Configure los destinos de los mensajes de auditoría y los registros

StorageGRID 11.8

NetApp
March 19, 2024

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-118/monitor/considerations-for-external-syslog-server.html on March 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configure los destinos de los mensajes de auditoría y los registros

Consideraciones que tener en cuenta sobre el uso de 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 reducir el tráfico de red en los nodos de administrador y gestionar la información de manera más eficiente. Para StorageGRID, el formato de paquete de mensajes syslog de salida es compatible con RFC 3164.

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

Cuándo usar un servidor de syslog externo

Un servidor syslog externo es especialmente útil si tiene un grid grande, utiliza varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría. El envío de información de auditoría a un servidor de syslog externo permite:

- Recopile y gestione información de auditoría como mensajes de auditoría, registros de aplicaciones y eventos de seguridad de forma más eficaz.
- Reduzca el tráfico de red de los nodos de administrador, ya que la información de auditoría se transfiere directamente desde los diversos nodos de almacenamiento al servidor de syslog externo, sin tener que pasar por un nodo de administración.

> Cuando se envían los registros a un servidor de syslog externo, al final del mensaje se truncan los registros individuales de más de 8.192 bytes para cumplir con las limitaciones comunes en las implementaciones de servidores de syslog externos.

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

Cómo configurar un servidor de syslog externo

Para obtener información sobre cómo configurar un servidor de syslog externo, consulte "Configure los mensajes de auditoría y el servidor de syslog externo".

Si planea configurar el uso del protocolo TLS o RELP/TLS, debe tener los siguientes certificados:

- **Certificados de CA de 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.
- **Certificado de cliente**: El 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.

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	S3 cucharón	El nombre de bloque de S3.
S3KY	Tecla S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.

Usemos P para representar el porcentaje de las operaciones de S3 que se sitúan, donde 0 ≤ P ≤ 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 promedio de la suma de los S3 nombres de cuenta, 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). Las fórmulas detalladas para estimar la tasa y el tamaño medio de los mensajes de auditoría para los valores de nivel de auditoría no predeterminados no están disponibles. Sin embargo, la siguiente tabla se puede utilizar para hacer una estimación aproximada de la tasa; puede utilizar la fórmula de tamaño medio proporcionada para los registros de auditoría, pero tenga en cuenta que es probable que resulte en una sobreestimación porque los mensajes de auditoría adicionales son, en promedio, más pequeños 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 = 8 x S3 Tasa de operaciones
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	S3 cucharón	El nombre de bloque de S3.
S3KY	Tecla S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos 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
- Codificación 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 S3 nombres de cuenta, 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 S3 nombres de cuenta, 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
```

Así pues, por ejemplo, si el grid tiene el tamaño de 1.000 S3 operaciones por segundo, su carga de trabajo será del 50 % PUTS y los nombres de sus S3 cuentas, nombres de bloques, además, los nombres de objetos tienen un promedio de 90 bytes, el tamaño de su servidor syslog externo debe ser compatible con 2.250 registros de aplicación por segundo y debería poder recibir (y normalmente almacenar) datos de la aplicación a una velocidad de 0,6 MB por segundo.

Configure los mensajes de auditoría y el servidor de syslog externo

Puede configurar una serie de valores relacionados con los mensajes de auditoría. Puede ajustar el número de mensajes de auditoría registrados; definir los encabezados de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente; configurar un servidor de syslog externo; y especificar dónde se envían los registros de auditoría, los registros de eventos de seguridad y los registros de software de StorageGRID.

Los mensajes de auditoría y los registros registran las actividades del sistema y los eventos de seguridad, y son herramientas esenciales para la supervisión y solución de problemas. Todos los nodos de StorageGRID generan mensajes y registros de auditoría para realizar un seguimiento de la actividad y los eventos del sistema.

De manera opcional, se puede configurar un servidor de syslog externo para guardar la información de auditoría de forma remota. El uso de un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la integridad de los datos de auditoría. Un servidor syslog externo es especialmente útil si tiene un grid grande, utiliza varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría. Consulte "Consideraciones sobre el servidor de syslog externo" para obtener más detalles.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Si planea configurar un servidor de syslog externo, revisó el "consideraciones que tener en cuenta sobre el uso de un servidor de syslog externo" y se aseguró de que el servidor tiene suficiente capacidad para

recibir y almacenar los archivos de registro.

- Si planea configurar un servidor de syslog externo con el protocolo TLS o RELP/TLS, tendrá los certificados de CA de servidor y de cliente requeridos, así como la clave privada de cliente.

Cambiar los niveles de mensajes de auditoría

Se puede establecer un nivel de auditoría diferente para cada una de las siguientes categorías de mensajes en el registro de auditoría:

Categoría de auditoría	Configuración predeterminada	Más información
Sistema	Normal	"Mensajes de auditoría del sistema"
Reducida	Error	"Mensajes de auditoría del almacenamiento de objetos"
Gestión	Normal	"Mensaje de auditoría de gestión"
El cliente lee	Normal	"El cliente lee los mensajes de auditoría"
Escrituras del cliente	Normal	"El cliente escribe mensajes de auditoría"
ILM	Normal	"Mensajes de auditoría de ILM"
Replicación entre grid	Error	"CGRR: Solicitud de Replicación de Cuadrícula Cruzada"

Estos valores predeterminados se aplican si instaló inicialmente StorageGRID con la versión 10.3 o posterior. Si utilizó inicialmente una versión anterior de StorageGRID, el valor predeterminado para todas las categorías se establece en Normal.

Durante las actualizaciones, las configuraciones a nivel de auditoría no serán efectivas inmediatamente.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**.
2. Para cada categoría de mensaje de auditoría, seleccione un nivel de auditoría de la lista desplegable:

Nivel de auditoría	Descripción
Apagado	No se registran mensajes de auditoría de la categoría.
Error	Sólo se registran los mensajes de error: Los mensajes de auditoría para los que el código de resultado no fue "correcto" (SUCS).

Nivel de auditoría	Descripción
Normal	Se registran los mensajes transaccionales estándar: Los mensajes que aparecen en estas instrucciones para la categoría.
Depurar	Obsoleto. Este nivel se comporta como el nivel de auditoría normal.

Los mensajes incluidos para cualquier nivel particular incluyen los que se registrarán en los niveles superiores. Por ejemplo, el nivel normal incluye todos los mensajes de error.

> Si no necesita un registro detallado de las operaciones de lectura del cliente para sus aplicaciones S3, cambie opcionalmente la configuración **Lecturas del cliente** a **Error** para disminuir el número de mensajes de auditoría registrados en el registro de auditoría.

3. Seleccione **Guardar**.

   Un banner verde indica que la configuración se ha guardado.

Definir cabeceras de solicitud HTTP

Opcionalmente, puede definir cualquier cabecera de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente. Estos encabezados de protocolo se aplican solo a solicitudes S3 y Swift.

Pasos

1. En la sección **Cabeceras de protocolo de auditoría**, defina los encabezados de solicitud HTTP que desea incluir en los mensajes de auditoría de lectura y escritura del cliente.

   Utilice un asterisco (*) como comodín para que coincida con cero o más caracteres. Utilice la secuencia de escape (*) para que coincida con un asterisco literal.

2. Seleccione **Agregar otro encabezado** para crear encabezados adicionales, si es necesario.

   Cuando se encuentran encabezados HTTP en una solicitud, se incluyen en el mensaje de auditoría en el campo HTRH.

   > Los encabezados de la solicitud del protocolo de auditoría sólo se registran si el nivel de auditoría para **Lecturas de cliente** o **Escrituras de cliente** no es **Desactivada**.

3. Seleccione **Guardar**

   Un banner verde indica que la configuración se ha guardado.

Utilice un servidor syslog externo

De manera opcional, es posible configurar un servidor de syslog externo para guardar registros de auditoría, registros de aplicaciones y registros de eventos de seguridad en una ubicación fuera del grid.

> Si no desea usar un servidor de syslog externo, omita este paso y vaya a. Seleccione destinos de información de auditoría.

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 el `audit-destinations` Endpoints, que se encuentran en la sección API privada de "API de gestión de grid". Por ejemplo, puede usar la API si desea usar diferentes servidores de syslog para diferentes grupos de nodos.

Introduzca la información de syslog

Acceda al asistente Configurar servidor de syslog externo y proporcione la información que StorageGRID necesita para acceder al servidor de syslog externo.

Pasos

1. En la página servidor de auditoría y syslog, seleccione **Configurar servidor de syslog externo**. O bien, si ha configurado previamente un servidor syslog externo, seleccione **Editar servidor syslog externo**.

   Aparece el asistente Configurar servidor de syslog externo.

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

   Se recomienda usar **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 "Gestionar certificados de seguridad".

   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.

5. Seleccione **continuar**.
6. Si seleccionó **TLS** o **RELP/TLS**, cargue los certificados de CA del servidor, el certificado de cliente y la clave privada del cliente.
   a. Seleccione **Buscar** para el certificado o la clave que desee utilizar.
   b. Seleccione el certificado o el archivo de claves.
   c. 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.

7. Seleccione **continuar**.

Permite gestionar el contenido de syslog

Puede seleccionar la información que desea enviar al servidor de syslog externo.

Pasos

1. Para el paso **Administrar contenido syslog** del asistente, seleccione cada tipo de información de auditoría que desee enviar al servidor syslog externo.

   - **Enviar registros de auditoría**: Envía eventos StorageGRID y actividades del sistema
   - **Enviar eventos de seguridad**: Envía eventos de seguridad como cuando un usuario no autorizado intenta iniciar sesión o un usuario inicia sesión como root
   - **Enviar registros de aplicaciones**: Envía archivos de registro útiles para la solución de problemas, incluyendo:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Solo nodos de administración)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

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

2. Utilice los menús desplegables para seleccionar la gravedad y la utilidad (tipo de mensaje) para cada categoría de información de auditoría que desee enviar.

   La definición de valores de gravedad y de utilidad puede ayudarle a agregar los registros de formas personalizables para facilitar el análisis.

   a. Para **Gravedad**, selecciona **Passthrough**, o selecciona un valor de gravedad entre 0 y 7.

      Si selecciona un valor, el valor seleccionado se aplicará a todos los mensajes de este tipo. La información sobre diferentes gravedades se perderá si se sustituye la gravedad por un valor fijo.

Gravedad	Descripción
Paso a través	Cada mensaje enviado al syslog externo para tener el mismo valor de gravedad que cuando se registró localmente en el nodo: • Para los registros de auditoría, la gravedad es «info». • Para eventos de seguridad, los valores de gravedad se generan en la distribución de Linux en los nodos. • Para los registros de aplicaciones, las gravedades varían entre “info” y “notice”, dependiendo de cuál sea el problema. Por ejemplo, agregar un servidor NTP y configurar un grupo de alta disponibilidad proporciona un valor de «info», mientras que detener intencionalmente el servicio SSM o RSM proporciona un valor de «notice».
0	Emergencia: El sistema no se puede utilizar

Gravedad	Descripción
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

b. Para **Facilty**, selecciona **Passthrough**, o selecciona un valor entre 0 y 23.

Si selecciona un valor, se aplicará a todos los mensajes de este tipo. La información sobre las diferentes instalaciones se perderá si se sustituye la instalación por un valor fijo.

Centro	Descripción
Paso a través	Cada mensaje enviado al syslog externo para tener el mismo valor de instalación que cuando se registró localmente en el nodo: • Para los registros de auditoría, la instalación enviada al servidor de syslog externo es «local7». • Para los eventos de seguridad, los valores de las instalaciones se generan mediante la distribución de linux en los nodos. • Para los registros de aplicaciones, los registros de aplicaciones enviados al servidor syslog externo tienen los siguientes valores de utilidad: ◦ `bycast.log`: usuario o daemon ◦ `bycast-err.log`: usuario, daemon, local3 o local4 ◦ `jaeger.log`: local2 ◦ `nms.log`: local3 ◦ `prometheus.log`: local4 ◦ `raft.log`: local5 ◦ `hagroups.log`: local6
0	kern (mensajes del núcleo)
1	usuario (mensajes de usuario)

Centro	Descripción
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
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 confirme que el servidor de syslog externo recibió un mensaje de prueba de cada nodo del grid y que el mensaje se procesó como se esperaba.

Pasos

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

   Un banner verde indica que se ha guardado la configuración.

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

   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 "Solucione problemas de un 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 el otro protocolos.

6. Seleccione **Detener y finalizar**.

   Volverá a la página **Audit and syslog Server**. Un banner de color verde indica que se guardó la configuración del servidor de syslog.

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

Seleccione destinos de información de auditoría

Es posible especificar dónde registros de auditoría, registros de eventos de seguridad y "Registros del software StorageGRID" se envían.

> Algunos destinos solo están disponibles si se configuró un servidor de syslog externo.

Pasos

1. En la página Audit and syslog server, seleccione el destino para obtener información de auditoría.

   Solo nodos locales y **Servidor syslog externo** típicamente proporcionan un mejor rendimiento.

Opción	Descripción
Solo nodos locales	Los mensajes de auditoría, los registros de eventos de seguridad y los registros de aplicaciones no se envían a los nodos de administración. En su lugar, solo se guardan en los nodos que los han generado («el nodo local»). La información de auditoría generada en cada nodo local se almacena en `/var/local/log/localaudit.log` **Nota**: StorageGRID elimina periódicamente los registros locales en una 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.
Nodos de administración/nodos locales	Se envían mensajes de auditoría al registro de auditoría (`/var/local/log/audit.log`) En los nodos de administración, los registros de eventos de seguridad y los registros de aplicaciones se almacenan en los nodos que los han generado.
Servidor de syslog externo	La información de auditoría se envía a un servidor de syslog externo y se guarda en los nodos locales. 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 (`/var/local/log/audit.log`) En los nodos de administración, y la información de auditoría se envía al 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.

2. Seleccione **Guardar**.

   Aparecerá un mensaje de advertencia.

3. Seleccione **OK** para confirmar que desea cambiar el destino para la información de auditoría.

   Un banner verde indica que se guardó la configuración de auditoría.

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

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.