Configurar destinos de mensagens e logs de auditoria

StorageGRID software

NetApp
December 03, 2025

Índice

Configurar destinos de mensagens e logs de auditoria

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. Usar 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 do pacote de mensagens syslog de saída é compatível com RFC 3164.

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

- Registros de auditoria contendo as mensagens de auditoria geradas durante a operação normal do sistema
- Eventos relacionados à segurança, como logins e escalonamentos para root
- Logs de aplicativos que podem ser solicitados caso seja necessário abrir um caso de suporte para solucionar um problema que você encontrou

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 em seus nós de administração porque as informações de auditoria são transferidas diretamente dos vários nós de armazenamento para o servidor syslog externo, sem precisar 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 servidores syslog externos.

> 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 mensagens de auditoria e servidor syslog externo" .

Se você planeja 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 Grid CA padrão será usado.

- **Certificado do cliente**: O certificado do cliente para autenticação no 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, também deverá usar uma chave privada de cliente. Se você fornecer uma chave privada criptografada, também deverá fornecer a senha. Não há benefício significativo de segurança no uso de 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 atingir uma taxa de transferência necessária, definida em termos de operações S3 por segundo ou bytes por segundo. Por exemplo, você pode ter um requisito para que sua grade manipule 1.000 operações S3 por segundo, ou 2.000 MB por segundo, de ingestões 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 você a estimar a taxa e o tamanho médio de mensagens de log de vários tipos que seu servidor syslog externo precisa ser capaz de manipular, expressos em termos das características de desempenho conhecidas ou desejadas da grade (operações S3 por segundo).

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

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

Fórmulas de estimativa para registros de auditoria

Se você não tiver nenhuma informação sobre sua carga de trabalho do S3 além do número de operações do S3 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, supondo que você deixe os Níveis de Auditoria definidos com os valores padrão (todas as categorias definidas como Normal, exceto Armazenamento, que é 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 operações S3 por segundo, seu servidor syslog externo deverá ser dimensionado para suportar 2.000 mensagens syslog por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de log de auditoria a uma taxa de 1,6 MB por segundo.

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

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Vamos usar P para representar a porcentagem de operações S3 que são PUTs, onde $0 \leq P \leq 1$ (portanto, 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 contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham 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, supondo que você deixe os Níveis de Auditoria definidos como padrões (todas as categorias definidas como Normal, exceto Armazenamento, que é 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 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 1.500 mensagens syslog por segundo e deverá 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 pressupõem 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 de 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 isso provavelmente resultará em uma superestimativa porque as mensagens de auditoria "extras" são, em média, menores que as mensagens de auditoria padrão.

Doença	Fórmula
Replicação: níveis de auditoria todos definidos como Depuração ou Normal	Taxa de log de auditoria = 8 x taxa de operações S3
Codificação de eliminação: níveis de auditoria todos definidos como Depuração ou Normal	Use a mesma fórmula das configurações padrão

Fórmulas de estimativa para eventos de segurança

Eventos de segurança não estão correlacionados com operações do S3 e normalmente produzem um volume insignificante de logs e dados. Por essas razões, nenhuma fórmula de estimativa é fornecida.

Fórmulas de estimativa para logs de aplicação

Se você não tiver nenhuma informação sobre sua carga de trabalho do S3 além do número de operações do S3 por segundo que sua grade deve suportar, você pode estimar o volume de logs de aplicativos que seu servidor syslog externo precisará manipular usando 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 operações S3 por segundo, seu servidor syslog externo deverá ser dimensionado para suportar 3.300 logs 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 souber mais sobre sua carga de trabalho, estimativas mais precisas serão possíveis. Para logs de aplicativos, as variáveis adicionais mais importantes são a estratégia de proteção de dados (replicação vs. codificação de eliminação), a porcentagem de operações S3 que são PUTs (vs. GETs/outros) e o tamanho médio, em bytes, dos seguintes campos S3 (as abreviações de 4 caracteres usadas na tabela são nomes de campos de log de auditoria):

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.

Código	Campo	Descrição
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.

Exemplos de estimativas de dimensionamento

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

- Replicação
- Codificação de apagamento

Se você usar replicação para proteção de dados

Deixe P representar a porcentagem de operações S3 que são PUTs, onde 0 ≤ P ≤ 1 (portanto, 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 nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo como /my/application/bucket-12345 (28 bytes) e os objetos tenham 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, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de manipular usando 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 for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 1.800 logs 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 eliminação para proteção de dados

Deixe P representar a porcentagem de operações S3 que são PUTs, onde 0 ≤ P ≤ 1 (portanto, 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 nomes de contas S3, bucket S3 e chave S3. Suponha que o nome da conta S3 seja sempre my-s3-account (13 bytes), os buckets tenham nomes de comprimento fixo

como /my/application/bucket-12345 (28 bytes) e os objetos tenham 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, poderá estimar o volume de logs de aplicativos que seu servidor syslog externo terá que ser capaz de manipular usando 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
```

Portanto, por exemplo, se sua grade for dimensionada para 1.000 operações S3 por segundo, sua carga de trabalho for 50% PUTs e seus nomes de conta S3, nomes de bucket e nomes de objeto tiverem em média 90 bytes, seu servidor syslog externo deverá ser dimensionado para suportar 2.250 logs de aplicativos por segundo e deverá ser capaz de receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Configurar mensagens de auditoria e servidor syslog externo

Você pode configurar uma série de configurações relacionadas às mensagens de auditoria. Você pode ajustar o número de mensagens de auditoria registradas; definir quaisquer cabeçalhos de solicitação HTTP que deseja incluir nas mensagens de auditoria de leitura e gravação do cliente; configurar um servidor syslog externo; e especificar para onde os logs de auditoria, logs de eventos de segurança e logs de software StorageGRID são enviados.

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

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. Ver"Configurar mensagens de auditoria e servidor syslog externo" para mais detalhes.

Antes de começar

- Você está conectado ao Grid Manager usando um"navegador da web compatível" .
- Você tem o"Permissão de acesso de manutenção ou root" .
- Se você planeja configurar um servidor syslog externo, você revisou o"considerações para usar um servidor syslog externo" e garantiu que o servidor tenha capacidade suficiente para receber e armazenar os arquivos de log.
- Se você planeja configurar um servidor syslog externo usando o protocolo TLS ou RELP/TLS, você tem a CA do servidor e os certificados de cliente necessários e a chave privada do cliente.

Alterar 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	Configuração padrão	Mais informações
Sistema	Normal	"Mensagens de auditoria do sistema"
Armazenar	Erro	"Mensagens de auditoria de armazenamento de objetos"
Gerenciamento	Normal	"Mensagem de auditoria de gestão"
O cliente lê	Normal	"O cliente leu mensagens de auditoria"
O cliente escreve	Normal	"O cliente escreve mensagens de auditoria"
ILM	Normal	"Mensagens de auditoria do ILM"
Replicação entre grades	Erro	"CGRR: Solicitação de replicação entre redes"

Esses padrões se aplicam se você instalou inicialmente o StorageGRID usando a versão 10.3 ou posterior. Se você usou inicialmente 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** > **Servidor de auditoria e syslog**.
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	Mensagens transacionais padrão são registradas — as mensagens listadas nestas instruções para a categoria.
Depurar	Obsoleto. Este nível se comporta da mesma forma que o nível de auditoria Normal.

As mensagens incluídas para qualquer nível específico 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 **Salvar**.

   Um banner verde indica que sua configuração foi salva.

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. Esses cabeçalhos de protocolo se aplicam somente a solicitações S3.

Passos

1. Na seção **Cabeçalhos do 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 caracteres. 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 no 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 **Salvar**

   Um banner verde indica que sua configuração foi salva.

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 sua grade.

> Se você não quiser usar um servidor syslog externo, pule esta etapa e vá paraSelecione destinos de informações de auditoria .

> Se as opções de configuração disponíveis neste procedimento não forem flexíveis o suficiente para atender às suas necessidades, opções de configuração adicionais podem ser aplicadas usando o `audit-destinations` endpoints, que estão na seção de 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 página Auditoria e servidor syslog, 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 **Inserir informações do syslog** 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.

   É recomendado usar **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 sua grade e o servidor syslog externo. Para obter mais informações, consulte "Gerenciar certificados de segurança" .

   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 Reliable Event Logging Protocol (RELP) estende a funcionalidade do protocolo syslog para fornecer entrega confiável de mensagens de eventos. Usar o RELP pode ajudar a evitar a perda de informações de auditoria caso seu servidor syslog externo precise reiniciar.

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

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

7. Selecione **Continuar**.

Gerenciar conteúdo do syslog

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

Passos

1. Para a etapa **Gerenciar conteúdo do syslog** do assistente, selecione cada tipo de informação de auditoria que deseja enviar ao 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 fazer login ou um usuário faz login como root

- **Enviar logs de aplicação**: Envia"Arquivos de log do software StorageGRID" útil 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 Grid Manager, Tenant Manager, endpoints de 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 informação de auditoria que você deseja enviar.

   Definir valores de gravidade e facilidade pode ajudar você a agregar os logs de maneiras personalizáveis para facilitar a análise.

   a. Para **Gravidade**, selecione **Passagem** ou selecione um valor de gravidade entre 0 e 7.

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

Gravidade	Descrição
Passagem	Cada mensagem enviada ao syslog externo deve ter o mesmo valor de gravidade de 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 gravidades variam entre "info" e "notice", dependendo do problema. Por exemplo, adicionar um servidor NTP e configurar um grupo HA fornece um valor de "info", enquanto interromper intencionalmente o serviço SSM ou RSM fornece um valor de "notice". • Para logs de acesso, a gravidade é "info".
0	Emergência: O sistema está inutilizável
1	Alerta: Ação deve ser tomada imediatamente
2	Crítico: Condições críticas

Gravidade	Descrição
3	Erro: Condições de erro
4	Aviso: Condições de aviso
5	Aviso: Condição normal, mas significativa
6	Informativo: Mensagens informativas
7	Depuração: mensagens de nível de depuração

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

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

Instalação	Descrição
Passagem	Cada mensagem enviada ao syslog externo deve ter o mesmo valor de recurso de quando foi registrada localmente no nó: • Para logs de auditoria, o recurso enviado ao servidor syslog externo é "local7". • Para eventos de segurança, os valores de facilidade são gerados pela distribuição Linux nos nós. • Para logs de aplicativos, os logs de aplicativos enviados ao servidor syslog externo têm os seguintes valores de facilidade: ◦ `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, o recurso enviado ao servidor syslog externo é "local0".
0	kern (mensagens do kernel)
1	usuário (mensagens em nível de usuário)
2	correspondência

Instalação	Descrição
3	daemon (daemons do sistema)
4	auth (mensagens de segurança/autorização)
5	syslog (mensagens geradas internamente pelo syslogd)
6	lpr (subsistema de impressora de linha)
7	notícias (subsistema de notícias da rede)
8	UUCP
9	cron (daemon do relógio)
10	segurança (mensagens de segurança/autorização)
11	FTP
12	NTP
13	logaudit (auditoria de log)
14	logalert (alerta de registro)
15	relógio (daemon do 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 na sua grade enviem mensagens de teste para o servidor syslog externo. Você deve usar essas mensagens de teste para ajudar a validar toda a sua 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 sua grade e que a mensagem foi processada conforme o esperado.

Passos

1. Se você não quiser enviar mensagens de teste porque 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 **Ignorar e concluir**.

   Um banner verde indica que a configuração foi salva.

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

   Os resultados dos testes aparecem continuamente na página até você interromper o teste. Enquanto o teste estiver em andamento, suas mensagens de auditoria continuarão 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.

   Ver"Solucionar problemas de um servidor syslog externo" para ajudar você a resolver quaisquer erros.

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

   Você retornará à página **Auditoria e servidor 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 destinos de informações de auditoria

Você pode especificar onde os logs de auditoria, logs de eventos de segurança e"Registros do software StorageGRID" são enviados.

O StorageGRID assume como padrão os destinos de auditoria de nós locais e armazena as informações de auditoria em `/var/local/log/localaudit.log`.

Ao usar `/var/local/log/localaudit.log`, as entradas de log de auditoria do Grid Manager e do Tenant Manager podem ser enviadas para um nó de armazenamento. Você pode descobrir 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 estarão disponíveis se você tiver configurado um servidor syslog externo.

Passos

1. Na página Auditoria e servidor syslog, selecione o destino para as informações de auditoria.

Somente nós locais e **servidor syslog externo** geralmente oferecem 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.
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 logs de aplicativos são armazenados nos nós que os 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` o arquivo normalmente está vazio ou ausente. Pode conter informações secundárias, como uma cópia adicional de algumas mensagens.
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 é habilitada somente após você configurar um servidor syslog externo.

Opção	Descrição
Nó 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 é habilitada somente após você configurar um servidor syslog externo.

2. Selecione **Salvar**.

   Uma mensagem de aviso é exibida.

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

   Um banner verde indica que a configuração de auditoria foi salva.

   Novos logs são enviados para os destinos selecionados. Os registros existentes permanecem em seu local atual.

Informações sobre direitos autorais

Informações sobre marcas comerciais