外部 **syslog** サーバを使用します

StorageGRID

NetApp
November 04, 2025

目次

外部 **syslog** サーバを使用します

外部 **syslog** サーバに関する考慮事項

必要な外部 syslog サーバのサイズを見積もるには、次のガイドラインに従います。

外部 **syslog** サーバとは何ですか？

外部 syslog サーバは、 StorageGRID の外部にあるサーバであり、 1 箇所でシステム監査情報を収集できます。外部 syslog サーバを使用すると、監査情報のデスティネーションを設定して、管理ノードのネットワークトラフィックを減らしたり、情報をより効率的に管理したりすることができます。外部 syslog サーバに送信できる監査情報のタイプは次のとおりです。

- 通常のシステム運用中に生成された監査メッセージを含む監査ログ
- ログインやルートへのエスカレーションなど、セキュリティ関連のイベント
- アプリケーションログ：発生した問題 のトラブルシューティングのためにサポートケースをオープンする必要がある場合に要求されることがあります

外部 **syslog** サーバのサイズを見積もる方法

通常、グリッドは、 1 秒あたりの S3 処理数または 1 秒あたりのバイト数で定義される、必要なスループットを達成するようにサイジングされます。たとえば、 1 秒あたりの S3 処理数が 1 、 000 件、つまり 1 秒あたり 2 、 000 MB のオブジェクトの取り込みと読み出しをグリッドで処理する必要があるとします。外部 syslog サーバのサイズは、グリッドのデータ要件に応じて決定する必要があります。

このセクションでは、外部 syslog サーバが処理可能である必要があるさまざまなタイプのログメッセージのレートと平均サイズを、グリッドの既知または望ましいパフォーマンス特性（ 1 秒あたりの S3 処理数）で見積もるためのヒューリスティック計算式をいくつか示します。

1 秒あたりの **S3** 処理数を推定式で使用します

グリッドをスループット用に 1 秒あたりのバイト数で表した場合、試算式を使用するには、このサイジングを 1 秒あたりの S3 処理に変換する必要があります。グリッドのスループットを変換するには、最初に平均オブジェクトサイズを確認する必要があります。これには、既存の監査ログと指標の情報を使用するか（存在する場合）、 StorageGRID を使用するアプリケーションに関する知識が必要です。たとえば、グリッドのサイズが 2 、 000 MB/ 秒で、平均オブジェクトサイズが 2MB の場合、 1 秒あたり 1 、 000 S3 処理可能なサイズ（ 2 、 000 MB/ 秒）になるようにグリッドをサイジングしました。

> 以降のセクションで説明する外部 syslog サーバのサイジングの計算式は、一般的な推定値（ワーストケースの見積もり値ではありません）を示しています。設定やワークロードによっては、 syslog メッセージや syslog データの量が、式で予測される値よりも増減することがあります。式はガイドラインとしてのみ使用することを意図しています。

監査ログの推定式

グリッドでサポートされる 1 秒あたりの S3 処理数以外の S3 ワークロードに関する情報がない場合は、次の式を使用して、外部 syslog サーバで処理する必要がある監査ログのボリュームを推定できます。 監査レベルをデフォルト値のままにしておくという前提では、次のようになります（ [エラー] に設定されている [ストレージ] を除くすべてのカテゴリは [通常] に設定されています）。

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

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、 1 秒あたり 2 、 000 件の syslog メッセージをサポートするように外部 syslog サーバをサイジングし、 1 秒あたり 1.6 MB の割合で監査ログデータを受信（通常は格納）できるようにする必要があります。

ワークロードの詳細がわかっている場合は、より正確な概算が可能です。監査ログの場合、最も重要な追加変数は、 PUT される S3 処理の割合（とが表示されます。次の S3 フィールドの平均サイズ（バイト）（このテーブルで使用される 4 文字の省略形は監査ログのフィールド名）も表示されます。

コード	フィールド	説明
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

P を使用して、 PUT の S3 処理の割合を表します。ここでは、 0 ≤ P ≤ 1 である（ 100% PUT ワークロードの場合は P = 1 、 100% GET ワークロードの場合は P = 0 ）。

次に、 K を使用して S3 アカウント名、 S3 バケット、 S3 キーの合計の平均サイズを表します。S3 アカウント名が常に my-s3 アカウント（ 13 バイト）、バケット名が /my-application/bucket-12345 （ 28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c （ 36 バイト）のような固定長のキーを持つとします。K の値は 90 （ 13+13+28+36 ）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理する必要がある監査ログのボリュームを見積もることができます。これは、監査レベルをデフォルト（ Storage を除くすべてのカテゴリは Normal に設定されたまま）にしておくことを前提としています。 エラーに設定されているもの）：

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

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、ワークロードの配置は 50% で、 S3 アカウント名やバケット名は オブジェクト名の平均値は 90 バイトで、 1 秒あたり 1 、 500 の syslog メッセージをサポートするように外部 syslog サーバをサイジングし、 1 秒あたり約 1MB の割合で監査ログデータを受信（通常は格納）できるようにする必要があります。

デフォルト以外の監査レベルの推定式

監査ログ用に提供される式では、デフォルトの監査レベル設定（「 Error 」に設定されているストレージを除く、すべてのカテゴリが「 Normal 」に設定されている）を使用するものとします。デフォルト以外の監査レベル設定に対する監査メッセージの割合と平均サイズを見積もるための詳細な式は使用できません。ただし、次の表を使用して料金を大まかに見積もることができます。 監査ログに提供されている平均サイズの式を使用することもできますが、「余分な」監査メッセージの平均サイズはデフォルトの監査メッセージよりも小さくなるため、見積もりが過剰になる可能性があることに注意してください。

条件	計算式
レプリケーション：すべての監査レベルをデバッグまたは通常に設定します	監査ログの速度 = 8 x S3 処理の速度
イレイジャーコーディング：すべての監査レベルをデバッグまたは正常に設定	デフォルト設定と同じ式を使用します

セキュリティイベントの推定式

セキュリティイベントはS3処理とは関係なく、一般に生成されるログやデータの量はごくわずかです。そのため、計算式は提供されません。

アプリケーションログの推定式

グリッドでサポートされる 1 秒あたりの S3 処理数以外の情報が S3 ワークロードにない場合は、次の式を使用して、外部 syslog サーバで処理する必要があるアプリケーションログのボリュームを推定できます。

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

たとえば、グリッドの 1 秒あたりの S3 処理数が 1 、 000 の場合、 1 秒あたりのアプリケーションログ数が 3 、 300 になるように外部 syslog サーバをサイジングし、 1 秒あたり約 1.2 MB の割合でアプリケーションログデータを受信（格納）できるようにする必要があります。

ワークロードの詳細がわかっている場合は、より正確な概算が可能です。アプリケーションログの場合、最も重要な追加変数はデータ保護戦略（レプリケーションとイレイジャーコーディング）。 PUT の S3 処理の割合（対GET / OTHER ）と、次の S3 フィールドの平均サイズ（バイト）（テーブルで使用される 4 文字の略語は監査ログのフィールド名）です。

コード	フィールド	説明
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	説明
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

サイジング試算の例

このセクションでは、次のデータ保護方法でグリッドの推定式を使用する方法の例を説明します。

- レプリケーション
- イレイジャーコーディング

レプリケーションをデータ保護に使用する場合

P は、 PUT の S3 処理の割合を表します。ここでは、 0 ≤ P ≤ 1 である（ 100% PUT ワークロードの場合は P = 1 、 100% GET ワークロードの場合は P = 0 ）。

S3 アカウント名、 S3 バケット、 S3 キーの合計の平均サイズを K で表します。S3 アカウント名が常に my-s3 アカウント（ 13 バイト）、バケット名が /my-application/bucket-12345 （ 28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c （ 36 バイト）のような固定長のキーを持つとします。K の値は 90 （ 13+13+28+36 ）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理可能なアプリケーションログのボリュームを推定できます。

```
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
```

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、ワークロードの配置が 50% で、 S3 アカウント名、バケット名、オブジェクト名の平均値が 90 バイトの場合、 1 秒あたりのアプリケーションログ数が 1800 になるように外部 syslog サーバをサイジングする必要があります。 そして、アプリケーションデータを 0.5 MB/ 秒のレートで受信（通常は保存）します。

イレイジャーコーディングをデータ保護に使用する場合

P は、 PUT の S3 処理の割合を表します。ここでは、 0 ≤ P ≤ 1 である（ 100% PUT ワークロードの場合は P = 1 、 100% GET ワークロードの場合は P = 0 ）。

S3 アカウント名、 S3 バケット、 S3 キーの合計の平均サイズを K で表します。S3 アカウント名が常に my-s3 アカウント（ 13 バイト）、バケット名が /my-application/bucket-12345 （ 28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c （ 36 バイト）のような固定長のキーを持つとします。K の値は 90 （ 13+13+28+36 ）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理可能なアプリケーションログのボリュームを推定できます。

```
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
```

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、ワークロードの配置は 50% で、 S3 アカウント名やバケット名は オブジェクト名の平均値は 90 バイトです。外部 syslog サーバは、 1 秒あたり 2 、 250 のアプリケーションログをサポートするようにサイズを設定する必要があります。これにより、 1 秒あたり 0.6 MB のレートでアプリケーションデータを受信（通常は格納）できるようになります。

監査メッセージレベルと外部syslogサーバの設定の詳細については、次を参照してください。

- "外部 syslog サーバを設定します"
- "監査メッセージとログの送信先を設定します"

外部 syslog サーバを設定します

監査ログ、アプリケーションログ、およびセキュリティイベントログをグリッド以外の場所に保存する場合は、この手順 を使用して外部 syslog サーバを設定します。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Maintenance または Root アクセス権限が必要です。
- ログファイルを受信して保存する容量を持つ syslog サーバを用意しておきます。詳細については、を参照してください "外部 syslog サーバに関する考慮事項"。
- TLS または RELP/TLS を使用する場合は、適切なサーバおよびクライアントの認定資格を取得している必要があります。

このタスクについて

外部の syslog サーバに監査情報を送信する場合は、先に外部サーバを設定する必要があります。

外部 syslog サーバに監査情報を送信すると、次のことが可能になります。

- 監査メッセージ、アプリケーションログ、セキュリティイベントなどの監査情報をより効率的に収集および管理できます
- 管理ノードを経由することなくさまざまなストレージノードから外部 syslog サーバに監査情報が直接転送されるため、管理ノードのネットワークトラフィックが軽減されます

外部 syslog サーバにログを送信する場合、外部 syslog サーバの実装で共通の制限に準拠するために、メッセージの末尾に 8192 バイトを超える単一のログが切り捨てられます。

外部 syslog サーバに障害が発生した場合にデータを完全にリカバリできるようにするために、各ノードに最大 20GB の監査レコード（ localaudit.log ）が保持されます。

この手順 で使用可能な構成オプションが要件を満たすほど柔軟性がない場合は、プライベートAPIを使用して追加の構成オプションを適用できます `audit-destinations` エンドポイント：たとえば、ノードのグループごとに異なる syslog サーバを使用できます。

外部サーバを設定します

ウィザードにアクセスします

起動するには、Configure external syslog serverウィザードにアクセスします。

手順

1. * configuration * > * Monitoring * > * Audit and syslog server * を選択します。
2. 監査および syslog サーバページで、 * 外部 syslog サーバの設定 * を選択します。以前に外部 syslog サーバを設定している場合は、 * 外部 syslog サーバの編集 * を選択します。

   Configure external syslog serverウィザードが表示されます。

syslog 情報を入力します

外部syslogサーバにアクセスするためにStorageGRID が必要とする情報を指定する必要があります。

手順

1. ウィザードの* syslog情報の入力*ステップで、* Host *フィールドに外部syslogサーバの有効な完全修飾ドメイン名またはIPv4またはIPv6アドレスを入力します。
2. 外部 syslog サーバのデスティネーションポートを入力します（ 1~65535 の整数で指定する必要があります）。デフォルトポートは 514 です。
3. 外部 syslog サーバへの監査情報の送信に使用するプロトコルを選択します。

   TLS または RELP/TLS *を使用することを推奨します。これらのいずれかのオプションを使用するには、サーバ証明書をアップロードする必要があります。証明書を使用して、グリッドと外部 syslog サーバの間の接続を保護できます。詳細については、を参照してください "セキュリティ証明書を管理する"。

   すべてのプロトコルオプションで、外部 syslog サーバによるサポートおよび設定が必要です。外部 syslog サーバと互換性のあるオプションを選択する必要があります。

   Reliable Event Logging Protocol (RELP) は、 syslog プロトコルの機能を拡張し、信頼性の高いイベントメッセージ配信を実現します。RELP を使用すると、外部 syslog サーバを再起動する必要がある場合に監査情報が失われないようにすることができます。

4. 「 * Continue * 」を選択します。
5. [[attach-certificate]]TLS * または * RELP/TLS * を選択した場合は、次の証明書をアップロードします。
   - * Server CA certificates* ：外部 syslog サーバを検証するための信頼された CA 証明書（ PEM エンコーディング）。省略すると、デフォルトの Grid CA 証明書が使用されます。ここでアップロードするファイルは CA バンドルである可能性があります。
   - * クライアント証明書 * ：外部 syslog サーバへの認証用のクライアント証明書（ PEM エンコード）。

◦ * クライアント秘密鍵 * ：クライアント証明書の秘密鍵（ PEM エンコーディング）。

> クライアント証明書を使用する場合は、クライアント秘密鍵も使用する必要があります。暗号化された秘密鍵を指定する場合は、パスフレーズも指定する必要があります。暗号化された秘密鍵を使用した場合、セキュリティ上の大きなメリットはありません。これは、鍵とパスフレーズを格納する必要があるためです。暗号化されていない秘密鍵を使用することを推奨します（使用可能な場合）。

i. 使用する証明書またはキーの [* 参照] を選択します。

ii. 証明書ファイルまたはキーファイルを選択します。

iii. ファイルをアップロードするには、 * 開く * を選択します。

証明書またはキーファイル名の横に緑のチェックマークが表示され、正常にアップロードされたことを通知します。

6. 「 * Continue * 」を選択します。

syslog の内容を管理します

外部syslogサーバに送信する情報を選択できます。

手順

1. ウィザードの* syslogコンテンツの管理*ステップで、外部syslogサーバに送信する監査情報の種類をそれぞれ選択します。
   - 監査ログの送信：StorageGRID イベントとシステムアクティビティを送信します
   - セキュリティイベントの送信:許可されていないユーザーがサインインしようとしたときや、ユーザーがrootとしてサインインしようとしたときなど、セキュリティイベントを送信します
   - アプリケーションログを送信：次のようなトラブルシューティングに役立つログファイルを送信します。
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` （管理ノードのみ）
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
2. ドロップダウンメニューを使用して、送信する監査情報のカテゴリの重大度とファシリティ（メッセージのタイプ）を選択します。

   重大度とファシリティに *Passthrough * を選択すると、リモート syslog サーバに送信される情報の重大度とファシリティは、ノードにローカルにログインしたときと同じになります。ファシリティと重大度を設定すると、カスタマイズ可能な方法でログを集約し、分析を容易にすることができます。

StorageGRID ソフトウェアログの詳細については、を参照してください "StorageGRID ソフトウェアのログ"。

a. 各メッセージを外部 syslog に送信する際に、ローカル syslog の場合と同じ重大度値を使用する場合は、 [**Severity]** に **[*Passthrough**] を選択します。

   監査ログの場合、*[Passthrough]*を選択すると、重大度は「info」です。

   セキュリティイベントの場合、* Passthrough *を選択すると、重大度の値はノード上のLinuxディストリビューションによって生成されます。

   アプリケーション・ログの場合、 *Passthrough * を選択すると、問題 の内容によって、重大度は「 info 」と「 notice 」の間で異なります。たとえば、NTPサーバを追加してHAグループを設定すると値は「info」になり、SSMサービスまたはRSMサービスを意図的に停止すると値は「notice」になります。

b. パススルー値を使用しない場合は、重大度値を0～7の範囲で選択します。

   選択した値は、このタイプのすべてのメッセージに適用されます。重大度を固定の値で上書きすることを選択すると、それぞれの情報が失われます。

重大度	説明
0	EMERGENCY ：システムが使用できない
1.	ALERT ：早急に対処が必要です
2.	Critical ：クリティカルな状態です
3.	Error ：エラー状態
4.	Warning ：警告状態です
5.	通知：通常の状態だが重要な状態
6.	INFORMATIONAL ：情報メッセージです
7.	DEBUG ：デバッグレベルのメッセージ

c. * Facility * の場合、各メッセージを外部 syslog に送信する際に、ローカル syslog の場合と同じファシリティ値を使用するには、 **Passthrough** を選択します。

   監査ログの場合、* Passthrough *を選択すると、外部syslogサーバに送信されるファシリティは「local7」になります。

   セキュリティ・イベントの場合は、 *Passthrough * を選択すると、ノード上の Linux ディストリビューションによってファシリティ値が生成されます。

   アプリケーション・ログの場合、 *Passthrough * を選択すると、外部 syslog サーバに送信されるアプ

リケーション・ログには、次のファシリティ値が設定されます。

アプリケーションログ	パススルー値
bycast.log	ユーザまたはデーモン
bycast-err.log	user 、 daemon 、 local3 、または local4
jaeger.log	local2
nms.log	ローカル 3
prometheus.log	「 LOCAL4 」
raft.log	local5
hagroups.log	local6

d. パススルー値を使用しない場合は、0～23のファシリティ値を選択します。

選択した値は、このタイプのすべてのメッセージに適用されます。施設を固定値でオーバーライドすることを選択すると、さまざまな施設に関する情報が失われます。

ファシリティ	説明
0	kern （カーネルメッセージ）
1.	ユーザ（ユーザレベルのメッセージ）
2.	メール
3.	デーモン（システムデーモン）
4.	AUTH （セキュリティ / 認証メッセージ）
5.	syslog （ syslogd で内部的に生成されるメッセージ）
6.	LPR （ラインプリンタサブシステム）
7.	News （ネットワークニュースサブシステム）
8.	UUCP
9.	cron クロックデーモン

ファシリティ	説明
10.	セキュリティ（セキュリティ / 認可メッセージ）
11.	FTP
12.	NTP
13	logaudit （ログ監査）
14	logalert （ログアラート）
15	clock （ clock デーモン）
16	local0
17	local1
18	local2
19	ローカル 3
20	「 LOCAL4 」
21	local5
22	local6
23	local7

3. 「 * Continue * 」を選択します。

テストメッセージを送信します

外部 syslog サーバの使用を開始する前に、グリッド内のすべてのノードが外部 syslog サーバにテストメッセージを送信するように要求する必要があります。外部 syslog サーバへのデータ送信にコミットする前に、これらのテストメッセージを使用してログ収集インフラ全体を検証する必要があります。

外部syslogサーバがグリッド内の各ノードからテストメッセージを受信し、メッセージが想定どおりに処理されたことを確認するまでは、外部syslogサーバの設定を使用しないでください。

手順

1. 外部syslogサーバが適切に設定され、グリッド内のすべてのノードから監査情報を受信できることが確実であるためにテストメッセージを送信しない場合は、*[スキップして終了]*を選択します。

設定が正常に保存されたことを示す緑のバナーが表示されます。

2. それ以外の場合は、テストメッセージを送信（推奨）を選択します。

   テスト結果は、テストを停止するまでページに継続的に表示されます。テストの実行中も、以前に設定した送信先に監査メッセージが引き続き送信されます。

3. エラーが発生した場合は、修正して、もう一度 [テストメッセージを送信する *] を選択します。

   を参照してください "外部 syslog サーバのトラブルシューティング" エラーの解決に役立ちます。

4. すべてのノードがテストに合格したことを示す緑のバナーが表示されるまで待ちます。
5. syslog サーバを調べて、テストメッセージが正常に受信および処理されているかどうかを確認します。

   UDP を使用している場合は、ログ収集インフラストラクチャ全体を確認します。UDP プロトコルでは、他のプロトコルと同様に厳しいエラー検出はできません。

6. 「 * ストップ & フィニッシュ * 」を選択します。

   監査および syslog サーバ * ページに戻ります。syslog サーバの設定が正常に保存されたことを示す緑のバナーが表示されます。

   外部 syslog サーバを含む送信先を選択するまで、 StorageGRID 監査情報は外部 syslog サーバに送信されません。

監査情報の送信先を選択します

セキュリティイベントログ、アプリケーションログ、および監査メッセージログの送信先を指定できます。

StorageGRID ソフトウェアログの詳細については、を参照してください "StorageGRID ソフトウェアのログ"。

手順

1. Audit and syslog server ページで、表示されたオプションから監査情報の宛先を選択します。

オプション	説明
デフォルト（管理ノード / ローカルノード）	監査メッセージが監査ログに送信されます (`audit.log`管理ノードでは、セキュリティイベントログとアプリケーションログが生成されたノード（「ローカルノード」とも呼ばれます）に格納されます。
外部 syslog サーバ	監査情報が外部 syslog サーバに送信され、ローカルノードに保存されます。送信される情報の種類は、外部 syslog サーバの設定方法によって異なります。このオプションは、外部 syslog サーバを設定した場合にのみ有効になります。

オプション	説明
管理ノードと外部 syslog サーバ	監査メッセージが監査ログに送信されます (`audit.log`）が管理ノードに送信され、監査情報が外部syslogサーバに送信されてローカルノードに保存されます。送信される情報の種類は、外部 syslog サーバの設定方法によって異なります。このオプションは、外部 syslog サーバを設定した場合にのみ有効になります。
ローカルノードのみ	管理ノードまたはリモート syslog サーバには監査情報は送信されません。監査情報は、生成したノードにのみ保存されます。 • 注： StorageGRID は、定期的にこれらのローカルログをローテーションから削除して、スペースを解放します。ノードのログファイルが 1GB に達すると、既存のファイルが保存され、新しいログファイルが開始されます。ログのローテーションの上限は 21 ファイルです。ログファイルの 22 番目のバージョンが作成されると、最も古いログファイルが削除されます。各ノードには平均約 20GB のログデータが格納されます。

すべてのローカルノードで生成された監査情報はに格納されます `/var/local/log/localaudit.log`

2. [保存（ Save ）] を選択します。次に、* OK *を選択して、ログの保存先への変更を確定します。
3. 監査情報のデスティネーションとして外部 syslog サーバ * または * 管理ノードと外部 syslog サーバ * のどちらかを選択した場合は、追加の警告が表示されます。警告テキストを確認します。

外部 syslog サーバがテスト用の StorageGRID メッセージを受信できることを確認する必要があります。

4. [OK]*を選択して、監査情報の保存先を変更することを確認します。

   監査設定が正常に保存されたことを示す緑のバナーが表示されます。

   選択した送信先に新しいログが送信されます。既存のログは現在の場所に残ります。

関連情報

"監査メッセージの概要"

"監査メッセージとログの送信先を設定します"

"システム監査メッセージ"

"オブジェクトストレージ監査メッセージ"

"管理監査メッセージ"

"クライアント読み取り監査メッセージ"

"StorageGRID の管理"

著作権に関する情報

商標に関する情報