監査ロギング
ONTAP 9

NetApp
February 12, 2026

目次

監査ロギング

ONTAP監査ログの実装について学ぶ

監査ログに記録された管理アクティビティは標準AutoSupportレポートに含まれ、特定のログアクティビティはEMSメッセージに含まれます。また、監査ログを指定した宛先に転送したり、ONTAP CLIまたはWebブラウザを使用して監査ログファイルを表示したりすることもできます。

ONTAP 9.11.1以降では、System Managerを使用して監査ログの内容を表示できます。

ONTAP 9.12.1以降には、監査ログの改ざんアラートが用意されています。audit.logファイルの改ざんをチェックするためのバックグラウンド ジョブが毎日実行され、変更または改ざんされたログ ファイルが見つかるとEMSアラートが送信されます。

ONTAP 9.17.1以降、およびONTAP 9.16.1 P4以降の9.16.1パッチリリースでは、"ピアクラスタから開始されたクラスタ間操作によるリモート管理アクティビティも記録できます。"。これらのアクティビティには、別のクラスタから発生するユーザ主導の操作と内部操作が含まれます。

ONTAPに記録される管理アクティビティ

ONTAPは、発行された要求、要求をトリガーしたユーザー、ユーザーのアクセス方法、要求の時刻など、クラスターで実行された管理アクティビティをログに記録します。

管理アクティビティは次のいずれかのタイプになります：

- **SET**リクエスト：
  - これらの要求は通常、非表示のコマンドまたは操作に適用されます。
  - これらの要求は、たとえば `create`、 `modify`、または `delete`コマンドを実行したときに発行されます。
  - SETリクエストはデフォルトでログに記録されます。
- **GET**リクエスト：
  - これらのリクエストは情報を取得し、管理インターフェイスに表示します。
  - これらの要求は、たとえば `show`コマンドを実行するときに発行されます。
  - GETリクエストはデフォルトではログに記録されませんが、ONTAP CLIから送信されたGETリクエスト(`-cliget`、ONTAP APIから送信されたGETリクエスト(`-ontapiget`、またはONTAP REST APIから送信されたGETリクエスト(`-httpget`をファイルに記録するかどうかを制御できます。

監査ログの記録とローテーション

ONTAPは、ノードの `/mroot/etc/log/mlog/audit.log`ファイルに管理アクティビティを記録します。CLIコマンド用の3つのシェル（clustershell、nodeshell、非対話型systemshell）からのコマンドとAPIコマンドがここに記録されます。対話型systemshellコマンドは記録されません。監査ログにはタイムスタンプが含まれ、クラスタ内のすべてのノードが同期されているかどうかを示します。

`audit.log`ファイルはAutoSupportツールによって指定された受信者に送信されます。また、Splunkやsyslogサーバーなど、指定した外部の宛先にコンテンツを安全に転送することもできます。

`audit.log`ファイルは毎日ローテーションされます。サイズが100MBに達した時点でもローテーションが実行され、以前の48個のコピーが保持されます（最大49個のファイル）。監査ファイルが毎日ローテーションを実行する場合、EMSメッセージは生成されません。監査ファイルがファイルサイズ制限を超えたためにローテーションされた場合は、EMSメッセージが生成されます。

GET監査を有効にする際は、急速なログローテーションによるデータ損失を防ぐため、ログ転送の設定を検討してください。詳細については、以下のナレッジベースの記事をご覧ください：https://kb.netapp.com/on-prem/ontap/Ontap_OS/OS-KBs/Enabling_audit-log_forwarding["監査ログ転送を有効にする"^]

ONTAP監査ログの変更について学ぶ

ONTAP 9以降、 `command-history.log`ファイルは `audit.log`に置き換えられ、 `mgwd.log`ファイルには監査情報が含まれなくなりました。ONTAP 9にアップグレードする場合は、レガシーファイルとその内容を参照するスクリプトやツールを確認してください。

ONTAP 9へのアップグレード後、既存の `command-history.log`ファイルは保持されます。新しい `audit.log`ファイルがローテーションイン（作成）されると、既存のファイルはローテーションアウト（削除）されます。

`command-history.log`ファイルをチェックするツールやスクリプトは、アップグレード時に `command-history.log`から `audit.log`へのソフトリンクが作成されるため、引き続き動作する可能性があります。ただし、 `mgwd.log`ファイルをチェックするツールやスクリプトは、そのファイルには監査情報が含まれなくなるため、動作しなくなります。

また、ONTAP 9以降の監査ログでは、以下のエントリは有用な情報とは見なされず、余計なログ アクティビティ発生の原因とされるため、記録されなくなりました。

- ONTAPによって実行される内部コマンド（username=rootのコマンド）
- コマンドのエイリアス（元のコマンドとは別に）

ONTAP 9以降では、TCPおよびTLSプロトコルを使用して監査ログを外部の宛先に安全に送信できます。

ONTAP監査ログの内容を表示する

ONTAP CLI、System Manager、または Web ブラウザを使用して、クラスタの `/mroot/etc/log/mlog/audit.log`ファイルの内容を表示できます。

クラスタのログ ファイルには、次のエントリが含まれます。

Time

ログ エントリのタイムスタンプ。

Application

クラスターへの接続に使用されるアプリケーション。可能な値の例としては `internal`、 `console`、 `ssh`、 `http`、 `ontapi`、 `snmp`、 `rsh`、 `telnet`、および `service-processor`などがあります。

ユーザ

リモート ユーザーのユーザー名。

状態

監査リクエストの現在の状態。 `success`、 `pending`、または `error`のいずれかになります。

メッセージ

コマンドのステータスに関するエラーまたは追加情報が含まれる可能性があるオプションのフィールド。

セッション**ID**

リクエストを受信したSession ID。各SSH セッション にはSession IDが割り当てられ、各HTTP、ONTAPI、またはSNMP リクエスト には一意のSession IDが割り当てられます。

Storage VM

ユーザーが接続した SVM。

Scope

要求がデータ ストレージ VM 上にある場合は `svm`が表示され、それ以外の場合は `cluster`が表示されます。

コマンド**ID**

CLIセッションで受信した各コマンドのID。これにより、リクエストとレスポンスを関連付けることができます。ZAPI、HTTP、およびSNMPリクエストにはコマンドIDはありません。

クラスタのログ エントリは、ONTAP CLIまたはWebブラウザから表示できます。ONTAP 9.11.1以降では、System Managerからも表示できます。

System Manager

- インベントリを表示するには、*イベントとジョブ > 監査ログ*を選択します。+ 各列には、フィルタリング、並べ替え、検索、表示、インベントリカテゴリのコントロールがあります。インベントリの詳細は Excel ワークブックとしてダウンロードできます。
- フィルターを設定するには、右上の*フィルター*ボタンをクリックし、目的のフィールドを選択します。+ Session IDリンクをクリックすると、障害が発生したセッションで実行されたすべてのコマンドを表示することもできます。

CLI

クラスタ内の複数のノードからマージされた監査エントリを表示するには、次のように入力します：+
`security audit log show <[parameters]>`

`security audit log show`コマンドを使用すると、クラスタ内の個々のノードの監査エントリ、または複数のノードからマージされた監査エントリを表示できます。また、Webブラウザを使用して、単一ノード上の `/mroot/etc/log/mlog` ディレクトリの内容を表示することもできます。link:https://docs.netapp.com/us-en/ontap-cli/security-audit-log-show.html["ONTAPコマンド リファレンス"^]の`security audit log show`の詳細をご覧ください。

Webブラウザ

Webブラウザを使用して、単一ノード上の `/mroot/etc/log/mlog`ディレクトリの内容を表示できます。"ウェブブラウザを使用してノードのログ、コアダンプ、MIBファイルにアクセスする方法について学習します"。

ONTAP監査GETリクエスト設定を管理する

SET要求はデフォルトでログに記録されますが、GET要求は記録されません。ただし、ONTAP HTML(`-httpget`、ONTAP CLI(`-cliget`、またはONTAP API(`-ontapiget`から送信されたGET要求をファイルに記録するかどうかを制御できます。

監査ログ設定はONTAP CLIから変更できます。ONTAP 9.11.1以降では、System Managerからも変更できます。

System Manager

1. *Events & Jobs > Audit Logs*を選択します。
2. 右上隅の  をクリックし、追加または削除するリクエストを選択します。

CLI

- デフォルトの設定要求に加えて、ONTAP CLI または API からの GET 要求を監査ログ（audit.log ファイル）に記録するように指定するには、次のように入力します：+ `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- 現在の設定を表示するには、次のように入力します：+ `security audit show`

> `security audit show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-audit-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPクラスタ間監査を有効にする

ONTAP 9.17.1以降、およびONTAP 9.16.1 P4以降の9.16.1パッチリリースでは、ONTAPでクラスタ間監査を有効にして、ピアクラスタから開始された操作をログに記録できます。このリモート監査は、複数のONTAPクラスタが相互に連携する環境で特に有用であり、リモートアクションの追跡可能性とアカウンタビリティを実現します。

クラスタ間監査では、ユーザーが開始したGET（読み取り）操作とSET（作成／変更／削除）操作を区別できます。デフォルトでは、宛先クラスタではユーザーが開始したSET操作のみが監査対象となります。GETや`show`CLIコマンドなど、データを読み取るリクエストは、クラスタ間リクエストであるかどうかにかかわらず、デフォルトでは監査されません。

開始する前に

- `advanced`レベルの権限が必要です
- クラスタは別のクラスタとピアリングする必要があり、両方のクラスタでONTAP 9.16.1 P4以降が実行されている必要があります。

> 一部のノードのみが ONTAP 9.16.1 P4 以降にアップグレードされている環境では、監査ログはアップグレードされたバージョンを実行しているノードでのみ記録されます。監査動作の一貫性を確保するため、すべてのノードをサポート対象バージョンにアップグレードすることをお勧めします。

クラスタ間監査を有効または無効にする

手順

1. `cluster-peer`パラメータを `on`または `off`に設定して、クラスター上のクラスター間監査を有効（または無効）にします：

```
security audit modify -cluster-peer {on|off}
```

2. 現在の監査状態を確認して、クラスタピア設定が有効になっているか無効になっているかを確認します：

```
security audit show
```

応答：

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

GET監査を有効にした場合の影響

ONTAP 9.17.1以降では、ピアクラスタで "CLI、HTTP、ONTAPI GET監査を有効にする"を実行すると、クラスタ間のユーザ開始GET要求の監査も有効になります。以前のONTAPバージョンでは、GET監査はローカルクラスタ上の要求にのみ適用されていました。ONTAP 9.17.1では、 `cluster-peer`オプションを `on`に設定してGET監査を有効にすると、ローカルクラスタとクラスタ間の両方の要求が監査されます。

ONTAP監査ログの保存先を管理する

監査ログは最大で10箇所に転送できます。たとえば、Splunkやsyslogサーバにログを転送し、監視や分析、バックアップなどの目的で使用できます。

タスク概要

転送を設定するには、syslog または Splunk ホストの IP アドレス、ポート番号、転送プロトコル、および転送されるログに使用する syslog 機能を指定する必要があります "syslog機能について学ぶ"。

`-protocol`パラメータを使用して、次のいずれかの送信値を選択できます：

UDP 暗号化なし
: UDP、セキュリティなし（デフォルト）

TCP 暗号化なし
: TCP、セキュリティなし

TCP暗号化
: Transport Layer Security（TLS）を使用したTransmission Control Protocol + TCP暗号化プロトコルを選択した場合は、*サーバーの検証*オプションが利用できます。

デフォルトのポートはUDPの場合は514、TCPの場合は6514ですが、ネットワークのニーズに合わせて任意のポートを指定できます。

`-message-format`コマンドを使用して、次のいずれかのメッセージ形式を選択できます：

legacy-NetApp

RFC-3164 Syslog 形式のバリエーション（形式：<PRIVAL>TIMESTAMP HOSTNAME：MSG）

rfc-5424

RFC-5424 に準拠した syslog 形式（形式：<PRIVAL>VERSION TIMESTAMP HOSTNAME: MSG）

監査ログは、ONTAP CLIから転送できます。ONTAP 9.11.1以降では、System Managerからも転送できます。

System Manager

- 監査ログの送信先を表示するには、*クラスター>設定*を選択します。+ログの送信先の数は*通知管理タイル*に表示されます。 をクリックすると詳細が表示されます。
- 監査ログの送信先を追加、変更、または削除するには、**[イベントとジョブ] > [監査ログ]** を選択し、画面の右上にある **[監査ログの送信先の管理]** をクリックします。+ Add をクリックするか、**[ホスト アドレス]** 列の をクリックして、エントリを編集または削除します。

CLI

1. 監査ログの転送先ごとに、デスティネーションIPアドレスかホスト名、およびいずれかのセキュリティ オプションを指定します。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

   - `cluster log-forwarding create`コマンドが宛先ホストにpingを実行して接続を確認できない場合、コマンドはエラーで失敗します。推奨されませんが、コマンドで `-force`パラメータを使用すると、接続の確認がバイパスされます。
   - `-verify-server`パラメータを `true`に設定すると、ログ転送先の証明書を検証することで、その ID が検証されます。 `-protocol`フィールドで `tcp-encrypted`値を選択した場合にのみ、値を `true`に設定できます。

2. `cluster log-forwarding show`コマンドを使用して、宛先レコードが正しいことを確認します。

```
cluster1::> cluster log-forwarding show

                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

関連情報

- "cluster log-forwarding show"
- "cluster log-forwarding create"

著作権に関する情報

商標に関する情報