其他驱动器时，一个驱动器出现故障。
- 在 RAID 6 池或卷组中，在升级池或卷组中的其他驱动器时，两个驱动器出现故障。

离线（并行）

在脱机升级期间，会同时升级相同驱动器类型的所有驱动器。此方法需要停止与所选驱动器关联的卷的 I/O 活动。由于可以同时（并行）升级多个驱动器，因此整体停机时间大大缩短。如果驱动器只能进行脱机升级，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固件运行所在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的驱动器。System Manager 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，也可以升级 IOM 固件和非易失性静态随机存取存储器 (NVSRAM)，以确保您拥有所有最新功能和错误修复。

开始之前

- 您知道是否要升级 IOM 固件。

  通常情况下，您应该同时升级所有组件。但是，如果不想在 SANtricity OS 软件升级过程中升级 IOM 固件，或者技术支持指示您降级 IOM 固件（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，应同时升级所有组件。但是，如果文件已修补或为自定义版本并且不希望覆盖它，则可能决定不升级控制器 NVSRAM 文件。

- 您知道是立即激活 OS 升级还是稍后激活。

  稍后激活的原因可能包括：

  - 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 负载较轻。控制器在激活期间发生故障转移，因此在升级完成之前，性能可能会低于正常水平。
  - 包类型 — 在升级其他存储阵列上的文件之前，您可能需要在一个存储阵列上测试新软件和固件。
- 您知道是否要从不安全的驱动器或内部安全的驱动器切换到使用外部密钥管理服务器 (KMS) 来确保驱动器安全。
- 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 OS 软件文件或仅升级控制器 NVSRAM 文件，或者您可以选择升级这两个文件。

仅在技术支持人员指示时执行此操作。

数据丢失或存储阵列损坏的风险 — 升级过程中请勿对存储阵列进行更改。保持存储阵列的电源。

步骤

1. 如果您的存储阵列仅包含一个控制器，或者您没有安装多路径驱动程序，请停止对存储阵列的 I/O 活动，以防止出现应用程序错误。如果您的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. 选择菜单：Support[Upgrade Center]。

3. 从支持站点将新文件下载到管理客户端。

   a. 单击 **NetApp** 支持 启动支持网站。

   b. 在 Support 网站上，单击 **Downloads** 选项卡，然后选择 **Downloads**。

   c. 选择 **E-Series SANtricity OS Controller Software**。

   d. 按照其余说明进行操作。

   > 8.42 及更高版本需要数字签名固件。如果您尝试下载未签名的固件，则会显示错误并中止下载。

4. 如果此时不想升级 IOM 固件，请单击 暂停 **IOM** 自动同步。

   如果您的存储阵列只有一个控制器，则 IOM 固件不会升级。

5. 在 SANtricity OS 软件升级下，单击 开始升级 。

   此时将显示升级 SANtricity OS 软件对话框。

6. 选择一个或多个文件以开始升级过程：

   a. 通过单击*浏览*并导航到您从支持网站下载的 OS 软件文件，选择 SANtricity OS 软件文件。

   b. 通过单击*浏览*并导航到您从支持站点下载的 NVSRAM 文件，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： 如果您选择要升级的 SANtricity OS 软件文件，则可以通过选中 立即传输文件，但不升级（稍后激活升级） 复选框将文件传输到控制器，而无需激活它们。

8. 单击 **Start**，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操作，但不能在传输或激活期间取消。

9. 可选： 要查看已升级内容的列表，请单击 **Save Log**。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `drive_upgrade_log-timestamp.txt`。

完成后

- 确认所有组件都显示在 Hardware 页面上。
- 通过检查软件和固件清单对话框来验证新的软件和固件版本（转到菜单：Support[Upgrade Center]，然后单击 **Software and Firmware Inventory** 的链接）。
- 如果升级了控制器 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或等待更方便的时间。

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：

- 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 负载较轻。控制器在激活期间发生故障转移，因此在升级完成之前，性能可能会低于正常水平。
- 包类型 — 在升级其他存储阵列上的文件之前，您可能需要在一个存储阵列上测试新软件和固件。

当您有已传输但未激活的软件或固件时，您会在 System Manager 主页的通知区域以及升级中心页面上看到通知。

激活过程启动后无法停止。

步骤

1. 选择菜单：Support[Upgrade Center]。
2. 在标记为 SANtricity 操作系统控制器软件升级的区域中，单击*激活*，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开始。如果升级前运行状况检查通过，则升级过程继续激活文件。如果升级前运行状况检查失败，请使用 Recovery Guru 或联系技术支持解决问题。对于某些类型的条件，技术支持可能会建议您通过选中 **Allow Upgrade** 复选框继续升级，尽管存在错误。

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

3. 可选： 要查看已升级内容的列表，请单击 **Save Log**。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `drive_upgrade_log-timestamp.txt`。

完成后

- 确认所有组件都显示在 Hardware 页面上。
- 通过检查软件和固件清单对话框来验证新的软件和固件版本（转到菜单：Support[Upgrade Center]，然后单击 **Software and Firmware Inventory** 的链接）。
- 如果升级了控制器 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，以确保您拥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、卷复制（到不受计划固件升级影响的卷组）或远程镜像备份数据。
- 存储阵列具有最佳状态。
- 所有驱动器都具有最佳状态。

- 存储阵列上未运行任何配置更改。
- 如果驱动器只能进行离线升级，则会停止与驱动器关联的所有卷的 I/O 活动。

步骤

1. 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 开始升级 。

   此时将显示一个对话框，其中列出当前正在使用的驱动器固件文件。

4. 从支持站点提取（解压缩）您下载的文件。
5. 单击 **Browse**，然后选择从 Support 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_HUC101212CSS600_30602291_MS01_2800_0002`，扩展名为 `.dlp`。

   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，则会出现文件冲突错误。确定要用于升级的驱动器固件文件并删除另一个。

6. 单击 **Next**。

   此时将显示 **Select Drives** 对话框，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显示在建议的固件信息区域中。如果您必须更改固件，请单击 **Back** 返回上一个对话框。

7. 选择要执行的升级类型：
   - 联机（默认值） — 显示可以支持固件下载的驱动器_在存储阵列处理 I/O 时_。选择此升级方法时，您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，这些驱动器会一次升级一个。
   - 离线（并行） — 显示仅在使用驱动器的任何卷上的所有 I/O 活动停止时才能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（默认）方法更快。
8. 在表格的第一列中，选择要升级的驱动器。
9. 单击 **Start**，并确认要执行此操作。

   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已完成。任何未开始的固件下载都将被取消。

   > 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**。

    此文件将以此名称保存在浏览器的 Downloads 文件夹中 `drive_upgrade_log-timestamp.txt`。

11. 如果在升级过程中出现以下任一错误，请采取适当的建议措施。

如果遇到此固件下载错误…	然后执行以下操作…
分配的驱动器出现故障	出现故障的一个原因可能是驱动器没有适当的签名。请确保受影响的驱动器是授权驱动器。有关详细信息，请与技术支持联系。 更换驱动器时，请确保更换驱动器的容量等于或大于您要更换的故障驱动器。 您可以在存储阵列接收 I/O 时更换出现故障的驱动器。
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电缆均未损坏。 • 确保所有电缆均已紧密连接。
集成热备用驱动器	必须先纠正此错误情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
不完整的卷组	如果一个或多个卷组或磁盘池不完整，则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 来解决问题。
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）	如果一个或多个独占操作正在进行中，则必须先完成操作，然后才能升级固件。使用 System Manager 来监控操作进度。
缺失卷	必须先纠正丢失的卷情况，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 Optimal 以外的状态	其中一个存储阵列控制器需要注意。必须先纠正此情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 来解决问题。
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。
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。
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。
MEL 相关检查	请联系技术支持以解决此问题。

如果遇到此固件下载错误…	然后执行以下操作…
在过去 7 天内报告了超过 10 起 DDE 信息性或危急 MEL 事件	请联系技术支持以解决此问题。
在过去 7 天内报告了超过 2 个 Page 2C Critical MEL 事件	请联系技术支持以解决此问题。
在过去 7 天内报告了 2 个以上已降级的驱动器通道关键 MEL 事件	请联系技术支持以解决此问题。
过去 7 天超过 4 个关键 MEL 条目	请联系技术支持以解决此问题。

完成后

您的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发生错误。

固件下载错误	说明	建议操作
分配的驱动器出现故障	无法升级存储阵列中分配的驱动器。	出现故障的一个原因可能是驱动器没有适当的签名。请确保受影响的驱动器是授权驱动器。有关详细信息，请与技术支持联系。 更换驱动器时，请确保更换驱动器的容量等于或大于您要更换的故障驱动器。 您可以在存储阵列接收 I/O 时更换出现故障的驱动器。
集成热备用驱动器	如果驱动器被标记为热备盘并且正在用于某个卷组，则固件升级过程将失败。	必须先纠正此错误情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 解决此问题。
不完整的卷组	如果任何属于卷组的驱动器被绕过、删除或无响应，则视为不完整的卷组。不完整的卷组会阻止固件升级。	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 来解决问题。
当前在任何卷组上运行的独占操作（后台媒体/奇偶校验扫描除外）	如果卷上正在进行任何独占操作，则无法升级固件。	如果一个或多个独占操作正在进行中，则必须先完成操作，然后才能升级固件。使用 System Manager 来监控操作进度。

固件下载错误	说明	建议操作
缺失卷	如果缺少任何卷，则无法升级固件。	必须先纠正丢失的卷情况，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 Optimal 以外的状态	如果任何一个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。必须先纠正此情况，然后才能升级固件。启动 System Manager 并使用 Recovery Guru 来解决问题。
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。
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。
MEL 相关检查	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。
在过去 7 天内报告了超过 10 起 DDE 信息性或危急 MEL 事件	无法升级固件，因为在过去七天内报告的 DDE 信息或关键 MEL 事件超过 10 个。	请联系技术支持以解决此问题。
在过去 7 天内报告了超过 2 个 Page 2C Critical MEL 事件	无法升级固件，因为在过去七天内报告了两个以上的页面 2C 关键 MEL 事件。	请联系技术支持以解决此问题。
在过去 7 天内报告了 2 个以上已降级的驱动器通道关键 MEL 事件	无法升级固件，因为在过去七天内报告了两个以上降级的驱动器通道严重 MEL 事件。	请联系技术支持以解决此问题。
过去 7 天超过 4 个关键 MEL 条目	无法升级固件，因为在过去七天中报告了四个以上的关键事件日志条目。	请联系技术支持以解决此问题。
需要提供有效的管理 IP 地址。	要执行此操作，需要提供有效的控制器 IP 地址。	请联系技术支持以解决此问题。
该命令要求为每个控制器提供一个活动管理 IP 地址。	此操作需要与存储阵列关联的每个控制器的控制器 IP 地址。	请联系技术支持以解决此问题。
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。

固件下载错误	说明	建议操作
固件下载上传过程中出错。	固件下载失败，因为控制器无法处理此请求。验证存储阵列是否最佳并重试此操作。	如果在验证存储阵列处于最佳状态后再次发生此错误，请联系技术支持以解决此问题。
固件激活过程中出错。	固件激活失败，因为控制器无法处理此请求。验证存储阵列是否最佳并重试此操作。	如果在验证存储阵列处于最佳状态后再次发生此错误，请联系技术支持以解决此问题。
等待控制器 {0} 重新启动时已达到超时。	重新启动后，管理软件无法重新连接到控制器 {0}。验证是否有到存储阵列的操作连接路径，如果未成功完成，则重试此操作。	如果在验证存储阵列处于最佳状态后再次发生此错误，请联系技术支持以解决此问题。

您可以使用 System Manager 中的 Recovery Guru 来更正其中一些情况。但是，对于某些情况，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可从存储阵列获得。此信息有助于技术支持了解阻止固件升级和下载的错误条件。

AutoSupport 常见问题解答，适用于 SANtricity System Manager

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

我正在收集哪些数据?

AutoSupport 功能和手动支持数据收集功能提供了在客户支持包中收集数据的方法，以便技术支持人员进行远程故障排除和问题分析。

客户支持捆绑包将存储阵列的所有类型信息收集到单个压缩文件中。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。这些信息仅由技术支持人员用于解决存储阵列的问题。

无法读取的扇区数据向我显示了什么?

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。日志中包含以下有关包含不可读扇区的卷的信息。字段是可排序的。

字段	说明
受影响的卷	显示卷的标签。如果缺失的卷包含不可读扇区，则会显示缺失卷的 World Wide Identifier。
logical unit number（逻辑单元号）(LUN)	显示卷的 LUN。如果卷没有 LUN，对话框将显示 NA。
分配给	显示有权访问卷的主机或主机群集。如果主机、主机群集甚至 Default Cluster 都无法访问该卷，则对话框将显示 NA。

要查看有关不可读扇区的其他信息，请单击卷旁边的加号 (+)。

字段	说明
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	显示卷的逻辑块地址 (LBA)。
驱动器位置	显示驱动器架、抽屉（如果您的驱动器架有抽屉）和托架位置。
驱动器逻辑块地址	显示驱动器的 LBA。
故障类型	显示以下故障类型之一： • 物理 — 物理介质错误。 • 逻辑 — 条带中其他位置的读取错误导致无法读取的数据。例如，由于卷中其他地方的媒体错误而导致无法读取的扇区。 • 不一致 — 冗余数据不一致。 • 数据保证 — 数据保证错误。

什么是健康映像？

健康映像是控制器处理器内存的原始数据转储，技术支持可以使用它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。在某些疑难解答情况下，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他们。

这些 **AutoSupport** 功能有什么作用？

该 AutoSupport 功能由三个单独的功能组成，您可以分别启用这些功能。

- 基本 **AutoSupport** — 允许您的存储阵列自动收集数据并将其发送给技术支持。
- **AutoSupport OnDemand** — 允许技术支持在需要解决问题时请求重新传输以前的 AutoSupport 派单。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器进行检查，以确定是否存在任何挂起的重传请求，并做出相应的响应。
- 远程诊断 — 允许技术支持在需要解决问题时请求新的最新 AutoSupport 派遣。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器签入，以确定是否存在任何挂起的新请求，并做出相应的响应。

通过 **AutoSupport** 功能收集哪些类型的数据？

AutoSupport 功能包含三种标准调度类型：事件调度、计划调度以及按需和远程诊断调度。

此 AutoSupport 数据不包含任何用户数据。

- 事件调度

当系统上发生需要主动通知技术支持的事件时，AutoSupport 功能会自动发送事件触发的派单。

  - 在托管存储阵列上发生支持事件时发送。
  - 包括事件发生时存储阵列状况的综合快照。

- 计划派单

  AutoSupport 功能会按常规时间表自动发送多个派单。

  - 每日调度 — 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** 和远程诊断派遣
  - **AutoSupport OnDemand** — 允许技术支持在需要解决问题时请求重新传输以前的 AutoSupport 派单。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器进行检查，以确定是否存在任何挂起的重传请求，并做出相应的响应。
  - 远程诊断 — 允许技术支持在需要解决问题时请求新的最新 AutoSupport 派遣。所有传输都是从存储阵列启动的，而不是从 AutoSupport 服务器启动的。存储阵列定期与 AutoSupport 服务器签入，以确定是否存在任何挂起的新请求，并做出相应的响应。

如何为 **AutoSupport** 功能配置交付方式?

AutoSupport 功能支持 HTTPS 和 SMTP 协议，用于将 AutoSupport 调度发送到技术支持。

开始之前

- 必须启用 AutoSupport 功能。您可以在 AutoSupport 页面上查看是否已启用此功能。
- 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获得）。

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，必须将 AutoSupport 传递方法设置为 HTTPS。
- 电子邮件 — 允许您使用电子邮件服务器作为发送 AutoSupport 派单的传递方法。

> **HTTPS** 和电子邮件方法之间的差异。使用 SMTP 的电子邮件传递方法与 HTTPS 传递方法有一些重要区别。首先，电子邮件方法的调度大小限制为 5MB，这意味着某些 ASUP 数据集将不会被调度。其次，AutoSupport OnDemand 功能仅在 HTTPS 传递方法上可用。

步骤

1. 选择菜单：Support[Support Center > AutoSupport] 选项卡。
2. 选择 配置 **AutoSupport** 交付方式。

   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，然后为该交付方法选择参数。执行以下操作之一：
   - 如果选择了 HTTPS，请选择以下交付参数之一：

- 直接 — 此交付参数是默认选择。选择此选项后，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。必须指定主机地址和端口号。但是，如果需要，只需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。PAC 文件允许系统自动选择适当的代理服务器，以建立与目标技术支持系统的连接。

◦ 如果选择"电子邮件"，请输入以下信息：

- 邮件服务器地址作为完全限定域名、IPv4 地址或 IPv6 地址。
- AutoSupport 调度电子邮件"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。
- 如果要加密邮件，请选择 **SMTPS** 或 **STARTTLS** 作为加密类型，然后选择加密邮件的端口号。否则，请选择 **None**。
- 如果需要，请输入用户名和密码，以便与传出发件人和邮件服务器进行身份验证。

4. 单击 测试配置 以使用指定的交付参数测试与技术支持服务器的连接。如果您启用了 AutoSupport 按需功能，系统还将测试 AutoSupport OnDemand 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再次运行测试。如果测试继续失败，请联系技术支持。

5. 单击 **Save**。

什么是配置数据?

选择收集配置数据时，系统会保存 RAID 配置数据库的当前状态。

RAID 配置数据库包括控制器上卷组和磁盘池的所有数据。"收集配置数据"功能保存的信息与 CLI 命令 `save storageArray dbmDatabase`相同。

在升级 **SANtricity** 操作系统软件之前，我需要知道什么?

在升级控制器的软件和固件之前，请注意这些项目。

- 您已阅读文档和 `readme.txt` 文件，并确定要进行升级。
- 您知道是否要升级 IOM 固件。

  通常情况下，您应该同时升级所有组件。但是，如果不想在 SANtricity 操作系统控制器软件升级过程中升级 IOM 固件，或者技术支持指示您降级 IOM 固件（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，应同时升级所有组件。但是，如果文件已修补或为自定义版本并且不希望覆盖它，则可能决定不升级控制器 NVSRAM 文件。

- 您知道要立即激活还是稍后激活。

  稍后激活的原因可能包括：

- 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 负载较轻。控制器在激活期间发生故障转移，因此在升级完成之前，性能可能会低于正常水平。
- 包类型 — 在升级其他存储阵列上的文件之前，您可能需要在一个存储阵列上测试新软件和固件。

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 是管理存储阵列的软件。
- 控制器固件 — 控制器固件管理主机和卷之间的 I/O。
- 控制器 **NVSRAM** — 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) 固件管理控制器和驱动器架之间的连接。它还监控组件的状态。
- **Supervisor** 软件 — Supervisor 软件是运行该软件的控制器上的虚拟机。

作为升级过程的一部分，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，以便主机可以与控制器正确交互。

要确定是否属于这种情况，请参见 "NetApp 互操作性表工具"。

如果您的存储阵列仅包含一个控制器，或者您没有安装多路径驱动程序，请停止对存储阵列的 I/O 活动，以防止出现应用程序错误。如果您的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。

请勿在升级过程中更改存储阵列。

在暂停 **IOM** 自动同步之前，我需要知道什么？

暂停 IOM 自动同步可防止 IOM 固件在下次发生 SANtricity 操作系统控制器软件升级时进行升级。

通常，控制器软件和 IOM 固件作为捆绑包进行升级。如果要在存储模块上保留特殊版本的 IOM 固件，则可以暂停 IOM 自动同步。否则，下次执行控制器软件升级时，将恢复到与控制器软件捆绑的 IOM 固件。

为什么我的固件升级进展如此缓慢？

固件升级进度取决于系统的整体负载。

在驱动器固件的在线升级期间，如果在快速重建过程中发生卷传输，则系统会对传输的卷启动完全重建。此操作可能需要相当长的时间。实际的完整重建时间取决于几个因素，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、重建优先级设置和驱动器性能。

在升级驱动器固件之前，我需要知道什么？

在升级驱动器固件之前，请注意这些项目。

- 作为预防措施，请使用磁盘到磁盘备份、卷复制（到不受计划的固件升级影响的卷组）或远程镜像来备份数据。
- 您可能只想升级几个驱动器来测试新固件的行为，以确保其正常工作。如果新固件运行正常，请升级其余驱动器。
- 如果您有任何故障驱动器，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，则停止与驱动器关联的所有卷的 I/O 活动。停止 I/O 活动时，不会发生与这

些卷关联的配置操作。

- 升级驱动器固件时请勿移除任何驱动器。
- 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？

根据池或卷组的状态，选择要在驱动器上执行的升级类型。

- 联机

  如果池或卷组支持冗余且为 Optimal，则可以使用 Online 方法升级驱动器固件。Online 方法在存储阵列使用这些驱动器处理相关卷的 I/O 时下载固件。您不必使用这些驱动器停止对关联卷的 I/O。这些驱动器每次升级一个到与驱动器关联的卷。如果驱动器未分配给池或卷组，则可以通过 Online 或 Offline 方法更新其固件。使用 Online 方法升级驱动器固件时，系统性能可能会受到影响。

- 离线

  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_仅在所有 I/O 活动停止时_升级使用这些驱动器的相关卷的固件。您必须停止使用这些驱动器对任何关联卷的所有 I/O。如果驱动器未分配给池或卷组，则可以通过联机或脱机方法更新其固件。

使用 SANtricity Unified Manager 7 进行多阵列管理

主界面

了解 SANtricity Unified Manager

SANtricity Unified Manager 是一个基于 Web 的界面，允许您在单个视图中管理多个存储阵列。

主页

当您登录到 Unified Manager 时，主页打开到 **Manage - All**。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，并在单个阵列或一组阵列上执行操作。

导航侧边栏

您可以从导航侧边栏访问 Unified Manager 特性和功能。

区域	说明
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。 当存储阵列具有非最佳状态时，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。

界面设置和帮助

在界面右上角，您可以访问帮助和其他文档。您还可以从登录名旁边的下拉菜单中访问管理选项。

用户登录名和密码

当前登录系统的用户显示在界面右上角。

有关用户和密码的更多信息，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 Unified Manager 可通过多种类型的浏览器进行访问。

支持以下浏览器和版本。

浏览器	最低版本
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

必须安装 Web Services Proxy，并且浏览器可以使用该代理。

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，以保护其免受未经授权的访问。

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。任何拥有管理员密码的用户都可以对存储阵列进行配置更改。

除了管理员密码外，Unified Manager 界面还包括预配置的用户配置文件，其中有一个或多个角色映射到它们。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，请参阅：

- "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，软件仅提示您输入一次密码。默认情况下，会话在不活动 30 分钟后超时，此时必须再次输入密码。如果其他用户从另一个管理客户端访问软件并在会话正在进行时更改密码，则在下次尝试配置操作或视图操作时会提示您输入密码。

出于安全原因，在软件进入"锁定"状态之前，您只能尝试输入五次密码。在此状态下，软件会拒绝后续密码尝试。您必须等待 10 分钟才能重置为"正常"状态，然后再次尝试输入密码。

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。
- 设置密码后，不会从密码中删除尾随空格。如果密码中包含空格，请务必包含空格。
- 为提高安全性，请至少使用 15 个字母数字字符，并经常更改密码。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **Local User Roles** 选项卡。
3. 从表中选择 **admin** 用户。

   "更改密码"按钮变为可用。

4. 选择 **Change Password**。

   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，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. 输入您的本地管理员密码以确认此操作，然后单击 **Change**。

在 SANtricity Unified Manager 中管理会话超时

您可以为 SANtricity Unified Manager 配置超时，以便在指定时间后断开用户非活动会话。

关于此任务

默认情况下， Unified Manager 的会话超时时间为 30 分钟。您可以调整该时间，也可以完全禁用会话超时。

> 如果使用嵌入在阵列中的 Security Assertion Markup Language (SAML) 功能配置 Access Management，则当用户的 SSO 会话达到最大限制时，可能会发生会话超时。这可能在 System Manager 会话超时之前发生。

步骤

1. 在菜单栏中，选择用户登录名旁边的下拉箭头。
2. 选择 **Enable/Disable session timeout**。

此时将打开启用/禁用会话超时对话框。

3. 使用微调器控件以分钟为单位增加或减少时间。

   您可以设置的最短超时时间为 15 分钟。

   要禁用会话超时，请清除 **Set the length of time…** 复选框。

4. 单击 **Save**。

存储阵列

了解 SANtricity Unified Manager 中的发现

要管理存储资源，必须首先发现网络中的存储阵列。

如何发现阵列?

使用"添加/发现"页面可以查找和添加要在组织网络中管理的存储阵列。可以发现多个阵列，也可以发现单个阵列。为此，输入网络 IP 地址，然后 Unified Manager 尝试单独连接到该范围内的每个 IP 地址。

了解详情：

- "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。从此页面，您可以滚动浏览网络中发现的存储阵列列表，查看其状态，并在单个阵列或一组阵列上执行操作。

如果要管理单个阵列，可以选择它并打开 System Manager。

了解详情：

- "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

SANtricity Unified Manager 必须先发现要在组织网络中管理的存储阵列，然后才能显示和管理存储资源。您可以发现多个阵列，也可以发现单个阵列。

发现多个存储阵列

如果选择发现多个阵列，则输入网络 IP 地址范围，然后 Unified Manager 会尝试单个连接到该范围内的每个 IP 地址。成功到达的任何存储阵列都会显示在"发现"页面上，并可能添加到您的管理域中。

发现单个存储阵列

如果选择发现单个阵列，则为存储阵列中的一个控制器输入单个 IP 地址，然后添加单个存储阵列。

Unified Manager 仅发现并显示分配给控制器的单个 IP 地址或范围内的 IP 地址。如果分配给这些控制器的备用控制器或 IP 地址超出此单个 IP 地址或 IP 地址范围，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

作为发现过程的一部分，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

作为发现过程的一部分，Unified Manager 会验证发现的存储阵列是否正在使用受信任来源的证书。Unified Manager 对它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

  对于由 Unified Manager 发现的阵列，可能需要安装证书颁发机构提供的其他受信任证书。

  使用 **Import** 按钮导入这些证书。如果您之前已连接到此阵列，则其证书链中的一个或两个控制器证书要么已过期，要么已吊销，要么缺少根证书或中间证书。在管理存储阵列之前，您必须替换过期或吊销的证书，或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。如果管理员尝试在不导入已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被标记为受信任，并且存储阵列将被添加到 Unified Manager。

  如果不信任与存储阵列的连接，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。

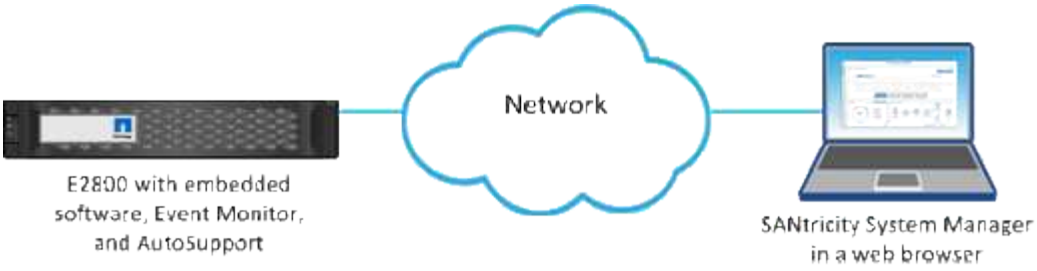
了解如何从 **Unified Manager** 访问 **SANtricity System Manager**

选择一个或多个存储阵列，并在要配置和管理存储阵列时使用"启动"选项打开 SANtricity System Manager。

System Manager 是控制器上的嵌入式应用程序，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，必须具有：

- 此处列出的阵列模型之一： "E-Series 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您的管理域。

开始之前

- 您必须使用包含 Security Admin 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 的访问管理磁贴设置存储阵列密码。
- 要解决不受信任的证书问题，您必须具有来自证书颁发机构 (CA) 的受信任证书文件，并且证书文件在本地系统上可用。

发现阵列是一个多步骤过程。

步骤 **1**：输入网络地址

输入要在本地子网中搜索的网络地址范围。成功到达的任何存储阵列都会显示在"发现"页面上，并可能被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 **Stop Discovery**。

步骤

1. 在 Manage 页面中，选择 **Add/Discover**。

   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搜索本地子网络，然后单击 **Start Discovery**。

   发现过程开始。此发现过程可能需要几分钟才能完成。发现存储阵列时，Discover 页面上的表将被填充。

   > 如果未发现可管理的阵列，请验证存储阵列已正确连接到您的网络，并且其分配的地址在范围内。单击 **New Discovery Parameters** 返回添加/发现页面。

4. 查看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 **Next**。

Unified Manager 将对要添加到管理域的每个阵列进行凭据检查。您可能需要解析与该阵列关联的任何自签名证书和不受信任的证书。

6. 单击 **Next** 继续向导中的下一步。

步骤 **2**：在发现过程中解析自签名证书

作为发现过程的一部分，系统会验证存储阵列是否正在使用受信任来源的证书。

步骤

1. 执行以下操作之一：
   - 如果信任到发现的存储阵列的连接，请继续到向导中的下一张卡。自签名证书将被标记为可信，存储阵列将被添加到 Unified Manager。
   - 如果不信任与存储阵列的连接，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 **Next** 继续向导中的下一步。

步骤 **3**：在发现期间解析不受信任的证书

当存储阵列尝试与 Unified Manager 建立安全连接，但连接无法确认为安全时，会发生不受信任的证书。在阵列发现过程中，可以通过导入由受信任的第三方颁发的证书颁发机构 (CA) 证书（或 CA 签名的证书）来解决不受信任的证书。

如果满足以下任一情况，则可能需要安装其他受信任的 CA 证书：

- 您最近添加了一个存储阵列。
- 一个或两个证书已过期。
- 一个或两个证书都被吊销。
- 一个或两个证书都缺少根证书或中间证书。

步骤

1. 选中要为其解析不受信任的证书的任何存储阵列旁边的复选框，然后选择 **Import** 按钮。

   此时将打开一个对话框，用于导入受信任的证书文件。

2. 单击 **Browse** 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 **Import**。

   文件已上传并验证。

   任何具有未解决的不受信任证书问题的存储阵列都不会添加到 Unified Manager。

4. 单击 **Next** 继续向导中的下一步。

步骤 **4**：提供密码

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： 将存储阵列关联到组：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 **Finish**。

完成后

存储阵列将添加到您的管理域并与选定组关联（如果指定）。

Unified Manager 连接到指定的存储阵列可能需要几分钟时间。

在 **SANtricity Unified Manager** 中发现单个阵列

使用"添加/发现单个存储阵列"选项可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 的访问管理磁贴设置存储阵列密码。

步骤

1. 在 Manage 页面中，选择 **Add/Discover**。

   此时将显示"添加/发现"对话框。

2. 选择 **Discover a single storage array** 单选按钮。
3. 输入存储阵列中一个控制器的 IP 地址，然后单击 **Start Discovery**。

   Unified Manager 连接到指定的存储阵列可能需要几分钟时间。

   当到指定控制器的 IP 地址的连接失败时，将显示 Storage Array Not Accessible（存储阵列不可访问）消息。

4. 如果出现提示，请解析任何自签名证书。

   作为发现过程的一部分，系统验证发现的存储阵列是否正在使用受信任来源的证书。如果它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公认的证书颁发机构 (CA) 签名的证书。

5. 如果出现提示，请解决任何不受信任的证书。

   当存储阵列尝试与 Unified Manager 建立安全连接，但连接无法确认为安全时，会发生不受信任的证书。通过导入由受信任的第三方颁发的证书颁发机构 (CA) 证书来解决不受信任的证书。

6. 单击 **Next**。
7. 可选： 将发现的存储阵列关联到组：从下拉列表中，选择要与存储阵列关联的所需组。

默认情况下，"All" 组处于选中状态。

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 **OK**。

完成后

存储阵列将添加到 Unified Manager 中，如果指定，它也将添加到您选择的组中。

如果启用了自动支持数据收集，则会自动为您添加的存储阵列收集支持数据。

管理阵列

在 **SANtricity Unified Manager** 中查看存储阵列状态

SANtricity Unified Manager 显示已发现的每个存储阵列的状态。

转到 **Manage - All** 页面。从此页面，您可以查看 Web Services Proxy 与该存储阵列之间的连接状态。

下表描述了状态指标。

状态	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。
不受信任的证书	与存储阵列的一个或多个连接不受信任，因为 HTTPS 证书是自签名的并且尚未导入，或者证书是 CA 签名的并且尚未导入根和中间 CA 证书。
需要注意	存储阵列存在问题，需要您进行干预才能纠正。
锁定	存储数组处于锁定状态。
未知	从未联系过存储阵列。当 Web Services Proxy 正在启动但尚未与存储阵列联系，或者存储阵列处于脱机状态并且自 Web Services Proxy 启动后从未联系过时，可能会发生这种情况。
脱机	Web Services Proxy 以前已与存储阵列联系，但现在已失去与该阵列的所有连接。

在 **SANtricity Unified Manager** 中管理单个存储阵列

如果要执行管理操作，可以使用"启动"选项打开一个或多个存储阵列的基于浏览器的 SANtricity System Manager。

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 **Launch**。

系统打开一个新窗口并显示 System Manager 登录页面。

3. 输入您的用户名和密码，然后单击 **Log in**。

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 Storage admin 权限的用户配置文件登录。
- 您必须知道存储阵列的当前密码，该密码在 System Manager 中设置。

关于此任务

在此任务中，输入存储阵列的当前密码，以便在 Unified Manager 中进行访问。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，则可能需要执行此操作。

步骤

1. 从 Manage 页面中，选择一个或多个存储阵列。
2. 选择菜单：Uncommon Tasks[Provide Storage Array Passwords]。
3. 输入每个存储阵列的密码，然后单击 **Save**。

从 **SANtricity Unified Manager** 中删除存储阵列

如果不想再从 SANtricity Unified Manager 管理一个或多个存储阵列，则可以将其删除。

关于此任务

您无法访问删除的任何存储阵列。但是，您可以通过将浏览器直接指向其 IP 地址或主机名来建立与任何已删除的存储阵列的连接。

删除存储阵列不会以任何方式影响存储阵列或其数据。如果不小心删除了存储阵列，可以再次添加它。

步骤

1. 选择 **Manage** 页面。
2. 选择要删除的一个或多个存储阵列。
3. 选择菜单：Uncommon Tasks[Remove storage array]。

   存储阵列已从 SANtricity Unified Manager 中的所有视图中删除。

设置导入

了解如何在 **SANtricity Unified Manager** 中导入存储阵列设置

导入设置功能允许您执行批量操作，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（如卷组和池）和系统设置（如自动负载平衡）。

了解详情：

- "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 并配置所需设置。然后从 Unified Manager 转到"管理"页面，将设置导入到一个或多个阵列。

了解详情：

- "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 Unified Manager 将设置从一个存储阵列导入到多个存储阵列。导入设置功能是一种批处理操作，可在需要在网络中配置多个阵列时节省时间。

可用于导入的设置

可以将以下配置导入到多个数组：

- 警报 — 使用电子邮件、syslog 服务器或 SNMP 服务器向管理员发送重要事件的警报方法。
- **AutoSupport** — 一种监控存储阵列运行状况并将自动派遣发送给技术支持的功能。
- 目录服务 — 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：
  - 卷的媒体扫描设置

- 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，请按照以下工作流程操作：

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 **Manage** 页面并导入设置。
4. 从 **Operations** 页面，查看 Import Settings 操作的结果。

在 **SANtricity Unified Manager** 中复制存储阵列配置的要求

将存储配置从一个存储阵列导入到另一个存储阵列之前，请查看要求和准则。

磁盘架

- 控制器所在的盘架在源阵列和目标阵列上必须相同。
- 源阵列和目标阵列上的盘架 ID 必须相同。
- 扩展盘架必须在相同插槽中安装相同驱动器类型（如果驱动器用于配置中，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 E2800 导入到 E5700），但 RBOD 机箱类型必须相同。
- HIC（包括主机的 DA 功能）在源阵列和目标阵列之间必须相同。
- 不支持从双工配置导入到单工配置；但是，允许从单工配置导入到双工配置。
- FDE 设置不包含在导入过程中。

状态

- 目标数组必须处于"最佳"状态。
- 源数组不必处于 Optimal 状态。

存储

- 驱动器容量可能因源阵列和目标阵列而异，只要目标上的卷容量大于源。（目标阵列可能具有更新、更大容量的驱动器，这些驱动器不会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。
- 精简卷未包含在导入过程中。

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（菜单：设置[警报]）。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：Settings[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 syslog 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。
- **Syslog** 警报 — Syslog 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 Manage 页面中，单击 **Import Settings**。

   导入设置向导打开。

2. 在 Select Settings 对话框中，选择 **Email alerts**、**SNMP alerts** 或 **Syslog alerts**，然后单击 **Next**。

   此时将打开一个用于选择源阵列的对话框。

3. 在选择源对话框中，选择具有要导入的设置的数组，然后单击 **Next**。
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。

   > 无法选择固件低于 8.50 的存储阵列。此外，如果 Unified Manager 无法与该阵列通信（例如，如果该阵列处于脱机状态，或者存在证书、密码或网络问题），则不会在此对话框中显示该阵列。

5. 单击 **Finish**。

   操作页面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

现在已将目标存储阵列配置为通过电子邮件、SNMP 或 syslog 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，此批处理操作可节省时间。

开始之前

- AutoSupport 在 System Manager 中为要用作源的存储阵列配置（菜单：支持[支持中心]）。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：Settings[System > Save Storage Array Configuration]）。

关于此任务

导入的设置包括单独的功能（基本 AutoSupport、AutoSupport OnDemand 和远程诊断）、维护窗口、交付方法和派遣计划。

步骤

1. 在 Manage 页面中，单击 **Import Settings**。

   导入设置向导打开。

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

   此时将打开一个用于选择源阵列的对话框。

3. 在选择源对话框中，选择具有要导入的设置的数组，然后单击 **Next**。
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。

   无法选择固件低于 8.50 的存储阵列。此外，如果 Unified Manager 无法与该阵列通信（例如，如果该阵列处于脱机状态，或者存在证书、密码或网络问题），则不会在此对话框中显示该阵列。

5. 单击 **Finish**。

   操作页面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

现在使用与源阵列相同的 AutoSupport 设置来配置目标存储阵列。

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：设置[访问管理]）。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：Settings[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 服务器的用户组到存储阵列的预定义角色的映射。

步骤

1. 在 Manage 页面中，单击 **Import Settings**。

   导入设置向导打开。

2. 在选择设置对话框中，选择 **Directory services**，然后单击 **Next**。

   此时将打开一个用于选择源阵列的对话框。

3. 在选择源对话框中，选择具有要导入的设置的数组，然后单击 **Next**。
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。

   无法选择固件低于 8.50 的存储阵列。此外，如果 Unified Manager 无法与该阵列通信（例如，如果该阵列处于脱机状态，或者存在证书、密码或网络问题），则不会在此对话框中显示该阵列。

5. 单击 **Finish**。

   操作页面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进行配置。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：Settings[System > Save Storage Array Configuration]）。

关于此任务

导入的设置包括卷的媒体扫描设置、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 Manage 页面中，单击 **Import Settings**。

   导入设置向导打开。

2. 在选择设置对话框中，选择 **System**，然后单击 **Next**。

   此时将打开一个用于选择源阵列的对话框。

3. 在选择源对话框中，选择具有要导入的设置的数组，然后单击 **Next**。
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。

无法选择固件低于 8.50 的存储阵列。此外，如果 Unified Manager 无法与该阵列通信（例如，如果该阵列处于脱机状态，或者存在证书、密码或网络问题），则不会在此对话框中显示该阵列。

5. 单击 **Finish**。

   操作页面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

目标存储阵列现在已配置为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，此批处理操作可节省时间。

开始之前

- 在 SANtricity System Manager 中为要用作源的存储阵列配置了存储。
- 目标存储阵列的现有配置在 System Manager 中备份（菜单：Settings[System > Save Storage Array Configuration]）。
- 源和目标阵列必须满足以下要求：
  - 控制器所在的货架必须相同。
  - 货架 ID 必须相同。
  - 扩展盘架必须在相同插槽中填充相同的驱动器类型。
  - RBOD 外壳类型必须相同。
  - HIC，包括主机的数据保证功能，必须相同。
  - 目标数组必须处于"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：
  - 不支持从双工配置导入到单工配置；但是，允许从单工配置导入到双工配置。
  - 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。
  - 精简卷未包含在导入过程中。

关于此任务

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

步骤

1. 在 Manage 页面中，单击 **Import Settings**。

   导入设置向导打开。

2. 在选择设置对话框中，选择 **Storage configuration**，然后单击 **Next**。

此时将打开一个用于选择源阵列的对话框。

3. 在选择源对话框中，选择具有要导入的设置的数组，然后单击 **Next**。
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。

> 无法选择固件低于 8.50 的存储阵列。此外，如果 Unified Manager 无法与该阵列通信（例如，如果该阵列处于脱机状态，或者存在证书、密码或网络问题），则不会在此对话框中显示该阵列。

5. 单击 **Finish**。

操作页面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

目标存储阵列现在已配置为与源阵列相同的存储配置。

SANtricity Unified Manager 导入设置常见问题

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

将导入哪些设置?

导入设置功能是一种批处理操作，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如何在 SANtricity System Manager 中配置源存储阵列。

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。
- **Syslog** 警报 — 设置包括 syslog 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** — 设置包括单独的功能（基本 AutoSupport、AutoSupport OnDemand 和远程诊断）、维护时段、交付方法和派遣计划。
- 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 服务器的用户组到存储阵列预定义角色的映射。
- 存储配置 — 配置包括卷（仅限厚卷和非存储库卷）、卷组、池和热备盘驱动器分配。
- 系统设置 — 配置包括卷的媒体扫描设置、控制器的 SSD 缓存和自动负载平衡（不包括主机连接报告）。

为什么我没有看到所有的存储阵列?

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。

由于以下原因，可能无法显示存储阵列：

- 固件版本低于 8.50。
- 此存储阵列已脱机。
- 系统无法与该阵列通信（例如，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

从"管理组"页面，您可以创建一组存储阵列组，以便于管理。

什么是数组组?

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。您可能需要对存储阵列进行分组，以便更轻松地运行监控或报告作业。

有两种类型的组：

- **All group** — All group 是默认组，包括组织中发现的所有存储阵列。可以从主视图访问 All group。
- 用户创建的组 — 用户创建的组包括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?

从"管理组"页面，您可以创建组，然后将数组添加到该组。

了解详情：

- "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。

配置组是一个两步过程。

步骤 **1**：创建组

您首先创建一个组。存储组定义了哪些驱动器提供组成卷的存储。

步骤

1. 在"管理"页面中，选择菜单：Manage Groups[Create storage array group]。
2. 在 **Name** 字段中，输入新组的名称。
3. 选择要添加到新组的存储阵列。
4. 单击 **Create**。

步骤 **2**：将存储阵列添加到组

您可以向用户创建的组添加一个或多个存储阵列。

步骤

1. 从主视图中，选择 **Manage**，然后选择要将存储阵列添加到的组。
2. 选择菜单：管理组 [Add storage arrays to group]。

3. 选择要添加到组的存储阵列。
4. 单击 **Add**。

从 SANtricity Unified Manager 中的组中删除存储阵列

如果不想再从特定存储组进行管理，则可以从组中删除一个或多个托管存储阵列。

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，您仍然可以使用浏览器管理它。如果存储阵列意外从组中删除，可以再次添加它。

步骤

1. 在"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 **Remove**。

在 SANtricity Unified Manager 中删除存储阵列组

您可以删除一个或多个不再需要的存储阵列组。

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"视图或其关联的任何其他组进行访问。

步骤

1. 从 Manage 页面中，选择菜单：Manage Groups[Delete storage array group]。
2. 选择要删除的一个或多个存储阵列组。
3. 单击 **Delete**。

在 SANtricity Unified Manager 中重命名存储阵列组

当当前名称不再有意义或适用时，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。

- 一个名称可以由字母、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，则会显示错误消息。系统会提示您选择其他名称。
- 将名称限制为 30 个字符。删除名称中的任何前导空格和尾随空格。
- 使用易于理解和记忆的独特、有意义的名称。
- 避免使用任意名称或将来会很快失去意义的名称。

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[Rename storage array group]。
3. 在 **Group Name** 字段中，为组键入一个新名称。
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 操作系统软件和 NVSRAM 升级。

升级如何运作?

下载最新的 OS 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 操作系统软件文件（可在支持页面的 Unified Manager 中获得链接）。在管理主机系统（在浏览器中访问 Unified Manager 的主机）上保存文件，然后解压缩文件。
2. 在 Unified Manager 中，您可以将 SANtricity 操作系统软件文件和 NVSRAM 文件加载到存储库（Web Services Proxy 服务器中存储文件的区域）。您可以从菜单中添加文件：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]。
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 操作系统软件页面（菜单：升级中心[升级 SANtricity 操作系统软件]），选择 SANtricity 操作系统软件文件和 NVSRAM 文件。选择软件文件后，此页面上将显示兼容存储阵列的列表。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供激活。在升级过程中，Unified Manager 会执行以下任务：
   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升级其他阵列，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 操作系统软件，一次一个控制器。激活期间，现有的 SANtricity 操作系统文件将替换为新文件。

   您还可以指定稍后激活软件。

立即或分阶段升级

您可以立即激活升级，也可以将其暂存以供稍后使用。出于以下原因，您可以选择稍后激活：

- 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 负载较轻。根据 I/O 负载和缓存大小，控制器升级通常需要 15 到 25 分钟才能完成。在激活期间，控制器会重新启动并进行故障转移，因此在升级完成之前，性能可能会低于正常水平。

- 包类型 — 在升级其他存储阵列上的文件之前，您可能需要在一个存储阵列上测试新软件和固件。

要激活暂存软件，请转到菜单：Support[Upgrade Center]，然后在标记为 SANtricity 操作系统控制器软件升级的区域中单击 **Activate**。

运行状况检查

运行状况检查是升级过程的一部分，但您也可以在开始之前单独运行运行状况检查（转到菜单：Upgrade Center[Pre-Upgrade Health Check]）。

运行状况检查会评估所有存储系统组件，以确保可以继续升级。以下情况可能会阻止升级：

- 分配的驱动器出现故障
- 正在使用的热备件
- 不完整的卷组
- 正在运行独占操作
- 缺失卷
- 处于非最佳状态的控制器
- 事件日志事件数过多
- 配置数据库验证失败
- 带有旧版本 DACstore 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"页面查看每个发现的存储阵列的当前 SANtricity 操作系统软件版本。版本显示在 SANtricity 操作系统软件列中。当您单击每行中的 SANtricity 操作系统版本时，控制器固件和 NVSRAM 信息在弹出对话框中可用。

需要升级的其他组件

作为升级过程的一部分，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，以便主机可以与控制器正确交互。

有关兼容性信息，请参见 "NetApp 互操作性矩阵"。此外，请参见适用于您的操作系统的 Express Guides 中的步骤。Express Guides 可从 "E 系列和 SANtricity 文档"获得。

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，则在升级过程中，存储阵列可以继续处理 I/O。在升级过程中，会发生以下过程：

1. 控制器 A 将其所有 LUN 故障切换到控制器 B。
2. 升级发生在控制器 A 上。

3. 控制器 A 收回其 LUN 和控制器 B 的所有 LUN。
4. 升级发生在控制器 B 上。

升级完成后，可能需要在控制器之间手动重新分配卷，以确保卷返回到正确的所有控制器。

升级软件和固件

在 **SANtricity Unified Manager** 中执行升级前运行状况检查

运行状况检查作为升级过程的一部分运行，但您也可以在开始之前单独运行运行状况检查。运行状况检查会评估存储阵列的组件，以确保升级可以继续。

步骤

1. 从主视图中，选择 管理，然后选择菜单：Upgrade Center[Pre-Upgrade Health Check]。

   将打开升级前运行状况检查对话框，并列出所有发现的存储系统。

2. 如果需要，请对列表中的存储系统进行筛选或排序，以便查看当前未处于 Optimal 状态的所有系统。
3. 选中要运行运行状况检查的存储系统的复选框。
4. 单击 **Start**。

   在执行运行状况检查时，进度会显示在对话框中。

5. 健康检查完成后，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升级其他阵列，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 Services Proxy 和 Unified Manager 的主机系统上提供了最新的 SANtricity 操作系统文件。
- 您知道是要现在激活软件升级还是以后激活。

  您可以选择稍后激活，原因如下：

  - 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 负载较轻。控制器在激活期间发生故障转移，因此在升级完成之前，性能可能会低于正常水平。
  - 软件包类型 — 在升级其他存储阵列上的文件之前，您可能需要在一个存储阵列上测试新的 OS 软件。

系统必须运行 SANtricity 操作系统 11.70.5 才能升级到 11.80.x 或更高版本。

关于此任务

数据丢失或存储阵列损坏的风险 - 升级过程中请勿对存储阵列进行更改。保持存储阵列的电源。

步骤

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

   此时将显示升级 SANtricity 操作系统软件页面。

4. 从 NetApp 支持站点将最新的 SANtricity 操作系统软件包下载到本地计算机。

   a. 单击 **Add new file to software repository**。

   b. 单击链接以查找最新的 **SANtricity OS Downloads**。

   c. 单击 **Download Latest Release** 链接。

   d. 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。

   8.42 及更高版本需要数字签名固件。如果您尝试下载未签名的固件，则会显示错误并中止下载。

5. 选择要用于升级控制器的 OS 软件文件和 NVSRAM 文件：

   a. 从 **Select a SANtricity OS software file** 下拉菜单中，选择您下载到本地计算机的 OS 文件。

   如果有多个可用文件，这些文件将从最新日期到最早日期进行排序。

   软件存储库列出与 Web Services Proxy 关联的所有软件文件。如果未看到要使用的文件，则可以单击链接*将新文件添加到软件存储库*，以浏览到要添加的 OS 文件所在的位置。

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

   如果存在多个文件，文件将从最新日期到最旧日期进行排序。

6. 在"兼容存储阵列"表中，查看与所选 OS 软件文件兼容的存储阵列，然后选择要升级的阵列。
   - 在"管理"视图中选定且与选定固件文件兼容的存储阵列默认选定在"兼容存储阵列"表中。
   - 无法使用所选固件文件更新的存储阵列在兼容存储阵列表中不可选择，如状态 不兼容 所示。
7. 可选： 要将软件文件传输到存储阵列而不激活它们，请选择 将 **OS** 软件传输到存储阵列，将其标记为暂存，并在稍后激活 复选框。
8. 单击 **Start**。
9. 根据您是选择立即激活还是稍后激活，执行以下操作之一：
   - 键入 **TRANSFER** 以确认要在您选择升级的阵列上传输建议的操作系统软件版本，然后单击 **Transfer**。

要激活传输的软件，请选择菜单：Upgrade Center[Activate Staged OS Software]。

- 键入 **UPGRADE** 以确认要在您选择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 **Upgrade**。

  系统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。

  升级操作期间发生以下操作：

- 升级前运行状况检查作为升级过程的一部分运行。升级前运行状况检查会评估所有存储阵列组件，以确保升级可以继续。
- 如果存储阵列的任何运行状况检查失败，则升级将停止。您可以单击省略号 (...) 并选择 **Save Log** 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 **Continue** 以继续升级。
- 您可以在升级前运行状况检查后取消升级操作。

10. 可选：*升级完成后，您可以通过单击省略号 **(...)** ，然后选择*保存日志，查看针对特定存储阵列升级的内容列表。

    此文件将以此名称保存在浏览器的 Downloads 文件夹中 `upgrade_log-<date>.json`。

在 **SANtricity Unified Manager** 中激活暂存操作系统软件

您可以选择立即激活软件文件或等待更方便的时间。此过程假设您选择稍后激活软件文件。

关于此任务

您可以在不激活固件文件的情况下传输固件文件。您可以选择稍后激活，原因如下：

- 一天中的时间 — 激活软件可能需要很长时间，因此您可能需要等待 I/O 负载较轻。控制器在激活过程中重新启动和故障转移，因此在升级完成之前，性能可能会低于正常水平。
- 包类型 — 在升级其他存储阵列上的文件之前，您可能需要在一个存储阵列上测试新软件和固件。

> 激活过程启动后无法停止。

步骤

1. 在主视图中，选择 管理。如有必要，单击状态列可在页面顶端对所有状态为"OS 升级（等待激活）"的存储阵列进行排序。
2. 选择要为其激活软件的一个或多个存储阵列，然后选择菜单：Upgrade Center[Activate Staged OS Software]。

   升级操作期间发生以下操作：

   - 升级前运行状况检查在激活过程中运行。升级前运行状况检查会评估所有存储阵列组件，以确保可以继续激活。
   - 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 **Save Log** 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 **Continue** 以继续激活。
   - 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，将进行激活。激活所需的时间取决于您的存储阵列配置和要激活的组件。

3. 可选：*激活完成后，您可以通过单击省略号 **(...)** ，然后选择 ***Save Log**，查看为特定存储阵列激活的内容列表。

   此文件将以此名称保存在浏览器的 Downloads 文件夹中 `activate_log-<date>.json`。

在 **Unified Manager** 中管理 **SANtricity** 软件存储库

软件存储库会列出与 Web Services Proxy 关联的所有软件文件。

如果未看到要使用的文件，则可以使用"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 Services Proxy 和 Unified Manager 的主机系统。您还可以选择删除软件存储库中可用的一个或多个 SANtricity 操作系统文件。

开始之前

如果您要添加 SANtricity 操作系统文件，请确保 OS 文件在本地系统上可用。

步骤

1. 在主视图中，选择 **Manage**，然后选择菜单：Upgrade Center[Manage Software Repository]。

   此时将显示"管理软件存储库"对话框。

2. 请执行以下操作之一：

选项	做这个.....
导入	a. 单击 导入。 b. 单击 **Browse**，然后导航到要添加的 OS 文件所在的位置。 OS 文件的文件名类似于 `N2800-830000-000.dlp`。 c. 选择要添加的一个或多个 OS 文件，然后单击*导入*。
删除	a. 选择要从软件存储库中删除的一个或多个 OS 文件。 b. 单击 **Delete**。

结果

如果选择导入，文件将被上传并验证。如果选择删除，文件将从软件存储库中删除。

清除 **SANtricity Unified Manager** 中的暂存操作系统软件

您可以删除暂存的 OS 软件，以确保不会在以后无意中激活待定版本。删除暂存的 OS 软件不会影响存储阵列上运行的当前版本。

步骤

1. 从主视图中，选择 管理，然后选择菜单：升级中心[Clear Staged OS Software]。

   此时将打开 Clear Staged OS Software（清除暂存操作系统软件）对话框，并列出所有已发现的带有挂起软

件或 NVSRAM 的存储系统。

2. 如果需要，请对列表中的存储系统进行筛选或排序，以便查看所有已暂存软件的系统。
3. 选中具有要清除的挂起软件的存储系统的复选框。
4. 单击 **Clear**。

   操作状态显示在对话框中。

镜像

了解 SANtricity Unified Manager 中的镜像

使用镜像功能在本地存储阵列和远程存储阵列之间异步或同步复制数据。

EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

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可能因数据损坏或丢失而导致的停机时间。同步镜像实时复制数据卷，以确保连续可用性。

了解详情：

- "镜像的工作原理"
- "镜像术语"

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。

了解详情：

- "镜像配置工作流程"
- "使用镜像的要求"
- "创建异步镜像对"
- "创建同步镜像对"

概念

了解 SANtricity 镜像

SANtricity Unified Manager 包括 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进行数据保护。

EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

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可能因数据损坏或丢失而导致的停机时间。异步镜像捕获特定时间点的主卷的状态，并仅复制自上次图像捕获以来发生变化的数据。主站点可以立即更新，辅助站点可以在带宽允许的情况下更新。当网络资源可用时，信息将被缓存并稍后发送。这种类型的镜像非常适合备份和存档等定期流程。

同步镜像实时复制数据卷，以确保连续可用性。其目的是在两个存储阵列之一发生灾难时，通过提供重要数据的副本，实现零丢失数据的恢复点目标 (RPO)。副本在任何时刻都与生产数据相同，因为每次对主卷执行写入操作时，都会对辅助卷执行写入操作。在使用在主卷上所做的更改更新辅助卷之前，主机不会收到写入成功确认。这种类型的镜像非常适合用于业务连续性目的，例如灾难恢复。

镜像类型之间的差异

下表介绍了两种镜像类型之间的主要区别。

属性	异步	同步
复制方法	时间点 — 镜像按需完成或根据用户定义的计划自动完成。	连续 — 镜像会自动连续执行，从每次主机写入中复制数据。
距离	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。	仅限于阵列之间的较短距离。通常，距离必须在本地存储阵列约 10 km（6.2 英里）范围内，以满足延迟和应用程序性能要求。
通信方法	标准 IP 或光纤通道网络。	仅光纤通道网络。
卷类型	标准或精简。	仅限标准。

镜像 **SANtricity** 配置工作流程

在 SANtricity Unified Manager 中配置异步或同步镜像，然后使用 SANtricity System Manager 管理同步。

异步镜像工作流

异步镜像涉及以下工作流程：

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，该组是本地阵列上的主卷和远程阵列上的辅助卷的容器。主卷和辅助卷称为"镜像对"。如果是首次创建镜像一致性组，请指定要执行手动同步还是计划同步。
   c. 从本地存储阵列中选择一个主卷，然后确定其保留容量。保留容量是用于复制操作的物理分配容量。
   d. 选择远程存储阵列作为传输的目标、辅助卷，然后确定其保留容量。
   e. 开始从主卷到辅助卷的初始数据传输。根据卷的大小，此初始传输可能需要几个小时。

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。完成镜像后，镜像对的状态为"最佳"。
3. 或者，您可以在 System Manager 中重新安排或手动执行后续数据传输。仅将新的和更改的数据块从主卷传输到辅助卷。

> 由于异步复制是周期性的，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。

同步镜像工作流

同步镜像涉及以下工作流程：

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. 从本地存储阵列中选择主卷。
   c. 选择远程存储阵列作为数据传输的目标，然后选择辅助卷。
   d. 选择同步和重新同步优先级。
   e. 开始从主卷到辅助卷的初始数据传输。根据卷的大小，此初始传输可能需要几个小时。
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。完成镜像后，镜像对的状态为"最佳"。这两个阵列试图通过正常操作保持同步。仅将新的和更改的块从主卷传输到辅助卷。
3. 或者，您可以在 System Manager 中更改同步设置。

> 由于同步复制是连续的，因此两个站点之间的复制链路必须提供足够的带宽容量。

了解 **SANtricity Unified Manager** 中的镜像术语

了解镜像术语如何适用于您的存储阵列。

术语	说明
本地存储阵列	本地存储阵列是您要执行操作的存储阵列。
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。组中的所有镜像对会同时重新同步，从而保持一致的恢复点。 同步镜像不使用镜像一致性组。

术语	说明
镜像对	镜像对由两个卷组成，一个主卷和一个辅助卷。 在异步镜像中，镜像对始终属于镜像一致性组。写入操作首先执行到主卷，然后复制到辅助卷。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	远程存储阵列通常被指定为辅助站点，它通常在镜像配置中保存数据的副本。
预留容量	保留容量是用于任何复制服务操作和存储对象的物理分配容量。主机无法直接读取。 这些卷是必需的，以便控制器可以持久保存将镜像保持在操作状态所需的信息。它们包含增量日志和写入时复制数据等信息。
二级卷	镜像对的辅助卷通常位于辅助站点，并保存数据的副本。
同步	在本地存储阵列和远程存储阵列之间的初始同步时进行同步。当通信中断后主卷和辅助卷不同步时，也会发生同步。当通信链路再次工作时，任何未复制的数据都将同步到辅助卷的存储阵列。

在 **SANtricity Unified Manager** 中使用镜像的要求

如果您计划配置镜像，请记住以下要求。

Unified Manager

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

存储阵列

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。
- 每个存储阵列必须有两个控制器。
- 必须在 Unified Manager 中发现两个存储阵列。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。

- 异步镜像在具有 Fibre Channel (FC) 或 iSCSI 主机端口的控制器上受支持，而同步镜像仅在具有 FC 主机端口的控制器上受支持。

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，则编号最高的端口在 HIC 上。登录到专用端口的任何主机都已注销，并且不接受任何主机登录请求。此端口上的 I/O 请求仅接受来自参与镜像操作的控制器。
- 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 结构环境。特别是，不支持 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，不必将存储阵列的任何前端 iSCSI 端口专用于异步镜像；这些端口为异步镜像流量和主机到阵列 I/O 连接共享。
- 控制器维护 iSCSI 启动程序尝试与之建立会话的远程存储系统列表。成功建立 iSCSI 连接的第一个端口用于与该远程存储阵列的所有后续通信。如果通信失败，将尝试使用所有可用端口进行新会话。

  E4000 控制器不支持 iSCSI 镜像。

- iSCSI 端口是逐个端口在阵列级别配置的。用于配置消息传递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
  - 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。

镜像卷候选项

- 在镜像对的主卷和辅助卷上，RAID 级别、缓存参数和段大小可以不同。

  对于 EF600 和 EF300 控制器，异步镜像对的主卷和辅助卷必须匹配相同的协议、托盘级别、段大小、安全类型和 RAID 级别。不符合条件的异步镜像对将不会出现在可用卷列表中。

- 辅助卷必须至少与主卷一样大。
- 一个卷只能参与一个镜像关系。
- 对于同步镜像对，主卷和辅助卷必须是标准卷。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有限制。确保存储阵列上配置的卷数小于支持的限制。当同步镜像处于活动状态时，创建的两个保留容量卷将计入卷限制。

- 对于异步镜像，主卷和辅助卷必须具有相同的 Drive Security 功能。
  - 如果主卷支持 FIPS，则辅助卷必须支持 FIPS。
  - 如果主卷具有 FDE 功能，则辅助卷必须具有 FDE 功能。
  - 如果主卷未使用 Drive Security，则辅助卷不得使用 Drive Security。
- 主卷和辅助卷不得启用 Resource Partitioning。

预留容量

异步镜像：

- 镜像对中的主卷和辅助卷需要保留容量卷来记录写入信息，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辅助卷都需要额外的保留容量，因此您必须确保镜像关系中的两个存储阵列都有可用的空闲容量。

同步镜像：

- 主卷和辅助卷需要保留容量来记录写入信息，以便从控制器重置和其他临时中断中恢复。
- 激活同步镜像时，将自动创建保留容量卷。由于镜像对中的主卷和辅助卷都需要保留容量，因此您必须确保在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

- 如果使用具有安全功能的驱动器，则主卷和辅助卷必须具有兼容的安全设置。此限制未强制执行；因此，您必须自己验证。
- 如果使用具有安全功能的驱动器，则主卷和辅助卷应使用相同的驱动器类型。此限制未强制执行；因此，您必须自己验证。
- 如果使用数据保障 (DA)，则主卷和辅助卷必须具有相同的 DA 设置。

配置镜像

在 **SANtricity Unified Manager** 中创建异步镜像对

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辅助卷。

开始之前

在创建镜像对之前，请满足 Unified Manager 的下列要求：

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

此外，请务必满足存储阵列和卷的以下要求：

- 每个存储阵列必须有两个控制器。

- 必须在 Unified Manager 中发现两个存储阵列。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。
- 您的本地和远程存储阵列通过光纤通道结构或 iSCSI 接口连接。
- 您已创建要在异步镜像关系中使用的主卷和辅助卷。
- 辅助卷必须至少与主卷一样大。

关于此任务

创建异步镜像对的过程是一个多步骤过程。

步骤 1：创建或选择镜像一致性组

在此步骤中，您创建新的镜像一致性组或选择现有的一致性组。镜像一致性组是主卷和辅助卷（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

1. 从 **Manage** 页面中，选择要用于源的本地存储阵列。
2. 选择菜单：Actions[Create Asynchronous Mirrored Pair]。

   创建异步镜像对向导打开。

3. 选择现有镜像一致性组或创建新镜像一致性组。

   要选择现有组，请确保选择了 现有镜像一致性组，然后从表中选择该组。一致性组可以包括多个镜像对。

   要创建新组，请执行以下操作：

   a. 选择 **A new mirror consistency group**，然后单击 **Next**。
   b. 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 30 个字符，也不能包含空格。
   c. 选择要与本地存储阵列建立镜像关系的远程存储阵列。

      如果您的远程存储阵列受密码保护，系统将提示输入密码。

   d. 选择是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，如果要稍后执行重新同步，则必须为主存储阵列启动 System Manager，然后转到菜单：Storage[Asynchronous Mirroring]，从 **Mirror Consistency Groups** 选项卡中选择组，然后选择菜单：More[Manually resynchronize]。
      - 自动 — 选择从上一次更新开始到下一次更新开始的所需时间间隔，以 分钟、小时 或 天 为单位。例如，如果同步间隔设置为 30 分钟，并且同步过程从下午 4:00 开始，则下一个过程从下午 4:30 开始。
   e. 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（由剩余容量的百分比定义）。
- 对于自动同步，您可以设置三种警报方法：当同步在特定时间长度内未完成时，当远程阵列上的恢复点数据早于特定时间限制时，以及当保留容量接近特定阈值时（由剩余容量的百分比定义）。

4. 选择 **Next** 并转到 步骤 2：选择主卷。

   如果定义了新的镜像一致性组，Unified Manager 将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。

   如果 Unified Manager 在本地存储阵列上成功创建镜像一致性组，但未能在远程存储阵列上创建它，它将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，则必须手动删除它。

步骤 **2**：选择主卷

在此步骤中，选择要在镜像关系中使用的主卷，并分配其保留容量。当您在本地存储阵列上选择主卷时，系统将显示该镜像对的所有合格卷的列表。任何不符合使用条件的卷都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扮演主要角色。

步骤

1. 从符合条件的卷列表中，选择要用作主卷的卷，然后单击 **Next** 以分配保留容量。
2. 从符合条件的候选项列表中，为主卷选择预留容量。

   请记住以下准则：

   - 保留容量的默认设置为基本卷容量的 20%，通常此容量就足够了。如果更改百分比，请单击 **Refresh Candidates**。
   - 所需的容量因 I/O 写入主卷的频率和大小以及保留容量所需的时间而异。
   - 一般来说，如果存在以下一种或两种情况，请为保留容量选择更大的容量：
     - 您打算将镜像对保留很长一段时间。
     - 由于繁重的 I/O 活动，主卷上的大部分数据块将发生变化。使用历史性能数据或其他操作系统实用程序来帮助您确定主卷的典型 I/O 活动。

3. 选择 **Next** 并转到 步骤 3：选择辅助卷。

步骤 **3**：选择辅助卷

在此步骤中，选择要在镜像关系中使用的辅助卷，并分配其保留容量。当您在远程存储阵列上选择辅助卷时，系统将显示该镜像对的所有合格卷的列表。任何不符合使用条件的卷都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担任辅助角色。

步骤

1. 从符合条件的卷列表中，选择要用作镜像对中的辅助卷的卷，然后单击 **Next** 以分配保留容量。
2. 从符合条件的候选项列表中，为二级卷选择预留容量。

   请记住以下准则：

- 保留容量的默认设置为基本卷容量的 20%，通常此容量就足够了。如果更改百分比，请单击 **Refresh Candidates**。
- 所需的容量因 I/O 写入主卷的频率和大小以及保留容量所需的时间而异。
- 一般来说，如果存在以下一种或两种情况，请为保留容量选择更大的容量：
  - 您打算将镜像对保留很长一段时间。
  - 由于繁重的 I/O 活动，主卷上的大部分数据块将发生变化。使用历史性能数据或其他操作系统实用程序来帮助您确定主卷的典型 I/O 活动。

3. 选择 **Finish** 以完成异步镜像序列。

结果

Unified Manager 执行以下操作：

- 开始本地存储阵列和远程存储阵列之间的初始同步。
- 在本地存储阵列和远程存储阵列上为镜像对创建保留容量。

如果要镜像的卷是精简卷，则在初始同步期间，仅将调配的块（分配的容量而不是报告的容量）传输到辅助卷。这样会减少必须传输才能完成初始同步的数据量。

在 **SANtricity Unified Manager** 中创建同步镜像对

要配置同步镜像，请创建镜像对，其中包括本地阵列上的主卷和远程阵列上的辅助卷。

此功能在 EF600/EF600C 或 EF300/EF300C 存储系统中不可用。

开始之前

在创建镜像对之前，请满足 Unified Manager 的下列要求：

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

此外，请务必满足存储阵列和卷的以下要求：

- 计划用于镜像的两个存储阵列可在 Unified Manager 中找到。
- 每个存储阵列必须有两个控制器。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 您的本地和远程存储阵列通过 Fibre Channel 结构连接。
- 您已创建要在同步镜像关系中使用的主卷和辅助卷。
- 主卷必须为标准卷。它不能是精简卷或快照卷。

- 辅助卷必须为标准卷。它不能是精简卷或快照卷。
- 辅助卷应至少与主卷一样大。

关于此任务

创建同步镜像对的过程是一个多步骤过程。

步骤 1：选择主卷

在此步骤中，选择要在同步镜像关系中使用的主卷。当您在本地存储阵列上选择主卷时，系统将显示该镜像对的所有合格卷的列表。不符合使用条件的任何卷都不会显示在该列表中。您选择的卷在镜像关系中占有主要角色。

步骤

1. 从 **Manage** 页面中，选择要用于源的本地存储阵列。
2. 选择菜单：Actions[Create Synchronous Mirrored Pair]。

   创建同步镜像对向导打开。

3. 从符合条件的卷列表中，选择要用作镜像中主卷的卷。
4. 选择 **Next** 并转到 步骤 2：选择辅助卷。

步骤 2：选择辅助卷

在此步骤中，选择要在镜像关系中使用的辅助卷。当您在远程存储阵列上选择辅助卷时，系统将显示该镜像对的所有合格卷的列表。任何不符合使用条件的卷都不会显示在该列表中。您选择的卷将保留镜像关系中的次要角色。

步骤

1. 选择要与本地存储阵列建立镜像关系的远程存储阵列。

   如果您的远程存储阵列受密码保护，系统将提示输入密码。

   - 存储阵列按其存储阵列名称列出。如果您尚未命名存储阵列，则它将被列为"unnamed"。
   - 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。
2. 从符合条件的卷列表中，选择要用作镜像中辅助卷的卷。

   如果选择的辅助卷的容量大于主卷，则可用容量将限于主卷的大小。

3. 单击 **Next** 并转到 步骤 3：选择同步设置。

步骤 3：选择同步设置

在此步骤中，您可以选择确定通信中断后数据同步方式的设置。您可以设置主卷的控制器所有者在通信中断后将数据与辅助卷重新同步的优先级。您还必须选择重新同步策略，手动或自动。

步骤

1. 使用滑块栏设置同步优先级。

   与服务 I/O 请求相比，同步优先级确定通信中断后有多少系统资源用于完成初始同步和重新同步操作。

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：Storage[Synchronous Mirroring > More > Edit Settings] 来修改主卷上的速率。

有五个同步优先级：

- 最低
- 低
- 中
- 高
- 最高

如果将同步优先级设置为最低等级，则会优先处理 I/O 活动，而重新同步操作则需要更长的时间。如果将同步优先级设置为最高等级，则会优先处理重新同步操作，而存储阵列的 I/O 活动可能受到影响。

2. 选择是手动还是自动重新同步远程存储阵列上的镜像对。
   - **Manual**（推荐选项）-- 选择此选项可要求在通信恢复到镜像对后手动恢复同步。此选项为恢复数据提供了最佳机会。
   - 自动 — 选择此选项可在通信恢复到镜像对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：Storage[Synchronous Mirroring]，突出显示表中的镜像对，然后选择 **More** 下的 **Resume**。
3. 单击 **Finish** 完成同步镜像序列。

结果

一旦镜像被激活，系统将执行以下操作：

- 开始本地存储阵列和远程存储阵列之间的初始同步。
- 设置同步优先级和重新同步策略。
- 保留控制器 HIC 的最高编号端口用于镜像数据传输。

  此端口上接收的 I/O 请求仅接受来自镜像对中辅助卷的远程首选控制器所有者。（允许在主卷上进行预留。）
- 创建两个保留容量卷，每个控制器一个，用于记录写入信息以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，如果将卷置于池中，则为每个卷保留 4 GiB。

完成后

转到 System Manager 并选择菜单：主页[查看正在进行的操作]以查看同步镜像操作的进度。此操作可能很长，并可能影响系统性能。

SANtricity Unified Manager 的存储镜像常见问题

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

在创建镜像一致性组之前，我需要知道什么？

在创建镜像一致性组之前，请遵循这些指南。

满足 Unified Manager 的以下要求：

- Web Services Proxy 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您自己的安全证书，并导航到菜单：Certificate[Certificate Management]。

此外，请务必满足存储阵列的以下要求：

- 必须在 Unified Manager 中发现两个存储阵列。
- 每个存储阵列必须有两个控制器。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 您的本地和远程存储阵列通过光纤通道结构或 iSCSI 接口连接。

EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

创建镜像对之前，我需要知道什么？

在创建镜像对之前，请遵循以下指南。

- 您必须有两个存储阵列。
- 每个存储阵列必须有两个控制器。
- 必须在 Unified Manager 中发现两个存储阵列。
- 主阵列和辅助阵列中的每个控制器都必须配置以太网管理端口，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。（它们可以各自运行不同的 OS 版本。）
- 您必须知道本地和远程存储阵列的密码。
- 必须在远程存储阵列上具有足够的可用容量，才能创建等于或大于要镜像的主卷的辅助卷。
- 异步镜像在具有 Fibre Channel (FC) 或 iSCSI 主机端口的控制器上受支持，而同步镜像仅在具有 FC 主机端口的控制器上受支持。

EF600/EF600C 或 EF300/EF300C 存储系统上不提供同步镜像。

为什么要更改此百分比？

对于异步镜像操作，保留容量通常为基本卷的 20%。通常这个容量就足够了。

所需的容量因向基本卷写入 I/O 的频率和大小以及您打算使用存储对象的复制服务操作的时长而异。一般来说，如果存在以下一种或两种情况，请为保留容量选择较大的百分比：

- 如果特定存储对象的复制服务操作的生命周期非常长。
- 如果由于大量 I/O 活动，基本卷上的大量数据块将发生变化。使用历史性能数据或其他操作系统实用程序来帮助您确定基本卷的典型 I/O 活动。

为什么我看到多个预留容量候选项？

如果池或卷组中有多个卷符合您为存储对象选择的容量百分比量，则您将看到多个候选项。

您可以通过更改要在基本卷上保留用于复制服务操作的物理驱动器空间百分比来刷新推荐候选列表。根据您的选择显示最佳候选。

为什么我没有看到所有的卷？

为镜像对选择主卷时，列表会显示所有符合条件的卷。

不符合使用条件的任何卷都不会显示在该列表中。由于以下任何原因，卷可能不符合条件：

- 卷不是最佳的。
- 此卷已参与镜像关系。
- 对于同步镜像，镜像对中的主卷和辅助卷必须是标准卷。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。

> 对于 EF600 和 EF300 控制器，异步镜像对的主卷和辅助卷必须匹配相同的协议、托盘级别、段大小、安全类型和 RAID 级别。不符合条件的异步镜像对将不会出现在可用卷列表中。

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辅助卷时，列表会显示该镜像对的所有合格卷。

任何不符合使用条件的卷都不会显示在该列表中。卷可能因以下任何原因而不符合条件：

- 此卷是非标准卷，例如快照卷。
- 卷不是最佳的。
- 此卷已参与镜像关系。
- 对于异步镜像，主卷和辅助卷之间的精简卷属性不匹配。
- 如果使用数据保障 (DA)，则主卷和辅助卷必须具有相同的 DA 设置。
  - 如果主卷启用了 DA，则辅助卷必须启用 DA。
  - 如果主卷未启用 DA，则辅助卷不得启用 DA。
- 对于异步镜像，主卷和辅助卷必须具有相同的 Drive Security 功能。
  - 如果主卷支持 FIPS，则辅助卷必须支持 FIPS。
  - 如果主卷具有 FDE 功能，则辅助卷必须具有 FDE 功能。
  - 如果主卷未使用 Drive Security，则辅助卷不得使用 Drive Security。

同步优先级对同步速率有何影响?

同步优先级定义了相对于系统性能为同步活动分配的处理时间。

主卷的控制器所有者在后台执行此操作。同时，控制器所有者处理对主卷的本地 I/O 写入和对辅助卷的相关远程写入。由于重新同步会从 I/O 活动中转移控制器处理资源，因此重新同步可能会对主机应用程序产生性能影响。

请记住这些准则，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。

可提供以下优先级费率：

- 最低
- 低
- 中
- 高
- 最高

最低优先级速率支持系统性能，但重新同步需要更长的时间。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。

这些指南大致反映了优先级之间的差异。

完全同步的优先级	与最高同步速率相比所用时间
最低	大约是最高优先级速率的八倍长。
低	大约是最高优先级速率的六倍长。
中	长度约为最高优先级速率的三倍半。
高	长度约为最高优先级速率的两倍。

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?

建议手动重新同步，因为它允许您以一种为恢复数据提供最佳机会的方式管理重新同步过程。

如果使用自动重新同步策略，并且在重新同步过程中发生间歇性通信问题，则辅助卷上的数据可能会暂时损坏。当重新同步完成时，数据将被更正。

证书

证书概述

证书管理允许您创建证书签名请求 (CSR)、导入证书和管理现有证书。

什么是证书?

Certificates 是用于识别网站和服务器等在线实体的数字文件，用于在互联网上进行安全通信。有两种类型的证书：*signed certificate* 由证书颁发机构 (CA) 进行验证，*self-signed certificate* 由实体的所有者而不是第三方进行验证。

了解详情：

- "证书的工作原理"
- "证书术语"

如何配置证书?

从证书管理，您可以为托管 Unified Manager 的管理站配置证书，也可以为阵列中的控制器导入证书。

了解详情：

- "为管理系统使用 CA 签名的证书"
- "导入阵列的证书"

概念

证书在 **SANtricity Unified Manager** 中的工作原理

证书是数字文件，用于识别在线实体（如网站和服务器），以便在互联网上进行安全通信。

已签名证书

证书确保 Web 通信仅在指定的服务器和客户端之间以加密形式私下传输且不被更改。使用 Unified Manager，您可以管理主机管理系统上的浏览器以及发现的存储阵列中的控制器的证书。

证书可以由受信任的颁发机构签名，也可以是自签名的。"签名"仅仅意味着有人验证了所有者的身份，并确定他们的设备可以被信任。存储阵列在每个控制器上都附带自动生成的自签名证书。您可以继续使用自签名证书，也可以获取 CA 签名证书，以便在控制器和主机系统之间建立更安全的连接。

> 虽然 CA 签名的证书可以提供更好的安全保护（例如，防止中间人攻击），但如果您拥有大型网络，它们也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，而不是在生产环境中。

签名的证书由证书颁发机构 (CA) 进行验证，CA 是受信任的第三方组织。签名证书包括有关实体所有者（通常是服务器或网站）、证书颁发日期和到期日期、实体的有效域以及由字母和数字组成的数字签名的详细信息。

当您打开浏览器并输入网址时，系统会在后台执行证书检查过程，以确定您连接的网站是否包含有效的 CA 签名证书。通常，使用签名证书保护的站点在地址中包含挂锁图标和 https 标识。如果您尝试连接到不包含 CA 签名证书的网站，浏览器将显示该网站不安全的警告。

CA 在申请过程中会采取步骤验证您的身份。他们可能会向您注册的公司发送电子邮件，验证您的公司地址，并执行 HTTP 或 DNS 验证。申请流程完成后，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：

- **Root** — 层次结构的顶端是根证书，其中包含用于对其他证书进行签名的私钥。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。
- 中级 — 从根分支出来的是中级证书。CA 颁发一个或多个中级证书，以充当受保护的根证书和服务器证书之间的中间人。
- 服务器 — 链条底部是服务器证书，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单独的服务器证书。

自签名证书

存储阵列中的每个控制器都包含一个预安装的自签名证书。自签名证书类似于 CA 签名的证书，但它由实体的所有者而不是第三方进行验证。与 CA 签名证书一样，自签名证书包含自己的私钥，并确保数据经过加密并通过服务器和客户端之间的 HTTPS 连接发送。

浏览器不"信任"自签名证书。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的链接，以便继续访问网站；通过这样做，您基本上接受了自签名证书。

Unified Manager 证书

Unified Manager 界面与 Web Services Proxy 一起安装在主机系统上。当您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是受信任的来源。如果浏览器未找到服务器的 CA 签名证书，则会打开一条警告消息。然后，您可以继续访问网站以接受该会话的自签名证书。或者，您可以从 CA 获得签名的数字证书，这样您就不会再看到警告消息。

控制器证书

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，也可以导入控制器的 CA 签名证书，以便 Web Services Proxy 服务器可以验证来自这些控制器的传入客户端请求。

了解 **SANtricity Unified Manager** 中的证书术语

以下术语适用于证书管理。

术语	说明
CA	证书颁发机构 (CA) 是颁发电子文档（称为数字证书）以实现 Internet 安全的受信任实体。这些证书可以识别网站所有者，从而实现客户端和服务器之间的安全连接。
CSR	证书签名请求 (CSR) 是从申请人发送到证书颁发机构 (CA) 的消息。CSR 验证 CA 颁发证书所需的信息。
证书	出于安全目的，证书可识别站点的所有者，从而防止攻击者模拟站点。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）的受信任实体的身份。
证书链	为证书添加安全层的文件层次结构。通常，链包括层次结构顶端的一个根证书、一个或多个中间证书以及标识实体的服务器证书。

术语	说明
中间证书	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，以充当受保护的根证书和服务器证书之间的中间人。
密钥库	密钥库是主机管理系统上的存储库，其中包含私钥以及相应的公钥和证书。这些密钥和证书标识您自己的实体，例如控制器。
根证书	根证书位于证书链中层次结构的顶端，并包含用于对其他证书进行签名的私钥。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。
已签名证书	由证书颁发机构 (CA) 验证的证书。此数据文件包含一个私钥，并确保通过 HTTPS 连接在服务器和客户端之间以加密形式发送数据。此外，签名证书包括有关实体所有者（通常是服务器或网站）的详细信息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中。也称为"CA 签名证书"或"管理证书"。
自签名证书	自签名证书由实体的所有者验证。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。自签名证书不使用与 CA 签名证书相同的信任链，因此最常用于测试环境。也称为"预安装"证书。
服务器证书	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单独的服务器证书。
信任存储	信任存储区是一个存储库，其中包含来自受信任的第三方（例如 CA）的证书。

为管理系统使用 **CA** 签名的证书

您可以获取和导入 CA 签名的证书，以安全访问托管 SANtricity Unified Manager 的管理系统。

开始之前

必须使用包含 Security admin 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 签名的证书是一个三步过程。

步骤 **1**：完成 **CSR** 文件

您必须首先生成证书签名请求 (CSR) 文件，该文件标识您的组织和安装 Web Services Proxy 和 Unified Manager 的主机系统。

或者，您可以使用 OpenSSL 等工具生成 CSR 文件，然后跳到步骤 2：提交 CSR 文件。

步骤

1. 选择 **Certificate Management**。

2. 在管理选项卡中，选择 **Complete CSR**。
3. 输入以下信息，然后单击 **Next**：
   - 组织 — 贵公司或组织的完整法定名称。包括后缀，例如 Inc. 或 Corp.。
   - 组织单位（可选） — 处理证书的组织部门。
   - 城市/地区 — 您的主机系统或企业所在的城市。
   - 州/地区（可选） — 您的主机系统或业务所在的州或地区。
   - 国家/地区 **ISO** 代码 — 您所在国家/地区的两位数 ISO（International Organization for Standardization）代码，例如 US。
4. 输入有关安装 Web Services Proxy 的主机系统的以下信息：
   - 通用名称 — 安装 Web Services Proxy 的主机系统的 IP 地址或 DNS 名称。确保此地址正确；它必须与您在浏览器中输入的访问 Unified Manager 的内容完全匹配。不包括 http:// 或 https://。DNS 名称不能以通配符开头。
   - 备用 **IP** 地址 — 如果通用名称是 IP 地址，您可以选择输入主机系统的任何其他 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 — 如果公用名称是 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。如果没有其他 DNS 名称，但您在第一个字段中输入了 DNS 名称，请将该名称复制到此处。DNS 名称不能以通配符开头。
5. 确保主机信息正确无误。如果不正确，当您尝试导入证书时，从 CA 返回的证书将失败。
6. 单击 **Finish**。
7. 转至 步骤 2：提交 CSR 文件。

步骤 **2**：提交 **CSR** 文件

创建证书签名请求 (CSR) 文件后，将其发送到证书颁发机构 (CA)，以接收托管 Unified Manager 和 Web Services Proxy 的系统的签名管理证书。

E-Series 系统要求签名证书采用 PEM 格式（Base64 ASCII 编码），其中包括以下文件类型：.pem、.crt、.cer 或 .key。

步骤

1. 找到下载的 CSR 文件。

   下载的文件夹位置取决于您的浏览器。

2. 将 CSR 文件提交给 CA（例如，Verisign 或 DigiCert），并以 PEM 格式请求已签名的证书。

   *向 CA 提交 CSR 文件后，请勿重新生成其他 CSR 文件。*每当您生成 CSR 时，系统都会创建私钥和公钥对。公钥是 CSR 的一部分，而私钥则保存在系统的密钥库中。当您收到签名的证书并导入它们时，系统将确保私钥和公钥都是原始对。如果密钥不匹配，则签名的证书将不起作用，您必须向 CA 请求新证书。

3. 当 CA 返回已签名的证书时，请转到 步骤 3：导入管理证书。

步骤 **3**：导入管理证书

收到来自证书颁发机构 (CA) 的签名证书后，将证书导入安装了 Web Services Proxy 和 Unified Manager 界面的主机系统中。

开始之前

- 您已收到来自 CA 的签名证书。这些文件包括根证书、一个或多个中间证书和服务器证书。
- 如果 CA 提供了一个链接的证书文件（例如 .p7b 文件），则必须将链接的文件解压缩为单个文件：根证书、一个或多个中间证书和服务器证书。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 Base-64 编码。导出完成后，将显示链中每个证书文件的 CER 文件。
- 已将证书文件复制到运行 Web Services Proxy 的主机系统。

步骤

1. 选择 **Certificate Management**。
2. 从 Management 选项卡中，选择 **Import**。

   此时将打开一个用于导入证书文件的对话框。

3. 单击 **Browse** 首先选择根证书文件和中间证书文件，然后选择服务器证书。如果从外部工具生成了 CSR，则还必须导入与 CSR 一起创建的私钥文件。

   文件名显示在对话框中。

4. 单击 **Import**。

结果

文件已上传并验证。证书信息显示在 Certificate Management 页面上。

重置管理证书

您可以将管理证书还原为原始的出厂自签名状态。

开始之前

必须使用包含 Security admin 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

此任务从安装了 Web Services Proxy 和 Unified Manager 的主机系统中删除当前管理证书。重置证书后，主机系统恢复使用自签名证书。

步骤

1. 选择 **Settings > Certificates**。
2. 选择 **Array Management** 选项卡，然后选择 **Reset**。

   将打开确认重置管理证书对话框。

3. 在字段中键入 `reset`，然后单击*重置*。

刷新浏览器后，浏览器可能会阻止对目标站点的访问，并报告该站点正在使用 HTTP Strict Transport Security。当您切换回自签名证书时会出现这种情况。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

系统恢复使用来自服务器的自签名证书。因此，系统会提示用户手动接受其会话的自签名证书。

使用阵列证书

在 **SANtricity Unified Manager** 中导入阵列的证书

如有必要，您可以导入存储阵列的证书，以便它们可以通过托管 SANtricity Unified Manager 的系统进行身份验证。证书可以由证书颁发机构 (CA) 签名，也可以进行自签名。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。
- 如果要导入受信任的证书，则必须使用 System Manager 为存储阵列控制器导入证书。

步骤

1. 选择 **Certificate Management**。
2. 选择 **Trusted** 选项卡。

   此页面显示存储阵列报告的所有证书。

3. 选择 **Import › Certificates** 以导入 CA 证书或 **Import › Self-signed storage array certificates** 以导入自签名证书。

   要限制视图，您可以使用 **Show certificates that are…** 筛选字段，或者可以通过单击其中一个列标题对证书行进行排序。

4. 在对话框中，选择证书，然后单击 **Import**。

   证书已上传并验证。

在 **SANtricity Unified Manager** 中删除可信证书

您可以删除一个或多个不再需要的证书，例如过期的证书。

开始之前

请先导入新证书，然后再删除旧证书。

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

步骤

1. 选择 **Certificate Management**。

2. 选择 **Trusted** 选项卡。
3. 在表中选择一个或多个证书，然后单击 删除。

   Delete 功能不适用于预安装的证书。

   确认删除受信任证书对话框打开。

4. 确认删除，然后单击 **Delete**。

   证书已从表中删除。

解决不受信任的证书

当存储阵列尝试与 SANtricity Unified Manager 建立安全连接，但连接无法确认为安全时，会发生不受信任的证书。

从"证书"页面，您可以通过从存储阵列导入自签名证书或导入由受信任的第三方颁发的证书颁发机构 (CA) 证书来解决不受信任的证书。

开始之前

- 您必须使用包含 Security Admin 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了证书签名请求（.CSR 文件），并将其发送到 CA。
  - CA 返回了受信任的证书文件。
  - 证书文件在您的本地系统上可用。

关于此任务

如果满足以下任一情况，则可能需要安装其他受信任的 CA 证书：

- 您最近添加了一个存储阵列。
- 一个或两个证书已过期。
- 一个或两个证书都被吊销。
- 一个或两个证书都缺少根证书或中间证书。

步骤

1. 选择 **Certificate Management**。
2. 选择 **Trusted** 选项卡。

   此页面显示存储阵列报告的所有证书。

3. 选择 **Import › Certificates** 以导入 CA 证书或 **Import › Self-Signed storage array certificates** 以导入自签名证书。

   要限制视图，您可以使用 **Show certificates that are…** 筛选字段，或者可以通过单击其中一个列标题对证书行进行排序。

4. 在对话框中，选择证书，然后单击 **Import**。

   证书已上传并验证。

管理证书

查看证书

您可以查看证书的摘要信息，包括使用证书的组织、颁发证书的机构、有效期和指纹（唯一标识符）。

开始之前

必须使用包含 Security admin 权限的用户配置文件登录。否则，不会显示证书功能。

步骤

1. 选择 **Certificate Management**。
2. 选择以下选项卡之一：
   - **Management** — 显示托管 Web Services Proxy 的系统的证书。管理证书可以自签名或由证书颁发机构 (CA) 批准。它允许安全访问 Unified Manager。
   - 受信任 — 显示 Unified Manager 可以访问的存储阵列和其他远程服务器（如 LDAP 服务器）的证书。证书可以从证书颁发机构 (CA) 颁发，也可以进行自签名。
3. 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**。

在 **SANtricity Unified Manager** 中导出证书

您可以导出证书以查看其完整详细信息。

开始之前

要打开导出的文件，必须具有证书查看器应用程序。

步骤

1. 选择 **Certificate Management**。
2. 选择以下选项卡之一：
   - **Management** — 显示托管 Web Services Proxy 的系统的证书。管理证书可以自签名或由证书颁发机构 (CA) 批准。它允许安全访问 Unified Manager。
   - 受信任 — 显示 Unified Manager 可以访问的存储阵列和其他远程服务器（如 LDAP 服务器）的证书。证书可以从证书颁发机构 (CA) 颁发，也可以进行自签名。
3. 从页面中选择一个证书，然后单击该行末尾的省略号。
4. 单击 **Export**，然后保存证书文件。
5. 在证书查看器应用程序中打开文件。

访问管理

了解 SANtricity Unified Manager 访问管理

访问管理是在 SANtricity Unified Manager 中配置用户身份验证的方法。

有哪些可用的身份验证方法?

以下身份验证方法可用：

- 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和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 (IdP) 进行管理。

了解详情：

- "访问管理的工作原理"
- "访问管理术语"
- "映射角色的权限"
- "SAML"

如何配置 **Access Management**?

SANtricity 软件已预配置为使用本地用户角色。如果要使用 LDAP，可以在"访问管理"页面下进行配置。

了解详情：

- "使用本地用户角色进行访问管理"
- "使用目录服务进行访问管理"
- "配置 SAML"

概念

访问管理在 **SANtricity Unified Manager** 中的工作原理

使用访问管理在 SANtricity Unified Manager 中建立用户身份验证。

配置工作流

访问管理配置的工作原理如下：

1. 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。

首次登录时，用户名 `admin`会自动显示且无法更改。 `admin`用户可以完全访问系统中的所有功能。首次登录时必须设置密码。

2. 管理员导航到用户界面中的访问管理，其中包括预配置的本地用户角色。这些角色是 RBAC（基于角色的访问控制）功能的实现。
3. 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。管理员可以将这些本地用户角色用作单一的身份验证方法，也可以将其与目录服务结合使用。除了为用户设置密码外，无需进行其他配置。
   - 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** — 身份验证通过身份提供程序 (IdP) 使用安全断言标记语言 (SAML) 2.0 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 用户映射到嵌入在存储阵列中的本地用户角色。
4. 管理员为用户提供 Unified Manager 的登录凭据。
5. 用户通过输入其凭据登录到系统。在登录过程中，系统会执行以下后台任务：
   - 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功能的访问权限。
   - 在顶部横幅中显示用户名。

Unified Manager 中可用的功能

对功能的访问取决于用户分配的角色，包括以下内容：

- **Storage admin** — 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。
- 安全管理员 — 访问 Access Management 和 Certificate Management 中的安全配置。
- **Support admin** — 访问存储阵列、故障数据和 MEL 事件上的所有硬件资源。无法访问存储对象或安全配置。
- **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

不可用的功能要么变为灰色，要么不显示在用户界面中。

了解 SANtricity Unified Manager 访问管理术语

了解 Access Management 条款如何适用于 SANtricity Unified Manager。

术语	说明
Active Directory	Active Directory (AD) 是一种 Microsoft 目录服务，它将 LDAP 用于 Windows 域网络。
绑定	绑定操作用于向目录服务器验证客户端。绑定通常需要帐户和密码凭据，但有些服务器允许匿名绑定操作。

术语	说明
CA	证书颁发机构 (CA) 是颁发电子文档（称为数字证书）以实现 Internet 安全的受信任实体。这些证书可以识别网站所有者，从而实现客户端和服务器之间的安全连接。
证书	出于安全目的，证书可识别站点的所有者，从而防止攻击者模拟站点。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）的受信任实体的身份。
LDAP	轻型目录访问协议（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。
RBAC	基于角色的访问控制 (RBAC) 是一种基于单个用户的角色来调节对计算机或网络资源的访问的方法。Unified Manager 包括预定义的角色。
SAML	Security Assertion Markup Language (SAML) 是用于两个实体之间的身份验证和授权的基于 XML 的标准。SAML 允许多因素身份验证，其中用户必须提供两个或多个项目来证明其身份（例如密码和指纹）。存储阵列的嵌入式 SAML 功能符合 SAML2.0 的身份断言、身份验证和授权。
SSO	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。
Web Services Proxy	Web Services Proxy 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 界面可与 Web Services Proxy 一起使用。

映射角色的权限

RBAC（基于角色的访问控制）功能包括具有映射到一个或多个角色的预定义用户。每个角色都包含访问 SANtricity Unified Manager 中任务的权限。

这些角色为用户提供对任务的访问权限，如下所示：

- **Storage admin** — 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。
- 安全管理员 — 访问 Access Management 和 Certificate Management 中的安全配置。
- **Support admin** — 访问存储阵列、故障数据和 MEL 事件上的所有硬件资源。无法访问存储对象或安全配置。
- **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

如果用户没有某个功能的权限，则该功能要么不可供选择，要么不显示在用户界面中。

使用 **SANtricity Unified Manager** 中的本地用户角色进行访问管理

管理员可以使用 SANtricity Unified Manager 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"。

配置工作流

本地用户角色已在系统中预配置。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：

1. 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。

> `admin` 用户可以完全访问系统中的所有功能。

2. 管理员审阅用户配置文件，这些配置文件是预定义的，无法修改。
3. 可选地，管理员为每个用户配置文件分配新密码。
4. 用户使用其分配的凭据登录到系统。

管理

当仅使用本地用户角色进行身份验证时，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。
- 允许用户无需密码即可登录。

使用 **SANtricity Unified Manager** 中的目录服务进行访问管理

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。

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：

1. 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。

> `admin` 用户可以完全访问系统中的所有功能。

2. 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。
3. 如果 LDAP 服务器使用安全协议 (LDAPS)，管理员将上传证书颁发机构 (CA) 证书链，以便在 LDAP 服务器和安装 Web Services Proxy 的主机系统之间进行身份验证。
4. 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。
5. 管理员测试 LDAP 服务器和 Web Services Proxy 之间的连接。
6. 用户使用其分配的 LDAP/目录服务凭据登录到系统。

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。
- 允许用户无需密码即可登录。

在 **SANtricity Unified Manager** 中使用 **SAML** 进行访问管理

对于访问管理，管理员可以使用嵌入在数组中的安全断言标记语言 (SAML) 2.0 功能。

配置工作流

SAML 配置的工作原理如下：

1. 管理员使用包含 Security Admin 权限的用户配置文件登录到 Unified Manager。

   此 `admin`用户具有对 System Manager 中所有功能的完全访问权限。

2. 管理员转到 Access Management 下的 **SAML** 选项卡。
3. 管理员配置与身份提供商 (IdP) 的通信。IdP 是用于向用户请求凭据并确定用户是否成功通过身份验证的外部系统。要配置与存储阵列的通信，管理员从 IdP 系统下载 IdP 元数据文件，然后使用 Unified Manager 将文件上传到存储阵列。
4. 管理员在服务提供商和 IdP 之间建立信任关系。服务提供商控制用户授权；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，管理员从 IdP 系统将元数据文件导入 IdP。

   管理员还应确保 IdP 支持在身份验证时返回名称 ID 的功能。

5. 管理员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。
6. 管理员测试 IdP URL 的 SSO 登录。此测试确保存储阵列和 IdP 可以通信。

   启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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。

7. 在 Unified Manager 中，管理员为存储阵列启用 SAML。
8. 用户使用其 SSO 凭据登录到系统。

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：

- 修改或创建新的角色映射
- 导出 Service Provider 文件

访问限制

启用 SAML 后，用户无法从旧版 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)
- 软件开发工具包 (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

使用本地用户角色

查看本地用户角色

从本地用户角色选项卡，您可以查看用户到默认角色的映射。这些映射是在 SANtricity Unified Manager 的 Web Services Proxy 中强制实施的 RBAC（基于角色的访问控制）的一部分。

开始之前

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。

关于此任务

无法更改用户和映射。只能修改密码。

步骤

1. 选择 **Access Management**。
2. 选择 **Local User Roles** 选项卡。

   用户显示在表中：

   - **admin** — 有权访问系统中所有功能的超级管理员。此用户包括所有角色。
   - **storage** — 负责所有存储配置的管理员。此用户包括以下角色：Storage Admin、Support Admin 和 Monitor。
   - **security** — 负责安全配置的用户，包括 Access Management 和 Certificate Management。此用户包括以下角色：Security Admin 和 Monitor。
   - **support** — 负责硬件资源、故障数据和固件升级的用户。此用户包括以下角色：Support Admin 和 Monitor。
   - **monitor** — 对系统具有只读访问权限的用户。此用户仅包括 Monitor 角色。
   - **rw**（读/写）-- 此用户包括以下角色：Storage Admin、Support Admin 和 Monitor。
   - **ro**（只读）-- 此用户仅包括 Monitor 角色。

在 **SANtricity Unified Manager** 中更改本地用户配置文件的密码

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都必须满足或超过当前设置的最低密码要求（在 View/Edit Settings 中）。
- 密码区分大小写。
- 设置密码后，不会从密码中删除尾随空格。如果密码中包含空格，请务必包含空格。
- 为提高安全性，请至少使用 15 个字母数字字符，并经常更改密码。

步骤

1. 选择 **Access Management**。
2. 选择 **Local User Roles** 选项卡。
3. 从表中选择一个用户。

   "更改密码"按钮变为可用。

4. 选择 **Change Password**。

   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，则可以选中此复选框，要求用户输入密码以访问系统。
6. 在两个字段中输入选定用户的新密码。
7. 输入您的本地管理员密码以确认此操作，然后单击 **Change**。

结果

如果用户当前已登录，密码更改将导致用户的活动会话终止。

在 **SANtricity Unified Manager** 中更改本地用户密码设置

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无需输入密码即可访问系统。

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的本地用户密码。

- 本地用户密码所需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。
- 如果您希望本地用户在不输入密码的情况下访问系统，请不要设置密码的最小长度。

步骤

1. 选择 **Access Management**。
2. 选择 **Local User Roles** 选项卡。
3. 选择 **View/Edit Settings**。

   此时将打开本地用户密码设置对话框。

4. 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"要求所有本地用户密码至少为"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，然后使用微调框为所有本地用户密码设置所需的最小长度。

     任何新的本地用户密码必须满足或超过当前设置。

5. 单击 **Save**。

使用目录服务

在 **SANtricity Unified Manager** 中添加目录服务器

要配置访问管理的身份验证，请在 LDAP 服务器和运行 SANtricity Unified Manager Web Services Proxy 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

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 必须在您的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 证书由非标准签名机构签名，则还必须上传该证书以进行身份验证。如果具有绑定帐户的凭据，还可以输入用户帐户名和密码。接下来，将 LDAP 服务器的用户组映射到本地用户角色。

步骤

1. 选择 **Access Management**。
2. 在 **Directory Services** 选项卡中，选择 **Add Directory Server**。

   此时将打开添加目录服务器对话框。

3. 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

设置	说明
配置设置	域
输入 LDAP 服务器的域名。对于多个域，请在逗号分隔的列表中输入域。登录名（ *username@domain* ）中使用域名来指定要进行身份验证的目录服务器。	服务器 URL
以 `ldap[s]://` **`host:`**`*port*` 的格式输入用于访问 LDAP 服务器的 URL。	上传证书（可选）
仅当在上面的服务器 URL 字段中指定了 LDAPS 协议时，才会显示此字段。 单击 **Browse** 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受信任证书或证书链。	绑定帐户（可选）
输入只读用户帐户，以便对 LDAP 服务器进行搜索查询并在组内进行搜索。以 LDAP 类型的格式输入帐户名称。例如，如果绑定用户名为 "bindacct"，则可以输入诸如 `CN=bindacct,CN=Users,DC=cpoc,DC=local` 之类的值。	绑定密码（可选）

设置	说明
输入绑定帐户时将显示此字段。 输入绑定帐户的密码。	添加前测试服务器连接
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。	权限设置
搜索基本 DN	输入 LDAP 上下文以搜索用户，通常采用的形式为 `CN=Users, DC=cpoc, DC=local`。
用户名属性	输入绑定到用户 ID 进行身份验证的属性。例如： `sAMAccountName`。
组属性	输入用户的组属性列表，用于组到角色的映射。例如： `memberOf, managedObjects`。

4. 单击 **Role Mapping** 选项卡。
5. 将 LDAP 组分配给预定义的角色。一个组可以有多个分配的角色。

字段详细信息

设置	说明
映射	组 DN
指定要映射的 LDAP 用户组的组标识名 (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 (\) 转义：\.[]{}()<>*+-=!?^$	
角色	单击该字段并选择要映射到组 DN 的本地用户角色之一。您必须单独选择要包含到此组的每个角色。要登录到 SANtricity Unified Manager，需要与其他角色一起使用 Monitor 角色。映射的角色包括以下权限： • **Storage admin** — 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。 • 安全管理员 — 访问 Access Management 和 Certificate Management 中的安全配置。 • **Support admin** — 访问存储阵列、故障数据和 MEL 事件上的所有硬件资源。无法访问存储对象或安全配置。 • **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

所有用户（包括管理员）都需要 Monitor 角色。

6. 如果需要，单击 **Add another mapping** 以输入更多组到角色的映射。
7. 完成映射后，单击 **Add**。

   系统执行验证，确保存储阵列和 LDAP 服务器可以通信。如果出现错误消息，请检查在对话框中输入的凭据，并在必要时重新输入信息。

在 **SANtricity Unified Manager** 中编辑目录服务器设置和角色映射

如果以前在 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的映射。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 必须定义目录服务器。

步骤

1. 选择 **Access Management**。
2. 选择 **Directory Services** 选项卡。
3. 如果定义了多个服务器，请从表中选择要编辑的服务器。
4. 选择 **View/Edit Settings**。

   此时将打开目录服务器设置对话框。

5. 在 **Server Settings** 选项卡中，更改所需的设置。

字段详细信息

设置	说明
配置设置	域
LDAP 服务器的域名。对于多个域，请以逗号分隔的列表输入域。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。	服务器 URL
用于以 `ldap[s]://host:port` 形式访问 LDAP 服务器的 URL。	绑定帐户（可选）
只读用户帐户，用于针对 LDAP 服务器进行搜索查询以及在组内进行搜索。	绑定密码（可选）
bind 帐户的密码。（输入 bind 帐户时将显示此字段。）	保存前测试服务器连接
检查系统是否可以与 LDAP 服务器配置通信。测试在您单击*保存*后进行。如果选中此复选框且测试失败，则不会更改配置。您必须解决错误或清除复选框才能跳过测试并重新编辑配置。	权限设置
搜索基本 DN	用于搜索用户的 LDAP 上下文，通常采用的形式为 `CN=Users, DC=cpoc, DC=local`。
用户名属性	绑定到用户 ID 进行身份验证的属性。例如： `sAMAccountName`。
组属性	用户的组属性列表，用于组到角色的映射。例如： `memberOf, managedObjects`。

6. 在 **Role Mapping** 选项卡中，更改所需的映射。

字段详细信息

设置	说明
映射	组 DN
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是正则表达式模式的一部分，则必须使用反斜杠（\）转义它们： \.[]{}()<>*+-=!?^$	
角色	要映射到组 DN 的角色。您必须单独选择要包含到此组的每个角色。要登录到 SANtricity Unified Manager，需要与其他角色一起使用监视器角色。这些角色包括： • **Storage admin** — 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。 • 安全管理员 — 访问 Access Management 和 Certificate Management 中的安全配置。 • **Support admin** — 访问存储阵列、故障数据和 MEL 事件上的所有硬件资源。无法访问存储对象或安全配置。 • **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

所有用户（包括管理员）都需要 Monitor 角色。

7. 如果需要，单击 **Add another mapping** 以输入更多组到角色的映射。
8. 单击 **Save**。

结果

完成此任务后，将终止所有活动的用户会话。仅保留当前用户会话。

删除目录服务器

若要断开目录服务器与 Web Services Proxy 之间的连接，可以从"访问管理"页删除服务器信息。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

必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。

关于此任务

完成此任务后，将终止所有活动的用户会话。仅保留当前用户会话。

步骤

1. 选择 **Access Management**。
2. 选择 **Directory Services** 选项卡。
3. 从列表中选择要删除的目录服务器。
4. 单击 **Remove**。

   此时将打开删除目录服务器对话框。

5. 在字段中键入 `remove`，然后单击*删除*。

   目录服务器配置设置、权限设置和角色映射将被删除。用户无法再使用此服务器的凭据登录。

使用 SAML

在 SANtricity Unified Manager 中配置 SAML

要为 Access Management 配置身份验证，可以使用存储阵列中嵌入的 Security Assertion Markup Language (SAML) 功能。此配置在 Identity Provider 和 Storage Provider 之间建立连接。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 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 的功能。
- 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 元数据文件从 IdP 系统下载，可在用于访问 Unified Manager 的本地系统上使用。

关于此任务

标识提供程序 (IdP) 是一个外部系统，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。IdP 可以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 (SP) 是控制用户身份验证和访问的系统。使用 SAML 配置访问管理时，存储阵列充当向身份提供程序请求身份验证的服务提供程序。要在 IdP 和存储阵列之间建立连接，请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 之前测试连接和 SSO 登录。

SAML 和 **Directory Services**。如果在将 Directory Services 配置为身份验证方法时启用 SAML，则 SAML 将取代 Unified Manager 中的 Directory Services。如果稍后禁用 SAML，Directory Services 配置将返回到以前的配置。

*编辑和禁用。*启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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过程。

步骤 1：上传 IdP 元数据文件

要向存储阵列提供 IdP 连接信息，请将 IdP 元数据导入 Unified Manager。IdP 系统需要此元数据才能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

1. 选择菜单：Settings[Access Management]。
2. 选择 **SAML** 选项卡。

   该页面显示了配置步骤的概述。

3. 单击 **Import Identity Provider (IdP) file** 链接。

   此时将打开导入身份提供程序文件对话框。

4. 单击 **Browse** 以选择并上传您复制到本地系统的 IdP 元数据文件。

   选择文件后，将显示 IdP 实体 ID。

5. 单击 **Import**。

步骤 2：导出服务提供程序文件

若要在 IdP 和存储阵列之间建立信任关系，请将 Service Provider 元数据导入 IdP。IdP 需要此元数据来与控制器建立信任关系并处理授权请求。该文件包括控制器域名或 IP 地址等信息，以便 IdP 可以与 Service Provider 进行通信。

步骤

1. 单击 **Export Service Provider files** 链接。

   此时将打开 Export Service Provider Files 对话框。

2. 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 以将元数据文件保存到您的本地系统。

   单击 导出 后，服务提供商元数据将下载到您的本地系统。记下文件的存储位置。

3. 从本地系统中，找到您导出的 XML 格式的 Service Provider 元数据文件。
4. 从 IdP 服务器导入 Service Provider 元数据文件以建立信任关系。您可以直接导入文件，也可以从文件中手动输入控制器信息。

步骤 3：映射角色

要向用户提供对 Unified Manager 的授权和访问权限，必须将 IdP 用户属性和组成员身份映射到存储阵列的预定义角色。

开始之前

- IdP 管理员在 IdP 系统中配置了用户属性和组成员身份。
- IdP 元数据文件已导入到 Unified Manager。

- 控制器的 Service Provider 元数据文件被导入到 IdP 系统中以用于信任关系。

步骤

1. 单击*映射 Unified Manager* 角色的链接。

   此时将打开角色映射对话框。

2. 将 IdP 用户属性和组分配给预定义的角色。一个组可以有多个分配的角色。

   字段详细信息

设置	说明
映射	用户属性
为要映射的 SAML 组指定属性（例如"成员"）。	属性值
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是正则表达式模式的一部分，则必须使用反斜杠(`\`转义：\.[]{}()<>*+-=!?^$	
角色	在字段中单击，然后选择要映射到属性的存储阵列的一个角色。您必须单独选择要包含的每个角色。要登录到 Unified Manager，需要与其他角色一起使用监视器角色。至少一个组也需要安全管理员角色。 映射的角色包括以下权限： • **Storage admin** — 对存储对象（例如卷和磁盘池）的完全读/写访问权限，但不能访问安全配置。 • 安全管理员 — 访问 Access Management 中的安全配置、证书管理、审核日志管理，以及打开或关闭旧版管理界面 (SYMbol) 的能力。 • **Support admin** — 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。 • **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

   所有用户（包括管理员）都需要监视器角色。如果没有监视器角色，Unified Manager 将无法为任何用户正常运行。

3. 如果需要，单击 **Add another mapping** 以输入更多组到角色的映射。

   启用 SAML 后，可以修改角色映射。

4. 完成映射后，单击 **Save**。

步骤 4：测试 SSO 登录

为了确保 IdP 系统和存储阵列可以通信，您可以选择测试 SSO 登录。此测试也在启用 SAML 的最后一步中执行。

开始之前

- IdP 元数据文件已导入到 Unified Manager。
- 控制器的 Service Provider 元数据文件被导入到 IdP 系统中以用于信任关系。

步骤

1. 选择 **Test SSO Login** 链接。

   此时将打开一个用于输入 SSO 凭据的对话框。

2. 输入具有 Security Admin 权限和 Monitor 权限的用户的登录凭据。

   系统测试登录时将打开一个对话框。

3. 查找"测试成功"消息。如果测试成功完成，请转到下一步以启用 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 Security Admin 和 Monitor 权限的组。
   - 您为 IdP 服务器上传的元数据正确。
   - SP 元数据文件中的控制器地址正确。

步骤 5：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。上一步描述了 SSO 登录测试流程。

开始之前

- IdP 元数据文件已导入到 Unified Manager。
- 控制器的 Service Provider 元数据文件被导入到 IdP 系统中以用于信任关系。
- 至少配置了一个 Monitor 和一个 Security Admin 角色映射。

> *编辑和禁用。*启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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

1. 从 **SAML** 选项卡中，选择 **Enable SAML** 链接。

   此时将打开确认启用 SAML 对话框。

2. 键入 `enable`，然后单击 **Enable**。
3. 输入 SSO 登录测试的用户凭据。

结果

系统启用 SAML 后，将终止所有活动会话，并开始通过 SAML 对用户进行身份验证。

更改 **SANtricity Unified Manager** 中的 **SAML** 角色映射

如果之前为访问管理配置了 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

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- IdP 管理员在 IdP 系统中配置了用户属性和组成员身份。
- 已配置并启用 SAML。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **SAML** 选项卡。
3. 选择 **Role Mapping**。

   此时将打开角色映射对话框。

4. 将 IdP 用户属性和组分配给预定义的角色。一个组可以有多个分配的角色。

   请小心，不要在启用 SAML 时删除权限，否则将失去对 Unified Manager 的访问权限。

   字段详细信息

设置	说明
映射	用户属性
为要映射的 SAML 组指定属性（例如"成员"）。	属性值
指定要映射的组的属性值。	角色

   所有用户（包括管理员）都需要监视器角色。如果没有监视器角色，Unified Manager 将无法为任何用户正常运行。

5. （可选）单击 **Add another mapping** 以输入更多组到角色的映射。
6. 单击 **Save**。

结果

完成此任务后，将终止所有活动的用户会话。仅保留当前用户会话。

在 **SANtricity Unified Manager** 中导出 **SAML** 服务提供程序文件

如有必要，您可以导出存储阵列的 Service Provider 元数据，然后将文件重新导入 Identity Provider (IdP) 系统。

开始之前

- 必须使用包含 Security admin 权限的用户配置文件登录。否则，将不会显示 Access Management 功能。
- 已配置并启用 SAML。

关于此任务

在此任务中，您可以从控制器导出元数据。IdP 需要此元数据来与控制器建立信任关系并处理身份验证请求。此文件包括 IdP 可用于发送请求的控制器域名或 IP 地址等信息。

步骤

1. 选择菜单：Settings[Access Management]。
2. 选择 **SAML** 选项卡。
3. 选择 **Export**。

   此时将打开 Export Service Provider Files 对话框。

4. 单击 **Export** 将元数据文件保存到本地系统。

   域名字段为只读。

   记下文件的存储位置。

5. 从本地系统中，找到您导出的 XML 格式的 Service Provider 元数据文件。
6. 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，也可以手动输入控制器信息。
7. 单击 **Close**。

SANtricity Unified Manager 用户访问管理常见问题

如果您只是在寻找问题的快速答案，此常见问题可以为您提供帮助。

为什么我无法登录？

如果您在尝试登录时遇到错误，请查看这些可能的原因。

由于以下原因之一，可能会发生登录错误：

- 您输入了错误的用户名或密码。
- 您的权限不足。
- 您多次尝试登录失败，这触发了锁定模式。请等待 10 分钟以重新登录。
- 已启用 SAML 身份验证。刷新浏览器以登录。

在添加目录服务器之前，我需要知道什么？

在 Access Management 中添加目录服务器之前，您必须满足某些要求。

- 必须在您的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，请查看指南。

RBAC（基于角色的访问控制）功能包括以下角色：

- **Storage admin** — 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。
- 安全管理员 — 访问 Access Management 和 Certificate Management 中的安全配置。
- **Support admin** — 访问存储阵列、故障数据和 MEL 事件上的所有硬件资源。无法访问存储对象或安全配置。
- **Monitor** — 对所有存储对象的只读访问，但无法访问安全配置。

所有用户（包括管理员）都需要 Monitor 角色。

如果使用 LDAP（轻型目录访问协议）服务器和目录服务，请确保：

- 管理员在目录服务中定义了用户组。
- 您知道 LDAP 用户组的组域名。

SAML

如果您使用存储阵列中嵌入的 Security Assertion Markup Language (SAML) 功能，请确保：

- 身份提供程序 (IdP) 管理员在 IdP 系统中配置了用户属性和组成员身份。
- 您知道组成员身份名称。
- 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是正则表达式模式的一部分，则必须使用反斜杠 (\ 转义它们：

```
\.[]{}()<>*+-=!?^$|
```

- 所有用户（包括管理员）都需要监视器角色。如果没有监视器角色，Unified Manager 将无法为任何用户正常运行。

在配置和启用 **SAML** 之前，我需要了解什么？

在配置和启用安全断言标记语言 (SAML) 身份验证功能之前，请确保满足下列要求并了解 SAML 限制。

要求

在开始之前，请确保：

- 在网络中配置了标识提供程序 (IdP)。IdP 是用于向用户请求凭据并确定用户是否成功通过身份验证的外部系统。您的安全团队负责维护 IdP。
- IdP 管理员在 IdP 系统中配置了用户属性和组。
- IdP 管理员已确保 IdP 支持在身份验证时返回名称 ID 的功能。
- 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 元数据文件是从 IdP 系统下载的，可在用于访问 Unified Manager 的本地系统上使用。
- 您知道存储阵列中控制器的 IP 地址或域名。

限制

除了上述要求之外，请务必了解以下限制：

- 启用 SAML 后，您_不能_通过用户界面禁用它，也不能编辑 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。我们建议您在最终配置步骤中启用 SAML 之前测试 SSO 登录。（系统在启用 SAML 之前还会执行 SSO 登录测试。）
- 如果以后禁用 SAML，系统会自动恢复以前的配置（本地用户角色和/或目录服务）。
- 如果当前为用户身份验证配置了 Directory Services，则 SAML 将覆盖该配置。
- 配置 SAML 时，以下客户端无法访问存储阵列资源：
  - 企业管理窗口 (EMW)
  - 命令行界面 (CLI)
  - 软件开发工具包 (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

什么是本地用户？

本地用户在系统中预定义，并包含特定权限。

本地用户包括：

- **admin** — 有权访问系统中所有功能的超级管理员。此用户包括所有角色。密码必须在首次登录时设置。
- **storage** — 负责所有存储配置的管理员。此用户包括以下角色：Storage Admin、Support Admin 和 Monitor。在设置密码之前，此帐户将被禁用。
- **security** — 负责安全配置的用户，包括 Access Management 和 Certificate Management。此用户包括以下角色：Security Admin 和 Monitor。在设置密码之前，此帐户将被禁用。
- **support** — 负责硬件资源、故障数据和固件升级的用户。此用户包括以下角色：Support Admin 和 Monitor。在设置密码之前，此帐户将被禁用。
- **monitor** — 对系统具有只读访问权限的用户。此用户仅包括 Monitor 角色。在设置密码之前，此帐户将被禁

用。

- **rw**（读/写）-- 此用户包括以下角色：Storage Admin、Support Admin 和 Monitor。此帐户在设置密码之前处于禁用状态。
- **ro**（只读）-- 此用户仅包括 Monitor 角色。此帐户在设置密码之前处于禁用状态。

早期版本

请查看以下链接，获取 E 系列硬件和 SANtricity 软件早期版本的文档。这些链接会将您带到其他文档网站。

早期版本的硬件文档

- "安装 E2712、E2724、E5612、E5624 控制器驱动器托盘和 DE1600 和 DE5600 扩展驱动器托盘"
- "安装 E2760 和 E5660 控制器驱动器托盘和 DE6600 扩展驱动器托盘"
- "安装 EF560 闪存阵列和 DE5600 闪存扩展托盘"
- "安装较旧的系统"
- "维护旧系统"
- "向 E2600 和 E2700 添加第二个控制器"
- "更改或添加主机协议"
- "从交流电转换为直流电"
- "控制器升级指南 - 传统控制器型号"

早期版本的软件文档

SANtricity 11.8 版本

- "System Manager 帮助"
- "Unified Manager 帮助"

SANtricity 11.7 版本

- "System Manager 帮助"
- "Unified Manager 帮助"

SANtricity 11.6 版本

- "System Manager 帮助"
- "Unified Manager 帮助"

SANtricity 11.5 版本

- "System Manager 帮助"

SANtricity 11.4 版本

- "AMW (E2700、E5600/EF560) 帮助"

- "EMW (E2700、E5600/EF560) 帮助"

法律声明

法律声明提供对版权声明、商标、专利等信息的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 标识和 NetApp 商标页面上所列的商标是 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。

"https://www.netapp.com/company/legal/trademarks/"

专利

当前 NetApp 拥有的专利列表可以在以下网址找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

通知文件提供有关 NetApp 软件中使用的第三方版权和许可的信息。

"E 系列/EF 系列 SANtricity 操作系统通知"

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 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。