Gestione los nodos de administrador

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

Gestione los nodos de administrador

Qué es un nodo de administrador

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Cada grid debe tener un nodo de administrador primario y puede tener cualquier cantidad de nodos de administrador no primarios por motivos de redundancia.

Cuando inicia sesión en el administrador de grid o en el administrador de inquilinos, se conecta a un nodo de administración. Puede conectarse a cualquier nodo de administrador y cada nodo de administrador muestra una vista similar del sistema StorageGRID. Sin embargo, se deben realizar los procedimientos de mantenimiento usando el nodo de administración principal.

Los nodos de administración también se pueden usar para equilibrar la carga del tráfico de clientes S3 y Swift.

Los nodos de administración alojan los siguientes servicios:

- Servicio AMS
- Servicio CMN
- Servicio NMS
- Servicio Prometheus
- Equilibrador de carga y servicios de alta disponibilidad (para admitir el tráfico de cliente S3 y Swift)

Los nodos de administración también admiten la interfaz de programa de aplicaciones de gestión (API de gestión) para procesar las solicitudes desde la API de gestión de grid y la API de gestión de inquilinos. Consulte Utilice la API de gestión de grid.

Qué es el servicio AMS

El servicio sistema de gestión de auditorías (AMS) realiza un seguimiento de la actividad y los eventos del sistema.

En qué consiste el servicio CMN

El servicio nodo de gestión de configuración (CMN) administra las configuraciones de todo el sistema de las características de conectividad y protocolo necesarias para todos los servicios. Además, el servicio CMN se utiliza para ejecutar y supervisar tareas de cuadrícula. Solo hay un servicio CMN por instalación de StorageGRID. El nodo de administración que aloja el servicio CMN se conoce como nodo de administración principal.

Qué es el servicio NMS

El servicio sistema de administración de red (NMS) activa las opciones de supervisión, generación de informes y configuración que se muestran a través de Grid Manager, la interfaz basada en explorador del sistema StorageGRID.

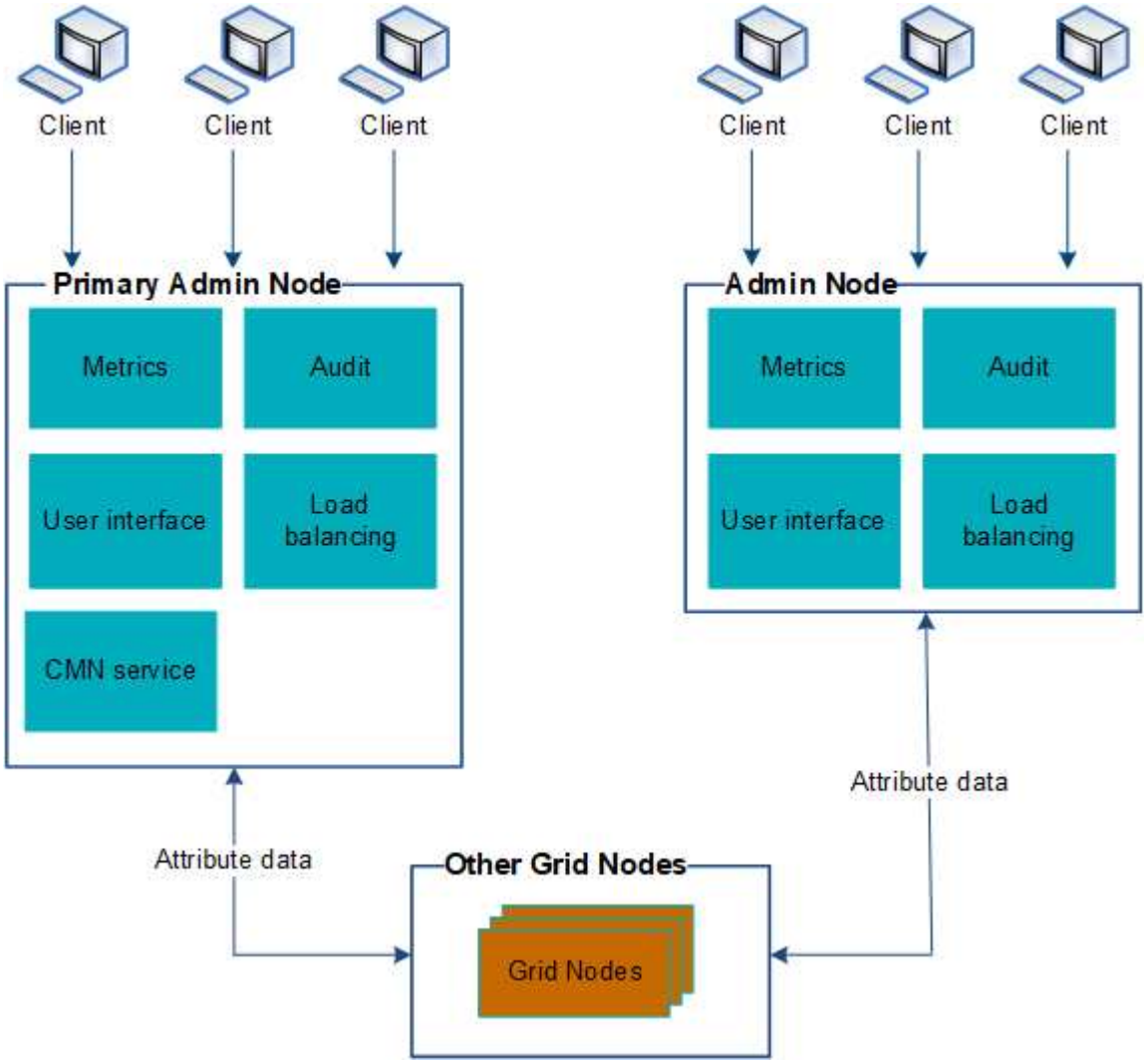
Qué es el servicio Prometheus

El servicio Prometheus recopila métricas de series temporales de los servicios de todos los nodos.

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 alarmas (sistema heredado) aún se activan y las notificaciones por correo electrónico y los mensajes de AutoSupport siguen enviados. Sin embargo, disponer de varios nodos de administrador no proporciona protección contra conmutación al nodo de respaldo, excepto notificaciones y mensajes de AutoSupport. En particular, las confirmaciones de alarma realizadas desde un nodo de administración no se copian a 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.

> Cuando se utiliza un grupo de alta disponibilidad, se interrumpe el acceso si falla el nodo de administración maestro. 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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.

Seleccione un remitente preferido

Si la implementación de StorageGRID incluye varios nodos de administrador, puede seleccionar qué nodo de administrador debe ser el remitente preferido de notificaciones. De forma predeterminada, se selecciona el nodo de administración principal, pero cualquier nodo de administración puede ser el remitente preferido.

Lo que necesitará

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

Acerca de esta tarea

La página **CONFIGURATION** > **System** > **Opciones de visualización** muestra qué nodo de administración está seleccionado actualmente para ser el emisor preferido. El nodo de administrador principal está seleccionado de forma predeterminada.

En operaciones normales del sistema, solo el remitente preferido envía las siguientes notificaciones:

- Mensajes de AutoSupport

- Notificaciones SNMP
- Mensajes de correo electrónico de alerta
- Correos electrónicos de alarma (sistema heredado)

Sin embargo, todos los demás nodos de administración (remitentes en espera) supervisan al remitente preferido. Si se detecta un problema, un remitente en espera también puede enviar estas notificaciones.

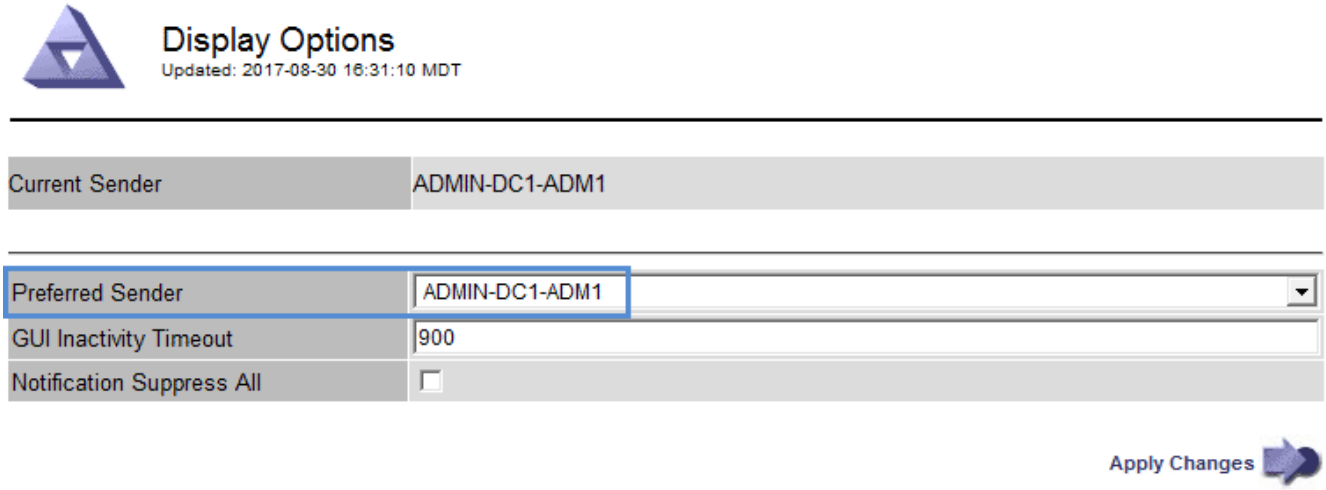
Tanto el remitente preferido como el remitente en espera pueden enviar notificaciones en los siguientes casos:

- Si los nodos de administración se convierten en "'desembarcados'" entre sí, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones, y pueden recibirse varias copias de las notificaciones.
- Después de que un remitente en espera detecta problemas con el remitente preferido y comienza a enviar notificaciones, es posible que el remitente preferido recupere su capacidad de enviar notificaciones. Si esto ocurre, es posible que se envíen notificaciones duplicadas. El remitente en espera dejará de enviar notificaciones cuando ya no detecte errores en el remitente preferido.

> Cuando prueba notificaciones de alarma y mensajes de AutoSupport, todos los nodos administrador envían el correo electrónico de prueba. Cuando prueba las notificaciones de alerta, debe iniciar sesión en cada nodo de administrador para verificar la conectividad.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. En el menú Opciones de pantalla, seleccione **Opciones**.
3. Seleccione el nodo de administración que desea establecer como remitente preferido de la lista desplegable.



4. Seleccione **aplicar cambios**.

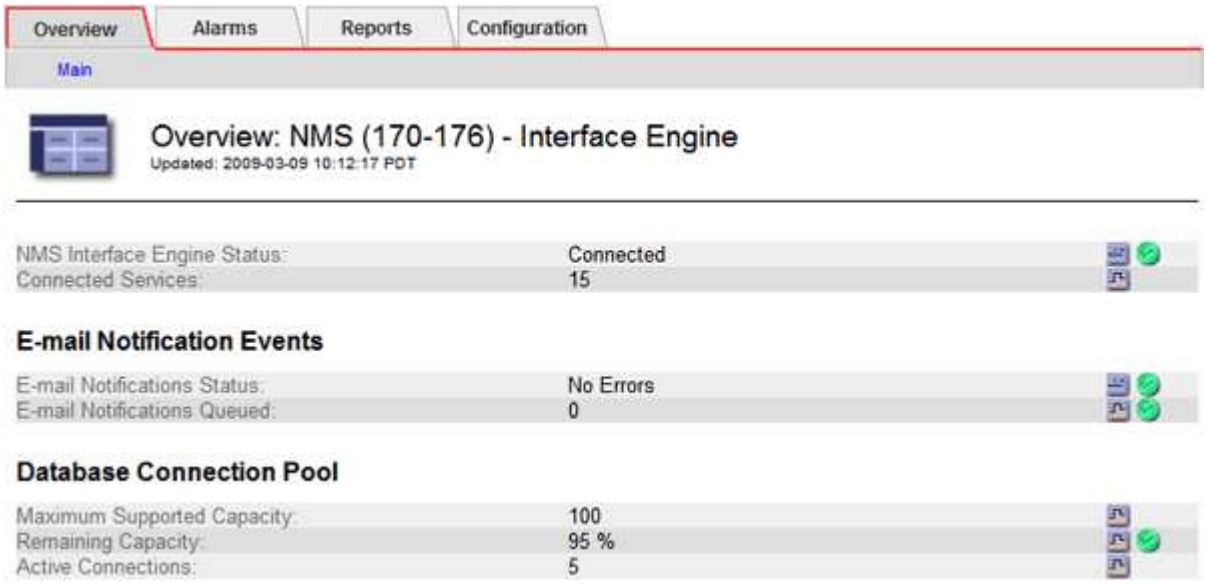
   El nodo de administrador se establece como el remitente preferido de notificaciones.

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**.

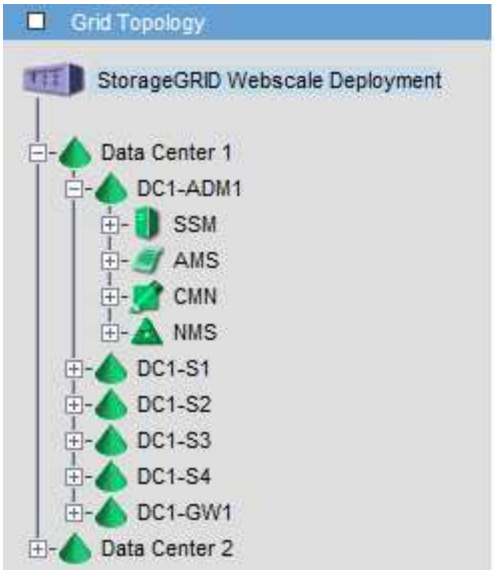


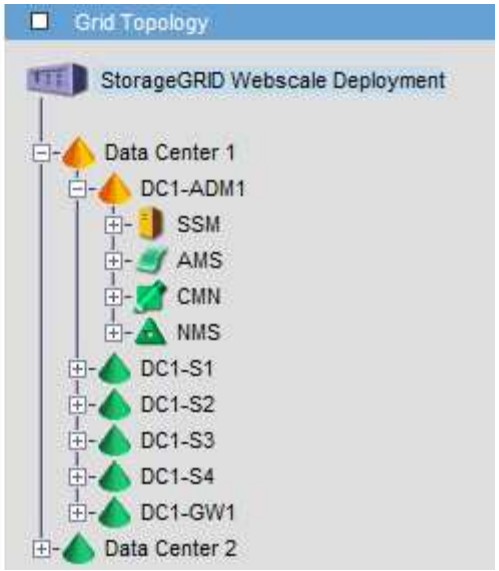
Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la 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. En el caso de que una notificación se descarta de la cola sin enviarse, se activa la alarma Minor DE MINUTOS (Estado de notificación por 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. Debido a que las confirmaciones no se copian en otros nodos de administración, es posible que el árbol de topología de cuadrícula no tenga 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

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. Para facilitar el acceso a los registros de auditoría, puede configurar el acceso de los clientes a recursos compartidos de auditoría de CIFS y NFS.

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.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID. Si dispone de la opción de utilizar CIFS o NFS, elija NFS.

Configurar clientes de auditoría para CIFS

El procedimiento utilizado para configurar un cliente de auditoría depende del método de autenticación: Windows Workgroup o Windows Active Directory (AD). Cuando se añade, el recurso compartido de auditoría se habilita automáticamente como un recurso compartido de solo lectura.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Configurar clientes de auditoría para Workgroup

Realice este procedimiento para cada nodo de administrador en una implementación de

StorageGRID desde la que desea recuperar mensajes de auditoría.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl+C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Establezca la autenticación para el grupo de trabajo de Windows:

   Si ya se ha establecido la autenticación, aparece un mensaje de aviso. Si ya se ha configurado la autenticación, vaya al paso siguiente.

   a. Introduzca: `set-authentication`
   b. Cuando se le solicite la instalación de Windows Workgroup o Active Directory, introduzca: `workgroup`

c. Cuando se le solicite, escriba un nombre del grupo de trabajo: *`workgroup_name`*

d. Cuando se le solicite, cree un nombre NetBIOS significativo: *`netbios_name`*

   o.

   Pulse **Intro** para utilizar el nombre de host del nodo de administración como nombre NetBIOS.

La secuencia de comandos reinicia el servidor Samba y se aplican los cambios. Esto debería tardar menos de un minuto. Después de establecer la autenticación, agregue un cliente de auditoría.

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

   Aparece la utilidad de configuración de CIFS.

6. Agregar un cliente de auditoría:

   a. Introduzca: `add-audit-share`

   > El recurso compartido se añade automáticamente como de solo lectura.

   b. Cuando se le solicite, agregue un usuario o grupo: *`user`*

   c. Cuando se le solicite, introduzca el nombre de usuario de auditoría: *`audit_user_name`*

   d. Cuando se le solicite, escriba una contraseña para el usuario de auditoría: *`password`*

   e. Cuando se le solicite, vuelva a introducir la misma contraseña para confirmarla: *`password`*

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

      Aparece la utilidad de configuración de CIFS.

   > No es necesario introducir un directorio. El nombre del directorio de auditoría está predefinido.

7. Si se permite que más de un usuario o grupo acceda al recurso compartido de auditoría, agregue los usuarios adicionales:

   a. Introduzca: `add-user-to-share`

      Se muestra una lista numerada de los recursos compartidos habilitados.

   b. Cuando se le solicite, escriba el número del recurso compartido auditoría-exportación: *`share_number`*

   c. Cuando se le solicite, agregue un usuario o grupo: `user`

      1. `group`

   d. Cuando se le solicite, introduzca el nombre del usuario o grupo de auditoría: *`audit_user or audit_group`*

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

      Aparece la utilidad de configuración de CIFS.

   f. Repita estos subpasos para cada usuario o grupo adicional que tenga acceso al recurso compartido de auditoría.

8. Si lo desea, compruebe la configuración: `validate-config`

   Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

   ```
   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
   (16384)
   ```

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

      Se muestra la configuración del cliente de auditoría.

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

      Aparece la utilidad de configuración de CIFS.

9. Cierre la utilidad de configuración CIFS: `exit`
10. Inicie el servicio Samba: `service smbd start`
11. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    o.

    De manera opcional, si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite este recurso compartido 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 los pasos para configurar el recurso compartido 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`
12. Cierre la sesión del shell de comandos: `exit`

Configurar clientes de auditoría para Active Directory

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

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).

- Tiene el nombre de usuario y la contraseña de CIFS Active Directory.
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl+C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Establezca la autenticación de Active Directory: `set-authentication`

   En la mayoría de las implementaciones, debe establecer la autenticación antes de agregar el cliente de auditoría. Si ya se ha establecido la autenticación, aparece un mensaje de aviso. Si ya se ha configurado la autenticación, vaya al paso siguiente.

   a. Cuando se le solicite la instalación de Workgroup o Active Directory: `ad`
   b. Cuando se le solicite, escriba el nombre del dominio de AD (nombre de dominio corto).
   c. Cuando se le solicite, introduzca la dirección IP o el nombre de host DNS del controlador de dominio.
   d. Cuando se le solicite, escriba el nombre completo del dominio.

Utilice letras mayúsculas.

e. Cuando se le solicite que habilite el soporte winbind, escriba **y**.

   Winbind se utiliza para resolver la información de usuarios y grupos desde los servidores AD.

f. Cuando se le solicite, introduzca el nombre NetBIOS.
g. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

6. Únase al dominio:
   a. Si no se ha iniciado todavía, inicie la utilidad de configuración de CIFS: `config_cifs.rb`
   b. Únase al dominio: `join-domain`
   c. Se le solicitará que pruebe si el nodo de administración es actualmente un miembro válido del dominio. Si este nodo de administrador no se ha Unido previamente al dominio, introduzca: `no`
   d. Cuando se le solicite, indique el nombre de usuario del administrador: *`administrator_username`*

      donde *`administrator_username`* Es el nombre de usuario de CIFS Active Directory, no el de StorageGRID.

   e. Cuando se le solicite, proporcione la contraseña del administrador: *`administrator_password`*

      lo eran *`administrator_password`* Es el nombre de usuario de CIFS Active Directory, no la contraseña de StorageGRID.

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

      Aparece la utilidad de configuración de CIFS.

7. Compruebe que se ha Unido correctamente al dominio:
   a. Únase al dominio: `join-domain`
   b. Cuando se le solicite que compruebe si el servidor es actualmente un miembro válido del dominio, especifique: `y`

      Si recibe el mensaje "'Join is OK,'" se ha Unido correctamente al dominio. Si no obtiene esta respuesta, intente configurar la autenticación y unirse al dominio de nuevo.

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

      Aparece la utilidad de configuración de CIFS.

8. Agregar un cliente de auditoría: `add-audit-share`
   a. Cuando se le solicite agregar un usuario o grupo, escriba: `user`
   b. Cuando se le solicite que introduzca el nombre de usuario de auditoría, introduzca el nombre de usuario de auditoría.
   c. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

9. Si se permite que más de un usuario o grupo acceda al recurso compartido de auditoría, agregue usuarios adicionales: `add-user-to-share`

   Se muestra una lista numerada de los recursos compartidos habilitados.

   a. Introduzca el número del recurso compartido auditoría-exportación.
   b. Cuando se le solicite agregar un usuario o grupo, escriba: `group`

      Se le solicitará el nombre del grupo de auditoría.

   c. Cuando se le solicite el nombre del grupo de auditoría, introduzca el nombre del grupo de usuarios de auditoría.
   d. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

   e. Repita este paso con cada usuario o grupo adicional que tenga acceso al recurso compartido de auditoría.

10. Si lo desea, compruebe la configuración: `validate-config`

    Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-interfaces.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-filesystem.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-interfaces.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-custom-config.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-shares.inc`
    - Rlimit_max: Aumentando rlimit_max (1024) al límite mínimo de Windows (16384)

    > No combine la configuración 'Security=ADS' con el parámetro 'Password Server'. (Por defecto Samba descubrirá el DC correcto para contactar automáticamente).

    i. Cuando se le solicite, pulse **Intro** para mostrar la configuración del cliente de auditoría.
    ii. Cuando se le solicite, pulse **Intro**.

       Aparece la utilidad de configuración de CIFS.

11. Cierre la utilidad de configuración CIFS: `exit`
12. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    o.

    De manera opcional, si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite 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 seguro remoto en Admin Node: `exit`

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

Añada un usuario o un grupo a un recurso compartido de auditoría CIFS

Es posible añadir un usuario o un grupo a un recurso compartido de auditoría CIFS que esté integrado con la autenticación de AD.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

El siguiente procedimiento es para un recurso compartido de auditoría integrado con la autenticación AD.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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 todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl+C**.

4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
-----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-----------------------------------------------------------------------
```

5. Comenzar a agregar un usuario o grupo: `add-user-to-share`

   Se muestra una lista numerada de los recursos compartidos de auditoría configurados.

6. Cuando se le solicite, introduzca el número del recurso compartido de auditoría (auditoría-exportación): *`audit_share_number`*

   Se le preguntará si desea proporcionar a un usuario o grupo acceso a este recurso compartido de auditoría.

7. Cuando se le solicite, agregue un usuario o grupo: `user` o. `group`
8. Cuando se le solicite el nombre de usuario o grupo para este recurso compartido de auditoría de AD, escriba el nombre.

   El usuario o grupo se agrega como de solo lectura para el recurso compartido de auditoría tanto en el sistema operativo del servidor como en el servicio CIFS. La configuración de Samba se vuelve a cargar para permitir al usuario o grupo acceder al recurso compartido del cliente de auditoría.

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

   Aparece la utilidad de configuración de CIFS.

10. Repita estos pasos para cada usuario o grupo que tenga acceso al recurso compartido de auditoría.
11. Si lo desea, compruebe la configuración: `validate-config`

    Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

    - No se puede encontrar el archivo /etc/samba/includes/cifs-interfaces.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-filesystem.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-custom-config.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-shares.inc.
      i. Cuando se le solicite, pulse **Intro** para mostrar la configuración del cliente de auditoría.
      ii. Cuando se le solicite, pulse **Intro**.

12. Cierre la utilidad de configuración CIFS: `exit`

13. Determine si necesita habilitar recursos compartidos de auditoría adicionales, de la siguiente forma:
    - 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 de un 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.
        iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`
14. Cierre la sesión del shell de comandos: `exit`

Quitar un usuario o un grupo de un recurso compartido de auditoría CIFS

No se puede eliminar el último usuario o grupo permitido para acceder al recurso compartido de auditoría.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con las contraseñas de la cuenta raíz (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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 CIFS: `config_cifs.rb`

```
-----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-----------------------------------------------------------------------
```

3. Comience a eliminar un usuario o grupo: `remove-user-from-share`

   Se muestra una lista numerada de los recursos compartidos de auditoría disponibles para el nodo de administración. El recurso compartido de auditoría se etiqueta audit-export.

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite que elimine un usuario o un grupo: `user` o. `group`

   Se muestra una lista numerada de usuarios o grupos para el recurso compartido de auditoría.

6. Introduzca el número correspondiente al usuario o grupo que desea eliminar: *`number`*

   Se actualiza el recurso compartido de auditoría y el usuario o grupo ya no tiene permiso de acceso al recurso compartido de auditoría. Por ejemplo:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Cierre la utilidad de configuración CIFS: `exit`
8. Si la implementación de StorageGRID incluye nodos de administración en otros sitios, deshabilite el recurso compartido de auditoría en cada sitio según sea necesario.
9. Cierre la sesión de cada shell de comando cuando la configuración se haya completado: `exit`

Cambiar un nombre de usuario o de grupo de recurso compartido de auditoría CIFS

Es posible cambiar el nombre de un usuario o de un grupo de un recurso compartido de auditoría de CIFS. Para ello, añada un nuevo usuario o grupo y, a continuación, elimine el anterior.

Acerca de esta tarea

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Pasos

1. Agregue un nuevo usuario o grupo con el nombre actualizado al recurso compartido de auditoría.
2. Elimine el nombre de usuario o grupo anterior.

Información relacionada

- Añada un usuario o un grupo a un recurso compartido de auditoría CIFS
- Quitar un usuario o un grupo de un recurso compartido de auditoría CIFS

Compruebe la integración de la auditoría de CIFS

El recurso compartido de auditoría es de solo lectura. Los archivos de registro están diseñados para que los lean las aplicaciones del equipo y la verificación no incluye abrir un archivo. Se considera suficiente verificación de que los archivos de registro de auditoría aparecen en una ventana del Explorador de Windows. Tras la verificación de la conexión, cierre todas las ventanas.

Configurar el cliente de auditoría para NFS

El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).
- 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.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).
- 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/audit/export`

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.

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 comando de Linux de ejemplo es (introduzca en una línea):

   `mount -t nfs -o hard,intr` *`Admin_Node_IP_address`*`:/var/local/audit/export` *`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.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

No se 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/audit/export`

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