Use um servidor syslog externo

StorageGRID

NetApp
March 12, 2025

Índice

Use um servidor syslog externo . . . 1
Considerações para servidor syslog externo . . . 1
O que é um servidor syslog externo? . . . 1
Como estimar o tamanho do servidor syslog externo . . . 1
Exemplo de estimativas de dimensionamento . . . 4
Configurar um servidor syslog externo . . . 5
Acesse o assistente de configuração do servidor syslog . . . 6
Selecione destinos de informações de auditoria . . . 15

Use um servidor syslog externo

Considerações para servidor syslog externo

Use as diretrizes a seguir para estimar o tamanho do servidor syslog externo de que você precisa.

O que é 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 configurar os destinos das informações de auditoria para que você possa reduzir o tráfego de rede em seus nós de administração e gerenciar as informações com mais eficiência. 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

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	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets não incluem este campo.

Vamos usar P para representar a porcentagem de S3 operações que são puts, onde $0 \leq P \leq 1$ (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: Taxa de operações de 8 x S3
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 são 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.
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	S3 balde	O nome do bucket S3.
S3KY	Tecla S3	O nome da chave S3, não incluindo o nome do intervalo. As operações em buckets 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 receber (e normalmente armazenar) dados de aplicativos a uma taxa de 0,6 MB por segundo.

Para obter mais informações sobre como configurar os níveis de mensagens de auditoria e um servidor syslog externo, consulte o seguinte:

- Configurar um servidor syslog externo
- Configurar mensagens de auditoria e destinos de log

Configurar um servidor syslog externo

Se você quiser salvar logs de auditoria, logs de aplicativos e logs de eventos de segurança em um local fora da grade, use este procedimento para configurar um servidor syslog externo.

O que você vai precisar

- Você está conetado ao Gerenciador de Grade usando um navegador da web suportado.
- Você tem permissões de Manutenção ou Acesso root.
- Você tem um servidor syslog com a capacidade de receber e armazenar os arquivos de log. Para obter mais informações, Considerações para servidor syslog externoconsulte .
- Você tem as certificações de servidor e cliente corretas se planeja usar TLS ou RELP/TLS.

Sobre esta tarefa

Se você quiser enviar informações de auditoria para um servidor syslog externo, primeiro você deve configurar o servidor externo.

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 8192 bytes são truncados no final da mensagem para estar em conformidade com as limitações comuns em implementações de servidor syslog externo.

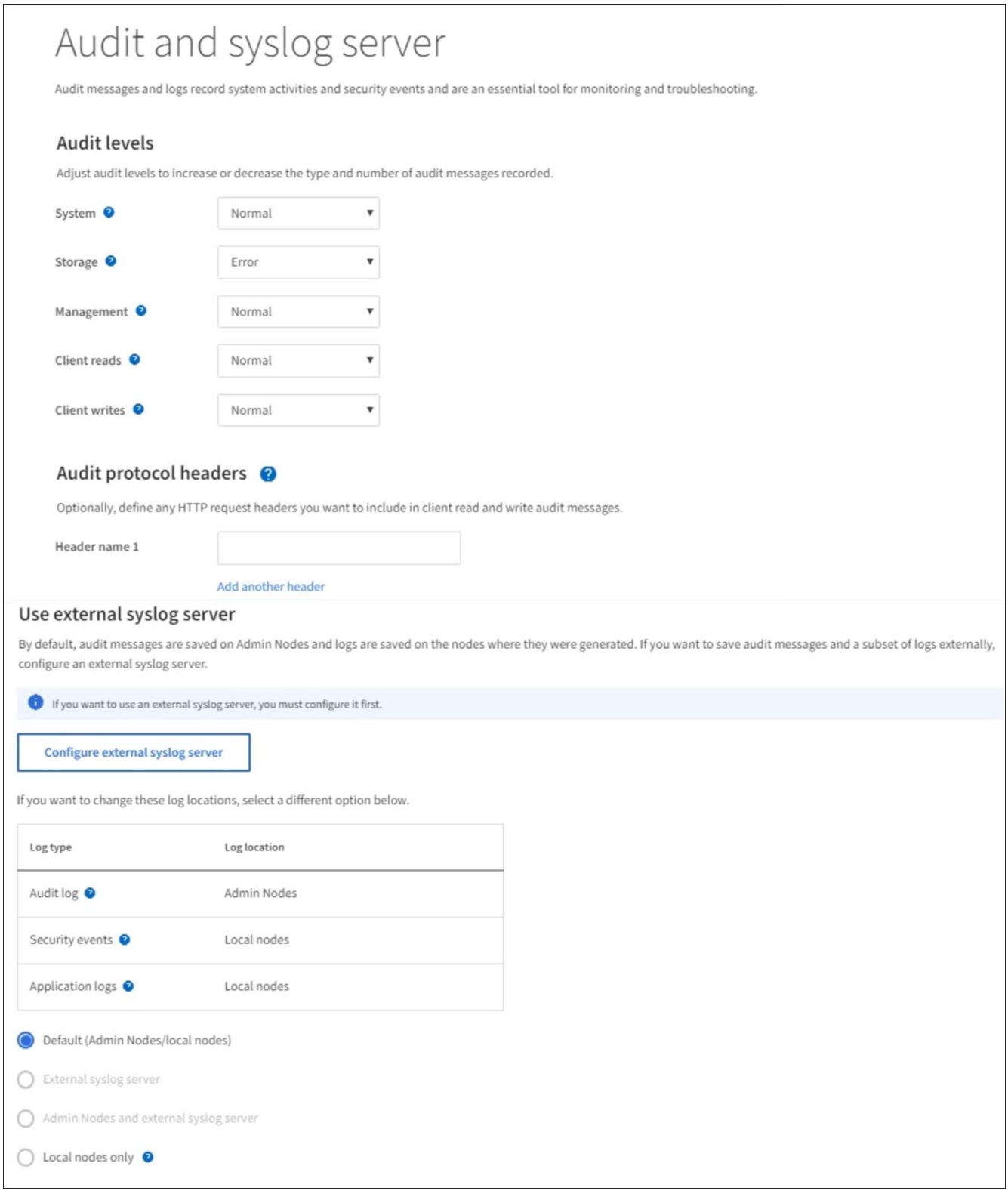
> Para maximizar as opções de recuperação completa de dados em caso de falha do servidor syslog externo, até 20GB Registros locais de Registros de auditoria (localaudit.log) são mantidos em cada nó.

> 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 endpoints privados da API `audit-destinations`. Por exemplo, é possível usar diferentes servidores syslog para diferentes grupos de nós.

Acesse o assistente de configuração do servidor syslog

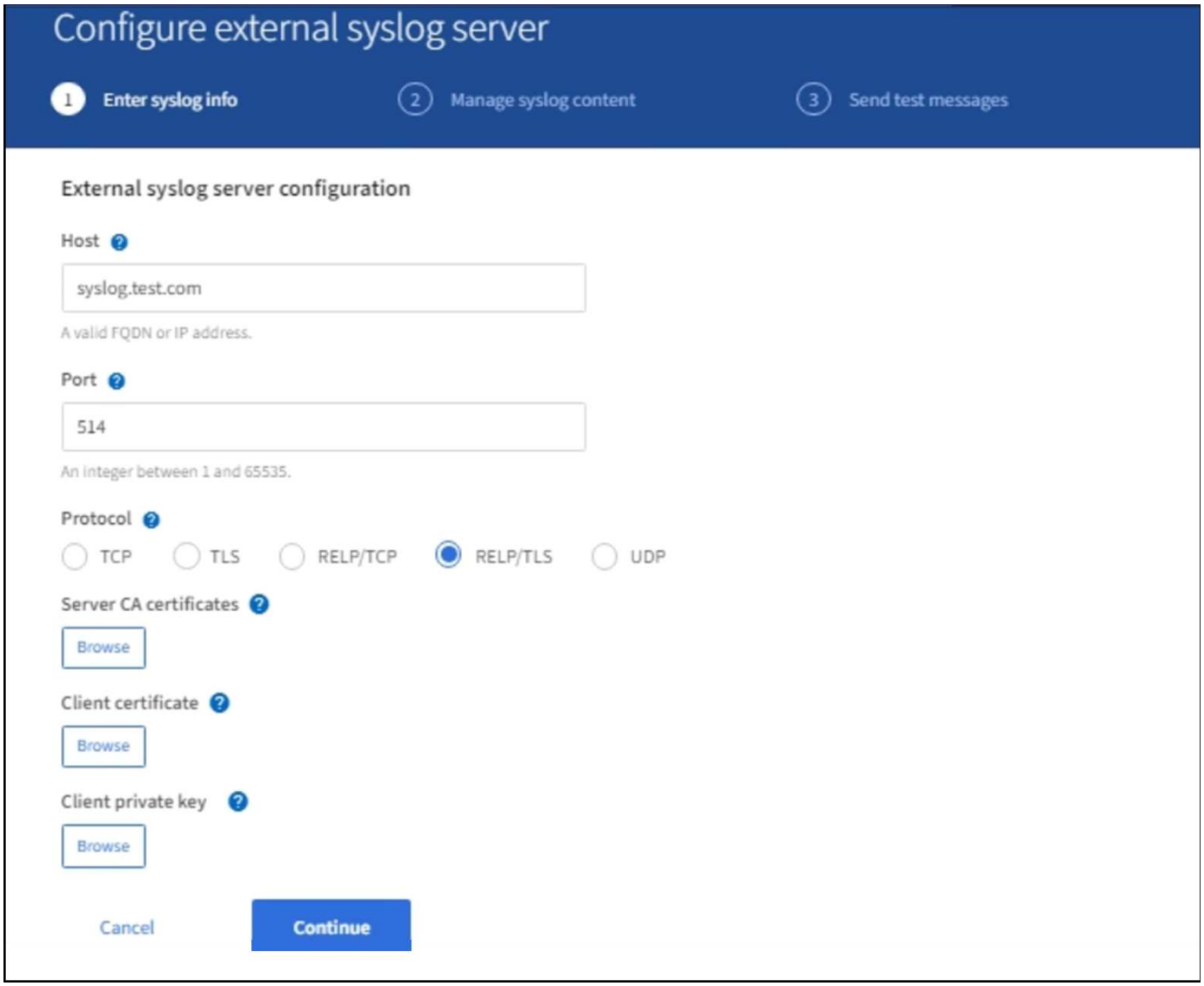
Passos

1. Selecione **CONFIGURATION Monitoring Audit and syslog Server**.



2. Na página servidor de auditoria e syslog, selecione **Configurar servidor syslog externo**. Se tiver configurado anteriormente um servidor syslog externo, selecione **Editar servidor syslog externo**.

Insira informações do syslog



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

   TLS ou RELP/TLS é recomendado. 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, Use os certificados de segurança do StorageGRIDconsulte .

   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.

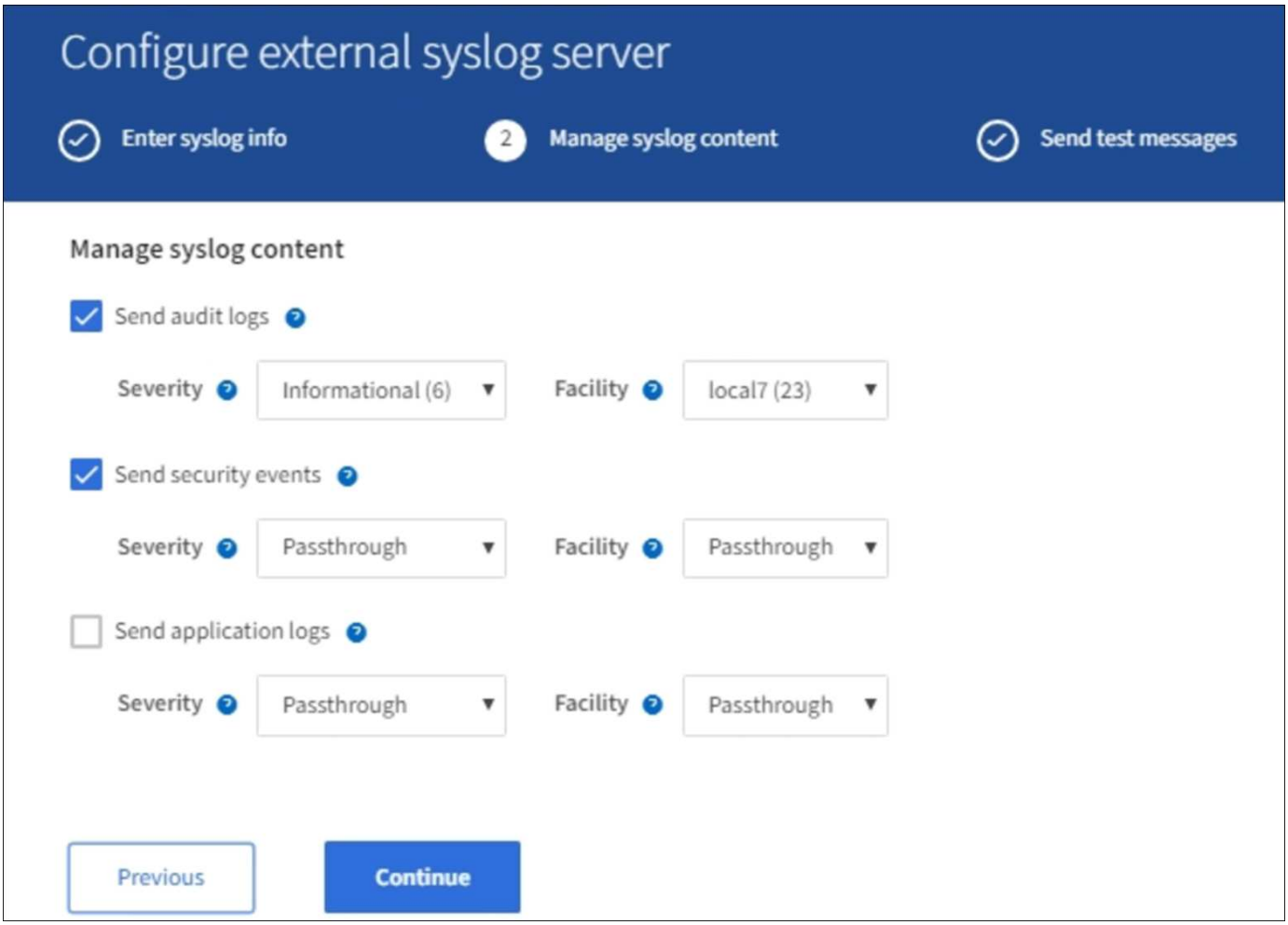
4. Selecione **continuar**.
5. se você selecionou **TLS** ou **RELP/TLS**, faça o upload dos seguintes certificados:
   - **Certificados de CA do servidor**: Um ou mais certificados de CA confiáveis para verificar o servidor syslog externo (na codificação PEM). Se omitido, o certificado padrão da CA de grade será usado. O arquivo que você carregar aqui pode ser um pacote de CA.
   - **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.

   i. Selecione **Procurar** para o certificado ou chave que deseja usar.
   ii. Selecione o ficheiro de certificado ou o ficheiro de chave.
   iii. 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.
6. Selecione **continuar**.

Gerenciar o conteúdo do syslog



1. Selecione cada tipo de informação de auditoria que pretende enviar para o servidor syslog externo.
   - * Enviar logs de auditoria*: Eventos do StorageGRID e atividades do sistema
   - **Enviar eventos de segurança**: Eventos de segurança, como quando um usuário não autorizado tenta entrar ou um usuário faz login como root
   - * Enviar logs de aplicativos*: Arquivos de log úteis para solução de problemas, incluindo:
     - bycast-err.log
     - bycast.log
     - jaeger.log
     - nms.log (somente nós administradores)
     - prometheus.log
     - raft.log
     - hagroups.log
2. Use os menus suspensos para selecionar a gravidade e a facilidade (tipo de mensagem) para a categoria de informações de auditoria que deseja enviar.

   Se você selecionar **passagem** para gravidade e facilidade, as informações enviadas para o servidor syslog remoto receberão a mesma gravidade e facilidade que fez quando conetado localmente no nó. Definir facilidade e gravidade pode ajudá-lo a agregar os logs de maneiras personalizáveis para facilitar a análise.

Para obter mais informações sobre os logs do software StorageGRID, Registos do software StorageGRIDconsulte .

a. Para **severidade**, selecione **passagem** se quiser que cada mensagem enviada para o syslog externo tenha o mesmo valor de gravidade que no syslog local.

   Para logs de auditoria, se você selecionar **Passthrough**, a gravidade é 'info'.

   Para eventos de segurança, se você selecionar **passagem**, os valores de gravidade serão gerados pela distribuição linux nos nós.

   Para logs de aplicativos, se você selecionar **passagem**, 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'.

b. Se não pretender utilizar o valor de passagem, selecione um valor de gravidade entre 0 e 7.

   O valor selecionado será aplicado a todas as mensagens deste tipo. As informações sobre diferentes gravidades serão perdidas quando você optar por substituir a gravidade com um valor fixo.

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

c. Para **Facility**, selecione **Passthrough** se quiser que cada mensagem enviada para o syslog externo tenha o mesmo valor de instalação que faz no syslog local.

   Para logs de auditoria, se você selecionar **passagem**, a facilidade enviada para o servidor syslog externo é 'local7'.

   Para eventos de segurança, se você selecionar **passagem**, os valores das instalações serão gerados pela distribuição linux nos nós.

   Para logs de aplicativos, se você selecionar **passagem**, os logs de aplicativos enviados para o servidor syslog externo têm os seguintes valores de instalação:

Registo de aplicações	Valor de passagem
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

d. Se você não quiser usar o valor de passagem, selecione o valor de instalação entre 0 e 23.

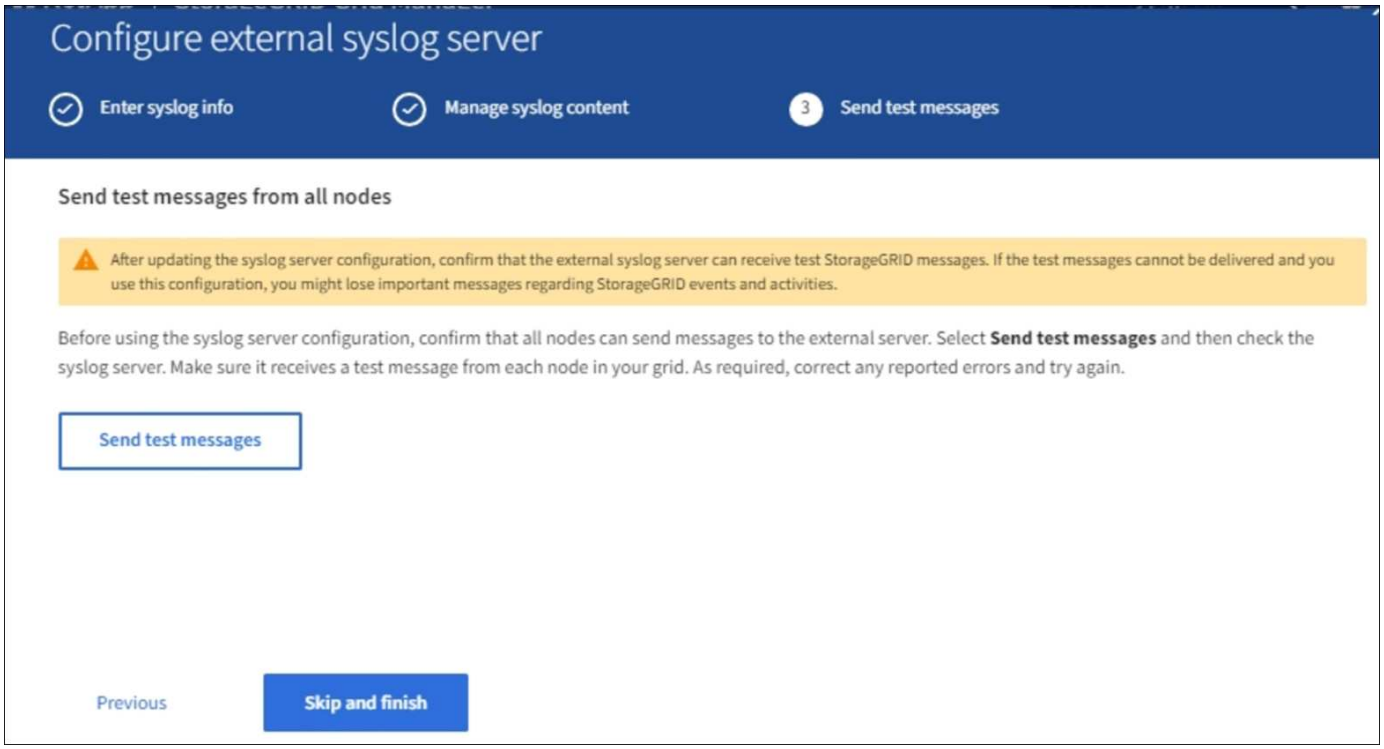
   O valor selecionado será aplicado a todas as mensagens deste tipo. Informações sobre diferentes instalações serão perdidas quando você optar por substituir instalações com um valor fixo.

Instalação	Descrição
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)
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

Instalação	Descrição
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.

1. Se você não quiser enviar mensagens de teste e tiver certeza de que seu servidor syslog externo está configurado corretamente e pode receber informações de auditoria de todos os nós da grade, selecione **Ignorar e concluir**.

   É apresentado um banner verde indicando que a sua configuração foi guardada com sucesso.

2. Caso contrário, selecione **Enviar mensagens de teste**.

   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, corrija-o e selecione **Enviar mensagens de teste** novamente. Solução de problemas do servidor syslog externoConsulte 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 coleção de logs. O protocolo UDP não permite uma deteção de erros tão rigorosa como os outros protocolos.

6. Selecione **Parar e terminar**.

   Você será devolvido à página **servidor de auditoria e syslog**. Um banner verde é exibido notificando que a configuração do servidor syslog foi salva com sucesso.

   Suas informações de auditoria do StorageGRID não são enviadas para o 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 eventos de segurança, os logs de aplicativos e os logs de mensagens de auditoria são enviados.

Para obter mais informações sobre os logs do software StorageGRID, Registos do software StorageGRIDconsulte .

1. Na página servidor de auditoria e syslog, selecione o destino das informações de auditoria nas opções listadas:

Opção	Descrição
Padrão (nós de administração/nós locais)	As mensagens de auditoria são enviadas para o log de auditoria (`audit.log`) no Admin Node, e os logs de eventos de segurança e de aplicativos são armazenados nos nós em que foram gerados (também chamados de "o nó local").
Servidor syslog externo	As informações de auditoria são enviadas para um servidor syslog externo e salvas no nó local. O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é ativada depois de ter configurado um servidor syslog externo.
Nó de administração e servidor syslog externo	As mensagens de auditoria são enviadas para o log de auditoria (`audit.log`) no nó Admin e as informações de auditoria são enviadas para o servidor syslog externo e salvas no nó local. O tipo de informação enviada depende de como você configurou o servidor syslog externo. Esta opção só é ativada depois de ter configurado um servidor syslog externo.
Somente nós locais	Nenhuma informação de auditoria é enviada para um Admin Node ou servidor syslog remoto. As informações de auditoria são salvas apenas nos nós que as geraram. **Nota**: O StorageGRID remove periodicamente esses 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 para o log é de 21 arquivos. Quando a versão 22nd 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.

As informações de auditoria geradas em cada nó local são armazenadas no `/var/local/log/localaudit.log`

1. Selecione **Guardar**. Em seguida, selecione OK para aceitar a alteração para o destino do log.
2. Se você selecionou **External syslog Server** ou **Admin Nodes e External syslog Server** como destino para informações de auditoria, um aviso adicional será exibido. Reveja o texto de aviso.

Você deve confirmar se o servidor syslog externo pode receber mensagens StorageGRID de teste.

1. Confirme se deseja alterar o destino para informações de auditoria selecionando **OK**.

   Um banner verde é exibido notificando que sua configuração de auditoria foi salva com êxito.

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

Informações relacionadas

Visão geral da mensagem de auditoria

Configurar mensagens de auditoria e destinos de log

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

Informações sobre direitos autorais

Informações sobre marcas comerciais