Configurar gerenciamento de log e servidor syslog externo

StorageGRID software

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/pt-br/storagegrid/monitor/considerations-for-external-syslog-server.html on February 12, 2026. Always check docs.netapp.com for the latest.

Índice

Configurar gerenciamento de log e servidor syslog externo

Considerações para usar um servidor syslog externo

Um servidor syslog externo é um servidor fora do StorageGRID que você pode usar para coletar informações de auditoria do sistema em um único local. O uso de um servidor syslog externo permite reduzir o tráfego de rede em seus nós de administração e gerenciar as informações com mais eficiência. Para StorageGRID, o formato de pacote de mensagens syslog de saída é compatível com RFC 3164.

Os tipos de informações de auditoria que você pode enviar para o servidor syslog externo incluem:

- Logs de auditoria contendo as mensagens de auditoria geradas durante a operação normal do sistema
- Eventos relacionados à segurança, como logins e escalações para o root
- Logs de aplicativos que podem ser solicitados se for necessário abrir um caso de suporte para solucionar um problema encontrado

Quando usar um servidor syslog externo

Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria. O envio de informações de auditoria para um servidor syslog externo permite que você:

- Colete e gerencie informações de auditoria, como mensagens de auditoria, logs de aplicativos e eventos de segurança com mais eficiência.
- Reduza o tráfego de rede nos nós de administração porque as informações de auditoria são transferidas diretamente dos vários nós de storage para o servidor syslog externo, sem ter que passar por um nó de administração.

> Quando os logs são enviados para um servidor syslog externo, logs únicos maiores que 8.192 bytes são truncados no final da mensagem para estar em conformidade com as limitações comuns em implementações de servidor syslog externo.

> Para maximizar as opções de recuperação completa de dados em caso de falha do servidor syslog externo, até 20 GB de logs locais de Registros de auditoria (`localaudit.log`) são mantidos em cada nó.

Como configurar um servidor syslog externo

Para aprender como configurar um servidor syslog externo, consulte"Configurar gerenciamento de log e servidor syslog externo" .

Se você pretende configurar o uso do protocolo TLS ou RELP/TLS, você deve ter os seguintes certificados:

- **Certificados de CA do servidor**: Um ou mais certificados de CA confiáveis para verificar o servidor syslog externo na codificação PEM. Se omitido, o certificado padrão da CA de grade será usado.

- **Certificado de cliente**: O certificado de cliente para autenticação para o servidor syslog externo na codificação PEM.
- **Chave privada do cliente**: Chave privada para o certificado do cliente na codificação PEM.

> Se você usar um certificado de cliente, você também deve usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, você também deve fornecer a senha. Não há benefício significativo de segurança ao usar uma chave privada criptografada porque a chave e a senha devem ser armazenadas; usar uma chave privada não criptografada, se disponível, é recomendado para simplificar.

Como estimar o tamanho do servidor syslog externo

Normalmente, sua grade é dimensionada para alcançar uma taxa de transferência necessária, definida em termos de S3 operações por segundo ou bytes por segundo. Por exemplo, você pode ter um requisito de que sua grade lide com 1.000 S3 operações por segundo, ou 2.000 MB por segundo, de inclusões e recuperações de objetos. Você deve dimensionar seu servidor syslog externo de acordo com os requisitos de dados da sua grade.

Esta seção fornece algumas fórmulas heurísticas que ajudam a estimar a taxa e o tamanho médio de mensagens de log de vários tipos que seu servidor syslog externo precisa ser capaz de lidar, expressas em termos das caraterísticas de desempenho conhecidas ou desejadas da grade (S3 operações por segundo).

Use S3 operações por segundo em fórmulas de estimativa

Se sua grade foi dimensionada para uma taxa de transferência expressa em bytes por segundo, você deve converter esse dimensionamento em S3 operações por segundo para usar as fórmulas de estimativa. Para converter a taxa de transferência de grade, primeiro você deve determinar o tamanho médio do objeto, o que pode ser feito usando as informações em logs e métricas de auditoria existentes (se houver), ou usando seu conhecimento dos aplicativos que usarão o StorageGRID. Por exemplo, se sua grade foi dimensionada para obter uma taxa de transferência de 2.000 MB/segundo e o tamanho médio do objeto é de 2 MB, então sua grade foi dimensionada para ser capaz de lidar com 1.000 S3 operações por segundo (2.000 MB / 2 MB).

> As fórmulas para o dimensionamento externo do servidor syslog nas seções a seguir fornecem estimativas de casos comuns (em vez de estimativas de casos piores). Dependendo da sua configuração e carga de trabalho, você pode ver uma taxa maior ou menor de mensagens syslog ou volume de dados syslog do que as fórmulas predizem. As fórmulas devem ser usadas apenas como diretrizes.

Fórmulas de estimativa para logs de auditoria

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os valores padrão (todas as categorias definidas como normal, exceto armazenamento, que está definido como erro):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Por exemplo, se sua grade for dimensionada para 1.000 S3 operações por segundo, seu servidor syslog

externo deve ser dimensionado para suportar 2.000 mensagens syslog por segundo e deve ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de 1,6 MB por segundo.

Se você sabe mais sobre sua carga de trabalho, estimativas mais precisas são possíveis. Para logs de auditoria, as variáveis adicionais mais importantes são a porcentagem de S3 operações que são puts (vs. GETS), e o tamanho médio, em bytes, dos S3 campos a seguir (abreviações de 4 carateres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Vamos usar P para representar a porcentagem de S3 operações que são puts, onde 0 ≤ P ≤ 1 (assim, para uma carga de trabalho DE 100% PUT, P 1, e para uma carga de trabalho DE 100% GET, P 0).

Vamos usar K para representar o tamanho médio da soma dos nomes de conta S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então o valor de K é 90 (13-13-28-36).

Se você puder determinar valores para P e K, poderá estimar o volume de logs de auditoria que seu servidor syslog externo precisará manipular usando as seguintes fórmulas, partindo do pressuposto de que você deixa os níveis de auditoria definidos para os padrões (todas as categorias definidas como normal, exceto armazenamento, que está definido como erro):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Por exemplo, se sua grade for dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts, e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1.500 mensagens syslog por segundo e deve ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de aproximadamente 1 MB por segundo.

Fórmulas de estimativa para níveis de auditoria não padrão

As fórmulas fornecidas para logs de auditoria assumem o uso de configurações de nível de auditoria padrão (todas as categorias definidas como normal, exceto armazenamento, que é definido como erro). Fórmulas detalhadas para estimar a taxa e o tamanho médio das mensagens de auditoria para configurações de nível de auditoria não padrão não estão disponíveis. No entanto, a tabela a seguir pode ser usada para fazer uma estimativa aproximada da taxa; você pode usar a fórmula de tamanho médio fornecida para logs de auditoria, mas esteja ciente de que é provável que isso resulte em uma estimativa excessiva porque as mensagens de auditoria "extra" são, em média, menores do que as mensagens de auditoria padrão.

Condição	Fórmula
Replicação: Níveis de auditoria todos definidos como Debug ou normal	Taxa de log de auditoria: 8 x S3 taxa de operações
Codificação de apagamento: Níveis de auditoria todos definidos como Debug ou normal	Use a mesma fórmula que para as configurações padrão

Fórmulas de estimativa para eventos de segurança

Os eventos de segurança não estão correlacionados com as operações do S3 e normalmente produzem um volume insignificante de logs e dados. Por estas razões, não são fornecidas fórmulas de estimativa.

Fórmulas de estimativa para logs de aplicativos

Se você não tiver informações sobre sua carga de trabalho S3 além do número de S3 operações por segundo que sua grade deve suportar, você pode estimar o volume de Registros de aplicativos que seu servidor syslog externo precisará lidar com as seguintes fórmulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Assim, por exemplo, se sua grade for dimensionada para 1.000 S3 operações por segundo, seu servidor syslog externo deve ser dimensionado para suportar 3.300 Registros de aplicativos por segundo e ser capaz de receber (e armazenar) dados de log de aplicativos a uma taxa de cerca de 1,2 MB por segundo.

Se você sabe mais sobre sua carga de trabalho, estimativas mais precisas são possíveis. Para logs de aplicativos, as variáveis adicionais mais importantes são a estratégia de proteção de dados (replicação vs. Codificação de apagamento), a porcentagem de operações S3 que são puts (vs. Gets/other) e o tamanho médio, em bytes, dos S3 campos a seguir (abreviações de 4 carateres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	S3 Nome da conta do locatário (remetente da solicitação)	O nome da conta de locatário para o usuário que enviou a solicitação. Vazio para pedidos anónimos.

Código	Campo	Descrição
SBAC	S3 Nome da conta do locatário (proprietário do balde)	O nome da conta do locatário para o proprietário do bucket. Usado para identificar acesso entre contas ou anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em baldes não incluem este campo.

Exemplo de estimativas de dimensionamento

Esta seção explica exemplos de como usar as fórmulas de estimativa para grades com os seguintes métodos de proteção de dados:

- Replicação
- Codificação de apagamento

Se você usar a replicação para proteção de dados

Deixe P representar a porcentagem de S3 operações que são colocadas, onde 0 ≤ P ≤ 1 (assim, para uma carga de trabalho DE 100% PUT, P 1 e para uma carga de trabalho DE 100% GET, P 0).

Deixe K representar o tamanho médio da soma dos S3 nomes de conta, S3 bucket e S3 key. Suponha que o nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13-13-28-36).

Se você puder determinar valores para P e K, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de lidar com as seguintes fórmulas.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 1800 Registros de aplicativos por segundo e receberá (e normalmente armazenará) dados de aplicativos a uma taxa de 0,5 MB por segundo.

Se você usar codificação de apagamento para proteção de dados

Deixe P representar a porcentagem de S3 operações que são colocadas, onde 0 ≤ P ≤ 1 (assim, para uma carga de trabalho DE 100% PUT, P 1 e para uma carga de trabalho DE 100% GET, P 0).

Deixe K representar o tamanho médio da soma dos S3 nomes de conta, S3 bucket e S3 key. Suponha que o

nome da conta S3 seja sempre my-S3-account (13 bytes), buckets têm nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes), e objetos têm chaves de comprimento fixo como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). Então K tem um valor de 90 (13-13-28-36).

Se você puder determinar valores para P e K, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de lidar com as seguintes fórmulas.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Assim, por exemplo, se sua grade é dimensionada para 1.000 S3 operações por segundo, sua carga de trabalho é de 50% puts e seus nomes de conta S3, nomes de bucket e nomes de objetos têm uma média de 90 bytes, seu servidor syslog externo deve ser dimensionado para suportar 2.250 Registros de aplicativos por segundo e deve ser capaz de receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Configurar gerenciamento de log

Conforme necessário, configure níveis de auditoria, cabeçalhos de protocolo e o local de mensagens e logs de auditoria.

Todos os nós do StorageGRID geram mensagens de auditoria e logs para rastrear atividades e eventos do sistema. Mensagens e logs de auditoria são ferramentas essenciais para monitoramento e solução de problemas.

Opcionalmente, você pode"configurar um servidor syslog externo" para salvar informações de auditoria remotamente. Usar um servidor externo minimiza o impacto no desempenho do registro de mensagens de auditoria sem reduzir a integridade dos dados de auditoria. Um servidor syslog externo é especialmente útil se você tiver uma grade grande, usar vários tipos de aplicativos S3 ou quiser reter todos os dados de auditoria.

Antes de começar

- Você está conetado ao Gerenciador de Grade usando um "navegador da web suportado".
- Você tem o "Permissão de manutenção ou acesso root".
- Se você planeja configurar um servidor syslog externo, você revisou e seguiu o"considerações para usar um servidor syslog externo" .
- Se você planeja configurar um servidor syslog externo usando o protocolo TLS ou RELP/TLS, você terá a CA de servidor e os certificados de cliente necessários e a chave privada do cliente.

Alterar os níveis de mensagens de auditoria

Você pode definir um nível de auditoria diferente para cada uma das seguintes categorias de mensagens no log de auditoria:

Categoria de auditoria	Predefinição	Mais informações
Sistema	Normal	"Mensagens de auditoria do sistema"

Categoria de auditoria	Predefinição	Mais informações
Armazenamento	Erro	"Mensagens de auditoria de armazenamento de objetos"
Gerenciamento	Normal	"Mensagem de auditoria de gerenciamento"
O cliente lê	Normal	"O cliente lê mensagens de auditoria"
O cliente escreve	Normal	"O cliente escreve mensagens de auditoria"
ILM	Normal	"Mensagens de auditoria ILM"
Replicação entre grade	Erro	"CGRR: Solicitação de replicação de Grade cruzada"

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

Passos

1. Selecione **Configuração** > **Monitoramento** > **Gerenciamento de logs**.
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).
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.

Se você não precisar de um registro detalhado das operações de leitura do cliente para seus aplicativos S3, opcionalmente altere a configuração **Leituras do cliente** para **Erro** para diminuir o número de mensagens de auditoria registradas no log de auditoria.

3. Selecione **Guardar**.

Definir cabeçalhos de solicitação HTTP

Opcionalmente, você pode definir quaisquer cabeçalhos de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação do cliente.

Passos

1. Na seção **cabeçalhos de protocolo de auditoria**, defina os cabeçalhos de solicitação HTTP que você deseja incluir nas mensagens de auditoria de leitura e gravação do cliente.

   Use um asterisco (**) como curinga para corresponder a zero ou mais carateres. Use a sequência de escape (**) para corresponder a um asterisco literal.

2. Selecione **Adicionar outro cabeçalho** para criar cabeçalhos adicionais, se necessário.

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

   > Os cabeçalhos de solicitação do protocolo de auditoria serão registrados somente se o nível de auditoria para **Leituras do cliente** ou **Gravações do cliente** não for **Desativado**.

3. Selecione **Guardar**

Configurar local do log

Por padrão, as mensagens e os logs de auditoria são salvos nos nós onde são gerados. Eles são rotacionados periodicamente e eventualmente excluídos para evitar que consumam espaço excessivo em disco. Se você quiser salvar mensagens de auditoria e um subconjunto de logs externamente,use um servidor syslog externo .

Se você quiser salvar os arquivos de log internamente, escolha um locatário e um bucket para armazenamento de log e habilite o arquivamento de log.

Use um servidor syslog externo

Opcionalmente, você pode configurar um servidor syslog externo para salvar logs de auditoria, logs de aplicativos e logs de eventos de segurança em um local fora da grade.

> Se você não quiser usar um servidor syslog externo, pule esta etapa e vá paraSelecione o local do log .

> Se as opções de configuração disponíveis neste procedimento não forem flexíveis o suficiente para atender aos seus requisitos, opções de configuração adicionais podem ser aplicadas usando os `audit-destinations` endpoints, que estão na seção API privada do "API de gerenciamento de grade". Por exemplo, você pode usar a API se quiser usar diferentes servidores syslog para diferentes grupos de nós.

Insira as informações do syslog

Acesse o assistente Configurar servidor syslog externo e forneça as informações que o StorageGRID precisa para acessar o servidor syslog externo.

Passos

1. Na guia Nó local e servidor externo, selecione **Configurar servidor syslog externo**. Ou, se você configurou anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

   O assistente Configurar servidor syslog externo é exibido.

2. Para a etapa **Enter syslog info** do assistente, insira um nome de domínio totalmente qualificado válido ou um endereço IPv4 ou IPv6 para o servidor syslog externo no campo **Host**.
3. Insira a porta de destino no servidor syslog externo (deve ser um número inteiro entre 1 e 65535). A porta padrão é 514.
4. Selecione o protocolo usado para enviar informações de auditoria para o servidor syslog externo.

   Recomenda-se a utilização de **TLS** ou **RELP/TLS**. Você deve carregar um certificado de servidor para usar qualquer uma dessas opções. O uso de certificados ajuda a proteger as conexões entre a grade e o servidor syslog externo. Para obter mais informações, "Gerenciar certificados de segurança"consulte .

   Todas as opções de protocolo exigem suporte e configuração do servidor syslog externo. Você deve escolher uma opção compatível com o servidor syslog externo.

   > ⓘ O Protocolo de Registro de Eventos confiável (RELP) estende a funcionalidade do protocolo syslog para fornecer entrega confiável de mensagens de eventos. O uso do RELP pode ajudar a evitar a perda de informações de auditoria se o servidor syslog externo tiver que reiniciar.

5. Selecione **continuar**.
6. se você selecionou **TLS** ou **RELP/TLS**, carregue os certificados CA do servidor, o certificado de cliente e a chave privada do cliente.
   a. Selecione **Procurar** para o certificado ou chave que deseja usar.
   b. Selecione o arquivo de certificado ou chave.
   c. Selecione **Open** para carregar o ficheiro.

      Uma verificação verde é exibida ao lado do nome do arquivo do certificado ou chave, notificando que ele foi carregado com sucesso.

7. Selecione **continuar**.

Gerenciar o conteúdo do syslog

Você pode selecionar quais informações enviar para o servidor syslog externo.

Passos

1. Para a etapa **Manage syslog Content** do assistente, selecione cada tipo de informação de auditoria que deseja enviar para o servidor syslog externo.
   - * Enviar logs de auditoria*: Envia eventos do StorageGRID e atividades do sistema
   - * Enviar eventos de segurança*: Envia eventos de segurança, como quando um usuário não autorizado tenta entrar ou um usuário faz login como root
   - * Enviar logs de aplicativos*: Envia "Arquivos de log do software StorageGRID" úteis para solução de problemas, incluindo:
     - `bycast-err.log`
     - `bycast.log`

- `jaeger.log`
- `nms.log` (Somente nós de administração)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

◦ * Enviar logs de acesso*: Envia logs de acesso HTTP para solicitações externas ao Gerenciador de Grade, Gerenciamento do locatário, pontos de extremidade do balanceador de carga configurados e solicitações de federação de grade de sistemas remotos.

2. Use os menus suspensos para selecionar a gravidade e a facilidade (tipo de mensagem) para cada categoria de informações de auditoria que você deseja enviar.

   Definir os valores de gravidade e facilidade pode ajudá-lo a agregar os logs de maneiras personalizáveis para facilitar a análise.

   a. Para **severidade**, selecione **passagem** ou selecione um valor de gravidade entre 0 e 7.

      Se selecionar um valor, o valor selecionado será aplicado a todas as mensagens deste tipo. As informações sobre diferentes gravidades serão perdidas se você substituir a gravidade com um valor fixo.

Gravidade	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de gravidade que quando foi registrada localmente no nó: • Para logs de auditoria, a gravidade é "info". • Para eventos de segurança, os valores de gravidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, as severidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA dá um valor de "info", enquanto parar intencionalmente o serviço SSM ou RSM dá um valor de "notice". • Para os logs de acesso, a gravidade é "INFO".
0	Emergência: O sistema não pode ser utilizado
1	Alerta: A ação deve ser tomada imediatamente
2	Crítico: Condições críticas
3	Erro: Condições de erro
4	Aviso: Condições de aviso
5	Aviso: Condição normal, mas significativa

Gravidade	Descrição
6	Informativo: Mensagens informativas
7	Debug: Mensagens no nível de depuração

b. Para **Facilty**, selecione **Passthrough** ou selecione um valor de instalação entre 0 e 23.

Se você selecionar um valor, ele será aplicado a todas as mensagens desse tipo. Informações sobre diferentes instalações serão perdidas se você substituir as instalações com um valor fixo.

Instalação	Descrição
Passagem	Cada mensagem enviada para o syslog externo para ter o mesmo valor de instalação que quando foi registrada localmente no nó: • Para logs de auditoria, a instalação enviada para o servidor syslog externo é "local7". • Para eventos de segurança, os valores das instalações são gerados pela distribuição linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados para o servidor syslog externo têm os seguintes valores de instalação: ◦ `bycast.log`: usuário ou daemon ◦ `bycast-err.log`: usuário, daemon, local3 ou local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6 • Para logs de acesso, a instalação enviada para o servidor syslog externo é "local0".
0	kern (mensagens do kernel)
1	utilizador (mensagens no nível do utilizador)
2	e-mail
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)
5	syslog (mensagens geradas internamente pelo syslogd)

Instalação	Descrição
6	lpr (subsistema de impressora de linha)
7	notícias (subsistema de notícias de rede)
8	UUCP
9	cron (daemon de relógio)
10	segurança (mensagens de segurança/autorização)
11	FTP
12	NTP
13	logaudit (auditoria de log)
14	alerta de registo (alerta de registo)
15	relógio (daemon de relógio)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selecione **continuar**.

Enviar mensagens de teste

Antes de começar a usar um servidor syslog externo, você deve solicitar que todos os nós da grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para ajudá-lo a validar toda a infraestrutura de coleta de logs antes de se comprometer a enviar dados para o servidor syslog externo.

Não use a configuração do servidor syslog externo até confirmar que o servidor syslog externo recebeu uma mensagem de teste de cada nó na grade e que a mensagem foi processada conforme esperado.

Passos

1. Se você não quiser enviar mensagens de teste porque você tem certeza de que seu servidor syslog externo está configurado corretamente e pode receber informações de auditoria de todos os nós em sua grade, selecione **Skip and finish**.

   Um banner verde indica que a configuração foi salva.

2. Caso contrário, selecione **Enviar mensagens de teste** (recomendado).

   Os resultados do teste aparecem continuamente na página até que você pare o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuam sendo enviadas para os destinos configurados anteriormente.

3. Se você receber algum erro durante a configuração do servidor syslog ou em tempo de execução, corrija-o e selecione **Enviar mensagens de teste** novamente.

   "Solucionar problemas de um servidor syslog externo"Consulte para ajudá-lo a resolver quaisquer erros.

4. Aguarde até que você veja um banner verde indicando que todos os nós passaram no teste.
5. Verifique o servidor syslog para determinar se as mensagens de teste estão sendo recebidas e processadas conforme esperado.

   Se você estiver usando UDP, verifique toda a sua infraestrutura de coleta de logs. O protocolo UDP não permite uma detecção de erros tão rigorosa quanto os outros protocolos.

6. Selecione **Parar e terminar**.

   Você será devolvido à página **servidor de auditoria e syslog**. Um banner verde indica que a configuração do servidor syslog foi salva.

   As informações de auditoria do StorageGRID não são enviadas ao servidor syslog externo até que você selecione um destino que inclua o servidor syslog externo.

Selecione o local do log

Você pode especificar onde os logs de auditoria, logs de eventos de segurança,"Logs do aplicativo StorageGRID" , e os logs de acesso são enviados.

O StorageGRID usa o padrão de destinos de auditoria de nó local e armazena as informações de auditoria no `/var/local/log/localaudit.log`.

Ao usar `/var/local/log/localaudit.log`o , as entradas de log de auditoria do Gerenciador de Grade e do Gerenciador de locatário podem ser enviadas para um nó de armazenamento. Você pode encontrar qual nó tem as entradas mais recentes usando o `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.

Alguns destinos só estão disponíveis se tiver configurado um servidor syslog externo.

Passos

1. Selecione **Local do log** > **Nó local e servidor externo**.
2. Para alterar o local do log para os tipos de log, selecione uma opção diferente.

Somente nós locais e **servidor syslog externo** normalmente fornecem melhor desempenho.

Opção	Descrição
Somente nós locais (padrão)	Mensagens de auditoria, logs de eventos de segurança e logs de aplicativos não são enviados aos nós de administração. Em vez disso, eles são salvos apenas nos nós que os geraram ("o nó local"). As informações de auditoria geradas em cada nó local são armazenadas em `/var/local/log/localaudit.log` . **Observação**: O StorageGRID remove periodicamente logs locais em uma rotação para liberar espaço. Quando o arquivo de log de um nó atinge 1 GB, o arquivo existente é salvo e um novo arquivo de log é iniciado. O limite de rotação do log é de 21 arquivos. Quando a 22ª versão do arquivo de log é criada, o arquivo de log mais antigo é excluído. Em média, cerca de 20 GB de dados de log são armazenados em cada nó. Para armazenar logs por um longo período de tempo,use um locatário e um bucket para armazenamento de logs .
Nós de administração/nós locais	As mensagens de auditoria são enviadas para o log de auditoria nos nós de administração, e os logs de eventos de segurança e de aplicativos são armazenados nos nós que as geraram. As informações de auditoria são armazenadas nos seguintes arquivos: • Nós de administração (primários e não primários): `/var/local/audit/export/audit.log` • Todos os nós: O `/var/local/log/localaudit.log` arquivo está normalmente vazio ou ausente. Ele pode conter informações secundárias, como uma cópia adicional de algumas mensagens.

Opção	Descrição
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas nos nós locais(`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é habilitada depois que você tiverconfigurou um servidor syslog externo .
Nós de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria(`/var/local/audit/export/audit.log`) em nós de administração, e as informações de auditoria são enviadas ao servidor syslog externo e salvas no nó local(`/var/local/log/localaudit.log`). O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é habilitada depois que você tiverconfigurou um servidor syslog externo .

3. Selecione **Guardar**.

   É apresentada uma mensagem de aviso.

4. Selecione **OK** para confirmar que deseja alterar o destino para informações de auditoria.

   Os novos registos são enviados para os destinos selecionados. Os registos existentes permanecem na sua localização atual.

Use um balde

Os logs são rotacionados periodicamente. Use um bucket S3 na mesma grade para armazenar logs por um longo período de tempo.

1. Selecione **Local do log** > **Usar um bucket**.
2. Marque a caixa de seleção **Ativar logs de arquivamento**.
3. Se o locatário e o bucket listados não forem os que você deseja usar, selecione **Alterar locatário e bucket** e, em seguida, selecione **Criar locatário e bucket** ou **Selecionar locatário e bucket**.

Criar inquilino e bucket

a. Digite um novo nome de inquilino.
b. Digite e confirme uma senha para o novo inquilino.
c. Digite um novo nome para o bucket.
d. Selecione **Criar e habilitar**.

Selecione locatário e intervalo

a. Selecione um nome de inquilino no menu suspenso.
b. Selecione um bucket no menu suspenso.
c. Selecione **Selecionar e habilitar**.

4. Selecione **Guardar**.

   Os logs serão armazenados no locatário e no bucket que você especificou. O nome da chave do objeto para os logs está neste formato:

   ```
   system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
   {last_modified_time}.gz
   ```

   Por exemplo:

   ```
   system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
   ```

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.