監査ログ
Active IQ Unified Manager

NetApp
October 15, 2025

目次

監査ログ 1
監査ログを構成する 2
監査ログのリモートログを有効にする 2

監査ログ

[監査ログ]を使用して、監査ログが侵害されていないかどうかを検出できます。ユーザが実行するアクティビティはすべて監視され、監査ログに記録されます。監査は、Active IQ Unified Managerのすべてのユーザー インターフェイスと公開されている API の機能に対して実行されます。

監査ログ: ファイル ビュー を使用すると、 Active IQ Unified Managerで使用可能なすべての監査ログ ファイルを表示およびアクセスできます。監査ログ: ファイル ビュー内のファイルは、作成日に基づいてリストされます。このビューには、インストールまたはアップグレードされてから現在までにシステムで取得されたすべての監査ログの情報が表示されます。Unified Managerで何らかの操作を実行すると、そのたびに情報が更新されてログに記録されます。各ログ ファイルのステータスは、「`File Integrity Status`」属性を使用してキャプチャされ、ログ ファイルの改ざんや削除を検出するためにアクティブに監視されます。システムで使用可能な監査ログは、次のいずれかのステータスになります。

州	説明
ACTIVE	ログを記録中のファイル。
NORMAL	圧縮されてシステムに格納されている、アクティブでないファイル。
TAMPERED	侵害されたファイル（権限のないユーザによって手動で編集された）。
MANUALL_DELETE	権限のあるユーザによって削除されたファイル。
ROLLOVER_DELETE	ローリング設定ポリシーに基づいてロールオフで削除されたファイル。
UNEXPECTED_DELETE	不明な理由で削除されたファイル。

[監査ログ]ページには、次のコマンド ボタンがあります。

- 設定
- 削除
- ダウンロード

削除 ボタンを使用すると、監査ログ ビューにリストされている監査ログを削除できます。監査ログを削除する際、あとで適切な削除だったことがわかるように、必要に応じてファイルの削除理由を指定することができます。この理由は、削除処理を実行したユーザの名前とともに[理由]列に表示されます。

ログ ファイルを削除すると、システムからファイルが削除されますが、DBテーブル内のエントリは削除されません。

監査ログ セクションの ダウンロード ボタンを使用してActive IQ Unified Managerから監査ログをダウンロードし、監査ログ ファイルをエクスポートできます。 「`NORMAL`」または「`TAMPERED`」とマークされたファイ

ルは圧縮された形式でダウンロードされます。 `.gzip`形式。

監査ログ ファイルは定期的にアーカイブされ、参照できるようにデータベースに保存されます。セキュリティと整合性を維持するために、アーカイブ前に監査ログはデジタル署名されます。

完全なAutoSupportバンドルには、アーカイブされた監査ログ ファイルとアクティブな監査ログ ファイルの両方が含まれます。一方、軽量なサポート バンドルには、アクティブな監査ログのみが含まれます。アーカイブされた監査ログは含まれません。

監査ログを構成する

監査ログ セクションの 構成 ボタンを使用して、監査ログ ファイルのローリング ポリシーを構成し、監査ログのリモート ログ記録を有効にすることもできます。

システムに保存するデータの希望量と頻度に応じて、最大ファイル サイズ と 監査ログ保持日数 の値を設定できます。フィールド **TOTAL AUDIT LOG SIZE** の値は、システム内に存在する監査ログ データの合計サイズです。ロールオーバー ポリシーは、監査ログ保持日数、最大ファイル サイズ、および 監査ログの合計サイズ フィールドの値によって決まります。監査ログのバックアップのサイズが **TOTAL AUDIT LOG SIZE** で設定された値に達すると、最初にアーカイブされたファイルが削除されます。つまり、最も古いファイルが削除されます。ただし、ファイル エントリはデータベース内で引き続き使用可能であり、「`Rollover Delete`」としてマークされます。 **AUDIT LOG RETENTION DAYS** の値は、監査ログ ファイルが保存される日数です。このフィールドで設定された値よりも古いファイルはロールオーバーされます。

手順

1. 監査ログ > > *構成*をクリックします。
2. 最大ファイル サイズ、監査ログの合計サイズ、および*監査ログの保持日数*に値を入力します。

   リモート ログを有効にする場合は、[リモート ログを有効にする] を選択する必要があります。 /// 2025-6-11、OTHERDOC-133

監査ログのリモートログを有効にする

監査ログの構成ダイアログボックスで*リモート ログを有効にする*チェックボックスをオンにすると、リモート監査ログを有効にすることができます。この機能を使用して、監査ログをリモートのsyslogサーバに転送できます。これにより、スペースに制約がある場合でも監査ログを管理できます。

監査ログのリモート ロギングは、Active IQ Unified Managerサーバ上の監査ログ ファイルが改ざんされた場合のバックアップとしても機能します。

手順

1. *監査ログの構成*ダイアログボックスで、*リモートログの有効化*チェックボックスをオンにします。

   リモート ロギングを設定するためのフィールドが表示されます。

2. 接続するリモート サーバーの **HOSTNAME** と **PORT** を入力します。
3. **SERVER CA CERTIFICATE** フィールドで、**BROWSE** をクリックして、対象サーバーの公開証明書を選択します。

証明書は、 `.pem`形式。ターゲットの`syslog`サーバから取得した、有効期限内の証明書を使用してください。証明書には、選択した「`hostname`」が `SubjectAltName`(SAN) 属性。

4. 次のフィールドに値を入力します: **CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   ミリ秒単位の値を指定してください。

5. **FORMAT** フィールドと **PROTOCOL** フィールドで必要な Syslog 形式と TLS プロトコル バージョンを選択します。
6. 対象の Syslog サーバーで証明書ベースの認証が必要な場合は、[クライアント認証を有効にする] チェックボックスをオンにします。

   監査ログ設定を保存する前に、クライアント認証証明書をダウンロードしてsyslogサーバにアップロードする必要があります。そうしないと、接続が失敗します。syslogサーバのタイプによっては、クライアント認証証明書のハッシュを作成する必要があります。

   例: syslog-ngでは、コマンドを使用して証明書の<ハッシュ>を作成する必要があります。 `openssl x509 -noout -hash -in cert.pem`次に、クライアント認証証明書を <ハッシュ> .0 という名前のファイルにシンボリック リンクする必要があります。

7. 保存 をクリックして、サーバーとの接続を構成し、リモート ログを有効にします。

   [監査ログ]ページにリダイレクトされます。

> 接続タイムアウト*の値は構成に影響する可能性があります。定義された値よりも応答に時間がかかると、接続エラーが発生して設定に失敗する可能性があります。正常な接続を確立するには、*接続タイムアウト の値を増やして、構成を再度試してください。

著作権に関する情報

商標に関する情報