監査ロギング
ONTAP 9

NetApp
April 24, 2024

目次

監査ロギング

ONTAP での監査ログの実装方法

監査ログに記録された管理アクティビティは標準の AutoSupport レポートに、特定のログアクティビティは EMS メッセージに含まれています。監査ログを指定の場所に転送したり、 CLI や Web ブラウザを使用して監査ログファイルを表示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以降では、ONTAPで監査ログの改ざんアラートが提供されます。ONTAPは、audit.logファイルの改ざんをチェックするために毎日のバックグラウンドジョブを実行し、変更または改ざんされたログファイルが見つかるとEMSアラートを送信します。

ONTAP では、クラスタで実行された管理アクティビティについて、発行された要求、要求を発行したユーザ、ユーザのアクセス方法、要求が発行された時間などの情報が記録されます。

管理アクティビティには次のタイプがあります。

- set要求。通常は表示以外のコマンドや操作が該当します
  - これらの要求は、を実行したときに発行されます `create`、 `modify`または `delete` たとえば、コマンドです。
  - set 要求はデフォルトで記録されます。
- get要求。情報を取得して管理インターフェイスに表示します
  - これらの要求は、を実行したときに発行されます `show` たとえば、コマンドです。
  - GET要求はデフォルトでは記録されませんが、ONTAP CLIから送信されるGET要求を制御できます (`-cliget`）、ONTAP APIから (`-ontapiget`）、またはREST APIから (`-httpget`）がファイルに記録されます。

ONTAP は、の管理アクティビティを記録します `/mroot/etc/log/mlog/audit.log` ノードのファイル。CLI コマンドの 3 つのシェル（クラスタシェル、ノードシェル、および非対話型システムシェル）からのコマンドに加え、 API コマンドがここに記録されます（対話型システムシェルのコマンドは記録されません）。監査ログには、クラスタ内のすべてのノードの時刻が同期しているかどうかを示すタイムスタンプが含まれています。

。 `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 サーバなど、指定した外部の送信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1日単位でローテーションされます。また、サイズが 100MB に達したときにもローテーションが実行されます。以前の 48 個のコピーは保持されます（最大合計 49 個のファイル）。監査ファイルが 1 日単位のローテーションを実行するときは、 EMS メッセージは生成されません。監査ファイルのサイズが上限を超えたためにローテーションが実行された場合は、 EMS メッセージが生成されます。

ONTAP 9 における監査ログの変更点

ONTAP 9以降では、を参照してください `command-history.log` ファイルはに置き換

えられます `audit.log`および `mgwd.log` ファイルに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、これらの従来のファイルとその中身を参照するスクリプトやツールを見直す必要があります。

ONTAP 9へのアップグレード後、既存 `command-history.log` ファイルは保持されます。これらは新規として回転（削除）されます `audit.log` ファイルはローテーションされます（作成されます）。

をチェックするツールとスクリプト `command-history.log` からのソフトリンクがあるため、ファイルは引き続き機能する場合があります `command-history.log` 終了： `audit.log` は、アップグレード時に作成されます。ただし、をチェックするツールとスクリプト `mgwd.log` ファイルに監査情報が含まれなくなったため、ファイルは失敗します。

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みなされず、原因の不要なログアクティビティでもあるため、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 プロトコルと 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。

監査ログの内容を表示します

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

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。

時間
: ログエントリのタイムスタンプ。

アプリケーション
: クラスタへの接続に使用するアプリケーション。指定可能な値の例はです `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, および `service-processor`。

ユーザ
: リモートユーザのユーザ名。

状態
: 監査要求の現在の状態 `success`, `pending`, または `error`。

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 を含むオプションのフィールド。

セッション**ID**
: 要求を受信したセッションID。各SSH_SESSION_ISにはセッションIDが割り当てられ、各HTTP 、ONTAPI、またはSNMP_REQUESTには一意のセッションIDが割り当てられます。

Storage VM

ユーザの接続に使用するSVM。

適用範囲

表示されます `svm` 要求がデータStorage VM上にある場合。それ以外の場合はと表示されます `cluster`。

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、要求と応答を関連付けることができます。ZAPI、HTTP、SNMPの各要求にはコマンドIDはありません。

クラスタのログエントリは、ONTAP CLIから、Webブラウザから、ONTAP 9.11.1以降のSystem Managerから表示できます。

System Manager の略

- インベントリを表示するには、[* Events & Jobs]>[Audit Logs]を選択します。[+] 各列には、カテゴリのフィルタ、並べ替え、検索、表示、およびインベントリを制御できます。インベントリの詳細は、Excelブックとしてダウンロードできます。
- フィルタを設定するには、右上の*[Filter]*ボタンをクリックし、目的のフィールドを選択します。[+] セッションIDリンクをクリックして、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 の使用

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、+と入力します `security audit log show` *`[parameters]`*

を使用できます `security audit log show` 個 々 のノードの監査エントリを表示するコマンド、またはクラスタ内の複数のノードの監査エントリをマージするコマンド。の内容を表示することもできます `/mroot/etc/log/mlog` Webブラウザを使用して、単一のノード上のディレクトリを作成します。詳細については、のマニュアルページを参照してください。

Web ブラウザ

の内容を表示できます `/mroot/etc/log/mlog` Webブラウザを使用して、単一のノード上のディレクトリを作成します。 "Webブラウザを使用してノードのログファイル、コアダンプファイル、MIBファイルにアクセスする方法について説明します"。

監査**GET**要求の設定を管理します

set要求はデフォルトで記録されますが、get要求は記録されません。ただし、ONTAP HTMLから送信されるGET要求を制御することはできます (`-httpget`）、ONTAP CLI (`-cliget`）、またはONTAP APIからアクセスできます (`-ontapiget`）がファイルに記録されます。

監査ログ設定は、ONTAP CLIから、ONTAP 9.11.1以降の監査ログ設定は、System Managerから変更できます。

System Manager の略

1. [* Events & Jobs]>[Audit Logs]を選択します。
2. をクリックします ⚙ 右上にあるをクリックし、追加または削除する要求を選択します。

CLI の使用

- デフォルトのset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、+と入力します `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- 現在の設定を表示するには、+と入力します `security audit show`

詳細については、マニュアルページを参照してください。

監査ログの送信先を管理します

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。

このタスクについて

転送を設定するには、転送されたログに使用する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、syslog機能を指定する必要があります。 "syslogファシリティについて説明します"。

次のいずれかの送信値を選択できます。

UDP暗号化なし

セキュリティなしのユーザデータグラムプロトコル（デフォルト）

TCP暗号化なし

セキュリティなしのTransmission Control Protocol

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]が選択されている場合は、[VERIFY SERVER]オプションを使用できます。

監査ログは、ONTAP CLIから転送できます。ONTAP 9.11.1以降は、System Managerから転送できます。

System Manager の略

- 監査ログの送信先を表示するには、* Cluster > Settings の順に選択します。**[+]** ログデスティネーションの数は、[通知管理]タイル*に表示されます。をクリックします ⋮ 詳細を表示します。
- 監査ログの送信先を追加、変更、または削除するには、[**Events & Jobs]>[Audit Logs]**を選択し、画面右上の**[*Manage Audit Destinations**]をクリックします。[+] をクリックします + Add またはをクリックします ⋮ エントリを編集または削除するには、* Host Address *列に入力します。

CLI の使用

1. 監査ログの転送先ごとに、デスティネーション IP アドレスまたはホスト名、および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 514 -protocol tcp-encrypted -facility user
```

   - 状況に応じて `cluster log-forwarding create` コマンドが接続を確認するためにデスティネーションホストにpingを実行できない場合、エラーが表示されてコマンドが失敗します。推奨されませんが、を使用してください `-force` パラメータを指定すると、接続の検証が省略されます。
   - を設定した場合 `-verify-server` パラメータの値 `true`では、ログの転送先のIDは、証明書を検証することによって検証されます。この値はに設定できます `true` を選択した場合のみ `tcp-encrypted` の値 `-protocol` フィールド。

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

```
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            514    tcp-encrypted   true   user
2 entries were displayed.
```

詳細については、マニュアルページを参照してください。