警报
SANtricity software

NetApp
November 03, 2025

目录

警报

了解 SANtricity System Manager 中的警报

您可以将SANtricity系统管理器配置为通过电子邮件、SNMP陷阱和系统日志消息发送存储阵列警报。

什么是警报?

_Alerts_向管理员通知存储阵列上发生的重要事件。事件可能包括电池故障、组件从最佳状态移至脱机状态或控制器出现冗余错误等问题。所有严重事件以及一些警告和信息性事件均视为"可处理"。

了解更多信息。

- "警报的工作原理"
- "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系统日志服务器。可从菜单：设置[警报]访问警报配置。

了解更多信息。

- "为警报配置邮件服务器和收件人"
- "为系统日志服务器配置警报"
- "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 中的警报工作原理

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：Support[事件日志]中获取)。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 5424消息传送标准。

了解 **SANtricity** 软件中的警报术语

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)。

组件	Description
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。

管理电子邮件警报

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、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。
   - 加密—如果要对消息进行加密、请选择* SMTPS*或* STARTTLS作为加密类型、然后选择加密消息的端口号。否则、请选择*无*。
   - 用户名和密码-如果需要、请输入用户名和密码、以便向传出发件人和邮件服务器进行身份验证。
   - 在电子邮件中包含联系信息-要在警报消息中包含发件人的联系信息、请选择此选项、然后输入姓名和电话号码。

     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。

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。

在 SANtricity System Manager 中添加警报的电子邮件地址

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。

在 SANtricity System Manager 中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。

在 SANtricity System Manager 中编辑警报邮件服务器

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

在 SANtricity System Manager 中配置 SNMP 警报

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

开始之前

- 必须为网络服务器配置SNMP服务应用程序。您需要此服务器的网络地址(IPv4或IPv6地址)、以便事件监控器可以向该地址发送陷阱消息。您可以使用多个服务器(最多允许10个服务器)。
- 已使用SNMP服务应用程序在服务器上复制和编译管理信息库(Management Information Base、MIB)文件。此MIB文件定义了要监控和管理的数据。

  如果您没有MIB文件、可以从NetApp支持站点获取：

- 转至 "NetApp 支持"。
- 单击*下载*选项卡、然后选择*下载*。
- 单击* E系列SANtricity 操作系统控制器软件*。
- 选择*下载最新版本*。
- 登录。
- 接受警告声明和许可协议。
- 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

关于此任务

此任务介绍如何识别陷阱目标的SNMP服务器、然后测试您的配置。

步骤

1. 选择菜单：设置[警报]。
2. 选择* SNMP *选项卡。

   首次设置时、SNMP选项卡会显示"Configure Communities/Users"。

3. 选择*配置社区/用户*。

   此时将打开选择SNMP版本对话框。

4. 为警报选择SNMP版本、可以是* SNMPv2c*或* SNMPv3 *。

   根据您的选择、将打开配置社区对话框或配置SNMPv3用户对话框。

5. 按照SNMPv2c (社区)或SNMPv3 (用户)的相应说明进行操作：
   - * SNMPv2c (社区)—在配置社区对话框中、为网络服务器输入一个或多个社区字符串。社区名称是一个字符串、用于标识一组已知的管理工作站、通常由网络管理员创建。它仅包含可打印的**ASCII**字符。您最多可以添加**256**个社区。完成后、单击*保存。
   - * SNMPv3 (用户)—在配置**SNMPv3**用户对话框中、单击*添加、然后输入以下信息：
     - 用户名-输入一个名称以标识用户、该名称最长可达31个字符。
     - 引擎**ID**-选择引擎ID、此ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择*本地*。如果您使用的是非标准配置、请选择*自定义*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
     - 身份验证凭据-选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
     - 隐私凭据-选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。完成后、单击*添加*、然后单击*关闭*。
6. 在选择了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*添加*。

- 陷阱目标-输入运行SNMP服务的服务器的IPv4或IPv6地址。
- 社区名称或用户名-从下拉列表中、为此陷阱目标选择社区名称(SNMPv2c)或用户名(SNMPv3)。(如果您仅定义了一个、则此名称已显示在此字段中。)
- 发送身份验证失败陷阱-如果要在SNMP请求因社区名称或用户名无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击*添加*后、陷阱目标和关联名称将显示在*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*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。

在 **SANtricity System Manager** 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)。
- 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*、然后选择*下载*。
  - 单击* E系列SANtricity 操作系统控制器软件*。
  - 选择*下载最新版本*。
  - 登录。
  - 接受警告声明和许可协议。
  - 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

步骤

1. 选择菜单：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或用户名、然后单击*添加*。
   - 陷阱目标-输入运行SNMP服务的服务器的IPv4或IPv6地址。
   - 社区名称或用户名-从下拉列表中、为此陷阱目标选择社区名称(SNMPv2c)或用户名(SNMPv3)。(如果您

仅定义了一个、则此名称已显示在此字段中。）

- 发送身份验证失败陷阱-如果要在SNMP请求因社区名称或用户名无法识别而被拒绝时向陷阱目标发出警报、请选择此选项(复选框)。单击*添加*后、陷阱目标以及关联的社区名称或用户名将显示在表中。

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。

在 SANtricity System Manager 中配置 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*、然后选择*下载*。
- 单击* E系列SANtricity 操作系统控制器软件*。
- 选择*下载最新版本*。
- 登录。
- 接受警告声明和许可协议。
- 向下滚动、直到看到您的控制器类型对应的MIB文件、然后单击链接以下载此文件。

关于此任务

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

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

步骤

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`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。

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：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*。
4. 输入新的社区名称、然后单击*保存*。团体名称只能包含可打印的ASCII字符。

结果

警报页面的SNMP选项卡会显示更新后的社区名称。

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：设置[警报]。
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*配置用户*。
4. 在对话框中、单击*查看/编辑设置*。
5. 编辑以下信息：
   - 用户名-更改标识用户的名称、该名称最长可达31个字符。
   - 引擎**ID**-选择引擎ID、此ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择*本地*。如果您使用的是非标准配置、请选择*自定义*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。
   - 身份验证凭据-选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更

改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。

- 隐私凭据-选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。

结果

警报页面的SNMP选项卡会显示更新后的设置。

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：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。

在 **SANtricity System Manager** 中为 **SNMPv3** 陷阱添加用户

对于SNMPv3陷阱、您最多可以添加256个用户。

步骤

1. 选择菜单：设置[警报]。
2. 选择* SNMP *选项卡。

   陷阱目标和用户名显示在表中。

3. 选择*配置用户*。

   此时将打开配置SNMPv3用户对话框。

4. 选择 * 添加 * 。
5. 输入以下信息、然后单击*添加*。

   - 用户名-输入一个名称以标识用户、该名称最长可达31个字符。
   - 引擎**ID**-选择引擎ID、此ID用于为消息生成身份验证和加密密钥、并且在管理域上必须是唯一的。在大多数情况下、应选择*本地*。如果您使用的是非标准配置、请选择*自定义*；此时将显示另一个字段、您必须在其中输入权威引擎ID作为十六进制字符串、并且字符数为偶数、长度介于10到32个字符之间。

- 身份验证凭据-选择一种身份验证协议、以确保用户的身份。接下来、输入一个身份验证密码、设置或更改身份验证协议时需要此密码。密码长度必须介于8到128个字符之间。
- 隐私凭据-选择用于对消息内容进行加密的隐私协议。接下来、输入隐私密码、设置或更改隐私协议时需要此密码。密码长度必须介于8到128个字符之间。

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：设置[警报]。
2. 选择* SNMP *选项卡。

   陷阱目标和社区名称将显示在*警报*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。

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：设置[警报]。
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*配置用户*。

   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*删除*。
5. 确认此操作、然后单击*删除*。

结果

用户名及其关联的陷阱目标将从警报页面中删除。

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

在 SANtricity System Manager 中配置 syslog 服务器以接收警报

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、"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。要进一步配置审核日志的系统日志设置、请参见 "为审核日志配置系统日志服务器"。

如果配置了多个系统日志服务器、则所有已配置的系统日志服务器都会收到审核日志。

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。

在 SANtricity System Manager 中添加用于警报的系统日志服务器

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 SANtricity System Manager 中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。

SANtricity System Manager 的存储系统警报常见问题解答

如果您只是想快速了解问题解答，此常见问题解答会很有帮助。

如果警报已禁用、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。