



从非主管理节点故障恢复

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/storagegrid-120/maintain/recovering-from-non-primary-admin-node-failures.html> on July 23, 2026. Always check docs.netapp.com for the latest.

目录

- 从非主管理节点故障恢复 1
 - 从非主 StorageGRID 管理节点故障中恢复 1
 - 从失败的非主 StorageGRID 管理节点复制审核日志 1
 - 替换非主 StorageGRID 管理节点 2
 - 选择"开始恢复"以配置非主 StorageGRID 管理节点 2
 - 在恢复的非主 StorageGRID 管理节点上还原审核日志 4
 - 在恢复非主管理节点时还原 StorageGRID 管理节点数据库 5
 - 恢复非主 StorageGRID 管理节点时还原 Prometheus 指标 7

从非主管理节点故障恢复

从非主 **StorageGRID** 管理节点故障中恢复

您必须完成以下任务才能从非主管理节点故障中恢复。一个管理节点托管配置管理节点 (CMN) 服务，称为主管理节点。虽然您可以有多个管理节点，但每个 StorageGRID 系统仅包含一个主管理节点。所有其他管理节点均为非主管理节点。

按照以下高级步骤恢复非主管理节点：

1. "从失败的非主管理节点复制审核日志"
2. "替换非主管理节点"
3. "选择"开始恢复"以配置非主管理节点"
4. "在已恢复的非主管理节点上还原审核日志"
5. "还原非主管理节点时还原管理节点数据库"
6. "恢复非主管理节点时还原 Prometheus 指标"

从失败的非主 **StorageGRID** 管理节点复制审核日志

如果您能够从失败的管理节点复制审核日志，则应保留它们以维护网格的系统活动和使用记录。您可以在恢复的非主管理节点启动和运行后将保留的审核日志还原到该节点。

此过程将审核日志文件从失败的管理节点复制到单独网格节点上的临时位置。然后，可以将这些保留的审核日志复制到替换的管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从故障管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点会开始将事件记录到新的空审核日志文件中，之前记录的数据将丢失。如果部署包含多个管理节点，则可以从另一个管理节点恢复审核日志。



如果现在无法在失败的管理节点上访问审核日志，则稍后可能能够访问它们，例如，在主机恢复之后。

1. 如果可能，请登录到发生故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果可用）。
 - a. 输入以下命令：`ssh admin@grid_node_IP`
 - b. 输入 `Passwords.txt` 文件中列出的密码。
 - c. 输入以下命令切换到 root：`su -`
 - d. 输入 `Passwords.txt` 文件中列出的密码。以 root 身份登录时，提示符将从 `$` 更改为 `#`。

2. 停止 AMS 服务，以防止其创建新的日志文件：`service ams stop`
3. 导航到审核导出目录：

```
cd /var/local/audit/export/
```

4. 将源 audit.log 文件重命名为唯一的编号文件名。例如，将 audit.log 文件重命名为 2023-10-25.txt.1。

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. 重新启动 AMS 服务： `service ams start`
6. 创建目录以将所有审核日志文件复制到单独网格节点上的临时位置： `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

出现提示时，输入 admin 的密码。

7. 将所有审核日志文件复制到临时位置： `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

出现提示时，输入 admin 的密码。

8. 以root用户身份注销： `exit`

替换非主 StorageGRID 管理节点

要恢复非主管理节点，首先必须更换物理或虚拟硬件。

您可以将出现故障的非主管理节点替换为在同一平台上运行的非主管理节点，也可以将在 VMware 或 Linux 主机上运行的非主管理节点替换为在服务设备上托管的非主管理节点。

使用与您为节点选择的替换平台相匹配的过程。完成节点替换过程（适用于所有节点类型）后，该过程将引导您进行非主管理节点恢复的下一步。

更换平台	操作步骤
VMware	" 替换 VMware 节点 "
Linux	" 替换 Linux 节点 "
服务设备	" 替换服务设备 "
OpenStack	NetApp 提供的用于 OpenStack 的虚拟机磁盘文件和脚本不再支持恢复操作。如果需要恢复在 OpenStack 部署中运行的节点，请下载适用于您的 Linux 操作系统的文件。然后，按照 " 更换 Linux 节点 " 的程序进行操作。

选择"开始恢复"以配置非主 StorageGRID 管理节点

替换非主管理节点后，必须在 Grid Manager 中选择 Start Recovery，将新节点配置为故障节点的替换节点。

开始之前

- 您已使用 "支持的 Web 浏览器" 登录到网格管理器。
- 您有 "维护或 root 访问权限"。
- 您有配置密码短语。
- 已部署并配置替换节点。

步骤

1. 在网格管理器中，选择*Maintenance* > **Tasks > Recovery**。
2. 在"挂起节点"列表中选择要恢复的网格节点。

节点出现故障后会显示在列表中，但在重新安装并准备好恢复之前，您无法选择节点。

3. 输入 **Provisioning Passphrase**。
4. 单击*开始恢复*。

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search 				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. 在"恢复网格节点"表中监控恢复进度。



在恢复过程运行时，您可以单击 **Reset** 开始新的恢复。此时将显示一个对话框，指示如果重置该过程，节点将处于不确定状态。

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

如果要在重置过程后重试恢复，则必须将节点恢复到预安装状态，如下所示：

- **VMware：**删除已部署的虚拟网格节点。然后，当您准备好重新启动恢复时，请重新部署该节点。
- **Linux：**在 Linux 主机上运行以下命令以重新启动节点：`storagegrid node force-recovery node-name`
- **设备：**如果要在重置过程后重试恢复，则必须通过在节点上运行 `sgareinstall` 将设备节点恢复到预安装状态。请参阅 "[准备设备以重新安装（仅更换平台）](#)"。

6. 如果已为 StorageGRID 系统启用单一登录 (SSO)，并且已将恢复的管理节点的依赖方信任配置为使用默认管理接口证书，请更新（或删除并重新创建）Active Directory Federation Services (AD FS) 中该节点的依赖方信任。使用在管理节点恢复过程中生成的新默认服务器证书。



要配置依赖方信任，请参阅"[\\${post_edited_translations.segment}](#)"。要访问默认服务器证书，请登录到管理节点的命令 shell。转到 `/var/local/mgmt-api` 目录，然后选择 `server.crt` 文件。

在恢复的非主 StorageGRID 管理节点上还原审核日志

如果您能够保留失败的非主管理节点中的审核日志，以便保留历史审核日志信息，则可以将其复制到正在恢复的非主管理节点。

开始之前

- 已安装且正在运行已恢复的管理节点。
- 在原始管理节点发生故障后，您已将审核日志复制到另一个位置。

关于此任务

如果管理节点出现故障，保存到该管理节点的审核日志可能会丢失。通过从故障管理节点复制审核日志，然后将这些审核日志还原到已恢复的管理节点，可能可以防止数据丢失。根据故障情况，可能无法从故障管理节点复制审核日志。在这种情况下，如果部署中有多个管理节点，则可以从另一个管理节点恢复审核日志，因为审核日志会复制到所有管理节点。

如果只有一个管理节点，并且无法从出现故障的节点复制审核日志，则恢复的管理节点将开始将事件记录到审核

日志，就像是全新安装一样。

您必须尽快恢复管理节点才能恢复日志记录功能。



默认情况下，审核信息将发送到管理节点上的审核日志。如果符合以下任一条件，您可以跳过这些步骤：

- 您配置了外部 syslog 服务器，现在将审核日志发送到 syslog 服务器，而不是发送到管理节点。
- 您明确指定仅应在生成审核消息的本地节点上保存审核消息。

有关详细信息，请参阅 ["配置日志管理和外部 syslog 服务器"](#)。

步骤

1. 登录到已恢复的管理节点：

a. 输入以下命令：

```
ssh admin@recovery_Admin_Node_IP
```

b. 输入 `Passwords.txt` 文件中列出的密码。

c. 输入以下命令切换到 root： `su -`

d. 输入 `Passwords.txt` 文件中列出的密码。

以 root 身份登录后，提示符将从 `$` 更改为 `#`。

2. 检查保留了哪些审核文件：

```
cd /var/local/log
```

3. 将保留的审核日志文件复制到恢复的管理节点：

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

出现提示时，输入 admin 的密码。

4. 出于安全考虑，在验证审核日志已成功复制到恢复的管理节点后，从失败的网格节点中删除审核日志。

5. 更新已恢复的管理节点上审核日志文件的用户和组设置：

```
chown ams-user:bycast *
```

6. 以root用户身份注销： `exit`

在恢复非主管理节点时还原 StorageGRID 管理节点数据库

如果要在失败的非主管理节点上保留有关属性和警报的历史信息，则可以从主管理节点还原管理节点数据库。

开始之前

- 已安装且正在运行已恢复的管理节点。

- StorageGRID 系统至少包括两个管理节点。
- 您拥有 Passwords.txt 文件。
- 您有配置密码短语。

关于此任务

如果管理节点发生故障，则存储在其管理节点数据库中的历史信息将丢失。此数据库包含以下信息：

- 警报历史记录
- 历史属性数据，在节点页面的旧式图表中使用

恢复管理节点时，软件安装过程会在恢复的节点上创建一个空的管理节点数据库。但是，新数据库仅包含当前属于系统或稍后添加的服务器和服务的信息。

如果还原了非主管理节点，则可以通过将管理节点数据库从主管理节点（*source Admin Node*）复制到恢复的节点来还原历史信息。



复制管理节点数据库可能需要几个小时。在源节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
 - a. 输入以下命令：`ssh admin@grid_node_IP`
 - b. 输入 `Passwords.txt` 文件中列出的密码。
 - c. 输入以下命令切换到 root：`su -`
 - d. 输入 `Passwords.txt` 文件中列出的密码。
2. 从源管理节点运行以下命令。然后，在出现提示时输入配置密码。`recover-access-points`
3. 从源管理节点停止 MI 服务：`service mi stop`
4. 从源管理节点，停止管理应用程序接口 (mgmt-api) 服务：`service mgmt-api stop`
5. 在恢复的管理节点上完成以下步骤：
 - a. 登录到已恢复的管理节点：
 - i. 输入以下命令：`ssh admin@grid_node_IP`
 - ii. 输入 `Passwords.txt` 文件中列出的密码。
 - iii. 输入以下命令切换到 root：`su -`
 - iv. 输入 `Passwords.txt` 文件中列出的密码。
 - b. 停止 MI 服务：`service mi stop`
 - c. 停止 mgmt-api 服务：`service mgmt-api stop`
 - d. 将 SSH 私钥添加到 SSH 代理。输入：`ssh-add`
 - e. 输入 `Passwords.txt` 文件中列出的 SSH 访问密码。
 - f. 将数据库从源管理节点复制到恢复的管理节点：`/usr/local/mi/bin/mi-clone-db.sh`

Source_Admin_Node_IP

g. 出现提示时，请确认您要覆盖已恢复的管理节点上的 MI 数据库。

数据库及其历史数据将复制到已恢复的管理节点。复制操作完成后，脚本将启动已恢复的管理节点。

h. 当您不再需要免密码访问其他服务器时，请从 SSH 代理中删除私钥。输入：`ssh-add -D`

6. 重新启动源 Admin Node 上的服务：`service servermanager start`

恢复非主 **StorageGRID** 管理节点时还原 **Prometheus** 指标

或者，您可以保留出现故障的非主管理节点上由 Prometheus 维护的历史指标。

开始之前

- 已安装且正在运行已恢复的管理节点。
- StorageGRID 系统至少包括两个管理节点。
- 您拥有 `Passwords.txt` 文件。
- 您有配置密码短语。

关于此任务

如果管理节点发生故障，则管理节点上 Prometheus 数据库中维护的指标将丢失。当您恢复管理节点时，软件安装过程将创建一个新的 Prometheus 数据库。恢复的管理节点启动后，它会记录指标，就像您执行了 StorageGRID 系统的新安装一样。

如果恢复了非主管理节点，则可以通过将 Prometheus 数据库从主管理节点（*source Admin Node*）复制到恢复的管理节点来恢复历史指标。



复制 Prometheus 数据库可能需要一个小时或更长时间。在源管理节点上停止服务时，某些 Grid Manager 功能将不可用。

步骤

1. 登录到源管理节点：
 - a. 输入以下命令：`ssh admin@grid_node_IP`
 - b. 输入 `'Passwords.txt'` 文件中列出的密码。
 - c. 输入以下命令切换到 root：`su -`
 - d. 输入 `'Passwords.txt'` 文件中列出的密码。
2. 从源管理节点停止 Prometheus 服务：`service prometheus stop`
3. 在恢复的管理节点上完成以下步骤：
 - a. 登录到已恢复的管理节点：
 - i. 输入以下命令：`ssh admin@grid_node_IP`
 - ii. 输入 `'Passwords.txt'` 文件中列出的密码。
 - iii. 输入以下命令切换到 root：`su -`

- iv. 输入 `Passwords.txt` 文件中列出的密码。
- b. 停止 Prometheus 服务: `service prometheus stop`
- c. 将 SSH 私钥添加到 SSH 代理。输入: `ssh-add`
- d. 输入 `Passwords.txt` 文件中列出的 SSH 访问密码。
- e. 将 Prometheus 数据库从源管理节点复制到恢复的管理节点:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. 出现提示时, 请按 **Enter** 确认您要销毁已恢复管理节点上的新 Prometheus 数据库。

原始 Prometheus 数据库及其历史数据将复制到恢复的管理节点。复制操作完成后, 脚本将启动恢复的管理节点。此时将显示以下状态:

数据库已克隆, 正在启动服务

- a. 当您不再需要免密码访问其他服务器时, 请从 SSH 代理中删除私钥。输入: `ssh-add -D`
4. 在源 Admin Node 上重新启动 Prometheus 服务.`service prometheus start`

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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