監査と Syslog

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 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。

システム上のアクティビティを2つの方法で監査できます。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ー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。

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

システム ログ情報はローカルな情報です。たとえば、Firewall 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**。

UNIX ファイル検索ユーティリティ Grep で処理可能なほとんどの構文を使用してメッセージをフィルタ処理できます。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。

始める前に

システム統計を表示するには、管理者またはメンテナンスユーザーであり、グローバルドメインにいる必要があります。

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 ログ内で特定のメッセージ内容を検索するには、次のようにします。

a) システム ログ フィルタの構文 （2 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。

Grep 互換の検索構文のみがサポートされています。

例：

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 27 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 27` や `Nov*27` ではなく）`Nov[[:space:]]*27` または `Nov.*27` 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。

b) 検索で大文字と小文字を区別するには、[大文字と小文字を区別する（Case-sensitive）] を選択します。（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。）

c) 入力した基準を満たしていないすべてのシステム ログ メッセージを検索するには、[除外（Exclusion）] を選択します。

d) [移動（Go）] をクリックします。

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 *1:* 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、および一致します。
`[[:alpha:]]`	任意の英文字と一致します	`[[:alpha:]]dmin` は、Admin、bdmin、お と一致します
`[[:upper:]]`	任意の大文字の英文字と一致します	`[[:upper:]]dmin` は、Admin、Bdmin、お と一致します

構文のコンポーネント	説明	例
`[[:lower:]]`	任意の小文字の英文字と一致します	`[[:lower:]]dmin` は、admin、bdmin、と一致します
`[[:digit:]]`	任意の数字と一致します	`[[:digit:]]dmin` は、0dmin、1dmin、と一致します
`[[:alnum:]]`	任意の英数字と一致します	`[[:alnum:]]dmin` は、1dmin、admin、bdmin と一致します
`[[:space:]]`	タブを含む、任意のスペースと一致します	`Feb[[:space:]]29` は 2 月 29 日のロ
`*`。	その前にある文字または式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 します `[ab]*` はすべてのものと一致します
`?`	ゼロ個または 1 つ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

システム監査について

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ーとの対話のそれぞれに対して監査レコードが生成されます。

関連トピック

標準レポートの概要

監査レコード

Secure Firewall Management Center 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 エントリまで数を削減します。

監査ログには、ログインエラーのユーザーまたは送信元 IP は表示されません。

- 誤ったパスワードを使用すると、送信元 IP は表示されません。

- ユーザーアカウントが存在しない場合、送信元 IP とユーザーの両方が表示されません。
- LDAP ユーザーの試行が失敗した場合、監査ログはトリガーされません。

関連トピック

Firewall Management Center の SSO ガイドライン

監査レコードの表示

Firewall Management Center 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。ユーザー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。

始める前に

この手順を実行するには、管理者ユーザーである必要があります。

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に特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベントビューに表示されることがあります。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。

これらの選択肢は、検索制約の結果に基づいてのみ適用されます。たとえば、**正常性イベント**を検索すると、結果のビューページに [ワークフロー（Workflow）] オプションが表示されます。同様に、[脆弱性（Vulnerabilities）] テーブルビューを使用している場合にのみ、特定の脆弱性を表示するオプション（[表示（View）]（👁））が表示されます。

- 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 （1 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（Reporting）] 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システム変更の概要を表示するには、[メッセージ（Message）] 列の該当するイベントの横にある [比較（Compare）] 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 （7 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 *2*: 監査ログのフィールド

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

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ーが単に表示したことを意味します。`Save` は、ユーザーがページの [保存（Save）] ボタンをクリックしたことを意味します。 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ーの現行ドメイン。 このフィールドは、マルチテナンシーのために Firewall 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`)
メンバー数（Count）	各行に表示される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）]（✕）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「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

監査ログを使用して、一部の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、サポートされている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ー名が、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。

始める前に

この手順を実行するには、管理者ユーザーである必要があります。

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）] 列の該当する監査ログイベントの横にある [比較（Compare）] 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

監査ポリシーで、Firepower System/ユーザー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、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、ユーザー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` ユーザー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。

始める前に

この手順を実行するには、管理者ユーザーである必要があります。

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 （8 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で、それらの抑制を解除することにした場合、`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 FiltertypeChanged 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 *3*:監査ブロック タイプ

タイプ	説明
アドレス	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。
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 （9 ページ）を参照してください。
ユーザー	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。ユーザー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、部分的なユーザー名 IPSAnalyst はユーザー名 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 *4*:サブシステム名

名前	どの機能のユーザー インタラクションを含んでいるか
Admin	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、ユーザーアカウントの管理、スケジュール設定など
Alerting	アラート機能（電子メール アラート、SNMP アラート、Syslog アラートなど）
監査ログ（Audit Log）	監査イベントの表示
Audit Log Search	監査イベントの検索

名前	どの機能のユーザー インタラクションを含んでいるか
コマンド ライン	コマンドライン インターフェイス
Configuration	電子メール アラート機能
コンテキスト クロス起動	システムに追加された外部リソース、またはダッシュボードとイベント ビューからアクセスされた外部リソース
COOP	継続的な運用機能
Date	イベント ビューの日時範囲
Default Subsystem	サブシステムが割り当てられていないオプション
Detection & Prevention Policy	侵入ポリシーのメニュー オプション
Error	システム レベルのエラー
eStreamer	eStreamer 構成
EULA	エンド ユーザー ライセンス契約書の確認
Event	侵入およびディスカバリ イベント ビュー
Events Reviewed	レビューされた侵入イベント
Events Search	あらゆるイベント検索
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	ユーザー ログイン後のユーザー インターフェイスの最初の表示
Health	ヘルス モニタリング
Health Events	ヘルス モニタリング イベントの表示
Help	オンライン ヘルプ
高可用性	高可用性ペアでの Firewall Management Center の確立と処理
IDS インパクト フラグ（IDS Impact Flag）	侵入イベントの影響フラグの設定
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 別の侵入ルール
インストール（Install）	更新のインストール

名前	どの機能のユーザー インタラクションを含んでいるか
Intrusion Events	侵入イベント
Login	Web インターフェイスのログイン/ログアウト機能
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	あらゆるメニュー 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
Permission Escalation	ユーザー ロールのエスカレーション
Preferences	ユーザー 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ー設定
Policy	侵入ポリシーを含むポリシー
Register	Firewall Management Center でのデバイスの登録
リモート ストレージ デバイス（RemoteStorageDevice）	リモート ストレージ デバイスの設定
Reports	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
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
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	ユーザー アカウントとロールの作成および変更

外部ロケーションへの監査ログの送信について

Firewall Management Center から監査ログを外部の場所に送信する場合は、以下を参照してください。

- 監査ログ
- 監査ログ証明書

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。