从主管理节点故障中恢复

StorageGRID 11.8

NetApp
March 19, 2024

目录

从主管理节点故障中恢复

从主管理节点故障中恢复：概述

要从主管理节点故障中恢复，您必须完成一组特定的任务。主管理节点托管网格的配置管理节点（ CMN ）服务。

应立即更换发生故障的主管理节点。主管理节点上的配置管理节点（ CMN ）服务负责为网格发出对象标识符块。这些标识符将在载入对象时分配给对象。除非存在可用标识符、否则无法加载新对象。由于网格中缓存了大约一个月的标识符，因此在 CMN 不可用时，对象载入可以继续。但是，在缓存的标识符用尽后，无法添加任何新对象。

> 您必须在大约一个月内修复或更换发生故障的主管理节点，否则网格可能无法载入新对象。确切的时间段取决于对象载入率：如果您需要更准确地评估网格的时间范围，请联系技术支持。

从发生故障的主管理节点复制审核日志

如果您能够从出现故障的主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。

关于此任务

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。

步骤

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. 重命名源 `audit.log` 文件的唯一编号文件名。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`

更换主管理节点

要恢复主管理节点，必须先更换物理或虚拟硬件。

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

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 将引导您进入主管理节点恢复的下一步。

更换平台	操作步骤
VMware	"更换 VMware 节点"
Linux	"更换 Linux 节点"
SG100 和 SG1000 服务设备	"更换服务设备"
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 "更换Linux节点"。

配置替代主管理节点

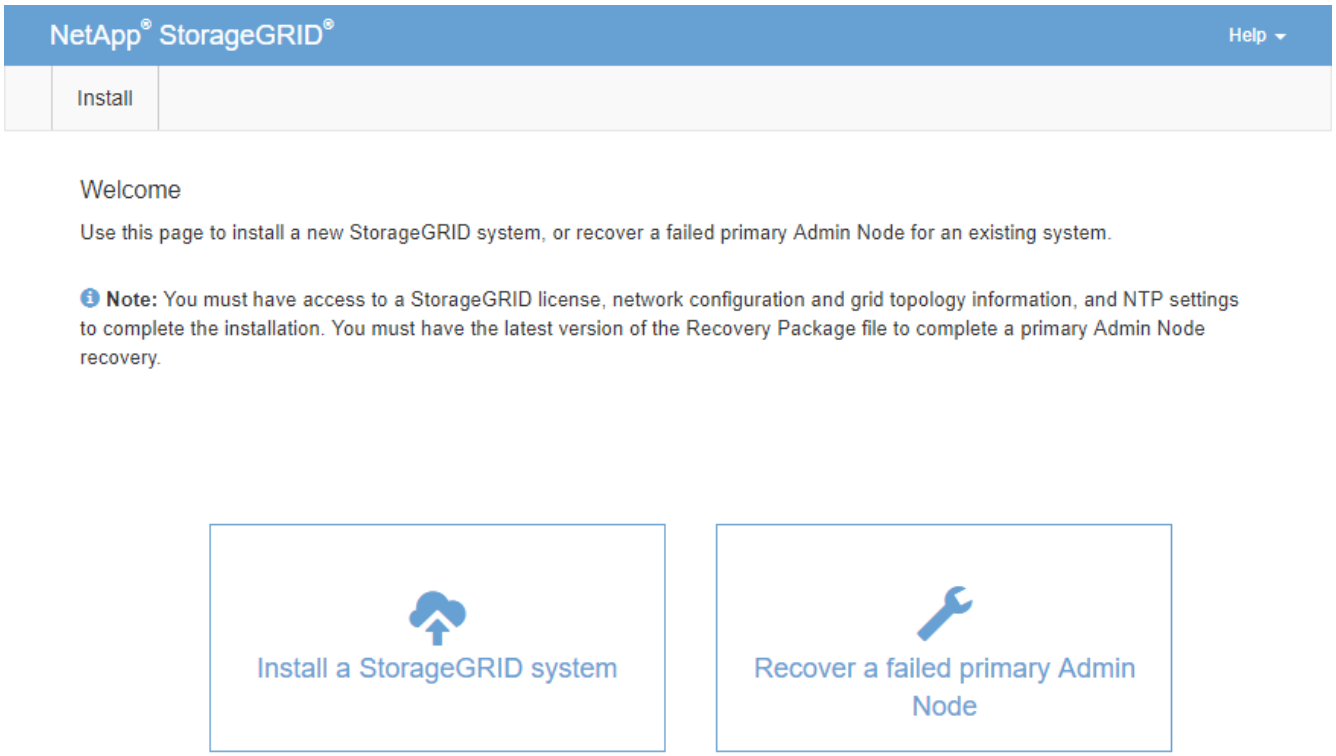
必须将替代节点配置为 StorageGRID 系统的主管理节点。

开始之前

- 对于虚拟机上托管的主管理节点、虚拟机已部署、启动并初始化。
- 对于服务设备上托管的主管理节点，您已更换此设备并安装了软件。请参见 "设备安装说明"。
- 您拥有恢复软件包文件的最新备份 (`sgws-recovery-package-id-revision.zip`) 。
- 您具有配置密码短语。

步骤

1. 打开Web浏览器并导航到 `https://primary_admin_node_ip`。



2. 单击 * 恢复发生故障的主管理节点 * 。
3. 上传恢复包的最新备份：
   a. 单击 * 浏览 * 。
   b. 找到 StorageGRID 系统的最新恢复软件包文件，然后单击 * 打开 * 。
4. 输入配置密码短语。
5. 单击 * 启动恢复 * 。

   恢复过程开始。随着所需服务的启动，网格管理器可能会在几分钟内不可用。恢复完成后，将显示登录页面。

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

7. 确定是否需要应用修补程序。
   a. 使用登录到网格管理器 "支持的 Web 浏览器"。
   b. 选择 * 节点 * 。
   c. 从左侧列表中，选择主管理节点。
   d. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。
   e. 选择任何其他网格节点。
   f. 在概述选项卡上，记下 * 软件版本 * 字段中显示的版本。
      - 如果“软件版本”字段中显示的版本相同，则不需要应用修补程序。
      - 如果“软件版本”字段中显示的版本不同，则必须执行此操作 "应用修补程序" 将已恢复的主管理节点更新到相同版本。

在已恢复的主管理节点上还原审核日志

如果能够保留故障主管理节点中的审核日志，则可以将其复制到要恢复的主管理节点。

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、就像安装是新的一样。

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"。

恢复主管理节点时还原管理节点数据库

如果要在出现故障的主管理节点上保留有关属性，警报和警报的历史信息，则可以还原管理节点数据库。只有当 StorageGRID 系统包含另一个管理节点时，才能还原此数据库。

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。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将管理节点数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史信息。如果您的系统只有一个主管理节点、则无法还原管理节点数据库。

复制管理节点数据库可能需要几小时的时间。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MI服务： `service mi stop`
3. 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`
4. 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`
5. 在源管理节点上重新启动服务： `service servermanager start`

恢复主管理节点时还原 **Prometheus** 指标

或者，您也可以在出现故障的主管理节点上保留 Prometheus 维护的历史指标。只有当您的 StorageGRID 系统包含另一个管理节点时，才能还原 Prometheus 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。

如果您还原了主管理节点，并且 StorageGRID 系统具有另一个管理节点，则可以通过将 Prometheus 数据库从非主管理节点（ _source 管理节点 _ ）复制到已恢复的主管理节点来还原历史指标。如果您的系统只有一个主管理节点、则无法还原Prometheus数据库。

> 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`