Información general de los mensajes de auditoría

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

Información general de los mensajes de auditoría 1
Auditar el flujo y la retención de mensajes 1
Cambiar los niveles de mensajes de auditoría 4
Acceso al archivo de registro de auditoría 6
Rotación del archivo de registro de auditoría 7

Información general de los mensajes de auditoría

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.

Se supone que tiene un conocimiento sólido de la naturaleza de las actividades auditadas dentro 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.

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.

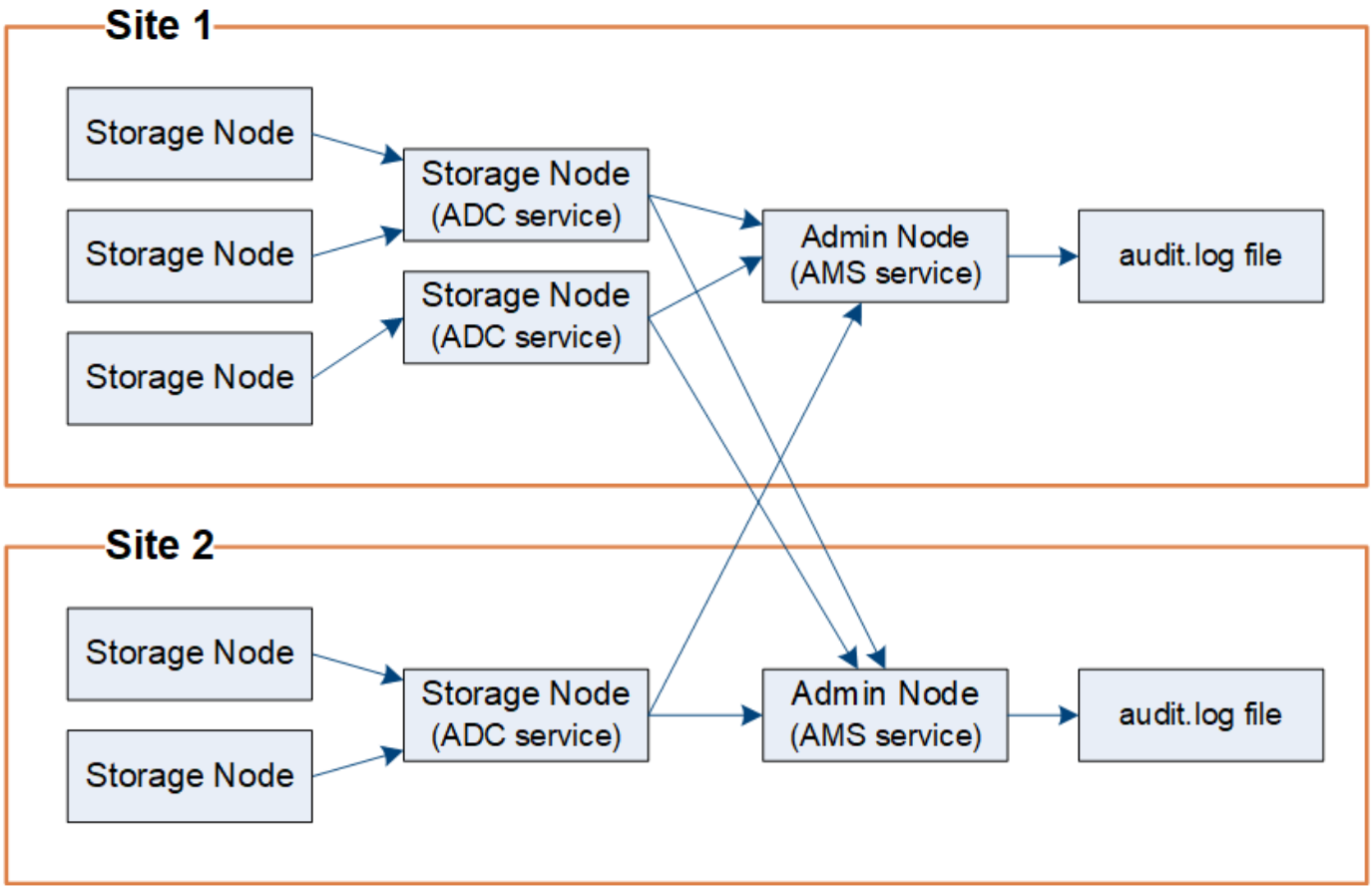
Flujo de mensajes de auditoría

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.

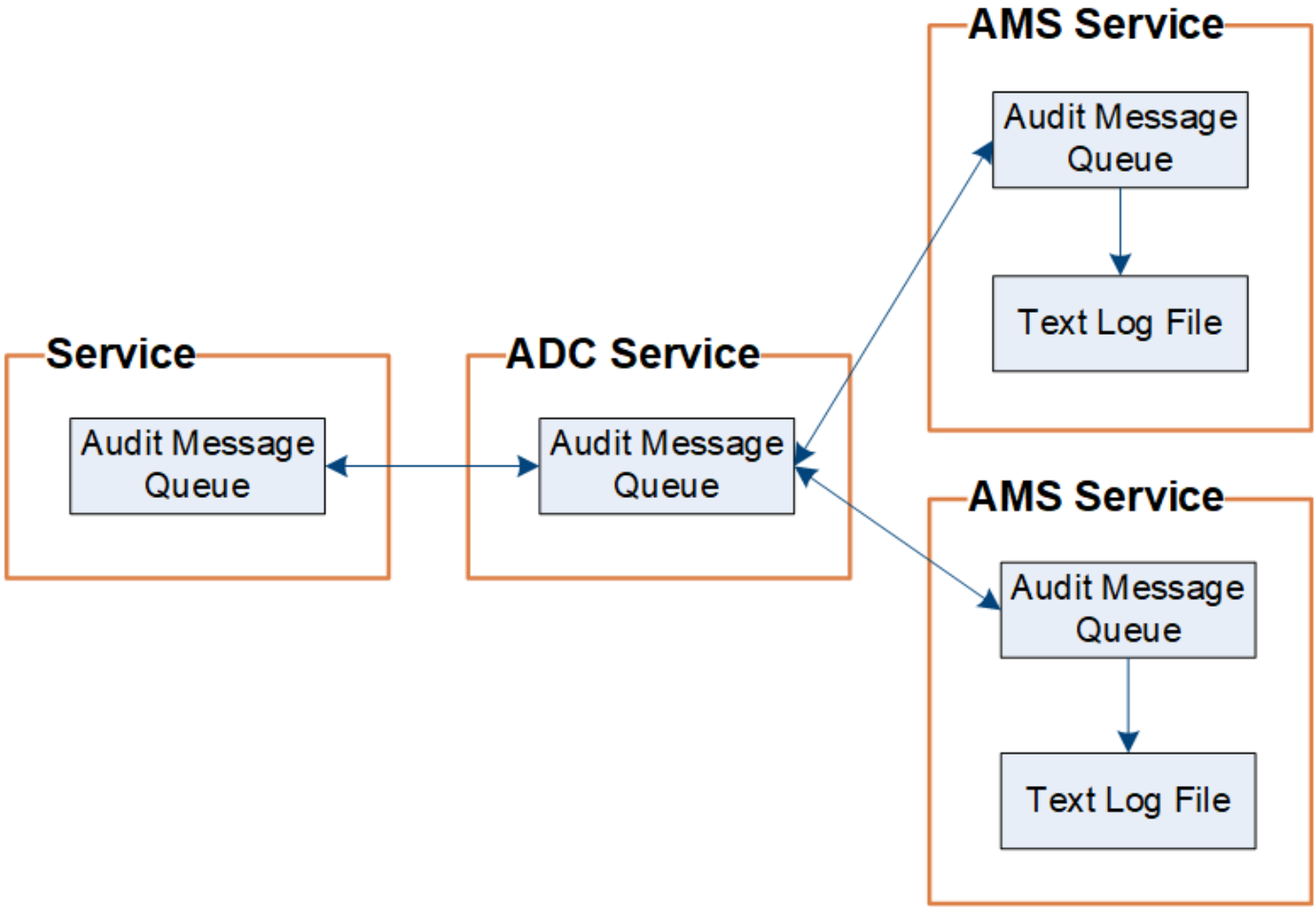
Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; se asigna el nombre al archivo de registro activo `audit.log`.



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.

- 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 "'Cambiar los niveles de mensajes de auditoría'."

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.

Cambiar los niveles de mensajes de auditoría

Puede ajustar los niveles de auditoría para aumentar o reducir el número de mensajes de auditoría registrados en el registro de auditoría de cada categoría de mensajes de auditoría.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Los mensajes de auditoría registrados en el registro de auditoría se filtran según la configuración de la página **Configuración** > **Supervisión** > **Auditoría**.

Puede establecer un nivel de auditoría diferente para cada una de las siguientes categorías de mensajes:

- **Sistema**: De forma predeterminada, este nivel se establece en normal.
- **Almacenamiento**: De forma predeterminada, este nivel se establece en error.

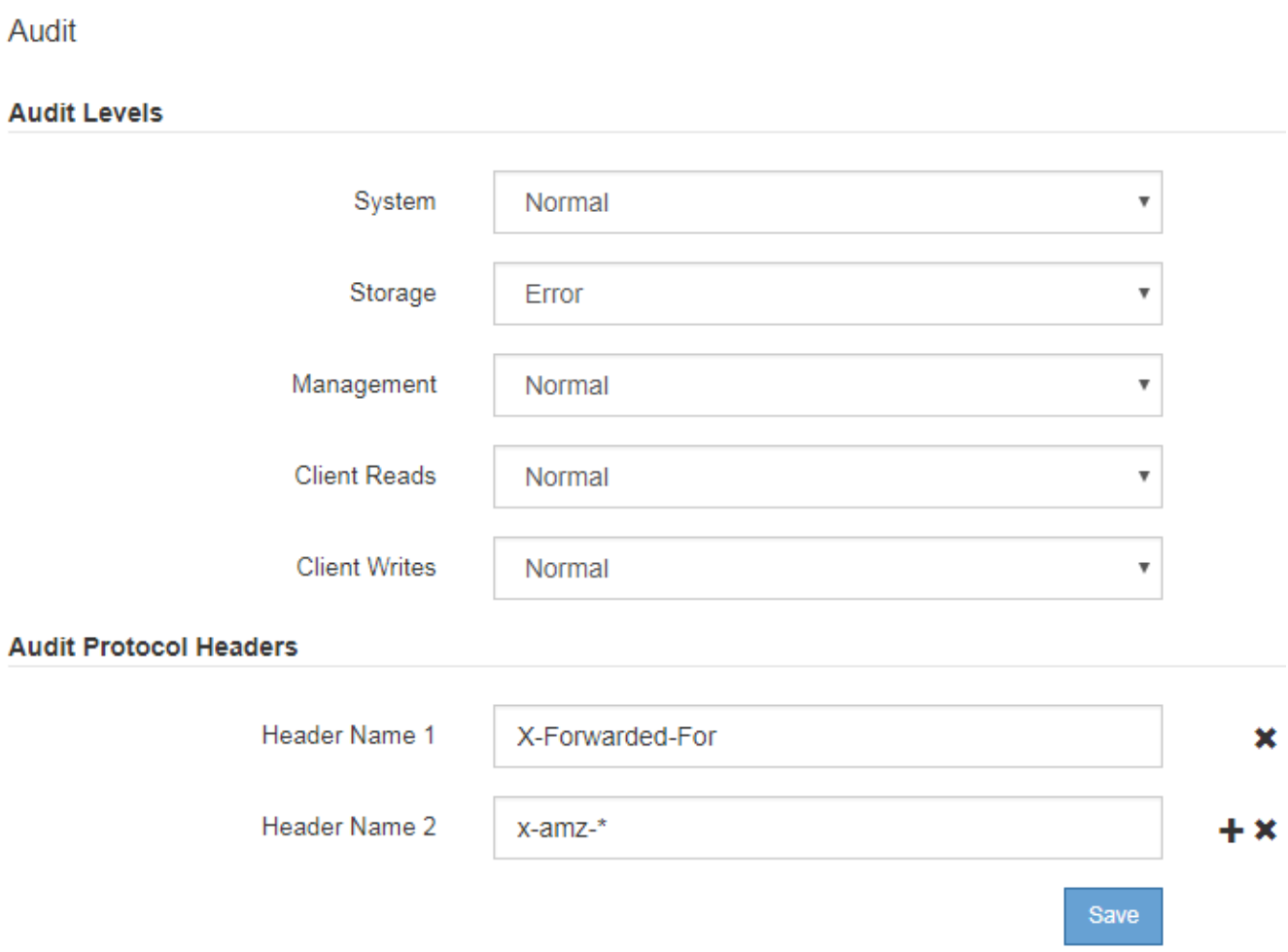
- **Administración**: De forma predeterminada, este nivel se establece en normal.
- **Lecturas de cliente**: De forma predeterminada, este nivel se establece en normal.
- **Escrituras de cliente**: De forma predeterminada, este nivel se establece en normal.

Estos valores predeterminados se aplican si instaló inicialmente StorageGRID con la versión 10.3 o posterior. Si ha actualizado desde una versión anterior de StorageGRID, la opción predeterminada para todas las categorías se establece en normal.

Durante las actualizaciones, las configuraciones a nivel de auditoría no serán efectivas inmediatamente.

Pasos

1. Seleccione **Configuración** > **Supervisión** > **Auditoría**.



2. Para cada categoría de mensaje de auditoría, seleccione un nivel de auditoría de la lista desplegable:

Nivel de auditoría	Descripción
Apagado	No se registran mensajes de auditoría de la categoría.
Error	Sólo se registran los mensajes de error: Los mensajes de auditoría para los que el código de resultado no fue "correcto" (SUCS).

Nivel de auditoría	Descripción
Normal	Se registran los mensajes transaccionales estándar: Los mensajes que aparecen en estas instrucciones para la categoría.
Depurar	Obsoleto. Este nivel se comporta como el nivel de auditoría normal.

Los mensajes incluidos para cualquier nivel particular incluyen los que se registrarán en los niveles superiores. Por ejemplo, el nivel normal incluye todos los mensajes de error.

3. En **encabezados de protocolo de auditoría**, introduzca el nombre de los encabezados de solicitud HTTP que se incluirán en los mensajes de auditoría de lectura y escritura de cliente. Utilice un asterisco (*) como comodín o la secuencia de escape (*) como un asterisco literal. Haga clic en el signo más para crear una lista de campos de nombre de encabezado.

   Los encabezados de protocolo de auditoría se aplican solo a solicitudes S3 y Swift.

   Cuando estos encabezados HTTP se encuentran en una solicitud, se incluyen en el mensaje de auditoría bajo el campo HTRH.

   Los encabezados de la solicitud del protocolo de auditoría sólo se registran si el nivel de auditoría para **Lecturas de cliente** o **Escrituras de cliente** no es **Desactivada**.

4. Haga clic en **Guardar**.

Información relacionada

"Mensajes de auditoría del sistema"

"Mensajes de auditoría del almacenamiento de objetos"

"Mensaje de auditoría de gestión"

"El cliente lee los mensajes de auditoría"

"Administre StorageGRID"

Acceso 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 (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`.

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

Información de la marca comercial