# Visão geral da mensagem de auditoria

StorageGRID

NetApp
March 10, 2025

# Índice

# Visão geral da mensagem de auditoria

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e registos de auditoria do StorageGRID. Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções destinam-se aos administradores responsáveis pela produção de relatórios de atividade e utilização do sistema que exijam a análise das mensagens de auditoria do sistema StorageGRID.

Presume-se que você tenha uma boa compreensão da natureza das atividades auditadas dentro do sistema StorageGRID. Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó Admin.

**Informações relacionadas**

"Administrar o StorageGRID"

# Auditoria de fluxo e retenção de mensagens

Todos os serviços StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para `audit.log` o arquivo.

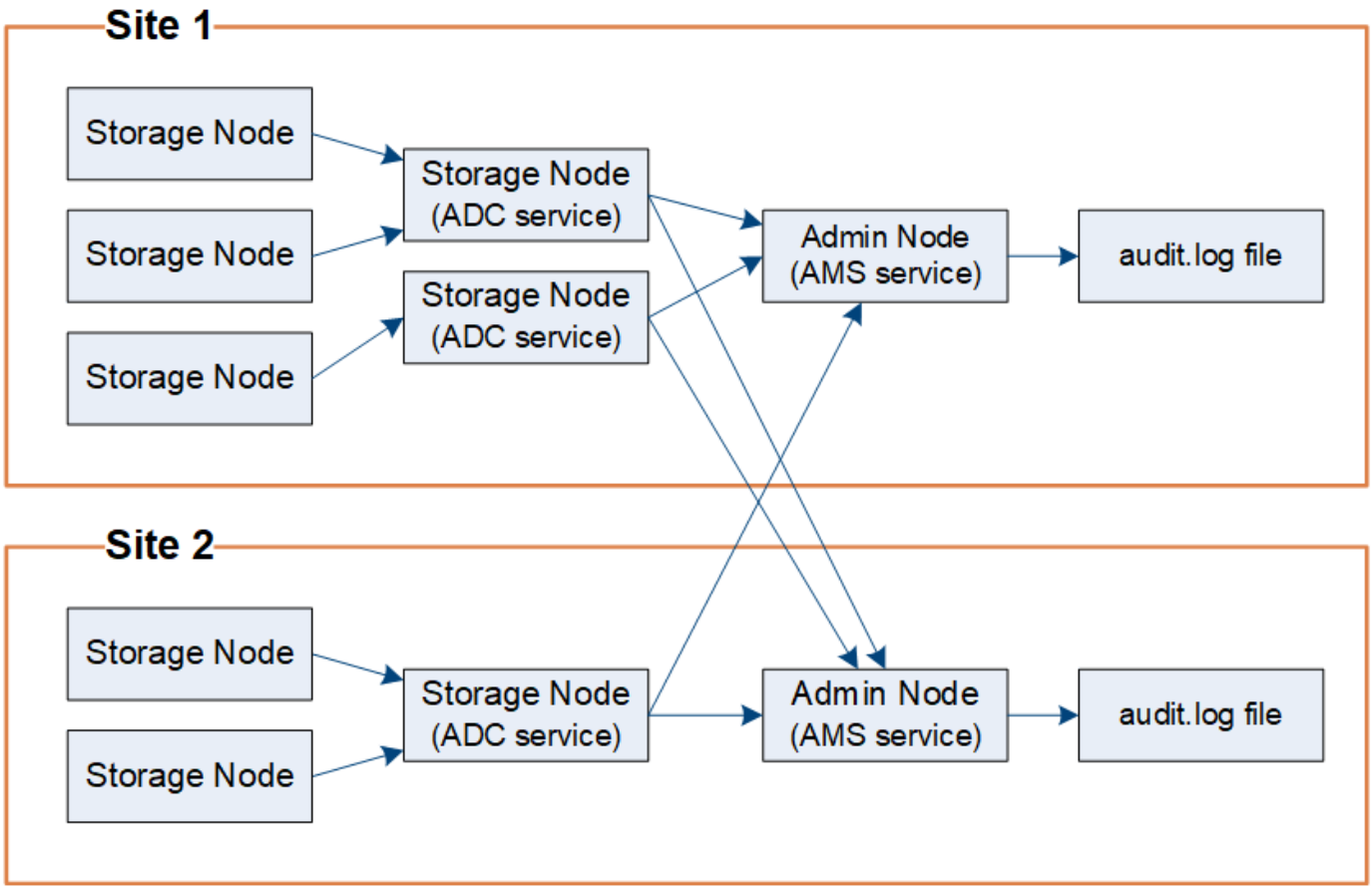
## Auditoria do fluxo de mensagens

As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços ADC no local do data center. O serviço ADC é ativado automaticamente para os três primeiros nós de storage instalados em cada local.

Por sua vez, cada serviço ADC atua como um relé e envia sua coleção de mensagens de auditoria para cada nó de administração no sistema StorageGRID, o que dá a cada nó de administração um Registro completo da atividade do sistema.

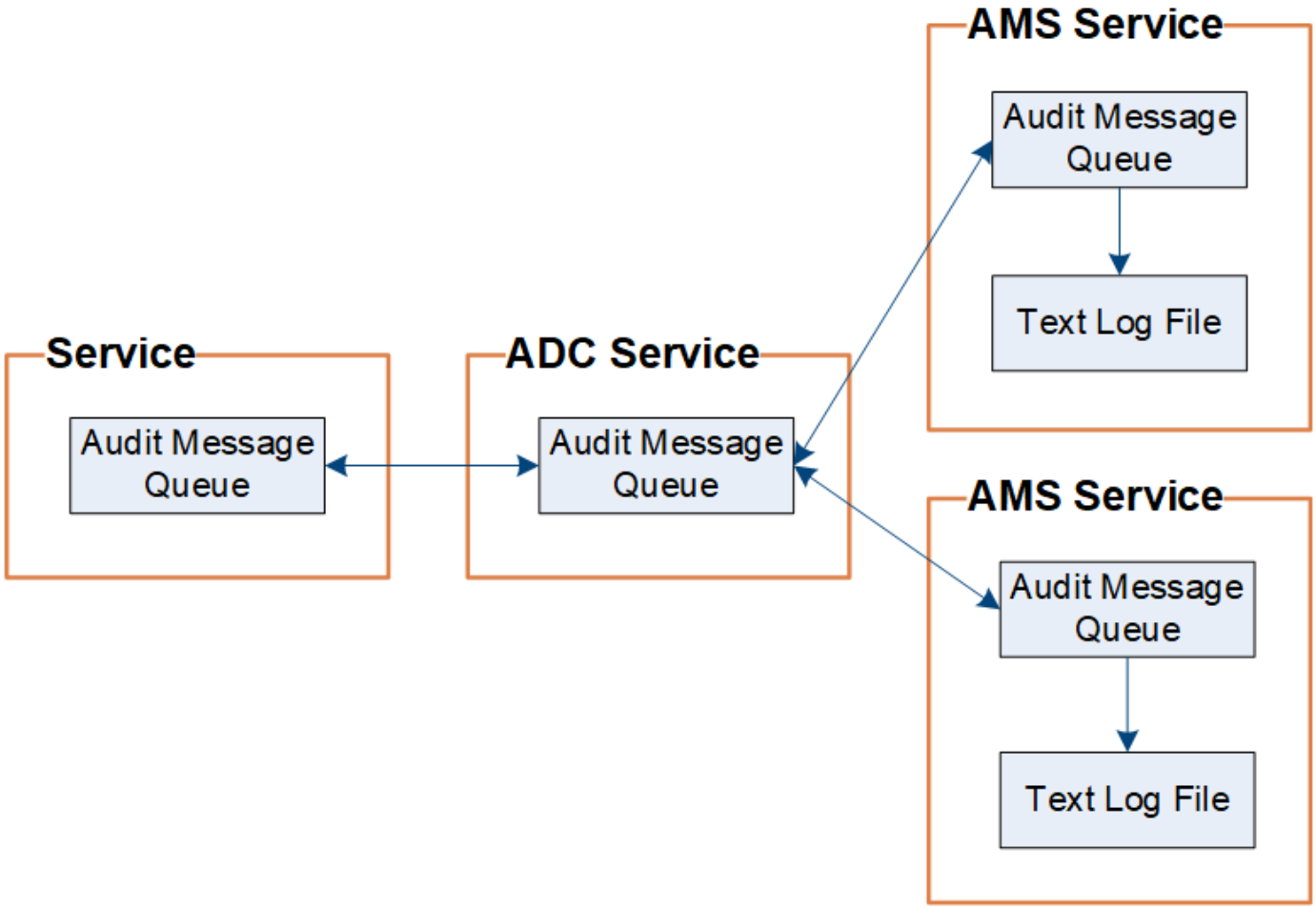
Cada nó Admin armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é `audit.log` nomeado .




**Retenção de mensagens de auditoria**

O StorageGRID usa um processo de cópia e exclusão para garantir que nenhuma mensagem de auditoria seja perdida antes que ela possa ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no diretório do Admin Node `/var/local/audit/export`. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.




A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conetividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível no diretório de cada nó `/var/local/`. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizarão o processamento de seu backlog e ficarão temporariamente indisponíveis para novas mensagens.

Especificamente, você pode ver os seguintes comportamentos:

- Se o `/var/local/audit/export` diretório usado por um nó Admin ficar cheio, o nó Admin será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações de clientes S3 e Swift não são afetadas. O alarme XAMS (Unreachable Audit Repositories) é acionado quando um repositório de auditoria é inacessível.
- Se o `/var/local/` diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para auditar mensagens até que o diretório esteja apenas 87% cheio. As solicitações de clientes S3 e Swift para outros nós não são afetadas. O alarme NRLY (relés de auditoria disponíveis) é acionado quando os relés de auditoria não são alcançáveis.

> ⓘ Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 e Swift com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria cresçam muito

grandes:

- A interrupção de um nó de administração ou de um nó de storage com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes podem ficar com backlogged.
- Uma taxa de atividade contínua que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC se torna cheio por razões não relacionadas às mensagens de auditoria. Quando isso acontece, o nó pára de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

#### Alerta de fila de auditoria grande e alarme de mensagens de auditoria enfileiradas (AMQS)

Para ajudá-lo a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administrador atinge determinados limites.

Se o alerta **fila de auditoria grande** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema - se houver um número significativo de transações recentes, o alerta e o alarme devem ser resolvidos com o tempo e podem ser ignorados.

Se o alerta ou o alarme persistir e aumentar a gravidade, veja um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para gravações do cliente e leituras do cliente para erro ou Desativado. Consulte ""Alteração dos níveis de mensagens de auditoria"."

#### Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora se ocorrer uma falha de rede ou nó. Por esse motivo, mensagens duplicadas podem existir no log de auditoria.

# Alteração dos níveis de mensagens de auditoria

Você pode ajustar os níveis de auditoria para aumentar ou diminuir o número de mensagens de auditoria registradas no log de auditoria para cada categoria de mensagens de auditoria.

#### O que você vai precisar

- Você deve estar conetado ao Gerenciador de Grade usando um navegador compatível.
- Você deve ter permissões de acesso específicas.

#### Sobre esta tarefa

As mensagens de auditoria registradas no log de auditoria são filtradas com base nas configurações da página **Configuração** > **Monitoramento** > **Auditoria**.

Você pode definir um nível de auditoria diferente para cada uma das seguintes categorias de mensagens:

- **Sistema**: Por padrão, esse nível é definido como normal.
- **Armazenamento**: Por padrão, esse nível é definido como erro.
- **Gerenciamento**: Por padrão, esse nível é definido como normal.
- **Leitura do cliente**: Por padrão, esse nível é definido como normal.

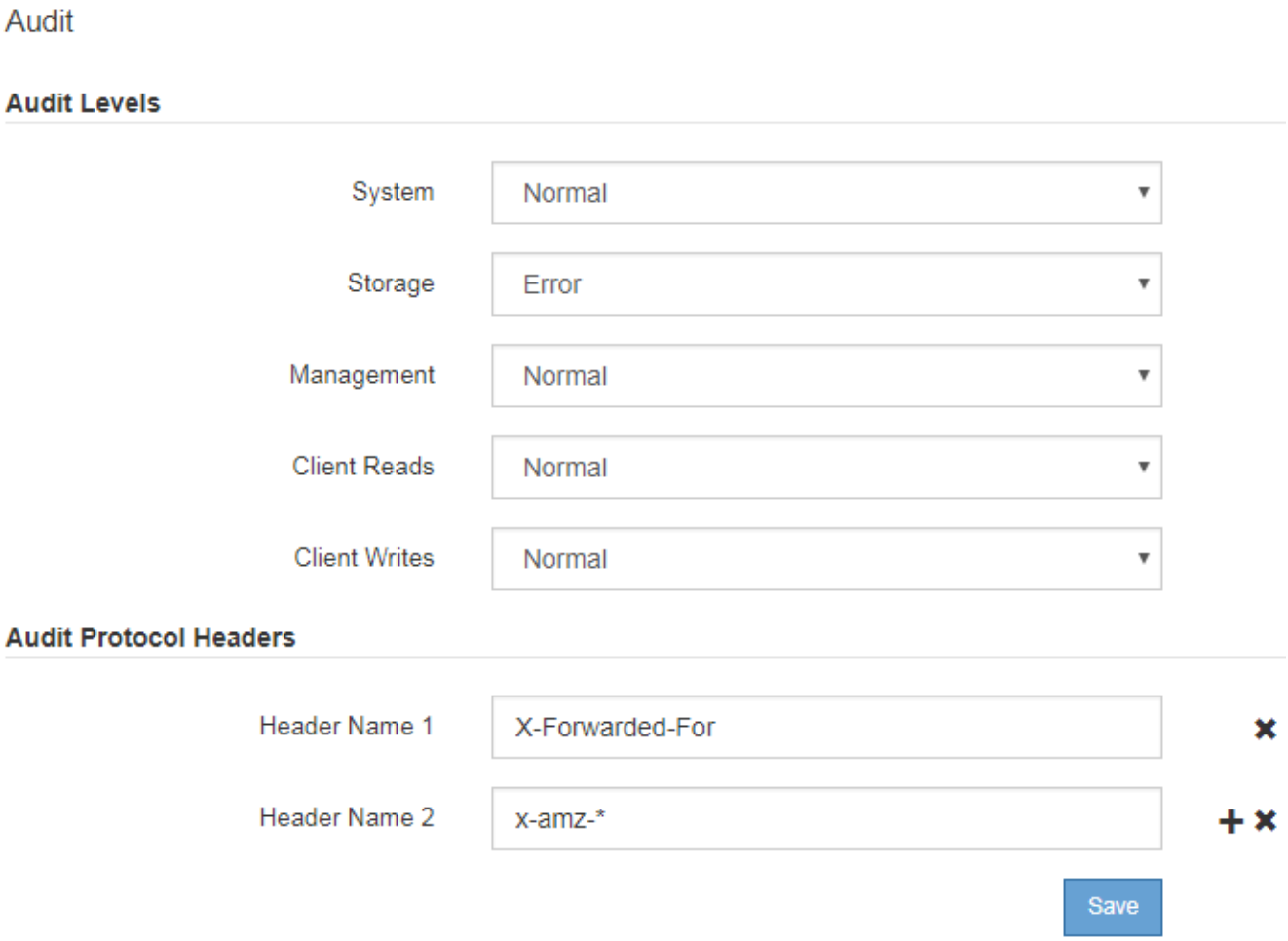
- * Gravações do cliente*: Por padrão, esse nível é definido como normal.

> Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10,3 ou posterior. Se você atualizou de uma versão anterior do StorageGRID, o padrão para todas as categorias é definido como normal.

> Durante as atualizações, as configurações de nível de auditoria não entrarão em vigor imediatamente.

**Passos**

1. Selecione **Configuração** > **Monitoramento** > **Auditoria**.




2. Para cada categoria de mensagem de auditoria, selecione um nível de auditoria na lista suspensa:

| Nível de auditoria | Descrição |
|---|---|
| Desligado | Nenhuma mensagem de auditoria da categoria é registrada. |
| Erro | Somente mensagens de erro são registradas - mensagens de auditoria para as quais o código de resultado não foi "bem-sucedido" (SUCS). |

| Nível de auditoria | Descrição |
| --- | --- |
| Normal | As mensagens transacionais padrão são registradas - as mensagens listadas nestas instruções para a categoria. |
| Depurar | Obsoleto. Este nível comporta-se da mesma forma que o nível normal de auditoria. |

As mensagens incluídas para qualquer nível particular incluem aquelas que seriam registradas nos níveis mais altos. Por exemplo, o nível normal inclui todas as mensagens de erro.

3. Em **Audit Protocol Headers**, insira o nome dos cabeçalhos de solicitação HTTP a serem incluídos nas mensagens de auditoria de leitura de cliente e gravação de cliente. Use um asterisco (**) como um curinga ou use a sequência de escape (**) como um asterisco literal. Clique no sinal de mais para criar uma lista de campos de nome de cabeçalho.

   Os cabeçalhos de protocolo de auditoria aplicam-se apenas às solicitações S3 e Swift.

   Quando esses cabeçalhos HTTP são encontrados em uma solicitação, eles são incluídos na mensagem de auditoria sob o campo HTRH.

   Os cabeçalhos de solicitação de protocolo de auditoria são registrados somente se o nível de auditoria para **leitura do cliente** ou **gravações do cliente** não for **desativado**.

4. Clique em **Salvar**.

**Informações relacionadas**

"Mensagens de auditoria do sistema"

"Mensagens de auditoria de armazenamento de objetos"

"Mensagem de auditoria de gerenciamento"

"O cliente lê mensagens de auditoria"

"Administrar o StorageGRID"

# Acessando o arquivo de log de auditoria

O compartilhamento de auditoria contém o arquivo ativo `audit.log` e todos os arquivos de log de auditoria compatados. Para facilitar o acesso aos logs de auditoria, você pode configurar o acesso do cliente para compartilhamentos de auditoria para NFS e CIFS (obsoleto). Você também pode acessar arquivos de log de auditoria diretamente da linha de comando do nó Admin.

**O que você vai precisar**

- Você deve ter permissões de acesso específicas.
- Tem de ter o `Passwords.txt` ficheiro.
- Você deve saber o endereço IP de um nó Admin.

**Passos**

1. Faça login em um nó Admin:
   a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
2. Vá para o diretório que contém os arquivos de log de auditoria:

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

3. Visualize o ficheiro de registo de auditoria atual ou guardado, conforme necessário.

**Informações relacionadas**

"Administrar o StorageGRID"

# Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos no diretório de um nó de administrador `/var/local/audit/export`. Os arquivos de log de auditoria ativos são `audit.log` nomeados .

Uma vez por dia, o arquivo ativo `audit.log` é salvo e um novo `audit.log` arquivo é iniciado. O nome do ficheiro guardado indica quando foi guardado, no formato *`yyyy-mm-dd.txt`*. Se mais de um log de auditoria for criado em um único dia, os nomes de arquivo usarão a data em que o arquivo foi salvo, anexado por um número, no formato *`yyyy-mm-dd.txt.n`*. Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são os primeiros e segundos arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`*, que preserva a data original. Com o tempo, isso resulta no consumo de storage alocado para logs de auditoria no nó Admin. Um script monitora o consumo de espaço do log de auditoria e exclui arquivos de log conforme necessário para liberar espaço no `/var/local/audit/export` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log`.

Este exemplo mostra o `audit.log` ficheiro ativo, o ficheiro do dia anterior (`2018-04-15.txt`) e o ficheiro comprimido para o dia anterior (`2018-04-14.txt.gz`).

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

## Informações sobre direitos autorais



## Informações sobre marcas comerciais