監査メッセージとログの送信先を構成する
StorageGRID software

NetApp
December 03, 2025

目次

監査メッセージとログの送信先を構成する

外部Syslogサーバーの使用に関する考慮事項

外部 Syslog サーバーは、 StorageGRIDの外部にあるサーバーであり、システム監査情報を 1 か所に収集するために使用できます。外部 Syslog サーバーを使用すると、管理ノード上のネットワーク トラフィックを削減し、情報をより効率的に管理できます。StorageGRIDの場合、送信 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 サーバーに送信できる監査情報の種類は次のとおりです。

- 通常のシステム操作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のセキュリティ関連のイベント
- 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開く必要がある場合に要求される可能性のあるアプリケーションログ

外部Syslogサーバーを使用する場合

外部 syslog サーバーは、大規模なグリッドがある場合、複数の種類の 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便利です。監査情報を外部 Syslog サーバーに送信すると、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。
- 監査情報は管理ノードを経由せずにさまざまなストレージノードから外部 syslog サーバーに直接転送されるため、管理ノード上のネットワーク トラフィックが削減されます。

> ログが外部 syslog サーバーに送信される場合、外部 syslog サーバーの実装における一般的な制限に準拠するために、8,192 バイトを超える単一ログはメッセージの末尾で切り捨てられます。

> 外部Syslogサーバの障害発生時に完全なデータ復旧のオプションを最大限にするために、監査記録のローカルログを最大20GBまで保存します。(`localaudit.log` ）が各ノードで維持されます。

外部Syslogサーバーの設定方法

外部Syslogサーバーの設定方法については、"監査メッセージと外部Syslogサーバーを構成する" 。

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

- サーバー **CA** 証明書: PEM エンコードで外部 syslog サーバーを検証するための 1 つ以上の信頼できる CA 証明書。省略した場合は、デフォルトのグリッド CA 証明書が使用されます。
- クライアント証明書: PEM エンコードされた外部 syslog サーバーへの認証用のクライアント証明書。

- クライアント秘密キー: PEM エンコードされたクライアント証明書の秘密キー。

> クライアント証明書を使用する場合は、クライアントの秘密キーも使用する必要があります。暗号化された秘密鍵を提供する場合は、パスフレーズも提供する必要があります。暗号化された秘密キーを使用すると、キーとパスフレーズを保存する必要があるため、セキュリティ上の大きな利点はありません。簡素化のため、使用可能な場合は、暗号化されていない秘密キーを使用することをお勧めします。

外部Syslogサーバー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 操作数または 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できるようにサイズ設定されます。たとえば、グリッドで 1 秒あたり 1,000 件の S3 操作、または 1 秒あたり 2,000 MB のオブジェクトの取り込みと取得を処理する必要があるとします。グリッドのデータ要件に応じて外部 Syslog サーバーのサイズを決定する必要があります。

このセクションでは、外部 Syslog サーバーが処理でき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 操作数) に基づいて見積もるのに役立ついくつかのヒューリスティックな式を示します。

推定式で **1** 秒あたりの **S3** 操作を使用する

グリッドのサイズが 1 秒あたりのバイト数で表されるスループットに合わせて設定されている場合、推定式を使用するには、このサイズを 1 秒あたりの S3 操作数に変換する必要があります。グリッド スループットを変換するには、まず平均オブジェクト サイズを決定する必要があります。これは、既存の監査ログとメトリック (存在する場合) の情報を使用するか、 StorageGRID を使用するアプリケーションに関する知識を使用して行うことができます。たとえば、グリッドが 2,000 MB/秒のスループットを実現するようにサイズ設定され、平均オブジェクト サイズが 2 MB の場合、グリッドは 1 秒あたり 1,000 件の S3 操作 (2,000 MB / 2 MB) を処理できるようにサイズ設定されていることになります。

> 次のセクションの外部 Syslog サーバーのサイズ設定の式は、最悪のケースの見積もりではなく、一般的なケースの見積もりを提供します。構成とワークロードによっては、数式で予測されるよりも syslog メッセージの割合や syslog データの量が多くなったり少なくなったりする場合があります。数式はガイドラインとしてのみ使用してください。

監査ログの推定式

グリッドがサポートすると予想される 1 秒あたりの S3 操作の数以外に S3 ワークロードに関する情報がない場合は、監査レベルをデフォルト値 (ストレージを除くすべてのカテゴリを [通常] に設定、ストレージは [エラー] に設定) のままにしておくことを前提として、次の式を使用して外部 syslog サーバーが処理する必要がある監査ログの量を見積もることができます。

```
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 件の S3 操作に対応している場合、外部 syslog サーバーのサイズは 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設定し、1 秒あたり 1.6 MB の速度で監査ログ データを受信 (通常は保存) できる必要があります。

作業負荷について詳しく知っていれば、より正確な見積もりが可能になります。監査ログの場合、最も重要な

追加変数は、PUT (GET と比較) である S3 操作の割合と、次の S3 フィールドの平均サイズ (バイト単位) です (表で使用されている 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（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
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。クロスアカウントまたは匿名アクセスを識別するために使用されます。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。

P を使用して、PUT である S3 操作の割合を表します (0 ≤ P ≤ 1) (つまり、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 を使用して、S3 アカウント名、S3 バケット、および 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-account (13 バイト) であり、バケットの名前が /my/application/bucket-12345 (28 バイト) のような固定長であり、オブジェクトが 5733a5d7-f069-41ef-8fbd-13247494c69c (36 バイト) のような固定長キーを持っているとします。するとKの値は90（13+13+28+36）になります。

P と K の値を決定できる場合は、監査レベルをデフォルト（ストレージを除くすべてのカテゴリを「通常」に設定、ストレージは「エラー」に設定）のままにしておくことを前提として、次の式を使用して外部 syslog サーバーが処理する必要がある監査ログの量を見積もることができます。

```
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 件の S3 操作に対応し、ワークロードの 50% が PUT であり、S3 アカウント名、バケット名、およびオブジェクト名の平均が 90 バイトである場合、外部 syslog サーバーは 1 秒あたり 1,500 件の syslog メッセージをサポートするサイズに設定し、監査ログ データを 1 秒あたり約 1 MB の速度で受信 (および通常は保存) できる必要があります。

デフォルト以外の監査レベルの推定式

監査ログに提供される数式では、デフォルトの監査レベル設定 (ストレージを除くすべてのカテゴリが [通常] に設定されているが、ストレージは [エラー] に設定されている) を使用することを前提としています。デフォルト以外の監査レベル設定の監査メッセージのレートと平均サイズを見積もるための詳細な数式は利用できません。ただし、次の表を使用して、レートの大まかな見積もりを行うことができます。監査ログに提供されている平均サイズの計算式を使用することもできますが、「追加の」監査メッセージは平均してデフォルトの監査メッセージよりも小さいため、過大な見積もり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: 監査レベルはすべてデバッグまたは通常に設定されています	監査ログレート = 8 x S3 操作レート
消去コーディング: 監査レベルはすべてデバッグまたは通常に設定されています	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 操作と相関しておらず、通常はごくわずかな量のログとデータが生成されます。これらの理由により、推定式は提供されません。

アプリケーションログの推定式

グリッドがサポートすると予想される 1 秒あたりの S3 操作の数以外に 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 サーバーが処理する必要があるアプリケーション ログの量を見積もることができます。

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

したがって、たとえば、グリッドのサイズが 1 秒あたり 1,000 回の S3 操作に対応している場合、外部 syslog サーバーのサイズは、1 秒あたり 3,300 回のアプリケーション ログをサポートし、1 秒あたり約 1.2 MB の速度でアプリケーション ログ データを受信 (および保存) できるようにする必要があります。

作業負荷について詳しく知っていれば、より正確な見積もりが可能になります。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消去コーディング)、PUT である S3 操作の割合 (GET/その他と比較)、および次の S3 フィールドの平均サイズ (バイト単位) です (表で使用されている 4 文字の略語は監査ログ 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（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
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。クロスアカウントまたは匿名アクセスを識別するために使用されます。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。

サイズ見積りの例

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について説明します。

- レプリケーション
- イレイジャー コーディング

データ保護のためにレプリケーションを使用する場合

P は、PUT である S3 操作の割合を表します。ここで、0 ≤ P ≤ 1 です (つまり、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 は、S3 アカウント名、S3 バケット、および 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-account (13 バイト) であり、バケットの名前が /my/application/bucket-12345 (28 バイト) のような固定長であり、オブジェクトが 5733a5d7-f069-41ef-8fbd-13247494c69c (36 バイト) のような固定長キーを持っているとします。するとKの値は90（13+13+28+36）になります。

P と K の値を特定できる場合は、次の式を使用して、外部 syslog サーバーが処理する必要があるアプリケーション ログの量を見積もることができます。

```
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
```

したがって、たとえば、グリッドのサイズが 1 秒あたり 1,000 件の S3 操作に対応し、ワークロードの 50% が PUT であり、S3 アカウント名、バケット名、およびオブジェクト名の平均が 90 バイトである場合、外部 syslog サーバーは 1 秒あたり 1,800 件のアプリケーション ログをサポートするようにサイズ設定する必要があり、0.5 MB/秒の速度でアプリケーション データを受信 (および通常は保存) することになります。

データ保護のために消失訂正符号を使用する場合

P は、PUT である S3 操作の割合を表します。ここで、0 ≤ P ≤ 1 です (つまり、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 は、S3 アカウント名、S3 バケット、および 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-account (13 バイト) であり、バケットの名前が /my/application/bucket-12345 (28 バイト) のような固定長であり、オブジェクトが 5733a5d7-f069-41ef-8fbd-13247494c69c (36 バイト) のような固定長キーを持っているとします。するとKの値は90（13+13+28+36）になります。

P と K の値を特定できる場合は、次の式を使用して、外部 syslog サーバーが処理する必要があるアプリケーション ログの量を見積もることができます。

```
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
```

したがって、たとえば、グリッドのサイズが 1 秒あたり 1,000 件の S3 操作に対応し、ワークロードの 50% が PUT であり、S3 アカウント名、バケット名、およびオブジェクト名の平均が 90 バイトである場合、外部

syslog サーバーは 1 秒あたり 2,250 件のアプリケーション ログをサポートするサイズに設定し、0.6 MB/秒の速度でアプリケーション データを受信 (および通常は保存) できる必要があります。

監査メッセージと外部Syslogサーバーを構成する

監査メッセージに関連するさまざまな設定を構成できます。記録される監査メッセージの数を調整したり、クライアントの読み取りおよび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たり、外部 Syslog サーバーを構成したり、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 ログの送信先を指定したりできます。

監査メッセージとログは、システム アクティビティとセキュリティ イベントを記録し、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ノードは、システム アクティビティとイベントを追跡するために監査メッセージとログを生成します。

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 サーバーを構成することもできます。外部サーバーを使用すると、監査データの完全性を低下させることなく、監査メッセージのログ記録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 syslog サーバーは、大規模なグリッドがある場合、複数の種類の 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便利です。見る"監査メッセージと外部Syslogサーバーを構成する"詳細については。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"メンテナンスまたはルートアクセス権限"。
- 外部Syslogサーバーを設定する予定の場合は、"外部Syslogサーバーの使用に関する考慮事項"また、サーバーにログ ファイルを受信して保存するのに十分な容量があることを確認しました。
- TLS または RELP/TLS プロトコルを使用して外部 syslog サーバーを構成する場合は、必要なサーバー CA およびクライアント証明書とクライアント秘密キーが必要です。

監査メッセージのレベルの変更

監査ログ内の次のメッセージ カテゴリごとに異なる監査レベルを設定できます。

監査カテゴリ	デフォルトの設定	詳細情報
システム	平常時	"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	平常時	"経営監査メッセージ"
クライアントが読む	平常時	"クライアント読み取り監査メッセージ"

監査カテゴリ	デフォルトの設定	詳細情報
クライアントが書く	平常時	"クライアント書き込み監査メッセージ"
ILM	平常時	"ILM監査メッセージ"
クロスグリッドレプリケーション	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は、最初にバージョン 10.3 以降を使用してStorageGRIDをインストールした場合に適用されます。最初にStorageGRIDの以前のバージョンを使用した場合、すべてのカテゴリのデフォルトは [標準] に設定されています。

アップグレード中は、監査レベルの構成はすぐには有効になりません。

手順

1. 構成 > 監視 > 監査および **syslog** サーバー 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	このカテゴリからの監査メッセージは記録されません。
エラー	エラー メッセージ (結果コードが「成功」(SUCS) ではなかった監査メッセージ) のみがログに記録されます。
平常時	標準のトランザクション メッセージ (カテゴリのこの手順にリストされているメッセージ) がログに記録されます。
デバッグ	廃止されました。このレベルは、通常の監査レベルと同じように動作します。

特定のレベルに含まれるメッセージには、上位レベルで記録されるメッセージも含まれます。たとえば、通常レベルにはすべてのエラー メッセージが含まれます。

S3 アプリケーションのクライアント読み取り操作の詳細な記録が必要ない場合は、オプションで クライアント読み取り 設定を エラー 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*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リクエストヘッダーを定義する

オプションで、クライアントの読み取りおよび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 リクエストにのみ適用されます。

手順

1. 監査プロトコル ヘッダー セクションで、クライアントの読み取りおよび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 個以上の文字を一致させるには、アスタリスク (*) をワイルドカードとして使用します。リテラルのアスタリスクと一致させるには、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。

   リクエスト内に HTTP ヘッダーが見つかった場合、それらは監査メッセージの HTRH フィールドの下に含められます。

   > ⓘ 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*でない場合にのみログに記録されます。

3. *保存*を選択

   緑色のバナーは、設定が保存されたことを示します。

外部syslogサーバーを使用する

オプションで、監査ログ、アプリケーション ログ、セキュリティ イベント ログをグリッド外部の場所に保存するように外部 Syslog サーバーを構成することもできます。

> ⓘ 外部のSyslogサーバーを使用しない場合は、この手順をスキップして、監査情報の送信先を選択する 。

> 💡 この手順で利用できる設定オプションが要件を満たすほど柔軟でない場合は、 `audit-destinations`エンドポイントは、"グリッド管理API" 。たとえば、異なるノード グループに異なる syslog サーバーを使用する場合は、API を使用できます。

Syslog情報を入力する

外部 Syslog サーバーの構成ウィザードにアクセスし、 StorageGRID が外部 Syslog サーバーにアクセスするために必要な情報を提供します。

手順

1. 監査および Syslog サーバー ページで、外部 **Syslog** サーバーの構成*を選択します。または、以前に外部 **Syslog** サーバーを設定している場合は、**[*外部 Syslog** サーバーの編集] を選択します。

   外部 Syslog サーバーの構成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 ステップでは、ホスト フィールドに外部 Syslog サーバー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 サーバーの宛先ポートを入力します (1 ～ 65535 の整数である必要があります)。デフォルトポートは514です。
4. 監査情報を外部 syslog サーバーに送信するために使用するプロトコルを選択します。

   TLS または **RELP/TLS** の使用をお勧めします。これらのいずれかのオプションを使用するには、サーバー証明書をアップロードする必要があります。証明書を使用すると、グリッドと外部 syslog サーバー間の接続を保護できます。詳細については、以下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 オプションには、外部 syslog サーバーによるサポートと構成が必要です。外部 syslog サーバーと互換性のあるオプションを選択する必要があります。

   信頼性の高いイベント ログ プロトコル (RELP) は、syslog プロトコルの機能を拡張して、イベント メッセージの信頼性の高い配信を実現します。 RELP を使用すると、外部 syslog サーバーを再起動する必要がある場合に監査情報が失われるのを防ぐことができます。

5. *続行*を選択します。
6. **TLS** または **RELP/TLS** を選択した場合は、サーバー CA 証明書、クライアント証明書、およびクライアント秘密キーをアップロードします。
   a. 使用する証明書またはキーについては*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色のチェックが表示され、正常にアップロードされたことが通知されます。

7. *続行*を選択します。

Syslogコンテンツの管理

外部 syslog サーバー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 サーバーに送信する監査情報の各タイプを選択します。
   - 監査ログを送信: 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を送信: 権限のないユーザーがサインインしようとしたときや、ユーザーがルートとしてサインインしたときなどの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: 送信"StorageGRIDソフトウェア ログ ファイル"次のようなトラブルシューティングに役立ちます:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`(管理ノードのみ)
     - `prometheus.log`

- raft.log
- hagroups.log

◦ アクセス ログの送信: Grid Manager、Tenant Manger、構成されたロード バランサのエンドポイント、およびリモート システムからのグリッド フェデレーション要求への外部要求の HTTP アクセス ログを送信します。

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各カテゴリの重大度と機能 (メッセージの種類) を選択します。

   重大度とファシリティの値を設定すると、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。

   a. *重大度*では*パススルー*を選択するか、0～7の重大度値を選択します。

      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。重大度を固定値で上書きすると、さまざまな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には、ノードにローカルに記録されたときと同じ重大度値が設定されます。 • 監査ログの場合、重大度は「情報」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 ログの場合、問題の内容に応じて重大度は「情報」と「通知」の間で異なります。たとえば、NTP サーバーを追加して HA グループを構成すると、値は「info」になりますが、SSM 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。 • アクセス ログの場合、重大度は「情報」です。
0	緊急事態: システムが使用できません
1	警告: 直ちに行動を起こす必要があります
2	重大: 重大な状態
3	エラー: エラー状態
4	警告: 警告条件
5	通知: 正常だが重大な状態
6	情報: 情報メッセージ
7	デバッグ: デバッグレベルのメッセージ

b. **Facilty** の場合は、**Passthrough** を選択するか、0 から 23 の間の facility 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。 facility を固定値で上書きすると、さまざまな facility 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には、ノードにローカルに記録されたときと同じファシリティ値が設定されます。 • 監査ログの場合、外部 Syslog サーバーに送信される機能は「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 サーバー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。 ◦ `bycast.log`: ユーザーまたはデーモン ◦ `bycast-err.log`: ユーザー、デーモン、local3、または local4 ◦ `jaeger.log`: ローカル2 ◦ `nms.log`: ローカル3 ◦ `prometheus.log`: ローカル4 ◦ `raft.log`: ローカル5 ◦ `hagroups.log`: ローカル6 • アクセス ログの場合、外部 syslog サーバーに送信される機能は「local0」です。
0	kern（カーネルメッセージ）
1	ユーザー（ユーザーレベルのメッセージ）
2	郵便
3	デーモン（システムデーモン）
4	auth (セキュリティ/承認メッセージ)
5	syslog (syslogd によって内部的に生成されたメッセージ)
6	lpr（ラインプリンターサブシステム）
7	ニュース（ネットワークニュースサブシステム）

ファシリティ	説明
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/認証メッセージ）
11	FTP
12	NTP
13	logaudit（ログ監査）
14	logalert（ログアラート）
15	クロック（クロックデーモン）
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	ローカル4
21	ローカル5
22	ローカル6
23	ローカル7

3. *続行*を選択します。

テストメッセージを送信する

外部 Syslog サーバー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 サーバー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 サーバーにデータを送信する前に、これらのテスト メッセージを使用して、ログ収集インフラストラクチャ全体を検証する必要があります。

外部 Syslog サーバー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、メッセージが期待どおりに処理されたことを確認するまで、外部 Syslog サーバーの構成を使用しないでください。

手順

1. 外部 syslog サーバーが適切に構成されており、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なため、テスト メッセージを送信したくない場合は、[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] を選択します (推奨)。

   テストを停止するまで、テスト結果はページに継続的に表示されます。テストの進行中は、監査メッセージは以前に設定した送信先に引き続き送信されます。

3. Syslog サーバーの構成中または実行時にエラーが発生した場合は、エラーを修正して、テスト メッセージの送信 を再度選択してください。

   見る"外部 syslog サーバーのトラブルシューティング"エラーを解決するのに役立ちます。

4. すべてのノードがテストに合格したことを示す緑色のバナーが表示されるまで待ちます。

5. Syslog サーバーをチェックして、テスト メッセージが期待どおりに受信され、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てください。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できません。

6. *停止して終了*を選択します。

   監査および **syslog** サーバー ページに戻ります。緑色のバナーは、Syslog サーバーの構成が保存されたことを示します。

   外部 Syslog サーバを含む宛先を選択するまで、 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する

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

StorageGRIDはデフォルトでローカルノードの監査先を設定し、監査情報を `/var/local/log/localaudit.log`。

使用する場合 `/var/local/log/localaudit.log`、グリッド マネージャおよびテナント マネージャの監査ログ エントリがストレージ ノードに送信される場合があります。どのノードに最新のエントリがあるかは、 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`指示。

一部の宛先は、外部 Syslog サーバーが設定されている場合にのみ使用できます。

手順

1. 「監査および Syslog サーバー」ページで、監査情報の送信先を選択します。

通常、ローカル ノードのみ と 外部 **syslog** サーバー の方が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（デフォルト）	監査メッセージ、セキュリティ イベント ログ、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、それらはそれを生成したノード (「ローカル ノード」) にのみ保存されます。各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、スペースを解放するために、定期的にローカル ログをローテーションで削除します。ノードのログ ファイルが 1 GB 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制限は 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。平均して、各ノードには約 20 GB のログ データが保存されます。
管理ノード/ローカルノード	監査メッセージは管理ノードの監査ログに送信され、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保存されます。監査情報は次のファイルに保存されます。 • 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • すべてのノード: `/var/local/log/localaudit.log`通常、ファイルは空であるか、存在しません。一部のメッセージの追加コピーなどの二次情報が含まれる場合があります。
外部 syslog サーバー	監査情報は外部のSyslogサーバーに送信され、ローカルノードに保存されます。(`/var/local/log/localaudit.log` ）。送信される情報の種類は、外部 Syslog サーバー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 サーバーを構成した後にのみ有効になります。
管理ノードと外部Syslogサーバー	監査メッセージは監査ログに送信されます (`/var/local/audit/export/audit.log`）が管理ノード上に作成され、監査情報は外部のSyslogサーバーに送信され、ローカルノードに保存されます。(`/var/local/log/localaudit.log` ）。送信される情報の種類は、外部 Syslog サーバー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 サーバーを構成した後にのみ有効になります。

2. *保存*を選択します。

   警告メッセージが表示されます。

3. 監査情報の保存先を変更することを確認するには、[**OK**] を選択します。

   緑色のバナーは、監査構成が保存されたことを示します。

新しいログは選択した宛先に送信されます。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