



# 从非主管理节点故障中恢复

## StorageGRID 11.8

NetApp  
March 19, 2024

# 目录

从非主管理节点故障中恢复 .....	1
从非主管理节点故障中恢复：概述 .....	1
从出现故障的非主管理节点复制审核日志 .....	1
更换非主管理节点 .....	2
选择 Start Recovery 以配置非主管理节点 .....	2
在已恢复的非主管理节点上还原审核日志 .....	4
恢复非主管理节点时还原管理节点数据库 .....	5
恢复非主管理节点时还原 Prometheus 指标 .....	6

# 从非主管理节点故障中恢复

## 从非主管理节点故障中恢复：概述

要从非主管理节点故障中恢复，您必须完成以下任务。一个管理节点托管配置管理节点（CMN）服务，称为主管理节点。尽管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。

## 从出现故障的非主管理节点复制审核日志

如果您能够从出现故障的管理节点复制审核日志，则应保留这些日志以维护网格中的系统活动和使用情况记录。您可以在恢复的非主管理节点启动并运行后将保留的审核日志还原到该节点。

此操作步骤 会将审核日志文件从故障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代管理节点。审核日志不会自动复制到新的管理节点。

根据故障类型，您可能无法从发生故障的管理节点复制审核日志。如果部署只有一个管理节点，则恢复的管理节点将开始在新的空文件中将事件记录到审核日志中，并且先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。



如果现在无法在故障管理节点上访问审核日志、您可以稍后访问这些日志、例如、在主机恢复之后。

1. 如果可能，请登录到出现故障的管理节点。否则，请登录到主管理节点或其他管理节点（如果有）。

- a. 输入以下命令：`ssh admin@grid_node_IP`
- b. 输入中列出的密码 `Passwords.txt` 文件
- c. 输入以下命令切换到root：`su -`
- d. 输入中列出的密码 `Passwords.txt` 文件

以root用户身份登录后、提示符将从变为 `$` to `#`。

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/log
```

4. 将源audit.log文件重命名为唯一编号的文件名。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`

## 更换非主管理节点

要恢复非主管理节点，必须首先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 VMware 上运行的非主管理节点或 Linux 主机替换为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代平台匹配的操作步骤。完成节点更换操作步骤（适用于所有节点类型）后，该操作步骤将指导您执行非主管理节点恢复的下一步。

更换平台	操作步骤
VMware	<a href="#">"更换 VMware 节点"</a>
Linux	<a href="#">"更换 Linux 节点"</a>
SG100 和 SG1000 服务设备	<a href="#">"更换服务设备"</a>
OpenStack	恢复操作不再支持 NetApp 为 OpenStack 提供的虚拟机磁盘文件和脚本。如果您需要恢复在 OpenStack 部署中运行的节点，请下载适用于 Linux 操作系统的文件。然后、按照的操作步骤 进行操作 <a href="#">"更换Linux节点"</a> 。

## 选择 Start Recovery 以配置非主管理节点

更换非主管理节点后，您必须在网络管理器中选择启动恢复，以将新节点配置为故障节点的替代节点。

开始之前

- 您将使用登录到网络管理器 ["支持的 Web 浏览器"](#)。
- 您拥有 ["维护或root访问权限"](#)。
- 您具有配置密码短语。
- 您已部署并配置替代节点。

## 步骤

1. 在网格管理器中，选择 \* 维护 \* > \* 任务 \* > \* 恢复 \*。
2. 在 Pending Nodes 列表中选择要恢复的网格节点。

节点发生故障后会显示在列表中、但您无法选择某个节点、直到它重新安装并准备好进行恢复为止。

3. 输入 \* 配置密码短语 \*。
4. 单击 \* 启动恢复 \*。

### Recovery

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

#### Pending Nodes

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。



在恢复操作步骤 运行期间，您可以单击 \* 重置 \* 以启动新的恢复。此时将显示一个对话框、指示如果重置操作步骤、节点将处于不明确状态。

### Info

#### 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

如果要在重置操作步骤 后重试恢复，必须将节点还原到预安装状态，如下所示：

- \* VMware \*：删除已部署的虚拟网络节点。然后，当您准备好重新启动恢复时，重新部署节点。
  - \* Linux \*：在Linux主机上运行此命令以重新启动节点：`storagegrid node force-recovery node-name`
  - 设备：如果要在重置操作步骤 后重试恢复、必须运行将设备节点还原到预安装状态 `sgareinstall` 在节点上。请参见 ["准备要重新安装的设备（仅限平台更换）"](#)。
6. 如果为 StorageGRID 系统启用了单点登录（SSO），并且已恢复的管理节点的依赖方信任已配置为使用默认管理接口证书，请在 Active Directory 联合身份验证服务（AD FS）中更新（或删除并重新创建）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、请参见 ["配置单点登录"](#)。要访问默认服务器证书，请登录到管理节点的命令 Shell。转至 `/var/local/mgmt-api` 目录、然后选择 `server.crt` 文件

## 在已恢复的非主管理节点上还原审核日志

如果您能够保留故障非主管理节点中的审核日志，以便保留历史审核日志信息，则可以将其复制到要恢复的非主管理节点。

### 开始之前

- 已恢复的管理节点已安装并正在运行。
- 在原始管理节点出现故障后、您已将审核日志复制到其他位置。

### 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。可以通过从出现故障的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来防止数据丢失。根据故障情况，可能无法从发生故障的管理节点复制审核日志。在这种情况下，如果部署具有多个管理节点，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、并且无法从故障节点复制审核日志、则恢复的管理节点会开始将事件记录到审核日志中、就像安装是新的样子。

您必须尽快恢复管理节点，才能还原日志记录功能。

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



- 您配置了外部系统日志服务器，审核日志现在将发送到系统日志服务器，而不是管理节点。
- 您明确指定仅应将审核消息保存在生成这些消息的本地节点上。

请参见 ["配置审核消息和日志目标"](#) 了解详细信息。

### 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. 输入中列出的密码 Passwords.txt 文件

c. 输入以下命令切换到root: `su -`

d. 输入中列出的密码 Passwords.txt 文件

以root用户身份登录后、提示符将从变为 `$` to `#`。

2. 检查已保留哪些审核文件:

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

3. 将保留的审核日志文件复制到已恢复的管理节点:

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

出现提示时, 输入 admin 的密码。

4. 为了安全起见, 请在验证审核日志是否已成功复制到已恢复的管理节点后, 从出现故障的网格节点中删除这些审核日志。

5. 更新已恢复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`

您还必须还原对审核共享的任何已有客户端访问。有关详细信息, 请参见 "[配置审核客户端访问](#)"。

## 恢复非主管理节点时还原管理节点数据库

如果要在出现故障的非主管理节点上保留有关属性, 警报和警报的历史信息, 则可以从主管理节点还原管理节点数据库。

开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您拥有 Passwords.txt 文件
- 您具有配置密码短语。

关于此任务

如果管理节点出现故障, 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
- 警报历史记录
- 历史属性数据, 用于 \* 支持 \* > \* 工具 \* > \* 网格拓扑 \* 页面上的图表和文本报告。

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一部分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小时的时间。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. 输入中列出的密码 `Passwords.txt` 文件
  - c. 输入以下命令切换到root：`su -`
  - d. 输入中列出的密码 `Passwords.txt` 文件
2. 从源管理节点运行以下命令。然后，根据提示输入配置密码短语。`recover-access-points`
3. 从源管理节点中、停止MI服务：`service mi stop`
4. 从源管理节点中、停止管理应用程序程序接口(Management Application Program Interface、mgmt-API)服务：`service mgmt-api stop`
5. 在已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. 输入中列出的密码 `Passwords.txt` 文件
    - iii. 输入以下命令切换到root：`su -`
    - iv. 输入中列出的密码 `Passwords.txt` 文件
  - b. 停止MI服务：`service mi stop`
  - c. 停止mgmt-API服务：`service mgmt-api stop`
  - d. 将 SSH 专用密钥添加到 SSH 代理。输入 `...ssh-add`
  - e. 输入中列出的SSH访问密码 `Passwords.txt` 文件
  - f. 将数据库从源管理节点复制到已恢复的管理节点：`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
  - g. 出现提示时，确认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。完成复制操作后，此脚本将启动已恢复的管理节点。
  - h. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入 `...ssh-add -D`
6. 在源管理节点上重新启动服务：`service servermanager start`

## 恢复非主管理节点时还原 Prometheus 指标

您也可以在出现故障的非主管理节点上保留 Prometheus 维护的历史指标。



## 开始之前

- 已恢复的管理节点已安装并正在运行。
- StorageGRID 系统至少包含两个管理节点。
- 您拥有 Passwords.txt 文件
- 您具有配置密码短语。

## 关于此任务

如果管理节点出现故障，则在管理节点上的 Prometheus 数据库中维护的指标将丢失。恢复管理节点后，软件安装过程将创建一个新的 Prometheus 数据库。在启动已恢复的管理节点后，它会将指标记录为您已执行 StorageGRID 系统的新安装。

如果还原了非主管理节点，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还原历史指标。



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. 输入中列出的密码 Passwords.txt 文件
  - c. 输入以下命令切换到root：`su -`
  - d. 输入中列出的密码 Passwords.txt 文件
2. 从源管理节点中、停止Prometheus服务：`service prometheus stop`
3. 在已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. 输入中列出的密码 Passwords.txt 文件
    - iii. 输入以下命令切换到root：`su -`
    - iv. 输入中列出的密码 Passwords.txt 文件
  - b. 停止Prometheus服务：`service prometheus stop`
  - c. 将 SSH 专用密钥添加到 SSH 代理。输入 `...ssh-add`
  - d. 输入中列出的SSH访问密码 Passwords.txt 文件
  - e. 将Prometheus数据库从源管理节点复制到已恢复的管理节点：  
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
  - f. 出现提示时，按 \* 输入 \* 确认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已恢复的管理节点。完成复制操作后，此脚本将启动已恢复的管理节点。此时将显示以下状态：

已克隆数据库，正在启动服务

a. 如果不再需要对其他服务器进行无密码访问，请从 SSH 代理中删除私钥。输入 `ssh-add -D`

4. 在源管理节点上重新启动Prometheus服务。`service prometheus start`

## 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。