監査ログ

Active IQ Unified Manager 9.13

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-913/config/task_configure_audit_logs.html on October 16, 2025. Always check docs.netapp.com for the latest.

目次

監査ログ 1
監査ログを設定しています 2
監査ログのリモートロギングを有効にする 2

監査ログ

監査ログを使用すると、監査ログが侵害されたかどうかを検出できます。ユーザが実行するすべてのアクティビティが監視され、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。

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してアクセスするには、*監査ログ：ファイルビュー*を使用します。監査ログ：ファイルビュー内のファイルは、作成日に基づいて一覧表示されます。このビューには、インストール時またはシステム内のにアップグレードされたときにキャプチャ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、情報が更新され、ログに記録されます。各ログファイルのステータスは、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る「 File Integrity Status 」属性を使用して取得されます。システムで監査ログが使用可能になると、監査ログの状態は次のいずれかになります。

状態	説明
アクティブ	ログが現在ログに記録されているファイル。
正常	非アクティブで圧縮され、システムに格納されているファイル。
改ざんされた	手動でファイルを編集したユーザーによって侵害されたファイル。
manual_delete_delete	許可されたユーザー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移動したために削除されたファイル。
予期しない削除です	不明な理由で削除されたファイル。

Audit Log 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

delete ボタンを使用すると、 Audit Logs ビューに表示されている監査ログを削除できます。監査ログを削除したり、ファイルを削除する理由を指定したりできます。これにより、あとで有効な削除を確認するのに役立ちます。理由列には、削除操作を実行したユーザの名前と理由が表示されます。

ログファイルを削除すると、原因によって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。

監査ログは、監査ログセクションの * download * ボタンを使用して Active IQ Unified Manager からダウンロードし、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` の形式で入力し

監査ログファイルは定期的にアーカイブされ、参照用にデータベースに保存されます。アーカイブの前に、監査ログはセキュリティと整合性を維持するためにデジタル署名されます。

フルAutoSupport バンドルの生成時に、サポート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。ただし、簡易サポートバンドルが生成されると、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。

監査ログを設定しています

監査ログセクションの *Configure * 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設定したり、監査ログのリモートロギングを有効にしたりできます。

システムに保存するデータの量と頻度に応じて、 * 最大ファイルサイズ * と * 監査ログの保持日数 * の値を設定できます。フィールド * total audit log size * は、システム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、「 * 監査ログの保持日数 * 」、「 * 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、監査ログの合計サイズ * 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。しかし、ファイルエントリはデータベースで引き続き使用でき、「ロールオーバー削除」とマークされます。監査ログの保持日数 * は、監査ログファイルを保持する日数です。このフィールドに設定された値より古いファイルは、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 * 、監査ログの保持日数 * の値を入力します。

   リモート・ロギングを有効にする場合は、 * リモート・ロギングを有効にする * を選択する必要があります。

監査ログのリモートロギングを有効にする

監査ログの設定ダイアログ・ボックスのリモート・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できますこの機能を使用すると、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に備えて、改ざんを防止するためのバックアップ機能を提供します。

手順

1. [監査ログの設定 *] 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します。

   リモートロギングを設定するための追加フィールドが表示されます。

2. 接続先のリモートサーバの * hostname * と * port * を入力します。
3. サーバー CA 証明書 * フィールドで、 * 参照 * をクリックしてターゲットサーバーのパブリック証明書を

選択します。

証明書はにアップロードする必要があります `.pem` の形式で入力しこの証明書は、ターゲットの syslog サーバから取得し、有効期限が切れていないことを確認する必要があります。証明書には、の一部として選択した「ホスト名」が含まれている必要があります `SubjectAltName` （SAN）属性。

4. 次のフィールドの値を入力します。 * charset* 、 * connection timeout * 、 * reconnection delay * 。

   これらのフィールドの値はミリ秒単位で指定します。

5. [**format**] フィールドと [**protocol**] フィールドで、必要な syslog 形式と TLS プロトコルのバージョンを選択します。
6. ターゲット 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選択します。

   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の作成が必要になる場合があります。

   例：syslog-ngには、コマンドを使用して証明書の<hash>が作成されている必要があります `openssl x509 -noout -hash -in cert.pem`をクリックし、クライアント認証証明書を<hash>.0のあと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. サーバとの接続を設定し、リモートロギングを有効にするには、 * Save * をクリックします。

   [監査ログ] ページに移動します。

> の値は、設定に影響する可能性があります。設定が定義された値よりも応答に時間がかかると、接続エラーが原因で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、設定をやり直してください。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。