Gestione los nodos de administrador

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-118/admin/using-multiple-admin-nodes.html on November 04, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

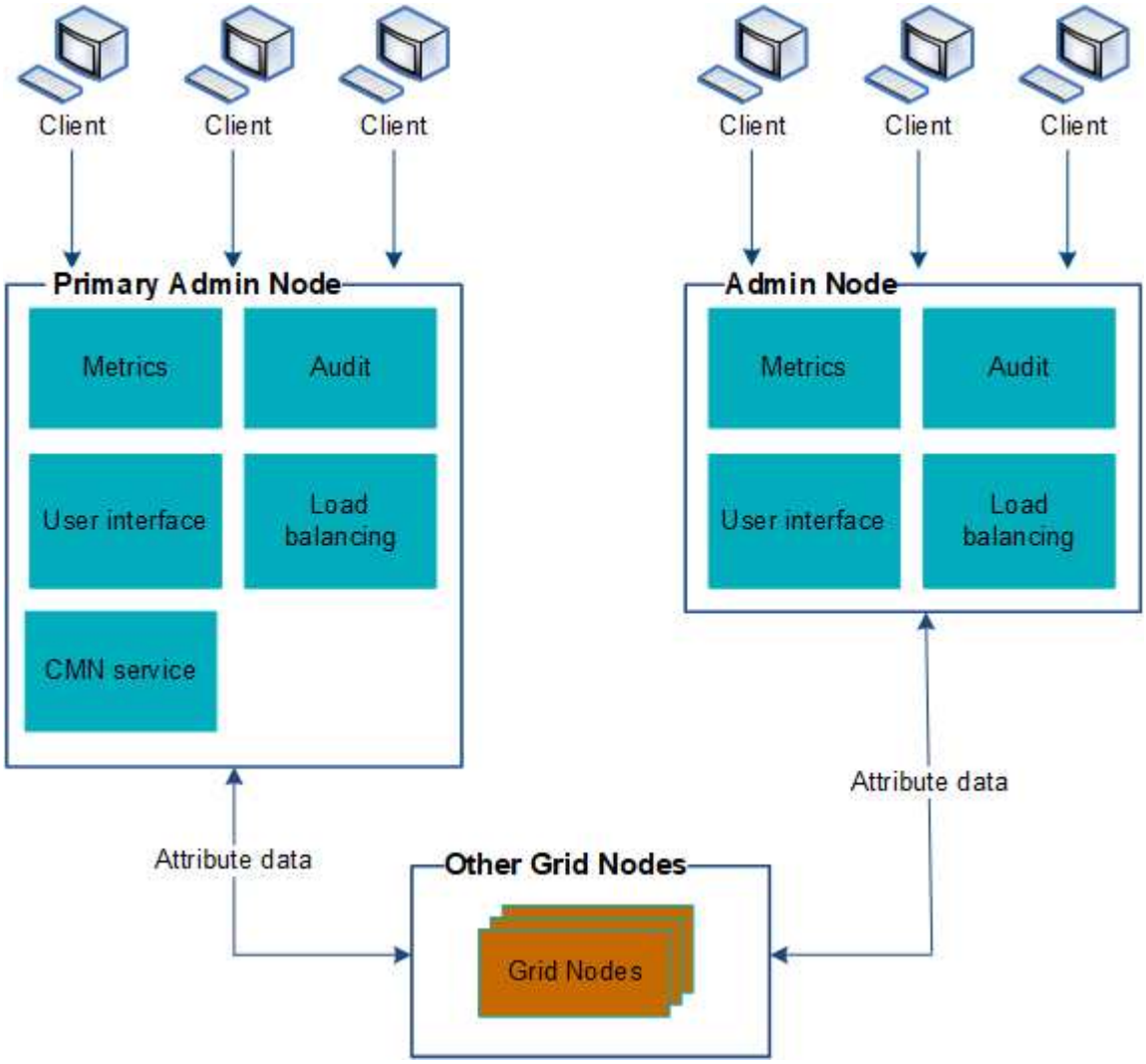
Gestione los nodos de administrador . . . 1
- Use varios nodos de administrador . . . 1
- Identifique el nodo de administración principal . . . 2
- Ver el estado de notificación y las colas . . . 2
- Cómo muestran los nodos de administración alarmas confirmadas (sistema heredado) . . . 3
- Configure el acceso de los clientes de auditoría . . . 4
  - Configure el acceso del cliente de auditoría para NFS . . . 4
  - Agregar un cliente de auditoría NFS a un recurso compartido de auditoría . . . 6
  - Comprobar la integración de auditoría de NFS . . . 8
  - Eliminar un cliente de auditoría NFS del recurso compartido de auditoría . . . 8
  - Cambiar la dirección IP de un cliente de auditoría de NFS . . . 10

Gestione los nodos de administrador

Use varios nodos de administrador

Un sistema StorageGRID puede incluir varios nodos de administrador para permitir supervisar y configurar continuamente el sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, las alertas y las alarmas (sistema heredado) siguen activándose y las notificaciones por correo electrónico y los paquetes de AutoSupport aún se envían. Sin embargo, tener varios nodos de administración no ofrece protección de conmutación al nodo de respaldo, excepto notificaciones y paquetes de AutoSupport. En particular, las confirmaciones de alarma realizadas desde un nodo de administración no se copian en otros nodos de administración.



Si falla un nodo de administración, existen dos opciones para ver y configurar el sistema StorageGRID:

- Los clientes web pueden volver a conectarse a cualquier otro nodo de administrador disponible.
- Si un administrador del sistema ha configurado un grupo de nodos de administración de alta disponibilidad, los clientes web pueden seguir accediendo a Grid Manager o al Gestor de inquilinos

mediante la dirección IP virtual del grupo de alta disponibilidad. Consulte "Gestión de grupos de alta disponibilidad".

> Al utilizar un grupo de alta disponibilidad, el acceso se interrumpe si el nodo de administración activo falla. Los usuarios deben volver a iniciar sesión después de que la dirección IP virtual del grupo ha conmute a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo se pueden realizar con el nodo de administrador principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar completamente.

Identifique el nodo de administración principal

El nodo de administración principal aloja el servicio CMN. Algunos procedimientos de mantenimiento solo se pueden realizar mediante el nodo de administrador principal.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > **Admin Node** y, a continuación, seleccione + Para expandir el árbol de topología y mostrar los servicios alojados en este nodo de administración.

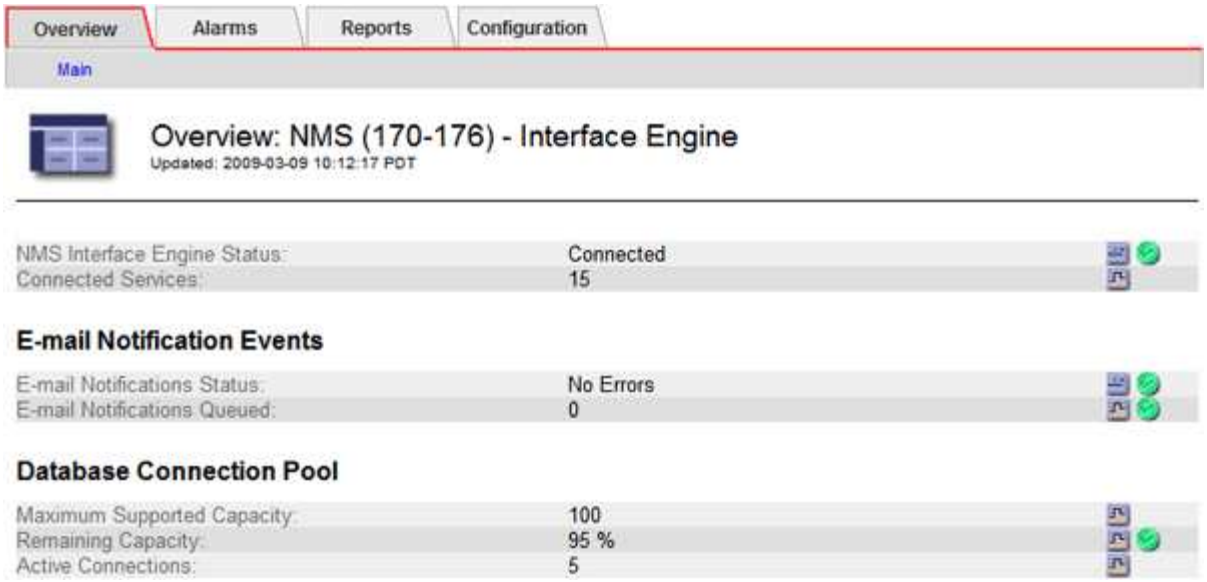
   El nodo de administración principal aloja el servicio CMN.

3. Si este nodo de administrador no aloja el servicio CMN, compruebe los demás nodos de administración.

Ver el estado de notificación y las colas

El servicio del sistema de administración de redes (NMS) en los nodos de administración envía notificaciones al servidor de correo. Puede ver el estado actual del servicio NMS y el tamaño de su cola de notificaciones en la página Motor de interfaz.

Para acceder a la página Motor de interfaz, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. Por último, seleccione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



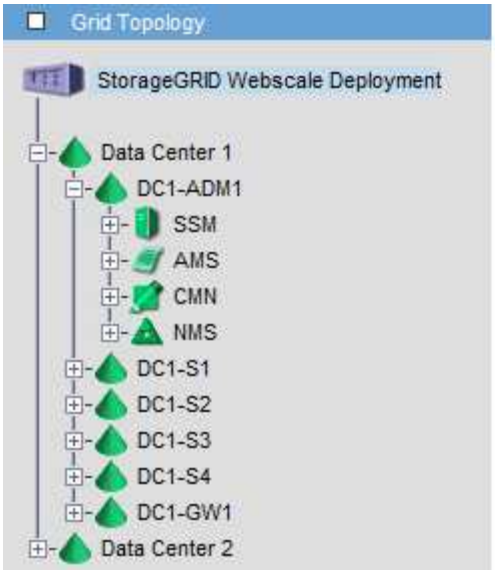
Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la notificación, un intento de mayor esfuerzo de reenviar la notificación al servidor de correo continúa durante un período de 60 segundos. Si la notificación no se envía al servidor de correo después de 60 segundos, la notificación se descarta de la cola de notificaciones y se realiza un intento de enviar la siguiente notificación de la cola.

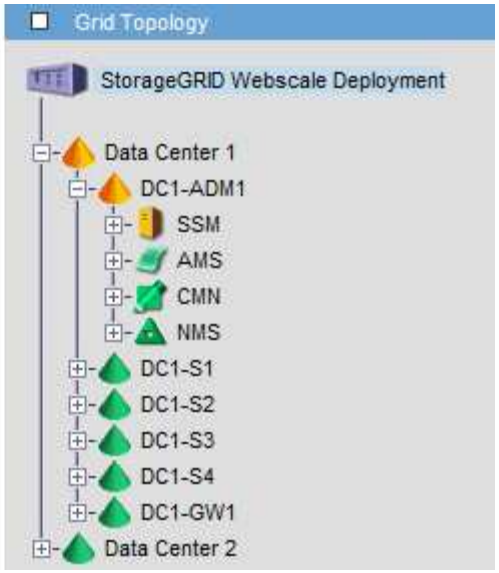
Puesto que las notificaciones se pueden borrar de la cola de notificaciones sin enviarse, es posible que se active una alarma sin que se envíe una notificación. Si se elimina una notificación de la cola sin que se envíe, se activa la alarma secundaria MINS (Estado de notificación de correo electrónico).

Cómo muestran los nodos de administración alarmas confirmadas (sistema heredado)

Cuando reconoce una alarma en un nodo de administración, la alarma confirmada no se copia en ningún otro nodo de administración. Puesto que las confirmaciones no se copian en otros nodos de administración, el árbol de topología de cuadrícula puede no tener el mismo aspecto para cada nodo de administración.

Esta diferencia puede ser útil al conectar clientes Web. Los clientes web pueden tener diferentes vistas del sistema StorageGRID de acuerdo con las necesidades del administrador.





Tenga en cuenta que las notificaciones se envían desde el nodo de administración donde se produce la confirmación.

Configure el acceso de los clientes de auditoría

Configure el acceso del cliente de auditoría para NFS

El nodo Admin, a través del servicio sistema de administración de auditorías (AMS), registra todos los eventos del sistema auditados en un archivo de registro disponible a través del recurso compartido de auditoría, que se agrega a cada nodo Admin en la instalación. El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

La compatibilidad con NFS ha quedado obsoleta y se eliminará en una futura versión.

Para acceder a los registros de auditoría, puede configurar el acceso de clientes a recursos compartidos de auditoría para NFS. O bien, puede hacerlo "usar un servidor de syslog externo".

El sistema StorageGRID utiliza un reconocimiento positivo para evitar la pérdida de mensajes de auditoría antes de que se escriban en el archivo de registro. Un mensaje permanece en cola en un servicio hasta que el servicio AMS o un servicio intermedio de retransmisión de auditoría ha reconocido el control de él. Para obtener más información, consulte "Revisar los registros de auditoría".

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña root/admin.
- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

Acerca de esta tarea

Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

      Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Confirme que todos los servicios tienen el estado en ejecución o verificado. Introduzca: `storagegrid-status`

   Si alguno de los servicios no aparece como en ejecución o verificado, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos. Pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración NFS. Introduzca: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Agregue el cliente de auditoría: `add-audit-share`
   a. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: `client_IP_address`
   b. Cuando se le solicite, pulse **Intro**.
6. Si se permite que más de un cliente de auditoría acceda al recurso compartido de auditoría, agregue la dirección IP del usuario adicional: `add-ip-to-share`
   a. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
   b. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*
   c. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

   d. Repita estos mismos pasos para cada cliente de auditoría adicional que tenga acceso al recurso compartido de auditoría.
7. De manera opcional, compruebe su configuración.
   a. Introduzca lo siguiente: `validate-config`

Los servicios se comprueban y visualizan.

b. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de NFS.

c. Cierre la utilidad de configuración NFS: `exit`

8. Determine si debe habilitar los recursos compartidos de auditoría en otros sitios.
   - Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.
   - Si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite estos recursos compartidos de auditoría según sea necesario:
     i. Inicie sesión de forma remota en el nodo de administración del sitio:
        A. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
        B. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
        C. Introduzca el siguiente comando para cambiar a la raíz: `su -`
        D. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
     ii. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.
     iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota. Introduzca: `exit`
9. Cierre la sesión del shell de comandos: `exit`

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido o elimine un cliente de auditoría existente eliminando su dirección IP.

Agregar un cliente de auditoría NFS a un recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido de auditoría.

La compatibilidad con NFS ha quedado obsoleta y se eliminará en una futura versión.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña de la cuenta root/admin.
- Tiene el `Configuration.txt` Archivo (disponible en el paquete de recuperación).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`

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

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

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

Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Introduzca: `add-ip-to-share`

Se muestra una lista de los recursos compartidos de auditoría de NFS habilitados en el nodo de administración. El recurso compartido de auditoría aparece como: `/var/local/log`

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*

El cliente de auditoría se agrega al recurso compartido de auditoría.

6. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de NFS.

7. Repita los pasos para cada cliente de auditoría que se debe agregar al recurso compartido de auditoría.
8. Si lo desea, compruebe la configuración: `validate-config`

Los servicios se comprueban y visualizan.

a. Cuando se le solicite, pulse **Intro**.

Aparece la utilidad de configuración de NFS.

9. Cierre la utilidad de configuración NFS: `exit`
10. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

De lo contrario, si la implementación de StorageGRID incluye nodos de administración en otros sitios, opcionalmente podrá habilitar estos recursos compartidos de auditoría según sea necesario:

a. Inicie sesión de forma remota en el nodo de administración de un sitio:

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

ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`

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

b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración.

c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`

11. Cierre la sesión del shell de comandos: `exit`

Comprobar la integración de auditoría de NFS

Después de configurar un recurso compartido de auditoría y agregar un cliente de auditoría NFS, puede montar el recurso compartido del cliente de auditoría y comprobar que los archivos estén disponibles en el recurso compartido de auditoría.

La compatibilidad con NFS ha quedado obsoleta y se eliminará en una futura versión.

Pasos

1. Verifique la conectividad (o variante para el sistema cliente) usando la dirección IP del cliente del nodo de administración que aloja el servicio AMS. Introduzca: `ping IP_address`

   Verifique que el servidor responde, indicando conectividad.

2. Monte el recurso compartido de sólo lectura de auditoría usando un comando apropiado para el sistema operativo cliente. Un ejemplo de comando de Linux es (introduzca en una línea):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/log myAudit`

   Utilice la dirección IP del nodo de administración que aloja el servicio AMS y el nombre de recurso compartido predefinido para el sistema de auditoría. El punto de montaje puede ser cualquier nombre seleccionado por el cliente (por ejemplo, *`myAudit`* en el comando anterior).

3. Verifique que los archivos estén disponibles en el recurso compartido de auditoría. Introduzca: `ls myAudit /*`

   donde *`myAudit`* es el punto de montaje del recurso compartido de auditoría. Debe haber al menos un archivo de registro en la lista.

Eliminar un cliente de auditoría NFS del recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Puede eliminar un cliente de auditoría existente eliminando su dirección IP.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña de la cuenta root/admin.

- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).

Acerca de esta tarea

No puede eliminar la última dirección IP permitida para acceder al recurso compartido de auditoría.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Elimine la dirección IP del recurso compartido de auditoría: `remove-ip-from-share`

   Se muestra una lista numerada de recursos compartidos de auditoría configurados en el servidor. El recurso compartido de auditoría aparece como: `/var/local/log`

4. Introduzca el número correspondiente al recurso compartido de auditoría: *`audit_share_number`*

   Se muestra una lista numerada de direcciones IP permitidas para acceder al recurso compartido de auditoría.

5. Introduzca el número correspondiente a la dirección IP que desea eliminar.

   El recurso compartido de auditoría se actualiza y ya no se permite el acceso desde ningún cliente de auditoría con esta dirección IP.

6. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

7. Cierre la utilidad de configuración NFS: `exit`
8. Si la implementación de StorageGRID es una puesta en marcha de varios sitios de centro de datos con nodos de administración adicionales en otros sitios, deshabilite estos recursos compartidos de auditoría según sea necesario:

a. Inicie sesión de forma remota en el nodo de administración de cada sitio:

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

   ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`

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

b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.

c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`

9. Cierre la sesión del shell de comandos: `exit`

Cambiar la dirección IP de un cliente de auditoría de NFS

Complete estos pasos si necesita cambiar la dirección IP de un cliente de auditoría de NFS.

Pasos

1. Agregue una nueva dirección IP a un recurso compartido de auditoría NFS existente.
2. Elimine la dirección IP original.

Información relacionada

- "Agregar un cliente de auditoría NFS a un recurso compartido de auditoría"
- "Eliminar un cliente de auditoría NFS del recurso compartido de auditoría"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.