



Descripción general

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

- Revisar registros de auditoría: Información general 1
 - Auditar el flujo y la retención de mensajes. 1
 - Acceda al archivo de registro de auditoría. 4
 - Rotación del archivo de registro de auditoría. 5

Revisar registros de auditoría: Información general

Estas instrucciones contienen información sobre la estructura y el contenido de los mensajes de auditoría y los registros de auditoría de StorageGRID. Esta información se puede utilizar para leer y analizar el registro de auditoría de la actividad del sistema.

Estas instrucciones son para los administradores responsables de generar informes sobre la actividad y el uso del sistema que requieran analizar los mensajes de auditoría del sistema StorageGRID.

Para usar el archivo de registro de texto, debe tener acceso al recurso compartido de auditoría configurado en el nodo de administración.

Para obtener información sobre la configuración de los niveles de mensajes de auditoría y el uso de un servidor de syslog externo, consulte [Configurar los mensajes de auditoría y los destinos de registro](#).

Información relacionada

- [Administre StorageGRID](#)

Auditar el flujo y la retención de mensajes

Todos los servicios de StorageGRID generan mensajes de auditoría durante el funcionamiento normal del sistema. Debe comprender la forma en que estos mensajes de auditoría pasan por el sistema StorageGRID al `audit.log` archivo.

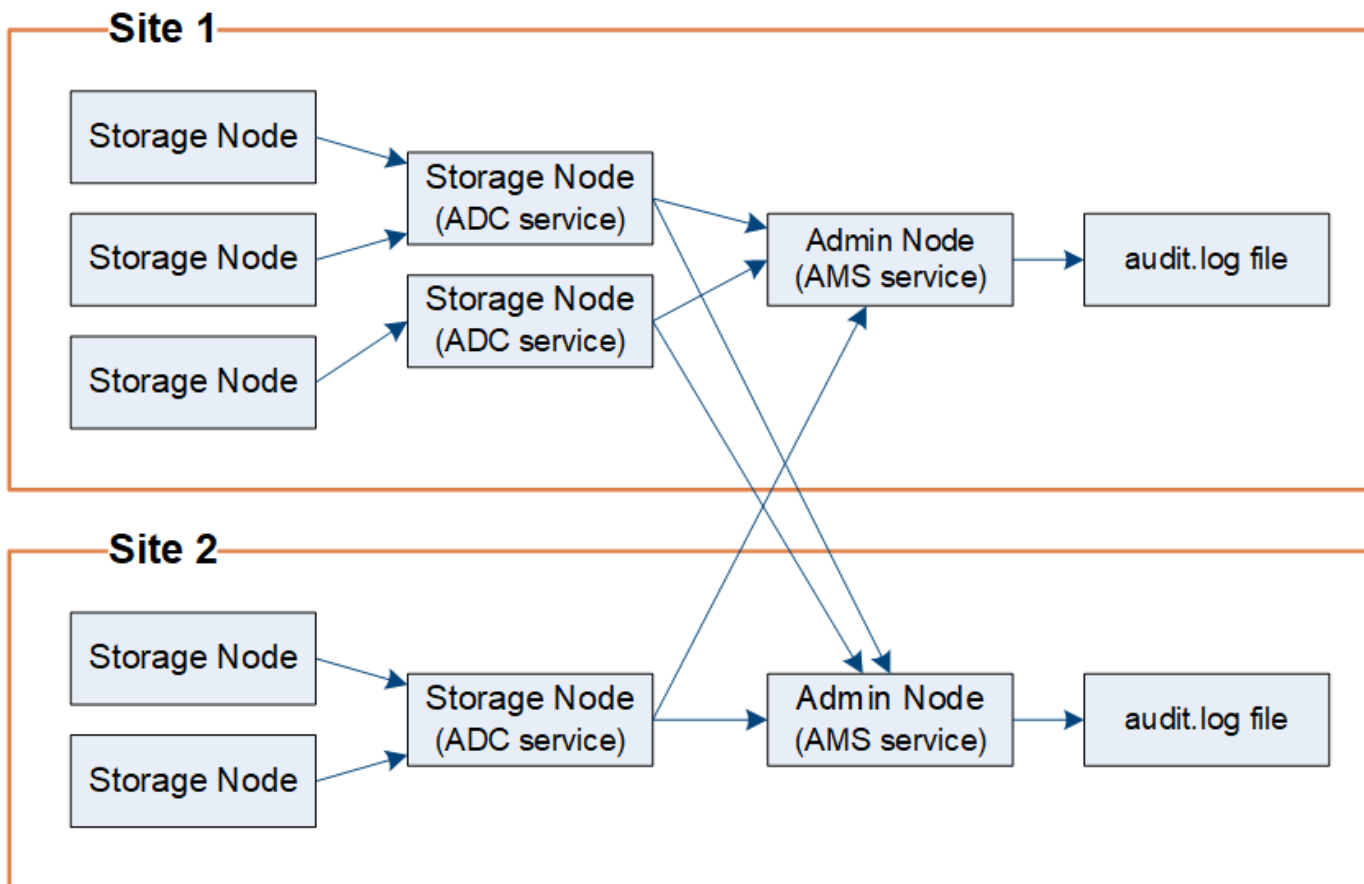
Flujo de mensajes de auditoría

Los mensajes de auditoría los procesan los nodos de administrador y los nodos de almacenamiento que tienen un servicio de controlador de dominio administrativo (ADC).

Como se muestra en el diagrama de flujo de mensajes de auditoría, cada nodo StorageGRID envía sus mensajes de auditoría a uno de los servicios ADC del sitio del centro de datos. El servicio ADC se habilita automáticamente para los primeros tres nodos de almacenamiento instalados en cada sitio.

A su vez, cada servicio ADC actúa como relé y envía su colección de mensajes de auditoría a cada nodo de administración del sistema StorageGRID, lo que proporciona a cada nodo de administración un registro completo de la actividad del sistema.

Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; se asigna el nombre al archivo de registro activo `audit.log`.



Retención de mensajes de auditoría

StorageGRID utiliza un proceso de copia y eliminación para garantizar que no se pierdan mensajes de auditoría antes de que puedan escribirse en el registro de auditoría.

Cuando un nodo genera o transmite un mensaje de auditoría, el mensaje se almacena en una cola de mensajes de auditoría en el disco del sistema del nodo de cuadrícula. Siempre se mantiene una copia del mensaje en la cola de mensajes de auditoría hasta que el mensaje se escribe en el archivo de registro de auditoría del nodo de administración `/var/local/audit/export` directorio. Esto ayuda a evitar la pérdida de un mensaje de auditoría durante el transporte.



La cola de mensajes de auditoría puede aumentar temporalmente debido a problemas de conectividad de red o capacidad de auditoría insuficiente. A medida que aumentan las colas, consumen más espacio disponible en cada nodo `/var/local/` directorio. Si el problema persiste y el directorio de mensajes de auditoría de un nodo está demasiado lleno, los nodos individuales priorizarán el procesamiento de su acumulación y no estarán disponibles temporalmente para los mensajes nuevos.

Específicamente, puede ver los siguientes comportamientos:

- Si la `/var/local/audit/export` el directorio utilizado por un nodo de administración se llena, el nodo de administración se marcará como no disponible para los nuevos mensajes de auditoría hasta que el directorio ya no esté lleno. Las solicitudes de los clientes S3 y Swift no se ven afectadas. La alarma XAMS (repositorios de auditoría no accesibles) se activa cuando no se puede acceder a un repositorio de auditoría.
- Si la `/var/local/` el directorio utilizado por un nodo de almacenamiento con el servicio ADC se llena al 92%, el nodo se marcará como no disponible para auditar mensajes hasta que el directorio sólo esté lleno al 87%. Las solicitudes de clientes S3 y Swift a otros nodos no se ven afectadas. La alarma NRLY (Relés de auditoría disponibles) se activa cuando no se pueden acceder a los relés de auditoría.



Si no hay nodos de almacenamiento disponibles con el servicio ADC, los nodos de almacenamiento almacenan los mensajes de auditoría localmente en la `/var/local/log/localaudit.log` archivo.

- Si la `/var/local/` El directorio que utiliza un nodo de almacenamiento se llena al 85%, el nodo empezará a rechazar las solicitudes de cliente S3 y Swift 503 `Service Unavailable`.

Los siguientes tipos de problemas pueden hacer que las colas de mensajes de auditoría crezcan muy grandes:

- La interrupción de un nodo de administrador o un nodo de almacenamiento con el servicio de ADC. Si uno de los nodos del sistema está inactivo, es posible que los nodos restantes se vuelvan a registrar.
- Tasa de actividad sostenida que supera la capacidad de auditoría del sistema.
- La `/var/local/` El espacio de un nodo de almacenamiento ADC se llena por motivos que no están relacionados con los mensajes de auditoría. Cuando esto sucede, el nodo deja de aceptar nuevos mensajes de auditoría y da prioridad a su acumulación actual, lo que puede provocar backlogs en otros nodos.

Alarma de alerta de cola de auditoría grande y mensajes de auditoría en cola (AMQS)

Para ayudarle a supervisar el tamaño de las colas de mensajes de auditoría a lo largo del tiempo, la alerta **cola de auditoría grande** y la alarma AMQS heredada se activan cuando el número de mensajes en una cola de nodos de almacenamiento o cola de nodos de administración alcanza determinados umbrales.

Si se activa la alerta **cola de auditoría grande** o la alarma AMQS heredada, comience comprobando la carga en el sistema—si ha habido un número significativo de transacciones recientes, la alerta y la alarma deben resolverse con el tiempo y pueden ignorarse.

Si la alerta o alarma persiste y aumenta su gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta constantemente durante horas o días, es probable que la carga de auditoría haya superado la capacidad de auditoría del sistema. Reduzca la tasa de operaciones del cliente o disminuya el número de mensajes de auditoría registrados cambiando el nivel de auditoría de las escrituras del cliente y las lecturas del cliente a error o Desactivado. Consulte "[Configurar los mensajes de auditoría y los destinos de registro](#)."

Mensajes duplicados

El sistema StorageGRID toma un método conservador si se produce un fallo en la red o en un nodo. Por este motivo, puede haber mensajes duplicados en el registro de auditoría.

Acceda al archivo de registro de auditoría

El recurso compartido de auditoría contiene el activo `audit.log` archivo y todos los archivos de registro de auditoría comprimidos. Para facilitar el acceso a los registros de auditoría, es posible configurar el acceso de clientes a recursos compartidos de auditoría de NFS y CIFS (CIFS está obsoleto). También es posible acceder a los archivos del registro de auditoría directamente desde la línea de comandos del nodo de administración.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Pasos

1. Inicie sesión en un nodo de administrador:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`

- b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Vaya al directorio que contiene los archivos del registro de auditoría:

```
cd /var/local/audit/export
```

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Información relacionada

[Administre StorageGRID](#)

Rotación del archivo de registro de auditoría

Los archivos de registros de auditoría se guardan en un nodo administrador `/var/local/audit/export` directorio. Se denomina los archivos de registro de auditoría activos `audit.log`.



De manera opcional, se puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor de syslog externo. Se siguen generando y almacenando registros locales de registros de auditoría cuando se configura un servidor de syslog externo. Consulte [Configurar los mensajes de auditoría y los destinos de registro](#).

Una vez al día, el activo `audit.log` el archivo se guardará y se guardará un nuevo `audit.log` se ha iniciado el archivo. El nombre del archivo guardado indica cuándo se guardó, en el formato `yyyy-mm-dd.txt`. Si se crea más de un registro de auditoría en un solo día, los nombres de los archivos utilizan la fecha en la que se guardó el archivo, añadido por un número, en formato `yyyy-mm-dd.txt.n`. Por ejemplo: `2018-04-15.txt` y `2018-04-15.txt.1` Son los primeros y segundos archivos de registro creados y guardados el 15 de abril de 2018.

Después de un día, el archivo guardado se comprime y cambia su nombre, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original. Con el tiempo, esto genera el consumo de almacenamiento asignado a los registros de auditoría en el nodo de administración. Una secuencia de comandos supervisa el consumo de espacio del registro de auditoría y elimina los archivos de registro según sea necesario para liberar espacio en la `/var/local/audit/export` directorio. Los registros de auditoría se eliminan según la fecha en la que se crearon, y la más antigua se eliminó primero. Puede supervisar las acciones del script en el siguiente archivo: `/var/local/log/manage-audit.log`.

En este ejemplo se muestra el activo `audit.log` archivo, el archivo del día anterior (`2018-04-15.txt`), y el archivo comprimido del día anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Información de copyright

Copyright © 2024 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.