システムの監査

次のトピックでは、システム上のアクティビティを監査する方法について説明します。

- システム監査について （1 ページ）
- 監査レコード （1 ページ）
- システム ログ （11 ページ）

システム監査について

システム上のアクティビティを 2 つの方法で監査できます。Firepower システムの一部であるアプライアンスによって、Web インターフェイスとユーザとの対話のそれぞれに対して監査レコードが生成され、システム ステータス メッセージがシステム ログに記録されます。

関連トピック

標準レポートの概要

監査レコード

Firepower Management Center および 7000 および 8000 シリーズ管理対象デバイスは、ユーザ アクティビティに関する読み取り専用の監査情報をログに記録します。監査ログは標準のイベント ビューに表示され、監査ビュー内の任意の項目に基づいて監査ログ メッセージを表示、ソート、およびフィルタリングできます。監査情報を簡単に削除したり、それに関するレポートを作成したりすることができ、ユーザが行った変更に関する詳細なレポートを表示することもできます。

監査ログには最大 100,000 のエントリが保存されます。監査ログ エントリの数が 100,000 を超えると、アプライアンスは最も古いレコードをデータベースからプルーニングして、100,000 エントリまで減らします。

（注） 7000 または 8000 シリーズ デバイスをリブートした直後にすばやく補助 CLI にログインした場合、そこで実行するコマンドは、ローカル Web インターフェイスが使用可能になるまでは監査ログに記録されません。

監査レコードの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

Firepower Management Center または 7000 および 8000 シリーズ デバイスで、監査レコードのテーブルを表示できます。事前定義された監査ワークフローには、イベントを示す単一のテーブル ビューが含まれます。ユーザは検索する情報に応じてテーブル ビューを操作することができます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）]** を使用して監査ログのワークフローにアクセスします。

ステップ 2 イベントが 1 つも表示されない場合は、時間範囲を調整することを考慮してください。詳細については、イベント時間の制約を参照してください。

（注） イベント ビューを時間によって制約している場合は、（グローバルかイベント固有かに関係なく）アプライアンスに設定されている時間枠の外で生成されたイベントが、イベント ビューに表示されます。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

ステップ 3 次の選択肢があります。

- テーブルのカラムの内容について詳しく調べるには、システム ログ （11 ページ）を参照してください。
- 現在のワークフロー ページでイベントをソートしたり、制限したりするには、テーブル ビュー ページの使用を参照してください。
- 現在のワークフロー ページ内で移動するには、時間枠の進行を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。詳細については、ワークフローの使用を参照してください。

- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用を参照してください。
- 特定の値で制約するには、行内の値をクリックします。ドリルダウン ページで値をクリックすると、次のページに移動し、その値だけに制約されます。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。詳細については、イベント ビューの制約を参照してください。

  ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。

- 監査レコードを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除します。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマークを参照してください。
- ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマークを参照してください。
- 現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成を参照してください。
- 監査ログに記録された変更の概要を表示するには、[メッセージ（Message）] カラムの該当するイベントの横にある比較アイコン（）をクリックします。詳細については、監査ログを使って変更を調査する （5 ページ）を参照してください。

関連トピック

イベント ビューの制約

監査ログのワークフロー フィールド

次の表で、表示および検索できる監査ログ フィールドについて説明します。

表 *1*: 監査ログのフィールド

フィールド	説明
時刻（Time）	アプライアンスが監査レコードを生成した日時。
ユーザ（User）	監査イベントをトリガーしたユーザのユーザ名。

フィールド	説明
サブシステム	監査レコードが生成されたときにユーザがたどったフル メニュー パス。たとえば、**[システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）]** は、監査ログを表示するためのメニュー パスです。 メニュー パスが該当しない数少ないケースでは、[サブシステム（Subsystem）] フィールドにイベント タイプのみが表示されます。たとえば、**Login** はユーザのログイン試行を分類します。
メッセージ（Message）	ユーザが実行したアクション、またはユーザがページでクリックしたボタン。 たとえば、`Page View` は、[サブシステム（Subsystem）] に示されているページをユーザが単に表示したことを意味します。`Save` は、ユーザがページの [保存（Save）] ボタンをクリックしたことを意味します。 Firepower システムに対する変更は比較アイコン（）付きで表示され、アイコンをクリックすると変更の概要を確認することができます。
ソース IP	ユーザが使用したホストに関連付けられている IP アドレス。 注：このフィールドを検索する場合は、特定の IP アドレスを入力する必要があります。監査ログの検索で IP 範囲を使用することはできません。
ドメイン（Domain）	監査イベントがトリガーされたときのユーザの現行ドメイン。このフィールドは、マルチテナンシーのために Firepower Management Center を設定したことがある場合に表示されます。
設定の変更（Configuration Change） （検索専用）	設定の変更の監査レコードを検索結果に表示するかどうかを指定します。(`yes` または `no`)

フィールド	説明
メンバー数（Count）	各行に表示された情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索

[監査イベント（Audit Events）] テーブル ビュー

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。カラムを無効にする場合は、非表示にするカラム見出しの [閉じる（Close）] アイコン（✖）をクリックした後、表示されるポップアップ ウィンドウで [適用（Apply）] をクリックします。カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されることに注意してください。

他のカラムを表示/非表示にしたり、無効になったカラムをビューに再び追加したりするには、該当するチェックボックスを選択またはクリアしてから [適用（Apply）] をクリックします。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（ワークフロー内の次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「テーブル ビュー（Table View）」が含まれます。

関連トピック

ワークフローの使用

監査ログを使って変更を調査する

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

監査ログを使用して、システムの変更に関する詳細レポートを表示できます。これらのレポートは、現在のシステム設定を、特定の変更が行われる直前の設定と比較します。

[設定の比較（Compare Configurations）] ページには、変更前のシステム設定と、現在実行中の設定との違いが横並び形式で表示されます。監査イベント タイプ、最終変更時間、および変更を行ったユーザ名が、各設定の上のタイトル バーに表示されます。

2 つの設定の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が2つの設定間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- 緑は、強調表示されている設定項目が一方の設定に含まれ、もう一方の設定には含まれないことを示します。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[システム（System）] > [モニタリング（Monitoring）] > [監査（Audit）]**を選択します。

ステップ 2 [メッセージ（Message）] カラムの該当する監査ログ イベントの横にある比較アイコン（）をクリックします。

ヒント タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックすると、個々の変更の間を移動できます。また、変更の概要が複数のページにまたがる場合は、右側のスクロール バーを使って追加の変更を表示できます。

監査レコードの抑制

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

監査ポリシーで、Firepower System/ユーザ間の特定のタイプのインタラクションを監査する必要がない場合は、それらのインタラクションによって、Firepower Management Center または 7000 および 8000 シリーズ デバイス上で監査レコードが生成されないように設定できます。たとえば、デフォルトでは、ユーザがオンライン ヘルプを表示するたびに、Firepower System は監査レコードを生成します。このようなインタラクションのレコードを保持する必要がない場合は、これらを自動的に抑制できます。

監査イベントの抑制を設定するには、アプライアンスの`admin`ユーザアカウントにアクセスできる必要があり、アプライアンスのコンソールにアクセスできる（またはセキュア シェルを開くことができる）必要があります。

⚠

注意 許可された担当者だけが、アプライアンスとその`admin`アカウントにアクセスできることを確認してください。

手順

`/etc/sf` ディレクトリに、次の形式で 1 つ以上の `AuditBlock` ファイルを作成します。タイプは、監査ブロック タイプ （7 ページ）で説明されているいずれかのタイプになります。

`AuditBlock.type`

（注） 特定のタイプの監査メッセージに関する `AuditBlock.type` ファイルを作成した後、もはやそれらを抑制しないことを決定した場合、`AuditBlock.type` ファイルの内容を削除する必要がありますが、ファイル自体は Firepower System に残してください。

監査ブロック タイプ

それぞれの監査ブロック タイプの内容は、以下の表に記載されているように、特定の形式でなければなりません。ファイル名の大文字/小文字が正しいことを確認します。また、ファイルの内容でも大文字と小文字が区別されることに注意してください。

`AuditBlock` ファイルを追加した場合、サブシステム `Audit` およびメッセージ `Audit Filter`*type*`Changed` を含む監査レコードが監査イベントに追加されることに注意してください。セキュリティ上の理由から、この監査レコードを抑制することは**できません**。

表 *2:* 監査ブロック タイプ

タイプ（Type）	説明
アドレス（Address）	`AuditBlock.address` という名前のファイルを作成し、監査ログから抑制する IP アドレスを 1 行に 1 つずつ含めます。アドレスの先頭からマッピングされる場合に限り、部分的な IP アドレスを使用できます。たとえば、部分的なアドレス `10.1.1` は、`10.1.1.0` から `10.1.1.255` までのアドレスと一致します。
メッセージ	`AuditBlock.message` という名前のファイルを作成し、抑制するメッセージ部分文字列を 1 行に 1 つずつ含めます。 たとえば `backup` をこのファイルに含めた場合、部分文字列の照合により `backup` という語を含むすべてのメッセージが抑制されることに注意してください。

タイプ（Type）	説明
サブシステム	`AuditBlock.subsystem` という名前のファイルを作成し、抑制するサブシステムを 1 行に 1 つずつ含めます。 部分文字列は照合**されない**ことに注意してください。正確な文字列を使用する必要があります。監査対象のサブシステムのリストについては、監査対象のサブシステム （8 ページ） を参照してください。
ユーザ（User）	`AuditBlock.user` という名前のファイルを作成し、抑制するユーザ アカウントを 1 行に 1 つずつ含めます。ユーザ名の先頭からマッピングされる場合に限り、部分的な文字列の照合を使用できます。たとえば、部分的なユーザ名 `IPSAnalyst` はユーザ名 `IPSAnalyst1` および `IPSAnalyst2` と一致します。

監査対象のサブシステム

次の表に、監査対象のサブシステムを示します。

表 *3:* サブシステム名

[名前（Name）]	含まれるユーザ インタラクション
管理	管理機能：システムとアクセス権の設定、時刻の同期、バックアップと復元、デバイス管理、ユーザ アカウントの管理、スケジュール設定など
アラート（Alerting）	アラート機能：電子メール、SNMP、syslog アラートなど
監査ログ（Audit Log）	監査イベントの表示
監査ログ検索（Audit Log Search）	監査イベントの検索
コマンド ライン	コマンドライン インターフェイス
設定（Configuration）	電子メール アラート機能
COOP	継続的な運用機能
日付（Date）	イベント ビューの日時範囲

[名前（Name）]	含まれるユーザ インタラクション
デフォルトのサブシステム（Default Subsystem）	サブシステムが割り当てられていないオプション
検出および防御ポリシー（Detection & Prevention Policy）	侵入ポリシーのメニュー オプション
エラー（Error）	システム レベルのエラー
eStreamer	eStreamer 構成
EULA	エンド ユーザ ライセンス契約書の確認
イベント	侵入およびディスカバリ イベント ビュー
イベント クリップボード（Events Clipboard）	侵入イベント クリップボード
レビューされたイベント（Events Reviewed）	レビューされた侵入イベント
イベント検索（Events Search）	すべてのイベント検索
ルール更新のインストールの失敗（Failed to install rule update）`rule_update_id`	ルール更新のインストール
ヘッダー	ユーザ ログイン後のユーザ インターフェイスの最初の表示
状態	ヘルス モニタリング
ヘルス イベント（Health Events）	ヘルス モニタリング イベントの表示
ヘルプ	オンライン ヘルプ
高可用性	高可用性ペアでの Firepower Management Center の確立と管理
IDS インパクト フラグ（IDS Impact Flag）	インパクト フラグの設定
IDS ポリシー（IDS Policy）	侵入ポリシー
IDS ルール SID：`sig_id` リビジョン：`rev_num`	SID による侵入ルール
[インシデント（Incidents）]	侵入インシデント
インストール（Install）	更新のインストール
侵入イベント	侵入イベント
ログイン（Login）	Web インターフェイスのログイン/ログアウト機能

[名前（Name）]	含まれるユーザ インタラクション
ログアウト	Web インターフェイス ログアウト機能
メニュー	すべてのメニュー オプション
[設定のエクスポート（Configuration export）] > [config_type] > [config_name]	特定のタイプ/名前の設定のインポート
権限エスカレーション（Permission Escalation）	ユーザ ロールのエスカレーション
初期設定	ユーザ アカウントのタイム ゾーンや個々のイベント設定などのユーザ設定
ポリシー	侵入ポリシーを含むすべてのポリシー
登録	Management Center でのデバイスの登録
RemoteStorageDevice	リモート ストレージ デバイスの設定
レポート	レポート リスト機能およびレポート デザイナ機能
ルール（Rules）	侵入ルール（侵入ルール エディタとルールのインポート プロセスを含む）
ルール更新のインポート ログ（Rule Update Import Log）	ルール更新のインポート ログの表示
ルール更新のインストール（Rule Update Install）	ルール更新のインストール
セッションの時間切れ	Web インターフェイスのセッション タイムアウト
ステータス（Status）	syslog およびホストやパフォーマンスの統計情報
システム（System）	システム全体のさまざまな設定
タスク キュー（Task Queue）	バックグラウンド プロセス ステータスの表示
Users	ユーザ アカウントとロールの作成および変更

システム ログ

[システム ログ（System Log）]（syslog）ページには、アプライアンスのシステム ログ情報が表示されます。システム ログには、システムによって生成された各メッセージが表示されます。次の項目が順にリストされます。

- メッセージが生成された日付
- メッセージが生成された時刻
- メッセージを生成したホスト
- メッセージ自体

システム ログの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Maint

システム ログ情報はローカルな情報です。たとえば、Firepower Management Center を使用して、管理対象デバイスのシステム ログ内のシステム ステータス メッセージを見ることは**できません**。

Firepower Management Center または 7000 & 8000 シリーズ デバイスでは、特定のコンポーネントでフィルタリングすることによって、システム ログ メッセージのビューを変更できます。

手順

ステップ 1 **[システム（System）] > [モニタリング（Monitoring）] > [Syslog]**を選択します。

ステップ 2 システム ログの特定のメッセージ内容を検索する場合は、システム ログ メッセージのフィルタリング （11 ページ）を参照してください。

システム ログ メッセージのフィルタリング

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin/Maint

Firepower Management Center または 7000 および 8000 シリーズ のデバイスで、特定のコンポーネントをフィルタリングして、システム ログ メッセージの表示を変更することができます。

フィルタリングにより、メッセージ内容に基づいて特定のメッセージを検索することができます。

フィルタリング機能は、UNIX ファイル検索ユーティリティ Grep を使用しているため、Grep で使用可能なほとんどの構文を使用できます。つまり、パターン マッチング用に Grep 互換の正規表現を使用できます。単一の語をフィルタとして使用したり、Grep でサポートされる正規表現を使用したりして内容を検索できます。

手順

ステップ 1 **[システム（System）] > [モニタリング（Monitoring）] > [Syslog]**を選択します。

ステップ 2 システム ログ フィルタの構文 （12 ページ）に記載されているように、フィルタのフィールドに単語またはクエリを入力します。

（注） Grep 互換の検索構文のみがサポートされています。たとえば、フィルタとして `ntp` を使ってすべての NTP 関連システム ログ メッセージを検索したり、`Nov` をフィルタとして使って 11 月に生成されたすべてのメッセージを検索したりできます。`Nov[[:space:]]*27` または `Nov.*27` を使用すると 11 月 27 日のメッセージを表示できますが、`Nov 27` または `Nov*27` を使ってこれらのメッセージを表示することはできません。

ステップ 3 大文字と小文字が区別されるようにするには、[大文字と小文字を区別する（Case-sensitive）] をチェックします。（デフォルトでは、フィルタで大文字/小文字は区別されません。）

ステップ 4 オプションで、[除外（Exclusion）] をチェックすると、入力した条件に一致しないすべてのシステム ログ メッセージが検索されます。

ステップ 5 [移動（Go）] をクリックします。

例

11 月 5 日に生成されたすべてのログ エントリを検索するには、`Nov[[:space:]]*5` を使用します。

ユーザ名 ”Admin” を含むすべてのログ エントリを検索するには `Admin` を使用します。

11 月 5 日のデバッグ情報の認証を含むすべてのログ エントリを検索するには、`Nov[[:space:]]*5.*AUTH.*DEBUG` を使用します。

システム ログ フィルタの構文

次の表に、システム ログ フィルタで使用できる正規表現構文を示します。

表 *4:* システム ログ フィルタ構文

構文のコンポーネント	説明	例
.	任意の文字またはスペースと一致します	Admi. は、Admin、AdmiN、Admi1、および Admi& と一致します。
[[:alpha:]]	任意の英文字 1 字と一致します	[[:alpha:]]dmin は、Admin、bdmin、および Cdmin と一致します
[[:upper:]]	任意の大文字の英文字 1 字と一致します	[[:upper:]]dmin は、Admin、Bdmin、および Cdmin と一致します
[[:lower:]]	任意の小文字の英文字 1 字と一致します	[[:lower:]]dmin は、admin、bdmin、および cdmin と一致します
[[:digit:]]	任意の数字 1 字と一致します	[[:digit:]]dmin は、0dmin、1dmin、および 2dmin と一致します
[[:alnum:]]	任意の英数字 1 字と一致します	[[:alnum:]]dmin は、1dmin、admin、2dmin、および bdmin と一致します
[[:space:]]	タブを含む、任意のスペース 1 字と一致します	Feb[[:space:]]29 は 2 月 29 日のログと一致します
*	その前にある文字または表現のゼロ個以上のインスタンスと一致します	ab* は、a、ab、abb、ca、cab、および cabb と一致します [ab]* はすべてのものと一致します
?	ゼロ個または 1 個のインスタンスと一致します	ab? は、a または ab と一致します
\	これを使用すると、通常は正規表現構文と解釈される文字を検索できます	alert\? は、alert? と一致します