



# 维护设备配置

## StorageGRID Appliances

NetApp  
April 11, 2024

# 目录

维护设备配置 .....	1
节点维护的通用过程：概述 .....	1
将设备置于维护模式 .....	1
更改 MTU 设置 .....	3
检查 DNS 服务器配置 .....	5
更新MAC地址引用 .....	7
监控维护模式下的节点加密 .....	8

# 维护设备配置

## 节点维护的通用过程：概述

按照以下说明维护StorageGRID 系统。

### 关于这些说明

这些说明介绍了所有节点通用的过程、例如、如何应用软件修补程序、恢复网格节点、恢复故障站点、停用网格节点或整个站点、执行网络维护、执行主机级和中间件维护过程以及执行网格节点过程。



在这些说明中，“Linux”是指Red Hat®Enterprise Linux®、Ubuntu®或Debian®部署。使用“[NetApp 互操作性表工具 \(IMT\)](#)”以获取支持的版本列表。

### 开始之前

- 您对 StorageGRID 系统有着广泛的了解。
- 您已查看 StorageGRID 系统的拓扑并了解网格配置。
- 您知道必须严格按照所有说明进行操作，并注意所有警告。
- 您了解、未介绍的维护过程不受支持或不需要服务项目。

### 设备的维护过程

每种类型的StorageGRID 设备的特定维护过程请参见设备维护部分：

- ["维护SG6100设备"](#)
- ["维护 SG6000 设备"](#)
- ["维护 SG5700 设备"](#)
- ["维护SG100和SG1000设备"](#)

## 将设备置于维护模式

在执行特定维护过程之前，您必须将设备置于维护模式。

### 开始之前

- 您将使用登录到网格管理器 ["支持的 Web 浏览器"](#)。
- 您具有维护或 root 访问权限。有关详细信息，请参见有关管理 StorageGRID 的说明。

### 关于此任务

在极少数情况下，将 StorageGRID 设备置于维护模式可能会使该设备无法进行远程访问。



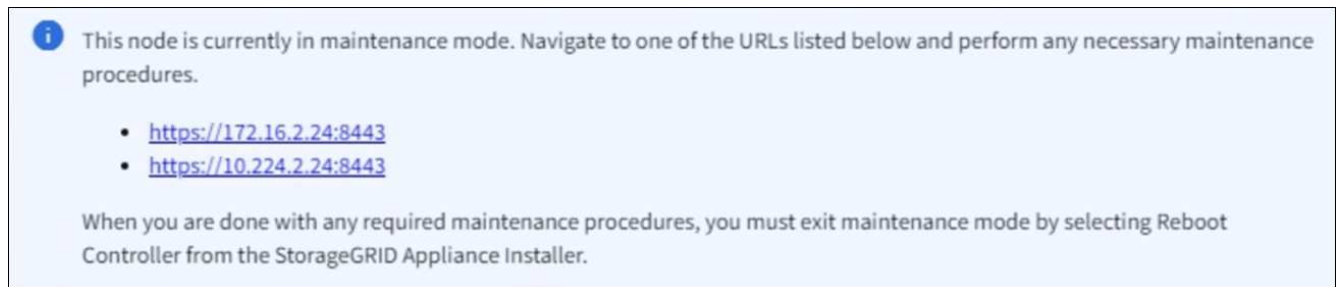
处于维护模式的 StorageGRID 设备的管理员帐户密码和 SSH 主机密钥与该设备运行时的密码和主机密钥保持不变。

## 步骤

1. 在网格管理器中，选择 \* 节点 \*。
2. 从节点页面的树视图中，选择设备存储节点。
3. 选择 \* 任务 \*。
4. 选择 \* 维护模式 \*。此时将显示确认对话框。
5. 输入配置密码短语，然后选择 \* 确定 \*。

进度条和一系列消息（包括 " 已发送请求 "，" 正在停止 StorageGRID " 和 " 正在重新启动 "）表示设备正在完成进入维护模式的步骤。

设备处于维护模式时，会显示一条确认消息，其中列出了可用于访问 StorageGRID 设备安装程序的 URL。



6. 要访问 StorageGRID 设备安装程序，请浏览到显示的任何 URL。

如果可能，请使用包含设备管理网络端口 IP 地址的 URL。




如果直接连接到设备的管理端口、请使用 `https://169.254.0.1:8443` 以访问 StorageGRID 设备安装程序页面。

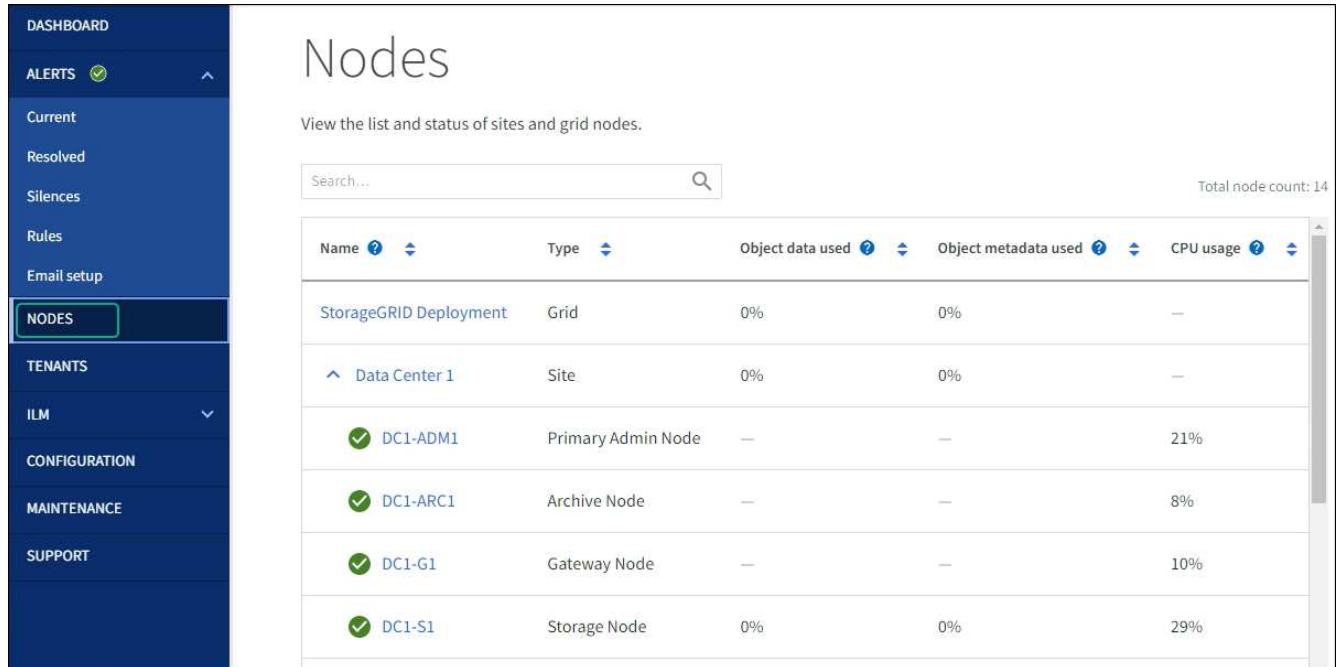
7. 在 StorageGRID 设备安装程序中，确认设备处于维护模式。

**⚠** This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

8. 执行任何必要的维护任务。
9. 完成维护任务后，退出维护模式并恢复正常节点操作。在 StorageGRID 设备安装程序中，选择 \* 高级 \* > \* 重新启动控制器 \*，然后选择 \* 重新启动至 StorageGRID \*。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网络管理器。n 节点\* 页面应显示正常状态(绿色复选标记图标  节点名称左侧)、表示没有处于活动状态的警报、并且节点已连接到网格。



## 更改 MTU 设置

您可以更改在为设备节点配置 IP 地址时分配的 MTU 设置。



关于此任务

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。

要在不重新启动设备节点的情况下更改 MTU 设置，[使用更改 IP 工具](#)。

如果在初始安装期间未在 StorageGRID 设备安装程序中配置客户端或管理网络，[使用维护模式更改 MTU 设置](#)。

## 使用更改 IP 工具更改 MTU 设置

开始之前

您拥有 Passwords.txt 文件以使用更改 IP 工具。

步骤

访问更改 IP 工具并按中所述更新 MTU 设置 "[更改节点网络配置](#)"。

## 使用维护模式更改 MTU 设置

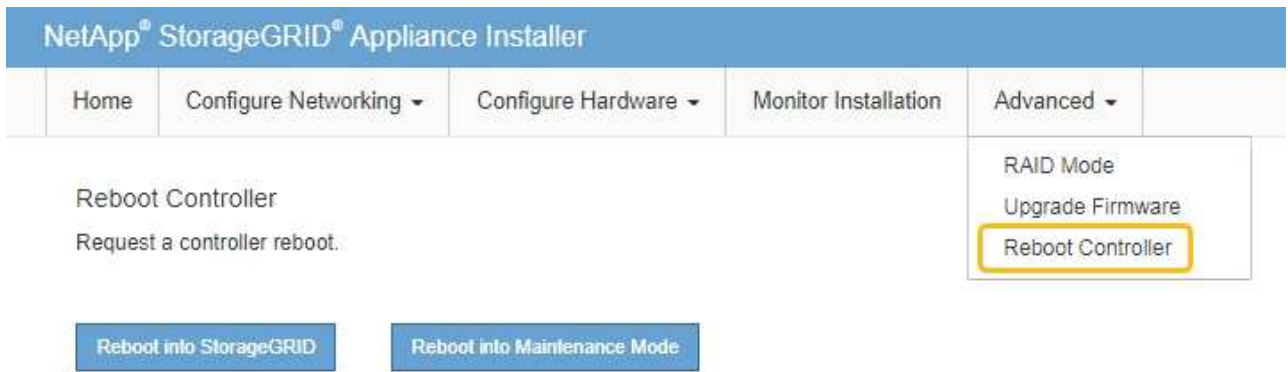
如果无法使用更改 IP 工具访问这些设置，请使用维护模式更改 MTU 设置。


开始之前

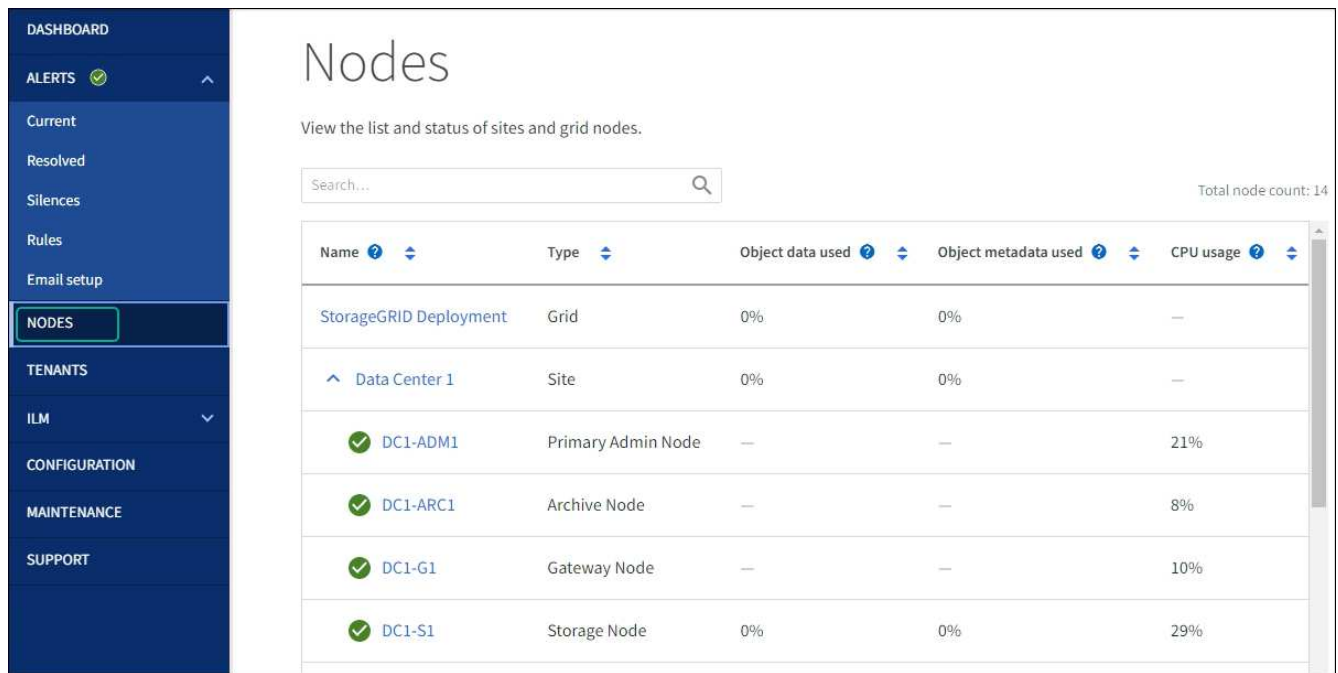
此设备已运行 "[已置于维护模式](#)"。

步骤

1. 从 StorageGRID 设备安装程序中，选择 \* 配置网络连接 \* > \* IP 配置 \*。
2. 对网格网络，管理网络和客户端网络的 MTU 设置进行所需的更改。
3. 如果对设置感到满意，请选择 \* 保存 \*。
4. 如果此操作步骤已成功完成，并且您在节点处于维护模式时还需要执行其他过程，请立即执行。完成后，或者如果遇到任何故障并希望重新启动，请选择 \* 高级 \* > \* 重新启动控制器 \*，然后选择以下选项之一：
  - 选择 \* 重新启动到 StorageGRID \*
  - 选择 \* 重新启动至维护模式 \* 以重新启动控制器，同时使节点仍处于维护模式。如果您在操作步骤期间遇到任何故障并希望重新启动，请选择此选项。节点重新启动至维护模式后，从出现故障的操作步骤中的相应步骤重新启动。



设备重新启动并重新加入网络可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网络，请返回网络管理器。n节点\*页面应显示正常状态(绿色复选标记图标  节点名称左侧)、表示没有处于活动状态的警报、并且节点已连接到网络。



## 检查 DNS 服务器配置

您可以检查并临时更改此设备节点当前正在使用的DNS服务器。

开始之前

此设备已运行 "已置于维护模式"。

关于此任务

如果加密设备无法连接到密钥管理服务器(KMS)或KMS集群、因为KMS的主机名指定为域名而非IP地址、则可能需要更改DNS服务器设置。对设备的 DNS 设置所做的任何更改都是临时的，在退出维护模式时将丢失。要使这些更改永久生效，请在网络管理器中指定 DNS 服务器 (\* 维护 \* > \* 网络 \* > \* DNS 服务器 \*)。

- 只有在节点加密的设备中，使用完全限定域名（而不是 IP 地址）为主机名定义 KMS 服务器时，才需要临时更改 DNS 配置。
- 当节点加密设备使用域名连接到 KMS 时，它必须连接到为网络定义的一个 DNS 服务器。然后，其中一个 DNS 服务器会将域名转换为 IP 地址。
- 如果节点无法访问网络的 DNS 服务器、或者您在节点加密设备节点脱机时更改了网络范围的 DNS 设置、则该节点将无法连接到 KMS。解析 DNS 问题描述 之前、无法对设备上的加密数据进行解密。


要解决 DNS 问题描述 阻止 KMS 连接的问题，请在 StorageGRID 设备安装程序中指定一个或多个 DNS 服务器的 IP 地址。通过这些临时 DNS 设置，设备可以连接到 KMS 并对节点上的数据进行解密。

例如、如果在加密节点脱机时网络的 DNS 服务器发生更改、则该节点在恢复联机后将无法访问 KMS、因为它仍在使用先前的 DNS 值。在 StorageGRID 设备安装程序中输入新的 DNS 服务器 IP 地址后，可以通过临时 KMS 连接对节点数据进行解密。

#### 步骤

1. 从 StorageGRID 设备安装程序中，选择 \* 配置网络连接 \* > \* DNS 配置 \*。
2. 验证指定的 DNS 服务器是否正确。

#### DNS Servers

 Configuration changes made on this page will not be passed to the StorageGRID software after appliance installation.

**Servers**

Server 1	<input style="width: 95%;" type="text" value="10.224.223.135"/>	✕
Server 2	<input style="width: 95%;" type="text" value="10.224.223.136"/>	+ ✕

3. 如果需要，请更改 DNS 服务器。



对 DNS 设置所做的更改是临时的，当您退出维护模式时，这些更改将丢失。

4. 对临时 DNS 设置感到满意后，请选择 \* 保存 \*。


节点使用此页面上指定的 DNS 服务器设置重新连接到 KMS，从而可以解密节点上的数据。

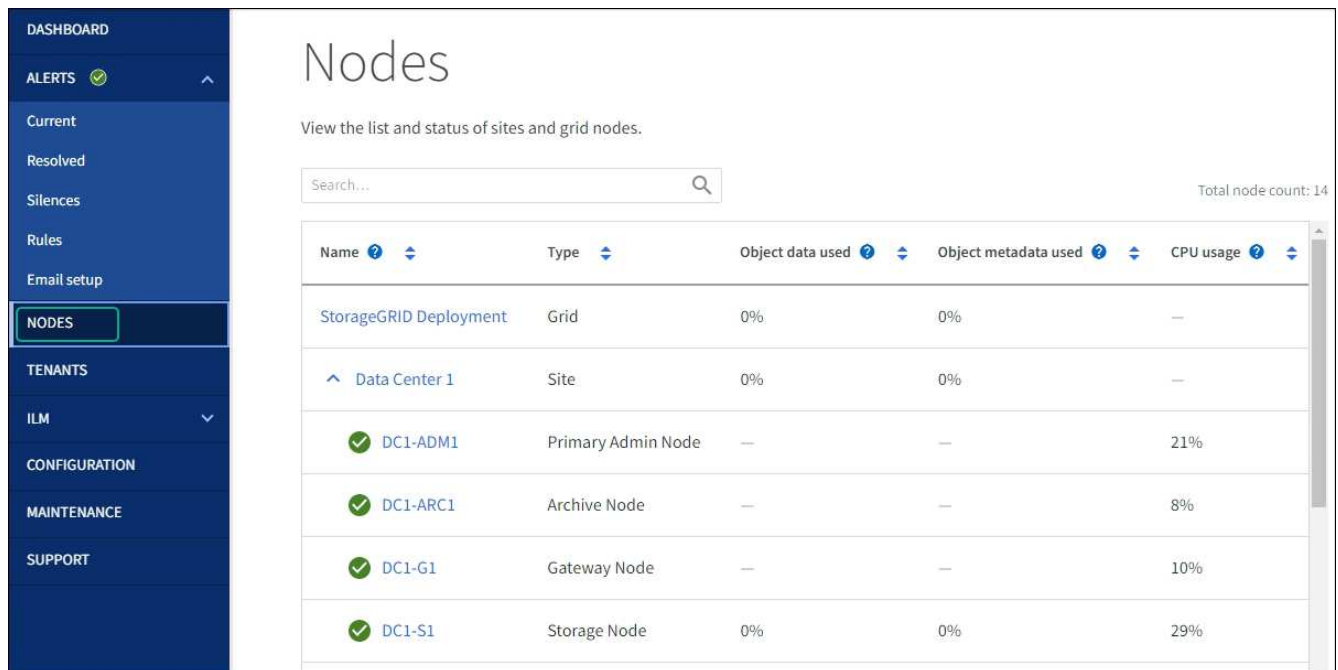
5. 解密节点数据后，重新启动节点。在 StorageGRID 设备安装程序中，选择 \* 高级 \* > \* 重新启动控制器 \*，然后选择以下选项之一：
  - 选择 \* 重新启动到 StorageGRID \* 以在节点重新加入网络的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
  - 选择 \* 重新启动至维护模式 \* 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。）如果在重新加入网络之前需要对节点执行其他维护操作，请选择此选项。





当节点重新启动并重新加入网格时，它将使用网格管理器中列出的系统范围的 DNS 服务器。重新加入网格后，在设备处于维护模式时，设备将不再使用 StorageGRID 设备安装程序中指定的临时 DNS 服务器。

设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网络管理器。n节点\*页面应显示正常状态(绿色复选标记图标  节点名称左侧)、表示没有处于活动状态的警报、并且节点已连接到网格。



## 更新MAC地址引用

在某些情况下、您可能需要在更换设备后更新MAC地址引用。

关于此任务

如果要更换的设备上的任何网络接口配置了DHCP、则可能需要更新DHCP服务器上的永久DHCP租约分配、以引用替代设备的MAC地址。此更新可确保为替代设备分配预期的IP地址。

## 步骤

1. 找到产品正面的标签。此标签列出了设备的BMC管理端口的MAC地址。
2. 要确定管理网络端口的 MAC 地址，必须在标签上的十六进制数字中添加 \* 。 2 \*

例如，如果标签上的 MAC 地址以 **09** 结尾，则管理端口的 MAC 地址将以 **0B** 结尾。如果标签上的 MAC 地址以 \* (y) FF\* 结尾，则管理端口的 MAC 地址将以 \* (y+1) 01\* 结尾。

您可以通过在 Windows 中打开 Calculator ，将其设置为程序编程模式，选择十六进制，键入 MAC 地址，然后键入 \* + 2 =\* 来轻松进行计算。

3. 请网络管理员将您删除的设备的 DNS/network 和 IP 地址与替换设备的 MAC 地址关联起来。



在为替代设备接通电源之前，您必须确保原始设备的所有 IP 地址均已更新。否则，设备将在启动时获取新的 DHCP IP 地址，并且可能无法重新连接到 StorageGRID 。此步骤将对连接到设备的所有 StorageGRID 网络执行适用场景。



如果原始设备使用静态 IP 地址，新设备将自动采用您删除的设备的 IP 地址。

## 监控维护模式下的节点加密

如果您在安装期间为设备启用了节点加密，则可以监控每个设备节点的节点加密状态，包括节点加密状态和密钥管理服务器（KMS）详细信息。

请参见 "[配置密钥管理服务器](#)" 有关为StorageGRID 设备实施KMS的信息。

### 开始之前

- 您在安装期间为设备启用了节点加密。安装此设备后、您无法启用节点加密。
- 您已拥有 "[已将设备置于维护模式](#)"。


## 步骤

1. 从 StorageGRID 设备安装程序中，选择 \* 配置硬件 \* > \* 节点加密 \* 。

## 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

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfe01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696


Server certificate



Client certificate



### Clear KMS Key

 Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

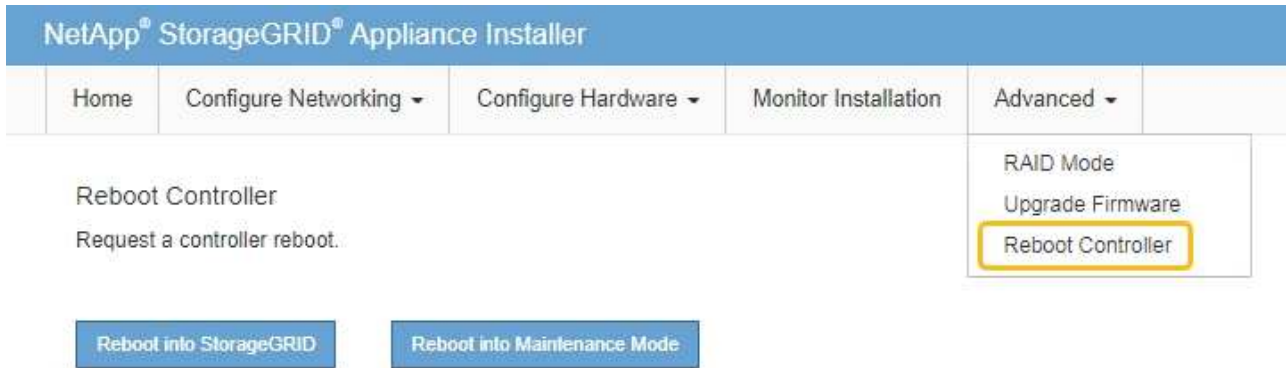
节点加密页面包括三个部分：


- "加密状态" 显示设备是启用还是禁用了节点加密。
- 密钥管理服务器详细信息显示了有关用于对设备进行加密的 KMS 的信息。您可以展开服务器和客户端证书部分以查看证书详细信息和状态。
  - 要解决证书本身的问题，例如续订已过期的证书，请参见 ["有关配置 KMS 的说明"](#)。
  - 如果连接到 KMS 主机时出现意外问题，请验证 ["DNS服务器正确"](#) 这样 ["已正确配置设备网络"](#)。
  - 如果无法解决证书问题，请联系技术支持。
- 清除 KMS 密钥会禁用设备的节点加密，删除设备与为 StorageGRID 站点配置的密钥管理服务器之间的关联，并删除设备中的所有数据。您必须 [清除 KMS 密钥](#) 在将设备安装到另一个 StorageGRID 系统之前。

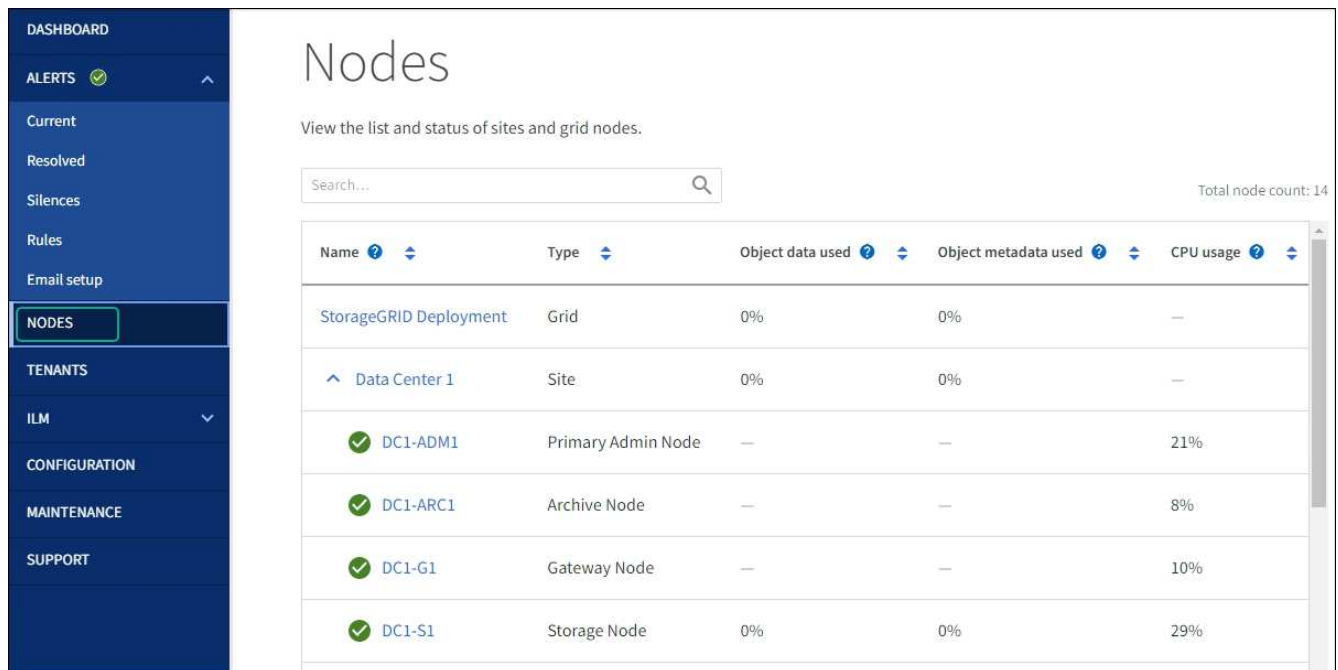


清除 KMS 配置将从设备中删除数据，从而使其永远无法访问。此数据不可恢复。

- 检查完节点加密状态后，重新启动节点。在 StorageGRID 设备安装程序中，选择 \* 高级 \* > \* 重新启动控制器 \*，然后选择以下选项之一：
  - 选择 \* 重新启动到 StorageGRID \* 以在节点重新加入网格的情况下重新启动控制器。如果您已完成维护模式下的工作并准备好将节点恢复正常运行，请选择此选项。
  - 选择 \* 重新启动至维护模式 \* 以重新启动控制器，同时使节点仍处于维护模式。（只有当控制器处于维护模式时，此选项才可用。）如果在重新加入网格之前需要对节点执行其他维护操作，请选择此选项。



设备重新启动并重新加入网格可能需要长达 20 分钟的时间。要确认重新启动已完成且节点已重新加入网格，请返回网格管理器。n节点\*页面应显示正常状态(绿色复选标记图标  节点名称左侧)、表示没有处于活动状态的警报、并且节点已连接到网格。



## 清除密钥管理服务器配置

清除密钥管理服务器（KMS）配置将禁用设备上的节点加密。清除 KMS 配置后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

开始之前

如果需要保留设备上的数据，则必须先执行节点停用操作步骤 或克隆节点，然后才能清除 KMS 配置。



清除 KMS 后，设备上的数据将被永久删除，并且无法再访问。此数据不可恢复。

"停用节点" 将其包含的任何数据移动到 StorageGRID 中的其他节点。

关于此任务

清除设备 KMS 配置将禁用节点加密，从而删除设备节点与 StorageGRID 站点的 KMS 配置之间的关联。然后，设备上的数据将被删除，并且设备将保持预安装状态。此过程无法反转。

必须清除 KMS 配置：

- 在将设备安装到不使用 KMS 或使用其他 KMS 的其他 StorageGRID 系统之前，请先安装此设备。



如果您计划在使用相同KMS密钥的StorageGRID 系统中重新安装设备节点、请勿清除KMS配置。

- 在恢复和重新安装 KMS 配置丢失且 KMS 密钥不可恢复的节点之前。
- 在退回您的站点上先前使用的任何设备之前。
- 停用已启用节点加密的设备后。



在清除 KMS 以将其数据移动到 StorageGRID 系统中的其他节点之前，请停用此设备。在停用设备之前清除 KMS 将导致数据丢失，并可能导致设备无法运行。

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 \* 配置硬件 \* > \* 节点加密 \*。



如果清除了 KMS 配置，则设备上的数据将被永久删除。此数据不可恢复。

3. 在窗口底部，选择 \* 清除 KMS 密钥和删除数据 \*。
4. 如果确实要清除KMS配置、请键入 **clear** 在警告对话框中，选择\*Clear KMS Key (清除KMS密钥)和Delete Data\*(删除数据)。

KMS 加密密钥和所有数据将从节点中删除，设备将重新启动。这可能需要长达 20 分钟。

5. 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。

6. 选择 \* 配置硬件 \* > \* 节点加密 \*。
7. 验证是否已禁用节点加密，以及是否已从窗口中删除 \* 密钥管理服务器详细信息 \* 和 \* 清除 KMS 密钥和删除数据 \* 控件中的密钥和证书信息。

在网格中重新安装设备之前、无法在此设备上重新启用节点加密。

完成后

在设备重新启动并确认 KMS 已清除且设备处于预安装状态后，您可以从 StorageGRID 系统中物理删除此设备。请参见 ["有关准备重新安装设备的说明"](#)。

## 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。