Configurare le destinazioni dei messaggi di controllo e del registro

StorageGRID 11.8

NetApp
May 17, 2024

Sommario

Configurare le destinazioni dei messaggi di controllo e del registro

Considerazioni sull'utilizzo di un server syslog esterno

Un server syslog esterno è un server esterno a StorageGRID che può essere utilizzato per raccogliere informazioni di controllo del sistema in una singola posizione. L'utilizzo di un server syslog esterno consente di ridurre il traffico di rete sui nodi Admin e di gestire le informazioni in modo più efficiente. Per StorageGRID, il formato del pacchetto di messaggi syslog in uscita è conforme con RFC 3164.

I tipi di informazioni di controllo che è possibile inviare al server syslog esterno includono:

- Registri di audit contenenti i messaggi di audit generati durante il normale funzionamento del sistema
- Eventi correlati alla sicurezza, come accessi ed escalation a root
- Log delle applicazioni che potrebbero essere richiesti se è necessario aprire un caso di supporto per risolvere un problema riscontrato

Quando utilizzare un server syslog esterno

Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. L'invio di informazioni di audit a un server syslog esterno consente di:

- Raccogliere e gestire in modo più efficiente le informazioni di audit come messaggi di audit, registri delle applicazioni ed eventi di sicurezza.
- Riduci il traffico di rete sui nodi amministrativi, perché le informazioni di audit vengono trasferite direttamente dai vari nodi storage al server syslog esterno, senza dover passare attraverso un nodo amministrativo.

> Quando i log vengono inviati a un server syslog esterno, i log singoli superiori a 8.192 byte vengono troncati alla fine del messaggio in conformità con le limitazioni comuni nelle implementazioni del server syslog esterno.

> Per massimizzare le opzioni per il recovery completo dei dati in caso di guasto del server syslog esterno, fino a 20 GB di registri locali di record di revisione (`localaudit.log`) sono mantenuti su ogni nodo.

Come configurare un server syslog esterno

Per informazioni su come configurare un server syslog esterno, vedere "Configurare i messaggi di controllo e il server syslog esterno".

Se si intende configurare l'utilizzo del protocollo TLS o RELP/TLS, è necessario disporre dei seguenti certificati:

- **Certificati CA del server**: Uno o più certificati CA attendibili per la verifica del server syslog esterno nella codifica PEM. Se omesso, verrà utilizzato il certificato Grid CA predefinito.

- **Certificato client**: Certificato client per l'autenticazione al server syslog esterno nella codifica PEM.
- **Chiave privata client**: Chiave privata per il certificato client nella codifica PEM.

> Se si utilizza un certificato client, è necessario utilizzare anche una chiave privata client. Se si fornisce una chiave privata crittografata, è necessario fornire anche la passphrase. L'utilizzo di una chiave privata crittografata non offre alcun vantaggio significativo in termini di sicurezza, in quanto è necessario memorizzare la chiave e la passphrase; per semplicità, si consiglia di utilizzare una chiave privata non crittografata, se disponibile.

Come valutare le dimensioni del server syslog esterno

Normalmente, il tuo grid è dimensionato per ottenere un throughput richiesto, definito in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potrebbe essere necessario che la griglia gestisca 1,000 operazioni S3 al secondo, o 2,000 MB al secondo, di acquisizione e recupero di oggetti. È necessario dimensionare il server syslog esterno in base ai requisiti dei dati del grid.

Questa sezione fornisce alcune formule euristiche che consentono di stimare la velocità e la dimensione media dei messaggi di log di vari tipi che il server syslog esterno deve gestire, espresse in termini di caratteristiche di performance note o desiderate della griglia (operazioni S3 al secondo).

Utilizzare le operazioni S3 al secondo nelle formule di stima

Se la griglia è stata dimensionata per un throughput espresso in byte al secondo, è necessario convertire questo dimensionamento in operazioni S3 al secondo per utilizzare le formule di stima. Per convertire il throughput della griglia, è necessario innanzitutto determinare la dimensione media degli oggetti, che è possibile utilizzare utilizzando le informazioni contenute nei registri di audit e nelle metriche esistenti (se presenti), oppure utilizzando la conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la griglia è stata dimensionata per ottenere un throughput di 2,000 MB/secondo e la dimensione media dell'oggetto è di 2 MB, la griglia è stata dimensionata in modo da poter gestire 1,000 operazioni S3 al secondo (2,000 MB/2 MB).

> Le formule per il dimensionamento del server syslog esterno nelle sezioni seguenti forniscono stime dei casi comuni (piuttosto che stime dei casi peggiori). A seconda della configurazione e del carico di lavoro, è possibile che venga visualizzata una velocità di messaggi syslog o un volume di dati syslog superiore o inferiore rispetto a quanto previsto dalle formule. Le formule devono essere utilizzate solo come linee guida.

Formule di stima per i log di audit

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule: Presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore):

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

Ad esempio, se la griglia è dimensionata per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 2,000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di 1.6 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i registri di audit, le variabili aggiuntive più importanti sono la percentuale di operazioni S3 che vengono messe (rispetto a. GETS) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni a 4 caratteri utilizzate nella tabella sono i nomi dei campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Utilizziamo P per rappresentare la percentuale di operazioni S3 che vengono messe, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Utilizzare K per rappresentare la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi il valore di K è 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione di Storage, Che è impostato su Error):

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

Ad esempio, se il tuo grid è dimensionato per 1,000 operazioni S3 al secondo, il tuo carico di lavoro è pari al 50% di put e i tuoi nomi account S3, nomi bucket, E i nomi degli oggetti hanno una media di 90 byte, il server syslog esterno deve essere dimensionato per supportare 1,500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di circa 1 MB al secondo.

Formule di stima per livelli di audit non predefiniti

Le formule fornite per i registri di controllo presuppongono l'utilizzo delle impostazioni predefinite del livello di controllo (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore). Non sono disponibili formule dettagliate per la stima del tasso e della dimensione media dei messaggi di audit

per le impostazioni del livello di audit non predefinite. Tuttavia, la seguente tabella può essere utilizzata per effettuare una stima approssimativa del tasso; è possibile utilizzare la formula delle dimensioni medie fornita per i registri di controllo, ma è probabile che si verifichi una sovrastima perché i messaggi di controllo "extra" sono, in media, più piccoli dei messaggi di controllo predefiniti.

Condizione	Formula
Replica: Tutti i livelli di controllo sono impostati su Debug o Normal	Tasso del registro di controllo = 8 x S3 tasso di operazioni
Erasure coding (codifica erasure): I livelli di audit sono tutti impostati su Debug o Normal (normale)	Utilizzare la stessa formula utilizzata per le impostazioni predefinite

Formule di stima per gli eventi di sicurezza

Gli eventi di sicurezza non sono correlati con le operazioni S3 e in genere producono un volume trascurabile di log e dati. Per questi motivi, non vengono fornite formule di stima.

Formule di stima per i log delle applicazioni

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume di log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule:

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

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 3,300 log delle applicazioni al secondo ed essere in grado di ricevere (e memorizzare) i dati del log delle applicazioni a una velocità di circa 1.2 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i log delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replica vs Erasure coding), la percentuale di operazioni S3 che vengono messe (rispetto a. Gets/Other) e la dimensione media, in byte, dei seguenti campi S3 (le abbreviazioni a 4 caratteri utilizzate nella tabella sono i nomi dei campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell’account tenant per l’utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell’account tenant per il proprietario del bucket. Utilizzato per identificare l’accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.

Codice	Campo	Descrizione
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Stime di dimensionamento di esempio

In questa sezione vengono illustrati esempi di utilizzo delle formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replica
- Erasure coding

Se si utilizza la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

```
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
```

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket e i nomi degli oggetti sono in media di 90 byte, il server syslog esterno deve essere dimensionato in modo da supportare 1800 log delle applicazioni al secondo, E riceverà (e in genere memorizzerà) i dati delle applicazioni a una velocità di 0.5 MB al secondo.

Se si utilizza l'erasure coding per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove 0 ≤ P ≤ 1 (quindi per un carico di lavoro PUT del 100%, P = 1 e per un carico DI lavoro GET del 100%, P = 0).

Sia K la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

```
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
```

Ad esempio, se il grid è dimensionato per 1.000 S3 operazioni al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket mentre i nomi degli oggetti hanno una media di 90 byte, il server syslog esterno dovrebbe essere dimensionato in modo da supportare 2.250 registri delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e generalmente archiviare) dati delle applicazioni a una velocità di 0,6 MB al secondo.

Configurare i messaggi di controllo e il server syslog esterno

È possibile configurare una serie di impostazioni relative ai messaggi di controllo. È possibile regolare il numero di messaggi di controllo registrati, definire eventuali intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client, configurare un server syslog esterno e specificare dove vengono inviati i registri di controllo, i registri degli eventi di protezione e i registri del software StorageGRID.

I messaggi e i registri di audit registrano le attività del sistema e gli eventi di sicurezza e sono strumenti essenziali per il monitoraggio e la risoluzione dei problemi. Tutti i nodi StorageGRID generano messaggi di audit e registri per tenere traccia dell'attività e degli eventi del sistema.

In alternativa, è possibile configurare un server syslog esterno per salvare le informazioni di revisione in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto delle prestazioni della registrazione dei messaggi di controllo senza ridurre la completezza dei dati di controllo. Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. Vedere "Considerazioni sul server syslog esterno" per ulteriori informazioni.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Se si prevede di configurare un server syslog esterno, è stata esaminata la "considerazioni sull'utilizzo di un server syslog esterno" e ha assicurato che il server abbia capacità sufficiente per ricevere e memorizzare i file di registro.
- Se si intende configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, si dispone della CA del server e dei certificati client richiesti e della chiave privata del client.

Modificare i livelli dei messaggi di controllo

È possibile impostare un livello di audit diverso per ciascuna delle seguenti categorie di messaggi nel registro di audit:

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di audit del sistema"
Storage	Errore	"Messaggi di audit dello storage a oggetti"
Gestione	Normale	"Messaggio di audit della gestione"
Letture del client	Normale	"Messaggi di audit in lettura del client"
Il client scrive	Normale	"Messaggi di audit di scrittura del client"
ILM	Normale	"Messaggi di controllo ILM"
Replica cross-grid	Errore	"CGRR: Richiesta di replica cross-grid"

Queste impostazioni predefinite si applicano se StorageGRID è stato installato inizialmente utilizzando la versione 10.3 o successiva. Se inizialmente è stata utilizzata una versione precedente di StorageGRID, l'impostazione predefinita per tutte le categorie è normale.

Durante gli aggiornamenti, le configurazioni a livello di audit non saranno effettive immediatamente.

Fasi

1. Selezionare **CONFIGURATION** > **Monitoring** > **Audit and syslog server**.
2. Per ciascuna categoria di messaggi di audit, selezionare un livello di audit dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Non vengono registrati messaggi di audit della categoria.
Errore	Vengono registrati solo messaggi di errore - messaggi di audit per i quali il codice risultato non è stato "riuscito" (SUCS).
Normale	Vengono registrati i messaggi transazionali standard, ovvero i messaggi elencati in queste istruzioni per la categoria.
Debug	Obsoleto. Questo livello si comporta come il livello di audit normale.

I messaggi inclusi per qualsiasi livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad esempio, il livello normale include tutti i messaggi di errore.

> Se non si richiede un record dettagliato delle operazioni di lettura del client per le applicazioni S3, modificare l'impostazione **letture del client** su **errore** per ridurre il numero di messaggi di audit registrati nel registro di audit.

3. Selezionare **Salva**.

   Un banner verde indica che la configurazione è stata salvata.

Definire le intestazioni delle richieste HTTP

Facoltativamente, è possibile definire qualsiasi intestazione di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client. Queste intestazioni di protocollo si applicano solo alle richieste S3 e Swift.

Fasi

1. Nella sezione **Audit Protocol headers**, definire le intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client.

   Utilizzare un asterisco (**) come carattere jolly per far corrispondere zero o più caratteri. Utilizzare la sequenza escape (**) per far corrispondere un asterisco letterale.

2. Selezionare **Add another header** (Aggiungi un'altra intestazione) per creare altre intestazioni, se necessario.

   Quando le intestazioni HTTP vengono trovate in una richiesta, vengono incluse nel messaggio di audit nel campo HTRH.

   > Le intestazioni delle richieste del protocollo di audit vengono registrate solo se il livello di audit per **letture client** o **scritture client** non è **disattivato**.

3. Selezionare **Salva**

   Un banner verde indica che la configurazione è stata salvata.

Usa un server syslog esterno

In alternativa, è possibile configurare un server syslog esterno per salvare registri di controllo, registri delle applicazioni e registri di eventi di sicurezza in una posizione esterna alla griglia.

> Se non si desidera utilizzare un server syslog esterno, ignorare questo passaggio e passare a. Selezionare le destinazioni delle informazioni di audit.

> Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili da soddisfare le proprie esigenze, è possibile applicare ulteriori opzioni di configurazione utilizzando `audit-destinations` Endpoint, che si trovano nella sezione API privata di "API di Grid Management". Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per diversi gruppi di nodi.

Inserire le informazioni di syslog

Accedere alla procedura guidata Configura server syslog esterno e fornire le informazioni di cui StorageGRID

ha bisogno per accedere al server syslog esterno.

Fasi

1. Dalla pagina Audit and syslog server (controllo e server syslog), selezionare **Configure external syslog server** (Configura server syslog esterno Oppure, se è stato precedentemente configurato un server syslog esterno, selezionare **Modifica server syslog esterno**.

   Viene visualizzata la procedura guidata Configura server syslog esterno.

2. Per la fase **inserire le informazioni syslog** della procedura guidata, immettere un nome di dominio completo valido o un indirizzo IPv4 o IPv6 per il server syslog esterno nel campo **host**.
3. Inserire la porta di destinazione sul server syslog esterno (deve essere un numero intero compreso tra 1 e 65535). La porta predefinita è 514.
4. Selezionare il protocollo utilizzato per inviare le informazioni di audit al server syslog esterno.

   Si consiglia di utilizzare **TLS** o **RELP/TLS**. Per utilizzare una di queste opzioni, è necessario caricare un certificato del server. L'utilizzo dei certificati consente di proteggere le connessioni tra la griglia e il server syslog esterno. Per ulteriori informazioni, vedere "Gestire i certificati di sicurezza".

   Tutte le opzioni del protocollo richiedono il supporto e la configurazione del server syslog esterno. È necessario scegliere un'opzione compatibile con il server syslog esterno.

   > Il protocollo RELP (Reliable Event Logging Protocol) estende le funzionalità del protocollo syslog per fornire un'erogazione affidabile dei messaggi di evento. L'utilizzo di RELP può contribuire a prevenire la perdita di informazioni di controllo nel caso in cui il server syslog esterno debba essere riavviato.

5. Selezionare **continua**.
6. se si seleziona **TLS** o **RELP/TLS**, caricare i certificati CA del server, il certificato client e la chiave privata del client.
   a. Selezionare **Sfoglia** per il certificato o la chiave che si desidera utilizzare.
   b. Selezionare il certificato o il file della chiave.
   c. Selezionare **Open** per caricare il file.

      Accanto al nome del certificato o del file della chiave viene visualizzato un segno di spunta verde che indica che il caricamento è stato eseguito correttamente.

7. Selezionare **continua**.

Gestire il contenuto syslog

È possibile selezionare le informazioni da inviare al server syslog esterno.

Fasi

1. Per la fase **Gestisci contenuto syslog** della procedura guidata, selezionare ogni tipo di informazione di audit che si desidera inviare al server syslog esterno.

   - **Invia log di audit**: Invia eventi StorageGRID e attività di sistema
   - **Invia eventi di sicurezza**: Invia eventi di sicurezza, ad esempio quando un utente non autorizzato tenta di effettuare l'accesso o un utente accede come root

- **Send application logs**: Invia file di log utili per la risoluzione dei problemi, tra cui:
  - `bycast-err.log`
  - `bycast.log`
  - `jaeger.log`
  - `nms.log` (Solo nodi di amministrazione)
  - `prometheus.log`
  - `raft.log`
  - `hagroups.log`

Per informazioni sui registri del software StorageGRID, vedere "Log del software StorageGRID".

2. Utilizzare i menu a discesa per selezionare la gravità e la struttura (tipo di messaggio) per ciascuna categoria di informazioni di controllo che si desidera inviare.

   L'impostazione dei valori di gravità e struttura consente di aggregare i registri in modo personalizzabile per semplificare l'analisi.

   a. Per **gravità**, selezionare **Passthrough** oppure selezionare un valore di gravità compreso tra 0 e 7.

      Se si seleziona un valore, il valore selezionato verrà applicato a tutti i messaggi di questo tipo. Le informazioni sui diversi livelli di gravità andranno perse se si sovrascrive la gravità con un valore fisso.

Severità	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di gravità di quando è stato registrato localmente sul nodo: • Per i registri di controllo, la gravità è "info". • Per gli eventi di sicurezza, i valori di gravità sono generati dalla distribuzione Linux sui nodi. • Per i registri delle applicazioni, i livelli di gravità variano tra "info" e "avviso", a seconda del problema. Ad esempio, aggiungendo un server NTP e configurando un gruppo ha si ottiene il valore "info", mentre arrestando intenzionalmente il servizio SSM o RSM si ottiene il valore "avviso".
0	Emergenza: Il sistema non è utilizzabile
1	Attenzione: L'azione deve essere eseguita immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore
4	Avvertenza: Condizioni di avviso
5	Avviso: Condizione normale ma significativa

Severità	Descrizione
6	Informativo: Messaggi informativi
7	Debug: Messaggi a livello di debug

b. Per **Facilty**, selezionare **Passthrough** o selezionare un valore di struttura compreso tra 0 e 23.

   Se si seleziona un valore, questo verrà applicato a tutti i messaggi di questo tipo. Le informazioni sulle diverse strutture andranno perse se si sostituisce la struttura con un valore fisso.

Struttura	Descrizione

Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di struttura di quando è stato collegato localmente al nodo:
	• Per i registri di controllo, la struttura inviata al server syslog esterno è "local7".
	• Per gli eventi di sicurezza, i valori della struttura vengono generati dalla distribuzione linux sui nodi.
	• Per i registri delle applicazioni, i registri delle applicazioni inviati al server syslog esterno presentano i seguenti valori di struttura:
	  ◦ `bycast.log`: utente o daemon
	  ◦ `bycast-err.log`: utente, daemon, local3 o local4
	  ◦ `jaeger.log`: local2
	  ◦ `nms.log`: local3
	  ◦ `prometheus.log`: local4
	  ◦ `raft.log`: local5
	  ◦ `hagroups.log`: local6

0	kern (messaggi kernel)
1	utente (messaggi a livello utente)
2	mail
3	daemon (daemon di sistema)
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)
6	lpr (sottosistema di stampanti di linea)

Struttura	Descrizione
7	news (sottosistema notizie di rete)
8	UUCP
9	cron (daemon di clock)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (audit del log)
14	logalert (avviso di log)
15	clock (daemon di clock)
16	local0
17	locale1
18	locale2
19	locale3
20	locale4
21	locale5
22	locale6
23	locale7

3. Selezionare **continua**.

Inviare messaggi di test

Prima di iniziare a utilizzare un server syslog esterno, è necessario richiedere a tutti i nodi della griglia di inviare messaggi di test al server syslog esterno. È necessario utilizzare questi messaggi di test per convalidare l'intera infrastruttura di raccolta dei log prima di inviare i dati al server syslog esterno.

> Non utilizzare la configurazione del server syslog esterno fino a quando non si conferma che il server syslog esterno ha ricevuto un messaggio di test da ciascun nodo della griglia e che il messaggio è stato elaborato come previsto.

Fasi

1. Se non si desidera inviare messaggi di test perché si è certi che il server syslog esterno sia configurato correttamente e che sia in grado di ricevere informazioni di controllo da tutti i nodi della griglia, selezionare **Ignora e termina**.

   Un banner verde indica che la configurazione è stata salvata.

2. In caso contrario, selezionare **Invia messaggi di prova** (scelta consigliata).

   I risultati del test vengono visualizzati continuamente sulla pagina fino a quando non si interrompe il test. Mentre il test è in corso, i messaggi di controllo continuano a essere inviati alle destinazioni precedentemente configurate.

3. Se si ricevono errori, correggerli e selezionare di nuovo **Invia messaggi di prova**.

   Vedere "Risolvere i problemi di un server syslog esterno" per risolvere eventuali errori.

4. Attendere che venga visualizzato un banner verde che indica che tutti i nodi hanno superato il test.
5. Controllare il server syslog per determinare se i messaggi di test vengono ricevuti ed elaborati come previsto.

   Se si utilizza UDP, controllare l'intera infrastruttura di raccolta dei log. Il protocollo UDP non consente un rilevamento degli errori rigoroso come l'altro protocolli.

6. Selezionare **Stop and Finish** (Interrompi e termina).

   Viene nuovamente visualizzata la pagina **Audit and syslog server**. Un banner verde indica che la configurazione del server syslog è stata salvata.

   Le informazioni di audit StorageGRID non vengono inviate al server syslog esterno finché non si seleziona una destinazione che include il server syslog esterno.

Selezionare le destinazioni delle informazioni di audit

È possibile specificare la posizione dei registri di controllo, dei registri eventi di protezione e. "Log del software StorageGRID" vengono inviati.

Alcune destinazioni sono disponibili solo se è stato configurato un server syslog esterno.

Fasi

1. Nella pagina Audit and syslog server (Server audit e syslog), selezionare la destinazione per le informazioni di audit.

   Solo nodi locali e **Server syslog esterno** in genere offrono prestazioni migliori.

Opzione	Descrizione
Solo nodi locali	I messaggi di controllo, i registri degli eventi di protezione e i registri delle applicazioni non vengono inviati ai nodi amministrativi. Vengono invece salvati solo sui nodi che li hanno generati ("nodo locale"). Le informazioni di controllo generate su ogni nodo locale sono memorizzate in `/var/local/log/localaudit.log` **Nota**: StorageGRID rimuove periodicamente i log locali in una rotazione per liberare spazio. Quando il file di log di un nodo raggiunge 1 GB, il file esistente viene salvato e viene avviato un nuovo file di log. Il limite di rotazione per il log è di 21 file. Quando viene creata la ventiduesima versione del file di log, il file di log più vecchio viene cancellato. In media, su ciascun nodo vengono memorizzati circa 20 GB di dati di log.
Nodi amministrativi/nodi locali	I messaggi di audit vengono inviati al registro di audit (`/var/local/log/audit.log`) Sui nodi Admin, i registri degli eventi di protezione e i registri delle applicazioni sono memorizzati sui nodi che li hanno generati.
Server syslog esterno	Le informazioni di audit vengono inviate a un server syslog esterno e salvate sui nodi locali. Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.
Nodo di amministrazione e server syslog esterno	I messaggi di audit vengono inviati al registro di audit (`/var/local/log/audit.log`) Sui nodi Admin, e le informazioni di controllo vengono inviate al server syslog esterno e salvate sul nodo locale. Il tipo di informazioni inviate dipende dalla configurazione del server syslog esterno. Questa opzione viene attivata solo dopo aver configurato un server syslog esterno.

2. Selezionare **Salva**.

   Viene visualizzato un messaggio di avviso.

3. Selezionare **OK** per confermare che si desidera modificare la destinazione per le informazioni di controllo.

   Un banner verde indica che la configurazione di controllo è stata salvata.

   I nuovi registri vengono inviati alle destinazioni selezionate. I registri esistenti rimangono nella posizione corrente.