Use un servidor de syslog externo

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

Use un servidor de syslog externo

Consideraciones sobre el servidor de syslog externo

Use las siguientes directrices para calcular el tamaño del servidor de syslog externo que necesita.

¿Qué es un servidor de syslog externo?

Un servidor de syslog externo es un servidor fuera de StorageGRID que se puede utilizar para recopilar información de auditoría del sistema en una sola ubicación. El uso de un servidor de syslog externo permite configurar los destinos de la información de auditoría para poder reducir el tráfico de red en los nodos de administración y gestionar la información de manera más eficiente. Los tipos de información de auditoría que se pueden enviar al servidor de syslog externo incluyen:

- Los registros de auditoría que contienen mensajes de auditoría generados durante el funcionamiento normal del sistema
- Eventos relacionados con la seguridad, como inicios de sesión y escalados a root
- Registros de la aplicación que se pueden solicitar si es necesario abrir un caso de soporte para solucionar un problema con el que se ha encontrado

Cómo calcular el tamaño del servidor de syslog externo

Normalmente, el tamaño de su grid se ajusta para lograr el rendimiento requerido, definido en términos de operaciones de S3 por segundo o bytes por segundo. Por ejemplo, es posible que exista un requisito de que su grid gestione 1,000 operaciones de S3 por segundo, o 2,000 MB por segundo, de gestión de contenidos y recuperaciones de objetos. Se debe ajustar el tamaño del servidor de syslog externo de acuerdo con los requisitos de datos de la cuadrícula.

En esta sección, se proporcionan algunas fórmulas heurísticas que ayudan a calcular la tasa y el tamaño medio de los mensajes de registro de distintos tipos que debe ser capaz de gestionar el servidor de syslog externo, expresadas en términos de las características de rendimiento conocidas o deseadas de la cuadrícula (operaciones de S3 por segundo).

Use las operaciones de S3 por segundo en fórmulas de estimación

Si se ha ajustado el tamaño de un grid para un rendimiento expresado en bytes por segundo, debe convertir este tamaño en operaciones de S3 por segundo para utilizar las fórmulas de estimación. Para convertir el rendimiento del grid, primero debe determinar el tamaño medio del objeto, que puede utilizar la información de los registros de auditoría y las métricas existentes (si las hubiera), o utilizar sus conocimientos de las aplicaciones que utilizarán StorageGRID. Por ejemplo, si se ha ajustado el tamaño de la cuadrícula para conseguir un rendimiento de 2,000 MB/segundo y el tamaño medio del objeto es de 2 MB, el tamaño de la cuadrícula fue capaz de gestionar 1,000 operaciones de S3 por segundo (2,000 MB/2 MB).

> Las fórmulas para el ajuste de tamaño del servidor de syslog externo en las siguientes secciones proporcionan estimaciones de casos comunes (en lugar de estimaciones con respecto a los peores casos). Según la configuración y la carga de trabajo, es posible que se vea una tasa mayor o menor de mensajes de syslog o volumen de datos de syslog que las fórmulas predicen. Las fórmulas se han diseñado para utilizarse únicamente como directrices.

Fórmulas de estimación para registros de auditoría

Si no tiene información sobre la carga de trabajo de S3 distinta al número de operaciones de S3 por segundo que se espera compatibilidad con la cuadrícula, puede calcular el volumen de registros de auditoría que tendrá que gestionar el servidor de syslog externo mediante las siguientes fórmulas, En el supuesto de que deja los niveles de auditoría establecidos en los valores predeterminados (todas las categorías se establecen en normal, excepto almacenamiento, que se establece en error):

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

Por ejemplo, si el tamaño del grid se ajusta a 1,000 operaciones de S3 por segundo, el tamaño del servidor de syslog externo debe admitir 2,000 mensajes de syslog por segundo y debe poder recibir (y, por lo general, almacenar) datos de registro de auditoría a una tasa de 1.6 MB por segundo.

Si conoce más acerca de su carga de trabajo, es posible realizar estimaciones más precisas. En los registros de auditoría, las variables adicionales más importantes son el porcentaje de operaciones de S3 que se colocan (vs OBTIENE) y el tamaño medio, en bytes, de los siguientes campos S3 (las abreviaturas de 4 caracteres que se utilizan en la tabla son nombres de campos del registro de auditoría):

Codificación	Campo	Descripción
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en bloques no incluyen este campo.

Usemos P para representar el porcentaje de las operaciones de S3 que se sitúan, donde $0 \leq P \leq 1$ (por lo que para una carga de trabajo PUT del 100 %, P = 1 y para un 100 % DE CARGA de trabajo GET, P = 0).

Usemos K para representar el tamaño medio de la suma de los nombres de cuenta de S3, S3 Bucket y S3 Key. Supongamos que el nombre de cuenta S3 es siempre mi cuenta s3 (13 bytes), los bloques tienen nombres de longitud fija como /my/Application/bucket-12345 (28 bytes) y los objetos tienen claves de longitud fija como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). A continuación, el valor de K es 90 (13+13+28+36).

Si puede determinar valores para P y K, puede calcular el volumen de registros de auditoría que tendrá que manejar el servidor de syslog externo con las siguientes fórmulas, en el supuesto de que deja los niveles de auditoría establecidos en los valores predeterminados (todas las categorías establecidas en normal, excepto

almacenamiento, Que está establecido en error):

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

Por ejemplo, si el tamaño de su grid se define para 1,000 operaciones de S3 por segundo, su carga de trabajo será del 50 % put y sus nombres de cuentas de S3, nombres de bloques Y los nombres de objetos tienen un promedio de 90 bytes, el tamaño del servidor de syslog externo debe ser compatible con 1,500 mensajes de syslog por segundo y debe poder recibir (y almacenar normalmente) datos de registro de auditoría a una velocidad de aproximadamente 1 MB por segundo.

Fórmulas de estimación para niveles de auditoría no predeterminados

En las fórmulas proporcionadas para los registros de auditoría se asume el uso de la configuración predeterminada del nivel de auditoría (todas las categorías se establecen en normal, excepto almacenamiento, que está establecido en error). No están disponibles fórmulas detalladas para estimar la tasa y el tamaño medio de los mensajes de auditoría para los ajustes de nivel de auditoría no predeterminados. Sin embargo, el cuadro siguiente puede ser utilizado para hacer una estimación aproximada de la tarifa; puede utilizar la fórmula de tamaño medio proporcionada para los registros de auditoría, pero tenga en cuenta que es probable que tenga como resultado una sobreestimación porque los mensajes de auditoría “adicionales” son, en promedio, menores que los mensajes de auditoría predeterminados.

Condición	Fórmula
Replicación: Todos los niveles de auditoría están establecidos en Depurar o normal	Tasa de registro de auditoría = tasa de operaciones de 8 x S3
Código de borrado: Todos los niveles de auditoría están establecidos en Depurar o normal	Utilice la misma fórmula que para la configuración predeterminada

Fórmulas de estimación para eventos de seguridad

Los eventos de seguridad no están correlacionados con las operaciones de S3 y suelen producir un volumen insignificante de registros y datos. Por estas razones, no se proporcionan fórmulas de estimación.

Fórmulas de estimación para registros de aplicaciones

Si no tiene información acerca de la carga de trabajo de S3 distinta a la cantidad de operaciones de S3 por segundo que se espera compatibilidad con la cuadrícula, puede calcular el volumen de las aplicaciones que registra el servidor de syslog externo deberá manejar mediante las siguientes fórmulas:

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

Por lo tanto, si el tamaño del grid se ajusta para 1,000 operaciones de S3 por segundo, el tamaño del servidor de syslog externo debe ser compatible con 3,300 registros de aplicaciones por segundo y poder recibir (y almacenar) datos de registro de aplicaciones a una velocidad de aproximadamente 1.2 MB por segundo.

Si conoce más acerca de su carga de trabajo, es posible realizar estimaciones más precisas. En los registros

de aplicaciones, las variables adicionales más importantes son la estrategia de protección de datos (replicación o Código de borrado), el porcentaje de operaciones de S3 que se colocan (frente a las Obtiene/otro) y el tamaño medio, en bytes, de los siguientes campos S3 (las abreviaturas de 4 caracteres que se utilizan en la tabla son nombres de campos de registro de auditoría):

Codificación	Campo	Descripción
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en bloques no incluyen este campo.

Ejemplo de estimaciones de tamaño

En esta sección se explican casos de ejemplo de cómo utilizar las fórmulas de estimación para cuadrículas con los siguientes métodos de protección de datos:

- Replicación
- Código de borrado

Si utiliza replicación para la protección de datos

Permita que P represente el porcentaje de las operaciones de S3 que put, donde 0 ≤ P ≤ 1 (de modo que para una carga de trabajo PUT del 100 %, P = 1 y para una carga de trabajo DEL 100 %, P = 0).

Deje que K represente el tamaño medio de la suma de los nombres de cuenta de S3, S3 Bucket y S3 Key. Supongamos que el nombre de cuenta S3 es siempre mi cuenta s3 (13 bytes), los bloques tienen nombres de longitud fija como /my/Application/bucket-12345 (28 bytes) y los objetos tienen claves de longitud fija como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). A continuación, K tiene un valor de 90 (13+13+28+36).

Si puede determinar valores para P y K, puede calcular el volumen de registros de aplicaciones que tendrá que manejar el servidor de syslog externo con las siguientes 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
```

Por lo tanto, si, por ejemplo, el tamaño de su grid se ajusta a 1,000 operaciones de S3 por segundo, su carga

de trabajo tiene un 50 % de sitúa y los nombres de cuentas, los nombres de bloques y los nombres de objetos de S3 tienen un promedio de 90 bytes, el tamaño de su servidor de syslog externo debe ser compatible con 1800 registros de aplicaciones por segundo, Y recibirá (y, normalmente, almacenará) datos de aplicaciones a una velocidad de 0.5 MB por segundo.

Si utiliza códigos de borrado para protección de datos

Permita que P represente el porcentaje de las operaciones de S3 que put, donde 0 ≤ P ≤ 1 (de modo que para una carga de trabajo PUT del 100 %, P = 1 y para una carga de trabajo DEL 100 %, P = 0).

Deje que K represente el tamaño medio de la suma de los nombres de cuenta de S3, S3 Bucket y S3 Key. Supongamos que el nombre de cuenta S3 es siempre mi cuenta s3 (13 bytes), los bloques tienen nombres de longitud fija como /my/Application/bucket-12345 (28 bytes) y los objetos tienen claves de longitud fija como 5733a5d7-f069-41ef-8fbd-13247494c69c (36 bytes). A continuación, K tiene un valor de 90 (13+13+28+36).

Si puede determinar valores para P y K, puede calcular el volumen de registros de aplicaciones que tendrá que manejar el servidor de syslog externo con las siguientes 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
```

Por ejemplo, si el tamaño de su grid se ajusta a 1,000 operaciones de S3 por segundo, su carga de trabajo será del 50 % put y sus nombres de cuentas de S3, nombres de bloques Y los nombres de objetos tienen un promedio de 90 bytes, el tamaño del servidor syslog externo debe ser compatible con 2,250 registros de aplicación por segundo y debe poder recibir y recibir (y normalmente almacenar) datos de aplicación a una velocidad de 0.6 MB por segundo.

Para obtener más información sobre la configuración de niveles de mensajes de auditoría y un servidor de syslog externo, consulte lo siguiente:

- Configure un servidor de syslog externo
- Configurar los mensajes de auditoría y los destinos de registro

Configure un servidor de syslog externo

Si desea guardar registros de auditoría, registros de aplicaciones y registros de eventos de seguridad en una ubicación fuera de la cuadrícula, utilice este procedimiento para configurar un servidor de syslog externo.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene un servidor de syslog con la capacidad para recibir y almacenar los archivos de registro. Para obtener más información, consulte Consideraciones sobre el servidor de syslog externo.
- Tiene las certificaciones de servidor y cliente correctas si tiene previsto utilizar TLS o RELP/TLS.

Acerca de esta tarea

Si desea enviar información de auditoría a un servidor de syslog externo, primero debe configurar el servidor

externo.

El envío de información de auditoría a un servidor de syslog externo permite:

- Recopilar y gestionar información de auditoría, como mensajes de auditoría, registros de aplicaciones y eventos de seguridad, de forma más eficiente
- Reduzca el tráfico de red en los nodos de administrador, ya que la información de auditoría se transfiere directamente de los distintos nodos de almacenamiento al servidor de syslog externo, sin tener que atravesar un nodo de administración

> Cuando se envían registros a un servidor de syslog externo, los registros únicos superiores a 8192 bytes se truncarán al final del mensaje para ajustarse a las limitaciones comunes en las implementaciones de servidores de syslog externos.

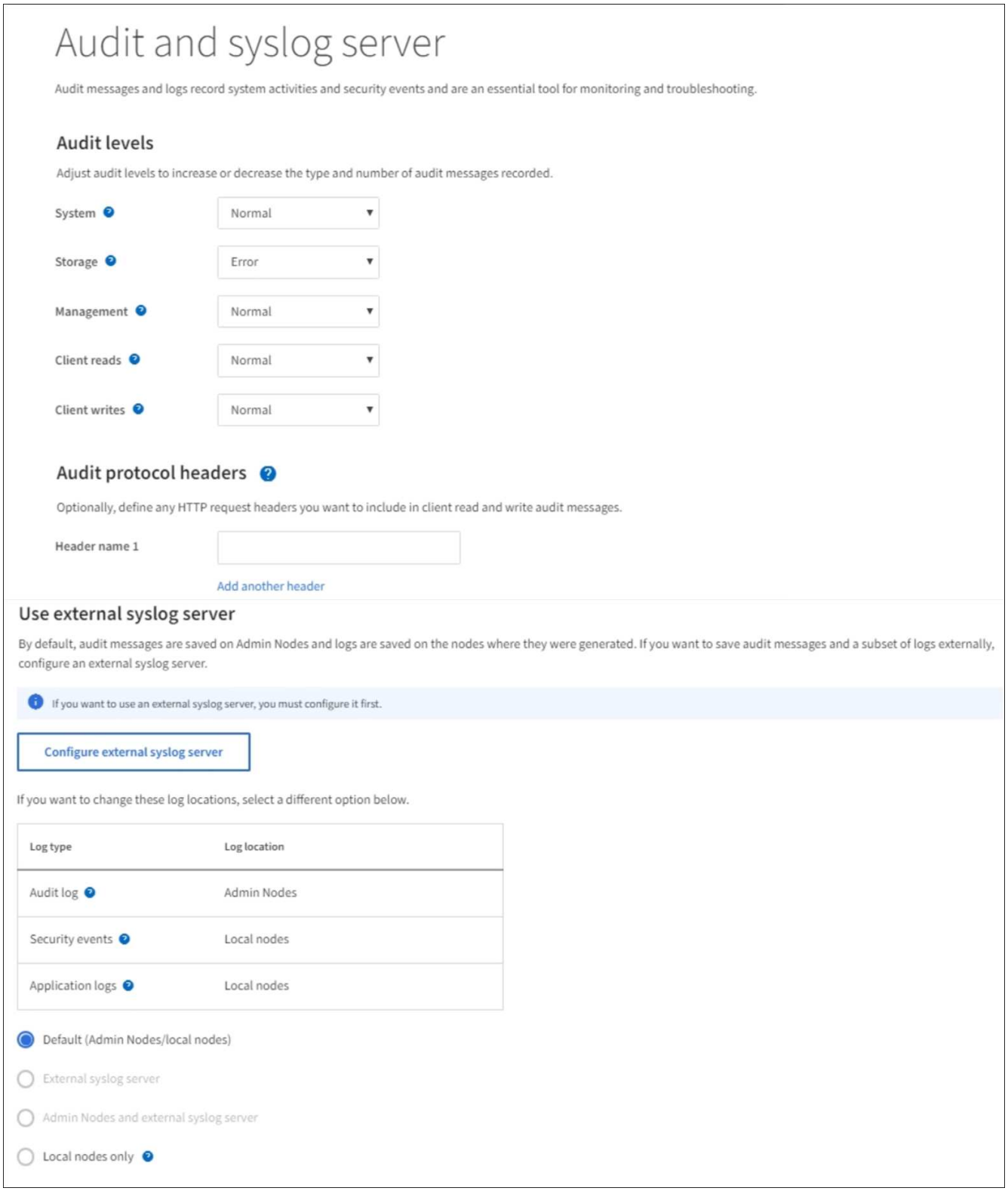
> Para maximizar las opciones de recuperación completa de datos en caso de un fallo del servidor de syslog externo, se mantienen hasta 20 GB de registros locales de registros de auditoría (localaudit.log) en cada nodo.

> Si las opciones de configuración disponibles en este procedimiento no son lo suficientemente flexibles para satisfacer sus requisitos, se pueden aplicar opciones de configuración adicionales mediante la API privada `audit-destinations` puntos finales. Por ejemplo, es posible usar diferentes servidores de syslog para diferentes grupos de nodos.

Acceda al asistente de configuración del servidor de syslog

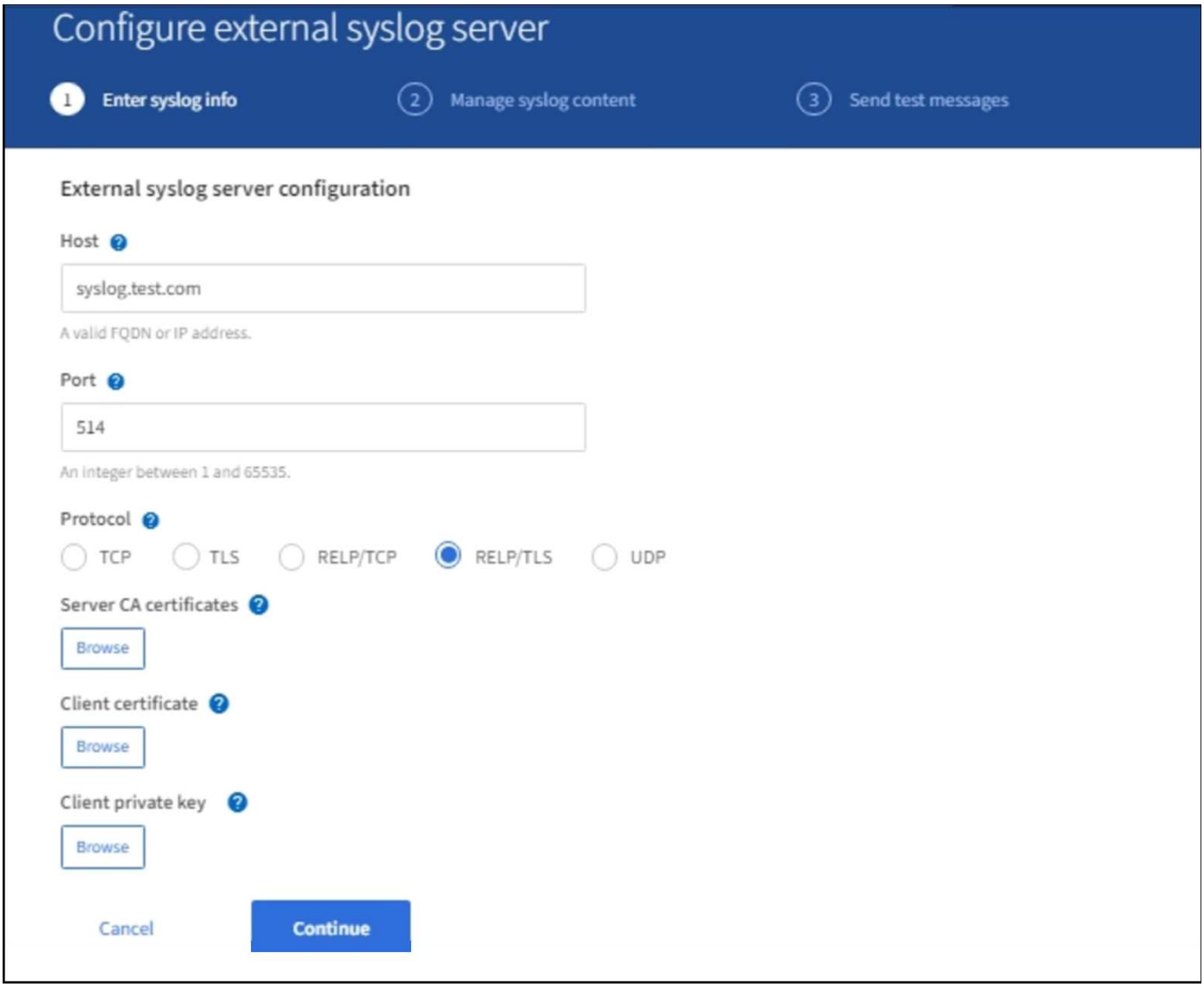
Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**.



2. En la página servidor de auditoría y syslog, seleccione **Configurar servidor de syslog externo**. Si ha configurado previamente un servidor de syslog externo, seleccione **Editar servidor de syslog externo**.

Introduzca la información de syslog



1. Introduzca un nombre de dominio completo válido o una dirección IPv4 o IPv6 para el servidor de syslog externo en el campo **Host**.
2. Introduzca el puerto de destino en el servidor de syslog externo (debe ser un entero entre 1 y 65535). El puerto predeterminado es 514.
3. Seleccione el protocolo utilizado para enviar información de auditoría al servidor de syslog externo.

   Se recomienda TLS o RELP/TLS. Debe cargar un certificado de servidor para usar cualquiera de estas opciones.

   El uso de certificados ayuda a proteger las conexiones entre el grid y el servidor de syslog externo. Para obtener más información, consulte Use los certificados de seguridad StorageGRID.

   Todas las opciones de protocolo requieren compatibilidad con el servidor de syslog externo y su configuración. Debe elegir una opción que sea compatible con el servidor de syslog externo.

   > El protocolo de registro de eventos fiable (RELP) amplía la funcionalidad del protocolo syslog para proporcionar una entrega fiable de los mensajes de eventos. El uso de RELP puede ayudar a evitar la pérdida de información de auditoría si el servidor syslog externo tiene que reiniciarse.

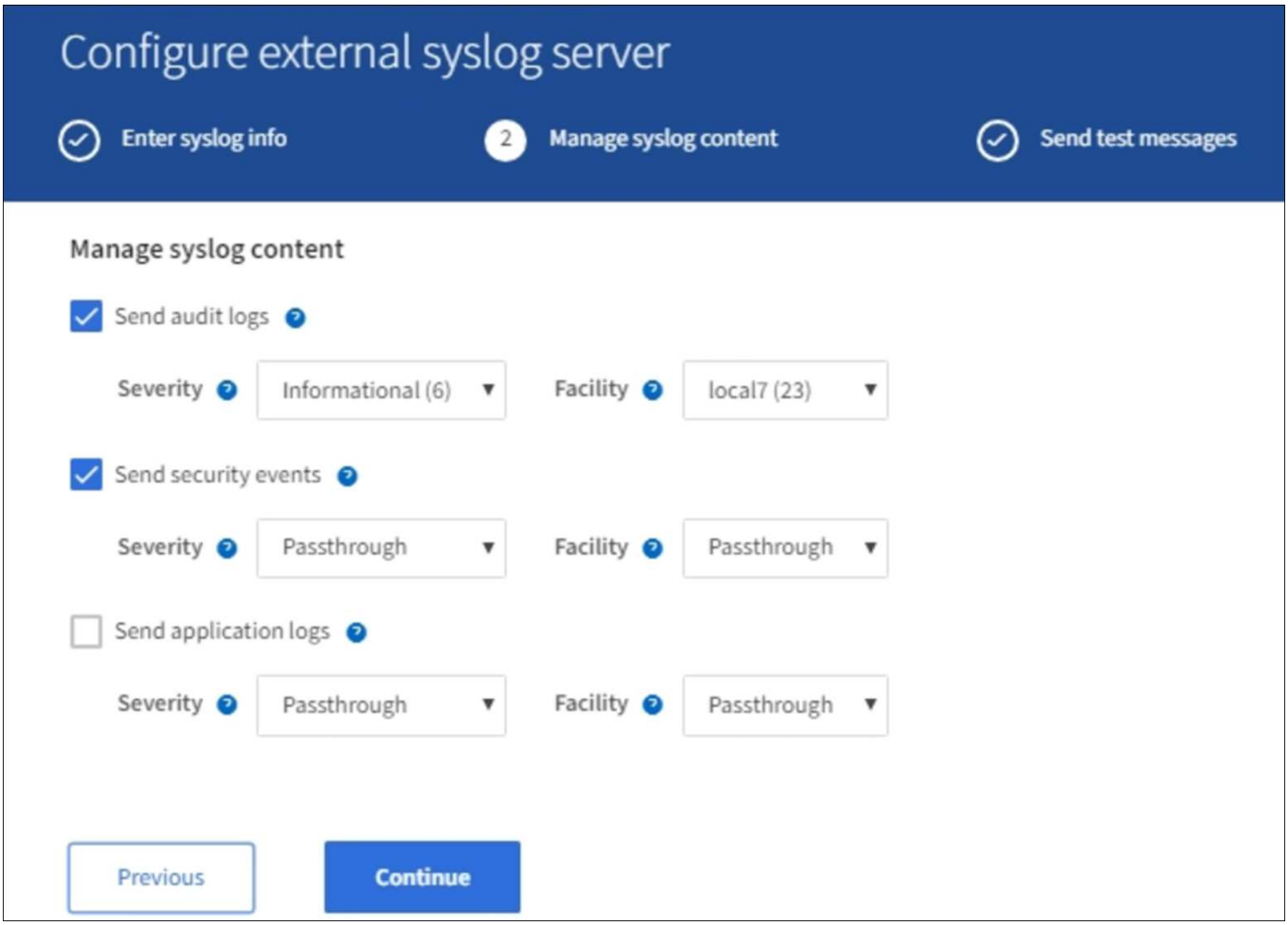
4. Seleccione **continuar**.
5. Si ha seleccionado **TLS** o **RELP/TLS**, cargue los siguientes certificados:
   - **Certificados de CA del servidor**: Uno o más certificados de CA de confianza para verificar el servidor syslog externo (en codificación PEM). Si se omite, se utilizará el certificado de CA de cuadrícula predeterminado. El archivo que cargue aquí puede ser un bundle de CA.
   - **Certificado de cliente**: Certificado de cliente para la autenticación al servidor syslog externo (en codificación PEM).
   - **Clave privada de cliente**: Clave privada para el certificado de cliente (en codificación PEM).

     Si utiliza un certificado de cliente, también debe usar una clave privada de cliente. Si proporciona una clave privada cifrada, también debe proporcionar la contraseña. No hay ninguna ventaja de seguridad significativa por el uso de una clave privada cifrada, ya que la clave y la frase de contraseña deben almacenarse; se recomienda usar una clave privada no cifrada, si está disponible, para facilitar la utilización.

     i. Seleccione **Buscar** para el certificado o la clave que desee utilizar.
     ii. Seleccione el archivo de certificado o el archivo de claves.
     iii. Seleccione **Abrir** para cargar el archivo.

   Aparece una comprobación verde junto al certificado o el nombre del archivo de claves, notificándole que se ha cargado correctamente.
6. Seleccione **continuar**.

Permite gestionar el contenido de syslog



1. Seleccione cada tipo de información de auditoría que desea enviar al servidor de syslog externo.
   - **Enviar registros de auditoría**: Eventos StorageGRID y actividades del sistema
   - **Enviar eventos de seguridad**: Eventos de seguridad como cuando un usuario no autorizado intenta iniciar sesión o un usuario inicia sesión como root
   - **Enviar registros de aplicación**: Archivos de registro útiles para la solución de problemas, incluidos:
     - bycast-err.log
     - bycast.log
     - jaeger.log
     - nms.log (solo nodos del administrador)
     - prometheus.log
     - raft.log
     - hagroups.log
2. Utilice los menús desplegables para seleccionar la gravedad y el servicio (tipo de mensaje) de la categoría de información de auditoría que desea enviar.

   Si selecciona **Paso a través** para severidad e instalación, la información enviada al servidor syslog remoto recibirá la misma gravedad y facilidad que cuando se haya iniciado sesión localmente en el nodo. Establecer las instalaciones y la gravedad pueden ayudarle a agregar los registros de formas personalizables para facilitar el análisis.

Para obtener más información sobre los registros del software StorageGRID, consulte Registros del software StorageGRID.

a. Para **severidad**, seleccione **Paso a través** si desea que cada mensaje enviado al syslog externo tenga el mismo valor de gravedad que en el syslog local.

   Para los registros de auditoría, si selecciona **Paso a través**, la gravedad es 'info'.

   Para eventos de seguridad, si selecciona **Paso a través**, la distribución linux genera los valores de gravedad en los nodos.

   Para los registros de la aplicación, si selecciona **Paso a través**, las gravedades varían entre "info" y "notice", dependiendo de cuál sea el problema. Por ejemplo, la adición de un servidor NTP y la configuración de un grupo ha proporcionan un valor de "información", mientras que la detención intencional del servicio ssm o rsm proporciona un valor de "aviso".

b. Si no desea utilizar el valor de paso a través, seleccione un valor de gravedad entre 0 y 7.

   El valor seleccionado se aplicará a todos los mensajes de este tipo. Se perderá información acerca de las diferentes gravedades cuando elija reemplazar la gravedad con un valor fijo.

Gravedad	Descripción
0	Emergencia: El sistema no se puede utilizar
1	Alerta: La acción se debe realizar de inmediato
2	Crítico: Condiciones críticas
3	Error: Condiciones de error
4	Advertencia: Condiciones de aviso
5	Aviso: Condición normal pero significativa
6	Informativo: Mensajes informativos
7	Debug: Mensajes de nivel de depuración

c. Para **Facility**, seleccione **PassThrough** si desea que cada mensaje enviado al syslog externo tenga el mismo valor de instalación que en el syslog local.

   Para los registros de auditoría, si selecciona **PassThrough**, la instalación enviada al servidor syslog externo es 'local7'.

   Para los eventos de seguridad, si selecciona **Paso a través**, los valores de la instalación los genera la distribución linux en los nodos.

   Para los registros de aplicaciones, si selecciona **Paso a través**, los registros de la aplicación enviados al servidor syslog externo tienen los siguientes valores de instalación:

Registro de aplicaciones	Valor de paso a través
bycast.log	usuario o demonio
bycast-err.log	usuario, daemon, local3 o local4
jaeger.log	local2
nms.log	local3
prometheus.log	local4
raft.log	local5
hagroups.log	local6

d. Si no desea utilizar el valor de paso a través, seleccione el valor de la instalación entre 0 y 23.

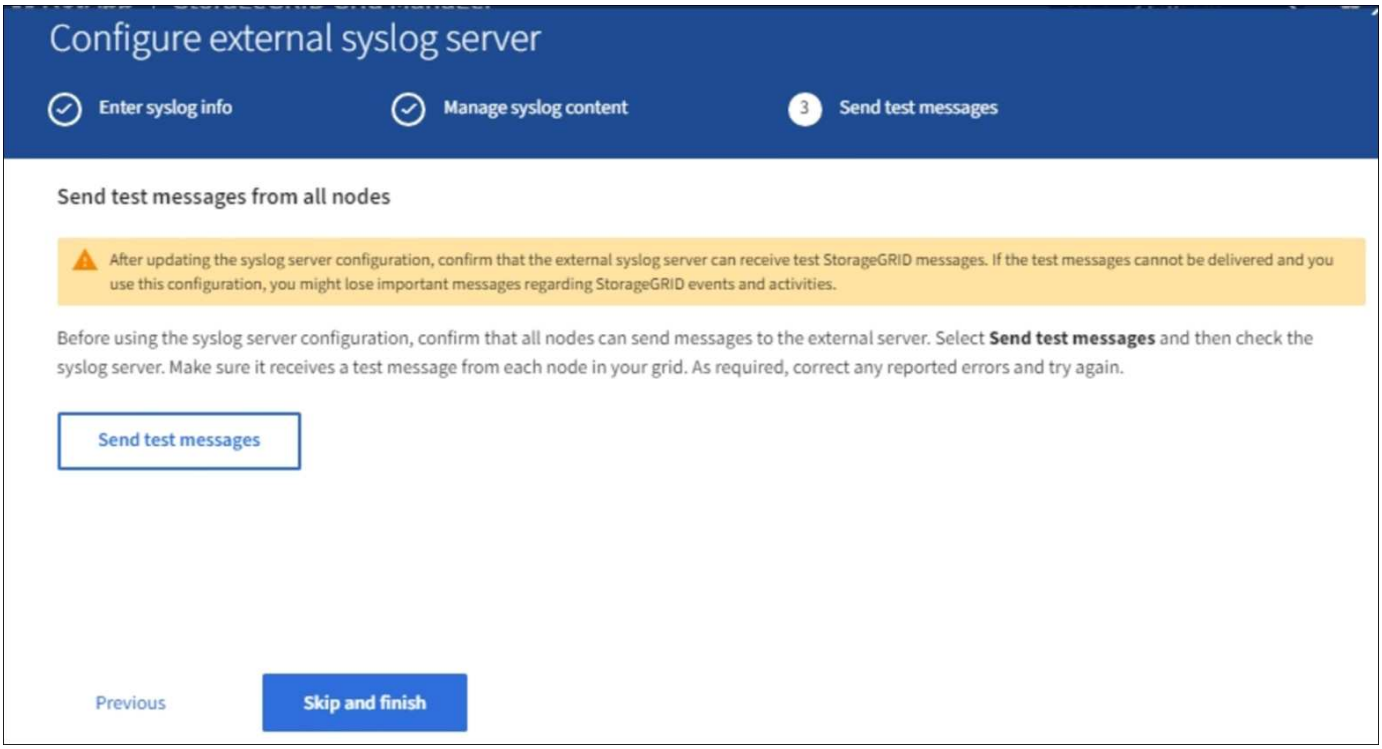
   El valor seleccionado se aplicará a todos los mensajes de este tipo. Se perderá información acerca de las distintas instalaciones cuando elija reemplazar la instalación con un valor fijo.

Centro	Descripción
0	kern (mensajes del núcleo)
1	usuario (mensajes de usuario)
2	correo
3	daemon (daemons del sistema)
4	auth (mensajes de seguridad/autorización)
5	syslog (mensajes generados internamente por syslogd)
6	lpr (subsistema de impresora de líneas)
7	noticias (subsistema de noticias de red)
8	UCP
9	cron (daemon de reloj)
10	seguridad (mensajes de seguridad/autorización)
11	FTP

Centro	Descripción
12	NTP
13	auditoría de registro (auditoría de registros)
14	alerta de registro (alerta de registro)
15	reloj (daemon de reloj)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Seleccione **continuar**.

Enviar mensajes de prueba



Antes de iniciar el uso de un servidor de syslog externo, debe solicitar que todos los nodos de la cuadrícula envíen mensajes de prueba al servidor de syslog externo. Se deben usar estos mensajes de prueba para ayudar a validar toda la infraestructura de recogida de registros antes de comprometerse a enviar datos al servidor de syslog externo.

> No use la configuración del servidor de syslog externo hasta que se confirme que el servidor de syslog externo recibió un mensaje de prueba de cada nodo de la cuadrícula y que el mensaje se procesó según lo esperado.

1. Si no desea enviar mensajes de prueba y está seguro de que el servidor syslog externo está configurado correctamente y puede recibir información de auditoría de todos los nodos de la cuadrícula, seleccione **Omitir y finalizar**.

   Aparece un banner verde que indica que la configuración se ha guardado correctamente.

2. De lo contrario, seleccione **Enviar mensajes de prueba**.

   Los resultados de la prueba aparecen continuamente en la página hasta que se detiene la prueba. Mientras la prueba está en curso, los mensajes de auditoría siguen enviarse a los destinos configurados anteriormente.

3. Si recibe algún error, corríjalo y vuelva a seleccionar **Enviar mensajes de prueba**. Consulte Solucionar problemas del servidor de syslog externo para ayudarle a resolver errores.
4. Espere hasta que vea un banner verde que indica que todos los nodos han superado la prueba.
5. Compruebe el servidor de syslog para determinar si se reciben y procesan los mensajes de prueba según lo esperado.

> Si está utilizando UDP, compruebe toda su infraestructura de recopilación de registros. El protocolo UDP no permite una detección de errores tan rigurosa como los demás protocolos.

6. Seleccione **Detener y finalizar**.

   Volverá a la página **Audit and syslog Server**. Aparece un banner verde para notificarle que la configuración del servidor de syslog se ha guardado correctamente.

   > La información de auditoría de StorageGRID no se envía al servidor de syslog externo hasta que se selecciona un destino que incluye el servidor de syslog externo.

Seleccione destinos de información de auditoría

Es posible especificar dónde se envían los registros de eventos de seguridad, los registros de aplicaciones y los registros de mensajes de auditoría.

> Para obtener más información sobre los registros del software StorageGRID, consulte Registros del software StorageGRID.

1. En la página Audit and syslog Server, seleccione el destino para la información de auditoría de las opciones que aparecen:

Opción	Descripción
Predeterminado (nodos de administrador/nodos locales)	Se envían mensajes de auditoría al registro de auditoría (`audit.log`) En el nodo Admin, y los registros de eventos de seguridad y de aplicaciones se almacenan en los nodos en los que se generaron (también denominado "nodo local").
Servidor de syslog externo	La información de auditoría se envía a un servidor de syslog externo y se guarda en el nodo local. El tipo de información enviada depende de la forma en que se configure el servidor de syslog externo. Esta opción solo se habilita después de configurar un servidor de syslog externo.
Nodo de administrador y servidor de syslog externo	Se envían mensajes de auditoría al registro de auditoría (`audit.log`) En el nodo Admin, y la información de auditoría se envía al servidor syslog externo y se guarda en el nodo local. El tipo de información enviada depende de la forma en que se configure el servidor de syslog externo. Esta opción solo se habilita después de configurar un servidor de syslog externo.
Solo nodos locales	No se envía información de auditoría a un nodo de administrador ni al servidor de syslog remoto. La información de auditoría solo se guarda en los nodos que la generaron. **Nota**: StorageGRID elimina periódicamente estos registros locales en rotación para liberar espacio. Cuando el archivo de registro de un nodo alcanza 1 GB, se guarda el archivo existente y se inicia un nuevo archivo de registro. El límite de rotación para el registro es de 21 archivos. Cuando se crea la versión 22ª del archivo de registro, se elimina el archivo de registro más antiguo. De media, se almacenan unos 20 GB de datos de registro en cada nodo.

> La información de auditoría generada en cada nodo local se almacena en `/var/local/log/localaudit.log`

1. Seleccione **Guardar**. A continuación, seleccione Aceptar para aceptar el cambio en el destino del registro.
2. Si ha seleccionado **servidor syslog externo** o **nodos de administración y servidor syslog externo** como destino de la información de auditoría, aparecerá una advertencia adicional. Revise el texto de advertencia.

> Debe confirmar que el servidor de syslog externo puede recibir mensajes de StorageGRID de prueba.

1. Confirme que desea cambiar el destino de la información de auditoría seleccionando **Aceptar**.

   Aparece un mensaje de cabecera verde en el que se le notifica que la configuración de auditoría se ha guardado correctamente.

   Los nuevos registros se envían a los destinos seleccionados. Los registros existentes permanecen en su ubicación actual.

Información relacionada

Información general de los mensajes de auditoría

Configurar los mensajes de auditoría y los destinos de registro

Mensajes de auditoría del sistema

Mensajes de auditoría del almacenamiento de objetos

Mensaje de auditoría de gestión

El cliente lee los mensajes de auditoría

Administre StorageGRID