# 设置

## SANtricity 11.6

NetApp
February 12, 2024

# 目录

# 设置

## 警报

### 概念

#### 警报的工作原理

警报会向管理员通知存储阵列上发生的重要事件。可以通过电子邮件， SNMP 陷阱和系统日志发送警报。

警报过程的工作原理如下：

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-将消息发送到电子邮件地址。
   - * SNMP *- SNMP陷阱将发送到SNMP服务器。
   - 系统日志-将消息发送到系统日志服务器。
2. 当存储阵列的事件监控器检测到问题描述 时、它会将有关该问题描述 的信息写入事件日志(可从*菜单：支持[事件日志]*获得)。例如、问题可能包括电池故障、组件从最佳状态移至脱机状态或控制器出现冗余错误等事件。
3. 如果事件监控器确定该事件为"可处理"事件、则会使用配置的警报方法(电子邮件、SNMP和/或系统日志)发送通知。所有严重事件以及一些警告和信息性事件均视为"可处理"。

#### 警报配置

您可以通过初始设置向导(仅适用于电子邮件警报)或警报页面配置警报。要检查当前配置、请转到*菜单：设置[警报]*。

"Alerts"图块显示警报配置、可以是以下配置之一：

- 未配置。
- 已配置；已至少设置一种警报方法。要确定配置了哪些警报方法、请将光标指向此图块。

#### 警报信息

警报可以包括以下类型的信息：

- 存储阵列的名称。
- 与事件日志条目相关的事件错误类型。
- 事件发生的日期和时间。
- 事件的简短问题描述。

> 系统日志警报遵循RFC 3164消息传送标准。

警报术语

## 了解警报术语如何应用于存储阵列。

| 组件 | Description |
| --- | --- |
| 事件监控器 | 事件监控器位于存储阵列上、并作为后台任务运行。当事件监控器检测到存储阵列上的异常时、它会将有关问题的信息写入事件日志。问题可能包括电池故障、组件从最佳状态移至脱机状态或控制器出现冗余错误等事件。如果事件监控器确定该事件为"可处理"事件、则会使用配置的警报方法(电子邮件、SNMP和/或系统日志)发送通知。所有严重事件以及一些警告和信息性事件均视为"可处理"。 |
| 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(Simple Network Management Protocol、SNMP)是一种Internet标准协议、用于在IP网络上的设备之间管理和共享信息。 |
| SNMP陷阱 | SNMP陷阱是发送到SNMP服务器的通知。此陷阱包含有关存储阵列重大问题的信息。 |
| 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 | 团体名称是一个字符串、其作用类似于SNMP环境中网络服务器的密码。 |
| MIB文件 | 管理信息库(Management Information Base、MIB)文件定义了要在存储阵列中监控和管理的数据。必须使用SNMP服务应用程序在服务器上复制和编译此文件。此MIB文件随System Manager软件一起提供、位于支持站点上。 |
| MIB变量 | 管理信息库(Management Information Base、MIB)变量可以返回存储阵列名称、阵列位置以及响应SNMP GetRequests的联系人等值。 |
| 系统日志 | 系统日志是网络设备用于向日志记录服务器发送事件消息的协议。 |
| UDP | 用户数据报协议(User Datagram Protocol、UDP)是一种传输层协议、用于在其数据包标头中指定源端口号和目标端口号。 |

## 操作说明

### 管理电子邮件警报

#### 为警报配置邮件服务器和收件人

## 要配置电子邮件警报、您必须指定邮件服务器地址和警报收件人的电子邮件地址。最多允许20个电子邮件地址。

开始之前

- 邮件服务器的地址必须可用。该地址可以是IPv4或IPv6地址、也可以是完全限定域名。

> 要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从硬件页面配置DNS服务器。

- 要用作警报发件人的电子邮件地址必须可用。此地址显示在警报消息的"发件人"字段中。SMTP协议中需要提供发件人地址；如果没有此地址、则会导致错误。
- 警报收件人的电子邮件地址必须可用。收件人通常是网络管理员或存储管理员的地址。您最多可以输入20个电子邮件地址。

关于此任务

此任务介绍如何配置邮件服务器、输入发件人和收件人的电子邮件地址以及测试从"警报"页面输入的所有电子邮件地址。

> 也可以从初始设置向导配置电子邮件警报。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*电子邮件*选项卡。

   如果尚未配置电子邮件服务器、电子邮件选项卡将显示配置邮件服务器。

3. 选择*配置邮件服务器*。

   此时将打开*配置邮件服务器*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。

     > 要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从*硬件*页面配置DNS服务器。

   - 电子邮件发件人地址-输入要用作电子邮件发件人的有效电子邮件地址。此地址将显示在电子邮件的"发件人"字段中。
   - 在电子邮件中包含联系信息-要在警报消息中包含发件人的联系信息、请选择此选项、然后输入姓名和电话号码。单击*保存*后、电子邮件地址将显示在*警报*页面的*电子邮件*选项卡中。
5. 选择*添加电子邮件*。

   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*添加*。

   电子邮件地址将显示在警报页面上。

7. 如果要确保电子邮件地址有效、请单击*测试所有电子邮件*向收件人发送测试消息。

结果

配置电子邮件警报后、每当发生可警报的事件时、事件监控器都会向指定的收件人发送电子邮件消息。

### 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警报页面的电子邮件选项卡中定义。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*电子邮件*选项卡。
3. 从*电子邮件地址*表中、选择要更改的地址、然后单击最右侧的*编辑*(铅笔)图标。

   该行将变为可编辑字段。

4. 输入新地址、然后单击*保存*(复选标记)图标。

   > 如果要取消更改、请选择*取消*(X)图标。

结果

警报页面的电子邮件选项卡将显示更新后的电子邮件地址。

### 为警报添加电子邮件地址

## 您最多可以为电子邮件警报添加20个收件人。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*电子邮件*选项卡。
3. 选择*添加电子邮件*。

   此时将打开*添加电子邮件*对话框。

4. 在空字段中、输入新的电子邮件地址。如果要添加多个地址、请选择*添加其他电子邮件*以打开另一个字段。
5. 单击 * 添加 * 。

结果

"警报"页面的*电子邮件*选项卡将显示新的电子邮件地址。

### 删除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、以使警报不再发送到电子邮件地址、也可以删除各个电子邮件地址。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*电子邮件*选项卡。
3. 从表中、执行以下操作之一：
   - 要删除邮件服务器以使警报不再发送到电子邮件地址、请选择邮件服务器所在的行。
   - 要删除电子邮件地址以使警报不再发送到此地址、请选择要删除的电子邮件地址所在的行。表右上角的*删除*按钮可供选择。
4. 单击*删除*、然后确认操作。

#### 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。该地址可以是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：设置[警报]*。
2. 选择*电子邮件*选项卡。
3. 选择*配置邮件服务器*。

   此时将打开配置邮件服务器对话框。

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。

     > 要使用完全限定域名、必须在两个控制器上配置DNS服务器。您可以从硬件页面配置DNS服务器。

   - 电子邮件发件人地址-编辑要用作电子邮件发件人的电子邮件地址。此地址将显示在电子邮件的"发件人"字段中。
   - 在电子邮件中包括联系信息-要编辑发件人的联系信息、请选择此选项、然后编辑姓名和电话号码。
5. 单击 * 保存 * 。

### 管理**SNMP**警报

#### 配置**SNMP**警报的社区和目标

## 要配置简单网络管理协议(Simple Network Management Protocol、SNMP)警报、您必须至少确定一台存储阵列的事件监控器可以发送SNMP陷阱的服务器。此配置需要服务器的社区名称和IP地址。

开始之前

- 必须为网络服务器配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
- 必须创建一个社区名称、该名称仅包含可打印的ASCII字符。社区名称是一个类似于网络服务器密码的字符串、通常由网络管理员创建。最多可以创建256个社区。
- 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。

  如果您没有MIB文件、可以从NetApp支持站点获取：

  - 转至 "NetApp 支持"。
  - 单击*下载*。
  - 单击*软件*。
  - 找到您的管理软件(例如SANtricity 系统管理器)、然后单击右侧的*执行！*。
  - 单击最新版本上的"查看并下载"。
  - 单击页面底部的*继续*。
  - 接受 EULA 。
  - 向下滚动、直到看到SNMP陷阱的* MIB文件*、然后单击链接下载此文件。

关于此任务

此任务介绍如何识别陷阱目标的SNMP服务器、然后测试您的配置。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择* SNMP *选项卡。

   如果尚未配置社区、则SNMP选项卡会显示"Configure Community"。

3. 选择*配置社区*。

   此时将打开*配置社区*对话框。

4. 在*社区名称*字段中、输入网络服务器的一个或多个社区字符串、然后单击*保存*。

   "警报"页面将显示"添加陷阱目标"。

5. 选择*添加陷阱目标*。

   此时将打开*添加陷阱目标*对话框。

6. 输入一个或多个陷阱目标、选择其关联的社区名称、然后单击*添加*。
   - 陷阱目标-输入运行SNMP服务的服务器的IPv4或IPv6地址。
   - 社区名称-从下拉列表中、选择此陷阱目标的社区名称。(如果您仅定义了一个社区名称、则此名称已显示在此字段中。)
   - 发送身份验证失败陷阱-如果要在SNMP请求因团体名称无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击*添加*后、陷阱目标和关联的社区名称将显示在*警报*页面的* SNMP*选项卡

中。

7. 要确保陷阱有效、请从表中选择一个陷阱目标、然后单击*测试陷阱目标*向配置的地址发送测试陷阱。

结果

每当发生可更改的事件时、事件监控器都会向服务器发送SNMP陷阱。

#### 编辑SNMP陷阱的社区名称

## 您可以编辑SNMP陷阱的团体名称、也可以将其他团体名称与SNMP陷阱目标关联。

开始之前

必须创建一个社区名称、该名称仅包含可打印的ASCII字符。社区名称是一个类似于网络服务器密码的字符串、由网络管理员创建。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择* SNMP *选项卡。

   陷阱目标和社区名称将显示在表中。

3. 按如下所示编辑社区名称：
   - 要编辑社区名称、请选择*配置社区*。输入新的社区名称、然后单击*保存*。团体名称只能包含可打印的ASCII字符。
   - 要将社区名称与新陷阱目标关联、请从表中选择社区名称、然后单击最右侧的*编辑*(铅笔)图标。从Community Name下拉列表中、为SNMP陷阱目标选择一个新的社区名称、然后单击*保存*(复选标记)图标。

     如果要取消更改、请选择*取消*(X)图标。

结果

"警报"页面的"* SNMP"选项卡将显示更新后的社区。

#### 为SNMP陷阱添加社区名称

## 您最多可以为SNMP陷阱添加256个社区名称。

开始之前

必须创建社区名称。社区名称是一个类似于网络服务器密码的字符串、通常由网络管理员创建。它仅包含可打印的ASCII字符。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择* SNMP *选项卡。

   陷阱目标和社区名称将显示在表中。

3. 选择*配置社区*。

此时将打开配置社区对话框。

4. 选择*添加其他社区*。
5. 输入新的社区名称、然后单击*保存*。

结果

新社区名称将显示在*警报*页面的* SNMP *选项卡中。

#### 删除SNMP陷阱的团体名称

## 您可以删除SNMP陷阱的社区名称。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择* SNMP *选项卡。

   陷阱目标和社区名称将显示在"Alerts"页面上。

3. 选择*配置社区*。

   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*删除*(X)图标。

   如果陷阱目标与此社区名称关联、则*确认删除社区*对话框将显示受影响的陷阱目标地址。

5. 确认此操作、然后单击*删除*。

结果

社区名称及其关联的陷阱目标将从*警报*页面中删除。

#### 配置SNMP MIB变量

## 对于SNMP警报、您可以选择配置SNMP陷阱中显示的管理信息库(Management Information Base、MIB)变量。这些变量可以返回存储阵列名称、阵列位置和联系人。

开始之前

必须使用SNMP服务应用程序在服务器上复制和编译MIB文件。

如果您没有MIB文件、可以按如下所示获取它：

- 转至 "NetApp 支持"。
- 单击*下载*。
- 单击*软件*。
- 找到您的管理软件(例如SANtricity 系统管理器)、然后单击右侧的*执行！*。
- 单击最新版本上的*查看并下载*。
- 单击页面底部的*继续*。

- 接受 EULA 。
- 向下滚动、直到看到SNMP陷阱的* MIB文件*、然后单击链接下载此文件。

关于此任务

此任务介绍如何为SNMP陷阱定义MIB变量。这些变量可返回以下值以响应SNMP GetRequests：

- *sysName*(存储阵列的名称)
- *sysLocation*(存储阵列的位置)
- _sysContact_S(管理员姓名)

步骤

1. 选择*菜单：设置[警报]*。
2. 选择* SNMP *选项卡。
3. 选择*配置SNMP MIB变量*。

   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*。
   - 名称- MIB变量`*sysName*`的值。例如、输入存储阵列的名称。
   - 位置- MIB变量`*sysLocation*`的值。例如、输入存储阵列的位置。
   - 联系人- MIB变量`_sysContact_S`的值。例如、输入负责存储阵列的管理员。

结果

这些值显示在存储阵列警报的SNMP陷阱消息中。

#### 为**SNMP**警报添加陷阱目标

## 您最多可以添加10个服务器来发送SNMP陷阱。

开始之前

- 要添加的网络服务器必须配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
- 必须创建一个社区名称、该名称仅包含可打印的ASCII字符。社区名称是一个类似于网络服务器密码的字符串、通常由网络管理员创建。最多可以创建256个社区。
- 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。

  如果您没有MIB文件、可以从NetApp支持站点获取：

  - 转至 "NetApp 支持"。
  - 单击*下载*。
  - 单击*软件*。
  - 找到您的管理软件(例如SANtricity 系统管理器)、然后单击右侧的*执行！*。

- 单击最新版本上的*查看并下载*。
- 单击页面底部的*继续*。
- 接受 EULA 。
- 向下滚动、直到看到SNMP陷阱的* MIB文件*、然后单击链接下载此文件。

步骤

1. 选择*设置*>*警报*。
2. 选择* SNMP *选项卡。

   表中将显示当前定义的陷阱目标。

3. 选择*添加陷阱配置*。

   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、然后单击*添加*。
   - 陷阱目标-输入运行SNMP服务的服务器的IPv4或IPv6地址。
   - 社区名称-从下拉列表中、选择此陷阱目标的社区名称。(如果您仅定义了一个社区名称、则此名称已显示在此字段中。)
   - 发送身份验证失败陷阱-如果要在SNMP请求因团体名称无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击*添加*后、陷阱目标和关联的社区名称将显示在表中。
5. 要确保陷阱有效、请从表中选择一个陷阱目标、然后单击*测试陷阱目标*向配置的地址发送测试陷阱。

结果

每当发生可更改的事件时、事件监控器都会向服务器发送SNMP陷阱。

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控器不再向该地址发送SNMP陷阱。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择* SNMP *选项卡。

   陷阱目标地址将显示在表中。

3. 选择陷阱目标、然后单击页面右上角的*删除*。
4. 确认此操作、然后单击*删除*。

   目标地址不再显示在*警报*页面上。

结果

已删除的陷阱目标不再从存储阵列的事件监控器接收SNMP陷阱。

管理系统日志警报

### 为系统日志服务器配置警报

## 要配置系统日志警报、必须输入系统日志服务器地址和UDP端口。最多允许五个系统日志服务器。

开始之前

- 系统日志服务器地址必须可用。此地址可以是完全限定域名、IPv4地址或IPv6地址。
- 系统日志服务器的UDP端口号必须可用。此端口通常为514。

关于此任务

此任务介绍如何输入系统日志服务器的地址和端口、然后测试您输入的地址。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*系统日志*选项卡。

   如果尚未定义系统日志服务器、则*警报*页面将显示"添加系统日志服务器"。

3. 单击*添加系统日志服务器*。

   此时将打开*添加系统日志服务器*对话框。

4. 输入一个或多个系统日志服务器的信息(最多五个)、然后单击*添加*。
   - 服务器地址-输入完全限定域名、IPv4地址或IPv6地址。
   - * UDP端口*-通常、系统日志的UDP端口为514。此表显示了已配置的系统日志服务器。
5. 要向服务器地址发送测试警报、请选择*测试所有系统日志服务器*。

结果

每当发生可警报的事件时、事件监控器都会向系统日志服务器发送警报。

### 编辑系统日志服务器中的警报

## 您可以编辑用于接收系统日志警报的服务器地址。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*系统日志*选项卡。
3. 从表中选择系统日志服务器地址、然后单击最右侧的*编辑*(铅笔)图标。

   该行将变为可编辑字段。

4. 编辑服务器地址和UDP端口号、然后单击*保存*(复选标记)图标。

结果

更新后的服务器地址将显示在表中。

为警报添加系统日志服务器

## 最多可以为系统日志警报添加五个服务器。

开始之前

- 系统日志服务器地址必须可用。此地址可以是完全限定域名、IPv4地址或IPv6地址。
- 系统日志服务器的UDP端口号必须可用。此端口通常为514。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*系统日志*选项卡。
3. 选择*添加系统日志服务器*。

   此时将打开添加系统日志服务器对话框。

4. 选择*添加另一个系统日志服务器*。
5. 输入系统日志服务器的信息、然后单击*添加*。

   - 系统日志服务器地址-输入完全限定域名、IPv4地址或IPv6地址。
   - * UDP端口*-通常、系统日志的UDP端口为514。

   您最多可以配置五个系统日志服务器。

结果

系统日志服务器地址将显示在表中。

删除警报的系统日志服务器

## 您可以删除系统日志服务器、使其不再接收警报。

步骤

1. 选择*菜单：设置[警报]*。
2. 选择*系统日志*选项卡。
3. 选择系统日志服务器地址、然后单击右上角的*删除*。

   此时将打开确认删除系统日志服务器对话框。

4. 确认此操作、然后单击*删除*。

结果

删除的服务器不再从事件监控器接收警报。

## 常见问题解答

### 如果警报已禁用、该怎么办？

如果您希望管理员接收有关存储阵列中发生的重要事件的通知、则必须配置警报方法。

对于使用SANtricity System Manager管理的存储阵列、您可以从警报页面配置警报。可以通过电子邮件、SNMP陷阱或系统日志消息发送警报通知。此外、还可以通过初始设置向导配置电子邮件警报。

### 如何配置**SNMP**或系统日志警报？

除了电子邮件警报之外、您还可以将警报配置为通过简单网络管理协议(Simple Network Management Protocol、SNMP)陷阱或系统日志消息发送。

要配置SNMP或系统日志警报、请转到菜单：设置[警报]。

### 阵列和警报之间的时间戳为何不一致？

存储阵列发送警报时、接收警报的目标服务器或主机的时区不正确。相反、存储阵列会使用本地时间(GMT)创建用于警报记录的时间戳。因此、您可能会看到存储阵列的时间戳与接收警报的服务器或主机之间不一致。

由于在发送警报时存储阵列的时区不正确、因此警报上的时间戳是与GMT相关的、其时区偏移为零。要计算适合您当地时区的时间戳、您应确定GMT的小时偏移量、然后在时间戳中添加或减去该值。

> 要避免此问题描述 、请在存储阵列控制器上配置网络时间协议(NTP)。NTP可确保控制器始终同步到正确的时间。

# system：存储阵列设置

## 概念

### 缓存设置和性能

缓存是控制器上临时易失性存储的一个区域、其访问速度比驱动器介质更快。

使用缓存时、整体I/O性能可按以下方式提高：

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

默认缓存设置可满足大多数环境的要求、但您可以根据需要进行更改。

#### 存储阵列缓存设置

对于存储阵列中的所有卷、您可以在系统页面中指定以下值：

- 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。当缓存保存未写入数据的指定起始百

分比时、将触发刷新。默认情况下、当缓存达到80%的全满时、控制器将开始刷新缓存。

- 缓存块大小—每个缓存块的最大大小、该块是一个用于缓存管理的组织单位。默认情况下、缓存块大小为8 KiB、但可以设置为4、8、16或32 KiB。理想情况下、缓存块大小应设置为应用程序的主要I/O大小。文件系统或数据库应用程序通常使用较小的大小、而较大的大小则适合需要大型数据传输或顺序I/O的应用程序

#### 卷缓存设置

对于存储阵列中的单个卷、您可以从卷页面(菜单：Storage[Volumes])中指定以下值：

- 读取缓存—读取缓存是一个缓冲区、用于存储已从驱动器读取的数据。用于读取操作的数据可能已位于上次操作的缓存中、因此无需访问驱动器。数据会一直保留在读取缓存中、直到被刷新为止。
  - 动态读取缓存预取—动态缓存读取预取允许控制器在从驱动器向缓存读取数据块时将其他顺序数据块复制到缓存。这种缓存增加了从缓存中填充未来数据请求的可能性。动态缓存读取预取对于使用顺序I/O的多媒体应用程序非常重要预提取到缓存中的数据速率和数据量会根据主机读取的速率和请求大小进行自调整。随机访问不会将发生原因 数据预先提取到缓存中。禁用读取缓存时、此功能不适用。
- 写入缓存—写入缓存是一个缓冲区、用于存储尚未写入驱动器的主机数据。数据会一直保留在写入缓存中、直到写入驱动器为止。写入缓存可以提高I/O性能。

> 可能的数据丢失-如果启用无电池写入缓存选项并且没有通用电源进行保护、则可能会丢失数据。此外、如果您没有控制器电池、并且启用了无电池写入缓存选项、则可能会丢失数据。

  - 无电池写入缓存—无电池写入缓存设置允许写入缓存继续运行、即使电池缺失、出现故障、已完全放电或未完全充电也是如此。通常不建议选择不带电池的写入缓存、因为断电后数据可能会丢失。通常、在电池充电或更换故障电池之前、控制器会暂时关闭写入缓存。
  - 使用镜像写入缓存-如果写入一个控制器的缓存内存中的数据也写入另一个控制器的缓存中、则使用镜像进行写入缓存。因此、如果一个控制器发生故障、另一个控制器可以完成所有未完成的写入操作。只有在启用了写入缓存且存在两个控制器的情况下、写入缓存镜像才可用。创建卷时的默认设置是使用镜像进行写入缓存。

### 自动负载平衡概述

自动负载平衡可随着时间的推移对负载变化做出动态响应、并自动调整卷控制器所有权、以便在工作负载在控制器之间移动时更正任何负载不平衡问题、从而改进I/O资源管理。

系统会持续监控每个控制器的工作负载、并在主机上安装的多路径驱动程序的配合下、在必要时自动实现平衡。在控制器之间自动重新平衡工作负载时、存储管理员无需再承担手动调整卷控制器所有权以适应存储阵列上的负载变化的负担。

启用自动负载平衡后、它将执行以下功能：

- 自动监控和平衡控制器资源利用率。
- 根据需要自动调整卷控制器所有权、从而优化主机和存储阵列之间的I/O带宽。

#### 启用和禁用自动负载平衡

默认情况下、所有存储阵列都会启用自动负载平衡。

您可能需要在存储阵列上禁用自动负载平衡、原因如下：

- 您不希望自动更改特定卷的控制器所有权以平衡工作负载。
- 您正在高度调整的环境中运行、在此环境中、负载分布会有针对性地进行设置、以便在控制器之间实现特定的分布。

#### 支持自动负载平衡功能的主机类型

即使在存储阵列级别启用了自动负载平衡、您为主机或主机集群选择的主机类型也会直接影响此功能的运行方式。

在控制器之间平衡存储阵列的工作负载时、自动负载平衡功能会尝试移动两个控制器均可访问且仅映射到能够支持自动负载平衡功能的主机或主机集群的卷。

此行为可防止主机因负载平衡过程而无法访问卷；但是、映射到不支持自动负载平衡的主机的卷会影响存储阵列平衡工作负载的能力。要使自动负载平衡平衡平衡工作负载、多路径驱动程序必须支持TPG、并且下表中必须包括主机类型。

> 要将主机集群视为能够自动负载平衡、该组中的所有主机都必须能够支持自动负载平衡。

| 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集群模式 | MPIO与NetApp E系列DSM |
| Linux DM-MP (内核3.10或更高版本) | DM-MP与`sCSI DH_ALUA`设备处理程序 |
| VMware | 采用`VMW_SATA_ALUA存储阵列类型`插件的原生 多路径插件(NMP) |

> 除次要例外情况外、不支持自动负载平衡的主机类型继续正常运行、无论是否启用了此功能。一个例外情况是、如果系统发生故障转移、则当数据路径返回时、存储阵列会将未映射或未分配的卷移回所属控制器。不会移动映射或分配给非自动负载平衡主机的任何卷。

请参见 "互操作性表工具" 有关特定多路径驱动程序、操作系统级别和控制器驱动器托盘支持的兼容性信息。

#### 验证操作系统与自动负载平衡功能的兼容性

在设置新系统(或迁移现有系统)之前、请验证操作系统与自动负载平衡功能的兼容性。

1. 转至 "互操作性表工具" 以查找解决方案 并验证支持。

   如果您的系统运行的是Red Hat Enterprise Linux 6或SUSE Linux Enterprise Server 11、请联系技术支持。

2. 更新并配置`/etc/multipath.conf文件`。
3. 确保适用的供应商和产品的`renet_attached _device_handler`和`detect_prio`均设置为`yes`、或者使用默认设置。

#### 默认主机操作系统类型

首次连接主机时、存储阵列会使用默认主机类型。它定义了在访问卷时存储阵列中的控制器如何与主机的操作系统配合使用。如果需要更改存储阵列相对于与其连接的主机的运行

## 方式、则可以更改主机类型。

通常、在将主机连接到存储阵列或连接其他主机之前、您会更改默认主机类型。

请牢记以下准则：

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

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

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

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

## 操作说明

编辑存储阵列名称

## 您可以更改SANtricity 系统管理器标题栏中显示的存储阵列名称。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*常规*下、查找*名称：*字段。

   如果尚未定义存储阵列名称、此字段将显示"未知"。

3. 单击存储阵列名称旁边的*编辑*(铅笔)图标。

   此字段将变为可编辑状态。

4. 输入新名称。

   名称可以包含字母、数字以及特殊字符下划线(_)、短划线(-)和哈希符号(#)。名称不能包含空格。一个名称的最大长度可以为30个字符。此名称必须是唯一的。

5. 单击*保存*(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

新名称将显示在SANtricity 系统管理器的标题栏中。

打开存储阵列定位灯

## 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：设置[系统]*。
2. 在*常规*下、单击*打开存储阵列定位器指示灯*。

   此时将打开*打开存储阵列定位器灯*对话框、并打开相应存储阵列的定位灯。

3. 在物理定位存储阵列后、返回对话框并选择*关闭*。

结果

定位器指示灯将熄灭、对话框将关闭。

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、以便与管理客户端(用于运行访问SANtricity System Manager的浏览器的系统)同步。

关于此任务

同步可确保事件日志中的事件时间戳与写入主机日志文件的时间戳匹配。在同步过程中、控制器仍保持可用和正常运行。

> 如果在System Manager中启用了NTP、请勿使用此选项同步时钟。相反、NTP会使用SNTP (简单网络时间协议)自动将时钟与外部主机同步。

> 同步后、您可能会注意到性能统计信息丢失或偏差、计划受到影响(ASUP、快照等)、日志数据中的时间戳发生偏差。使用NTP可避免此问题。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*常规*下、单击*同步存储阵列时钟*。

   此时将打开同步存储阵列时钟对话框。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*同步*。

结果

同步成功后、事件日志和主机日志的事件时间戳相同。

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、以节省设置具有相同配置的其他存储阵列所需的时间。

开始之前

存储阵列不得执行任何更改其逻辑配置设置的操作。这些操作的示例包括创建或删除卷、下载控制器固件、分配或修改热备用驱动器或向卷组添加容量(驱动器)。

关于此任务

保存存储阵列配置会生成一个命令行界面(CLI)脚本、其中包含存储阵列设置、卷配置、主机配置或存储阵列的主机到卷分配。您可以使用此生成的命令行界面脚本将配置复制到具有完全相同硬件配置的另一个存储阵列。

但是、您不应使用此生成的命令行界面脚本进行灾难恢复。要执行系统还原、请使用手动创建的配置数据库备份文件、或者联系技术支持以从最新的AutoSupport数据中获取此数据。

此操作不会_保存以下设置：

- 电池的使用寿命
- 控制器的时间
- 非易失性静态随机存取存储器(NVSRAM)设置
- 任何高级功能
- 存储阵列密码
- 硬件组件的运行状态和状态
- 卷组的运行状态(最佳除外)和状态
- 复制服务、例如镜像和卷复制

> 应用程序错误的风险—如果存储阵列正在执行将更改任何逻辑配置设置的操作、请勿使用此选项。这些操作的示例包括创建或删除卷、下载控制器固件、分配或修改热备用驱动器或向卷组添加容量(驱动器)。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*保存存储阵列配置*。
3. 选择要保存的配置项：
   - 存储阵列设置
   - 卷配置
   - 主机配置
   - 主机到卷分配

   > 如果选择*主机到卷分配*项、则默认情况下也会选择*卷配置*项和*主机配置*项。如果不同时保存*卷配置*和*主机配置*、则无法保存*主机到卷分配*。

4. 单击 * 保存 * 。

   此文件将保存在浏览器的"Downloads"文件夹中、名为`storage-array-configuration.cfg`。

完成后

要将已保存的存储阵列配置加载到另一个存储阵列、请使用带有`-f`选项的SANtricity 命令行界面(SMcli)应用`.cfg`文件。

> 您也可以使用Unified Manager界面将存储阵列配置加载到其他存储阵列(选择*菜单：管理[导入设置]*)。

清除存储阵列配置

## 如果要从存储阵列中删除所有池、卷组、卷、主机定义和主机分配、请使用清除配置操作。

开始之前

- 在清除存储阵列配置之前、请备份数据。

关于此任务

有两个清晰的存储阵列配置选项：

- 卷—通常、您可以使用卷选项将测试存储阵列重新配置为生产存储阵列。例如、您可以配置要测试的存储阵列、然后在完成测试后、删除测试配置并为生产环境设置存储阵列。
- 存储阵列—通常、您可以使用存储阵列选项将存储阵列移动到其他部门或组。例如、您可能正在工程部门使用存储阵列、而工程部门现在正在获取一个新的存储阵列、因此您希望将当前存储阵列移动到要重新配置它的管理部门。

  存储阵列选项会删除一些其他设置。

| | **Volume** | 存储阵列 |
|---|---|---|
| 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—此操作将删除存储阵列中的所有数据。(它不会执行安全擦除。) 此操作启动后、您将无法取消。只有在技术支持要求时、才执行此操作。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*清除存储阵列配置*。

3. 在下拉列表中、选择*卷*或*存储阵列*。
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

- 此时将删除当前配置、从而销毁存储阵列上的所有现有数据。
- 所有驱动器均已取消分配。

配置登录横幅

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

关于此任务

创建横幅时、它会显示在对话框的登录屏幕之前。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*常规*部分下、选择*配置登录横幅*。

   此时将打开配置登录横幅对话框。

3. 输入要显示在登录横幅中的文本。

   请勿使用HTML或其他标记标记标记进行格式化。

4. 单击 * 保存 * 。

结果

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

管理会话超时

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

关于此任务

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

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

步骤

1. 选择*菜单：设置[系统]*。
2. 在*常规*部分下、选择*启用/禁用会话超时*。

   此时将打开*启用/禁用会话超时*对话框。

3. 使用spinner控件以分钟为单位增加或减少时间。

   您可以为System Manager设置的最小超时时间为15分钟。

   > 要禁用会话超时、请取消选中*设置时间长度…*复选框。

4. 单击 * 保存 * 。

更改存储阵列的缓存设置

## 对于存储阵列中的所有卷、您可以根据刷新和块大小调整缓存内存设置。

关于此任务

缓存内存是控制器上的临时易失性存储区域、其访问速度比驱动器介质更快。要调整缓存性能、您可以调整以下设置：

| 缓存设置 | **Description** |
| --- | --- |
| 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、当未写入的数据达到80%容量时、将开始缓存刷新。较高的百分比是主要执行写入操作的环境的理想选择、因此新的写入请求可以通过缓存进行处理、而无需转到磁盘。如果环境中的I/O不稳定(发生数据突发)、则设置越低越好、系统就会在数据突发之间频繁地刷新缓存。但是、如果开始百分比低于80%、则发生原因可能会降低性能。 |
| 缓存块大小 | 缓存块大小决定了每个缓存块的最大大小、该块是一个用于缓存管理的组织单位。默认情况下、块大小为32 KiB。System Manager允许缓存块大小为4、8、16或32 KiB。应用程序使用不同的块大小、这会影响存储性能。对于文件系统或数据库应用程序来说、较小的大小是一个不错的选择。较大的大小非常适合生成顺序I/O的应用程序、例如多媒体。 |

步骤

1. 选择*菜单：设置[系统]*。
2. 向下滚动到*其他设置*、然后单击*更改缓存设置*。

   此时将打开更改缓存设置对话框。

3. 调整以下值：
   - 启动按需缓存刷新-选择一个适合您环境中使用的I/O的百分比。如果您选择的值低于80%、则可能会注意到性能下降。
   - 缓存块大小—选择适合您的应用程序的大小。
4. 单击 * 保存 * 。

设置主机连接报告

## 您可以启用主机连接报告、以便存储阵列持续监控控制器与已配置主机之间的连接、然后在连接中断时向您发出警报。默认情况下，此功能处于启用状态。

关于此任务

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

> 禁用主机连接报告还会禁用自动负载平衡、从而监控和平衡控制器资源利用率。

步骤

1. 选择*菜单：设置[系统]*。
2. 向下滚动到*其他设置*、然后单击*启用/禁用主机连接报告*。

   此选项下方的文本指示此选项当前是启用还是禁用。

   此时将打开确认对话框。

3. 单击 * 是 * 继续。

   通过选择此选项、您可以在已启用/已禁用之间切换此功能。

设置自动负载平衡

## 自动负载平衡功能可确保在两个控制器之间动态管理和平衡来自主机的传入I/O流量。默认情况下、此功能处于启用状态、但您可以在System Manager中禁用此功能。

关于此任务

启用自动负载平衡后、它将执行以下功能：

- 自动监控和平衡控制器资源利用率。
- 根据需要自动调整卷控制器所有权、从而优化主机和存储阵列之间的I/O带宽。

您可能需要在存储阵列上禁用自动负载平衡、原因如下：

- 您不希望自动更改特定卷的控制器所有权以平衡工作负载。
- 您正在高度调整的环境中运行、在此环境中、负载分布会有针对性地进行设置、以便在控制器之间实现特定的分布。

步骤

1. 选择*菜单：设置[系统]*。
2. 向下滚动到*其他设置*、然后单击*启用/禁用自动负载平衡*。

   此选项下方的文本指示此功能当前是启用还是禁用。

   此时将打开确认对话框。

3. 单击*是*继续进行确认。

   通过选择此选项、您可以在已启用/已禁用之间切换此功能。

   > 如果将此功能从禁用更改为启用、则主机连接报告功能也会自动启用。

更改默认主机类型

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

关于此任务

请牢记以下准则：

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

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

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

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

步骤

1. 选择*菜单：设置[系统]*。
2. 向下滚动到*其他设置*、然后单击*更改默认主机操作系统类型*。
3. 选择要用作默认值的主机操作系统类型。
4. 单击 * 更改 * 。

启用或禁用原有管理界面

## 您可以启用或禁用原有管理界面(符号)、这是存储阵列与管理客户端之间的一种通信方法。

关于此任务

默认情况下、原有管理界面处于打开状态。如果禁用此功能、则存储阵列和管理客户端将使用更安全的通信方法(基于https的REST API)；但是、如果禁用此功能、某些工具和任务可能会受到影响。

> 对于EF600存储系统、此功能默认处于禁用状态。

此设置将影响以下操作：

- 开(默认)—使用命令行界面和其他一些工具(例如OCI适配器)配置镜像所需的设置。
- 关—在存储阵列与管理客户端之间的通信中强制实施机密性以及访问外部工具所需的设置。配置目录服务器(LDAP)时的建议设置。

步骤

1. 选择*菜单：设置[系统]*。

2. 向下滚动到*其他设置*、然后单击*更改管理界面*。
3. 在对话框中、单击*是*继续。

## 常见问题解答

什么是控制器缓存?

### 控制器缓存是一种物理内存空间、可简化两种类型的I/O (输入/输出)操作：控制器和主机之间以及控制器和磁盘之间。

对于读写数据传输、主机和控制器通过高速连接进行通信。但是、从控制器后端到磁盘的通信速度较慢、因为磁盘是相对较慢的设备。

当控制器缓存接收数据时、控制器向主机应用程序确认它现在保存数据。这样、主机应用程序就无需等待I/O写入磁盘。相反、应用程序可以继续运行。服务器应用程序也可以轻松访问缓存的数据、从而无需额外的磁盘读取即可访问数据。

控制器缓存会通过多种方式影响存储阵列的整体性能：

- 缓存可用作缓冲区、因此无需同步主机和磁盘数据传输。
- 用于从主机执行读取或写入操作的数据可能位于先前操作的缓存中、因此无需访问磁盘。
- 如果使用了写入缓存、则主机可以在将先前写入操作中的数据写入磁盘之前发送后续写入命令。
- 如果启用了缓存预取、则会优化顺序读取访问。缓存预取使读取操作更有可能在缓存中找到其数据、而不是从磁盘读取数据。

> 可能丢失数据-如果启用*不使用电池的写入缓存*选项并且没有通用电源进行保护、则可能会丢失数据。此外、如果您没有控制器电池、并且启用了*无电池写入缓存*选项、则可能会丢失数据。

什么是缓存刷新?

### 当缓存中未写入的数据量达到某个级别时、控制器会定期将缓存的数据写入驱动器。此写入过程称为"刷新"。

控制器使用两种算法来刷新缓存：基于需求和基于年龄。控制器使用基于需求的算法、直到缓存的数据量降至缓存刷新阈值以下。默认情况下、当80%的缓存正在使用时、将开始刷新。

在System Manager中、您可以设置"开始`S请求缓存刷新`"阈值、以便最适合您环境中使用的I/O类型。在以写入操作为主的环境中、您应将"开始需求缓存刷新`S`"百分比设置为高、以增加缓存处理任何新写入请求而无需转到磁盘的可能性。高百分比设置会限制缓存刷新的数量、以使更多数据保留在缓存中、从而增加缓存命中的几率。

在I/O不稳定(发生数据突发)的环境中、您可以使用低缓存刷新、以便系统在数据突发之间频繁地刷新缓存。在处理各种负载的多样化I/O环境中、或者在负载类型未知时、将阈值设置为50%、以作为一个良好的中间地带。请注意、如果您选择的起始百分比低于80%、则性能可能会降低、因为主机读取所需的数据可能不可用。选择较低的百分比还会增加保持缓存级别所需的磁盘写入次数、从而增加系统开销。

基于期限的算法指定写入数据在符合向磁盘转储的条件之前可以保留在缓存中的时间段。在达到缓存刷新阈值之前、控制器会使用基于期限的算法。默认值为10秒、但此时间段仅在非活动期间计算在内。您不能在System Manager中修改刷新计时、而是必须在命令行界面(CLI)中使用*设置存储阵列*命令。

可能丢失数据-如果启用*不使用电池的写入缓存*选项并且没有通用电源进行保护、则可能会丢失数据。此外、如果您没有控制器电池、并且启用了*无电池写入缓存*选项、则可能会丢失数据。

什么是缓存块大小?

存储阵列的控制器将其缓存组织为"块"、这些块是一个内存块、大小可以为8、16、32 KiB。存储系统上的所有卷共享相同的缓存空间；因此、这些卷只能具有一个缓存块大小。

应用程序使用不同的块大小、这可能会影响存储性能。默认情况下、System Manager中的块大小为32 KiB、但您可以将该值设置为8、16、32 KiB。对于文件系统或数据库应用程序来说、较小的大小是一个不错的选择。对于需要大型数据传输、顺序I/O或高带宽(如多媒体)的应用程序来说、较大的大小是一个不错的选择。

何时应同步存储阵列时钟?

如果您发现System Manager中显示的时间戳与管理客户端(通过浏览器访问System Manager的计算机)中显示的时间戳不对齐、则应手动同步存储阵列中的控制器时钟。只有在System Manager中未启用NTP (网络时间协议)时、才需要执行此任务。

强烈建议您使用NTP服务器、而不是手动同步时钟。NTP会使用SNTP (简单网络时间协议)自动将时钟与外部服务器同步。

您可以从同步存储阵列时钟对话框中检查同步状态、该对话框可从系统页面访问。如果对话框中显示的时间不匹配、请运行同步。您可以定期查看此对话框、此对话框指示控制器时钟显示的时间是否已偏离并不再同步。

什么是主机连接报告?

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

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

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

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

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

# system：iSCSI设置

## 概念

### iSCSI术语

了解iSCSI术语如何应用于存储阵列。

| 期限 | Description |
| --- | --- |
| CHAP | 质询握手身份验证协议(CHAP)方法可在初始链路期间验证目标和启动程序的身份。身份验证基于名为CHAP_secret__的共享安全密钥。 |
| 控制器 | 控制器由主板，固件和软件组成。它控制驱动器并实施 System Manager 功能。 |
| DHCP | 动态主机配置协议(DHCP)是Internet协议(IP)网络上使用的一种协议、用于动态分布网络配置参数、例如IP地址。 |
| IB | InfiniBand （ IB ）是高性能服务器和存储系统之间数据传输的一种通信标准。 |
| ICMP ping响应 | Internet控制消息协议(Internet Control Message Protocol、ICMP)是网络计算机的操作系统用来发送消息的协议。ICMP消息可确定主机是否可访问以及从该主机获取数据包所需的时间。 |
| IQN | iSCSI限定名称(IQN)标识符是iSCSI启动程序或iSCSI目标的唯一名称。 |
| iSER | 适用于RDMA的iSCSI扩展(iSER)是一种协议、用于扩展iSCSI协议、以便在InfiniBand或以太网等RDMA传输上运行。 |
| iSNS | Internet存储名称服务(iSNS)是一种协议、允许在TCP/IP网络上自动发现、管理和配置iSCSI和光纤通道设备。 |
| MAC 地址 | 以太网使用介质访问控制标识符(MAC地址)来区分连接同一物理传输网络接口上两个端口的不同逻辑通道。 |
| 管理客户端 | 管理客户端是指安装了浏览器以访问System Manager的计算机。 |
| MTU | 最大传输单元(Maximum Transmission Unit、MTU)是可在网络中发送的最大数据包或帧。 |
| RDMA | 远程直接内存访问(RDMA)是一项技术、允许网络计算机在主内存中交换数据、而无需涉及任一计算机的操作系统。 |
| 未命名的发现会话 | 启用未命名发现会话选项后、无需iSCSI启动程序指定目标IQN来检索控制器的信息。 |

## 操作说明

### 配置**iSCSI**端口

## 如果控制器包含iSCSI主机连接、则可以从系统页面配置iSCSI端口设置。

开始之前

- 控制器必须包含iSCSI端口；否则、iSCSI设置不可用。

- 您必须知道网络速度(端口与主机之间的数据传输速率)。

> 只有当存储阵列支持iSCSI时、才会显示iSCSI设置和功能。

步骤

1. 选择*菜单：设置[系统]*。
2. 在* iSCSI设置*下、选择*配置iSCSI端口*。

   > 只有在System Manager检测到控制器上的iSCSI端口时、才会显示*配置iSCSI端口*选项。

3. 选择包含要配置的iSCSI端口的控制器。
4. 在下拉列表中，选择要配置的端口，然后单击 * 下一步 * 。
5. 选择配置端口设置，然后单击 * 下一步 * 。

   要查看所有端口设置，请单击对话框右侧的 * 显示更多端口设置 * 链接。

   字段详细信息

| 端口设置 | **Description** |
| --- | --- |
| 启用 IPv4/Enable IPv6 | 选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。<br>> 如果要禁用端口访问、请取消选中这两个复选框。 |
| TCP 侦听端口（可通过单击 * 显示更多端口设置 * 来使用。） | 如有必要，请输入新的端口号。<br><br>侦听端口是控制器用于侦听主机 iSCSI 启动程序的 iSCSI 登录的 TCP 端口号。默认侦听端口为 3260 。您必须输入 3260 或 49152 到 65535 之间的值。 |
| MTU 大小（可通过单击 * 显示更多端口设置 * 来获取。） | 如有必要，请为最大传输单元（ Maximum Transmission Unit ， MTU ）输入一个新大小（以字节为单位）。<br><br>默认最大传输单元（ Maximum Transmission Unit ， MTU ）大小为每帧 1500 字节。您必须输入一个介于 1500 和 9000 之间的值。 |
| 启用 ICMP ping 响应 | 选择此选项可启用 Internet 控制消息协议（ Internet Control Message Protocol ， ICMP ）。网络计算机的操作系统使用此协议发送消息。这些 ICMP 消息可确定主机是否可访问以及从该主机获取数据包所需的时间。 |

   如果选择了 * 启用 IPv* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv4 设置。如果选择了 * 启用 IPv6* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv6 设置。如果同时选择了这两个选项，则 IPv4 设置对话框将首先打开，然后单击 * 下一步 * ， IPv6 设置对话框将打开。

6. 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 | Description |
| --- | --- |
| 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、可以剪切地址并将其粘贴到字段中。) 对于IPv4、请包括网络子网掩码和网关。对于 IPv6 ，请包括可路由的 IP 地址和路由器 IP 地址。 |
| 启用 VLAN 支持（可通过单击 * 显示更多设置 * 来获取。） | 选择此选项可启用 VLAN 并输入其 ID 。VLAN 是一种逻辑网络，其行为与相同交换机，相同路由器或这两者所支持的其他物理和虚拟局域网（ LAN ）在物理上是分开的。 |
| 启用以太网优先级（可通过单击 * 显示更多设置 * 来使用）。 | 选择此选项可启用用于确定网络访问优先级的参数。使用滑块选择介于1 (最低)和7 (最高)之间的优先级。<br><br>在以太网等共享局域网（ LAN ）环境中，许多工作站可能会争用网络访问权限。访问权限按先到先得原则提供。两个工作站可能会同时尝试访问网络，这会导致两个工作站重新关闭并等待，然后再重试。对于只有一个工作站连接到交换机端口的交换式以太网，此过程会最小化。 |

7. 单击 * 完成 * 。

配置**iSCSI**身份验证

为了提高iSCSI网络的安全性、您可以在控制器(目标)和主机(启动程序)之间设置身份验证。System Manager使用质询握手身份验证协议(Challenge Handshake Authentication Protocol、CHAP)方法、在初始链接期间验证目标和启动程序的身份。身份验证基于名为CHAP *secret*的共享安全密钥。

开始之前

您可以在为目标(控制器)设置CHAP密钥之前或之后为启动程序(iSCSI主机)设置CHAP密钥。在按照此任务中的说明进行操作之前、您应等待主机先建立iSCSI连接、然后在各个主机上设置CHAP密钥。建立连接后、主机的IQN名称及其CHAP密钥将在iSCSI身份验证对话框中列出(如本任务所述)、您无需手动输入它们。

关于此任务

您可以选择以下身份验证方法之一：

- 单向身份验证—使用此设置允许控制器对iSCSI主机的身份进行身份验证(单向身份验证)。
- 双向身份验证—使用此设置可允许控制器和iSCSI主机执行身份验证(双向身份验证)。此设置可通过使控制器对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主机对控制器的身份进行身份验证。

只有当存储阵列支持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：设置[系统]*。
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、其中显示了当前设置的方法。此外、还会显示是否已配置任何主机的CHAP机密。

3. 选择以下选项之一：
   - 无身份验证-如果不希望控制器对iSCSI主机的身份进行身份验证、请选择此选项并单击*完成*。此时、对话框将关闭、您将完成配置。
   - 单向身份验证—要允许控制器对iSCSI主机的身份进行身份验证、请选择此选项并单击*下一步*以显示配置目标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、请选择此选项并单击*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密钥必须介于12到57个可打印ASCII字符之间。

   > 如果先前为控制器配置了CHAP密钥、则会屏蔽字段中的字符。如有必要、您可以替换现有字符(新字符不会屏蔽)。

5. 执行以下操作之一：
   - 如果要配置_one-way_身份验证、请单击*完成*。此时、对话框将关闭、您将完成配置。
   - 如果要配置_two-way_身份验证、请单击*下一步*以显示配置启动程序CHAP对话框。
6. 对于双向身份验证、请输入或确认任何iSCSI主机(启动程序)的CHAP密钥、该密钥可以是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*启动程序CHAP机密*字段留空。

   > 如果先前为主机配置了CHAP密钥、则字段中的字符将被屏蔽。如有必要、您可以替换现有字符(新字符不会屏蔽)。

7. 单击 * 完成 * 。

结果

除非未指定身份验证、否则在控制器和iSCSI主机之间的iSCSI登录序列期间会进行身份验证。

### 启用**iSCSI**发现设置

您可以启用与在iSCSI网络中发现存储设备相关的设置。通过目标发现设置、您可以使用Internet存储名称服务(iSNS)协议注册存储阵列的iSCSI信息、还可以确定是否允许未命名的发现会话。

开始之前

如果iSNS服务器使用静态IP地址、则该地址必须可用于iSNS注册。支持IPv4和IPv6。

关于此任务

您可以启用与iSCSI发现相关的以下设置：

- 启用**iSNS**服务器以注册目标-启用后、存储阵列将从iSNS服务器注册其iSCSI限定名称(IQN)和端口信息。此设置允许iSNS发现、以便启动程序可以从iSNS服务器检索IQN和端口信息。
- 启用未命名的发现会话-启用未命名的发现会话后、启动程序(iSCSI主机)无需在发现类型连接的登录顺序期间提供目标(控制器)的IQN。禁用后、主机需要提供IQN、以便与控制器建立发现会话。但是、正常(I/O轴承)会话始终需要目标IQN。禁用此设置可以防止未经授权的iSCSI主机仅使用其IP地址连接到控制器。

> 只有当存储阵列支持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：设置[系统]*。
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*启用iSNS服务器*…字段下方、此对话框指示控制器是否已注册。

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：
   - 自动从**DHCP**服务器获取配置-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、则必须将控制器上的所有iSCSI端口配置为也使用DHCP。如有必要、请更新控制器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"。` 此选项需要包含iSNS服务器IPv4地址、以数据字节0xA-0xd (10-13)为单位。

   - 手动指定静态配置-如果要输入iSNS服务器的静态IP地址、请选择此选项。(如果需要、可以剪切地址并将其粘贴到字段中。) 在字段中、输入IPv4地址或IPv6地址。如果同时配置了这两者、则IPv4为默认值。此外、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、无需iSCSI启动程序指定目标IQN即可检索控制器的信息。
   - 禁用后、除非启动程序提供目标IQN、否则会阻止发现会话。禁用未命名的发现会话可提高安全性。
5. 单击 * 保存 * 。

结果

当System Manager尝试向iSNS服务器注册控制器时、会显示一个进度条。此过程可能需要长达五分钟的时间。

### 查看**iSCSI**统计信息包

## 您可以查看与存储阵列的iSCSI连接的相关数据。

关于此任务

System Manager将显示这些类型的iSCSI统计信息。所有统计信息均为只读、无法设置。

- 以太网**MAC**统计信息-提供介质访问控制(MAC)的统计信息。MAC还提供了一种称为物理地址或MAC地址的寻址机制。MAC地址是分配给每个网络适配器的唯一地址。MAC地址有助于将数据包传送到子网络中的目标。
- 以太网**TCP/IP**统计信息—提供TCP/IP的统计信息、即iSCSI设备的传输控制协议(Transmission Control Protocol、TCP)和Internet协议(Internet Protocol、IP)。通过TCP、联网主机上的应用程序可以创建彼此的连

接、并通过这些连接以数据包的形式交换数据。IP是一种面向数据的协议、用于在数据包交换的网络间通信数据。IPv4统计信息和IPv6统计信息分别显示。

- 本地目标/启动程序(协议)统计信息—显示iSCSI目标的统计信息、该目标可对其存储介质进行块级访问、并显示在异步镜像操作中用作启动程序时存储阵列的iSCSI统计信息。
- * DCBX运行状态统计信息*-显示各种数据中心桥接交换(DCBX)功能的运行状态。
- * LLDP TLV统计信息*-显示链路层发现协议(Link Layer Discovery Protocol、LLDP)类型长度值(TLV)统计信息。
- * DCBX TLV统计信息*-显示用于标识数据中心桥接(Data Center Bridging、DCB)环境中的存储阵列主机端口的信息。此信息将与网络对等方共享、以便于识别和使用。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*查看iSCSI统计信息包*。
3. 单击一个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。

   设置基线将为统计信息的收集设置一个新的起点。所有iSCSI统计信息都使用相同的基线。

## 查看 iSCSI 会话

您可以查看有关与存储阵列的iSCSI连接的详细信息。iSCSI会话可以与异步镜像关系中的主机或远程存储阵列进行。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*查看/结束iSCSI会话*。

   此时将显示当前iSCSI会话的列表。

3. 要查看有关特定iSCSI会话的追加信息 、请选择一个会话、然后单击*查看详细信息*。

字段详细信息

| 项目 | Description |
| --- | --- |
| 会话标识符(SSID) | 一个十六进制字符串、用于标识iSCSI启动程序与iSCSI目标之间的会话。SSID由ISID和TPGT组成。 |
| 启动程序会话ID (ISID) | 会话标识符的启动程序部分。启动程序将在登录期间指定ISID。 |
| 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 | 启动程序的全球唯一名称。 |
| 启动程序iSCSI标签 | 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。此别名允许组织将用户友好型字符串与iSCSI名称相关联。但是、别名不能替代iSCSI名称。启动程序iSCSI别名只能在主机上设置、而不能在System Manager中设置 |
| 主机 | 向存储阵列发送输入和输出的服务器。 |
| 连接ID (CID) | 启动程序与目标之间会话中连接的唯一名称。启动程序将生成此ID、并在登录请求期间将其呈现给目标。在注销以关闭连接期间、也会显示连接ID。 |
| 以太网端口标识符 | 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 | 对要访问iSCSI网络的用户进行身份验证的技术。有效值为* CHAP 和*无。 |
| 标题摘要方法 | 显示iSCSI会话可能的标头值的技术。HeaderDigest和DataDigest可以是*无*或* CRC32C*。两者的默认值均为*无*。 |
| 数据摘要方法 | 用于显示iSCSI会话的可能数据值的技术。HeaderDigest和DataDigest可以是*无*或* CRC32C*。两者的默认值均为*无*。 |
| 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*。 |
| 目标别名 | 与目标关联的标签。 |

| 项目 | Description |
| --- | --- |
| 启动程序别名 | 与启动程序关联的标签。 |
| 目标IP地址 | iSCSI会话的目标的IP地址。不支持DNS名称。 |
| 初始R2T | 初始传输就绪状态。状态可以是*是*或*否*。 |
| 最大突发长度 | 此iSCSI会话的最大SCSI有效负载(以字节为单位)。最大突发长度可以介于512到262、144 (256 KB)之间。默认值为* 262、144 (256 KB)*。 |
| 第一个突发长度 | 此iSCSI会话中未经请求的数据的SCSI有效负载(以字节为单位)。第一个突发长度可以介于512到131、072 (128 KB)之间。默认值为*、65、536 (64 KB)*。 |
| 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介于0到3600之间。默认值为*。2 |
| 要保留的默认时间 | 连接终止或连接重置后仍可进行连接的最大秒数。默认保留时间可以为0到3600。默认值为*20*。 |
| 最大未完成R2T | 此iSCSI会话未完成的最大"可传输"数。最大未完成的可传输值可以介于1到16之间。默认值为* 1 *。 |
| 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*。 |
| 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 | 目标的官方名称(而不是别名)。格式为_iqn_的目标名称。 |
| 启动程序名称 | 启动程序的官方名称(而不是别名)。使用_iqn_或_eui_格式的启动程序名称。 |

4. 可选：*要将报告保存到文件中、请单击*保存。

   此文件将保存在浏览器的"Downloads"文件夹中、文件名为`iscsi-session-connections.txt`。

### 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进行。

#### 关于此任务

您可能希望结束iSCSI会话的原因如下：

- 未经授权的访问-如果iSCSI启动程序已登录且无法访问、您可以结束iSCSI会话以强制iSCSI启动程序退出存储阵列。iSCSI启动程序可能已登录、因为无身份验证方法可用。
- 系统停机时间-如果需要关闭存储阵列、但您发现iSCSI启动程序仍处于登录状态、则可以结束iSCSI会话以将iSCSI启动程序从存储阵列中移出。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*查看/结束iSCSI会话*。

   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*结束会话*、然后确认要执行此操作。

### 通过**InfiniBand**端口配置**iSER**

## 如果控制器包含基于InfiniBand的iSER端口、则可以配置与主机的网络连接。

开始之前

- 控制器必须包含基于InfiniBand端口的iSER；否则、基于InfiniBand的iSER设置在System Manager中不可用。
- 您必须知道主机连接的IP地址。

步骤

1. 选择*菜单：设置[系统]*
2. 在*基于InfiniBand设置的iSER *下、选择*基于InfiniBand端口配置iSER *。
3. 单击具有要配置的iSER over InfiniBand端口的控制器。单击 * 下一步 * 。
4. 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。
5. 单击 * 完成 * 。
6. 单击*是*重置基于InfiniBand的iSER端口。

### 查看基于**InfiniBand**的**iSER**统计信息

## 如果存储阵列的控制器包含基于InfiniBand的iSER端口、则可以查看有关主机连接的数据。

关于此任务

System Manager会显示以下类型的基于InfiniBand的iSER统计信息。所有统计信息均为只读、无法设置。

- 本地目标(协议)统计信息—提供基于InfiniBand的iSER目标的统计信息、其中显示了对其存储介质的块级访问。
- 基于**InfiniBand**接口的**iSER**统计信息-提供InfiniBand接口上所有iSER端口的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*查看基于InfiniBand统计信息的iSER *。
3. 单击一个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。

   设置基线将为统计信息的收集设置一个新的起点。所有基于InfiniBand的iSER统计信息都使用相同的基线。

## 常见问题解答

使用**iSNS**服务器进行注册时会发生什么情况?

### 使用Internet存储名称服务(iSNS)服务器信息时、可以将主机(启动程序)配置为查询iSNS服务器以从目标(控制器)检索信息。

此注册可为iSNS服务器提供控制器的iSCSI限定名称(IQN)和端口信息、并允许在启动程序(iSCSI主机)和目标(控制器)之间进行查询。

**iSCSI**自动支持哪些注册方法?

### iSCSI实施支持Internet存储名称服务(iSNS)发现方法或使用发送目标命令。

iSNS方法允许在启动程序(iSCSI主机)和目标(控制器)之间进行iSNS发现。您注册目标控制器以向iSNS服务器提供控制器的iSCSI限定名称(IQN)和端口信息。

如果不配置iSNS、则iSCSI主机可以在iSCSI发现会话期间发送发送目标命令。作为响应、控制器将返回端口信息(例如目标IQN、端口IP地址、侦听端口和目标端口组)。如果使用iSNS、则不需要此发现方法、因为主机启动程序可以从iSNS服务器检索目标IP。

如何解读基于**InfiniBand**统计信息的**iSER**?

### 查看基于InfiniBand的iSER统计信息对话框可显示本地目标(协议)统计信息和基于InfiniBand的iSER (IB)接口统计信息。所有统计信息均为只读、无法设置。

- 本地目标**(**协议**)**统计信息—提供基于InfiniBand的iSER目标的统计信息、其中显示了对其存储介质的块级访问。
- * iSER over InfiniBand Interface statistics*—提供InfiniBand接口上所有基于InfiniBand端口的iSER的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

要通过**InfiniBand**配置或诊断**iSER**、还需要执行哪些操作?

### 下表列出了可用于配置和管理基于InfiniBand会话的iSER的System Manager功能。

只有当存储阵列的控制器包含基于InfiniBand的iSER主机管理端口时、iSER over InfiniBand设置才可用。

通过**InfiniBand**配置和诊断**iSER**

| Action | 位置 |
| --- | --- |
| 通过InfiniBand端口配置iSER | 1. 选择 * 硬件 * 。<br>2. 选择*显示磁盘架的背面*。<br>3. 选择一个控制器。<br>4. 选择*通过InfiniBand端口配置iSER *。<br><br>或<br><br>1. 选择*菜单：设置[系统]*。<br>2. 向下滚动到*基于InfiniBand设置的iSER *、然后选择*基于InfiniBand端口配置iSER *。 |
| 查看基于InfiniBand的iSER统计信息 | 1. 选择*菜单：设置[系统]*。<br>2. 向下滚动到*基于InfiniBand设置的iSER *、然后选择*基于InfiniBand统计信息查看iSER *。 |

# system：NVMe设置

## 概念

### NVMe 概述

某些控制器包含一个端口、用于在网络结构上实施NVMe (非易失性内存快速协议)。NVMe支持主机与存储阵列之间的高性能通信。

#### 什么是NVMe?

_NVM_表示"非易失性内存"、是许多类型的存储设备中使用的永久性内存。_NVME (NVM Express)是一种标准化接口或协议、专为与NVM设备进行高性能多队列通信而设计。

#### 什么是基于网络结构的NVMe?

基于网络结构的NVMe (NVMe-oF)是一种技术规范、可通过网络在主机计算机和存储之间传输基于*NVMe*消息的命令和数据。*NVMe*存储阵列*(*称为*_subsystem*)可由使用网络结构的主机访问。NVMe命令已启用并封装在主机端和子系统端的传输抽象层中。这样可以将高性能NVMe接口从主机端到端扩展到存储、并对命令集进行标准化和简化。

NVMe-oF存储作为本地块存储设备提供给主机。卷(称为_namespacage_)可以与任何其他块存储设备一样挂载到文件系统。您可以使用REST API、SMcli或SANtricity 系统管理器根据需要配置存储。

#### 什么是NVMe限定名称(NQN)?

NVMe限定名称(NQN)用于标识远程存储目标。存储阵列的NVMe限定名称始终由子系统分配、不能修改。整个阵列只有一个NVMe限定名称。NVMe限定名称的长度限制为223个字符。您可以将其与iSCSI限定名称进行比较。

#### 什么是命名空间和命名空间ID?

命名空间相当于SCSI中与阵列中的卷相关的逻辑单元。命名空间ID (NSID)相当于SCSI中的逻辑单元号(LUN)。您可以在创建命名空间时创建NSID、并将其设置为1到255之间的值。

#### 什么是NVMe控制器?

与SCSI I_T Nexus类似、SCSI I_T Nexus表示从主机启动程序到存储系统目标的路径、在主机连接过程中创建的NVMe控制器可在主机与存储阵列中的命名空间之间提供访问路径。主机的NQN加上主机端口标识符可唯一标识NVMe控制器。虽然NVMe控制器只能与单个主机关联、但它可以访问多个命名空间。

您可以使用SANtricity 系统管理器配置哪些主机可以访问哪些命名空间、并为主机设置命名空间ID。然后、在创建NVMe控制器时、将创建可由NVMe控制器访问的命名空间ID列表、并使用这些ID配置允许的连接。

### NVMe术语

了解NVMe术语如何应用于您的存储阵列。

| 期限 | Description |
|---|---|
| InfiniBand | InfiniBand （ IB ）是高性能服务器和存储系统之间数据传输的一种通信标准。 |
| 命名空间 | 命名空间是指为块访问而格式化的NVM存储。它类似于SCSI中的逻辑单元、它与存储阵列中的卷相关。 |
| 命名空间ID | 命名空间ID是NVMe控制器在命名空间中的唯一标识符、可设置为1到255之间的值。它类似于SCSI中的逻辑单元号(Logical Unit Number、LUN)。 |
| NQN | NVMe限定名称(NQN)用于标识远程存储目标(存储阵列)。 |
| NVM | 非易失性内存(NVM)是许多类型的存储设备中使用的永久性内存。 |
| NVMe | Non-Volatile Memory Express (NVMe)是一种专为SSD驱动器等基于闪存的存储设备设计的接口。与以前的逻辑设备接口相比、NVMe可降低I/O开销并提高性能。 |
| NVMe-oF | 基于网络结构的非易失性Memory Express (NVMe-oF)是一种规范、可使NVMe命令和数据通过网络在主机和存储之间传输。 |
| NVMe控制器 | NVMe控制器是在主机连接过程中创建的。它可在主机与存储阵列中的命名空间之间提供访问路径。 |
| NVMe队列 | 队列用于通过NVMe接口传递命令和消息。 |

| 期限 | Description |
| --- | --- |
| NVMe 子系统 | 具有NVMe主机连接的存储阵列。 |
| RDMA | 通过在网络接口卡(NIC)硬件中实施传输协议、远程直接内存访问(Remote Direct Memory Access、RDMA)可以更直接地将数据移入和移出服务器。 |
| RoCE | 基于融合以太网的 RDMA （ RoCE ）是一种网络协议，允许通过以太网远程直接内存访问（ RDMA ）。 |
| SSD | 固态磁盘（ SSD ）是指使用固态内存（ Flash ）持久存储数据的数据存储设备。SSD 可模拟传统硬盘驱动器，并可与硬盘驱动器使用相同的接口。 |

## 操作说明

### 配置基于**InfiniBand**的**NVMe**端口

## 如果您的控制器包含基于InfiniBand的NVMe连接、则可以从系统页面配置NVMe端口设置。

开始之前

- 您的控制器必须包含基于InfiniBand的NVMe主机端口；否则、System Manager中不提供基于InfiniBand的NVMe设置。
- 您必须知道主机连接的IP地址。

> 只有当存储阵列的控制器包含基于InfiniBand的NVMe端口时、才会显示基于InfiniBand的NVMe设置和功能。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*基于InfiniBand的NVMe设置*下、选择*配置基于InfiniBand端口的NVMe *。
3. 选择具有要配置的基于InfiniBand的NVMe端口的控制器。单击 * 下一步 * 。
4. 从下拉列表中选择要配置的HIC端口、然后输入IP地址。

   如果要为EF600存储阵列配置支持200 GB的HIC、则此对话框会显示两个IP地址字段、一个用于物理端口(外部)、一个用于虚拟端口(内部)。您应为这两个端口分配唯一的IP地址。通过这些设置、主机可以在每个端口之间建立一条路径、并使HIC实现最高性能。如果不为虚拟端口分配IP地址、HIC将以大约一半的速度运行。

5. 单击 * 完成 * 。
6. 单击*是*重置基于InfiniBand的NVMe端口。

### 配置基于**RoCE**的**NVMe**端口

## 如果您的控制器包括通过RoCE连接NVMe (基于融合以太网的RDMA)、则可以从系统页面

## 配置NVMe端口设置。

开始之前

- 您的控制器必须包含一个基于RoCE的NVMe主机端口；否则、System Manager中不提供基于RoCE的NVMe设置。
- 您必须知道主机连接的IP地址。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*基于ROCE的NVMe设置*下、选择*配置基于ROCE的NVMe端口*。
3. 选择具有要配置的基于RoCE的NVMe端口的控制器。单击 * 下一步 * 。
4. 从下拉列表中选择要配置的HIC端口。单击 * 下一步 * 。
5. 配置端口设置。

   要查看所有端口设置，请单击对话框右侧的 * 显示更多端口设置 * 链接。

   字段详细信息

| 端口设置 | **Description** |
| --- | --- |
| 已配置以太网端口速度 | 在端口上选择与SFP速度功能匹配的速度。 |
| 启用 IPv4/Enable IPv6 | 选择一个或两个选项以启用对 IPv4 和 IPv6 网络的支持。<br>ⓘ 如果要禁用端口访问、请取消选中这两个复选框。 |
| MTU 大小（可通过单击 * 显示更多端口设置 * 来获取。） | 如有必要，请为最大传输单元（ Maximum Transmission Unit ， MTU ）输入一个新大小（以字节为单位）。<br>默认最大传输单元（ Maximum Transmission Unit ， MTU ）大小为每帧 1500 字节。您必须输入一个介于 1500 和 9000 之间的值。 |

如果选择了 * 启用 IPv* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv4 设置。如果选择了 * 启用 IPv6* ，则在单击 * 下一步 * 后，将打开一个对话框，用于选择 IPv6 设置。如果同时选择了这两个选项，则 IPv4 设置对话框将首先打开，然后单击 * 下一步 * ， IPv6 设置对话框将打开。

1. 自动或手动配置 IPv4 和 / 或 IPv6 设置。

字段详细信息

| 端口设置 | Description |
| --- | --- |
| 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、可以剪切地址并将其粘贴到字段中。) 对于IPv4、请包括网络子网掩码和网关。对于 IPv6 ，请包括可路由的 IP 地址和路由器 IP 地址。如果要为EF600存储阵列配置支持200 GB的HIC、则此对话框会显示两组网络参数字段、一组用于物理端口(外部)、一组用于虚拟端口(内部)。您应为这两个端口分配唯一的参数。通过这些设置、主机可以在每个端口之间建立一条路径、并使HIC实现最高性能。如果不为虚拟端口分配IP地址、HIC将以大约一半的速度运行。 |

2. 单击 * 完成 * 。

查看基于网络结构的**NVMe**统计信息

## 您可以查看有关通过网络结构连接到存储阵列的NVMe的数据。

关于此任务

System Manager会显示这些类型的基于网络结构的NVMe统计信息。所有统计信息均为只读、无法设置。

- * NVMe子系统统计信息*-显示NVMe控制器及其队列的统计信息。NVMe控制器可在主机与存储阵列中的命名空间之间提供访问路径。您可以查看连接故障、重置和关闭等项的NVMe子系统统计信息。
- * RDMA接口统计信息*-提供RDMA接口上所有基于网络结构的NVMe端口的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。只有当基于网络结构的NVMe端口可用时、才会显示此选项卡。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

步骤

1. 选择*菜单：设置[系统]*。
2. 选择*查看基于网络结构的NVMe统计信息*。
3. 可选：*要设置基线、请单击*设置新基线。

   设置基线将为统计信息的收集设置一个新的起点。所有NVMe统计信息都使用相同的基线。

## 常见问题解答

如何解读基于网络结构的**NVMe**统计信息？

## 查看基于网络结构的NVMe统计信息对话框显示NVMe子系统和RDMA接口的统计信息。所有统计信息均为只读、无法设置。

- * NVMe子系统统计信息*-显示NVMe控制器及其队列的统计信息。NVMe控制器可在主机与存储阵列中的命名空间之间提供访问路径。您可以查看连接故障、重置和关闭等项的NVMe子系统统计信息。有关这些统计信息的详细信息、请单击*查看表标题的图例*。
- * RDMA接口统计信息*-提供RDMA接口上所有基于网络结构的NVMe端口的统计信息、其中包括与每个交换机端口关联的性能统计信息和链路错误信息。只有当基于网络结构的NVMe端口可用时、才会显示此选项卡。有关统计信息的详细信息、请单击*查看表标题的图例*。

您可以将其中每个统计信息作为原始统计信息或基线统计信息进行查看。原始统计信息是自控制器启动以来收集的所有统计信息。基线统计信息是自设置基线时间以来收集的时间点统计信息。

要配置或诊断基于**InfiniBand**的**NVMe**、还需要执行哪些操作?

## 下表列出了可用于配置和管理基于InfiniBand的NVMe会话的System Manager功能。

只有当存储阵列的控制器包含基于InfiniBand的NVMe端口时、基于InfiniBand的NVMe设置才可用。

配置和诊断基于**InfiniBand**的**NVMe**

| Action | 位置 |
| --- | --- |
| 配置基于InfiniBand的NVMe端口 | 1. 选择 * 硬件 * 。<br>2. 选择*显示磁盘架的背面*。<br>3. 选择一个控制器。<br>4. 选择 * 配置基于 InfiniBand 端口的 NVMe * 。<br>或<br>1. 选择*菜单：设置[系统]*。<br>2. 向下滚动到*基于InfiniBand的NVMe设置*、然后选择*配置基于InfiniBand端口的NVMe *。 |
| 查看基于InfiniBand的NVMe统计信息 | 1. 选择*菜单：设置[系统]*。<br>2. 向下滚动到*基于InfiniBand的NVMe设置*、然后选择*查看基于网络结构的NVMe统计信息*。 |

要通过**RoCE**配置或诊断**NVMe**、还需要执行哪些操作?

## 您可以从硬件和设置页面配置和管理基于RoCE的NVMe。

只有当存储阵列的控制器包含基于RoCE的NVMe端口时、基于RoCE的NVMe设置才可用。

通过**RoCE**配置和诊断**NVMe**

| Action | 位置 |
| --- | --- |
| 配置基于RoCE的NVMe端口 | 1. 选择 * 硬件 * 。<br>2. 选择*显示磁盘架的背面*。<br>3. 选择一个控制器。<br>4. 选择 * 配置基于 RoCE 的 NVMe 端口 * 。<br><br>或<br><br>1. 选择*菜单：设置[系统]*。<br>2. 向下滚动到*基于RoCE的NVMe设置*、然后选择*配置基于RoCE的NVMe端口*。 |
| 查看基于网络结构的NVMe统计信息 | 1. 选择*菜单：设置[系统]*。<br>2. 向下滚动到*基于RoCE的NVMe设置*、然后选择*查看基于网络结构的NVMe统计信息*。 |

为什么一个物理端口有两个**IP**地址?

## EF600存储阵列可以包含两个HIC—一个外部HIC和一个内部HIC。

在此配置中、外部HIC连接到内部辅助HIC。您可以从外部HIC访问的每个物理端口都具有来自内部HIC的关联虚拟端口。

要获得最大200 GB性能、必须为物理端口和虚拟端口分配唯一的IP地址、以便主机可以与每个端口建立连接。如果不为虚拟端口分配IP地址、HIC将以大约一半的速度运行。

为什么一个物理端口有两组参数?

## EF600存储阵列可以包含两个HIC—一个外部HIC和一个内部HIC。

在此配置中、外部HIC连接到内部辅助HIC。您可以从外部HIC访问的每个物理端口都具有来自内部HIC的关联虚拟端口。

要获得最大200 GB的性能、您必须为物理端口和虚拟端口分配参数、以便主机可以与每个端口建立连接。如果不为虚拟端口分配参数、HIC将以大约一半的可用速度运行。

# 系统：附加功能

## 概念

附加功能的工作原理

## 附加项是System Manager标准配置中不包含的功能、可能需要使用密钥才能启用。附加功能可以是单个高级功能、也可以是捆绑的功能包。

以下步骤概述了如何启用高级功能或功能包：

1. 获取以下信息：
   - 机箱序列号和功能启用标识符、用于标识要安装的功能的存储阵列。这些项目可在System Manager中使用。
   - 功能激活代码、购买此功能时可从支持站点获取。
2. 请联系您的存储提供商或访问高级功能激活站点以获取功能密钥。提供机箱序列号、启用标识符和功能代码以进行激活。
3. 使用System Manager、使用功能密钥文件启用高级功能或功能包。

附加功能术语

## 了解附加功能术语如何应用于存储阵列。

| 期限 | **Description** |
| --- | --- |
| 功能启用标识符 | 功能启用标识符是用于标识特定存储阵列的唯一字符串。此标识符可确保在您获得高级功能时、它仅与该特定存储阵列相关联。此字符串将显示在System页面的Add-Ons下。 |
| 功能密钥文件 | 功能密钥文件是指您收到的用于解锁和启用高级功能或功能包的文件。 |
| 功能包 | 功能包是更改存储阵列属性(例如、将协议从光纤通道更改为iSCSI)的捆绑包。要启用功能包、需要使用特殊密钥。 |
| 高级功能 | 高级功能是一个额外的选项、需要使用密钥才能启用它。System Manager的标准配置不包括此功能。 |

## 操作说明

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、必须先获取功能密钥文件。一个密钥仅与一个存储阵列相关联。

关于此任务

此任务介绍如何收集功能所需的信息、然后发送功能密钥文件请求。所需信息包括：

- 机箱序列号
- 功能启用标识符
- 功能激活代码

步骤

1. 在System Manager中、找到并记录机箱序列号。您可以通过将鼠标悬停在支持中心磁贴上来查看此序列号。

2. 在 System Manager 中，找到功能启用标识符。转到*菜单：设置[系统]、然后向下滚动到*加载项。查找*功能启用标识符*。记录功能启用标识符的编号。
3. 找到并记录用于激活功能的代码。对于功能包、此代码将在执行转换的相应说明中提供。

   NetApp说明可从获取 "NetApp E系列系统文档中心"。

   对于高级功能、您可以从支持站点访问激活代码、如下所示：

   a. 登录到 "NetApp 支持"。
   b. 请访问您的产品对应的*软件许可证*。
   c. 输入存储阵列机箱的序列号、然后单击*执行*。
   d. 在*许可证密钥*列中查找功能激活代码。
   e. 记录所需功能的功能激活代码。
4. 通过向存储供应商发送包含以下信息的电子邮件或文本文档来请求功能密钥文件：机箱序列号、启用标识符和功能激活代码。

   您也可以转到 "NetApp 许可证激活：存储阵列高级功能激活" 并输入所需信息以获取功能或功能包。(此站点上的说明适用于高级功能、而不适用于功能包。)

完成后

如果您有功能密钥文件、则可以启用高级功能或功能包。

启用高级功能

## 高级功能是一个额外的选项、需要启用密钥。

开始之前

- 您已获取功能密钥。如有必要、请联系技术支持以获取密钥。
- 您已在管理客户端(具有用于访问System Manager的浏览器的系统)上加载密钥文件。

关于此任务

此任务介绍如何使用System Manager启用高级功能。

> 如果要禁用高级功能、必须在命令行界面(CLI)中使用禁用存储阵列功能命令(`disable storageArray (featurePack | feature=featureAttributeList)`)。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*加载项*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*浏览*、然后选择密钥文件。

   此时将在对话框中显示文件名。

4. 单击 * 启用 * 。

启用功能包

## 功能包是更改存储阵列属性(例如、将协议从光纤通道更改为iSCSI)的捆绑包。要启用功能包、需要使用特殊密钥。

开始之前

- 您已按照相应说明执行转换并为系统准备新的存储阵列属性。

  可从获取转换说明 "NetApp E系列系统文档中心"。

- 存储阵列处于脱机状态、因此没有主机或应用程序正在访问它。
- 备份所有数据。
- 您已获取功能包文件。

  功能包文件将加载到管理客户端(具有用于访问System Manager的浏览器的系统)上。

您必须计划停机维护时段、并停止主机和控制器之间的所有I/O操作。此外、请注意、在成功完成转换之前、您无法访问存储阵列上的数据。

关于此任务

此任务介绍如何使用System Manager启用功能包。完成后、必须重新启动存储阵列。

步骤

1. 选择*菜单：设置[系统]*。
2. 在 * 加载项 * 下，选择 * 更改功能包 * 。
3. 单击*浏览*、然后选择密钥文件。

   此时将在对话框中显示文件名。

4. 在字段中键入 * 更改 * 。
5. 单击 * 更改 * 。

   功能包迁移将开始、控制器将重新启动。系统将删除未写入的缓存数据、从而确保不会发生I/O活动。两个控制器都会自动重新启动、以使新功能包生效。重新启动完成后，存储阵列将恢复为响应状态。

下载命令行界面**(CLI)**

## 您可以从System Manager下载命令行界面(CLI)软件包。CLI提供了一种基于文本的方法来配置和监控存储阵列。它通过https进行通信、并使用外部安装的管理软件包中提供的CLI语法。下载CLI不需要任何密钥。

开始之前

- 要运行命令行界面命令的管理系统必须具有Java Runtime Environment (JRE) 8及更高版本。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*加载项*下、选择*命令行界面*。

   ZIP包将下载到浏览器。

3. 将ZIP文件保存到要对存储阵列运行CLI命令的管理系统、然后提取该文件。

   现在、您可以从操作系统提示符运行命令行界面命令、例如DOS C：提示符。可从System Manager用户界面右上角的帮助菜单中获取CLI命令参考。

# 系统：安全密钥管理

## 概念

### 驱动器安全功能的工作原理

驱动器安全性是一种存储阵列功能，可通过全磁盘加密（ Full Disk Encryption ， FDE ）驱动器或联邦信息处理标准（ Federal Information Processing Standard ， FIPS ）驱动器提供额外的安全层。如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。

### 如何实施驱动器安全性

要实施驱动器安全性、请执行以下步骤。

1. 为存储阵列配备支持安全保护的驱动器、可以是FDE驱动器、也可以是FIPS驱动器。(对于需要FIPS支持的卷、请仅使用FIPS驱动器。在卷组或池中混用FIPS和FDE驱动器将导致所有驱动器被视为FDE驱动器。此外、FDE驱动器不能添加到纯FIPS卷组或池中或用作备用磁盘。)
2. 创建一个安全密钥、该密钥是一个字符串、由控制器和驱动器共享、用于进行读/写访问。您可以从控制器的永久性内存创建内部密钥、也可以从密钥管理服务器创建外部密钥。对于外部密钥管理、必须使用密钥管理服务器建立身份验证。
3. 为池和卷组启用驱动器安全性：
   - 创建池或卷组(在候选项表的*安全功能*列中查找*是*)。
   - 创建新卷时、请选择池或卷组(在Pool and volume group candidates表中、查找*安全功能*旁边的*是*)。

### 驱动器安全在驱动器级别的工作原理

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

驱动器安全功能可通过支持安全功能的驱动器提供额外的保护层。如果为驱动器安全选择了这些驱动器上的卷组或池、则这些驱动器会先查找安全密钥、然后再允许访问数据。您可以随时为池和卷组启用驱动器安全性、而不会影响驱动器上的现有数据。但是、如果不擦除驱动器上的所有数据、则无法禁用驱动器安全性。

#### 驱动器安全性在存储阵列级别的工作原理

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

如果从存储阵列中删除启用了安全保护的驱动器并将其重新安装在其他存储阵列中、则该驱动器将处于安全锁定状态。重新定位的驱动器会先查找安全密钥、然后再使数据可再次访问。要解锁数据、请应用源存储阵列中的安全密钥。成功解锁过程后、重新定位的驱动器将使用已存储在目标存储阵列中的安全密钥、并且不再需要导入的安全密钥文件。

> 对于内部密钥管理、实际安全密钥存储在控制器上不可访问的位置。它不是以人为可读的格式提供的、也不是用户可访问的格式。

#### 驱动器安全在卷级别的工作原理

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

在创建启用了安全保护的卷组和池之前、请牢记以下准则：

- 卷组和池必须全部由具有安全功能的驱动器组成。(对于需要FIPS支持的卷、请仅使用FIPS驱动器。在卷组或池中混用FIPS和FDE驱动器将导致所有驱动器被视为FDE驱动器。此外、FDE驱动器不能添加到纯FIPS卷组或池中或用作备用磁盘。)
- 卷组和池必须处于最佳状态。

### 安全密钥管理的工作原理

## 在实施驱动器安全功能时、启用了安全保护的驱动器(FIPS或FDE)需要一个安全密钥才能进行数据访问。安全密钥是指这些类型的驱动器与存储阵列中的控制器之间共享的字符串。

无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。如果从存储阵列中删除启用了安全保护的驱动器、则该驱动器的数据将被锁定。在将驱动器重新安装到其他存储阵列中时、它会先查找安全密钥、然后再重新访问数据。要解锁数据、必须应用原始安全密钥。

您可以使用以下方法之一创建和管理安全密钥：

- 控制器永久性内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

#### 内部密钥管理

内部密钥会保留在控制器的永久性内存上。要实施内部密钥管理、请执行以下步骤：

1. 在存储阵列中安装支持安全保护的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
2. 确保已启用驱动器安全功能。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。
3. 创建内部安全密钥、其中包括定义标识符和密码短语。标识符是与安全密钥关联的字符串、存储在控制器以及与该密钥关联的所有驱动器上。密码短语用于对安全密钥进行加密、以用于备份。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不可访问位置。然后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

外部密钥管理

外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上进行维护。要实施外部密钥管理、请执行以下步骤：

1. 在存储阵列中安装支持安全保护的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
2. 确保已启用驱动器安全功能。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。
3. 完成并下载用于在存储阵列和密钥管理服务器之间进行身份验证的客户端证书签名请求(CSR)。转到*菜单：设置[证书>密钥管理>完成CSR]*。
4. 使用下载的CSR文件从密钥管理服务器创建并下载客户端证书。
5. 确保您的本地主机上具有密钥管理服务器的客户端证书和证书副本。
6. 创建外部密钥、其中包括定义密钥管理服务器的IP地址以及用于KMIP通信的端口号。在此过程中、您还可以加载证书文件。要创建外部密钥、请转到*菜单：设置[系统>安全密钥管理>创建外部密钥]*。

系统将使用您输入的凭据连接到密钥管理服务器。然后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

驱动器安全术语

## 了解驱动器安全术语如何应用于存储阵列。

| 期限 | **Description** |
| --- | --- |
| 驱动器安全功能 | 驱动器安全性是一种存储阵列功能，可通过全磁盘加密（Full Disk Encryption，FDE）驱动器或联邦信息处理标准（Federal Information Processing Standard，FIPS）驱动器提供额外的安全层。如果将这些驱动器与驱动器安全功能结合使用，则需要使用安全密钥才能访问其数据。从阵列中物理删除驱动器后、这些驱动器将无法运行、直到将其安装到另一个阵列中为止、此时、这些驱动器将处于安全锁定状态、直到提供了正确的安全密钥为止。 |
| FDE驱动器 | 全磁盘加密(Full Disk Encryption、FDE)驱动器在硬件级别对磁盘驱动器执行加密。硬盘驱动器包含一个ASIC芯片、用于在写入期间对数据进行加密、然后在读取期间对数据进行解密。 |
| FIPS驱动器 | FIPS驱动器使用联邦信息处理标准(FIPS) 140-2级别2。它们本质上是FDE驱动器、符合美国政府标准、可确保强大的加密算法和方法。FIPS驱动器的安全标准高于FDE驱动器。 |
| 管理客户端 | 一种本地系统(计算机、平板电脑等)、其中包括用于访问System Manager的浏览器。 |

| 期限 | Description |
| --- | --- |
| 密码短语 | 密码短语用于对安全密钥进行加密、以用于备份。在因驱动器迁移或机头交换而导入备份的安全密钥时、必须提供用于加密安全密钥的相同密码短语。密码短语可以包含8到32个字符。<br><br>驱动器安全密码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(Full Disk Encryption、FDE)驱动器、也可以是联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器、这些驱动器可在写入期间对数据进行加密、并在读取期间对数据进行解密。这些驱动器被视为安全驱动器-*capable"*、因为可以使用驱动器安全功能提高安全性。如果为这些驱动器使用的卷组和池启用了驱动器安全功能、则这些驱动器将变为*secure—_enabled*. |
| 已启用安全保护的驱动器 | 启用了安全保护的驱动器与驱动器安全功能结合使用。启用驱动器安全功能后、如果将驱动器安全应用于安全-*capable"*驱动器上的池或卷组、则这些驱动器将变为安全-enabled__。只能通过配置了正确安全密钥的控制器进行读写访问。这种增强的安全性可防止未经授权访问从存储阵列中物理删除的驱动器上的数据。 |
| 安全密钥 | 安全密钥是指在存储阵列中启用了安全保护的驱动器和控制器之间共享的字符串。无论何时关闭和打开驱动器的电源、启用了安全保护的驱动器都会变为安全锁定状态、直到控制器应用安全密钥为止。如果从存储阵列中删除启用了安全保护的驱动器、则该驱动器的数据将被锁定。在将驱动器重新安装到其他存储阵列中时、它会先查找安全密钥、然后再重新访问数据。要解锁数据、必须应用原始安全密钥。您可以使用以下方法之一创建和管理安全密钥：<br><br>• 内部密钥管理—在控制器的永久性内存上创建和维护安全密钥。<br>• 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创建密钥期间与安全密钥关联的字符串。标识符存储在控制器以及与安全密钥关联的所有驱动器上。 |

## 操作说明

创建内部安全密钥

### 要使用驱动器安全功能、您可以创建一个内部安全密钥、该密钥由存储阵列中的控制器和支持安全功能的驱动器共享。内部密钥会保留在控制器的永久性内存上。

开始之前

- 存储阵列中必须安装支持安全功能的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
- 必须启用驱动器安全功能。否则、将在此任务期间打开无法创建安全密钥对话框。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。

如果存储阵列中同时安装了FDE和FIPS驱动器、则它们将共享同一个安全密钥。

关于此任务

在此任务中、您可以定义要与内部安全密钥关联的标识符和密码短语。

> 驱动器安全密码短语与存储阵列的管理员密码无关。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*创建内部密钥*。

   如果尚未生成安全密钥、则会打开*创建安全密钥*对话框。

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、此名称和时间戳由控制器固件生成)、也可以输入您自己的值。最多可以输入189个字母数字字符、不带空格、标点符号或符号。

     > 系统会自动生成附加到您输入的字符串两端的其他字符。生成的字符可确保标识符是唯一的。

   - 定义密码短语/重新输入密码短语-输入并确认密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
     - 大写字母(一个或多个)。请注意、密码短语区分大小写。
     - 一个数字(一个或多个)。
     - 非字母数字字符、例如！、*、@(一个或多个)。

   > 请务必记录您的条目以供日后使用。如果您需要从存储阵列移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

4. 单击 * 创建 * 。

   安全密钥存储在控制器上的不可访问位置。除了实际密钥之外、还会从浏览器下载一个加密密钥文件。

   > 下载文件的路径可能取决于浏览器的默认下载位置。

5. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

结果

现在、您可以创建启用了安全保护的卷组或池、也可以在现有卷组和池上启用安全性。

> 每当关闭驱动器电源然后再次打开时、所有启用了安全保护的驱动器都会更改为安全锁定状态。在这种状态下、只有在驱动器初始化期间控制器应用正确的安全密钥后、才能访问数据。如果有人以物理方式删除已锁定的驱动器并将其安装到其他系统中、则安全锁定状态将阻止对其数据进行未经授权的访问。

完成后

您应验证此安全密钥、以确保此密钥文件未损坏。

创建外部安全密钥

## 要对密钥管理服务器使用驱动器安全功能、必须创建一个外部密钥、该密钥由密钥管理服务器和存储阵列中支持安全功能的驱动器共享。

开始之前

- 阵列中必须安装支持安全功能的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。

> 如果存储阵列中同时安装了FDE和FIPS驱动器、则它们将共享同一个安全密钥。

- 必须启用驱动器安全功能。否则、在此任务期间将打开一个*无法创建安全密钥*对话框。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。
- 本地主机上提供了客户端和服务器证书、因此存储阵列和密钥管理服务器可以相互进行身份验证。客户端证书用于验证控制器、而服务器证书用于验证密钥管理服务器。

关于此任务

在此任务中、您可以定义密钥管理服务器的IP地址及其使用的端口号、然后加载用于外部密钥管理的证书。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*创建外部密钥*。

> 如果当前已配置内部密钥管理、则会打开一个对话框、要求您确认是否要切换到外部密钥管理。

此时将打开*创建外部安全密钥*对话框。

3. 在*连接到密钥服务器*下、在以下字段中输入信息：
   - 密钥管理服务器地址—输入用于密钥管理的服务器的完全限定域名或IP地址(IPv4或IPv6)。
   - 密钥管理端口号-输入用于密钥管理互操作性协议(Key Management Interoperability Protocol、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。
   - 选择客户端证书-单击第一个*浏览*按钮以选择存储阵列控制器的证书文件。
   - 选择密钥管理服务器的服务器证书-单击第二个*浏览*按钮以选择密钥管理服务器的证书文件。
4. 单击 * 下一步 * 。
5. 在*创建/备份密钥*下的以下字段中输入信息：
   - 定义密码短语/重新输入密码短语-输入并确认密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
     - 大写字母(一个或多个)。请注意、密码短语区分大小写。
     - 一个数字(一个或多个)。
     - 非字母数字字符、例如！、*、@(一个或多个)。

请务必记录您的条目以供日后使用。如果您需要从存储阵列中移动启用了安全保护的驱动器、则必须知道解锁驱动器数据的密码短语。

6. 单击 * 完成 * 。

   系统将使用您输入的凭据连接到密钥管理服务器。然后、安全密钥的副本将存储在本地系统上。

   下载文件的路径可能取决于浏览器的默认下载位置。

7. 记下您的密码短语以及下载的密钥文件的位置、然后单击*关闭*。

   此页面将显示以下消息、其中包含用于外部密钥管理的其他链接：

   当前密钥管理方法：外部

8. 选择*测试通信*以测试存储阵列与密钥管理服务器之间的连接。

   测试结果将显示在对话框中。

结果

启用外部密钥管理后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

每当关闭驱动器电源然后再次打开时、所有启用了安全保护的驱动器都会更改为安全锁定状态。在这种状态下、只有在驱动器初始化期间控制器应用正确的安全密钥后、才能访问数据。如果有人以物理方式删除已锁定的驱动器并将其安装到其他系统中、则安全锁定状态将阻止对其数据进行未经授权的访问。

完成后

- 您应验证此安全密钥、以确保此密钥文件未损坏。

更改安全密钥

## 您可以随时将安全密钥替换为新密钥。如果您的公司存在潜在的安全违规行为、并且希望确保未经授权的人员无法访问驱动器的数据、您可能需要更改安全密钥。

开始之前

安全密钥已存在。

关于此任务

此任务介绍如何更改安全密钥并将其替换为新的安全密钥。完成此过程后、旧密钥将失效。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*更改密钥*。

   此时将打开更改安全密钥对话框。

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(由控制器固件生成的存储阵列名称和时间戳)或输入您自己的值。最多可以输入189个字母数字字符、不带空格、标点符号或符号。

  系统会自动生成其他字符、并将其附加到您输入的字符串的两端。生成的字符有助于确保标识符是唯一的。

- 定义密码短语/重新输入密码短语—在每个字段中输入您的密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：
  - 大写字母(一个或多个)。请注意、密码短语区分大小写。
  - 一个数字(一个或多个)。
  - 非字母数字字符、例如！、*、@(一个或多个)。

  请务必记录您的条目以供日后使用—如果您需要从存储阵列移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

4. 单击 * 更改 * 。

   新的安全密钥会覆盖上一个密钥、而上一个密钥不再有效。

   下载文件的路径可能取决于浏览器的默认下载位置。

5. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

完成后

您应验证此安全密钥、以确保此密钥文件未损坏。

## 从外部密钥管理切换到内部密钥管理

您可以将驱动器安全管理方法从外部密钥服务器更改为存储阵列使用的内部方法。然后、以前为外部密钥管理定义的安全密钥将用于内部密钥管理。

开始之前

已创建外部密钥。

关于此任务

在此任务中、您可以禁用外部密钥管理并将新的备份副本下载到本地主机。现有密钥仍用于驱动器安全、但将在存储阵列中进行内部管理。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*禁用外部密钥管理*。

   此时将打开*禁用外部密钥管理*对话框。

3. 在*定义密码短语/重新输入密码短语*中、输入并确认用于备份密钥的密码短语。此值可以包含8到32个字符、并且必须包括以下每个字符：

- 大写字母(一个或多个)。请注意、密码短语区分大小写。
- 一个数字(一个或多个)。
- 非字母数字字符、例如！、*、@(一个或多个)。

> 请务必记录您的条目以供日后使用_。如果您需要从存储阵列移动启用了安全保护的驱动器、则必须知道用于解锁驱动器数据的标识符和密码短语。

4. 单击 * 禁用 * 。

   备份密钥将下载到本地主机。

5. 记下您的密钥标识符、密码短语以及下载的密钥文件的位置、然后单击*关闭*。

结果

现在、驱动器安全性可通过存储阵列在内部进行管理。

完成后

- 您应验证此安全密钥、以确保此密钥文件未损坏。

编辑密钥管理服务器设置

## 如果您配置了外部密钥管理、则可以随时查看和编辑密钥管理服务器设置。

开始之前

必须配置外部密钥管理。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*查看/编辑密钥管理服务器设置*。
3. 编辑以下字段中的信息：
   - 密钥管理服务器地址—输入用于密钥管理的服务器的完全限定域名或IP地址(IPv4或IPv6)。
   - * KMIP端口号*-输入用于密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)通信的端口号。
4. 单击 * 保存 * 。

备份安全密钥

## 创建或更改安全密钥后、您可以为密钥文件创建备份副本、以防其损坏。

开始之前

- 安全密钥已存在。

关于此任务

此任务介绍如何备份先前创建的安全密钥。在此操作步骤 期间、您将为备份创建一个新的密码短语。此密码短语不需要与创建原始密钥或上次更改时使用的密码短语匹配。密码短语仅适用于您要创建的备份。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*备份密钥*。

   此时将打开备份安全密钥对话框。

3. 在*定义密码短语/重新输入密码短语*字段中、输入并确认此备份的密码短语。

   此值可以包含8到32个字符、并且必须包括以下每个字符：

   - 大写字母(一个或多个)
   - 一个数字(一个或多个)
   - 非字母数字字符、例如！、*、@(一个或多个)

   请务必记录您的条目、以供日后使用。要访问此安全密钥的备份、您需要使用密码短语。

4. 单击*备份*。

   安全密钥的备份将下载到本地主机、然后打开*确认/记录安全密钥备份*对话框。

   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. 在安全位置记下您的密码短语、然后单击*关闭*。

完成后

您应验证备份安全密钥。

## 验证安全密钥

您可以验证安全密钥、以确保其未损坏、并验证您是否具有正确的密码短语。

开始之前

已创建安全密钥。

关于此任务

此任务介绍如何验证您先前创建的安全密钥。这是确保密钥文件未损坏且密码短语正确的重要步骤、它可确保在将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列后、您可以访问驱动器数据。

步骤

1. 选择*菜单：设置[系统]*。
2. 在*安全密钥管理*下、选择*验证密钥*。

   此时将打开*验证安全密钥*对话框。

3. 单击*浏览*、然后选择密钥文件(例如、`drivesecury.slk`)。
4. 输入与选定密钥关联的密码短语。

选择有效的密钥文件和密码短语后、*验证*按钮将变为可用。

5. 单击*验证*。

   验证结果将显示在对话框中。

6. 如果结果显示"The security key validated successfully"、请单击*关闭*。如果显示错误消息、请按照对话框中显示的建议说明进行操作。

使用安全密钥解锁驱动器

## 如果要将启用了安全保护的驱动器从一个存储阵列移动到另一个存储阵列、则必须将相应的安全密钥导入到新存储阵列中。导入密钥会解锁驱动器上的数据。

开始之前

- 目标存储阵列(要移动驱动器的存储阵列)必须已配置安全密钥。迁移的驱动器将重新密钥设置到目标存储阵列。
- 您必须知道与要解锁的驱动器关联的安全密钥。
- 管理客户端(具有用于访问System Manager的浏览器的系统)上提供了安全密钥文件。如果要将驱动器移动到由其他系统管理的存储阵列、则需要将安全密钥文件移动到该管理客户端。

关于此任务

此任务介绍如何解锁已从存储阵列中删除并重新安装在另一个存储阵列中的已启用安全的驱动器中的数据。阵列发现驱动器后、将显示"需要注意"情况、并为这些重新定位的驱动器显示"需要安全密钥"状态。您可以通过将驱动器数据的安全密钥导入到存储阵列中来解锁驱动器数据。在此过程中、您可以选择安全密钥文件并输入密钥的密码短语。

> 密码短语与存储阵列的管理员密码不同。

如果新存储阵列中安装了其他启用了安全保护的驱动器、则这些驱动器使用的安全密钥可能与您要导入的安全密钥不同。在导入过程中、旧安全密钥仅用于解锁要安装的驱动器的数据。成功完成解锁过程后、新安装的驱动器将重新密钥到目标存储阵列的安全密钥。

步骤

1. 选择菜单：设置[系统]。
2. 在*安全密钥管理*下、选择*解锁安全驱动器*。

   此时将打开解除安全驱动器锁定对话框。表中显示了需要安全密钥的所有驱动器。

3. *可选：*将鼠标悬停在驱动器编号上方可查看驱动器的位置(磁盘架编号和托架编号)。
4. 单击*浏览*、然后选择与要解锁的驱动器对应的安全密钥文件。

   您选择的密钥文件将显示在对话框中。

5. 输入与此密钥文件关联的密码短语。

   输入的字符将被屏蔽。

6. 单击*解锁*。

如果解锁操作成功、则对话框将显示："The associated secure drives have been unlocked"。

结果

锁定并解除锁定所有驱动器后、存储阵列中的每个控制器都将重新启动。但是、如果目标存储阵列中已有一些未锁定的驱动器、则控制器不会重新启动。

## 常见问题解答

在创建安全密钥之前、我需要了解哪些信息？

### 安全密钥由存储阵列中的控制器和启用了安全保护的驱动器共享。如果从存储阵列中删除了启用了安全保护的驱动器、则安全密钥可防止数据遭受未经授权的访问。

您可以使用以下方法之一创建和管理安全密钥：

- 控制器永久性内存上的内部密钥管理。
- 外部密钥管理服务器上的外部密钥管理。

在创建内部安全密钥之前、必须执行以下操作：

1. 在存储阵列中安装支持安全保护的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
2. 确保已启用驱动器安全功能。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。

然后、您可以创建内部安全密钥、其中包括定义标识符和密码短语。标识符是与安全密钥关联的字符串、存储在控制器以及与该密钥关联的所有驱动器上。密码短语用于对安全密钥进行加密、以用于备份。完成后、安全密钥将存储在控制器上不可访问的位置。然后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

在创建外部安全密钥之前、必须执行以下操作：

1. 在存储阵列中安装支持安全保护的驱动器。这些驱动器可以是全磁盘加密(Full Disk Encryption、FDE)驱动器或联邦信息处理标准(Federal Information Processing Standard、FIPS)驱动器。
2. 确保已启用驱动器安全功能。如有必要、请联系您的存储供应商、了解有关启用驱动器安全功能的说明。
3. 完成并下载用于在存储阵列和密钥管理服务器之间进行身份验证的客户端证书签名请求(CSR)。转到*菜单：设置[证书>密钥管理>完成CSR]*。
4. 使用下载的CSR文件从密钥管理服务器创建并下载客户端证书。
5. 确保您的本地主机上具有密钥管理服务器的客户端证书和证书副本。

然后、您可以创建外部密钥、其中包括定义密钥管理服务器的IP地址以及用于KMIP通信的端口号。在此过程中、您还可以加载证书文件。完成后、系统将使用您输入的凭据连接到密钥管理服务器。然后、您可以创建启用了安全保护的卷组或池、也可以对现有卷组和池启用安全性。

为什么需要定义密码短语？

### 密码短语用于对存储在本地管理客户端上的安全密钥文件进行加密和解密。如果没有密码短语、则无法对安全密钥进行解密、并使用此安全密钥从启用了安全功能的驱动器中解锁

数据、如果此驱动器重新安装在另一个存储阵列中。

为什么记录安全密钥信息很重要?

如果丢失安全密钥信息并且没有备份、则在重新定位启用了安全保护的驱动器或升级控制器时可能会丢失数据。您需要使用安全密钥来解锁驱动器上的数据。

请务必记录安全密钥标识符、关联的密码短语以及安全密钥文件保存在本地主机上的位置。

备份安全密钥前需要了解哪些信息?

如果原始安全密钥损坏、并且您没有备份、则在驱动器从一个存储阵列迁移到另一个存储阵列时、您将无法访问这些驱动器上的数据。

备份安全密钥之前、请记住以下准则:

- 确保您知道原始密钥文件的安全密钥标识符和密码短语。

> 只有内部密钥使用标识符。创建标识符时、系统会自动生成其他字符并将其附加到标识符字符串的两端。生成的字符可确保标识符是唯一的。

- 您可以为备份创建新的密码短语。此密码短语不需要与创建原始密钥或上次更改时使用的密码短语匹配。密码短语仅适用于您要创建的备份。

> 驱动器安全密码短语不应与存储阵列的管理员密码相混淆。Drive Security的密码短语用于保护安全密钥的备份。管理员密码可保护整个存储阵列、防止未经授权的访问。

- 备份安全密钥文件将下载到管理客户端。下载文件的路径可能取决于浏览器的默认下载位置。请务必记录安全密钥信息的存储位置。

在解除安全驱动器锁定之前、我需要了解哪些信息?

要从已迁移到新存储阵列且已启用安全保护的驱动器解锁数据、您必须导入其安全密钥。

在解除锁定启用了安全保护的驱动器之前、请记住以下准则:

- 目标存储阵列(用于移动驱动器)必须已具有安全密钥。迁移的驱动器将重新密钥设置到目标存储阵列。
- 对于要迁移的驱动器、您知道安全密钥标识符以及与安全密钥文件对应的密码短语。
- 管理客户端(具有用于访问System Manager的浏览器的系统)上提供了安全密钥文件。
- 如果要重置锁定的NVMe驱动器、必须输入驱动器的安全ID。要找到安全ID、您必须物理移除驱动器、并在驱动器标签上找到PSID字符串(最多32个字符)。在开始操作之前、请确保已重新安装驱动器。

什么是读/写可访问性?

驱动器设置窗口包含有关驱动器安全属性的信息。"读/写可访问"是驱动器数据已锁定时显示的属性之一。

要查看驱动器安全属性、请转到硬件页面。选择一个驱动器、单击*查看设置*、然后单击*显示更多设置*。如果

驱动器已解锁、则页面底部的读/写可访问属性值为*是*。驱动器锁定时、读/写可访问属性值为*否、安全密钥无效*。您可以通过导入安全密钥来解锁安全驱动器(转到菜单：设置(系统>解锁安全驱动器)。

验证安全密钥时需要了解哪些信息？

### 创建安全密钥后、您应验证密钥文件以确保其未损坏。

如果验证失败、请执行以下操作：

- 如果安全密钥标识符与控制器上的标识符不匹配、请找到正确的安全密钥文件、然后重试验证。
- 如果控制器无法对安全密钥进行解密以进行验证、则您输入的密码短语可能不正确。仔细检查密码短语、必要时重新输入、然后重试验证。如果此错误消息再次出现、请选择密钥文件的备份(如果可用)、然后重试验证。
- 如果仍然无法验证安全密钥、则原始文件可能已损坏。创建密钥的新备份并验证该副本。

内部安全密钥与外部安全密钥管理有何区别？

### 在实施驱动器安全功能时、当从存储阵列中删除启用了安全保护的驱动器时、您可以使用内部安全密钥或外部安全密钥锁定数据。

安全密钥是一个字符串、在存储阵列中启用了安全保护的驱动器和控制器之间共享。内部密钥会保留在控制器的永久性内存上。外部密钥使用密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)在单独的密钥管理服务器上进行维护。

# 访问管理

## 概念

访问管理的工作原理

### 访问管理是在SANtricity System Manager中建立用户身份验证的一种方法。

访问管理配置和用户身份验证的工作原理如下：

1. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。

   > 首次登录时、系统会自动显示用户名`admin`、并且无法更改。`admin`用户可以完全访问系统中的所有功能。

2. 管理员可在用户界面中导航到访问管理。存储阵列已预先配置为使用本地用户角色、这是RBAC (基于角色的访问控制)功能的实施。
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—身份验证通过在存储阵列中强制实施的RBAC功能进行管理。本地用户角色包括预定义的用户配置文件以及具有特定访问权限的角色。管理员可以使用这些本地用户角色作为单一身份验证方法、也可以将其与目录服务结合使用。除了为用户设置密码之外、无需进行任何配置。
   - 目录服务—身份验证通过LDAP (轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)进行管理。管理员连接到LDAP服务器、然后将LDAP用户映射到存储阵列中嵌入的本地用户角色。

- * SAML *-身份验证通过使用安全断言标记语言(SAML) 2.0的身份提供程序(IdP)进行管理。管理员在IdP系统和存储阵列之间建立通信、然后将IdP用户映射到存储阵列中嵌入的本地用户角色。

4. 管理员为用户提供System Manager的登录凭据。
5. 用户通过输入凭据登录到系统。

> 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。

登录期间、系统将执行以下后台任务：

- 根据用户帐户对用户名和密码进行身份验证。
- 根据分配的角色确定用户的权限。
- 为用户提供对用户界面中任务的访问权限。
- 显示界面右上角的用户名。

#### System Manager中提供的任务

任务访问权限取决于用户分配的角色、这些角色包括：

- 存储管理—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
- 安全管理—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
- 支持管理—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。
- 监控—对所有存储对象的只读访问、但无法访问安全配置。

不可用的任务将灰显或不显示在用户界面中。例如、具有"监控"角色的用户可以查看有关卷的所有信息、但无法访问用于修改该卷的功能。诸如*复制服务*和*添加到工作负载*等功能的选项卡将灰显；只有*查看/编辑设置*可用。

#### SANtricity Unified Manager和SANtricity 存储管理器中的限制

如果为存储阵列配置了SAML、则用户无法通过SANtricity 统一管理器或SANtricity 存储管理器界面发现或管理该阵列的存储。

配置本地用户角色和目录服务后、用户必须输入凭据、然后才能执行以下任一功能：

- 重命名存储阵列
- 正在升级控制器固件
- 正在加载存储阵列配置
- 正在执行脚本
- 正在尝试在未使用的会话超时时时执行活动操作

访问管理术语

## 了解访问管理术语如何应用于存储阵列。

| 期限 | **Description** |
| --- | --- |
| Active Directory | Active Directory (AD)是一种Microsoft目录服务、使用LDAP进行Windows域网络。 |
| 绑定 | 绑定操作用于向目录服务器对客户端进行身份验证。绑定通常需要帐户和密码凭据、但某些服务器允许匿名绑定操作。 |
| CA | 证书颁发机构(Certificate Authority、CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。 |
| 证书 | 出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。 |
| IdP | 身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。 |
| LDAP | 轻型目录访问协议(Lightweight Directory Access Protocol、LDAP)是一种用于访问和维护分布式目录信息服务的应用程序协议。此协议允许许多不同的应用程序和服务连接到LDAP服务器以验证用户。 |
| RBAC | 基于角色的访问控制(Role-Based Access Control、RBAC)是一种根据各个用户的角色来管理对计算机或网络资源的访问的方法。RBAC控制会在存储阵列上强制实施、并包括预定义的角色。 |
| SAML | 安全断言标记语言(SAML)是一种基于XML的标准、用于在两个实体之间进行身份验证和授权。SAML支持多因素身份验证、在这种身份验证中、用户必须提供两个或更多项来证明其身份(例如密码和指纹)。存储阵列的嵌入式SAML功能符合SAML2.0标准、可用于身份断言、身份验证和授权。 |
| SP | 服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。 |
| 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。 |

映射角色的权限

## 在存储阵列上强制实施的RBAC (基于角色的访问控制)功能包括预定义的用户配置文件、其中一个或多个角色映射到这些配置文件。每个角色都具有访问SANtricity System Manager中任务的权限。

用户配置文件和映射的角色可从任一System Manager的用户界面中的*菜单：设置[访问管理>本地用户角色]*进行访问。

这些角色可为用户提供对任务的访问权限、如下所示：

- 存储管理—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
- 安全管理—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
- 支持管理—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。
- 监控—对所有存储对象的只读访问、但无法访问安全配置。

如果用户没有执行某个任务的权限、则该任务将灰显或不会显示在用户界面中。

### 具有本地用户角色的访问管理

## 对于访问管理、管理员可以使用在存储阵列中强制实施的RBAC (基于角色的访问控制)功能。这些功能称为"本地用户角色"。

#### 配置工作流

已为存储阵列预先配置本地用户角色。要使用本地用户角色进行身份验证、管理员可以执行以下操作：

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SANtricity 系统管理器。

   `admin`用户可以完全访问系统中的所有功能。

2. 管理员会查看用户配置文件、这些配置文件是预定义的、无法修改。
3. *可选：*管理员为每个用户配置文件分配新密码。
4. 用户使用分配的凭据登录到系统。

#### 管理

如果仅使用本地用户角色进行身份验证、则管理员可以执行以下管理任务：

- 更改密码。
- 设置密码的最小长度。
- 允许用户在不使用密码的情况下登录。

### 使用目录服务进行访问管理

## 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SANtricity 系统管理器。

   `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)、则管理员将上传证书颁发机构(CA)证书链、以便在LDAP服务器和存储阵列之间进行身份验证。
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/Directory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。

## 使用**SAML**进行访问管理

对于访问管理、管理员可以使用阵列中嵌入的安全断言标记语言(Security Assertion Markup Language、SAML) 2.0功能。

配置工作流

SAML配置的工作原理如下：

1. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。

   `admin`用户可以完全访问System Manager中的所有功能。

2. 管理员转到访问管理下的* SAML *选项卡。
3. 管理员配置与身份提供程序(Identity Provider、IdP)的通信。IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。要配置与存储阵列的通信、管理员将从IdP系统下载IdP元数据文件、然后使用System Manager将此文件上传到存储阵列。
4. 管理员在服务提供商和IdP之间建立信任关系。服务提供商负责控制用户授权；在这种情况下、存储阵列中的控制器充当服务提供商。要配置通信、管理员可以使用System Manager导出每个控制器的服务提供商元数据文件。然后、管理员从IdP系统将这些元数据文件导入到IdP中。

   管理员还应确保IdP支持在身份验证时返回名称ID。

5. 管理员会将存储阵列的角色映射到IdP中定义的用户属性。为此、管理员可以使用System Manager创建映射。
6. 管理员测试对IdP URL的SSO登录。此测试可确保存储阵列和IdP能够进行通信。

   启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

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：

- 修改或创建新角色映射
- 导出服务提供商文件

访问限制

启用SAML后、用户将无法通过SANtricity 统一管理器或SANtricity 存储管理器界面发现或管理该阵列的存储。

此外、以下客户端无法访问存储阵列服务和资源：

- 企业管理窗口(EMW)
- 命令行界面（ CLI ）
- 软件开发人员套件(SDK)客户端
- 带内客户端
- HTTP基本身份验证REST API客户端
- 使用标准REST API端点登录

## 操作说明

查看本地用户角色

### 在本地用户角色选项卡中、您可以查看用户配置文件与默认角色的映射。这些映射是在存储阵列中强制实施的RBAC (基于角色的访问控制)的一部分。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

无法更改用户配置文件和映射。只能修改密码。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择*本地用户角色*选项卡。

   下表显示了用户配置文件：

   - * root admin*(admin)—超级管理员、有权访问系统中的所有功能。此用户配置文件包含所有角色。
   - 存储管理(存储)—负责所有存储配置的管理员。此用户配置文件包括以下角色：存储管理员、支持管理员和监控。

- 安全性管理(安全性)—负责安全配置的用户、包括访问管理、证书管理和启用了安全保护的驱动器功能。此用户配置文件包括以下角色：安全管理员和监控。
- 支持管理(支持)—负责硬件资源、故障数据和固件升级的用户。此用户配置文件包括以下角色：Support Admin和Monitor。
- 监控(监控)—对系统具有只读访问权限的用户。此用户配置文件仅包含监控角色。

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必须满足或超过当前最低密码设置(在"查看/编辑设置"中)。
- 密码区分大小写。
- 设置密码时、密码中的后缀空格不会被删除。如果密码中包含空格、请小心操作。
- 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。

> 在System Manager中更改密码也会在命令行界面(CLI)中进行更改。此外、密码还会将发生原因用户的活动会话更改为终止。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择*本地用户角色*选项卡。
3. 从表中选择一个用户。

   更改密码按钮将变为可用。

4. 选择 * 更改密码 * 。

   此时将打开更改密码对话框。

5. 如果未为本地用户密码设置最小密码长度、则可以选中此框以要求选定用户输入密码以访问存储阵列、然后您可以键入选定用户的新密码。
6. 输入本地管理员密码、然后单击*更改*。

结果

如果用户当前已登录、则更改密码会导致用户的活动会话终止。

更改本地用户密码设置

## 您可以为存储阵列上的所有新的或更新的本地用户密码设置所需的最小长度。您还可以允许本地用户在不输入密码的情况下访问存储阵列。

开始之前

- 您必须以本地管理员身份登录、其中包括root管理员权限。

关于此任务

设置本地用户密码的最小长度时、请记住以下准则：

- 设置更改不会影响现有本地用户密码。
- 本地用户密码的最小长度设置必须介于0到30个字符之间。
- 任何新的本地用户密码都必须满足或超过当前的最小长度设置。
- 如果希望本地用户在未输入密码的情况下访问存储阵列、请勿设置密码的最小长度。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择*本地用户角色*选项卡。
3. 选择*查看/编辑设置*按钮。

   此时将打开*本地用户密码设置*对话框。

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"至少需要所有本地用户密码"复选框。
   - 要为所有本地用户密码设置最小密码长度、请选中"要求所有本地用户密码至少为"复选框、然后使用spinner框设置所有本地用户密码所需的最小长度。

     任何新的本地用户密码都必须满足或超过当前设置。

5. 单击 * 保存 * 。

添加目录服务器

## 要为访问管理配置身份验证、您可以在存储阵列和LDAP服务器之间建立通信、然后将LDAP用户组映射到阵列的预定义角色。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 必须在目录服务中定义用户组。
- LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
- 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

关于此任务

添加目录服务器分为两步。首先输入域名和URL。如果服务器使用安全协议、则如果CA证书由非标准签名颁发机构签名、则还必须上传此CA证书以进行身份验证。如果您拥有绑定帐户的凭据、则还可以输入您的用户帐户名称和密码。接下来、将LDAP服务器的用户组映射到存储阵列的预定义角色。

> 在操作步骤 添加LDAP服务器期间、原有管理界面将被禁用。原有管理界面(符号)是存储阵列与管理客户端之间的一种通信方法。禁用后、存储阵列和管理客户端将使用更安全的通信方法(基于https的REST API)。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 从*目录服务*选项卡中、选择*添加目录服务器*。

   此时将打开添加目录服务器对话框。

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

| 正在设置 ... | Description |
| --- | --- |
| 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 |
| 输入用于访问LDAP服务器的URL、格式为`ldap：//主机：端口`。 | 上传证书(可选) |
| 只有在上述服务器URL字段中指定了LDAPS协议时、才会显示此字段。<br><br>单击*浏览*并选择要上传的CA证书。这是用于对LDAP服务器进行身份验证的可信证书或证书链。 | 绑定帐户(可选) |
| 输入一个只读用户帐户、用于对LDAP服务器进行搜索查询以及在组中进行搜索。以LDAP类型格式输入帐户名称。例如、如果绑定用户名为"bindAcct"、则可以输入"cn=bindAcct、cn=users、DC=cpoc、DC=local"等值。 | 绑定密码(可选) |

| 正在设置 ... | Description |
| --- | --- |
| 输入上述绑定帐户时、将显示此字段。<br>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* |
| 搜索基础DN | 输入LDAP环境以搜索用户、通常形式为`CN=Users、DC=cOPC、DC=local`。 |
| username属性 | 输入绑定到用户ID的属性以进行身份验证。例如：`sAMAccountName`。 |
| 组属性 | 输入用户上的组属性列表、用于组到角色映射。例如：`memberOf`、`managedObjects`。 |

4. 单击"*角色映射"*选项卡。
5. 将LDAP组分配给预定义角色。一个组可以分配多个角色。

字段详细信息

| 正在设置 ... | Description |
| --- | --- |
| 映射 | 组DN |
| 为要映射的LDAP用户组指定组可分辨名称(DN)。 | 角色 |

包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

1. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
2. 完成映射后、单击*添加*。

   系统将执行验证、以确保存储阵列和LDAP服务器可以进行通信。如果显示错误消息、请检查在对话框中输入的凭据、并根据需要重新输入信息。

编辑目录服务器设置和角色映射

## 如果您之前在Access Management中配置了目录服务器、则可以随时更改其设置。设置包括服务器连接信息和组到角色映射。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 必须定义目录服务器。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择*目录服务*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*查看/编辑设置*。

   此时将打开*目录服务器设置*对话框。

5. 在*服务器设置*选项卡中、更改所需设置。

| 正在设置 ... | Description |
|---|---|
| 配置设置 | 域 |
| LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(*username@domain*)以指定要对其进行身份验证的目录服务器。 | 服务器URL |
| 用于访问LDAP服务器的URL、格式为`ldap：//主机：端口`。 | 绑定帐户(可选) |
| 用于对LDAP服务器进行搜索查询以及在组内进行搜索的只读用户帐户。 | 绑定密码(可选) |

| 正在设置 ... | Description |
| --- | --- |
| 绑定帐户的密码。(输入绑定帐户时会显示此字段。) | 保存前测试服务器连接 |
| 检查存储阵列是否可以与LDAP服务器配置进行通信。单击对话框底部的*保存*后、将进行测试。如果选中此复选框且测试失败、则不会更改配置。您必须解决此错误或取消选中此复选框、才能跳过测试并重新编辑配置。 | 权限设置 |
| 搜索基础DN | 用于搜索用户的LDAP环境、通常采用`CN=Users、DC=cOPC、DC=local`的形式。 |
| username属性 | 绑定到用户ID进行身份验证的属性。例如：`sAMAccountName`。 |
| 组属性 | 用户上的组属性列表、用于组到角色映射。例如：`memberOf`、`managedObjects`。 |

6. 在*角色映射*选项卡中、更改所需的映射。

| 正在设置 ... | Description |
| --- | --- |
| 映射 | 组DN |
| 要映射的LDAP用户组的域名。 | 角色 |

> 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

7. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
8. 单击 * 保存 * 。

结果

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

删除目录服务器

要中断目录服务器与存储阵列之间的连接、您可以从访问管理页面中删除服务器信息。如果您配置了新服务器、然后要删除旧服务器、则可能需要执行此任务。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择*目录服务*选项卡。
3. 从列表中、选择要删除的目录服务器。
4. 单击 * 删除 * 。

   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*。

   此时将删除目录服务器配置设置、权限设置和角色映射。用户无法再使用此服务器的凭据登录。

## 配置SAML

要为访问管理配置身份验证、您可以使用存储阵列中嵌入的安全断言标记语言(SAML)功能。此配置将在身份提供程序和存储提供程序之间建立连接。

关于此任务

身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。要在IdP和存储阵列之间建立连接、您需要在这两个实体之间共享元数据文件。接下来、将IdP用户实体映射到存储阵列角色。最后、在启用SAML之前、您需要测试连接和SSO登录。

- SAML和目录服务*。如果在将目录服务配置为身份验证方法时启用SAML、则SAML将取代System Manager中的目录服务。如果稍后禁用SAML、则目录服务配置将返回到其先前的配置。

*正在编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

配置SAML身份验证是一个多步骤操作步骤。

#### 第1步：上传IdP元数据文件

要为存储阵列提供IdP连接信息、请将IdP元数据导入到System Manager中。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- IdP管理员已配置IdP系统。

- IdP管理员已确保IdP支持在身份验证时返回名称ID。
- 管理员已确保IdP服务器和控制器时钟保持同步(通过NTP服务器或通过调整控制器时钟设置)。
- IdP元数据文件从IdP系统下载、并可从用于访问System Manager的本地系统上获得。

关于此任务

在此任务中、您将元数据文件从IdP上传到System Manager。IdP系统需要使用此元数据将身份验证请求重定向到正确的URL并验证收到的响应。您只需为存储阵列上传一个元数据文件、即使有两个控制器也是如此。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择* SAML *选项卡。

   此页面将显示配置步骤的概述。

3. 单击*导入身份提供程序(IdP)文件*链接。

   此时将打开*导入身份提供程序文件*对话框。

4. 单击*浏览*以选择您复制到本地系统的IdP元数据文件并将其上传。

   选择文件后、将显示IdP实体ID。

5. 单击 * 导入 * 。

第**2**步：导出服务提供商文件

要在IdP和存储阵列之间建立信任关系、请将服务提供商元数据导入到IdP中。

开始之前

- 您知道存储阵列中每个控制器的IP地址或域名。

关于此任务

在此任务中、您将从控制器导出元数据(每个控制器一个文件)。IdP需要使用此元数据与控制器建立信任关系并处理授权请求。此文件包含控制器域名或IP地址等信息、以便IdP可以与服务提供商进行通信。

步骤

1. 单击*导出服务提供商文件*链接。

   此时将打开*导出服务提供商文件*对话框。

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*将元数据文件保存到本地系统。如果存储阵列包含两个控制器、请对*控制器B*字段中的第二个控制器重复此步骤。

   单击*导出*后、服务提供商元数据将下载到本地系统。记下文件的存储位置。

3. 在本地系统中、找到您导出的服务提供商元数据文件。

   每个控制器都有一个XML格式的文件。

4. 从IdP服务器导入服务提供商元数据文件以建立信任关系。您可以直接导入文件、也可以手动输入文件中的控制器信息。

#### 第3步：映射角色

要为用户提供对System Manager的授权和访问权限、您必须将IdP用户属性和组成员资格映射到存储阵列的预定义角色。

开始之前

- IdP管理员已在IdP系统中配置用户属性和组成员资格。
- IdP元数据文件将导入到System Manager中。
- 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。

关于此任务

在此任务中、您可以使用System Manager将IdP组映射到本地用户角色。

步骤

1. 单击链接以映射System Manager角色。

   此时将打开角色映射对话框。

2. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。

   字段详细信息

| 正在设置 ... | Description |
|---|---|
| 映射 | 用户属性 |
| 指定要映射的SAML组的属性(例如、"member for")。 | 属性值 |
| 指定要映射的组的属性值。 | 角色 |

> 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

3. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。

> 启用SAML后、可以修改角色映射。

4. 完成映射后、单击*保存*。

#### 第4步：测试SSO登录

为了确保IdP系统和存储阵列可以进行通信、您可以选择测试SSO登录。在启用SAML的最后一步中、也会执行此测试。

开始之前

- IdP元数据文件将导入到System Manager中。
- 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。

步骤

1. 选择*测试SSO登录*链接。

   此时将打开一个对话框、用于输入SSO凭据。

2. 输入具有安全管理员权限和监控权限的用户的登录凭据。

   在系统测试登录时、将打开一个对话框。

3. 查找Test Successful消息。如果测试成功完成、请转至下一步以启用SAML。

   如果测试未成功完成、则会显示一条错误消息、其中包含更多信息。请确保：

   - 该用户属于具有安全管理员和监控权限的组。
   - 您为IdP服务器上传的元数据正确无误。
   - SP元数据文件中的控制器地址正确。

#### 第5步：启用SAML

最后一步是启用SAML用户身份验证。

开始之前

- IdP元数据文件将导入到System Manager中。
- 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。
- 至少配置了一个监控器和一个安全管理员角色映射。

关于此任务

此任务介绍如何完成用户身份验证的SAML配置。在此过程中、系统还会提示您测试SSO登录。上一步介绍了SSO登录测试过程。

> *正在编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

步骤

1. 从* SAML *选项卡中、选择*启用SAML *链接。

   此时将打开*确认启用SAML *对话框。

2. 键入`enable`、然后单击*启用*。

3. 输入用于SSO登录测试的用户凭据。

结果

系统启用SAML后、它将终止所有活动会话并开始通过SAML对用户进行身份验证。

### 更改**SAML**角色映射

## 如果先前已为访问管理配置SAML、则可以更改IdP组与存储阵列的预定义角色之间的角色映射。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- IdP管理员已在IdP系统中配置用户属性和组成员资格。
- 已配置并启用SAML。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择* SAML *选项卡。
3. 选择*角色映射*。

   此时将打开*角色映射*对话框。

4. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。

   请注意、在启用SAML时、您不会删除权限、否则您将无法访问System Manager。

   字段详细信息

| 正在设置 ... | Description |
|---|---|
| 映射 | 用户属性 |
| 指定要映射的SAML组的属性(例如、"member for")。 | 属性值 |
| 指定要映射的组的属性值。 | 角色 |

包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

1. *可选：*单击*添加另一个映射*以输入更多组到角色的映射。
2. 单击 * 保存 * 。

结果

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

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服务提供商元数据并将文件重新导入到身份提供程序(Identity Provider、IdP)系统中。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 已配置并启用SAML。

关于此任务

在此任务中、您将从控制器导出元数据(每个控制器一个文件)。IdP需要使用此元数据与控制器建立信任关系并处理身份验证请求。此文件包含IdP可用于发送请求的控制器域名或IP地址等信息。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择* SAML *选项卡。
3. 选择*导出*。

   此时将打开*导出服务提供商文件*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均为只读字段。

   记下文件的存储位置。

5. 在本地系统中、找到您导出的服务提供商元数据文件。

   每个控制器都有一个XML格式的文件。

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、也可以手动输入文件中的控制器信息。
7. 单击 * 关闭 * 。

查看审核日志活动

## 通过查看审核日志、具有安全管理员权限的用户可以监控用户操作、身份验证失败、无效登录尝试以及用户会话生命周期。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

步骤

1. 选择*菜单：设置[访问管理]*。

2. 选择*审核日志*选项卡。

   审核日志活动以表格形式显示、其中包括以下信息列：

   - 日期/时间-存储阵列检测到事件的时间戳(GMT)。
   - 用户名-与事件关联的用户名。对于存储阵列上的任何未经身份验证的操作、"N/A"将显示为用户名。未经过身份验证的操作可能由内部代理或其他机制触发。
   - 状态代码—操作的HTTP状态代码(200、400等)以及与事件关联的描述性文本。
   - "已访问**URL"**-完整URL (包括主机)和查询字符串。
   - 客户端**IP**地址-与事件关联的客户端的IP地址。
   - 源—与事件关联的日志记录源、可以是System Manager、CLI、Web服务或支持Shell。

3. 使用审核日志页面上的选项可查看和管理事件。

选择详细信息

| 选择 | Description |
| --- | --- |
| 显示事件 | 按日期范围(过去24小时、过去7天、过去30天或自定义日期范围)显示的限制事件。 |
| 筛选器 | 限制按字段中输入的字符显示的事件。请使用引号("")来精确匹配字词、输入`或`返回一个或多个字词、或者输入短划线("-")来省略字词。 |
| 刷新 | 选择*刷新*可将页面更新为最新事件。 |
| 查看/编辑设置 | 选择*查看/编辑设置*以打开一个对话框、在此可以指定完整的日志策略以及要记录的操作级别。 |
| 删除事件 | 选择*删除*以打开一个对话框、在此可以从页面中删除旧事件。 |
| 显示/隐藏列 | 单击*显示/隐藏*列图标 可选择其他列以显示在表中。其他列包括：<br>• 方法- HTTP方法(例如POST、GET、DELETE等)。<br>• 已执行命令行界面命令—为安全命令行界面请求执行的命令行界面命令(语法)。<br>• 命令行界面返回状态—命令行界面状态代码或客户端请求输入文件。<br>• *符号操作步骤 *—符号操作步骤 已执行。<br>• * SSH事件类型*-安全Shell (SSH)事件类型、例如login、logout和login_fail。<br>• * SSH会话PID*—SSH会话的进程ID号。<br>• * SSH会话持续时间*-用户登录的秒数。 |
| 切换列筛选器 | 单击*切换*图标 打开每个列的筛选字段。在列字段中输入字符、以限制这些字符显示的事件。再次单击图标以关闭筛选字段。 |
| 撤消更改 | 单击*撤消*图标 以将此表恢复为默认配置。 |
| 导出 | 单击*导出*将表数据保存到逗号分隔值(CSV)文件。 |

定义审核日志策略

## 您可以更改覆盖策略以及审核日志中记录的事件类型。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

此任务介绍如何更改审核日志设置、其中包括用于覆盖旧事件的策略以及用于记录事件类型的策略。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择"Audit Log"*选项卡。
3. 选择*查看/编辑设置*。

   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

| 正在设置 ... | Description |
| --- | --- |
| 覆盖策略 | 确定达到最大容量时用于覆盖旧事件的策略：<br>• 允许在审核日志已满时覆盖审核日志中最早的事件-当审核日志达到50、000条记录时覆盖旧事件。<br>• 需要手动删除审核日志事件-指定不会自动删除事件；而是以设置的百分比显示阈值警告。必须手动删除事件。<br>如果禁用了覆盖策略、并且审核日志条目达到最大限制、则没有安全管理员权限的用户将无法访问System Manager。要还原没有安全管理员权限的用户的系统访问权限、分配有安全管理员角色的用户必须删除旧事件记录。<br>如果为归档审核日志配置了系统日志服务器、则覆盖策略不适用。 |
| 要记录的操作级别 | 确定要记录的事件类型：<br>• 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。<br>• 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 * 保存 * 。

从审核日志中删除事件

您可以清除旧事件的审核日志、从而使搜索事件更易于管理。删除后、您可以选择将旧事件保存到CSV (逗号分隔值)文件中。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

此任务介绍如何从审核日志中删除旧事件。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 选择*审核日志*选项卡。
3. 选择 * 删除 * 。

   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旧事件的数量。
5. 如果要将已删除的事件导出到CSV文件(建议)、请保持选中状态。在下一步中单击*删除*时、系统将提示您输入文件名和位置。否则、如果您不想将事件保存到CSV文件、请单击复选框以取消选中它。
6. 单击 * 删除 * 。

   此时将打开确认对话框。

7. 在字段中键入`delete`、然后单击*删除*。

   最早的事件将从审核日志页面中删除。

为审核日志配置系统日志服务器

## 如果要将审核日志归档到外部系统日志服务器、则可以配置该服务器与存储阵列之间的通信。建立连接后、审核日志会自动保存到系统日志服务器。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果您的服务器使用安全协议(例如TLS)、则本地系统上必须具有证书颁发机构(CA)证书。CA证书用于标识服务器和客户端之间安全连接的网站所有者。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 从*审核日志*选项卡中、选择*配置系统日志服务器*。

   此时将打开*配置系统日志服务器*对话框。

3. 单击 * 添加 * 。

   此时将打开*添加系统日志服务器*对话框。

4. 输入服务器的信息、然后单击*添加*。
   - 服务器地址-输入完全限定域名、IPv4地址或IPv6地址。

- 协议-从下拉列表中选择一个协议(例如TLS、UDP或TCP)。
- 上传证书(可选)—如果您选择了TLS协议但尚未上传签名的CA证书、请单击*浏览*上传证书文件。如果没有可信证书、则不会将审核日志归档到系统日志服务器。

> 如果证书稍后变得无效、TLS握手将失败。因此、将向审核日志发布错误消息、并且不再向系统日志服务器发送消息。要解决此问题描述 、您必须修复系统日志服务器上的证书、然后转到*菜单：设置[审核日志>配置系统日志服务器>测试全部]*。

- 端口-输入系统日志接收器的端口号。

  单击*添加*后、*配置系统日志服务器*对话框将打开、并在页面上显示已配置的系统日志服务器。

5. 要测试服务器与存储阵列的连接、请选择*全部测试*。

结果

配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。

编辑审核日志记录的系统日志服务器设置

## 您可以更改用于归档审核日志的系统日志服务器的设置、也可以为该服务器上传新的证书颁发机构(CA)证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果要上传新的CA证书、则此证书必须在本地系统上可用。

步骤

1. 选择*菜单：设置[访问管理]*。
2. 从*审核日志*选项卡中、选择*配置系统日志服务器*。

   已配置的系统日志服务器将显示在页面上。

3. 要编辑服务器信息、请选择服务器名称右侧的*编辑*(铅笔)图标、然后在以下字段中进行所需的更改：
   - 服务器地址-输入完全限定域名、IPv4地址或IPv6地址。
   - 协议-从下拉列表中选择一个协议(例如TLS、UDP或TCP)。
   - 端口-输入系统日志接收器的端口号。
4. 如果将协议更改为安全TLS协议(从UDP或TCP)、请单击*导入可信证书*以上传CA证书。
5. 要测试与存储阵列的新连接、请选择*全部测试*。

结果

配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。

## 常见问题解答

### 为什么我无法登录？

## 如果在尝试登录到System Manager时收到错误、请查看这些可能的原因。

System Manager登录错误可能是由于以下原因之一：

- 您输入的用户名或密码不正确。
- 您的权限不足。
- 目录服务器(如果已配置)可能不可用。如果是这种情况、请尝试使用本地用户角色登录。
- 您尝试多次登录失败、从而触发锁定模式。等待10分钟以重新登录。
- 已触发锁定条件、并且您的审核日志可能已满。转至访问管理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。

由于以下原因之一、可能会在远程存储阵列上登录错误以执行镜像任务：

- 您输入的密码不正确。
- 您尝试多次登录失败、从而触发锁定模式。请等待10分钟以重新登录。
- 已达到控制器上使用的最大客户端连接数。检查是否存在多个用户或客户端。

### 在添加目录服务器之前、我需要了解哪些信息？

## 在Access Management中添加目录服务器之前、请确保满足以下要求。

- 必须在目录服务中定义用户组。
- LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
- 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

### 关于映射到存储阵列角色、我需要了解哪些信息？

## 在将组映射到角色之前、请查看以下准则。

存储阵列的嵌入式RBAC (基于角色的访问控制)功能包括以下角色：

- 存储管理—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
- 安全管理—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
- 支持管理—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。无法访问存储对象或安全配置。
- 监控—对所有存储对象的只读访问、但无法访问安全配置。

#### 目录服务

如果您使用的是LDAP (轻型目录访问协议)服务器和目录服务、请确保：

- 管理员已在目录服务中定义用户组。
- 您知道LDAP用户组的组域名。
- 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

**SAML**

如果您使用的是存储阵列中嵌入的安全断言标记语言(SAML)功能、请确保：

- 身份提供程序(Identity Provider、IdP)管理员已在IdP系统中配置用户属性和组成员资格。
- 您知道组成员资格名称。
- 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则System Manager将无法正常运行。

哪些外部管理工具可能会受到此更改的影响？

## 在System Manager中进行某些更改时、例如切换管理界面或使用SAML进行身份验证方法、某些外部工具和功能可能会受到限制、无法使用。

管理接口

除非启用旧版管理接口设置、否则直接与旧版管理界面(符号)通信的工具(例如SANtricity SMI-S Provider或OnCommand Insight (OCI))无法正常工作。此外、如果禁用了此设置、则不能使用传统CLI命令或执行镜像操作。

有关详细信息，请联系技术支持。

**SAML** 身份验证

启用SAML后、以下客户端将无法访问存储阵列服务和资源：

- 企业管理窗口(EMW)
- 命令行界面（ CLI ）
- 软件开发人员套件(SDK)客户端
- 带内客户端
- HTTP基本身份验证REST API客户端
- 使用标准REST API端点登录

有关详细信息，请联系技术支持。

在配置和启用**SAML**之前、我需要了解哪些信息？

## 在配置和启用安全断言标记语言(SAML)身份验证功能之前、请确保满足以下要求并了解SAML限制。

要求

开始之前、请确保：

- 已在网络中配置身份提供程序(Identity Provider、IdP)。IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。您的安全团队负责维护IdP。
- IdP管理员已在IdP系统中配置用户属性和组。
- IdP管理员已确保IdP支持在身份验证时返回名称ID。
- 管理员已确保IdP服务器和控制器时钟保持同步(通过NTP服务器或通过调整控制器时钟设置)。
- IdP元数据文件从IdP系统下载、并可从用于访问System Manager的本地系统上获得。
- 您知道存储阵列中每个控制器的IP地址或域名。

限制

除了上述要求之外、请确保您了解以下限制：

- 启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。建议您先测试SSO登录、然后再在最终配置步骤中启用SAML。(系统还会在启用SAML之前执行SSO登录测试。)
- 如果您将来禁用SAML、则系统会自动还原先前的配置(本地用户角色和/或目录服务)。
- 如果当前已为用户身份验证配置目录服务、则SAML将覆盖此配置。
- 配置SAML后、以下客户端将无法访问存储阵列资源：
  - 企业管理窗口(EMW)
  - 命令行界面（ CLI ）
  - 软件开发人员套件(SDK)客户端
  - 带内客户端
  - HTTP基本身份验证REST API客户端
  - 使用标准REST API端点登录

审核日志中记录了哪些类型的事件?

## 审核日志可以记录修改事件、也可以同时记录修改和只读事件。

根据策略设置、将显示以下类型的事件：

- 修改事件- System Manager中涉及系统更改的用户操作、例如配置存储。
- 修改和只读事件-涉及系统更改的用户操作以及涉及查看或下载信息的事件、例如查看卷分配。

在配置系统日志服务器之前、我需要了解哪些信息?

## 您可以将审核日志归档到外部系统日志服务器。

在配置系统日志服务器之前、请记住以下准则。

- 确保您知道服务器地址、协议和端口号。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果您的服务器使用安全协议(例如TLS)、则本地系统上必须具有证书颁发机构(CA)证书。CA证书用于标识服务器和客户端之间安全连接的网站所有者。

- 配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。
- 覆盖策略设置(可从*查看/编辑设置*获得)不会影响使用系统日志服务器配置管理日志的方式。
- 审核日志采用RFC 5424消息格式。

系统日志服务器不再接收审核日志。我该怎么办?

## 如果您为系统日志服务器配置了TLS协议、则如果证书因任何原因而无效、则服务器将无法接收消息。审核日志中会发布一条有关此无效证书的错误消息。

要解决此问题描述 、必须先修复系统日志服务器的证书。建立有效的证书链后、请转到*菜单：设置[审核日志>配置系统日志服务器>测试全部]*。

# 证书

## 概念

证书的工作原理

## 证书是数字文件、用于标识网站和服务器等在线实体、以实现Internet上的安全通信。

证书可确保Web通信仅在指定服务器和客户端之间以加密格式单独传输、不会被更改。使用System Manager、您可以管理主机管理系统(充当客户端)上的浏览器与存储系统中的控制器(充当服务器)之间的证书。

证书可以由可信的颁发机构签名、也可以是自签名证书。"签名"只是指有人验证了所有者的身份并确定其设备可以受信任。存储阵列会在每个控制器上随附一个自动生成的自签名证书。您可以继续使用自签名证书、也可以获取CA签名证书、以便在控制器和主机系统之间建立更安全的连接。

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

签名证书

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

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

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

- root—层次结构顶部是根证书、其中包含用于对其他证书进行签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
- intermediate—从根分层是中间证书。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。

- 服务器—链的底部是服务器证书、用于标识您的特定实体、例如网站或其他设备。存储阵列中的每个控制器都需要一个单独的服务器证书。

#### 自签名证书

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

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

#### 用于密钥管理服务器的证书

如果您使用的是具有驱动器安全功能的外部密钥管理服务器、则还可以管理用于在该服务器和控制器之间进行身份验证的证书。

### 证书术语

以下术语适用于证书管理。

| 期限 | **Description** |
| --- | --- |
| CA | 证书颁发机构(Certificate Authority、CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。 |
| CSR | 证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述 所需的信息。 |
| 证书 | 出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。 |
| 证书链 | 一种文件层次结构、用于向证书添加一层安全保护。通常、此链包含一个位于层次结构顶部的根证书、一个或多个中间证书以及用于标识实体的服务器证书。 |
| 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、充当受保护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对服务器进行验证、以便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、其中包含私钥及其对应的公有 密钥和证书。这些密钥和证书用于标识您自己的实体、例如控制器。 |

| 期限 | Description |
| --- | --- |
| OCSP服务器 | 联机证书状态协议(OCSP)服务器可确定证书颁发机构(CA)是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问服务器。 |
| 根证书 | 根证书位于证书链中的层次结构顶部、其中包含用于对其他证书签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。 |
| 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专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。此外、签名证书还包括实体所有者的详细信息(通常为服务器或网站)以及由字母和数字组成的数字签名。签名证书使用信任链、因此最常用于生产环境。也称为"CA签名证书"或"管理证书"。 |
| 自签名证书 | 自签名证书由实体的所有者进行验证。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。它还包括由字母和数字组成的数字签名。自签名证书与CA签名证书使用的信任链不同、因此最常用于测试环境。也称为"预安装"证书。 |
| 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一个单独的服务器证书。 |

## 操作说明

### 对控制器使用**CA**签名的证书

## 您可以获取CA签名的证书、以便在控制器与用于访问System Manager的浏览器之间进行安全通信。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

使用CA签名证书是一个三步操作步骤。

#### 第**1**步：完成并提交控制器的**CSR**

您必须先为存储阵列中的每个控制器生成证书签名请求(CSR)文件、然后将此文件提交给证书颁发机构(CA)。

开始之前

- 您必须知道每个控制器的IP地址或DNS名称。

关于此任务

CSR可提供有关您的组织、控制器的IP地址或DNS名称以及用于标识控制器中Web服务器的密钥对的信息。在此任务期间、如果存储阵列中只有一个控制器、则会生成一个CSR文件；如果有两个控制器、则会生成两个CSR文件。

> 提交给CA后、请勿生成新的CSR。生成CSR时、系统会创建一个专用密钥对和公有 密钥对。公有 密钥是CSR的一部分、而私钥则保留在密钥库中。当您收到签名证书并将其导入到密钥库中时、系统会确保私钥和公有 密钥都是原始对。因此、在向CA提交新的CSR后、您不能生成新的CSR。否则、控制器将生成新密钥、而从CA收到的证书将不起作用。

步骤

1. 选择*菜单：设置[证书]*。
2. 从*阵列管理*选项卡中、选择*完成CSR*。

   > 如果显示一个对话框、提示您接受第二个控制器的自签名证书、请单击*接受自签名证书*以继续。

3. 输入以下信息、然后单击*下一步*：
   - 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
   - 组织单位(可选)—组织中负责处理证书的部门。
   - 城市/位置—存储阵列或业务所在的城市。
   - 省/自治区/直辖市(可选)—存储阵列或业务所在的省/自治区/直辖市。
   - 国家/地区**ISO**代码—您所在国家/地区的两位数ISO (国际标准化组织)代码、例如美国。

   > 某些字段可能会预先填充相应的信息、例如控制器的IP地址。请勿更改预先填充的值、除非您确定这些值不正确。例如、如果尚未完成CSR、则控制器IP地址将设置为"`localhost.`"。在这种情况下、您必须将"`localhost`"更改为控制器的DNS名称或IP地址。

4. 验证或输入有关存储阵列中控制器A的以下信息：
   - 控制器**A**公用名-默认情况下、显示控制器A的IP地址或DNS名称。请确保此地址正确无误；它必须与您在浏览器中输入的内容完全匹配、才能访问System Manager。
   - 控制器**A**备用**IP**地址-如果公用名称为IP地址、则可以选择为控制器A输入任何其他IP地址或别名对于多个条目、请使用逗号分隔格式。
   - 控制器**A**备用**DNS**名称-如果公用名是DNS名称、请为控制器A输入任何其他DNS名称对于多个条目、请使用逗号分隔格式。如果没有备用DNS名称、但您在第一个字段中输入了DNS名称、请将此名称复制到此处。如果存储阵列只有一个控制器、则可以使用*完成*按钮。如果存储阵列有两个控制器、则可以使用*下一步*按钮。

   > 首次创建CSR请求时、请勿单击*跳过此步骤*链接。在错误恢复情况下提供此链接。在极少数情况下、一个控制器上的CSR请求可能会失败、而另一个控制器上的CSR请求则可能不会失败。通过此链接、您可以跳过在已定义的控制器A上创建CSR请求的步骤、并继续执行在控制器B上重新创建CSR请求的下一步

5. 如果只有一个控制器、请单击*完成*。如果有两个控制器、请单击*下一步*以输入控制器B的信息(与上述相同)、然后单击*完成*。

   对于单个控制器、会将一个CSR文件下载到本地系统。对于双控制器、将下载两个CSR文件。下载内容的文件夹位置取决于您的浏览器。

6. 找到已下载的CSR文件。文件夹位置取决于您的浏览器。

7. 将CSR文件提交到CA并请求PEM格式的签名证书。
8. 等待CA返回证书、然后转到 [第2步：导入控制器的签名证书]。

第**2**步：导入控制器的签名证书

收到签名证书后、您可以导入控制器的文件。

开始之前

- CA返回签名证书文件。
- 这些文件位于本地系统上。
- 如果CA提供了链式证书(例如.p7b文件)、则必须将链式文件解压缩到各个文件中：根证书、一个或多个中间证书以及用于标识控制器的服务器证书。您可以使用Windows `certmgr`实用程序解压缩文件(右键单击并选择*菜单：所有任务[导出]*)。导出完成后、系统将为链中的每个证书文件显示一个CER"文件。

关于此任务

此任务介绍如何上传证书文件。

步骤

1. 选择*菜单：设置[证书]*。
2. 从*阵列管理*选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入证书文件。

3. 单击*浏览*按钮、首先选择根文件和中间文件、然后选择控制器的每个服务器证书。两个控制器的根文件和中间文件相同。对于每个控制器、只有服务器证书是唯一的。

   文件名将显示在对话框中。

4. 单击 * 导入 * 。

   文件已上传并进行验证。

结果

会话将自动终止。要使证书生效、您必须重新登录。重新登录后、新的CA签名证书将用于会话。

重置管理证书

## 您可以将控制器上的证书从使用CA签名证书还原到出厂设置的自签名证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 必须事先导入CA签名的证书。

关于此任务

重置功能会从每个控制器中删除当前CA签名的证书文件。然后、这些控制器将还原为使用自签名证书。

步骤

1. 选择*菜单：设置[证书]*。
2. 从*阵列管理*选项卡中、选择*重置*。

   此时将打开确认*重置管理证书*对话框。

3. 在字段中键入`reset`、然后单击*重置*。

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

结果

控制器将还原为使用自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

查看导入的证书信息

## 在证书页面中、您可以查看存储阵列的证书类型、颁发机构和有效日期范围。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

步骤

1. 选择菜单：设置[证书]。
2. 选择一个选项卡以查看有关证书的信息。

| 选项卡 | **Description** |
| --- | --- |
| 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*显示证书…*下的筛选器字段可查看用户安装或预安装的证书。<br>• 用户安装。用户上传到存储阵列的证书、如果控制器充当客户端(而不是服务器)、LDAPS证书和身份联合证书、则这些证书可能包括可信证书。<br>• 预安装。存储阵列附带的自签名证书。 |
| 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。 |

作为客户端时导入控制器的证书

## 如果控制器因无法验证网络服务器的信任链而拒绝连接、您可以从"可信"选项卡导入证书、以使控制器(充当客户端)能够接受来自该服务器的通信。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

- 证书文件安装在本地系统上。

关于此任务

如果要允许其他服务器(例如使用TLS的LDAP服务器或系统日志服务器)与控制器联系、则可能需要从"受信任"选项卡导入证书。

步骤

1. 选择*菜单：设置[证书]*。
2. 从*可信*选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入可信证书文件。

3. 单击*浏览*以选择控制器的证书文件。

   文件名显示在对话框中。

4. 单击 * 导入 * 。

结果

这些文件将上传并进行验证。

启用证书撤消检查

## 您可以启用对已撤销证书的自动检查、以便联机证书状态协议(OCSP)服务器阻止用户进行非安全连接。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 在两个控制器上都配置了DNS服务器、这样可以为OCSP服务器使用完全限定域名。此任务可从硬件页面访问。
- 如果要指定自己的OCSP服务器、则必须知道该服务器的URL。

关于此任务

如果CA颁发的证书不正确或私钥受到损坏、则自动撤消检查非常有用。

在此任务期间、您可以配置OCSP服务器或使用证书文件中指定的服务器。OCSP服务器会确定CA是否已在计划的到期日期之前撤销任何证书、然后在证书被撤销时阻止用户访问站点。

步骤

1. 选择*菜单：设置[证书]*。
2. 选择*可信*选项卡。

   您还可以从*密钥管理*选项卡启用撤消检查。

3. 单击*不常见任务*、然后从下拉菜单中选择*启用撤消检查*。
4. 选择*我要启用撤消检查*、以便复选框中显示复选标记、对话框中显示其他字段。

5. 在* OCSP响应器地址*字段中、您可以选择输入OCSP响应器服务器的URL。如果不输入地址、系统将使用证书文件中的OCSP服务器URL。
6. 单击*测试地址*以确保系统可以打开与指定URL的连接。
7. 单击 * 保存 * 。

结果

如果存储阵列尝试使用已撤销的证书连接到服务器、则连接将被拒绝并记录事件。

删除可信证书

## 您可以从"受信任"选项卡中删除先前导入的用户安装的证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 如果要使用新版本更新受信任证书、则必须先导入更新后的证书、然后才能删除旧证书。

> 如果在导入替代证书之前删除用于对控制器和其他服务器(例如LDAP服务器)进行身份验证的证书、则可能无法访问系统。

关于此任务

此任务介绍如何删除用户安装的证书。无法删除预安装的自签名证书。

步骤

1. 选择*菜单：设置[证书]*。
2. 选择*可信*选项卡。

   此表显示了存储阵列的受信任证书。

3. 从表中、选择要删除的证书。
4. 单击*菜单：不常见任务[删除]*

   此时将打开确认删除可信证书对话框。

5. 在字段中键入`delete`、然后单击*删除*。

使用**CA**签名的证书通过密钥管理服务器进行身份验证

## 要在密钥管理服务器和存储阵列控制器之间实现安全通信、您必须配置相应的证书集。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

在控制器和密钥管理服务器之间进行身份验证是一个两步操作步骤。

#### 第1步：完成并提交CSR、以便使用密钥管理服务器进行身份验证

您必须先生成证书签名请求(CSR)文件、然后使用CSR从密钥管理服务器信任的证书颁发机构(CA)请求签名客户端证书。您还可以使用下载的CSR文件从密钥管理服务器创建和下载客户端证书。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

关于此任务

此任务介绍如何生成CSR文件、然后使用此文件从密钥管理服务器信任的CA请求签名客户端证书。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。在此任务期间、您必须提供有关您的组织的信息。

步骤

1. 选择*菜单：设置[证书]*。
2. 从*密钥管理*选项卡中、选择*完成CSR*。
3. 输入以下信息：
   - 公用名—用于标识此CSR的名称、例如存储阵列名称、该名称将显示在证书文件中。
   - 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
   - 组织单位(可选)—组织中负责处理证书的部门。
   - 城市/位置-组织所在的城市或位置。
   - 省/自治区/直辖市(可选)—组织所在的省/自治区/直辖市。
   - 国家/地区ISO代码—贵组织所在的两位数ISO (国际标准化组织)代码、例如美国。
4. 单击 * 下载 * 。

   此时、CSR文件将保存到本地系统。

5. 从密钥管理服务器信任的CA请求签名客户端证书。
6. 拥有客户端证书后、请转到 [第2步：导入密钥管理服务器的证书]。

#### 第2步：导入密钥管理服务器的证书

下一步是、在存储阵列和密钥管理服务器之间导入用于身份验证的证书。证书有两种类型：客户端证书用于验证存储阵列的控制器、而密钥管理服务器证书用于验证服务器。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 您有一个签名的客户端证书文件(请参见 第1步：完成并提交CSR、以便使用密钥管理服务器进行身份验证)、并且您已将该文件复制到要访问System Manager的主机。客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。
- 您必须从密钥管理服务器检索服务器证书文件、然后将该文件复制到要访问System Manager的主机。密钥管理服务器证书用于验证密钥管理服务器、以便存储阵列可以信任其IP地址。

> 有关服务器证书的详细信息、请参见密钥管理服务器的文档。

关于此任务

此任务介绍如何在存储阵列控制器和密钥管理服务器之间上传用于身份验证的证书文件。您必须加载控制器的客户端证书文件和密钥管理服务器的服务器证书文件。

步骤

1. 选择*菜单：设置[证书]*。
2. 从*密钥管理*选项卡中、选择*导入*。

   此时将打开一个对话框、用于导入证书文件。

3. 在*选择客户端证书*旁边、单击*浏览*按钮为存储阵列的控制器选择客户端证书文件。

   此时、文件名将显示在对话框中。

4. 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。

   此时、文件名将显示在对话框中。

5. 单击 * 导入 * 。

   这些文件将上传并进行验证。

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

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
- 必须事先导入证书。

步骤

1. 选择*菜单：设置[证书]*。
2. 选择*密钥管理*选项卡。
3. 从表中、选择要导出的证书、然后单击*导出*。

   此时将打开保存对话框。

4. 输入文件名并单击*保存*。

## 常见问题解答

为什么会显示"无法访问其他控制器"对话框?

## 在执行与CA证书相关的某些操作(例如、导入证书)时、您可能会看到一个对话框、提示您接受第二个控制器的自签名证书。

在具有两个控制器的存储阵列(双工配置)中、如果SANtricity 系统管理器无法与第二个控制器通信、或者您的浏

览器在操作的某个时间点无法接受证书、则有时会显示此对话框。

如果此对话框打开、请单击*接受自签名证书*以继续。如果另一个对话框提示您输入密码、请输入用于访问System Manager的管理员密码。

如果此对话框再次出现、并且您无法完成证书任务、请尝试以下过程之一：

- 使用其他浏览器类型访问此控制器、接受证书并继续。
- 使用System Manager访问第二个控制器、接受自签名证书、然后返回到第一个控制器并继续。

如何知道需要将哪些证书上传到**System Manager**才能进行外部密钥管理？

## 对于外部密钥管理、您可以导入两种类型的证书、以便在存储阵列和密钥管理服务器之间进行身份验证、从而使这两个实体可以相互信任。

客户端证书可验证存储阵列的控制器、以便密钥管理服务器可以信任其密钥管理互操作性协议(Key Management Interoperability Protocol、KMIP)请求。要获取客户端证书、请使用System Manager为存储阵列完成CSR。然后、您可以将CSR上传到密钥管理服务器并从该服务器生成客户端证书。获得客户端证书后、将该文件复制到要访问System Manager的主机。

密钥管理服务器证书用于验证密钥管理服务器、以便存储阵列可以信任其IP地址。从密钥管理服务器检索服务器证书文件、然后将该文件复制到要访问System Manager的主机。

关于证书撤消检查、我需要了解哪些信息？

## 使用System Manager、您可以使用联机证书状态协议(Online Certificate Status Protocol、OCSP)服务器来检查已撤销的证书、而不是上传证书撤消列表(Certificate Revocation List、CRL)。

已撤销的证书不应再受信任。证书可能会因多种原因而被撤销；例如、如果证书颁发机构(CA)颁发的证书不正确、私钥被泄露或标识的实体不符合策略要求。

在System Manager中与OCSP服务器建立连接后、存储阵列将在连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时执行撤消检查。存储阵列会尝试验证这些服务器的证书、以确保它们未被撤消。然后、服务器将为该证书返回"good "、"revoked"或"unknown"值。如果证书已撤销或阵列无法与OCSP服务器联系、则连接将被拒绝。

> 在System Manager或命令行界面(CLI)中指定OCSP响应程序地址会覆盖在证书文件中找到的OCSP地址。

将为哪些类型的服务器启用撤消检查？

## 每当存储阵列连接到AutoSupport 服务器、外部密钥管理服务器(External Key Management Server、EKMS)、基于SSL的轻型目录访问协议(Lightweight Directory Access Protocol over SSL、LDAPS)服务器或系统日志服务器时、它都会执行撤消检查。