# Recuperarse de fallas del nodo de administración no principal

StorageGRID software

NetApp
December 03, 2025

# Tabla de contenidos

# Recuperarse de fallas del nodo de administración no principal

## Recuperarse de fallas del nodo de administración no principal

Debe completar las siguientes tareas para recuperarse de una falla del nodo de administración no principal. Un nodo de administración aloja el servicio del nodo de administración de configuración (CMN) y se conoce como el nodo de administración principal. Aunque puede tener varios nodos de administración, cada sistema StorageGRID incluye solo un nodo de administración principal. Todos los demás nodos de administración son nodos de administración no principales.

Siga estos pasos de alto nivel para recuperar un nodo de administración no principal:

1. "Copiar registros de auditoría del nodo de administración no principal que falló"
2. "Reemplazar el nodo de administración no principal"
3. "Seleccione Iniciar recuperación para configurar el nodo de administración no principal"
4. "Restaurar el registro de auditoría en un nodo de administración no principal recuperado"
5. "Restaurar la base de datos del nodo de administración al recuperar un nodo de administración no principal"
6. "Restaurar las métricas de Prometheus al recuperar un nodo de administración no principal"

## Copiar registros de auditoría de un nodo de administración no principal fallido

Si puede copiar los registros de auditoría del nodo de administración fallido, debe conservarlos para mantener el registro de la red sobre la actividad y el uso del sistema. Puede restaurar los registros de auditoría conservados en el nodo de administración no principal recuperado después de que esté en funcionamiento.

Este procedimiento copia los archivos de registro de auditoría del nodo de administración fallido a una ubicación temporal en un nodo de red separado. Estos registros de auditoría conservados se pueden luego copiar al nodo de administración de reemplazo. Los registros de auditoría no se copian automáticamente al nuevo nodo de administración.

Dependiendo del tipo de falla, es posible que no pueda copiar los registros de auditoría de un nodo de administración fallido. Si la implementación solo tiene un nodo de administración, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría en un nuevo archivo vacío y se pierden los datos registrados previamente. Si la implementación incluye más de un nodo de administración, puede recuperar los registros de auditoría de otro nodo de administración.

Si no se puede acceder a los registros de auditoría en el nodo de administración fallido ahora, es posible que pueda acceder a ellos más tarde, por ejemplo, después de la recuperación del host.

1. Si es posible, inicie sesión en el nodo de administración que falló. De lo contrario, inicie sesión en el nodo de administración principal o en otro nodo de administración, si está disponible.

   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   c. Introduzca el siguiente comando para cambiar a root: `su -`

   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Detenga el servicio AMS para evitar que cree un nuevo archivo de registro:`service ams stop`

3. Navegue hasta el directorio de exportación de auditoría:

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

4. Cambie el nombre del archivo audit.log de origen a un nombre de archivo numerado único. Por ejemplo, cambie el nombre del archivo audit.log a `2023-10-25.txt.1` .

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

5. Reiniciar el servicio AMS: `service ams start`

6. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Cuando se le solicite, ingrese la contraseña de administrador.

7. Copie todos los archivos de registro de auditoría a la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Cuando se le solicite, ingrese la contraseña de administrador.

8. Cerrar sesión como root: `exit`

# Reemplazar el nodo de administración no principal

## Para recuperar un nodo de administración no principal, primero debe reemplazar el hardware físico o virtual.

Puede reemplazar un nodo de administración no principal fallido con un nodo de administración no principal que se ejecute en la misma plataforma, o puede reemplazar un nodo de administración no principal que se ejecute en VMware o un host Linux con un nodo de administración no principal alojado en un dispositivo de servicios.

Utilice el procedimiento que coincida con la plataforma de reemplazo que seleccione para el nodo. Después de completar el procedimiento de reemplazo de nodo (que es adecuado para todos los tipos de nodos), ese procedimiento lo dirigirá al siguiente paso para la recuperación del nodo de administración no principal.

| Plataforma de reemplazo | Procedimiento |
| --- | --- |
| VMware | "Reemplazar un nodo de VMware" |
| Linux | "Reemplazar un nodo Linux" |
| Servicios de electrodomésticos | "Reemplazar un dispositivo de servicios" |
| OpenStack | Los archivos de disco de máquina virtual y los scripts proporcionados por NetApp para OpenStack ya no son compatibles con las operaciones de recuperación. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para su sistema operativo Linux. A continuación, siga el procedimiento para"Reemplazar un nodo Linux" . |

# Seleccione Iniciar recuperación para configurar el nodo de administración no principal

Después de reemplazar un nodo de administración no principal, debe seleccionar Iniciar recuperación en el Administrador de red para configurar el nuevo nodo como reemplazo del nodo fallido.

**Antes de empezar**

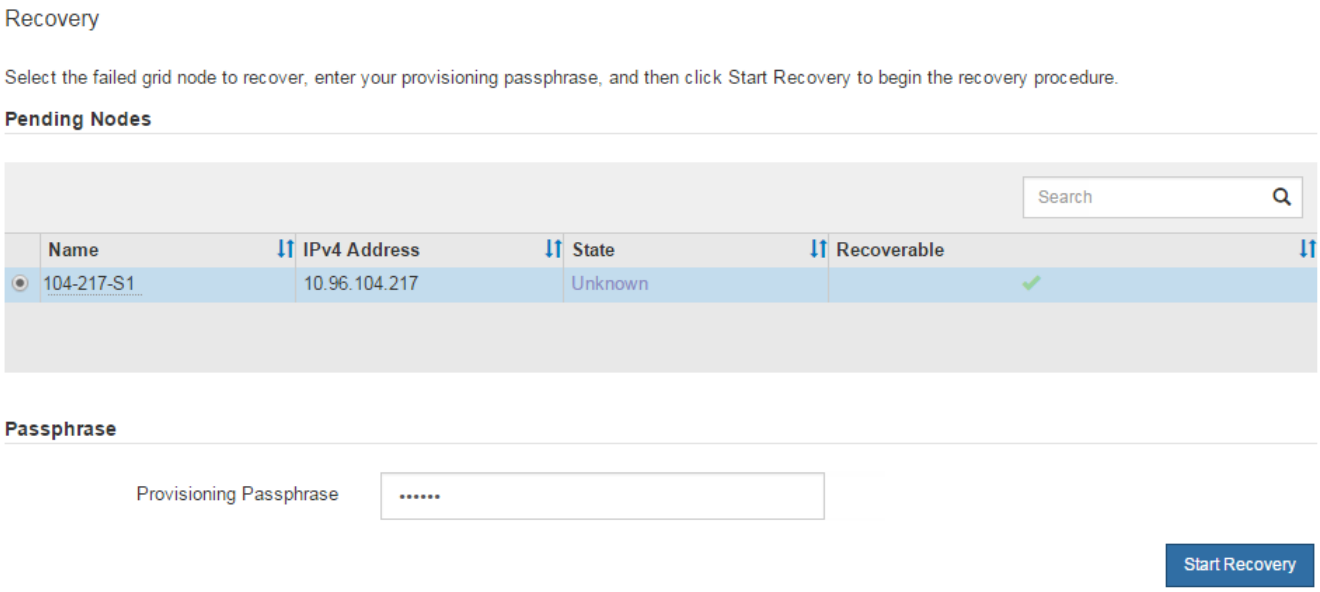
- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de mantenimiento o acceso root" .
- Tienes la contraseña de aprovisionamiento.
- Ha implementado y configurado el nodo de reemplazo.

**Pasos**

1. Desde el Administrador de red, seleccione **MANTENIMIENTO** > **Tareas** > **Recuperación**.
2. Seleccione el nodo de la cuadrícula que desea recuperar en la lista de Nodos pendientes.

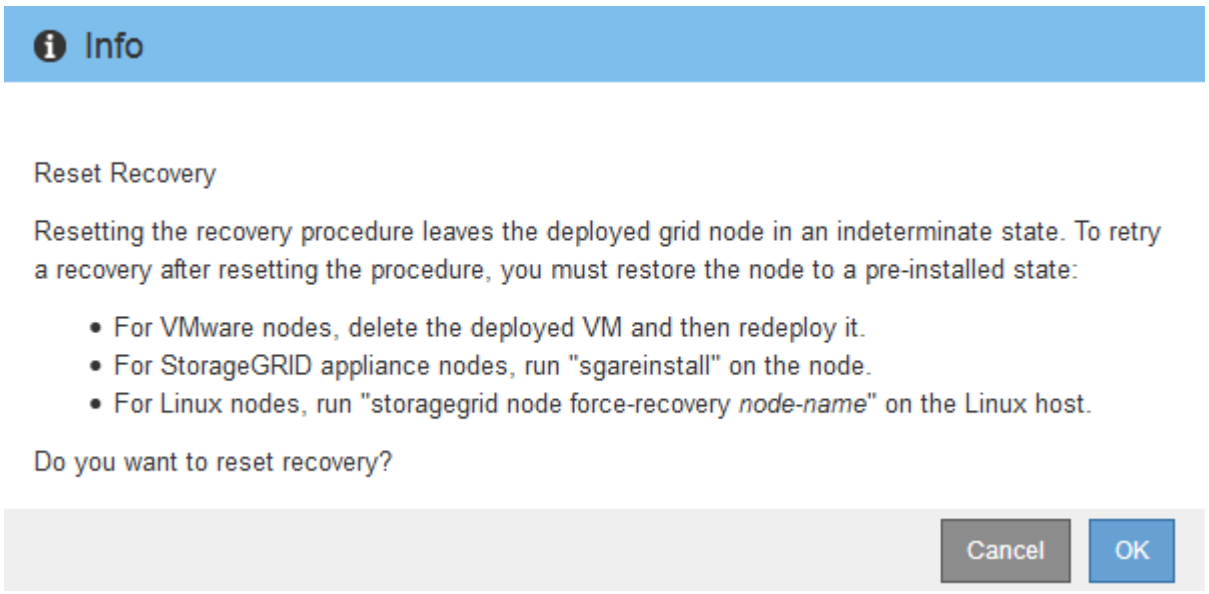
   Los nodos aparecen en la lista después de fallar, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **contraseña de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.




5. Supervise el progreso de la recuperación en la tabla Nodo de cuadrícula en recuperación.

> Mientras se ejecuta el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.




Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la siguiente manera:

- **VMware**: eliminar el nodo de red virtual implementado. Luego, cuando esté listo para reiniciar la recuperación, vuelva a implementar el nodo.
- **Linux**: reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo**: Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo. Ver "Preparar el dispositivo para la reinstalación (solo reemplazo de plataforma)" .

6. Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID y la confianza de usuario autenticado para el nodo de administración que recuperó estaba configurada para usar el certificado de interfaz de administración predeterminado, actualice (o elimine y vuelva a crear) la confianza de usuario autenticado del nodo en los Servicios de federación de Active Directory (AD FS). Utilice el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.

> Para configurar una relación de confianza entre usuarios, consulte"Configurar el inicio de sesión único" . Para acceder al certificado de servidor predeterminado, inicie sesión en el shell de comandos del nodo de administración. Ir a la `/var/local/mgmt-api` directorio y seleccione el `server.crt` archivo.

# Restaurar el registro de auditoría en el nodo de administración no principal recuperado

Si pudo conservar el registro de auditoría del nodo de administración no principal que falló, de modo que se conserve la información histórica del registro de auditoría, puede copiarlo al nodo de administración no principal que está recuperando.

**Antes de empezar**

- El nodo de administración recuperado está instalado y funcionando.
- Ha copiado los registros de auditoría a otra ubicación después de que el nodo de administración original fallara.

**Acerca de esta tarea**

Si un nodo de administración falla, es posible que se pierdan los registros de auditoría guardados en ese nodo de administración. Es posible que sea posible preservar los datos de la pérdida copiando los registros de auditoría del nodo de administración fallido y luego restaurándolos en el nodo de administración recuperado. Dependiendo de la falla, es posible que no sea posible copiar los registros de auditoría del nodo de administración fallido. En ese caso, si la implementación tiene más de un nodo de administración, puede recuperar registros de auditoría de otro nodo de administración, ya que los registros de auditoría se replican en todos los nodos de administración.

Si solo hay un nodo de administración y no se puede copiar el registro de auditoría del nodo fallido, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría como si la instalación fuera nueva.

Debe recuperar un nodo de administración lo antes posible para restaurar la funcionalidad de registro.

> De forma predeterminada, la información de auditoría se envía al registro de auditoría en los nodos de administración. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:
>
> - Configuró un servidor syslog externo y los registros de auditoría ahora se envían al servidor syslog en lugar de a los nodos de administración.
> - Usted especificó explícitamente que los mensajes de auditoría deben guardarse solo en los nodos locales que los generaron.
>
> Ver"Configurar mensajes de auditoría y destinos de registro" Para más detalles.

**Pasos**

1. Inicie sesión en el nodo de administración recuperado:

   a. Introduzca el siguiente comando:
   `ssh admin@recovery_Admin_Node_IP`

   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   c. Introduzca el siguiente comando para cambiar a root: `su -`

   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Después de iniciar sesión como root, el mensaje cambia de `$` a `#` .

2. Compruebe qué archivos de auditoría se han conservado:

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

3. Copie los archivos de registro de auditoría conservados al nodo de administración recuperado:

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

   Cuando se le solicite, ingrese la contraseña de administrador.

4. Por seguridad, elimine los registros de auditoría del nodo de red fallido después de verificar que se hayan copiado correctamente al nodo de administración recuperado.
5. Actualice la configuración de usuario y grupo de los archivos de registro de auditoría en el nodo de administración recuperado:

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

6. Cerrar sesión como root: `exit`

# Restaurar la base de datos del nodo de administración al recuperar un nodo de administración no principal

Si desea conservar la información histórica sobre los atributos y las alertas de un nodo de administración no principal que ha fallado, puede restaurar la base de datos del nodo de administración desde el nodo de administración principal.

**Antes de empezar**

- El nodo de administración recuperado está instalado y funcionando.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

**Acerca de esta tarea**

Si un nodo de administración falla, se pierde la información histórica almacenada en su base de datos. Esta base de datos incluye la siguiente información:

- Historial de alertas

- Datos de atributos históricos, que se utilizan en gráficos de estilo heredado en la página Nodos

Cuando recupera un nodo de administración, el proceso de instalación del software crea una base de datos de nodo de administración vacía en el nodo recuperado. Sin embargo, la nueva base de datos sólo incluye información de los servidores y servicios que actualmente forman parte del sistema o que se agregarán posteriormente.

Si restauró un nodo de administración no principal, puede restaurar la información histórica copiando la base de datos del nodo de administración desde el nodo de administración principal (el *nodo de administración de origen*) al nodo recuperado.

> Copiar la base de datos del nodo de administración puede tardar varias horas. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de origen.

**Pasos**

1. Inicie sesión en el nodo de administración de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
2. Ejecute el siguiente comando desde el nodo de administración de origen. Luego, ingrese la contraseña de aprovisionamiento si se le solicita. `recover-access-points`
3. Desde el nodo de administración de origen, detenga el servicio MI: `service mi stop`
4. Desde el nodo de administración de origen, detenga el servicio de interfaz de programación de aplicaciones de administración (mgmt-api): `service mgmt-api stop`
5. Complete los siguientes pasos en el nodo de administración recuperado:
   a. Inicie sesión en el nodo de administración recuperado:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a root: `su -`
      iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   b. Detener el servicio MI: `service mi stop`
   c. Detener el servicio mgmt-api: `service mgmt-api stop`
   d. Agregue la clave privada SSH al agente SSH. Ingresar:`ssh-add`
   e. Ingrese la contraseña de acceso SSH que aparece en el `Passwords.txt` archivo.
   f. Copie la base de datos del nodo de administración de origen al nodo de administración recuperado: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Cuando se le solicite, confirme que desea sobrescribir la base de datos MI en el nodo de administración recuperado.

      La base de datos y sus datos históricos se copian al nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado.

h. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar:`ssh-add -D`

6. Reinicie los servicios en el nodo de administración de origen: `service servermanager start`

# Restaurar las métricas de Prometheus al recuperar un nodo de administración no principal

Opcionalmente, puede conservar las métricas históricas mantenidas por Prometheus en un nodo de administración no principal que haya fallado.

**Antes de empezar**

- El nodo de administración recuperado está instalado y funcionando.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

**Acerca de esta tarea**

Si un nodo de administración falla, se pierden las métricas mantenidas en la base de datos de Prometheus en el nodo de administración. Cuando recupera el nodo de administración, el proceso de instalación del software crea una nueva base de datos de Prometheus. Una vez iniciado el nodo de administración recuperado, registra las métricas como si hubiera realizado una nueva instalación del sistema StorageGRID .

Si restauró un nodo de administración no principal, puede restaurar las métricas históricas copiando la base de datos de Prometheus desde el nodo de administración principal (el *nodo de administración de origen*) al nodo de administración recuperado.

> Copiar la base de datos de Prometheus podría tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de administración de origen.

**Pasos**

1. Inicie sesión en el nodo de administración de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
2. Desde el nodo de administración de origen, detenga el servicio Prometheus: `service prometheus stop`
3. Complete los siguientes pasos en el nodo de administración recuperado:
   a. Inicie sesión en el nodo de administración recuperado:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a root: `su -`

iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

b. Detener el servicio Prometheus: `service prometheus stop`

c. Agregue la clave privada SSH al agente SSH. Ingresar:`ssh-add`

d. Ingrese la contraseña de acceso SSH que aparece en el `Passwords.txt` archivo.

e. Copie la base de datos de Prometheus del nodo de administración de origen al nodo de administración recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Cuando se le solicite, presione **Enter** para confirmar que desea destruir la nueva base de datos de Prometheus en el nodo de administración recuperado.

   La base de datos original de Prometheus y sus datos históricos se copian al nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado. Aparece el siguiente estado:

Base de datos clonada, iniciando servicios

a. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar:`ssh-add -D`

4. Reinicie el servicio Prometheus en el nodo de administración de origen.`service prometheus start`