



Konfigurieren Sie Überwachungsmeldungen und Protokollziele

StorageGRID

NetApp
March 12, 2025

Inhalt

Konfigurieren Sie Überwachungsmeldungen und Protokollziele	1
Überlegungen zur Verwendung eines externen Syslog-Servers	1
Wann sollte ein externer Syslog-Server verwendet werden	1
So konfigurieren Sie einen externen Syslog-Server	1
Wie schätzen Sie die Größe des externen Syslog-Servers ein	2
Beispiel für eine Einschätzung der Dimensionierung	5
Konfigurieren von Audit-Meldungen und externem Syslog-Server	6
Meldungsebenen ändern	7
Definieren Sie HTTP-Anforderungsheader	8
Verwenden Sie einen externen syslog-Server	8
Wählen Sie Ziele für Audit-Informationen aus	14

Konfigurieren Sie Überwachungsmeldungen und Protokollziele

Überlegungen zur Verwendung eines externen Syslog-Servers

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 den Netzwerkverkehr auf Ihren Admin-Knoten reduzieren und die Informationen effizienter verwalten. Für StorageGRID ist das Format des ausgehenden Syslog-Nachrichtenpakets mit RFC 3164 kompatibel.

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

Wann sollte ein externer Syslog-Server verwendet werden

Ein externer Syslog-Server ist besonders nützlich, wenn Sie ein großes Grid haben, mehrere Arten von S3 Applikationen verwenden oder alle Audit-Daten aufbewahren möchten. Durch das Senden von Audit-Informationen an einen externen Syslog-Server können Sie:

- Erfassen und managen Sie Audit-Informationen wie Audit-Nachrichten, Anwendungsprotokolle und Sicherheitsereignisse effizienter.
- Reduzieren Sie den Netzwerkverkehr auf Ihren Admin-Knoten, da die Audit-Informationen direkt von den verschiedenen Storage-Knoten auf den externen Syslog-Server übertragen werden, ohne einen Admin-Knoten durchlaufen zu müssen.



Wenn Protokolle an einen externen Syslog-Server gesendet werden, werden einzelne Protokolle mit mehr als 8,192 Byte am Ende der Nachricht abgeschnitten, um den üblichen Einschränkungen in externen Syslog-Server-Implementierungen zu entsprechen.



Um die Optionen für die vollständige Datenwiederherstellung im Falle eines Ausfalls des externen Syslog-Servers (`localaudit.log`) zu maximieren, werden auf jedem Knoten bis zu 20 GB lokale Protokolle von Audit-Datensätzen gepflegt.

So konfigurieren Sie einen externen Syslog-Server

Informationen zum Konfigurieren eines externen Syslog-Servers finden Sie unter "[Konfigurieren von Audit-Meldungen und externem Syslog-Server](#)".

Wenn Sie das TLS- oder RELP/TLS-Protokoll konfigurieren möchten, müssen Sie über die folgenden Zertifikate verfügen:

- **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.
- **Client-Zertifikat:** Das Client-Zertifikat zur Authentifizierung am externen Syslog-Server in PEM-Codierung.
- **Privater Client-Schlüssel:** Privater Schlüssel für das Client-Zertifikat in PEM-Codierung.



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.

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-Protokoll Daten von 1.6 MB pro Sekunde empfangen (und in der Regel speichern) können.

Wenn Sie mehr über Ihre Arbeitslast wissen, sind genauere Schätzungen möglich. Für Prüfprotokolle sind die wichtigsten zusätzlichen Variablen der Prozentsatz der S3-Operationen, die Puts (vs. GETS) sind, und die durchschnittliche Größe der folgenden S3-Felder in Byte (4-stellige Abkürzungen in der Tabelle sind Namen von Audit-Protokollfeldern):

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 $0 \leq P \leq 1$ (für einen 100 % PUT-Workload, $P = 1$ und für einen 100 % GET-Workload, $P = 0$).

Verwenden wir K, um die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Bucket und S3-Schlüssel darzustellen. 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	Auditprotokollrate = 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. Für Anwendungsprotokolle sind die wichtigsten zusätzlichen Variablen die Datenschutzstrategie (Replikation vs. Erasure Coding), der Prozentsatz der S3-Operationen, die Put (vs. Gets/other) sind, und die durchschnittliche Größe der folgenden S3-Felder in Byte (4-stellige Abkürzungen, die in der Tabelle verwendet werden, sind Audit-Log-Feldnamen):

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
- Erasure Coding

Wenn Sie Replizierung für die Datensicherung verwenden

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

K darf die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Buckets und S3-Schlüssel repräsentieren. 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 $0 \leq P \leq 1$ (für einen 100 % PUT-Workload, $P = 1$ und für einen 100 % GET-Workload, $P = 0$).

K darf die durchschnittliche Größe der Summe der S3-Kontonamen, S3-Buckets und S3-Schlüssel repräsentieren. 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 für 1,000 S3-Vorgänge pro Sekunde dimensioniert ist, beträgt der Workload 50 % Put, Ihre S3-Kontonamen, Bucket-Namen und Objektnamen sind durchschnittlich 90 Byte lang. Ihr externer Syslog-Server sollte so dimensioniert sein, dass er 2,250 Anwendungsprotokolle pro Sekunde unterstützt und Anwendungsdaten mit einer Rate von 0.6 MB pro Sekunde empfangen (und normalerweise speichern) kann.

Konfigurieren von Audit-Meldungen und externem Syslog-Server

Sie können eine Reihe von Einstellungen für Überwachungsmeldungen konfigurieren. Sie können die Anzahl der aufgezeichneten Überwachungsmeldungen anpassen, HTTP-Anforderungsheader definieren, die Sie in die Audit-Nachrichten des Clients einbeziehen möchten, einen externen Syslog-Server konfigurieren und angeben, wo Überwachungsprotokolle, Sicherheitsereignisprotokolle und StorageGRID-Softwareprotokolle gesendet werden.

Audit-Meldungen und -Protokolle zeichnen Systemaktivitäten und Sicherheitsereignisse auf und sind wichtige Tools für das Monitoring und die Fehlerbehebung. Alle StorageGRID Nodes generieren Audit-Meldungen und -Protokolle, um die Systemaktivität und -Ereignisse nachzuverfolgen.

Optional können Sie einen externen Syslog-Server konfigurieren, um Audit-Informationen Remote zu speichern. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Audit-Nachrichten auf die Performance minimiert, ohne dass die Vollständigkeit der Audit-Daten reduziert wird. Ein externer Syslog-Server ist besonders nützlich, wenn Sie ein großes Grid haben, mehrere Arten von S3 Applikationen verwenden oder alle Audit-Daten aufbewahren möchten. Weitere Informationen finden Sie unter ["Konfigurieren von Audit-Meldungen und externem Syslog-Server"](#) .

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Berechtigung für Wartung oder Root-Zugriff"](#).
- Wenn Sie planen, einen externen Syslog-Server zu konfigurieren, haben Sie das überprüft ["Überlegungen zur Verwendung eines externen Syslog-Servers"](#) und sichergestellt, dass der Server über genügend Kapazität verfügt, um die Protokolldateien zu empfangen und zu speichern.

- Wenn Sie einen externen Syslog-Server mit TLS- oder RELP/TLS-Protokoll konfigurieren möchten, verfügen Sie über die erforderlichen Server-CA- und Client-Zertifikate und den privaten Client-Schlüssel.

Meldungsebenen ändern

Sie können für jede der folgenden Meldungskategorien im Prüfprotokoll eine andere Überwachungsstufe festlegen:

Audit-Kategorie	Standardeinstellung	Weitere Informationen
System	Normal	"Systemaudits Meldungen"
Storage	Fehler	"Audit-Meldungen zu Objekt-Storage"
Vereinfachtes	Normal	"Management-Audit-Nachricht"
Client-Lesevorgänge	Normal	"Client liest Audit-Meldungen"
Client-Schreibvorgänge	Normal	"Audit-Meldungen des Clients schreiben"
ILM	Normal	"ILM-Prüfmeldungen"
Grid-übergreifende Replizierung	Fehler	"CGRR: Grid-übergreifende Replikationsanforderung"



Diese Standardeinstellungen gelten, wenn Sie StorageGRID ursprünglich mit Version 10.3 oder höher installiert haben. Wenn Sie zunächst eine frühere Version von StorageGRID verwendet haben, wird der Standardwert für alle Kategorien auf Normal gesetzt.



Bei Upgrades sind Audit-Level-Konfigurationen nicht sofort wirksam.

Schritte

1. Wählen Sie **CONFIGURATION > Monitoring > Audit und Syslog-Server**.
2. Wählen Sie für jede Kategorie der Überwachungsmeldung eine Überwachungsstufe aus der Dropdown-Liste aus:

Audit-Level	Beschreibung
Aus	Es werden keine Überwachungsmeldungen aus der Kategorie protokolliert.
Fehler	Nur Fehlermeldungen sind protokollierte - Audit-Meldungen, für die der Ergebniscode nicht „erfolgreich“ (SUCCS) war.
Normal	Standardtransaktionsmeldungen werden protokolliert – die in diesen Anweisungen für die Kategorie aufgeführten Nachrichten.

Audit-Level	Beschreibung
Debuggen	Veraltet. Dieser Level verhält sich mit dem normalen Prüfstand.

Die Meldungen, die für eine bestimmte Ebene enthalten sind, enthalten diejenigen, die auf den höheren Ebenen protokolliert werden würden. Die normale Ebene umfasst beispielsweise alle Fehlermeldungen.



Wenn Sie für Ihre S3-Anwendungen keine detaillierte Aufzeichnung der Client-Leseoperationen benötigen, ändern Sie optional die Einstellung **Client-Lesevorgänge** auf **Fehler**, um die Anzahl der im Audit-Protokoll aufgezeichneten Audit-Meldungen zu verringern.

3. Wählen Sie **Speichern**.

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

Definieren Sie HTTP-Anforderungsheader

Sie können optional alle HTTP-Anforderungsheader definieren, die Sie in die Audit-Nachrichten des Clients aufnehmen möchten. Diese Protokoll-Header gelten nur für S3-Anforderungen.

Schritte

1. Definieren Sie im Abschnitt **Audit Protocol headers** die HTTP-Anforderungsheader, die Sie in die Audit-Nachrichten des Clients aufnehmen möchten.

Verwenden Sie ein Sternchen (*) als Platzhalter, um Null oder mehr Zeichen zu entsprechen. Verwenden Sie die Escape-Sequenz (*), um mit einem wortwörtliche Sternchen überein.

2. Wählen Sie **Einen anderen Header hinzufügen** aus, um ggf. zusätzliche Header zu erstellen.

Wenn HTTP-Header in einer Anfrage gefunden werden, sind sie in der Überwachungsmeldung unter dem Feld HTRH enthalten.



Header für Auditprotokoll-Anfragen werden nur protokolliert, wenn die Audit-Ebene für **Client** oder **Client-Schreibvorgänge** nicht **aus** ist.

3. Wählen Sie **Speichern**

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

Verwenden Sie einen externen syslog-Server

Optional können Sie einen externen Syslog-Server konfigurieren, um Audit-Protokolle, Anwendungsprotokolle und Sicherheitsereignisprotokolle an einem Ort außerhalb des Grids zu speichern.



Wenn Sie keinen externen Syslog-Server verwenden möchten, überspringen Sie diesen Schritt und gehen Sie zu [Wählen Sie Ziele für Audit-Informationen aus](#).



Wenn die in diesem Verfahren verfügbaren Konfigurationsoptionen nicht flexibel genug sind, um Ihre Anforderungen zu erfüllen, können zusätzliche Konfigurationsoptionen über die Endpunkte angewendet werden `audit-destinations`, die sich im Abschnitt [Private API](#) des befinden "[Grid Management API](#)". Sie können beispielsweise die API verwenden, wenn Sie unterschiedliche Syslog-Server für verschiedene Knotengruppen verwenden möchten.

Geben Sie Syslog-Informationen ein

Greifen Sie auf den Assistenten zum Konfigurieren des externen Syslog-Servers zu und geben Sie die Informationen an, die StorageGRID für den Zugriff auf den externen Syslog-Server benötigt.

Schritte

1. 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 **externen Syslog-Server bearbeiten** aus.

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

2. Geben Sie für den Schritt **Enter syslog info** des Assistenten einen gültigen vollständig qualifizierten Domännennamen oder eine IPv4- oder IPv6-Adresse für den externen Syslog-Server in das Feld **Host** ein.
3. Geben Sie den Zielport auf dem externen Syslog-Server ein (muss eine Ganzzahl zwischen 1 und 65535 sein). Der Standardport ist 514.
4. 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.

5. Wählen Sie **Weiter**.
6. Wenn Sie **TLS** oder **RELP/TLS** ausgewählt haben, laden Sie die Server-CA-Zertifikate, das Client-Zertifikat und den privaten Client-Schlüssel hoch.
 - a. Wählen Sie **Durchsuchen** für das Zertifikat oder den Schlüssel, das Sie verwenden möchten.
 - b. Wählen Sie das Zertifikat oder die Schlüsseldatei aus.
 - c. 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.

7. 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
 - **Senden von Anwendungsprotokollen:** Sendet "[Protokolldateien der StorageGRID Software](#)" nützliche Informationen für die Fehlersuche, einschließlich:
 - `bycast-err.log`
 - `bycast.log`
 - `jaeger.log`
 - `nms.log` (Nur Admin-Nodes)
 - `prometheus.log`
 - `raft.log`
 - `hagroups.log`
 - **Zugriffsprotokolle senden:** Sendet HTTP-Zugriffsprotokolle für externe Anfragen an Grid Manager, Tenant Manager, konfigurierte Load Balancer-Endpunkte und Grid Federation-Anfragen von Remote-Systemen.
2. Verwenden Sie die Dropdown-Menüs, um den Schweregrad und die Einrichtung (Meldungstyp) für jede zu sendende Kategorie von Audit-Informationen auszuwählen.

Durch das Festlegen von Schweregraden und Einrichtungswerten können Sie die Protokolle auf anpassbare Weise für eine einfachere Analyse zusammenfassen.

- a. Wählen Sie für **Severity Passthrough** aus, oder wählen Sie einen Schweregrad zwischen 0 und 7 aus.

Wenn Sie einen Wert auswählen, wird der ausgewählte Wert auf alle Nachrichten dieses Typs angewendet. Informationen über verschiedene Schweregrade gehen verloren, wenn Sie den Schweregrad mit einem festen Wert überschreiben.

Schweregrad	Beschreibung
Passthrough	<p>Jede an das externe Syslog gesendete Nachricht hat denselben Schweregrad wie bei der lokalen Anmeldung am Knoten:</p> <ul style="list-style-type: none"> • Für Prüfprotokolle lautet der Schweregrad „Info“. • Bei Sicherheitsereignissen werden die Schweregrade von der Linux-Distribution auf den Knoten generiert. • Bei Anwendungsprotokollen variieren die Schweregrade zwischen „Info“ und „Hinweis“, je nachdem, was das Problem ist. Wenn beispielsweise ein NTP-Server hinzugefügt und eine HA-Gruppe konfiguriert wird, wird der Wert „Info“ angezeigt, während der SSM- oder RSM-Service absichtlich angehalten wird, wird der Wert „Hinweis“ angezeigt. • Für Zugriffsprotokolle lautet der Schweregrad „Info“.
0	Notfall: System ist unbrauchbar
1	Warnung: Maßnahmen müssen sofort ergriffen werden
2	Kritisch: Kritische Bedingungen
3	Fehler: Fehlerbedingungen
4	Warnung: Warnbedingungen
5	Hinweis: Normaler, aber bedeutender Zustand
6	Information: Informationsmeldungen
7	Debug: Debug-Level-Meldungen

b. Wählen Sie für **Facilty Passthrough** aus, oder wählen Sie einen Wert zwischen 0 und 23 aus.

Wenn Sie einen Wert auswählen, wird dieser auf alle Nachrichten dieses Typs angewendet. Informationen zu verschiedenen Einrichtungen gehen verloren, wenn Sie die Einrichtung mit einem festen Wert überschreiben.

Anlage	Beschreibung
Passthrough	<p>Jede Nachricht, die an das externe Syslog gesendet wird, hat denselben Einrichtungswert wie bei der lokalen Anmeldung am Knoten:</p> <ul style="list-style-type: none"> • Für Audit-Protokolle lautet die an den externen Syslog-Server gesendete Einrichtung „local7“. • Bei Sicherheitsereignissen werden die Einrichtungswerte von der linux-Distribution auf den Knoten generiert. • Für Anwendungsprotokolle weisen die an den externen Syslog-Server gesendeten Anwendungsprotokolle die folgenden Einrichtungswerte auf: <ul style="list-style-type: none"> ◦ <code>bypass.log</code>: Benutzer oder Daemon ◦ <code>bypass-err.log</code>: Benutzer, Daemon, local3 oder local4 ◦ <code>jaeger.log</code>: Local2 ◦ <code>nms.log</code>: Local3 ◦ <code>prometheus.log</code>: Local4 ◦ <code>raft.log</code>: Local5 ◦ <code>hagroups.log</code>: Local6 • Für Zugriffsprotokolle lautet die an den externen Syslog-Server gesendete Einrichtung „local0“.
0	kern (Kernelmeldungen)
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)

Anlage	Beschreibung
11	FTP
12	NTP
13	Logaudit (Protokollaudit)
14	Logalert (Protokollwarnung)
15	Uhr (Uhrzeitdaemon)
16	Local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
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 die Konfiguration 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.

Weitere Informationen finden Sie unter, "[Fehlerbehebung für einen externen Syslog-Server](#)" um Sie bei der Behebung von Fehlern zu unterstützen.

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 die Syslog-Server-Konfiguration gespeichert wurde.



StorageGRID-Audit-Informationen werden erst dann 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 Überwachungsprotokolle, Sicherheitsereignisprotokolle und "[StorageGRID-Softwareprotokolle](#)" gesendet werden sollen.

StorageGRID verwendet standardmäßig lokale Überwachungsziele für Knoten und speichert die Audit-Informationen in `/var/local/log/localaudit.log`.



Bei Verwendung von `/var/local/log/localaudit.log` werden die Audit-Protokolleinträge für Grid Manager und Tenant Manager möglicherweise an einen Storage Node gesendet. Mit dem Befehl finden Sie den Node mit den neuesten Einträgen `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`.

Einige Ziele sind nur verfügbar, wenn Sie einen externen Syslog-Server konfiguriert haben.

Schritte

1. Wählen Sie auf der Seite Audit and syslog Server das Ziel für Audit-Informationen aus.



Nur lokale Knoten und **externer Syslog-Server** bieten normalerweise eine bessere Leistung.

Option	Beschreibung
Nur lokale Knoten (Standard)	<p>Überwachungsmeldungen, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden nicht an Admin-Nodes gesendet. Stattdessen werden sie nur auf den Knoten gespeichert, die sie generiert haben („der lokale Knoten“). Die auf jedem lokalen Knoten generierten Audit-Informationen werden in gespeichert <code>/var/local/log/localaudit.log</code>.</p> <p>Hinweis: StorageGRID entfernt periodisch lokale Protokolle in einer Rotation, 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 Protokoll Daten gespeichert.</p>
Admin-Nodes/lokale Nodes	<p>Audit-Meldungen werden an das Überwachungsprotokoll auf Admin-Nodes gesendet, Sicherheitsereignisprotokolle und Anwendungsprotokolle werden auf den Knoten gespeichert, die sie generiert haben. Die Audit-Informationen werden in folgenden Dateien gespeichert:</p> <ul style="list-style-type: none"> • Admin-Nodes (primär und nicht primär): <code>/var/local/audit/export/audit.log</code> • Alle Knoten: Die <code>/var/local/log/localaudit.log</code> Datei ist normalerweise leer oder fehlt. Sie kann sekundäre Informationen enthalten, z. B. eine zusätzliche Kopie einiger Nachrichten.
Externer Syslog-Server	<p>Audit-Informationen werden an einen externen Syslog-Server gesendet und auf den lokalen Knoten gespeichert (<code>/var/local/log/localaudit.log</code>). 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.</p>
Admin-Node und externer Syslog-Server	<p>Audit-Meldungen werden an das Audit-Protokoll gesendet (<code>/var/local/audit/export/audit.log</code>) auf Admin-Knoten, und Audit-Informationen werden an den externen Syslog-Server gesendet und auf dem lokalen Knoten gespeichert (<code>/var/local/log/localaudit.log</code>). 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.</p>

2. Wählen Sie **Speichern**.

Es wird eine Warnmeldung angezeigt.

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

Ein grünes Banner zeigt an, dass die Überwachungskonfiguration gespeichert wurde.

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

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.