監査メッセージとログの送信先の設定

StorageGRID 11.8

NetApp
March 19, 2024

目次

監査メッセージとログの送信先の設定

外部**syslog**サーバを使用する場合の考慮事項

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。外部のsyslogサーバを使用すると、管理ノードのネットワークトラフィックを軽減し、情報をより効率的に管理できます。StorageGRIDの場合、発信syslogメッセージパケット形式はRFC 3164に準拠しています。

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**サーバを使用する状況

外部のsyslogサーバは、大規模なグリッドを使用する場合、複数のタイプのS3アプリケーションを使用する場合、またはすべての監査データを保持する場合に特に役立ちます。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します。
- 監査情報はさまざまなストレージノードから外部syslogサーバに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を削減します。管理ノードを経由する必要はありません。

> 外部syslogサーバにログを送信すると、8、192バイトを超える単一のログがメッセージの最後で切り捨てられ、外部syslogサーバの実装における一般的な制限事項に準拠します。

> 外部syslogサーバに障害が発生した場合にフルデータリカバリのオプションを最大化するには、最大20 GBの監査レコードのローカルログを使用します。（`localaudit.log`）は各ノードで維持されます。

外部**syslog**サーバの設定方法

外部syslogサーバの設定方法については、を参照してください。 "監査メッセージと外部syslogサーバの設定"。

TLSまたはRELP/TLSプロトコルを使用するように設定する場合は、次の証明書が必要です。

- サーバ**CA**証明書：PEMエンコードで外部syslogサーバを検証するための1つ以上の信頼されたCA証明書。省略すると、デフォルトの Grid CA 証明書が使用されます。
- クライアント証明書：PEMエンコードによる外部syslogサーバへの認証用のクライアント証明書。
- クライアント秘密鍵：PEMエンコードでのクライアント証明書の秘密鍵。

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）。

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 ）。

ここでは、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	監査ログ速度= 8 x S3処理速度
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。
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 ）。

KをS3アカウント名、S3バケット、S3キーの合計の平均サイズとします。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 ）。

KをS3アカウント名、S3バケット、S3キーの合計の平均サイズとします。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処理に対応している場合、ワークロードは50%のPUTになり、S3アカウント名、バケット名 オブジェクト名の平均は90バイトです。外部syslogサーバは、1秒あた

り2、250個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し、1秒あたり0.6MBの速度でアプリケーションデータを受信（格納）できるようにする必要があります。

監査メッセージと外部syslogサーバの設定

監査メッセージに関連するいくつかの設定を行うことができます。記録する監査メッセージの数の調整、クライアントの読み取り/書き込み監査メッセージに含めるHTTP要求ヘッダーの定義、外部syslogサーバの設定、監査ログ、セキュリティイベントログ、およびStorageGRIDソフトウェアログの送信先の指定を行うことができます。

監査メッセージとログには、システムのアクティビティとセキュリティイベントが記録され、監視とトラブルシューティングに不可欠なツールです。すべての StorageGRID ノードで監査メッセージとログが生成され、システムアクティビティとイベントが追跡されます。

必要に応じて、監査情報をリモートで保存するように外部syslogサーバを設定できます。外部サーバを使用すると、監査データの完全性を損なうことなく、監査メッセージロギングによるパフォーマンスへの影響を最小限に抑えることができます。外部のsyslogサーバは、大規模なグリッドを使用する場合、複数のタイプのS3アプリケーションを使用する場合、またはすべての監査データを保持する場合に特に役立ちます。を参照してください "外部 syslog サーバに関する考慮事項" を参照してください。

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"。
- を使用することができます "Maintenance権限またはRoot Access権限"。
- 外部syslogサーバを設定する場合は、 "外部syslogサーバを使用する場合の考慮事項" また、ログファイルを受信して保存するのに十分な容量がサーバにあることを確認します。
- TLSまたはRELP/TLSプロトコルを使用して外部syslogサーバを設定する場合は、必要なサーバCAとクライアント証明書、およびクライアント秘密鍵が必要です。

監査メッセージレベルの変更

監査ログでは、次のカテゴリのメッセージごとに異なる監査レベルを設定できます。

監査カテゴリ	デフォルト設定です	詳細情報
システム	正常	"システム監査メッセージ"
ストレージ	エラー	"オブジェクトストレージ監査メッセージ"
管理	正常	"管理監査メッセージ"
クライアント読み取り	正常	"クライアント読み取り監査メッセージ"
クライアントからの書き込み	正常	"クライアント書き込み監査メッセージ"

監査カテゴリ	デフォルト設定です	詳細情報
ILM	正常	"ILM監査メッセージ"
グリッド間レプリケーション	エラー	"CGRR：クロスグリッドレプリケーション要求"

これらのデフォルト値は、 StorageGRID 10.3 以降を最初にインストールした場合に適用されます。以前のバージョンのStorageGRIDを最初に使用した場合、すべてのカテゴリのデフォルトは[標準]に設定されます。

アップグレード中は、監査レベルの設定はすぐには有効になりません。

手順

1. * configuration * > * Monitoring * > * Audit and syslog server * を選択します。
2. 監査メッセージのカテゴリごとに、ドロップダウンリストから監査レベルを選択します。

監査レベル	説明
オフ	このカテゴリの監査メッセージはログに記録されません。
エラー	エラーメッセージのみがログに記録されます — 結果コードが「成功」（ SUCS ）以外の監査メッセージ。
正常	標準のトランザクション・メッセージはログに記録されますこのメッセージは ' カテゴリに関する次の手順に記載されています
デバッグ	非推奨。このレベルの動作は Normal 監査レベルと同じです。

特定のレベルに含まれるメッセージには、上位レベルでロギングされるメッセージも含まれます。たとえば、 Normal レベルには Error レベルのメッセージがすべて含まれます。

S3アプリケーションに対するクライアント読み取り処理の詳細なレコードを確認する必要がない場合は、必要に応じて* Client Reads 設定を Error *に変更して、監査ログに記録される監査メッセージの数を減らします。

3. [保存（ Save ）] を選択します。

緑色のバナーは、設定が保存されたことを示します。

HTTP要求ヘッダーの定義

必要に応じて、クライアントの読み取り/書き込み監査メッセージに含めるHTTP要求ヘッダーを定義できます。これらのプロトコルヘッダーは、S3要求とSwift要求にのみ適用されます。

手順

1. [Audit protocol headers]セクションで、クライアントの読み取り/書き込み監査メッセージに含めるHTTP要求ヘッダーを定義します。

   0 個以上の文字に一致させるには、ワイルドカードとしてアスタリスク（ * ）を使用します。リテラルアスタリスクに一致させるには、エスケープシーケンス（ \ * ）を使用します。

2. 必要に応じて、「 * 別のヘッダーを追加」を選択して追加のヘッダーを作成します。

   要求に HTTP ヘッダーが含まれている場合、 HTTP ヘッダーは HTRH フィールドの下の監査メッセージに含まれます。

   監査プロトコル要求ヘッダーは、 * クライアント読み取り * または * クライアント書き込み * の監査レベルが * オフ * でない場合にのみ記録されます。

3. [保存（ Save ）] を選択します

   緑色のバナーは、設定が保存されたことを示します。

[use-external-syslog-server]]外部syslogサーバを使用する

必要に応じて、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の外部の場所に保存するように外部のsyslogサーバを設定できます。

外部syslogサーバを使用しない場合は、この手順を省略して 監査情報の送信先を選択します。

この手順で使用可能な構成オプションが要件を満たすのに十分な柔軟性を備えていない場合は、 `audit-destinations` エンドポイント（のプライベートAPIセクションにあります）"Grid 管理 API"。たとえば、ノードのグループごとに異なるsyslogサーバを使用する場合は、APIを使用できます。

syslog情報の入力

外部syslogサーバの設定ウィザードにアクセスし、StorageGRIDが外部syslogサーバにアクセスするために必要な情報を入力します。

手順

1. 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。または、以前に外部syslogサーバを設定した場合は、*[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。

2. 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。
3. 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）。デフォルトのポートは514です。
4. 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。

5. 「 * Continue * 」を選択します。
6. [[attach-certificate]* TLS または RELP/TLS *を選択した場合は、サーバCA証明書、クライアント証明書、およびクライアント秘密鍵をアップロードします。
   a. 使用する証明書またはキーの [* 参照] を選択します。
   b. 証明書またはキーファイルを選択します。
   c. 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。
7. 「 * 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`

   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"。

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ごとに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の値を設定すると、ログをカスタマイズ可能な方法で集約して分析を容易にすることができます。

   a. では、[Passthrough]*を選択するか、重大度値を0~7で選択します。

      値を選択すると、選択した値がこのタイプのすべてのメッセージに適用されます。固定値で重大度を上書きすると、異なる重大度に関する情報が失われます。

重大度	説明
パススルー	外部syslogに送信される各メッセージの重大度は、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。 • 監査ログの場合、重大度は「info」です。 • セキュリティイベントの場合、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重大度は、問題の内容に応じて「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が「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が「notice」になります。
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

   b. *Facilty*では、*Passthrough*を選択するか、0～23のファシリティ値を選択します。

      値を選択すると、このタイプのすべてのメッセージに適用されます。固定値でファシリティを上書きすると、さまざまなファシリティに関する情報が失われます。

ファシリティ	説明
パススルー	外部syslogに送信される各メッセージのファシリティ値は、ノードにローカルにログインしたときと同じです。 • 監査ログの場合、外部syslogサーバに送信されるファシリティは「local7」です。 • セキュリティイベントの場合、ファシリティ値はノード上の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、外部syslogサーバに送信されるアプリケーションログのファシリティ値は次のとおりです。 ◦ `bycast.log`:ユーザーまたはデーモン ◦ `bycast-err.log`：user、daemon、local3、またはlocal4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3 ◦ `prometheus.log`：local4 ◦ `raft.log`: local5 ◦ `hagroups.log`：local6
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
10	セキュリティ（セキュリティ / 認可メッセージ）
11	FTP

ファシリティ	説明
12	NTP
13	logaudit （ログ監査）
14	logalert （ログアラート）
15	clock （ clock デーモン）
16	ローカル0
17	ローカル1
18	ローカル2
19	ローカル 3
20	「 LOCAL4 」
21.	ローカル5
22	ローカル6
23	ローカル7

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。

   緑色のバナーは、設定が保存されたことを示します。

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を行います" 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、他のプロトコルほど厳密なエラー検出は許可されていません。 プロトコル。

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。緑色のバナーは、syslogサーバの設定が保存されたことを示します。

   外部syslogサーバを含むデスティネーションを選択するまで、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

監査ログ、セキュリティイベントログ、 "StorageGRID ソフトウェアのログ" が送信されます。

一部の送信先は、外部syslogサーバが設定されている場合にのみ使用できます。

手順

1. [Audit and syslog server]ページで、監査情報の保存先を選択します。

   *ローカルノードのみ*および*外部syslogサーバ*の方が一般的にパフォーマンスが向上します。

オプション	説明
ローカルノードのみ	監査メッセージ、セキュリティイベントログ、およびアプリケーションログは管理ノードに送信されません。代わりに、それらはそれらを生成したノード（「ローカルノード」）にのみ保存されます。すべてのローカルノードで生成された監査情報は、`/var/local/log/localaudit.log` 注：StorageGRIDは定期的にローカルログをローテーションで削除し、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。

オプション	説明
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（`/var/local/log/audit.log`）が管理ノードに格納され、セキュリティイベントログとアプリケーションログは、それらを生成したノードに格納されます。
外部 syslog サーバ	監査情報は外部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。
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（`/var/local/log/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。

2. [保存（ Save ）] を選択します。

   警告メッセージが表示されます。

3. [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。

   緑色のバナーは、監査設定が保存されたことを示します。

   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。

著作権に関する情報

商標に関する情報