Verwenden Sie einen externen Syslog-Server

StorageGRID 11.7

NetApp
April 12, 2024

Inhalt

Verwenden Sie einen externen Syslog-Server

Überlegungen für externen Syslog-Server

Anhand der folgenden Richtlinien können Sie die Größe des benötigten externen Syslog-Servers einschätzen.

Was ist ein externer Syslog-Server?

Ein externer Syslog-Server ist ein Server außerhalb von StorageGRID, mit dem Sie Audit-Informationen zum System an einem Ort sammeln können. Mithilfe eines externen Syslog-Servers können Sie die Ziele Ihrer Audit-Informationen konfigurieren, sodass Sie den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten können. Folgende Arten von Audit-Informationen können Sie an den externen Syslog-Server senden:

- Prüfprotokolle mit den während des normalen Systembetriebs erzeugten Audit-Meldungen
- Sicherheitsbezogene Ereignisse wie Anmeldungen und Eskalationen im Root-Bereich
- Anwendungsprotokolle, die angefordert werden können, wenn ein Support-Fall geöffnet werden muss, um die Behebung eines aufgetretenen Problems zu beheben

Wie schätzen Sie die Größe des externen Syslog-Servers ein

In der Regel wird das Grid so dimensioniert, dass es einen erforderlichen Durchsatz erzielt, der mit S3-Operationen pro Sekunde oder Byte pro Sekunde definiert wird. Möglicherweise müssen Sie z. B. angeben, dass Ihr Grid 1,000 S3-Operationen pro Sekunde oder 2,000 MB pro Sekunde der Objektingest und -Abruf verarbeiten muss. Sie sollten die Größe Ihres externen Syslog-Servers entsprechend den Datenanforderungen Ihres Grid festlegen.

Dieser Abschnitt enthält einige heuristische Formeln, mit denen Sie die Rate und die durchschnittliche Größe von Protokollmeldungen verschiedener Arten bewerten können, die Ihr externer Syslog-Server in der Lage sein muss, anhand der bekannten oder gewünschten Performance-Merkmale des Grid (S3-Operationen pro Sekunde) auszuführen.

In Schätzformeln S3-Operationen pro Sekunde verwenden

Wenn Ihr Grid für einen Durchsatz in Byte pro Sekunde ausgedrückt wurde, müssen Sie diese Größe in S3-Vorgänge pro Sekunde konvertieren, um die Abschätzung-Formeln zu verwenden. Um den Grid-Durchsatz zu konvertieren, müssen Sie zunächst die durchschnittliche Objektgröße festlegen, die Sie anhand der Informationen in vorhandenen Audit-Protokollen und -Metriken (falls vorhanden) durchführen können, oder indem Sie Ihre Kenntnisse über die Anwendungen nutzen, die StorageGRID verwenden. Beispiel: Wenn Ihr Grid einen Durchsatz von 2,000 MB/s erreicht hat und die durchschnittliche Objektgröße 2 MB beträgt, wurde das Grid so dimensioniert, dass es 1,000 S3-Operationen pro Sekunde (2,000 MB/2 MB) verarbeiten kann.

> Die Formeln für die externe Syslog-Server-Größenbemessung in den folgenden Abschnitten liefern allgemeine Schätzungen (und nicht die Schlimmstfall-Schätzungen). Je nach Konfiguration und Workload wird möglicherweise eine höhere oder niedrigere Rate von Syslog-Meldungen oder ein höheres Volumen an Syslog-Daten angezeigt als die Formel „Predict“. Die Formeln sind nur als Richtlinien zu verwenden.

Schätzformeln für Prüfprotokolle

Wenn Sie über keine Informationen zu Ihrem S3-Workload verfügen außer der Anzahl der S3-Vorgänge pro Sekunde, die Ihr Grid unterstützen soll, können Sie die Menge der Audit-Protokolle schätzen, die Ihr externer Syslog-Server anhand der folgenden Formeln verarbeiten muss. Unter der Annahme, dass Sie die Audit-Level auf die Standardwerte (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist):

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

Wenn Ihr Grid beispielsweise für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, sollte der externe Syslog-Server entsprechend angepasst werden und 2,000 Syslog-Nachrichten pro Sekunde unterstützen. Er sollte Audit-Protokolldaten von 1.6 MB pro Sekunde empfangen (und in der Regel speichern) können.

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Die wichtigsten zusätzlichen Variablen sind für Audit-Protokolle der Prozentsatz der am häufigsten verwendeten S3-Vorgänge (im Vergleich zu RUFT) und die mittlere Größe der folgenden S3-Felder in Byte (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.

Verwenden wir P, um den Prozentsatz der an Put-Vorgängen abzubilden, wobei 0 ≤ P ≤ 1 (für einen 100 % PUT-Workload, P = 1 und für einen 100 % GET-Workload, P = 0).

Verwenden wir K als Darstellung der durchschnittlichen Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann ist der Wert von K 90 (13+13+28+36).

Wenn Sie Werte für P und K festlegen können, können Sie die Menge der Audit-Protokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss. Dabei wird davon ausgegangen, dass Sie die Audit-Level auf die Standardwerte setzen (alle Kategorien sind auf Normal gesetzt, außer Speicher, Die auf Fehler gesetzt ist):

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

Wenn Ihr Grid beispielsweise 1,000 S3-Operationen pro Sekunde angepasst ist, beträgt der Workload 50 % Put-Vorgänge sowie die S3-Kontonamen und Bucket-Namen Und Objektnamen durchschnittlich 90 Byte, Ihr externer Syslog-Server sollte Größe haben, um 1,500 Syslog-Nachrichten pro Sekunde zu unterstützen. Er sollte Audit-Protokolldaten mit einer Rate von ca. 1 MB pro Sekunde empfangen (und in der Regel speichern) können.

Schätzformeln für nicht standardmäßige Audit-Level

Die für Prüfprotokolle bereitgestellten Formeln setzen voraus, dass die standardmäßigen Einstellungen für die Revisionsstufe verwendet werden (alle Kategorien sind auf Normal gesetzt, außer Speicher, der auf Fehler gesetzt ist). Detaillierte Formeln zur Schätzung der Rate und der durchschnittlichen Größe von Überwachungsmeldungen für nicht standardmäßige Überwachungseinstellungen sind nicht verfügbar. Die folgende Tabelle kann jedoch verwendet werden, um eine grobe Schätzung der Rate zu machen; Sie können die Formel für die durchschnittliche Größe von Audit-Protokollen verwenden, aber beachten Sie, dass sie wahrscheinlich zu einer Überschätzung führen wird, da die „zusätzlichen“ Audit-Meldungen im Durchschnitt kleiner sind als die standardmäßigen Audit-Meldungen.

Zustand	Formel
Replikation: Audit-Level alle auf Debug oder Normal eingestellt	Audit-Protokollrate = 8 x S3-Betriebsrate
Verfahren zur Einhaltung von Datenkonsistenz: Für Audit-Level ist Debug oder Normal festgelegt	Verwenden Sie die gleiche Formel wie für die Standardeinstellungen

Schätzformeln für Sicherheitsereignisse

Sicherheitsereignisse werden nicht mit S3-Vorgängen in Beziehung gesetzt und erzeugen in der Regel eine vernachlässigbare Menge an Protokollen und Daten. Aus diesen Gründen werden keine Schätzformeln bereitgestellt.

Schätzformeln für Anwendungsprotokolle

Wenn neben der Anzahl der S3-Vorgänge pro Sekunde, die Ihr Grid unterstützen soll, keine Informationen zu Ihrem S3-Workload vorhanden sind, können Sie das Volumen der Anwendungen schätzen. Protokolle, die Ihr externer Syslog-Server verarbeiten muss, werden gemäß den folgenden Formeln verwendet:

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

Wenn Ihr Grid also für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, sollte der externe Syslog-Server entsprechend dimensioniert sein, um 3,300 Applikations-Logs pro Sekunde zu unterstützen und Applikations-Protokolldaten von etwa 1.2 MB pro Sekunde zu empfangen (und zu speichern).

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Die wichtigsten zusätzlichen Variablen sind für Applikations-Protokolle die Datensicherungsstrategie (Replizierung vs Erasure

Coding) – der Prozentsatz der S3-Operationen, die durchgeführt werden (im Vergleich zu Ruft/Other) und die durchschnittliche Größe der folgenden S3-Felder (in der Tabelle werden 4-Zeichen-Abkürzungen verwendet):

Codieren	Feld	Beschreibung
SACC	S3-Mandantenkontoname (Absender der Anfrage)	Der Name des Mandantenkontos für den Benutzer, der die Anforderung gesendet hat. Für anonyme Anfragen leer.
SBAC	S3-Mandantenkontoname (Bucket-Eigentümer)	Der Mandantenkontoname für den Bucket-Eigentümer. Wird zur Identifizierung von Account- oder anonymen Zugriffen verwendet.
S3BK	S3-Bucket	Der S3-Bucket-Name
S3KY	S3-Schlüssel	Der S3-Schlüsselname, nicht einschließlich des Bucket-Namens. Vorgänge in Buckets enthalten dieses Feld nicht.

Beispiel für eine Einschätzung der Dimensionierung

In diesem Abschnitt werden Beispielbeispiele erläutert, wie man die Schätzformeln für Raster mit den folgenden Methoden der Datensicherung verwendet:

- Replizierung
- Verfahren Zur Einhaltung Von Datenkonsistenz

Wenn Sie Replizierung für die Datensicherung verwenden

Stellen Sie P den Prozentsatz der an Put-Vorgängen dar, wobei 0 ≤ P ≤ 1 (für einen 100 % PUT-Workload, P = 1 und für einen 100 % GET-Workload, P = 0).

K stellen die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel dar. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss.

```
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
```

Wenn Ihr Grid beispielsweise für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, beträgt der Workload 50 % und Ihre S3-Kontonamen, Bucket-Namen und Objektnamen durchschnittlich 90 Byte, sollte der externe Syslog-Server entsprechend angepasst werden, um 1800 Applikations-Logs pro Sekunde zu unterstützen,

Und erhalten Applikationsdaten mit einer Rate von 0.5 MB pro Sekunde (und in der Regel auch dort).

Bei Verwendung von Erasure Coding zur Datensicherung

Stellen Sie P den Prozentsatz der an Put-Vorgängen dar, wobei 0 ≤ P ≤ 1 (für einen 100 % PUT-Workload, P = 1 und für einen 100 % GET-Workload, P = 0).

K stellen die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel dar. Angenommen, der S3-Kontoname ist immer mein-s3-Konto (13 Byte), Buckets haben feste Längennamen wie /my/Application/bucket12345 (28 Bytes), und Objekte haben Schlüssel mit fester Länge wie 5733a5d7-f069-41ef-8fbd-13247494c69c (36 Bytes). Dann hat K einen Wert von 90 (13+13+28+36).

Wenn Sie Werte für P und K bestimmen können, können Sie die Menge der Anwendungsprotokolle schätzen, die Ihr externer Syslog-Server mit den folgenden Formeln verarbeiten muss.

```
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
```

Wenn Ihr Grid beispielsweise 1,000 S3-Vorgänge pro Sekunde beträgt, beträgt der Workload 50 % der Put-Vorgänge sowie Ihre S3-Kontonamen und Bucket-Namen Und Objektnamen durchschnittlich 90 Byte, Ihr externer Syslog-Server sollte Größe haben, um 2,250 Anwendungsprotokolle pro Sekunde zu unterstützen. Sie sollten in der Lage sein, Anwendungsdaten zu empfangen und zu empfangen (und in der Regel speichern) mit einer Rate von 0.6 MB pro Sekunde.

Weitere Informationen zum Konfigurieren von Meldungsebenen und einem externen Syslog-Server finden Sie unter:

- "Konfigurieren Sie einen externen Syslog-Server"
- "Konfigurieren von Überwachungsmeldungen und Protokollzielen"

Konfigurieren Sie einen externen Syslog-Server

Wenn Sie Audit-Protokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Speicherort außerhalb des Grid speichern möchten, konfigurieren Sie einen externen Syslog-Server mithilfe dieses Verfahrens.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie verfügen über einen Syslog-Server mit der Kapazität, die Protokolldateien zu empfangen und zu speichern. Weitere Informationen finden Sie unter "Überlegungen für externen Syslog-Server".
- Sie haben die richtigen Server- und Client-Zertifizierungen, wenn Sie TLS oder RELP/TLS verwenden möchten.

Über diese Aufgabe

Wenn Sie Audit-Informationen an einen externen Syslog-Server senden möchten, müssen Sie zuerst den externen Server konfigurieren.

Durch das Senden von Audit-Informationen an einen externen Syslog-Server können Sie:

- Effizientere Erfassung und Verwaltung von Audit-Informationen wie Audit-Nachrichten, Applikationsprotokollen und Sicherheitsereignissen
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da Audit-Informationen direkt von den verschiedenen Speicherknoten auf den externen Syslog-Server übertragen werden, ohne über einen Admin-Knoten gehen zu müssen

> Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit einer Größe von mehr als 8192 Byte am Ende der Nachricht gekürzt, um den allgemeinen Einschränkungen in externen Syslog-Server-Implementierungen zu entsprechen.

> Um die Optionen für eine vollständige Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers zu maximieren, werden auf jedem Knoten bis zu 20 GB an lokalen Protokollen von Audit-Datensätzen (localaudit.log) aufbewahrt.

> Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können zusätzliche Konfigurationsoptionen mithilfe der privaten API angewendet werden `audit-destinations` Endpunkte: So ist es beispielsweise möglich, unterschiedliche Syslog-Server für unterschiedliche Node-Gruppen zu verwenden.

Konfigurieren Sie den externen Server

Greifen Sie auf den Assistenten zu

Rufen Sie zum Starten den Assistenten zum Konfigurieren des externen Syslog-Servers auf.

Schritte

1. Wählen Sie **CONFIGURATION** > **Monitoring** > **Audit und Syslog-Server**.
2. Wählen Sie auf der Seite Audit- und Syslog-Server die Option **externen Syslog-Server konfigurieren** aus. Wenn Sie zuvor einen externen Syslog-Server konfiguriert haben, wählen Sie **Externe Syslog-Server bearbeiten**.

   Der Assistent zum Konfigurieren des externen Syslog-Servers wird angezeigt.

Syslog-Informationen eingeben

Sie müssen die Informationen angeben, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. Geben Sie für den Schritt **Enter syslog info** des Assistenten einen gültigen vollständig qualifizierten Domänennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server in das Feld **Host** ein.
2. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine Ganzzahl zwischen 1 und 65535 sein). Der Standardport ist 514.
3. Wählen Sie das Protokoll aus, das zum Senden von Audit-Informationen an den externen Syslog-Server verwendet wird.

Die Verwendung von **TLS** oder **RELP/TLS** wird empfohlen. Sie müssen ein Serverzertifikat hochladen, um eine dieser Optionen verwenden zu können. Mithilfe von Zertifikaten lassen sich die Verbindungen zwischen dem Grid und dem externen Syslog-Server sichern. Weitere Informationen finden Sie unter "Verwalten von Sicherheitszertifikaten".

Für alle Protokolloptionen muss der externe Syslog-Server unterstützt und konfiguriert werden. Sie müssen eine Option wählen, die mit dem externen Syslog-Server kompatibel ist.

> ⓘ Reliable Event Logging Protocol (RELP) erweitert die Funktionalität des Syslog-Protokolls für eine zuverlässige Bereitstellung von Ereignismeldungen. Mithilfe von RELP können Sie den Verlust von Audit-Informationen verhindern, wenn Ihr externer Syslog-Server neu gestartet werden muss.

4. Wählen Sie **Weiter**.
5. Wenn Sie **TLS** oder **RELP/TLS** ausgewählt haben, laden Sie die folgenden Zertifikate hoch:
   - **Server CA-Zertifikate**: Ein oder mehrere vertrauenswürdige CA-Zertifikate zur Überprüfung des externen Syslog-Servers (in PEM-Codierung). Wenn nicht angegeben, wird das Standard-Grid-CA-Zertifikat verwendet. Die Datei, die Sie hier hochladen, kann ein CA-Bundle sein.
   - **Clientzertifikat**: Das Clientzertifikat zur Authentifizierung an den externen Syslog-Server (in PEM-Codierung).
   - **Privater Client-Schlüssel**: Privater Schlüssel für das Clientzertifikat (in PEM-Kodierung).

     > ⓘ Wenn Sie ein Clientzertifikat verwenden, müssen Sie auch einen privaten Clientschlüssel verwenden. Wenn Sie einen verschlüsselten privaten Schlüssel angeben, müssen Sie auch die Passphrase angeben. Die Verwendung eines verschlüsselten privaten Schlüssels bietet keine wesentlichen Sicherheitsvorteile, da Schlüssel und Passphrase gespeichert werden müssen. Aus Gründen der Einfachheit wird die Verwendung eines unverschlüsselten privaten Schlüssels empfohlen.

     i. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel, das Sie verwenden möchten.
     ii. Wählen Sie die Zertifikatdatei oder die Schlüsseldatei aus.
     iii. Wählen Sie **Öffnen**, um die Datei hochzuladen.

     Neben dem Zertifikat- oder Schlüsseldateinamen wird eine grüne Prüfung angezeigt, die Sie darüber informiert, dass das Zertifikat erfolgreich hochgeladen wurde.
6. Wählen Sie **Weiter**.

Syslog-Inhalte managen

Sie können auswählen, welche Informationen an den externen Syslog-Server gesendet werden sollen.

Schritte

1. Wählen Sie für den Schritt **syslog-Inhalt verwalten** des Assistenten jeden Typ von Audit-Informationen aus, die Sie an den externen syslog-Server senden möchten.
   - **Audit-Protokolle senden**: Sendet StorageGRID-Ereignisse und Systemaktivitäten
   - **Sicherheitsereignisse senden**: Sendet Sicherheitsereignisse, z. B. wenn ein nicht autorisierter Benutzer versucht sich anzumelden oder sich ein Benutzer als root anmeldet
   - **Send Application logs**: Sendet Log-Dateien nützlich für die Fehlersuche einschließlich:

- `bycast-err.log`
- `bycast.log`
- `jaeger.log`
- `nms.log` (Nur Admin-Nodes)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

2. Verwenden Sie die Dropdown-Menüs, um den Schweregrad und die Einrichtung (Nachrichtentyp) für die Kategorie der zu sendenden Audit-Informationen auszuwählen.

   Wenn Sie **Passthrough** für Schweregrad und Einrichtung auswählen, erhalten die an den Remote-Syslog-Server gesendeten Informationen denselben Schweregrad und dieselbe Einrichtung wie bei der lokalen Anmeldung am Node. Durch die Festlegung von Standort und Schweregrad können Sie die Protokolle individuell zusammenlegen und so die Analyse erleichtern.

   Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter "StorageGRID-Softwareprotokolle".

   a. Wählen Sie für **Severity Passthrough** aus, wenn jede Nachricht, die an das externe Syslog gesendet wird, den gleichen Schweregrad wie im lokalen Syslog hat.

      Wenn Sie für Überwachungsprotokolle **Passthrough** auswählen, lautet der Schweregrad 'Info'.

      Wenn Sie für Sicherheitsereignisse **Passthrough** auswählen, werden die Schweregrade von der Linux-Distribution auf den Knoten generiert.

      Wenn Sie bei Anwendungsprotokollen **Passthrough** auswählen, variieren die Schweregrade je nach Problem zwischen 'info' und 'Hinweis'. Wenn Sie beispielsweise einen NTP-Server hinzufügen und eine HA-Gruppe konfigurieren, wird der Wert „Info“ angezeigt, während der SSM- oder RSM-Dienst absichtlich angehalten wird, wird der Wert „Hinweis“ angezeigt.

   b. Wenn Sie den Passthrough-Wert nicht verwenden möchten, wählen Sie einen Schweregrad zwischen 0 und 7 aus.

      Der ausgewählte Wert wird auf alle Meldungen dieses Typs angewendet. Informationen zu den verschiedenen Schweregraden gehen verloren, wenn Sie den Schweregrad mit einem festen Wert überschreiben.

Schweregrad	Beschreibung
0	Notfall: System ist unbrauchbar
1	Warnung: Maßnahmen müssen sofort ergriffen werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen

Schweregrad	Beschreibung
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber bedeutender Zustand
6	Information: Informationsmeldungen
7	Debug: Debug-Level-Meldungen

c. Wählen Sie für **Einrichtung Passthrough** aus, wenn jede Nachricht, die an das externe Syslog gesendet wird, den gleichen Wert wie im lokalen Syslog hat.

   Wenn Sie für Überwachungsprotokolle **Passthrough** auswählen, lautet die an den externen Syslog-Server gesendete Einrichtung „local7“.

   Wenn Sie bei Sicherheitsereignissen **Passthrough** wählen, werden die Facility-Werte durch die linux-Distribution auf den Knoten generiert.

   Wenn Sie bei Anwendungsprotokollen **Passthrough** auswählen, haben die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Facility-Werte:

Applikationsprotokoll	Durchlasswert
bycast.log	Benutzer oder Daemon
bycast-err.log	Benutzer, Daemon, local3 oder local4
jaeger.log	local2
nms.log	Lokalisierung 3
prometheus.log	local4
raft.log	Lokalisierung 5
hagroups.log	Lokalisierung 6

d. Wenn Sie den Passthrough-Wert nicht verwenden möchten, wählen Sie den Einrichtungswert zwischen 0 und 23 aus.

   Der ausgewählte Wert wird auf alle Meldungen dieses Typs angewendet. Informationen über verschiedene Einrichtungen gehen verloren, wenn Sie eine Anlage mit einem festen Wert überschreiben möchten.

Anlage	Beschreibung
0	kern (Kernelmeldungen)

Anlage	Beschreibung
1	Benutzer (Meldungen auf Benutzerebene)
2	E-Mail
3	Daemon (Systemdemonen)
4	Auth (Sicherheits-/Autorisierungsmeldungen)
5	Syslog (intern erzeugte Nachrichten durch syslogd)
6	lpr (Liniendrucker-Subsystem)
7	nachrichten (Netzwerk-News-Subsystem)
8	UUCP
9	Cron (Clock Daemon)
10	Sicherheit (Sicherheits-/Autorisierungsmeldungen)
11	FTP
12	NTP
13	Logaudit (Protokollaudit)
14	Logalert (Protokollwarnung)
15	Uhr (Uhrzeitdaemon)
16	Local0
17	local1
18	local2
19	Lokalisierung 3
20	local4
21	Lokalisierung 5
22	Lokalisierung 6

Anlage	Beschreibung
23	Local7

3. Wählen Sie **Weiter**.

Versenden von Testmeldungen

Bevor Sie beginnen, einen externen Syslog-Server zu verwenden, sollten Sie anfordern, dass alle Knoten im Raster Testmeldungen an den externen Syslog-Server senden. Sie sollten diese Testmeldungen verwenden, um Sie bei der Validierung Ihrer gesamten Protokollierungs-Infrastruktur zu unterstützen, bevor Sie Daten an den externen Syslog-Server senden.

> Verwenden Sie die Konfiguration des externen Syslog-Servers erst, wenn Sie bestätigen, dass der externe Syslog-Server von jedem Knoten in Ihrem Raster eine Testmeldung erhalten hat und dass die Nachricht erwartungsgemäß verarbeitet wurde.

Schritte

1. Wenn Sie keine Testnachrichten senden möchten, weil Sie sicher sind, dass Ihr externer Syslog-Server korrekt konfiguriert ist und Audit-Informationen von allen Knoten in Ihrem Raster empfangen kann, wählen Sie **Überspringen und Beenden**.

   Ein grünes Banner zeigt an, dass Ihre Konfiguration erfolgreich gespeichert wurde.

2. Andernfalls wählen Sie **Testmeldungen senden** (empfohlen).

   Die Testergebnisse werden kontinuierlich auf der Seite angezeigt, bis Sie den Test beenden. Während der Test läuft, werden Ihre Audit-Meldungen weiterhin an Ihre zuvor konfigurierten Ziele gesendet.

3. Wenn Sie Fehler erhalten, korrigieren Sie diese und wählen Sie **Testmeldungen senden** erneut.

   Siehe "Fehlerbehebung beim externen Syslog-Server" Um Ihnen bei der Behebung von Fehlern zu helfen.

4. Warten Sie, bis ein grünes Banner angezeigt wird, dass alle Nodes die Tests bestanden haben.
5. Überprüfen Sie den Syslog-Server, ob Testmeldungen empfangen und verarbeitet werden wie erwartet.

   > Wenn Sie UDP verwenden, überprüfen Sie Ihre gesamte Log-Collection-Infrastruktur. Das UDP-Protokoll ermöglicht keine so strenge Fehlererkennung wie die anderen Protokolle.

6. Wählen Sie **Stop and Finish**.

   Sie gelangen zurück zur Seite **Audit und Syslog Server**. Ein grünes Banner zeigt an, dass Ihre Syslog-Serverkonfiguration erfolgreich gespeichert wurde.

   > Die StorageGRID-Audit-Informationen werden erst an den externen Syslog-Server gesendet, wenn Sie ein Ziel auswählen, das den externen Syslog-Server enthält.

Wählen Sie Ziele für Audit-Informationen aus

Sie können festlegen, wo Sicherheitsereignisprotokolle, Anwendungsprotokolle und Prüfmeldungsprotokolle gesendet werden.

Weitere Informationen zu StorageGRID-Softwareprotokollen finden Sie unter "StorageGRID-Softwareprotokolle".

Schritte

1. Wählen Sie auf der Seite Audit- und Syslog-Server aus den aufgeführten Optionen das Ziel für Audit-Informationen aus:

Option	Beschreibung
Standard (Admin-Nodes/lokale Nodes)	Audit-Meldungen werden an das Audit-Protokoll gesendet (`audit.log`) Auf dem Admin-Knoten werden Sicherheitsereignisprotokolle und Anwendungsprotokolle auf den Knoten gespeichert, in denen sie erzeugt wurden (auch als "der lokale Knoten" bezeichnet).
Externer Syslog-Server	Audit-Informationen werden an einen externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Admin-Node und externer Syslog-Server	Audit-Meldungen werden an das Audit-Protokoll gesendet (`audit.log`) Auf dem Admin-Knoten und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert. Die Art der gesendeten Informationen hängt davon ab, wie Sie den externen Syslog-Server konfiguriert haben. Diese Option ist erst aktiviert, nachdem Sie einen externen Syslog-Server konfiguriert haben.
Nur lokale Nodes	Es werden keine Audit-Informationen an einen Admin-Node oder Remote-Syslog-Server gesendet. Audit-Informationen werden nur auf den generierten Nodes gespeichert. **Hinweis**: StorageGRID entfernt regelmäßig diese lokalen Protokolle in einer Drehung, um Speicherplatz freizugeben. Wenn die Protokolldatei für einen Knoten 1 GB erreicht, wird die vorhandene Datei gespeichert und eine neue Protokolldatei gestartet. Die Rotationsgrenze für das Protokoll beträgt 21 Dateien. Wenn die 22. Version der Protokolldatei erstellt wird, wird die älteste Protokolldatei gelöscht. Auf jedem Node werden durchschnittlich etwa 20 GB an Protokolldaten gespeichert.

In werden Audit-Informationen, die für jeden lokalen Node generiert werden, gespeichert `/var/local/log/localaudit.log`

2. Wählen Sie **Speichern**. Wählen Sie dann **OK**, um die Änderung am Protokollziel zu akzeptieren.
3. Wenn Sie entweder **Externer Syslog-Server** oder **Admin-Knoten und externer Syslog-Server** als Ziel für Audit-Informationen ausgewählt haben, wird eine zusätzliche Warnung angezeigt. Überprüfen Sie den Warntext.

Sie müssen bestätigen, dass der externe Syslog-Server Test-StorageGRID-Meldungen empfangen kann.

4. Wählen Sie **OK**, um zu bestätigen, dass Sie das Ziel für die Audit-Informationen ändern möchten.

   Ein grünes Banner zeigt an, dass Ihre Audit-Konfiguration erfolgreich gespeichert wurde.

   Neue Protokolle werden an die ausgewählten Ziele gesendet. Vorhandene Protokolle verbleiben an ihrem aktuellen Speicherort.

Verwandte Informationen

"Übersicht über Überwachungsnachrichten"

"Konfigurieren von Überwachungsmeldungen und Protokollzielen"

"Systemaudits Meldungen"

"Audit-Meldungen zu Objekt-Storage"

"Management-Audit-Nachricht"

"Client liest Audit-Meldungen"

"StorageGRID verwalten"