



设置硬件 StorageGRID Appliances

NetApp
May 10, 2024

This PDF was generated from <https://docs.netapp.com/zh-cn/storagegrid-appliances/installconfig/configuring-hardware.html> on May 10, 2024. Always check docs.netapp.com for the latest.

目录

- 设置硬件 1
 - 设置硬件：概述 1
 - 配置StorageGRID 连接 2
 - 配置SANtricity 系统管理器(SG6000和SG5700)..... 32
 - 配置BMC接口(SG100、SG110、SG1000、SG1100、SG6000、和SG6100)..... 39
 - 可选：启用节点或驱动器加密 47
 - 可选：更改RAID模式(SG5760和SG6000)..... 52
 - 可选：重新映射设备的网络端口..... 54

设置硬件

设置硬件：概述

为设备通电后、您可以配置StorageGRID 要使用的网络连接。

配置所需的网络连接

对于所有设备、您可以执行多项任务来配置所需的网络连接、例如：

- 访问设备安装程序
- 配置网络链路
- 验证端口级别的网络连接

可能需要的其他配置

根据您要配置的设备类型、可能需要进行其他硬件配置。

SANtricity 系统管理器

对于SG6000和SG5700、您需要配置SANtricity 系统管理器。SANtricity 软件用于监控这些设备的硬件。

BMC 接口

以下设备具有必须配置的BMC界面：

- SG100
- SG110
- SG1000
- SG1100
- SG6000
- SG6100

可选配置

- 存储设备
 - 为SANtricity系统管理器(SG5700和SG6000)配置要用于监控硬件的软件
 - 更改RAID模式
 - 访问SG6000-CN控制器的BMC接口
- 服务设备
 - 访问SG100、SG110、SG1000和SG1100的BMC界面

配置StorageGRID 连接

访问 StorageGRID 设备安装程序

您必须访问 StorageGRID 设备安装程序以验证安装程序版本，并配置设备与三个 StorageGRID 网络之间的连接：网格网络，管理网络（可选）和客户端网络（可选）。

开始之前

- 您正在使用可以连接到 StorageGRID 管理网络的任何管理客户端，或者您使用的是服务笔记本电脑。
- 客户端或服务笔记本电脑具有 "支持的 [Web 浏览器](#)"。
- 服务设备或存储设备控制器已连接到您计划使用的所有StorageGRID 网络。
- 您知道这些网络上的服务设备或存储设备控制器的IP地址、网关和子网。
- 您已配置计划使用的网络交换机。

关于此任务

要首次访问StorageGRID设备安装程序、您可以使用服务设备或存储设备控制器上的管理网络端口(假设已连接到管理网络)的DHCP分配IP地址。 或者、您也可以将服务笔记本电脑直接连接到服务设备或存储设备控制器。

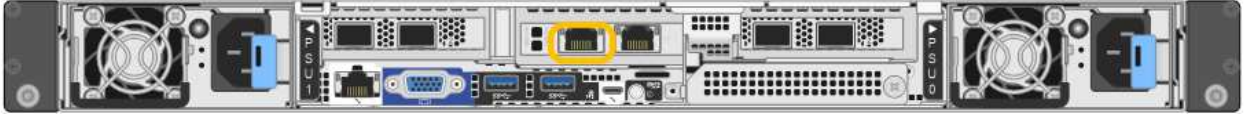
步骤

1. 如果可能、请对服务设备或存储设备控制器上的管理网络端口使用DHCP地址。下图突出显示了管理网络端口。(如果未连接管理网络、请使用网格网络上的IP地址。)

SG100



SG110



SG1000



SG1100



E5700SG

对于E5700SG、您可以执行以下任一操作：

- 。查看 E5700SG 控制器上的七段显示器。如果 E5700SG 控制器上的管理端口 1 和 10/25GbE 端口 2 和 4 连接到使用 DHCP 服务器的网络，则控制器会在打开机箱电源时尝试获取动态分配的 IP 地址。控制器完成启动过程后，其七段显示屏将显示 * HO*，然后是两个数字的重复序列。

```
HO -- IP address for Admin Network -- IP address for Grid Network  
HO
```

顺序：

- 第一组数字是管理网络上设备存储节点的 DHCP 地址（如果已连接）。此 IP 地址将分配给 E5700SG 控制器上的管理端口 1。
- 第二组数字是网络网络上设备存储节点的 DHCP 地址。首次为设备接通电源时，此 IP 地址将分配给 10/25-GbE 端口 2 和 4。

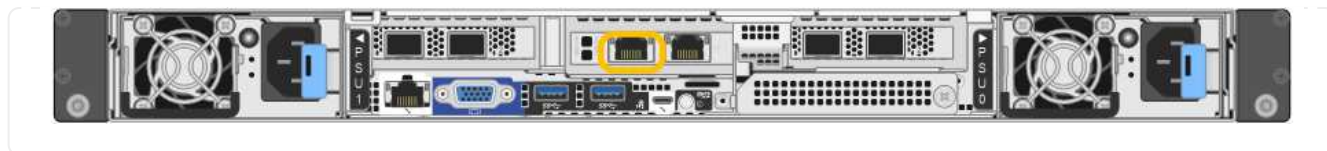


如果无法使用 DHCP 分配 IP 地址，则会显示 0.0.0.0。

SG6000-CN



GF6112



- a. 从网络管理员处获取管理网络上设备的DHCP地址。
- b. 在客户端中、输入StorageGRID 设备安装程序的以下URL： + **`https://Appliance_IP:8443`**

适用于 *Appliance_IP*，请使用DHCP地址(如果有，请使用管理网络的IP地址)。

- c. 如果系统提示您显示安全警报，请使用浏览器的安装向导查看并安装证书。

下次访问此 URL 时，不会显示此警报。

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。

NetApp® StorageGRID® Appliance Installer

[Home](#)[Configure Networking ▼](#)[Configure Hardware ▼](#)[Monitor Installation](#)[Advanced ▼](#)

Home

i The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type

Storage ▼

Node name

MM-2-108-SGA-lab25

Cancel

Save

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.1.178

Connection state

Connection to 172.16.1.178 ready

Cancel

Save

Installation

Current state

Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

[Start Installation](#)

2. 如果无法使用DHCP获取IP地址、则可以使用链路本地连接。

SG100

使用以太网缆线将服务笔记本电脑直接连接到服务设备上最右侧的 RJ-45 端口。



SG110

使用以太网电缆将服务笔记本电脑直接连接到设备最右侧的RJ-45端口。



SG1000

使用以太网缆线将服务笔记本电脑直接连接到服务设备上最右侧的 RJ-45 端口。



SG1100

使用以太网电缆将服务笔记本电脑直接连接到设备最右侧的RJ-45端口。



E5700SG

使用以太网缆线将服务笔记本电脑连接到 E5700SG 控制器上的管理端口 2。



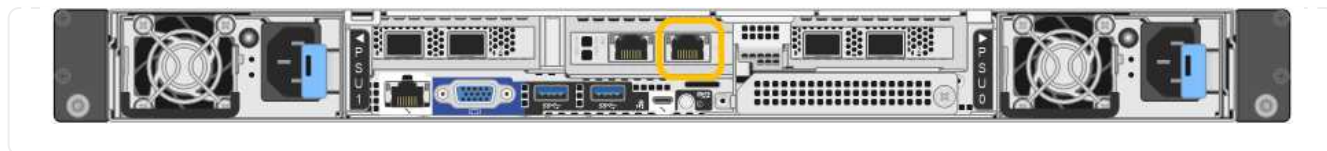
SG6000-CN

使用以太网缆线将服务笔记本电脑直接连接到 SG6000-CN 控制器上最右侧的 RJ-45 端口。



GF6112

使用以太网电缆将服务笔记本电脑直接连接到设备最右侧的RJ-45端口。



- a. 在服务笔记本电脑上打开 Web 浏览器。
- b. 输入StorageGRID 设备安装程序的URL：+ **https://169.254.0.1:8443**

此时将显示 StorageGRID 设备安装程序主页页面。首次访问此页面时显示的信息和消息取决于设备当前与 StorageGRID 网络的连接方式。可能会显示错误消息，这些消息将在后续步骤中解决。



如果无法通过链路本地连接访问主页、请将服务笔记本电脑的IP地址配置为 169.254.0.2、然后重试。

完成后

访问 StorageGRID 设备安装程序后：

- 验证设备上的 StorageGRID 设备安装程序版本是否与 StorageGRID 系统上安装的软件版本匹配。如有必要，请升级 StorageGRID 设备安装程序。

"[验证并升级 StorageGRID 设备安装程序版本](#)"

- 查看 StorageGRID 设备安装程序主页页面上显示的所有消息，并根据需要配置链路配置和 IP 配置。

NetApp® StorageGRID® Appliance Installer

Home

Configure Networking •

Configure Hardware •

Monitor Installation

Advanced •

Home

This Node

Node type

Gateway

Node name

xlr8r-10

Cancel

Save

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

192.168.7.44

Connection state

Connection to 192.168.7.44 ready

Cancel

Save

Installation

Current state

Ready to start installation of xlr8r-10 into grid with Admin Node 192.168.7.44 running StorageGRID 11.6.0, using StorageGRID software downloaded from the Admin Node.

Start Installation

验证并升级 StorageGRID 设备安装程序版本

设备上的 StorageGRID 设备安装程序版本必须与 StorageGRID 系统上安装的软件版本匹配，以确保所有 StorageGRID 功能均受支持。

开始之前

您已访问 StorageGRID 设备安装程序。

关于此任务

StorageGRID 设备出厂时预安装了 StorageGRID 设备安装程序。如果要设备添加到最近升级的 StorageGRID 系统，则可能需要先手动升级 StorageGRID 设备安装程序，然后再将设备安装为新节点。

升级到新的 StorageGRID 版本时，StorageGRID 设备安装程序会自动升级。您无需升级已安装设备节点上的 StorageGRID 设备安装程序。只有在安装包含早期版本的 StorageGRID 设备安装程序的设备时，才需要此操作步骤。

步骤

1. 从 StorageGRID 设备安装程序中，选择 * 高级 * > * 升级固件 *。
2. 将当前固件版本与 StorageGRID 系统上安装的软件版本进行比较。（从网格管理器的顶部，选择帮助图标并选择 * 关于 *。）

两个版本中的第二位数字应匹配。例如，如果您的 StorageGRID 系统运行的是 11.* 6*。x.y，则 StorageGRID 设备安装程序版本应为 3.* 6*。z。

3. 如果设备安装了 StorageGRID 设备安装程序的低级版本、请转到 ["NetApp 下载：StorageGRID 设备"](#)。

使用您的 NetApp 帐户的用户名和密码登录。

4. 下载适当版本的 * StorageGRID Appliances * 支持文件以及相应的校验和文件。

StorageGRID 设备的支持文件为 .zip 归档文件、其中包含所有 StorageGRID 设备型号的当前和先前固件版本。

下载 StorageGRID 设备的支持文件后、解压缩 .zip 归档并查看 README 文件、了解有关安装 StorageGRID 设备安装程序的重要信息。

5. 按照 StorageGRID 设备安装程序的升级固件页面上的说明执行以下步骤：
 - a. 上传适用于您的控制器类型的支持文件(固件映像)。某些固件版本还需要上传校验和文件。如果系统提示您输入校验和文件、也可以在 StorageGRID 设备的支持文件中找到该文件。
 - b. 升级非活动分区。
 - c. 重新启动和交换分区。
 - d. 重新上传适用于您的控制器类型的支持文件(固件映像)。某些固件版本还需要上传校验和文件。如果系统提示您输入校验和文件、也可以在 StorageGRID 设备的支持文件中找到该文件。
 - e. 升级第二个（非活动）分区。

相关信息

["访问 StorageGRID 设备安装程序"](#)

配置网络链路

您可以为用于将设备连接到网格网络，客户端网络和管理网络的端口配置网络链路。您可以设置链路速度以及端口和网络绑定模式。



如果使用 ConfigBuilder 生成 JSON 文件、则可以自动配置网络链路。请参见 ["自动安装和配置设备"](#)。

开始之前

- 您已拥有 ["已获取附加设备"](#) 电缆类型和链路速度所需。
- 您已根据计划使用的链路速度在端口中安装了正确的收发器。
- 您已将网络端口连接到支持所选速度的交换机。

如果您计划使用聚合端口绑定模式， LACP 网络绑定模式或 VLAN 标记：

- 您已将设备上的网络端口连接到可支持 VLAN 和 LACP 的交换机。
- 如果多个交换机参与 LACP 绑定，则这些交换机支持多机箱链路聚合组（MLAG）或等效项。
- 您了解如何将交换机配置为使用 VLAN，LACP 和 MLAG 或等效项。
- 您知道要用于每个网络的唯一 VLAN 标记。此 VLAN 标记将添加到每个网络数据包中，以确保网络流量路由到正确的网络。

关于此任务

只有在要使用非默认设置时，才需要在链路配置页面上配置设置。



LACP传输哈希策略为layer2+3。

这些图和表汇总了每个设备的端口绑定模式和网络绑定模式选项。有关详细信息，请参见以下内容：

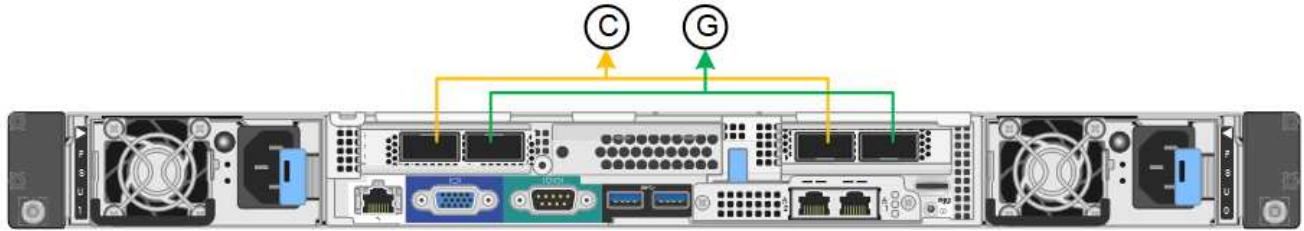
- ["端口绑定模式\(SG1000和SG100\)"](#)
- ["端口绑定模式\(SG1100和SG110\)"](#)
- ["端口绑定模式\(E5700SG\)"](#)
- ["端口绑定模式\(SG6000-CN\)"](#)
- ["端口绑定模式\(SGF6112\)"](#)

SG100和SG1000

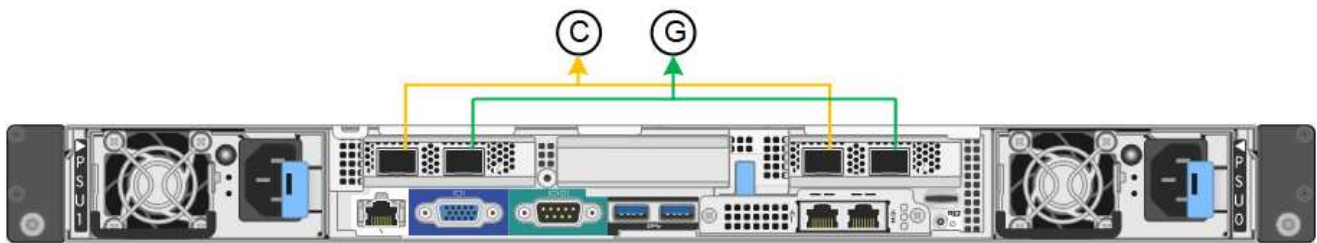
固定端口绑定模式(默认)

图中显示了SG1000或SG100上的四个网络端口是如何在固定端口绑定模式(默认配置)下绑定的。

SG1000 :



SG100 :



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

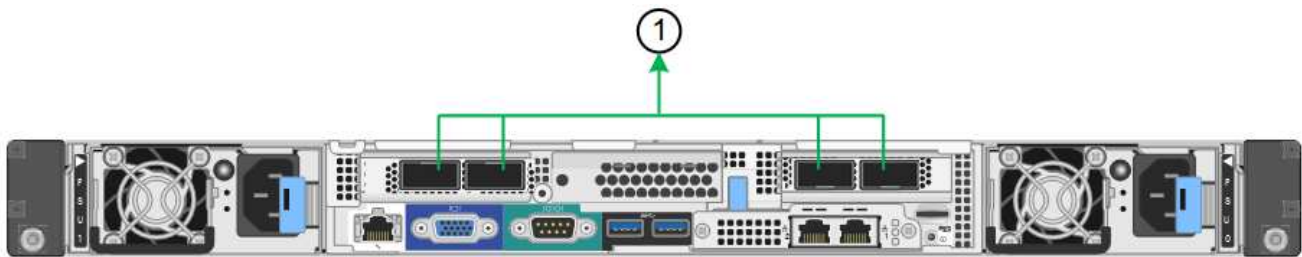
下表总结了用于配置四个网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup（默认）	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用主动备份绑定。未使用端口1和3。VLAN 标记是可选的。	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用主动备份绑定。端口 1 和 3 对客户端网络使用主动备份绑定。为了方便网络管理员，可以为两个网络指定 VLAN 标记。
LACP（802.3ad）	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用 LACP 绑定。未使用端口1和3。VLAN 标记是可选的。	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用 LACP 绑定。端口 1 和 3 对客户端网络使用 LACP 绑定。为了方便网络管理员，可以为两个网络指定 VLAN 标记。

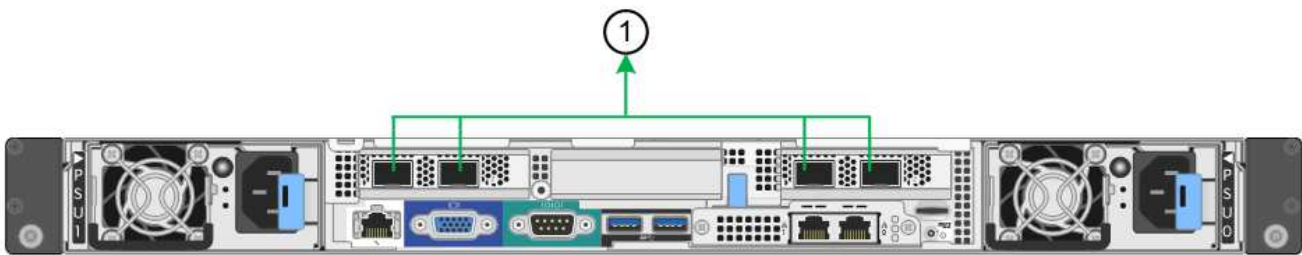
聚合端口绑定模式

这些图显示了四个网络端口如何在聚合端口绑定模式下绑定。

SG1000 :



SG100 :



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表总结了用于配置四个网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （802.3ad）	<ul style="list-style-type: none">端口 1-4 对网格网络使用一个 LACP 绑定。一个 VLAN 标记用于标识网格网络数据包。	<ul style="list-style-type: none">端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

管理端口的**Active-Backup**网络绑定模式

这些图显示了设备上的两个1-GbE管理端口是如何在管理网络的Active-Backup网络绑定模式下绑定的。

SG1000 :



SG100 :

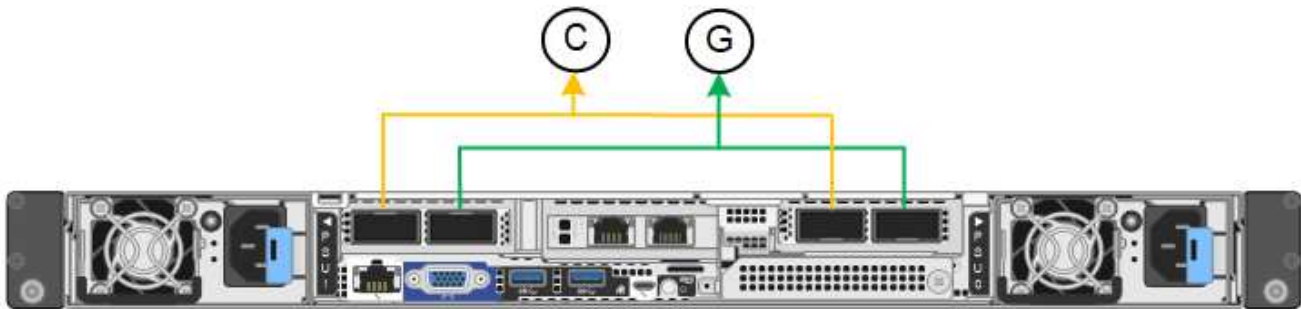


SG110和SG1100

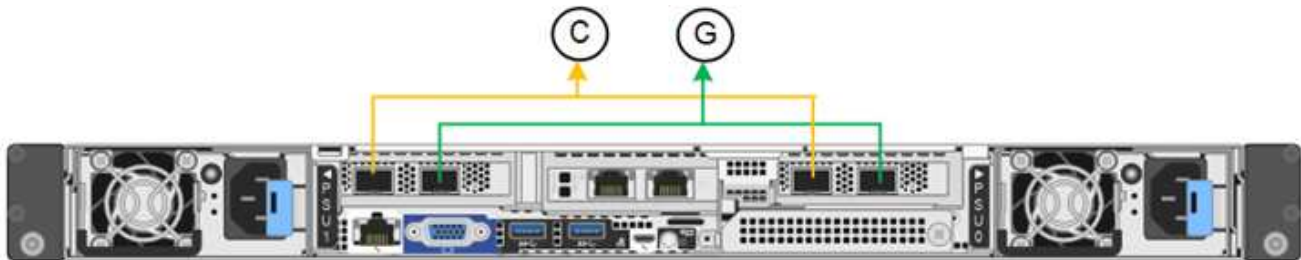
固定端口绑定模式(默认)

图中显示了SG1100或SG110上的四个网络端口是如何在固定端口绑定模式(默认配置)下绑定的。

SG1100:



SG110:



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网络网络的端口 2 和 4 绑定在一起。

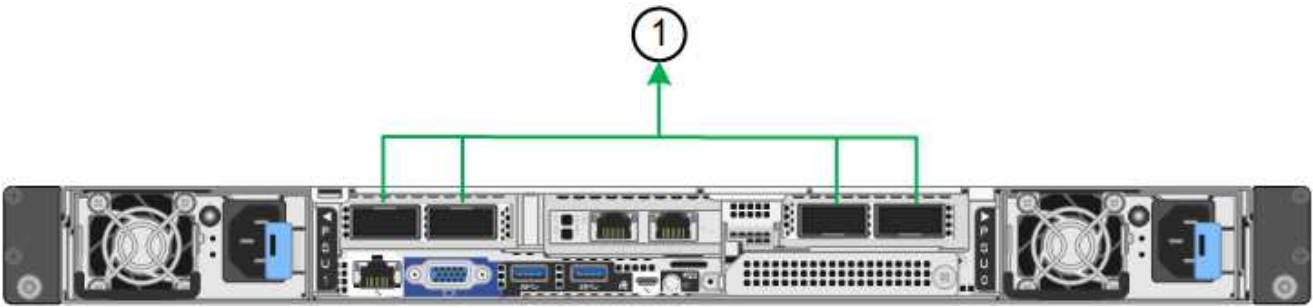
下表总结了用于配置四个网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup（默认）	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用主动备份绑定。未使用端口 1 和 3。VLAN 标记是可选的。	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用主动备份绑定。端口 1 和 3 对客户端网络使用主动备份绑定。为了方便网络管理员，可以为两个网络指定 VLAN 标记。
LACP（802.3ad）	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用 LACP 绑定。未使用端口 1 和 3。VLAN 标记是可选的。	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用 LACP 绑定。端口 1 和 3 对客户端网络使用 LACP 绑定。为了方便网络管理员，可以为两个网络指定 VLAN 标记。

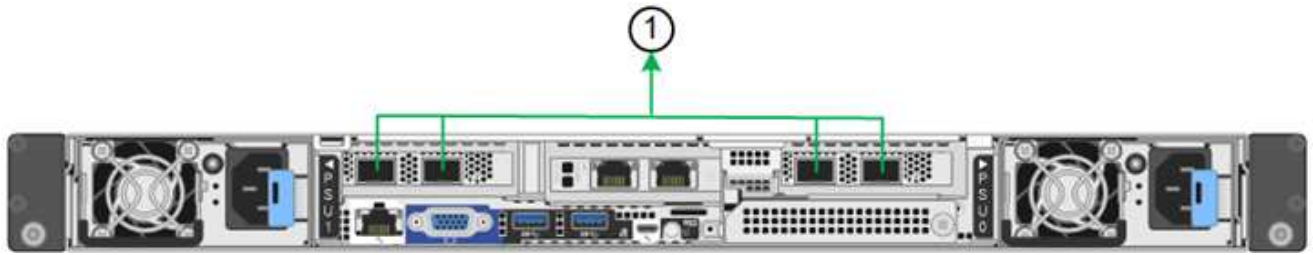
聚合端口绑定模式

这些图显示了四个网络端口如何在聚合端口绑定模式下绑定。

SG1100:



SG110:



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

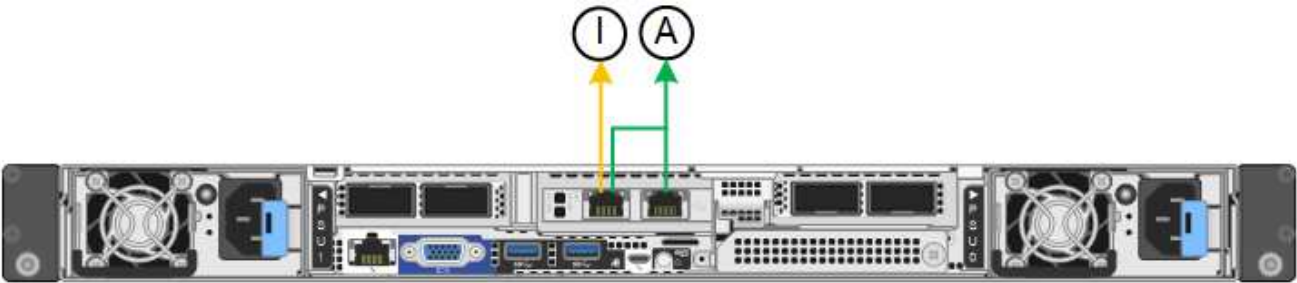
下表总结了用于配置网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （802.3ad）	<ul style="list-style-type: none">端口 1-4 对网格网络使用一个 LACP 绑定。一个 VLAN 标记用于标识网格网络数据包。	<ul style="list-style-type: none">端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

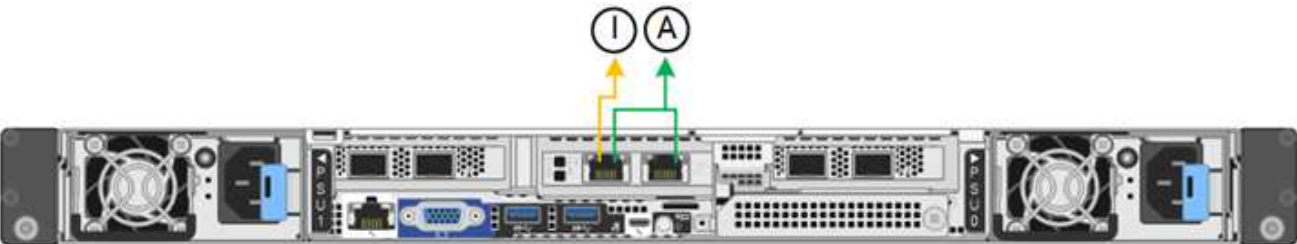
管理端口的**Active-Backup**网络绑定模式

这些图显示了设备上的两个1-GbE管理端口是如何在管理网络的Active-Backup网络绑定模式下绑定的。

SG1100:



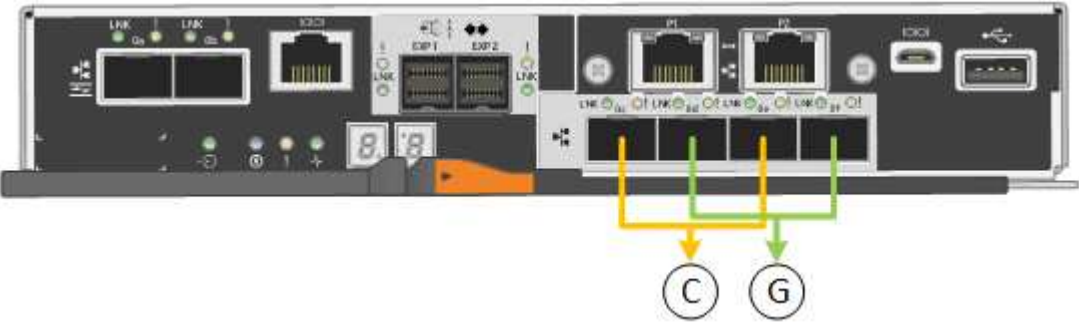
SG110:



SG5700

固定端口绑定模式(默认)

此图显示了在固定端口绑定模式（默认配置）下四个 10/225-GbE 端口的绑定方式。



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。

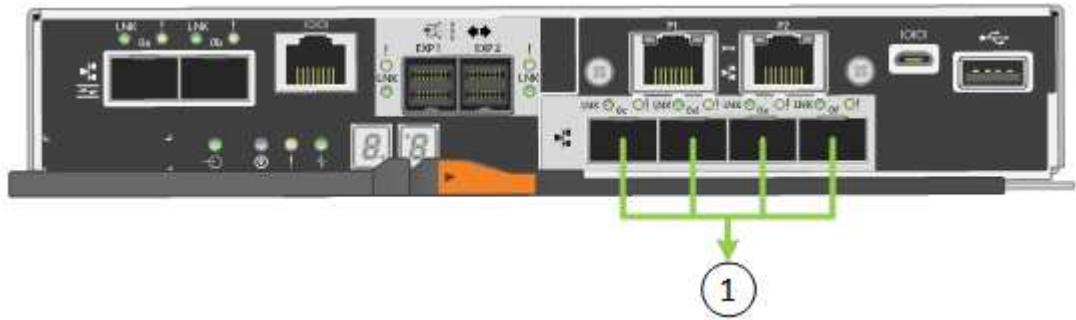
Callout	哪些端口已绑定
g	网格网络的端口 2 和 4 绑定在一起。

下表总结了用于配置四个 10/225-GbE 端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用主动备份绑定。 未使用端口1和3。 VLAN 标记是可选的。 	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用主动备份绑定。 端口 1 和 3 对客户端网络使用主动备份绑定。 为了方便网络管理员，可以为两个网络指定 VLAN 标记。
LACP （802.3ad）	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用 LACP 绑定。 未使用端口1和3。 VLAN 标记是可选的。 	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用 LACP 绑定。 端口 1 和 3 对客户端网络使用 LACP 绑定。 为了方便网络管理员，可以为两个网络指定 VLAN 标记。

聚合端口绑定模式

此图显示了四个 10/25GbE 端口在聚合端口绑定模式下的绑定方式。



Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表总结了用于配置四个 10/225-GbE 端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （802.3ad）	<ul style="list-style-type: none">端口 1-4 对网格网络使用一个 LACP 绑定。一个 VLAN 标记用于标识网格网络数据包。	<ul style="list-style-type: none">端口 1-4 对网格网络和客户端网络使用一个 LACP 绑定。通过两个 VLAN 标记，可以将网格网络数据包与客户端网络数据包隔离。

管理端口的**Active-Backup**网络绑定模式

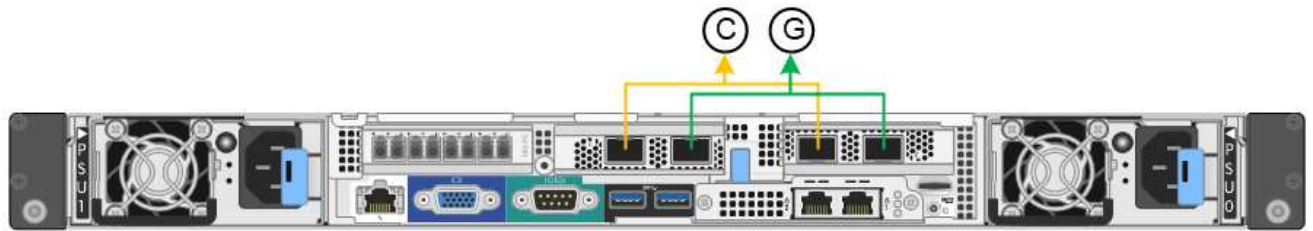
此图显示了 E5700SG 控制器上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。



SG6000

固定端口绑定模式(默认)

此图显示了四个网络端口如何在固定端口绑定模式下绑定(默认配置)



Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

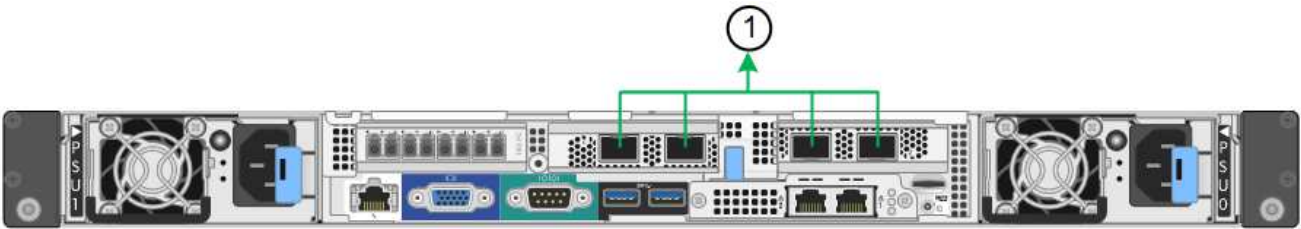
下表总结了用于配置网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用主动备份绑定。未使用端口1和3。VLAN 标记是可选的。	<ul style="list-style-type: none">端口 2 和 4 对网格网络使用主动备份绑定。端口 1 和 3 对客户端网络使用主动备份绑定。为了方便网络管理员，可以为两个网络指定 VLAN 标记。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
LACP（802.3ad）	<ul style="list-style-type: none"> 端口 2 和 4 对网络网络使用 LACP 绑定。 未使用端口 1 和 3。 VLAN 标记是可选的。 	<ul style="list-style-type: none"> 端口 2 和 4 对网络网络使用 LACP 绑定。 端口 1 和 3 对客户端网络使用 LACP 绑定。 为了方便网络管理员，可以为两个网络指定 VLAN 标记。

聚合端口绑定模式

此图显示了四个网络端口在聚合端口绑定模式下的绑定方式。



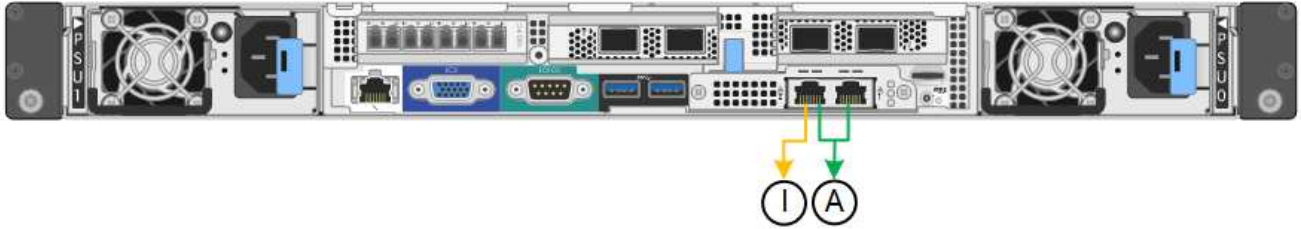
Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网络网络和客户端网络流量。

下表总结了用于配置网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP（802.3ad）	<ul style="list-style-type: none"> 端口 1-4 对网络网络使用一个 LACP 绑定。 一个 VLAN 标记用于标识网络网络数据包。 	<ul style="list-style-type: none"> 端口 1-4 对网络网络和客户端网络使用一个 LACP 绑定。 通过两个 VLAN 标记，可以将网络网络数据包与客户端网络数据包隔离。

管理端口的**Active-Backup**网络绑定模式

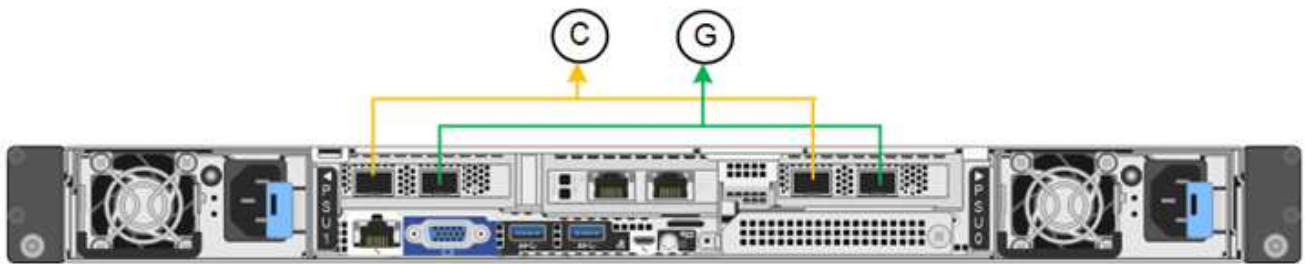
此图显示了 SG6000-CN 控制器上的两个 1-GbE 管理端口如何在管理网络的主动备份网络绑定模式下绑定。



GF6112

固定端口绑定模式(默认)

此图显示了四个网络端口如何在固定端口绑定模式下绑定(默认配置)。



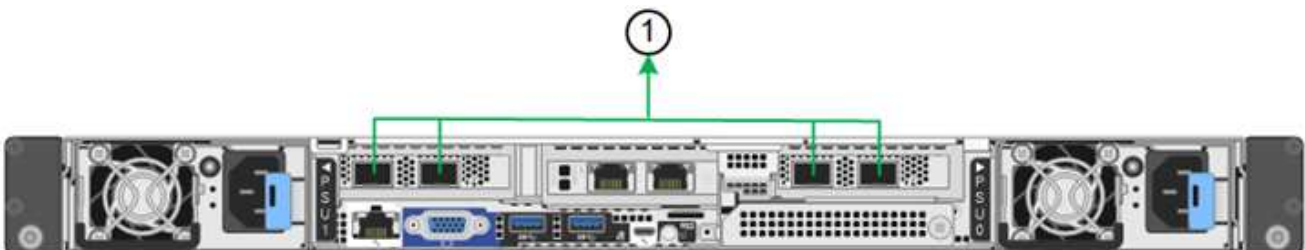
Callout	哪些端口已绑定
C	如果使用此网络，则端口 1 和 3 将绑定到客户端网络。
g	网格网络的端口 2 和 4 绑定在一起。

下表总结了用于配置网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
Active-Backup （默认）	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用主动备份绑定。 未使用端口1和3。 VLAN 标记是可选的。 	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用主动备份绑定。 端口 1 和 3 对客户端网络使用主动备份绑定。 为了方便网络管理员，可以为两个网络指定 VLAN 标记。
LACP （ 802.3ad ）	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用 LACP 绑定。 未使用端口1和3。 VLAN 标记是可选的。 	<ul style="list-style-type: none"> 端口 2 和 4 对网格网络使用 LACP 绑定。 端口 1 和 3 对客户端网络使用 LACP 绑定。 为了方便网络管理员，可以为两个网络指定 VLAN 标记。

聚合端口绑定模式

此图显示了四个网络端口如何在聚合端口绑定模式下绑定。



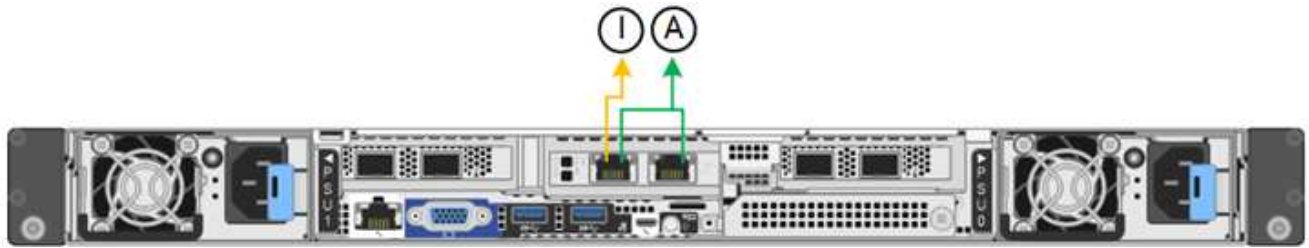
Callout	哪些端口已绑定
1.	所有四个端口都分组在一个 LACP 绑定中，从而允许所有端口用于网格网络和客户端网络流量。

下表总结了用于配置网络端口的选项。只有在要使用非默认设置时，才需要在链路配置页面上配置设置。

网络绑定模式	客户端网络已禁用（默认）	已启用客户端网络
仅 LACP （802.3ad）	<ul style="list-style-type: none">端口 1-4 对网络网络使用一个 LACP 绑定。一个 VLAN 标记用于标识网络网络数据包。	<ul style="list-style-type: none">端口 1-4 对网络网络和客户端网络使用一个 LACP 绑定。通过两个 VLAN 标记，可以将网络网络数据包与客户端网络数据包隔离。

管理端口的Active-Backup网络绑定模式

此图显示了如何在管理网络的Active-Backup网络绑定模式下绑定SGF6112上的两个1-GbE管理端口。



步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * 链接配置 *。

" 网络链路配置 " 页面显示设备示意图，其中包含编号为的网络和管理端口。

链路状态表列出了已编号端口的链路状态、链路速度和其他统计信息。

首次访问此页面时：

- * 链路速度 * 设置为 * 自动 *。
- * 端口绑定模式 * 设置为 * 固定 *。
- 对于网络网络，* 网络绑定模式 * 设置为 * 主动备份 *。
- 此时将启用 * 管理网络 *，并将网络绑定模式设置为 * 独立 *。
- 已禁用 * 客户端网络 *。

2. 从 * 链路速度 * 下拉列表中选择网络端口的链路速度。

您用于网络网络和客户端网络的网络交换机也必须支持此速度并为此速度进行配置。您必须使用适当的适配器或收发器来设置所配置的链路速度。请尽可能使用自动链路速度，因为此选项会与链路配对节点协商链路速度和正向错误更正（FEC）模式。

如果您计划对SG6000或SG5700网络端口使用25-GbE链路速度：

- 使用SFP28收发器和SFP28双轴电缆或光缆。
- 对于SG5700，从*链接速度*下拉列表中选择*25GbE*。
- 对于SG6000，请从*Link speed*下拉列表中选择*Auto*。

3. 启用或禁用计划使用的 StorageGRID 网络。

网络网络为必填项。您无法禁用此网络。

- a. 如果设备未连接到管理网络，请清除管理网络的*Enable network*复选框。
- b. 如果设备已连接到客户端网络，请选中客户端网络的*Enable network*复选框。

此时将显示数据 NIC 端口的客户端网络设置。

4. 请参见表，并配置端口绑定模式和网络绑定模式。

此示例显示：

- 为网格和客户端网络选择了 * 聚合 * 和 * LACP *。您必须为每个网络指定唯一的 VLAN 标记。您可以选择 0 到 4095 之间的值。
- 已为管理网络选择 * 主动备份 *。

Link Settings

Link speed

Port bond mode ☐ Fixed ☒ Aggregate

Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.

Grid Network

Enable network ☒

Network bond mode ☐ Active-Backup ☒ LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging ☒

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Admin Network

Enable network ☒

Network bond mode ☐ Independent ☒ Active-Backup

Connect the Admin Network to ports 5 and 6. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 6, then connecting to port 6 and using link-local IP address 169.254.0.1 for access.

MAC Addresses d8:c4:97:2a:e4:95

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

Client Network

Enable network ☒

Network bond mode ☐ Active-Backup ☒ LACP (802.3ad)

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging ☒

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

5. 对所做的选择感到满意后，单击 * 保存 *。



如果更改了所连接的网络或链路，则可能会断开连接。如果您未在1分钟内重新连接、请使用分配给设备的其他IP地址之一重新输入StorageGRID 设备安装程序的URL：+
https://appliance_IP:8443

配置 StorageGRID IP 地址

您可以使用StorageGRID 设备安装程序配置用于StorageGRID 网络、管理和客户端网络上的服务设备或设备存储节点的IP地址和路由信息。

如果使用ConfigBuilder生成JSON文件、则可以自动配置IP地址。请参见 ["自动安装和配置设备"](#)。

关于此任务

您必须为每个已连接网络上的设备分配一个静态 IP ， 或者为 DHCP 服务器上的地址分配一个永久租约。

要更改链路配置、请参见以下说明：

- ["更改SG100或SG1000服务设备的链路配置"](#)
- ["更改SG110或SG1100服务设备的链路配置"](#)
- ["更改 E5700SG 控制器的链路配置"](#)
- ["更改SG6000-CN控制器的链路配置"](#)
- ["更改SG6100设备的链路配置"](#)

步骤

1. 在 StorageGRID 设备安装程序中，选择 * 配置网络连接 * > * IP 配置 * 。

此时将显示 "IP Configuration" 页面。

2. 要配置网格网络，请在页面的 * 网格网络 * 部分中选择 * 静态 * 或 * DHCP * 。
3. 如果选择 * 静态 * ， 请按照以下步骤配置网格网络：
 - a. 使用 CIDR 表示法输入静态 IPv4 地址。
 - b. 输入网关。

如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

- c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。



网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。



为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的MTU值都必须相同。

- d. 单击 * 保存 * 。

更改 IP 地址时，网关和子网列表可能也会发生更改。

如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL 。例如、+ **`https://appliance_IP:8443`**

- e. 确认网格网络子网列表正确无误。

如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。



未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 .

- f. 单击 * 保存 *。

4. 如果选择了 * DHCP *，请按照以下步骤配置网格网络：

- a. 选择 * DHCP * 单选按钮后，单击 * 保存 *。

系统会自动填充 * IPv4 地址 *，* 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

- b. 确认网格网络子网列表正确无误。

如果您有网格子网，则需要网格网络网关。指定的所有网格子网都必须可通过此网关访问。启动 StorageGRID 安装时，还必须在主管理节点上的网格网络子网列表中定义这些网格网络子网。



未列出默认路由。如果未启用客户端网络，则默认路由将使用网格网络网关。

- 要添加子网，请单击插入图标 最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 .

- c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000。否则，请保留默认值 1500。



网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。



为了获得最佳网络性能，应在所有节点的网格网络接口上配置类似的 MTU 值。如果网格网络在各个节点上的 MTU 设置有明显差异，则会触发 * 网格网络 MTU 不匹配 * 警报。并非所有网络类型的 MTU 值都必须相同。

- a. 单击 * 保存 *。

5. 要配置管理网络，请在页面的 * 管理网络 * 部分中选择 * 静态 * 或 * DHCP *。



要配置管理网络，请在链路配置页面上启用管理网络。

Admin Network

The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites.

IP Assignment ☒ Static ☐ DHCP

IPv4 Address (CIDR)

Gateway

Subnets (CIDR) +

MTU

6. 如果选择 * 静态 *，请按照以下步骤配置管理网络：

- a. 使用 CIDR 表示法为设备上的管理端口 1 输入静态 IPv4 地址。

管理端口 1 位于设备右端的两个 1-GbE RJ45 端口的左侧。

- b. 输入网关。

如果您的网络没有网关，请重新输入相同的静态 IPv4 地址。

- c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000。否则，请保留默认值 1500。



网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

- d. 单击 * 保存 *。

更改 IP 地址时，网关和子网列表可能也会发生更改。



如果与 StorageGRID 设备安装程序的连接断开，请使用您刚刚分配的新静态 IP 地址重新输入 URL。例如、+ **https://appliance:8443**

- e. 确认管理网络子网列表正确无误。

您必须验证是否可以使用提供的网关访问所有子网。



无法创建默认路由以使用管理网络网关。

- 要添加子网，请单击插入图标  最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 .

f. 单击 * 保存 *。

7. 如果选择了 * DHCP *，请按照以下步骤配置管理网络：

a. 选择 * DHCP * 单选按钮后，单击 * 保存 *。

系统会自动填充 * IPv4 地址 *，* 网关 * 和 * 子网 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。



您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

b. 确认管理网络子网列表正确无误。

您必须验证是否可以使用提供的网关访问所有子网。



无法创建默认路由以使用管理网络网关。

- 要添加子网，请单击插入图标  最后一个条目右侧。
- 要删除未使用的子网，请单击删除图标 .

c. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000。否则，请保留默认值 1500。



网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

d. 单击 * 保存 *。

8. 要配置客户端网络，请在页面的 * 客户端网络 * 部分中选择 * 静态 * 或 * DHCP *。



要配置客户端网络、请在链路配置页面上启用客户端网络。

Client Network

The Client Network is an open network used to provide access to client applications, including S3 and Swift. The Client Network enables grid nodes to communicate with any subnet reachable through the Client Network gateway. The Client Network does not become operational until you complete the StorageGRID configuration steps.

IP Assignment ☒ Static ☐ DHCP

IPv4 Address (CIDR)

Gateway

MTU

9. 如果选择 * 静态 *，请按照以下步骤配置客户端网络：

- 使用 CIDR 表示法输入静态 IPv4 地址。
- 单击 * 保存 *。
- 确认客户端网络网关的 IP 地址正确无误。



如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关、在启用客户端网络的情况下无法移动到其他接口。

- 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000。否则，请保留默认值 1500。



网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

- 单击 * 保存 *。

10. 如果选择了 * DHCP *，请按照以下步骤配置客户端网络：

- 选择 * DHCP * 单选按钮后，单击 * 保存 *。

系统会自动填充 * IPv4 地址 * 和 * 网关 * 字段。如果 DHCP 服务器设置为分配 MTU 值，则 * MTU * 字段将填充该值，并且该字段将变为只读。

您的 Web 浏览器会自动重定向到 StorageGRID 设备安装程序的新 IP 地址。

- a. 确认网关是否正确。



如果启用了客户端网络，则会显示默认路由。默认路由使用客户端网络网关、在启用客户端网络的情况下无法移动到其他接口。

- b. 如果要使用巨型帧，请将 MTU 字段更改为适用于巨型帧的值，例如 9000 。否则，请保留默认值 1500 。



网络的 MTU 值必须与节点所连接的交换机端口上配置的值匹配。否则，可能会发生网络性能问题或数据包丢失。

验证网络连接

您应确认可以从设备访问所使用的 StorageGRID 网络。要验证通过网络网关的路由，您应测试 StorageGRID 设备安装程序与不同子网上的 IP 地址之间的连接。您还可以验证 MTU 设置。

步骤

1. 从 StorageGRID 设备安装程序的菜单栏中，单击 * 配置网络连接 * > * Ping 和 MTU 测试 * 。

此时将显示 Ping 和 MTU 测试页面。

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

Network	<input type="text" value="Grid"/>
Destination IPv4 Address or FQDN	<input type="text"/>
Test MTU	<input type="checkbox"/>
<input type="button" value="Test Connectivity"/>	

2. 从 * 网络 * 下拉框中，选择要测试的网络：网络，管理员或客户端。
3. 输入该网络上某个主机的 IPv4 地址或完全限定域名（FQDN）。

例如，您可能需要对网络或主管理节点上的网关执行 ping 操作。

4. (可选)选中*Test MTU*复选框，验证通过网络到目标的整个路径的MTU设置。

例如，您可以测试设备节点与其他站点的节点之间的路径。

5. 单击 * 测试连接 *。

如果网络连接有效，则会显示 "Ping test passed" 消息，并列出 ping 命令输出。

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

Network	<div>Grid</div>
Destination IPv4 Address or FQDN	<div>10.96.104.223</div>
Test MTU	<input checked="" type="checkbox"/>
<div>Test Connectivity</div>	

Ping test passed

Ping command output

```
PING 10.96.104.223 (10.96.104.223) 1472(1500) bytes of data.  
1480 bytes from 10.96.104.223: icmp_seq=1 ttl=64 time=0.318 ms  
  
--- 10.96.104.223 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms  
  
Found MTU 1500 for 10.96.104.223 via br0
```

相关信息

- ["配置网络链路"](#)
- ["更改 MTU 设置"](#)

验证端口级别的网络连接

要确保 StorageGRID 设备安装程序与其他节点之间的访问不会受到防火墙的阻碍，请确认 StorageGRID 设备安装程序可以连接到指定 IP 地址或地址范围内的特定 TCP 端口或端口集。

关于此任务

使用 StorageGRID 设备安装程序中提供的端口列表，您可以测试设备与网格网络中其他节点之间的连接。

此外，您还可以在管理和客户端网络以及 UDP 端口上测试连接，例如用于外部 NFS 或 DNS 服务器的端口。有关这些端口的列表，请参见 ["网络端口参考"](#)。



端口连接表中列出的网格网络端口仅适用于StorageGRID 11.7或更高版本。要验证每种节点类型的端口是否正确，您应始终参考适用于您的 StorageGRID 版本的网络连接准则。

步骤

1. 在 StorageGRID 设备安装程序中，单击 * 配置网络连接 * > * 端口连接测试 (nmap) *。

此时将显示端口连接测试页面。

端口连接表列出了网格网络上需要 TCP 连接的节点类型。对于每种节点类型，此表列出了设备应可访问的网格网络端口。

您可以测试表中列出的设备端口与网格网络中的其他节点之间的连接。

2. 从 * 网络 * 下拉列表中，选择要测试的网络： * 网格 * ， * 管理 * 或 * 客户端 * 。
3. 为该网络上的主机指定一个 IPv4 地址范围。

例如，您可能需要探测网络或主管理节点上的网关。

使用连字符指定一个范围，如示例所示。

4. 输入 TCP 端口号，以逗号分隔的端口列表或端口范围。

Port Connectivity Test

Network

Grid ▼

IPv4 Address Ranges

10.224.6.160-161

Port Ranges

22,2022

Protocol

☒ TCP ☐ UDP

Test Connectivity

5. 单击 * 测试连接 * 。

- 如果选定的端口级别网络连接有效，则绿色横幅中会显示 "Port connectivity test passed" 消息。nmap 命令输出列在横幅下方。

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- 如果与远程主机建立了端口级网络连接，但主机未侦听一个或多个选定端口，则黄色横幅中会显示 "Port connectivity test failed" 消息。nmap 命令输出列在横幅下方。

主机未侦听的任何远程端口的状态为 "closed"。`例如，当您尝试连接的节点处于预安装状态且 StorageGRID NMS 服务尚未在该节点上运行时，您可能会看到此黄色横幅。

 Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    open  https
1504/tcp  closed evb-elm
1505/tcp  open  funkproxy
1506/tcp  open  utcd
1508/tcp  open  diagmond
7443/tcp  open  oracleas-https
9999/tcp  open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 如果无法为一个或多个选定端口建立端口级网络连接，则红色横幅中会显示 "Port connection test failed" 消息。nmap 命令输出列在横幅下方。

红色横幅表示已尝试通过 TCP 连接到远程主机上的某个端口，但未向发送方返回任何内容。如果未返回任何响应，则此端口的状态为 "已筛选"，并且可能会被防火墙阻止。



此外，还会列出带有 "closed" 的端口。

❗ Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT      STATE      SERVICE
22/tcp    open       ssh
79/tcp    filtered   finger
80/tcp    open       http
443/tcp   open       https
1504/tcp  closed     evb-elm
1505/tcp  open       funkproxy
1506/tcp  open       utcd
1508/tcp  open       diagmond
7443/tcp  open       oracleas-https
9999/tcp  open       abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

配置SANtricity 系统管理器(SG6000和SG5700)

您可以使用 SANtricity 系统管理器监控存储控制器，存储磁盘和存储控制器架中其他硬件组件的状态。此外，您还可以为 E 系列 AutoSupport 配置代理，使您能够在不使用管理端口的情况下从设备发送 AutoSupport 消息。

设置并访问 SANtricity 系统管理器

您可能需要访问存储控制器上的 SANtricity 系统管理器来监控存储控制器架中的硬件或配置 E 系列 AutoSupport。

开始之前

- 您正在使用 "支持的 Web 浏览器"。
- 要通过网络管理器访问SANtricity 系统管理器、您已安装StorageGRID 、并且具有存储设备管理员权限或root访问权限。
- 要使用SANtricity 设备安装程序访问StorageGRID 系统管理器、您必须具有SANtricity 系统管理器管理员用户名和密码。
- 要使用Web浏览器直接访问SANtricity 系统管理器、您具有SANtricity 系统管理器管理员用户名和密码。



要使用网络管理器或 StorageGRID 设备安装程序访问 SANtricity 系统管理器，您必须安装 SANtricity 固件 8.70 或更高版本。您可以使用 StorageGRID 设备安装程序并选择 * 帮助 * > * 关于 * 来检查固件版本。



从网络管理器或设备安装程序访问 SANtricity 系统管理器通常仅用于监控硬件和配置 E 系列 AutoSupport。SANtricity 系统管理器中的许多功能和操作(例如升级固件)不适用于监控StorageGRID 设备。为避免出现问题，请始终按照适用于您的设备的硬件安装和维护说明进行操作。

关于此任务

根据您所处的安装和配置过程的阶段，有三种方法可以访问 SANtricity System Manager：

- 如果此设备尚未部署为 StorageGRID 系统中的节点，则应使用 StorageGRID 设备安装程序中的高级选项卡。



部署节点后，您将无法再使用 StorageGRID 设备安装程序访问 SANtricity 系统管理器。

- 如果此设备已部署为 StorageGRID 系统中的节点，请使用网络管理器中节点页面上的 SANtricity 系统管理器选项卡。
- 如果无法使用 StorageGRID 设备安装程序或网络管理器，则可以直接使用连接到管理端口的 Web 浏览器访问 SANtricity 系统管理器。

此操作步骤 包含首次访问 SANtricity System Manager 的步骤。如果您已设置 SANtricity 系统管理器，请转到 [配置硬件警报步骤](#)。



使用网络管理器或 StorageGRID 设备安装程序，您可以访问 SANtricity 系统管理器，而无需配置或连接设备的管理端口。

您可以使用 SANtricity 系统管理器监控以下内容：

- 存储阵列级别性能，I/O 延迟，CPU 利用率和吞吐量等性能数据
- 硬件组件状态
- 支持的功能包括查看诊断数据

您可以使用 SANtricity 系统管理器配置以下设置：

- 存储控制器架中组件的电子邮件警报，SNMP 警报或系统日志警报
- 存储控制器架中组件的 E 系列 AutoSupport 设置。

有关 E 系列 AutoSupport 的更多详细信息，请参见 ["NetApp E 系列系统文档站点"](#)。

- 驱动器安全密钥，用于解锁安全驱动器（如果启用了驱动器安全功能，则需要执行此步骤）
- 用于访问 SANtricity 系统管理器的管理员密码

步骤

1. 执行以下操作之一：

- 使用 StorageGRID 设备安装程序并选择 * 高级 * > * SANtricity 系统管理器 *
- 使用网络管理器并选择 * N 节点 * > **appliance Storage Node** > * SANtricity 系统管理器 *



如果这些选项不可用或未显示登录页面，请使用 [存储控制器的 IP 地址](#)。浏览到存储控制器 IP 以访问 SANtricity System Manager。

2. 设置或输入管理员密码。

SANtricity 系统管理器使用一个管理员密码，该密码在所有用户之间共享。

[More \(10 total\) >](#)**1** Welcome

2 Verify Hardware

3 Verify Hosts

4 Select Applications

5 Define Workloads

6 Act

Welcome to the SANtricity® System Manager! With System Manager, you can...

- Configure your storage array and set up alerts.
- Monitor and troubleshoot any problems when they occur.
- Keep track of how your system is performing in real time.

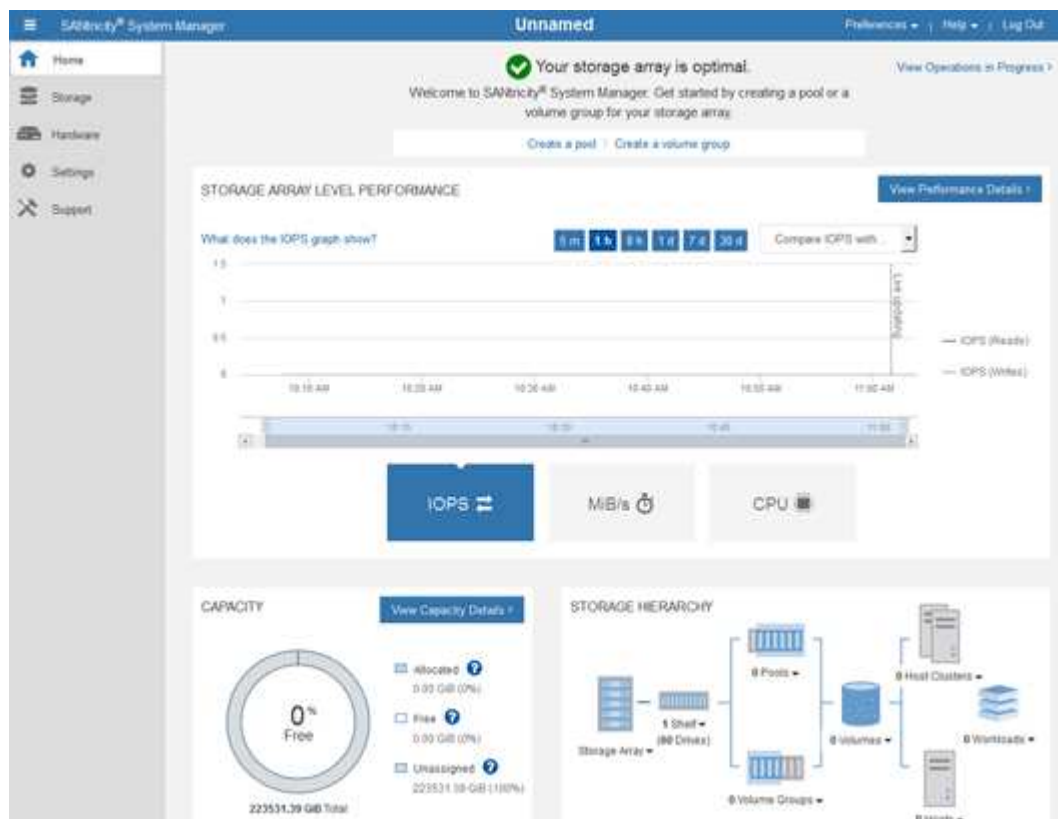
Cancel

Next >

3. 选择 * 取消 * 以关闭向导。



请勿完成StorageGRID 设备的设置向导。



4. 【config_hardware_alerts_sg6000 , start=4】配置硬件警报。

a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。

- b. 使用联机帮助的 * 设置 * > * 警报 * 部分了解警报。
 - c. 按照 "如何" 说明设置电子邮件警报，SNMP 警报或系统日志警报。
5. 管理存储控制器架中组件的 AutoSupport。
- a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
 - b. 使用联机帮助的 * 支持 * > * 支持中心 * 部分了解 AutoSupport 功能。
 - c. 按照 "如何" 说明管理 AutoSupport。

有关配置StorageGRID 代理以在不使用管理端口的情况下发送E系列AutoSupport 消息的具体说明、请转至 ["有关配置存储代理设置的说明"](#)。

6. 如果为设备启用了驱动器安全功能，请创建并管理安全密钥。
- a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
 - b. 使用联机帮助的 * 设置 * > * 系统 * > * 安全密钥管理 * 部分了解驱动器安全性。
 - c. 按照 "如何" 说明创建和管理安全密钥。
7. 也可以更改管理员密码。
- a. 选择 * 帮助 * 以访问 SANtricity 系统管理器的联机帮助。
 - b. 使用联机帮助的 * 主页 * > * 存储阵列管理 * 部分了解管理员密码。
 - c. 按照 "如何" 说明更改密码。

在 SANtricity System Manager 中查看硬件状态

您可以使用 SANtricity 系统管理器监控和管理存储控制器架中的各个硬件组件，并查看硬件诊断和环境信息，例如组件温度以及与驱动器相关的问题。

开始之前

- 您正在使用 ["支持的 Web 浏览器"](#)。
- 要通过网格管理器访问SANtricity System Manager、您需要具有存储设备管理员权限或root访问权限。
- 要使用SANtricity 设备安装程序访问StorageGRID 系统管理器、您必须具有SANtricity 系统管理器管理员用户名和密码。
- 要使用Web浏览器直接访问SANtricity 系统管理器、您具有SANtricity 系统管理器管理员用户名和密码。



要使用网格管理器或 StorageGRID 设备安装程序访问 SANtricity 系统管理器，您必须安装 SANtricity 固件 8.70 或更高版本。



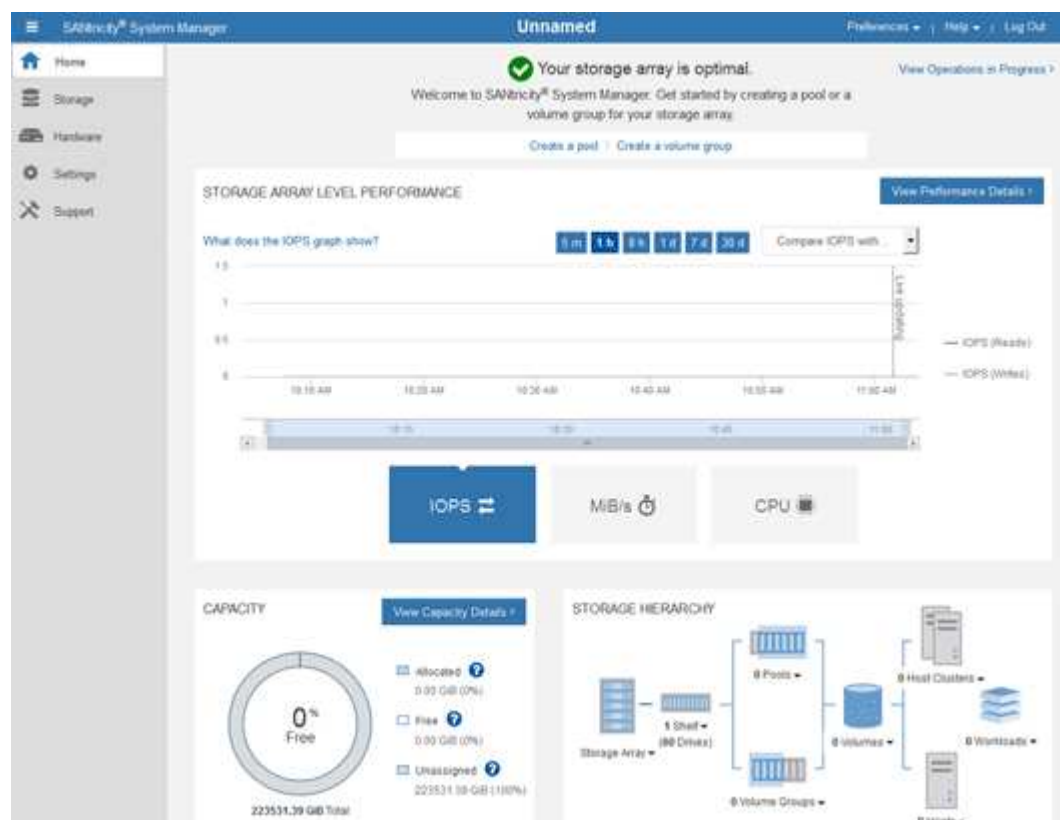
从网格管理器或设备安装程序访问 SANtricity 系统管理器通常仅用于监控硬件和配置 E 系列 AutoSupport。SANtricity 系统管理器中的许多功能和操作(例如升级固件)不适用于监控StorageGRID 设备。为避免出现问题，请始终按照适用于您的设备的硬件安装和维护说明进行操作。

步骤

1. [访问 SANtricity 系统管理器](#)。
2. 如果需要，请输入管理员用户名和密码。

3. 单击 * 取消 * 以关闭设置向导并显示 SANtricity 系统管理器主页。

此时将显示 SANtricity System Manager 主页。在 SANtricity 系统管理器中，控制器架称为存储阵列。



4. 查看显示的设备硬件信息，并确认所有硬件组件的状态均为最佳。

- a. 单击 * 硬件 * 选项卡。
- b. 单击 * 显示磁盘架的背面 *。

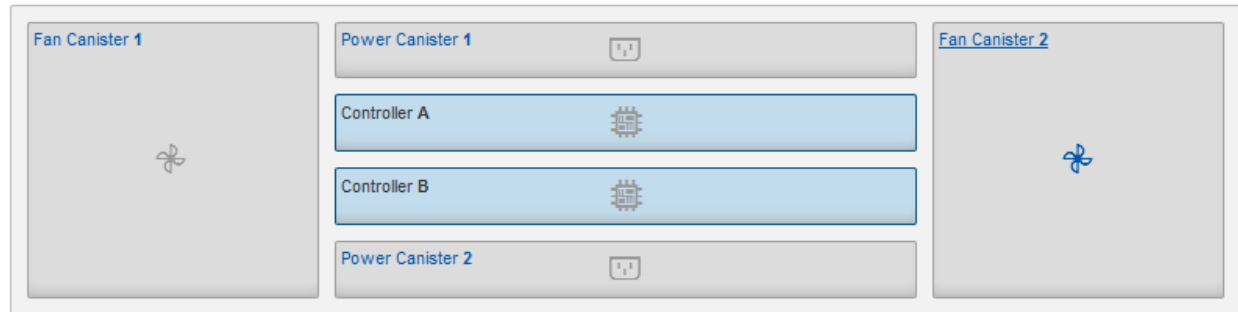
HARDWARE

[Learn More >](#)

Legend ▾

☐ Show status icon details ?

Controller Shelf 99 ▾

[Show front of shelf](#)

从磁盘架背面，您可以查看两个存储控制器，每个存储控制器中的电池，两个电源箱，两个风扇箱和扩展架（如果有）。您还可以查看组件温度。

- 要查看每个存储控制器的设置，请选择控制器，然后从上下文菜单中选择 * 查看设置 *。
- 要查看磁盘架背面其他组件的设置，请选择要查看的组件。
- 单击 * 显示磁盘架正面 *，然后选择要查看的组件。

从磁盘架正面，您可以查看存储控制器磁盘架或扩展磁盘架（如果有）的驱动器和驱动器抽盒。

如果需要关注任何组件的状态，请按照 [Recovery Guru](#) 中的步骤解决问题描述 或联系技术支持。

使用 **StorageGRID** 设备安装程序设置存储控制器的 IP 地址

每个存储控制器上的管理端口 1 用于将设备连接到 SANtricity System Manager 的管理网络。如果无法从 SANtricity 设备安装程序访问 StorageGRID 系统管理器，请为每个存储控制器设置一个静态 IP 地址，以确保不会断开与控制器架中硬件和控制器固件的管理连接。

开始之前

- 您正在使用可以连接到 StorageGRID 管理网络的任何管理客户端，或者您使用的是服务笔记本电脑。
- 客户端或服务笔记本电脑具有受支持的 Web 浏览器。

关于此任务

DHCP 分配的地址可以随时更改。为控制器分配静态 IP 地址，以确保一致的可访问性。



只有当您无法从 SANtricity 设备安装程序(高级>* SANtricity 系统管理器*)或网络管理器(节点>* SANtricity 系统管理器*)访问 StorageGRID 系统管理器时，才应遵循此操作步骤。

步骤

1. 在客户端中、输入StorageGRID 设备安装程序的URL：+ **https://Appliance_Controller_IP:8443**

适用于 `Appliance_Controller_IP` 下、使用任何StorageGRID 网络上设备的IP地址。

此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * 存储控制器网络配置 * 。

此时将显示存储控制器网络配置页面。

3. 根据您的网络配置，对于 IPv4 ， IPv6 或这两者，请选择 * 已启用 * 。
4. 记下自动显示的 IPv4 地址。

DHCP 是为存储控制器管理端口分配 IP 地址的默认方法。



显示 DHCP 值可能需要几分钟的时间。

IPv4 Address Assignment ☐ Static ☒ DHCP

IPv4 Address (CIDR)	10.224.5.166/21
Default Gateway	10.224.0.1

5. (可选) 设置存储控制器管理端口的静态 IP 地址。



您应该为管理端口分配静态 IP ， 或者为 DHCP 服务器上的地址分配永久租约。

- a. 选择 * 静态 * 。
- b. 使用 CIDR 表示法输入 IPv4 地址。
- c. 输入默认网关。

IPv4 Address Assignment ☒ Static ☐ DHCP

IPv4 Address (CIDR)	10.224.2.200/21
Default Gateway	10.224.0.1

- d. 单击 * 保存 * 。

应用所做的更改可能需要几分钟的时间。

连接到SANtricity 系统管理器时、您将使用新的静态IP地址作为URL：+ **https://Storage_Controller_IP**

配置BMC接口(SG100、SG110、SG1000、SG1100、SG6000、和SG6100)

BMC界面：概述(SG100、SG110、SG1000、SG1100、SG6000、和SG6100)

SG6100、SG6000或服务设备上的底板管理控制器(BMC)用户界面可提供有关硬件的状态信息、并可用于配置设备的SNMP设置和其他选项。

在安装设备时、请使用本节中的以下过程配置BMC：

- "更改BMC界面的管理员或root密码"
- "设置 BMC 管理端口的 IP 地址"
- "访问 BMC 界面"
- "配置SNMP设置"
- "为BMC警报设置电子邮件通知"

如果设备已安装到网格中且正在运行StorageGRID软件、请使用以下过程：



- "将设备置于维护模式" 以访问StorageGRID设备安装程序。
- 请参见 "设置 BMC 管理端口的 IP 地址" 有关使用StorageGRID设备安装程序访问BMC界面的信息。

更改BMC界面的管理员或root密码

为了安全起见、您必须更改BMC管理员或root用户的密码。

开始之前

管理客户端正在使用 "支持的 Web 浏览器"。

关于此任务

首次安装设备时、BMC将使用管理员或root用户的默认密码。您必须更改管理员或root用户的密码、以保护您的系统。

默认用户取决于您安装StorageGRID设备的时间。对于新安装，默认用户为*admin*；对于旧安装，默认用户为*root*。

步骤

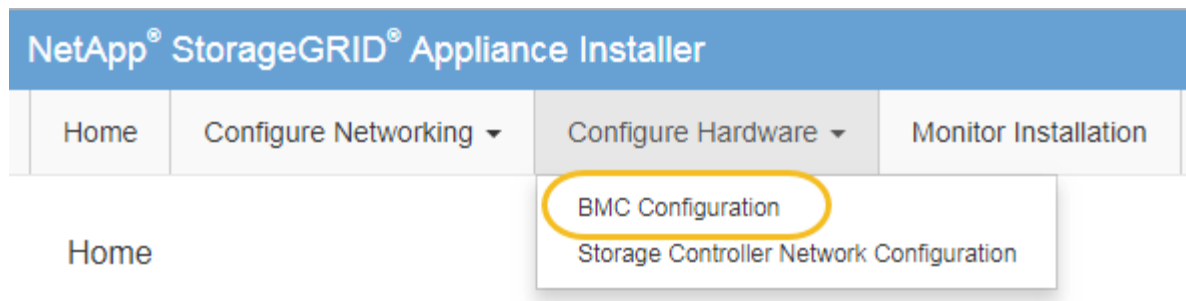
1. 在客户端中、输入StorageGRID设备安装程序的URL：

`https://Appliance_IP:8443`

适用于 `Appliance_IP` 下、使用任何StorageGRID 网络上设备的IP地址。

此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * BMC 配置 *。



此时将显示 Baseboard Management Controller Configuration 页面。

3. 在提供的两个字段中输入管理员或root帐户的新密码。
4. 选择 * 保存 *。

设置 **BMC** 管理端口的 **IP** 地址

在访问BMC界面之前、请先配置SGF6112、SG6000-CN控制器或服务设备上BMC管理端口的IP地址。

如果使用ConfigBuilder生成JSON文件、则可以自动配置IP地址。请参见 ["自动安装和配置设备"](#)。

开始之前

- 管理客户端正在使用 ["支持的 Web 浏览器"](#)。
- 您正在使用可连接到 StorageGRID 网络的任何管理客户端。
- BMC 管理端口将连接到您计划使用的管理网络。

SG100



SG110



SG1000



SG1100



SG6000



SG6100



关于此任务

出于支持目的，BMC 管理端口允许进行低级硬件访问。



您只能将此端口连接到安全，可信的内部管理网络。如果没有此类网络可用，请保持 BMC 端口未连接或被阻止，除非技术支持请求 BMC 连接。

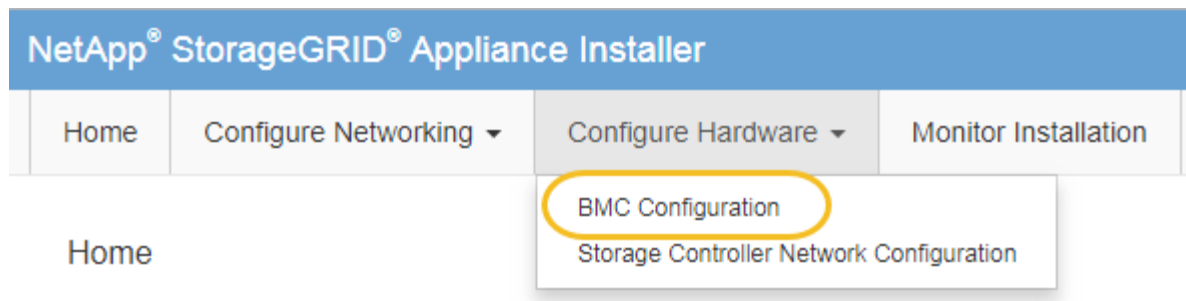
步骤

1. 在客户端中、输入StorageGRID 设备安装程序的URL：+ **`https://Appliance_IP:8443`**

适用于 `Appliance_IP` 下、使用任何StorageGRID 网络上设备的IP地址。

此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 配置硬件 * > * BMC 配置 *。



此时将显示 Baseboard Management Controller Configuration 页面。

3. 记下自动显示的 IPv4 地址。

DHCP 是为该端口分配 IP 地址的默认方法。



显示 DHCP 值可能需要几分钟的时间。

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
MAC Address	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	10.224.0.1

Cancel	Save
--------	------

4. 也可以为 BMC 管理端口设置静态 IP 地址。



您应该为 BMC 管理端口分配静态 IP，或者为 DHCP 服务器上的地址分配永久租约。

- 选择 * 静态 *。
- 使用 CIDR 表示法输入 IPv4 地址。
- 输入默认网关。

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>
Default gateway	<input type="text" value="10.224.0.1"/>

d. 单击 * 保存 *。

应用所做的更改可能需要几分钟的时间。

访问 **BMC** 界面

您可以使用以下设备型号上BMC管理端口的DHCP或静态IP地址访问BMC接口：

- SG100
- SG110
- SG1000
- SG1100
- SG6000
- SG6100

开始之前

- 管理客户端正在使用 ["支持的 Web 浏览器"](#)。
- 设备上的BMC管理端口已连接到您计划使用的管理网络。

SG100



SG110



SG1000



SG1100



SG6000



SG6100



步骤

1. 输入BMC接口的URL：+ **`https://BMC_Port_IP`**

适用于`BMC_Port_IP`下、使用DHCP或静态IP地址作为BMC管理端口。

此时将显示 BMC 登录页面。



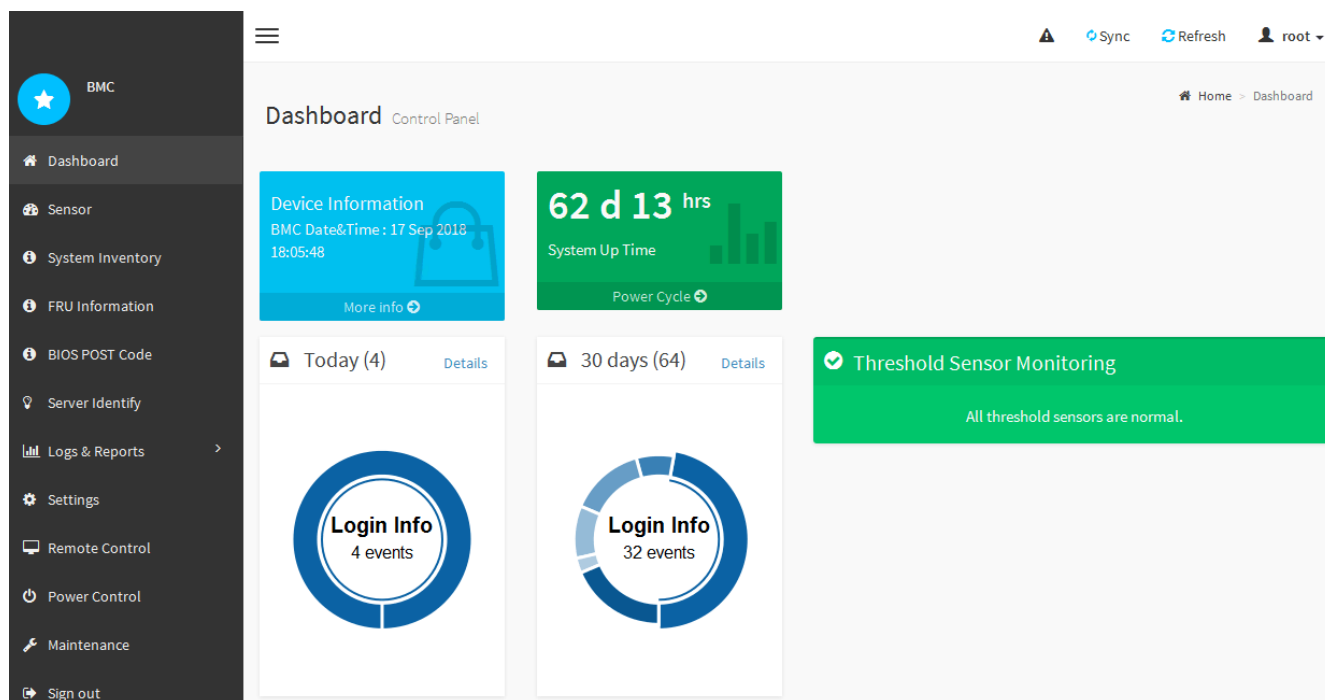
如果尚未配置 `BMC_Port_IP`，按照中的说明进行操作 ["配置BMC接口"](#)。如果由于硬件问题而无法遵循此操作步骤，并且尚未配置 BMC IP 地址，则仍可访问此 BMC。默认情况下，BMC 使用 DHCP 获取 IP 地址。如果在BMC网络上启用了DHCP、则网络管理员可以提供分配给BMC MAC的IP地址、该地址印在设备正面的标签上。如果BMC网络上未启用DHCP、BMC将在几分钟后不会响应、并为自己分配默认静态IP 192.168.0.120。您可能需要将膝上型计算机直接连接到BMC端口、并更改网络设置以为膝上型计算机分配IP、例如 192.168.0.200/24，以便浏览到 192.168.0.120。

2. 使用您在时设置的密码输入管理员或root用户名和密码 **"已更改默认密码"**：



默认用户取决于您安装StorageGRID设备的时间。对于新安装，默认用户为*admin*；对于旧安装，默认用户为*root*。

3. 选择 * 登录 *。



4. 或者，也可以选择 * 设置 * > * 用户管理 * 并单击任何 "已 d" 用户来创建其他用户。



当用户首次登录时，系统可能会提示他们更改密码以提高安全性。

配置BMC的SNMP设置

如果您熟悉为硬件配置SNMP、则可以使用BMC界面为SG6100、SG6000和服务设备配置SNMP设置。您可以提供安全社区字符串，启用 SNMP 陷阱并最多指定五个 SNMP 目标。

开始之前

- 您知道如何访问 BMC 信息板。
- 您在为 SNMPv1-v2c 设备配置 SNMP 设置方面具有经验。



如果此设备发生故障且需要更换，则此操作步骤 所做的 BMC 设置可能不会保留下来。请确保您已应用所有设置，以便在更换硬件后根据需要轻松重新应用这些设置。

步骤

1. 从 BMC 信息板中，选择 * 设置 * > * SNMP 设置 *。
2. 在 SNMP 设置页面上，选择 * 启用 SNMP V1/V2 *，然后提供只读社区字符串和读写社区字符串。

只读社区字符串类似于用户 ID 或密码。您应更改此值，以防止入侵者获取有关网络设置的信息。读写社区

字符串可保护设备免受未经授权的更改。

3. (可选) 选择 * 启用陷阱 * ，然后输入所需信息。



使用 IP 地址输入每个 SNMP 陷阱的目标 IP 。不支持DNS名称。

如果希望设备在SNMP控制台处于异常状态时立即向其发送通知、请启用陷阱。根据设备的不同、陷阱可能指示各种组件的硬件故障、链路启动/关闭条件、超过温度阈值或流量过高。

4. 或者，也可以单击 * 发送测试陷阱 * 来测试您的设置。
5. 如果设置正确，请单击 * 保存 * 。

为BMC警报设置电子邮件通知

如果您希望在出现警报时发送电子邮件通知、请使用BMC界面配置SMTP设置、用户、LAN目标、警报策略和事件筛选器。



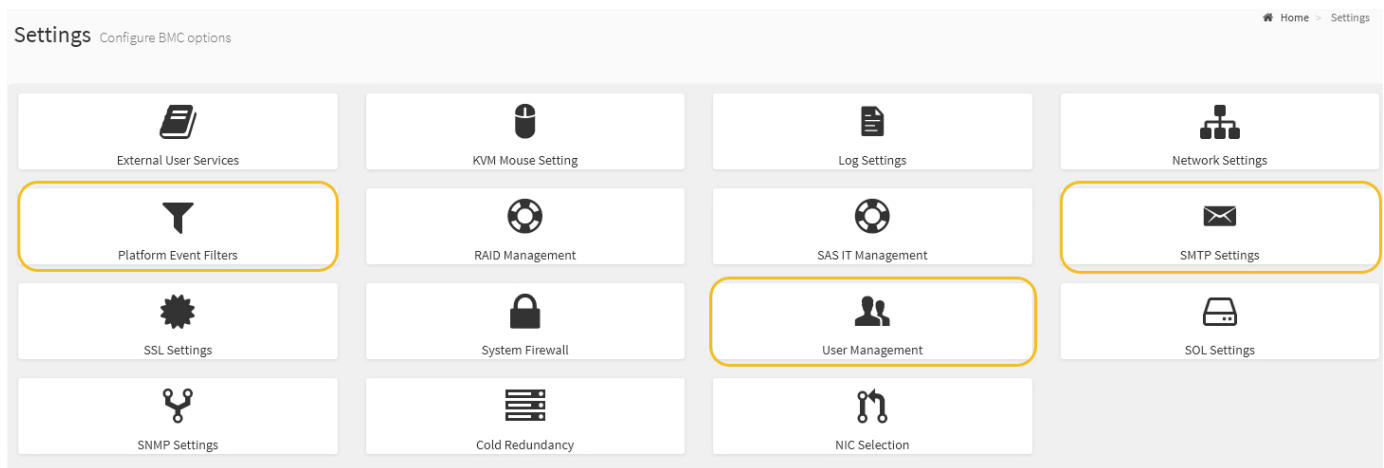
如果SG6000-CN控制器或服务设备发生故障并需要更换、则可能无法保留此操作步骤 所做的BMC设置。请确保您已应用所有设置，以便在更换硬件后根据需要轻松重新应用这些设置。

开始之前

您知道如何访问 BMC 信息板。

关于此任务

在 BMC 界面中，您可以使用设置页面上的 * SMTP 设置 * ， * 用户管理 * 和 * 平台事件筛选器 * 选项来配置电子邮件通知。



步骤

1. "配置BMC的SNMP设置"。
 - a. 选择 * 设置 * > * SMTP 设置 * 。
 - b. 对于发件人电子邮件 ID ，请输入有效的电子邮件地址。

此电子邮件地址在 BMC 发送电子邮件时作为发件人地址提供。

2. 设置用户以接收警报。

- a. 从 BMC 信息板中，选择 * 设置 * > * 用户管理 *。
- b. 至少添加一个用户以接收警报通知。

您为用户配置的电子邮件地址是 BMC 向其发送警报通知的地址。例如，您可以添加一个通用用户，例如 "notification-user"，并使用技术支持团队 Email 发送名单的电子邮件地址。

3. 配置警报的 LAN 目标。

- a. 选择 * 设置 * > * 平台事件筛选器 * > * LAN 目标 *。
- b. 至少配置一个 LAN 目标。
 - 选择 * 电子邮件 * 作为目标类型。
 - 对于 BMC 用户名，请选择先前添加的用户名。
 - 如果您添加了多个用户、并且希望所有用户都接收通知电子邮件、请为每个用户添加一个 LAN 目标。
- c. 发送测试警报。

4. 配置警报策略，以便定义 BMC 发送警报的时间和位置。

- a. 选择 * 设置 * > * 平台事件筛选器 * > * 警报策略 *。
- b. 为每个 LAN 目标至少配置一个警报策略。
 - 对于策略组编号，请选择 * 1 *。
 - 对于策略操作，选择 * 始终向此目标发送警报 *。
 - 对于 LAN 通道，选择 * 1 *。
 - 在目标选择器中，选择策略的 LAN 目标。

5. 配置事件筛选器以将不同事件类型的警报定向到相应的用户。

- a. 选择 * 设置 * > * 平台事件筛选器 * > * 事件筛选器 *。
- b. 对于警报策略组编号，输入 * 1 *。
- c. 为要通知警报策略组的每个事件创建筛选器。
 - 您可以为电源操作，特定传感器事件或所有事件创建事件筛选器。
 - 如果不确定要监控哪些事件，请选择 "Sensor Type"（传感器类型）为 "All 传感器"（所有传感器），并选择 "Event Options"（事件选项）为 "All Events"（所有事件）。如果收到不需要的通知，您可以稍后更改所做的选择。

可选：启用节点或驱动器加密

您可以在节点和磁盘级别启用加密、以防止设备中的磁盘物理丢失或从站点中删除。

- **节点加密** 使用软件加密来保护设备中的所有磁盘。它不需要特殊的驱动器硬件。节点加密由设备软件使用外部密钥管理服务(KMS)管理的密钥执行。
- **驱动器加密** 使用硬件加密来保护自加密驱动器(SED)、也称为全磁盘加密(FED)驱动器、包括符合联邦信息处理标准(FIPS)的驱动器。驱动器加密在每个驱动器中使用由StorageGRID密钥管理器管理的加密密钥执行。

您可以对受支持的驱动器执行这两个加密级别、以提高安全性。

请参见 ["StorageGRID加密方法"](#) 有关可用于StorageGRID设备的所有加密方法的信息。

启用节点加密

如果启用了节点加密，则可以通过安全密钥管理服务器（KMS）加密来保护设备中的磁盘，防止物理丢失或从站点中删除。您必须在设备安装期间选择并启用节点加密。在KMS加密过程启动后、您无法禁用节点加密。

如果使用ConfigBuilder生成JSON文件、则可以自动启用节点加密。请参见 ["自动安装和配置设备"](#)。

开始之前

查看有关的信息 ["正在配置KMS"](#)。

关于此任务

启用了节点加密的设备将连接到为 StorageGRID 站点配置的外部密钥管理服务器（KMS）。每个 KMS（或 KMS 集群）负责管理站点上所有设备节点的加密密钥。这些密钥对启用了节点加密的设备中每个磁盘上的数据进行加密和解密。

可以在 StorageGRID 中安装 KMS 之前或之后在网格管理器中设置此设备。有关更多详细信息，请参见管理 StorageGRID 的说明中有关 KMS 和设备配置的信息。

- 如果在安装设备之前设置了 KMS，则在设备上启用节点加密并将其添加到配置了 KMS 的 StorageGRID 站点时，KMS 控制的加密将开始。
- 如果在安装此设备之前未设置 KMS，则在为包含此设备节点的站点配置了 KMS 并可使用此 KMS 后，将对启用了节点加密的每个设备执行 KMS 控制的加密。



如果在安装设备时启用了节点加密、则会分配一个临时密钥。设备上的数据在连接到密钥管理系统(Key Management System、KMS)并设置KMS安全密钥之前不会受到保护。请参见 ["Kms设备配置概述"](#) 适用于追加信息。

如果没有解密磁盘所需的KMS密钥、则无法检索设备上的数据、并且实际上会丢失。如果无法从KMS中检索到解密密钥、则会出现这种情况。如果客户清除 KMS 配置，KMS 密钥过期，与 KMS 的连接断开或从安装了 KMS 密钥的 StorageGRID 系统中删除设备，则无法访问此密钥。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

`https://Controller_IP:8443`

Controller_IP 是三个StorageGRID 网络中任何一个网络上计算控制器(而不是存储控制器)的IP地址。

此时将显示 StorageGRID 设备安装程序主页页面。



使用KMS密钥对设备加密后、如果不使用同一个KMS密钥、则无法对设备磁盘进行解密。

2. 选择 * 配置硬件 * > * 节点加密 *。

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

⚠ You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption
☒

Save

Key Management Server Details

3. 选择 * 启用节点加密 *。

在安装设备之前，您可以清除*启用节点加密*，而不会丢失数据。安装开始时、设备节点会访问StorageGRID 系统中的KMS加密密钥并开始磁盘加密。安装此设备后、您将无法禁用节点加密。



在将启用了节点加密的设备添加到具有KMS的StorageGRID 站点之后、您无法停止对此节点使用KMS加密。

4. 选择 * 保存 *。

5. 将设备部署为 StorageGRID 系统中的节点。

当设备访问为 StorageGRID 站点配置的 KMS 密钥时，便会开始使用由 KMS 控制的加密。安装程序会在 KMS 加密过程中显示进度消息，此过程可能需要几分钟时间，具体取决于设备中的磁盘卷数。



设备最初会配置一个随机的非 KMS 加密密钥，该密钥会分配给每个磁盘卷。磁盘会使用此临时加密密钥进行加密，这种加密密钥不安全，直到启用了节点加密的设备访问为 StorageGRID 站点配置的 KMS 密钥为止。

完成后

您可以查看节点加密状态，KMS 详细信息以及设备节点处于维护模式时正在使用的证书。请参见 ["监控维护模式下的节点加密"](#) 以了解相关信息。

驱动器加密

在写入和读取过程中、驱动器加密在自加密驱动器(SED)硬件上进行管理。对这些驱动器上数据的访问由用户定义的密码短语控制。驱动器加密用于在StorageGRID设备中缓存所用的直连固态驱动器(SSD)。

当设备关闭或从设备中删除驱动器时、加密的SRD会自动锁定。加密的SED在恢复供电后保持锁定状态、直到输入正确的密码短语为止。要允许在不手动重新输入密码短语的情况下访问驱动器、此密码短语会存储在StorageGRID设备上、以便在设备重新启动时解锁设备中保留的加密驱动器。知道SED密码短语的任何人都可以访问使用SED密码短语加密的驱动器。

驱动器加密不适用于SANtricity-managed驱动器。如果您的设备具有StorageGRID和SANtricity控制器、则可以在中启用驱动器安全性 ["SANtricity 系统管理器"](#)。

您可以在初始设备安装期间启用驱动器加密、然后再加载Grid Manager。您还可以通过将设备置于维护模式来启用节点加密或更改密码短语。

开始之前

查看有关的信息 ["StorageGRID加密方法"](#)。

关于此任务

首次启用驱动器加密时会设置密码短语。如果更换了某个计算节点或将加密的SED移至新计算节点、则必须手动重新输入密码短语。



请确保将驱动器加密密码短语存储在安全位置。如果加密的SED安装在另一个StorageGRID设备中、则在不手动输入相同密码短语的情况下、无法访问该SED。

启用驱动器加密

1. 访问StorageGRID设备安装程序。

- 在初始设备安装期间、打开浏览器并输入设备计算控制器的IP地址之一。

`https://Controller_IP:8443`

Controller_IP 是三个StorageGRID 网络中任何一个网络上计算控制器(而不是存储控制器)的IP地址。

- 对于现有StorageGRID设备、["将产品置于维护模式"](#)。

2. 从StorageGRID设备安装程序的主页页面中, 选择*Configure Harder*>*Drive Encryption*。

3. 选择*启用驱动器加密*。



启用驱动器加密并设置密码短语后、SED驱动器将进行硬件加密。如果不使用相同的密码短语、则无法访问驱动器的内容。

4. 选择 * 保存 *。

驱动器加密后、将显示驱动器密码短语信息。



在对驱动器进行初始加密时、密码短语会设置为默认空值、并且当前密码短语文本会指示"default (not sSecure)"。虽然此驱动器上的数据已加密、但在设置唯一密码之前、无需输入密码短语即可访问此驱动器。

5. 输入用于加密驱动器访问的唯一密码短语、然后再次输入密码短语进行确认。密码短语必须至少为8个字符、长度不得超过32个字符。

6. 输入密码短语显示文本、以帮助您重新调用密码短语。

将密码短语和密码短语显示文本保存在安全位置、例如密码管理应用程序。

7. 选择 * 保存 *。

查看驱动器加密状态

1. "将设备置于维护模式"。
2. 从StorageGRID设备安装程序中，选择*配置硬件*>*驱动器加密*。

访问加密驱动器

在更换计算节点或将驱动器移至新计算节点后、您必须输入密码短语才能访问加密驱动器。

1. 访问StorageGRID设备安装程序。
 - 打开浏览器、然后输入设备计算控制器的IP地址之一。

`https://Controller_IP:8443`

Controller_IP 是三个StorageGRID 网络中任何一个网络上计算控制器(而不是存储控制器)的IP地址。

- "将设备置于维护模式"。
2. 从StorageGRID设备安装程序中，选择警告横幅中的*Drive Encryption (驱动器加密)*链接。
 3. 输入先前在*新密码短语*和*重新键入新密码短语*中设置的驱动器加密密码短语。



如果为密码短语和密码短语显示文本输入值、而这些值与先前输入的值不匹配、则驱动器身份验证将失败。您需要重新启动设备并输入正确的密码短语和密码短语显示文本。

4. 输入先前在*新密码短语显示文本*中设置的密码短语显示文本。
5. 选择 * 保存 *。

驱动器解锁后、将不再显示警告横幅。

6. 返回StorageGRID设备安装程序主页页面、并在安装部分横幅中选择*重新启动*、以重新启动计算节点并访问加密驱动器。

更改驱动器加密密码短语

1. 访问StorageGRID设备安装程序。
 - 打开浏览器、然后输入设备计算控制器的IP地址之一。

`https://Controller_IP:8443`

Controller_IP 是三个StorageGRID 网络中任何一个网络上计算控制器(而不是存储控制器)的IP地址。

- "将设备置于维护模式"。
2. 从StorageGRID设备安装程序中，选择*配置硬件*>*驱动器加密*。
 3. 输入新的唯一驱动器访问密码短语、然后再次输入密码短语进行确认。密码短语必须至少为8个字符、长度不得超过32个字符。



您必须事先通过驱动器访问权限的身份验证、然后才能更改驱动器加密密码短语。

4. 输入密码短语显示文本、以帮助您重新调用密码短语。
5. 选择 * 保存 *。



设置新密码短语后、如果不使用新密码短语和密码短语显示文本、则无法对加密的驱动器解密。

6. 将新密码短语和密码短语显示文本保存在安全位置、例如密码管理应用程序。

禁用驱动器加密

1. 访问StorageGRID设备安装程序。
 - 打开浏览器、然后输入设备计算控制器的IP地址之一。

`https://Controller_IP:8443`

Controller_IP 是三个StorageGRID 网络中任何一个网络上计算控制器(而不是存储控制器)的IP地址。

- "将设备置于维护模式"。
2. 从StorageGRID设备安装程序中, 选择*配置硬件*>*驱动器加密*。
 3. 清除*启用驱动器加密*。
 4. 要在禁用驱动器加密后擦除所有驱动器数据, 请选择*擦除驱动器上的所有数据*。



只有在将设备添加到网格之前、才能从StorageGRID设备安装程序中使用数据清理选项。从维护模式访问StorageGRID设备安装程序时、您无法访问此选项。

5. 选择 * 保存 *。

驱动器内容将被加密或以加密方式擦除、加密密码短语将被擦除、现在无需密码短语即可访问SED。

可选：更改RAID模式(SG5760和SG6000)

在某些型号的设备上、您可以更改为设备上的其他RAID模式、以满足您的存储和恢复要求。您只能在部署设备存储节点之前更改此模式。

如果使用ConfigBuilder生成JSON文件、则可以自动更改RAID模式。请参见 "[自动安装和配置设备](#)"。

关于此任务

如果您的设备支持、您可以选择以下卷配置选项之一：

- **动态磁盘池(DDP)**：此模式对每八个数据驱动器使用两个奇偶校验驱动器。这是所有设备的默认和建议模式。与RAID 6相比、DDP可提供更高的系统性能、减少驱动器发生故障后的重建时间、并简化管理。DDP还在SG5760设备中提供抽盒丢失保护。



由于有两个SSD、DDP不会在SG6060设备中提供抽盒丢失保护。对于添加到SG6060中的任何扩展架、抽屉丢失保护功能均有效。

- * DDP16*：此模式每 16 个数据驱动器使用两个奇偶校验驱动器，因此与 DDP 相比，存储效率更高。与RAID 6相比、DDP16可提供更好的系统性能、减少驱动器发生故障后的重建时间、简化管理并具有同等的存储效率。要使用 DDP16 模式，您的配置必须至少包含 20 个驱动器。DDP16 不提供抽盒丢失保护。
- * RAID6*：此模式每 16 个或更多数据驱动器使用两个奇偶校验驱动器。这是一种硬件保护方案、它会在每个磁盘上使用奇偶校验条带、并允许RAID集中出现两个磁盘故障、以免丢失任何数据。要使用 RAID 6 模式，您的配置必须至少包含 20 个驱动器。虽然与DDP相比、RAID 6可以提高设备的存储效率、但不建议在大多数StorageGRID 环境中使用。



如果已配置任何卷或先前已安装 StorageGRID，则更改 RAID 模式会删除和更换这些卷。这些卷上的所有数据都将丢失。

SG5760

开始之前

- 您有一个SG5760、其中包含60个驱动器。如果您使用的是SG5712、则必须使用默认DDP模式。
- 您正在使用可以连接到 StorageGRID 的任何客户端。
- 客户端具有 "支持的 Web 浏览器"。

步骤

1. 使用服务笔记本电脑打开Web浏览器并访问StorageGRID 设备安装程序：
`https://E5700SG_Controller_IP:8443`

其中 *E5700SG_Controller_IP* 是E5700SG控制器的任何IP地址。

2. 选择 * 高级 * > * RAID 模式 *。
3. 在 * 配置 RAID 模式 * 页面上，从模式下拉列表中选择所需的 RAID 模式。
4. 单击 * 保存 *。

SG6000

开始之前

- 您正在使用可以连接到 StorageGRID 的任何客户端。
- 客户端具有 "支持的 Web 浏览器"。

步骤

1. 打开浏览器，然后输入设备计算控制器的 IP 地址之一。

`https://Controller_IP:8443`

Controller_IP 是三个StorageGRID 网络中任何一个网络上计算控制器(而不是存储控制器)的IP地址。

此时将显示 StorageGRID 设备安装程序主页页面。

2. 选择 * 高级 * > * RAID 模式 *。
3. 在 * 配置 RAID 模式 * 页面上，从模式下拉列表中选择所需的 RAID 模式。
4. 单击 * 保存 *。

可选：重新映射设备的网络端口

您可以选择将设备节点上的内部端口重新映射到不同的外部端口。例如，由于使用了防火墙问题描述，您可能需要重新映射端口。

开始之前

- 您先前已访问 StorageGRID 设备安装程序。

关于此任务

不能对负载均衡器端点使用重新映射的端口。如果需要删除重新映射的端口、请按照中的步骤进行操作 ["删除端口重新映射"](#)。

步骤

1. 从StorageGRID 设备安装程序中，选择*Configure Networking*>*Remap Ports*。

此时将显示 Remap Port 页面。

2. 从 * 网络 * 下拉框中，为要重新映射的端口选择网络：网格，管理员或客户端。
3. 从 * 协议 * 下拉框中，选择 IP 协议： TCP 或 UDP 。
4. 从 * 映射方向 * 下拉框中，选择要为此端口重新映射的流量方向：入站，出站或双向。
5. 对于 * 原始端口 * ，输入要重新映射的端口的编号。
6. 对于 * 映射到端口 * ，请输入要使用的端口编号。
7. 选择*添加规则*。

此时，新端口映射将添加到表中，重新映射将立即生效。

8. 要删除端口映射，请选择要删除的规则对应的单选按钮，然后选择*删除选定规则*。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。