



Recuperação de falhas não primárias no nó de administração

StorageGRID

NetApp
March 12, 2025

Índice

Recuperação de falhas não primárias no nó de administração	1
Recuperar de falhas não primárias no Admin Node: Visão geral	1
Copiar registos de auditoria do nó de administração não primário com falha	1
Substitua o nó de administração não primário	2
Selecione Iniciar recuperação para configurar o nó de administração não primário	3
Restaure o log de auditoria no nó de administração não primário recuperado	5
Restaure o banco de dados Admin Node ao recuperar o nó Admin não primário	6
Restaure as métricas do Prometheus ao recuperar o nó de administração não primário	8

Recuperação de falhas não primárias no nó de administração

Recuperar de falhas não primárias no Admin Node: Visão geral

Você deve concluir as tarefas a seguir para se recuperar de uma falha não primária do Admin Node. Um nó de administração hospeda o serviço CMN (Configuration Management Node) e é conhecido como nó de administração principal. Embora você possa ter vários nós de administração, cada sistema StorageGRID inclui apenas um nó de administração principal. Todos os outros nós de administração são nós de administração não primários.

Copiar registros de auditoria do nó de administração não primário com falha

Se você conseguir copiar logs de auditoria do nó de administração com falha, você deve preservá-los para manter o Registro da grade de atividade e uso do sistema. Você pode restaurar os logs de auditoria preservados para o nó de administração não primário recuperado depois que ele estiver ativo e em execução.

Este procedimento copia os arquivos de log de auditoria do nó de administração com falha para um local temporário em um nó de grade separado. Esses logs de auditoria preservados podem então ser copiados para o nó de administração de substituição. Os logs de auditoria não são copiados automaticamente para o novo nó de administração.

Dependendo do tipo de falha, talvez você não consiga copiar logs de auditoria de um nó de administrador com falha. Se a implantação tiver apenas um Admin Node, o Admin Node recuperado inicia a gravação de eventos para o log de auditoria em um novo arquivo vazio e os dados gravados anteriormente são perdidos. Se a implantação incluir mais de um nó Admin, você poderá recuperar os logs de auditoria de outro nó Admin.



Se os logs de auditoria não estiverem acessíveis no nó Admin com falha agora, você poderá acessá-los mais tarde, por exemplo, após a recuperação do host.

1. Inicie sessão no nó de administração com falha, se possível. Caso contrário, faça login no nó de administração principal ou em outro nó de administração, se disponível.
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Pare o serviço AMS para impedir que ele crie um novo arquivo de log: `service ams stop`

3. Navegue até o diretório de exportação de auditoria:

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

4. Renomeie o arquivo `audit.log` de origem para um nome de arquivo numerado exclusivo. Por exemplo, renomeie o arquivo `audit.log` para `2023-10-25.txt.1`.

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

5. Reinicie o serviço AMS: `service ams start`

6. Crie o diretório para copiar todos os arquivos de log de auditoria para um local temporário em um nó de grade separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando solicitado, insira a senha para admin.

7. Copie todos os arquivos de log de auditoria para o local temporário: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando solicitado, insira a senha para admin.

8. Faça logout como root: `exit`

Substitua o nó de administração não primário

Para recuperar um nó de administração não primário, primeiro você deve substituir o hardware físico ou virtual.

Você pode substituir um nó de administrador não primário com falha por um nó de administrador não primário executado na mesma plataforma ou substituir um nó de administrador não primário em execução em VMware ou em um host Linux por um nó de administrador não primário hospedado em um dispositivo de serviços.

Use o procedimento que corresponde à plataforma de substituição selecionada para o nó. Depois de concluir o procedimento de substituição do nó (que é adequado para todos os tipos de nó), esse procedimento irá direcioná-lo para a próxima etapa para a recuperação do nó de administração não primário.

Plataforma de substituição	Procedimento
VMware	"Substitua um nó VMware"
Linux	"Substitua um nó Linux"
Aparelhos de serviços	"Substitua um dispositivo de serviços"

Plataforma de substituição	Procedimento
OpenStack	Os arquivos e scripts de disco de máquina virtual fornecidos pela NetApp para OpenStack não são mais compatíveis com operações de recuperação. Se você precisar recuperar um nó em execução em uma implantação OpenStack, baixe os arquivos para seu sistema operacional Linux. Em seguida, siga o procedimento para "Substituindo um nó Linux" .

Selecione Iniciar recuperação para configurar o nó de administração não primário

Depois de substituir um nó Admin não primário, você deve selecionar Iniciar recuperação no Gerenciador de Grade para configurar o novo nó como um substituto para o nó com falha.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador da web suportado"](#).
- Você tem o ["Permissão de manutenção ou acesso root"](#).
- Você tem a senha de provisionamento.
- Você implantou e configurou o nó de substituição.

Passos

1. No Gerenciador de Grade, selecione **MAINTENANCE > Tasks > Recovery**.
2. Selecione o nó de grade que você deseja recuperar na lista de nós pendentes.

Os nós aparecem na lista depois que eles falham, mas você não pode selecionar um nó até que ele seja reinstalado e esteja pronto para recuperação.

3. Introduza a **frase-passe de provisionamento**.
4. Clique em **Iniciar recuperação**.

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. Monitore o progresso da recuperação na tabela Recovering Grid Node (Recovering Grid Node).



Enquanto o procedimento de recuperação estiver em execução, você pode clicar em **Reset** para iniciar uma nova recuperação. Uma caixa de diálogo é exibida, indicando que o nó será deixado em um estado indeterminado se você redefinir o procedimento.

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

Se pretender tentar novamente a recuperação após reiniciar o procedimento, tem de restaurar o nó para um estado pré-instalado, da seguinte forma:

- **VMware:** Exclua o nó de grade virtual implantado. Em seguida, quando estiver pronto para reiniciar a recuperação, reimplante o nó.
- *** Linux*:** Reinicie o nó executando este comando no host Linux: `storagegrid node force-recovery node-name`
- **Appliance:** Se você quiser repetir a recuperação após redefinir o procedimento, você deve restaurar o nó do dispositivo para um estado pré-instalado executando `sgareinstall` no nó. ["Prepare o aparelho para reinstalação \(apenas substituição da plataforma\)"](#) Consulte .

6. Se o logon único (SSO) estiver ativado para o seu sistema StorageGRID e a confiança da parte confiável para o nó Admin que você recuperou foi configurada para usar o certificado de interface de gerenciamento padrão, atualizar (ou excluir e recriar) a confiança da parte confiável do nó nos Serviços de Federação do ative Directory (AD FS). Use o novo certificado de servidor padrão que foi gerado durante o processo de recuperação do Admin Node.



Para configurar uma confiança de parte confiável, "[Configurar o logon único](#)" consulte . Para acessar o certificado padrão do servidor, faça login no shell de comando do nó Admin. Vá para `/var/local/mgmt-api` o diretório e selecione o `server.crt` arquivo.

Restaure o log de auditoria no nó de administração não primário recuperado

Se você conseguiu preservar o log de auditoria do nó de administração não primário com falha, de modo que as informações de log de auditoria histórica sejam mantidas, você pode copiá-lo para o nó de administração não primário que você está recuperando.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- Você copiou os logs de auditoria para outro local depois que o nó Admin original falhou.

Sobre esta tarefa

Se um nó Admin falhar, os logs de auditoria salvos nesse nó Admin são potencialmente perdidos. Pode ser possível preservar dados de perda copiando logs de auditoria do nó de administração com falha e restaurando esses logs de auditoria para o nó de administração recuperado. Dependendo da falha, talvez não seja possível copiar logs de auditoria do nó de administração com falha. Nesse caso, se a implantação tiver mais de um nó Admin, você poderá recuperar logs de auditoria de outro nó Admin à medida que os logs de auditoria são replicados para todos os nós Admin.

Se houver apenas um nó Admin e o log de auditoria não puder ser copiado do nó com falha, o nó Admin recuperado inicia a gravação de eventos para o log de auditoria como se a instalação fosse nova.

Você deve recuperar um nó Admin o mais rápido possível para restaurar a funcionalidade de log.

Por padrão, as informações de auditoria são enviadas para o log de auditoria nos nós de administração. Você pode ignorar estas etapas se qualquer uma das seguintes situações se aplicar:



- Você configurou um servidor syslog externo e os logs de auditoria agora estão sendo enviados para o servidor syslog em vez de para nós de administrador.
- Você especificou explicitamente que as mensagens de auditoria devem ser salvas somente nos nós locais que as geraram.

"[Configurar mensagens de auditoria e destinos de log](#)" Consulte para obter detalhes.

Passos

1. Faça login no nó de administração recuperado:
 - a. Digite o seguinte comando `ssh admin@recovery_Admin_Node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Depois de iniciar sessão como root, o aviso muda de `$` para `#`.

2. Verifique quais arquivos de auditoria foram preservados:

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

3. Copie os arquivos de log de auditoria preservados para o Admin Node recuperado:

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

Quando solicitado, insira a senha para admin.

4. Para segurança, exclua os logs de auditoria do nó de grade com falha depois de verificar se eles foram copiados com sucesso para o nó de administração recuperado.

5. Atualize as configurações de usuário e grupo dos arquivos de log de auditoria no Admin Node recuperado:

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

6. Faça logout como root: `exit`

Você também deve restaurar qualquer acesso de cliente pré-existente ao compartilhamento de auditoria. Para obter mais informações, "[Configurar acesso de cliente de auditoria](#)" consulte .

Restaure o banco de dados Admin Node ao recuperar o nó Admin não primário

Se você quiser manter as informações históricas sobre atributos, alarmes e alertas em um nó de administração não primário que falhou, você pode restaurar o banco de dados do nó de administração do nó principal.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Se um nó Admin falhar, as informações históricas armazenadas em seu banco de dados Admin Node serão perdidas. Esta base de dados inclui as seguintes informações:

- Histórico de alertas
- Histórico de alarmes
- Dados de atributos históricos, que são usados nos gráficos e relatórios de texto disponíveis na página **SUPPORT > Tools > Grid topology**.

Quando você recupera um Admin Node, o processo de instalação do software cria um banco de dados Admin Node vazio no nó recuperado. No entanto, o novo banco de dados inclui apenas informações para servidores e serviços que atualmente fazem parte do sistema ou adicionados posteriormente.

Se você restaurou um nó de administração não primário, você poderá restaurar as informações históricas copiando o banco de dados do nó de administração do nó principal (o *nó de administração de origem*) para o nó recuperado.



Copiar o banco de dados Admin Node pode levar várias horas. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no nó de origem.

Passos

1. Faça login no nó de administração de origem:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Execute o seguinte comando a partir do Admin Node de origem. Em seguida, insira a senha de provisionamento, se solicitado. `recover-access-points`
3. No Admin Node de origem, pare o serviço MI: `service mi stop`
4. No Admin Node de origem, pare o serviço Management Application Program Interface (mgmt-api):
`service mgmt-api stop`
5. Execute as seguintes etapas no nó de administração recuperado:
 - a. Faça login no nó de administração recuperado:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Parar o serviço MI: `service mi stop`
 - c. Pare o serviço mgmt-api: `service mgmt-api stop`
 - d. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`
 - e. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
 - f. Copie o banco de dados do Admin Node de origem para o Admin Node recuperado:
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Quando solicitado, confirme se você deseja substituir o banco de dados MI no Admin Node recuperado.

O banco de dados e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado.

- h. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza: `ssh-add -D`

6. Reinicie os serviços no Admin Node de origem: `service servermanager start`

Restaure as métricas do Prometheus ao recuperar o nó de administração não primário

Opcionalmente, você pode manter as métricas históricas mantidas pelo Prometheus em um nó Admin não primário que falhou.

Antes de começar

- O Admin Node recuperado está instalado e em execução.
- O sistema StorageGRID inclui pelo menos dois nós de administração.
- Você tem o `Passwords.txt` arquivo.
- Você tem a senha de provisionamento.

Sobre esta tarefa

Se um nó Admin falhar, as métricas mantidas no banco de dados Prometheus no nó Admin serão perdidas. Quando você recupera o Admin Node, o processo de instalação do software cria um novo banco de dados Prometheus. Depois que o nó de administração recuperado é iniciado, ele registra as métricas como se você tivesse executado uma nova instalação do sistema StorageGRID.

Se você restaurou um nó Admin não primário, você poderá restaurar as métricas históricas copiando o banco de dados Prometheus do nó Admin primário (o *source Admin Node*) para o nó Admin recuperado.



Copiar o banco de dados Prometheus pode levar uma hora ou mais. Alguns recursos do Gerenciador de Grade ficarão indisponíveis enquanto os serviços forem interrompidos no Admin Node de origem.

Passos

1. Faça login no nó de administração de origem:
 - a. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - c. Digite o seguinte comando para mudar para root: `su -`
 - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. No Admin Node de origem, pare o serviço Prometheus: `service prometheus stop`
3. Execute as seguintes etapas no nó de administração recuperado:
 - a. Faça login no nó de administração recuperado:
 - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
 - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Pare o serviço Prometheus: `service prometheus stop`
 - c. Adicione a chave privada SSH ao agente SSH. Introduza: `ssh-add`

- d. Insira a senha de acesso SSH listada no `Passwords.txt` arquivo.
- e. Copie o banco de dados Prometheus do nó Admin de origem para o nó Admin recuperado:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Quando solicitado, pressione **Enter** para confirmar que deseja destruir o novo banco de dados Prometheus no nó Admin recuperado.

O banco de dados Prometheus original e seus dados históricos são copiados para o Admin Node recuperado. Quando a operação de cópia é concluída, o script inicia o nó Admin recuperado. É apresentado o seguinte estado:

Banco de dados clonado, iniciando serviços

- a. Quando você não precisar mais de acesso sem senha a outros servidores, remova a chave privada do agente SSH. Introduza:`ssh-add -D`
4. Reinicie o serviço Prometheus no Admin Node de origem.`service prometheus start`

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.