監査メッセージの概要

StorageGRID 11.5

NetApp
April 11, 2024

目次

監査メッセージの概要

ここでは、 StorageGRID 監査メッセージおよび監査ログの構造と内容について説明します。この情報を使用して、システムアクティビティの監査証跡を判読し、分析できます。

ここに記載する手順は、システムのアクティビティおよび使用状況のレポート生成を担当する管理者を対象としています。このようなレポートの生成には、 StorageGRID システムの監査メッセージの分析が必要となります。

StorageGRID システム内の監査対象アクティビティの性質を十分に理解していることを前提としています。テキストログファイルを使用するには、管理ノード上に設定されている監査共有へのアクセスが必要です。

関連情報

"StorageGRID の管理"

監査メッセージのフローと保持

すべての StorageGRID サービスは通常のシステム運用中に監査メッセージを生成します。これらの監査メッセージがStorageGRID システムからにどのように転送されるかを理解しておく必要があります `audit.log` ファイル。

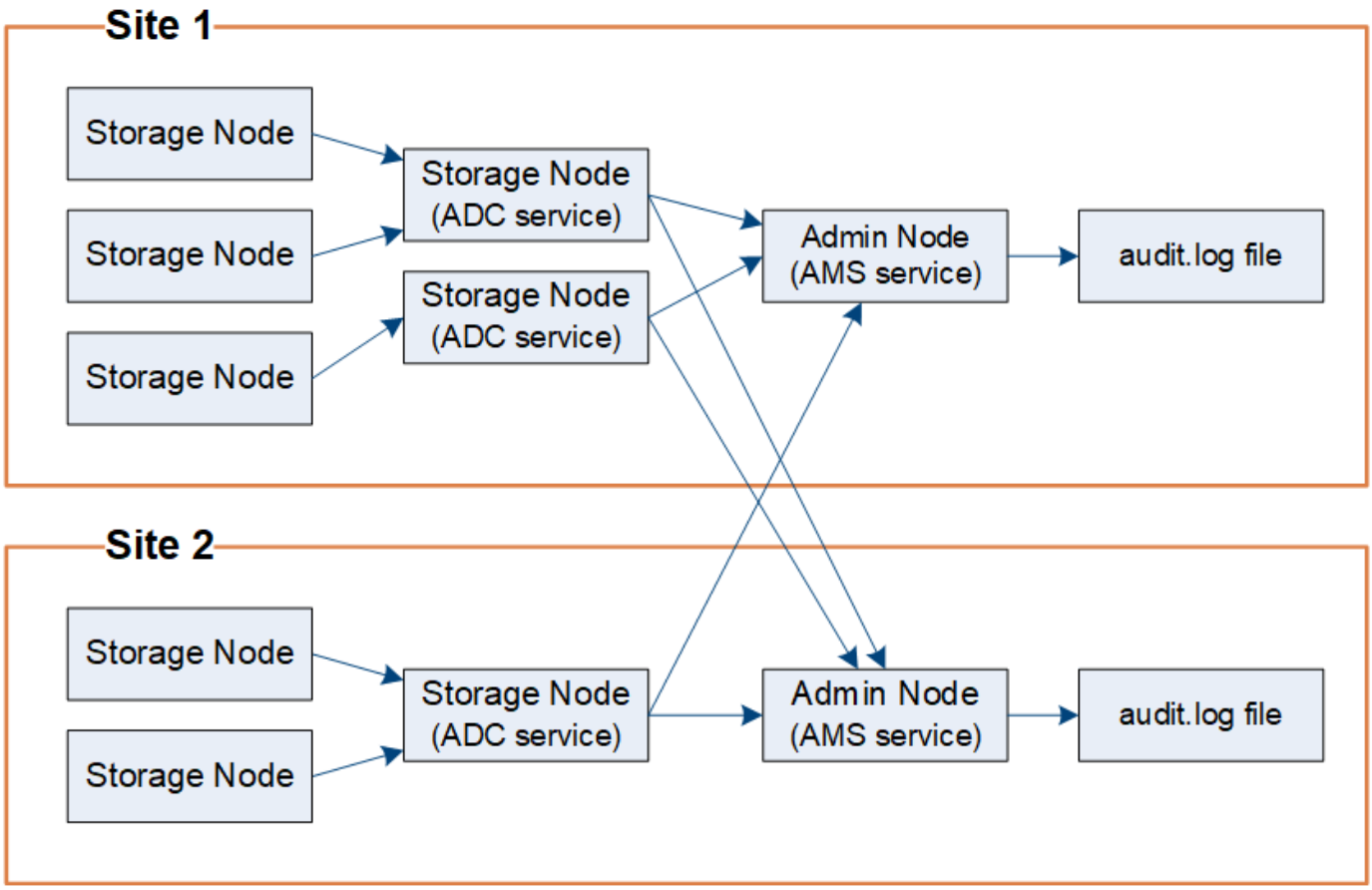
監査メッセージのフロー

監査メッセージは、管理ノードおよび Administrative Domain Controller （ ADC ）サービスが用意されているストレージノードによって処理されます。

監査メッセージのフロー図に示すように、各 StorageGRID ノードは監査メッセージをデータセンターサイトにあるいずれかの ADC サービスに送信します。ADC サービスは、各サイトに設置されている最初の 3 つのストレージノードで自動的に有効になります。

次に、各 ADC サービスはリレーとして機能し、監査メッセージの集合を StorageGRID システム内のすべての管理ノードに送信します。これにより、システムアクティビティの完全な記録が各管理ノードに提供されます。

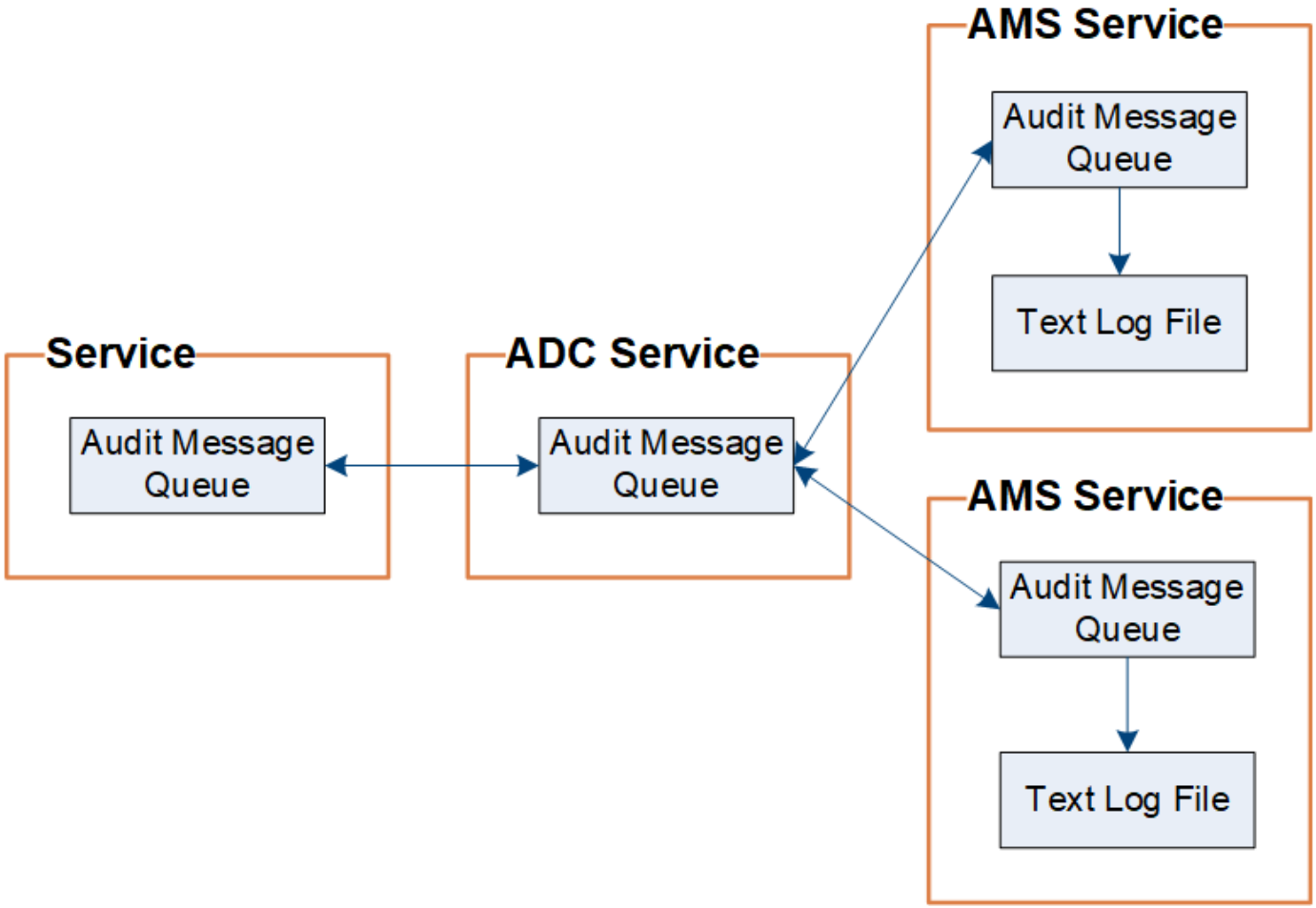
各管理ノードでは、監査メッセージがテキストログファイルに保存されます。アクティブなログファイルの名前はです `audit.log`。



監査メッセージの保持

StorageGRID では、コピー / 削除プロセスを使用して、監査ログに書き込まれる前に監査メッセージが失われないようにします。

ノードが生成またはリレーした監査メッセージは、グリッドノードのシステムディスク上の監査メッセージキューに格納されます。メッセージが管理ノード内の監査ログファイルに書き込まれるまで、メッセージのコピーは常に監査メッセージキューに保持されます `/var/local/audit/export` ディレクトリ。これにより、監査メッセージが転送中に失われることはありません。



ネットワーク接続の問題または監査容量の不足が原因で、監査メッセージキューが一時的に増加する可能性があります。キューが増加すると、各ノードの使用可能スペースがキューによってさらに消費されます `/var/local/` ディレクトリ。問題 が解除されず、ノードの監査メッセージディレクトリがいっぱいになると、個々のノードがバックログの処理の優先順位を設定し、一時的に新しいメッセージに使用できなくなります。

具体的には、次のような動作が発生することがあります。

- 状況に応じて `/var/local/audit/export` 管理ノードで使用されるディレクトリがいっぱいになると、ディレクトリに空きが出るまでその管理ノードを新しい監査メッセージに使用できないことを示すフラグが設定されます。S3 および Swift クライアント要求には影響しません。監査リポジトリにアクセスできない場合に XAMS （ Unreachable Audit Repositories ）アラームがトリガーされます。
- 状況に応じて `/var/local/` ADCサービスを採用するストレージノードで使用されるディレクトリが92%フルになると、ディレクトリが87%フルになるまでそのノードを監査メッセージに使用できないことを示すフラグが設定されます。他のノードに対する S3 および Swift クライアント要求には影響しません。監査リレーにアクセスできない場合に NRLY （ Available Audit Relays ）アラームがトリガーされます。

  ADCサービスを採用するストレージノードがない場合は、ストレージノードが監査メッセージをローカルに格納します。

- 状況に応じて `/var/local/` ストレージノードで使用されるディレクトリが85%フルになると、ノードはS3およびSwiftクライアントの要求を拒否し始めます `503 Service Unavailable`。

原因 監査メッセージキューが大幅に増加すると、次のような問題が発生する可能性があります。

- 管理ノードまたは ADC サービスを採用するストレージノードの停止。システムのいずれかのノードが停止すると、残りのノードはバックログ状態になる可能性があります。
- システムの監査キャパシティを超えるアクティビティ率の継続。
- 。 `/var/local/` 監査メッセージには関連のない理由でADCストレージノード上ののスペースがいっぱいになる。この場合、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログの優先順位を設定します。これにより、他のノードで原因 バックログが発生する可能性があります。

Large audit queue アラートと **Audit Messages Queued** （ **AMQS** ）アラーム

時間の経過に伴う監査メッセージキューのサイズを監視できるように、ストレージノードキューまたは管理ノードキュー内のメッセージの数が特定のしきい値に達すると、 * Large audit queue * アラートと従来の AMQS アラームがトリガーされます。

「 Large audit queue * 」アラートまたは従来の AMQS アラームがトリガーされた場合は、最初にシステムの負荷を確認します。最近のトランザクションの数が膨大であった場合は、アラートとアラームは時間が経過すると解決するため、無視してかまいません。

アラートまたはアラームが解決せず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。クライアントの書き込みとクライアントの読み取りでエラーまたはオフの監査レベルを変更して、クライアントの処理速度を下げるか、ログに記録される監査メッセージの数を減らしてください。「」を参照"監査メッセージレベルの変更". 」

重複メッセージです

StorageGRID システムは、ネットワークまたはノードの障害が発生した場合に保守的なアプローチを採用します。そのため、監査ログでメッセージが重複する可能性があります。

監査メッセージレベルの変更

監査レベルを調整して、監査ログに記録する監査メッセージの数を監査メッセージカテゴリごとに増減できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

監査ログに記録された監査メッセージは、* Configuration > Monitoring > Audit *ページの設定に基づいてフィルタリングされます。

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。

- システム：デフォルトでは、このレベルは[標準]に設定されています。
- * Storage *：デフォルトでは、このレベルはErrorに設定されています。
- 管理：デフォルトでは、このレベルは[標準]に設定されています。
- クライアント読み取り:デフォルトでは、このレベルはNormalに設定されています。

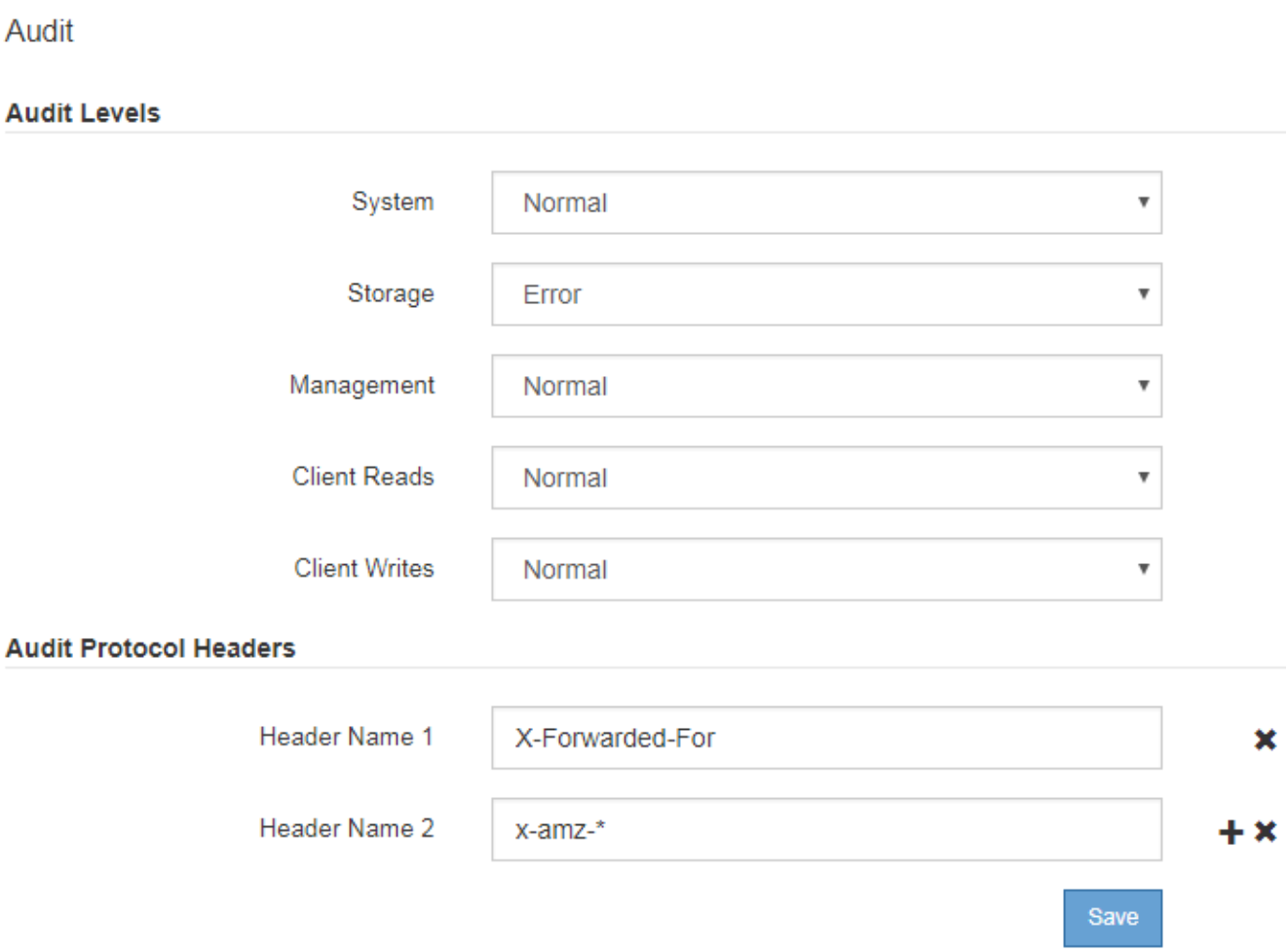
- クライアント書き込み：デフォルトでは、このレベルはNormalに設定されます。

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 からアップグレードした場合、すべてのカテゴリのデフォルトは Normal 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 *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。

監査レベル	説明
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。

3. 監査プロトコルヘッダー*で、クライアント読み取りおよびクライアント書き込み監査メッセージに含めるHTTP要求ヘッダーの名前を入力します。ワイルドカードとしてアスタリスク（*）を使用するか、リテラルアスタリスクとしてエスケープシーケンス（*）を使用します。プラス記号をクリックして、ヘッダー名フィールドのリストを作成します。

   監査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。

   このようなHTTPヘッダーが要求に含まれている場合、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。

4. [保存（ Save ）] をクリックします。

関連情報

"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"

監査ログファイルへのアクセス

監査共有にはアクティブなが含まれています `audit.log` ファイルおよび圧縮された監査ログファイル。監査ログへのアクセスを簡単にするためには、NFSとCIFSの両方についてクライアントから監査共有へのアクセスを設定します（現在CIFSは廃止）。管理ノードのコマンドラインから直接監査ログファイルにアクセスすることもできます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. 監査ログファイルが保存されているディレクトリに移動します。

```
cd /var/local/audit/export
```

3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

関連情報

"StorageGRID の管理"

監査ログファイルのローテーション

監査ログファイルは管理ノードに保存されます `/var/local/audit/export` ディレクトリ。アクティブな監査ログファイルの名前はです `audit.log`。

1日に1回、アクティブです `audit.log` ファイルが保存され、新しいファイルが作成されます `audit.log` ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています *`yyyy-mm-dd.txt`*。1日に複数の監査ログが作成される場合、ファイル名には、ファイルが保存された日付と番号が付加された日付が使用されます *`yyyy-mm-dd.txt.n`*。例： `2018-04-15.txt` および `2018-04-15.txt.1` 2018年4月15日に作成および保存された1つ目のログファイルおよび2つ目のログファイルです。

1日後、保存されたファイルは圧縮され、という形式で名前が変更されます *`yyyy-mm-dd.txt.gz`*`元の日付を保持します。そのため、時間の経過とともに、管理ノード上の監査ログ用に割り当てられたストレージが消費されます。スクリプトによって監査ログのスペース消費が監視され、のスペースを解放するために、必要に応じてログファイルが削除されます `/var/local/audit/export` ディレクトリ。監査ログは、作成日に基づいて、古い順に削除されます。スクリプトの処理は、次のファイルで監視できます。 `/var/local/log/manage-audit.log`。

この例は、アクティブを示しています `audit.log` ファイル。前日のファイルです (`2018-04-15.txt`）、および前日の圧縮ファイルです (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

著作権に関する情報

商標に関する情報