CHAPTER 14

システム ステータスの監視

この章では、システムの状態とアクティビティの監視方法について説明します。内容は次のとおりです。

ログに記録される情報について

ACE Web Application Firewall と Manager には、システム アクティビティを監視するための豊富な機能が含まれます。このような機能としては、ダイナミック トラフィック統計情報のカスタマイズ可能なビューを提供する Manager Dashboard、Performance Monitor、広範なエラー ロギング、Manager でポリシーの変更を示す監査ログ、インシデント レポートなどがあります。

（注） この章では、Manager Web コンソールで利用可能な監視ツールについて説明します。SNMP や Syslog などの、システムを監視する外部ツールについては、『*Cisco ACE Web Application Firewall Administration Guide*』を参照してください。

ログは、ネットワークに侵入する潜在的に悪意のあるトラフィックに関する情報を提供することによりシステムのセキュリティを強化します。ログは、インジェクション攻撃やコマンド インジェクション攻撃に合致するよう設計されたシグニチャを含むさまざまな攻撃シグニチャに合致する要求を識別します。また、ログを使用することにより、サーバ処理エラーがログに取り込まれて報告されるため、バックエンド インフラストラクチャでの問題を特定することもできます。パフォーマンス報告ツールを使用すると、システムを調整してパフォーマンスを最大化できます。

Manager Dashboard は、ログに提供された情報の概要を示します。ログイン成功後に最初に表示されるページで、注意が必要な状況（考えられる攻撃など）について警告します。このページは、ユーザの興味を引くグラフを表示するようカスタマイズできます。サービス定義別にトランザクション レート、エラー数、および遅延を示すグラフを利用できます。

ACE Web Application Firewall システムのログの種類は次のとおりです。

- *イベント ログ*は、ACE Web Application Firewall および Manager の処理アクティビティと管理アクティビティに影響を与えるシステム イベントに関するデータを記録します。イベント ログによって記録されるイベントの例は、メッセージ トランザクション、システムの起動とシャットダウン、Web コンソール ユーザの認証、ポリシーの導入、さまざまなエラー、およびその他のアクティビティです。

- *パフォーマンス ログ*は、パフォーマンス分析を補助するための、システムのトラフィックに関するさまざまな統計情報を保持します。パフォーマンス ログは、トランザクション数、処理時間、バックエンド ラウンドトリップ時間などに関する情報を提供します。この情報は Performance Monitor と、Manager Dashboard の Traffic Monitor セクションに追加できるグラフに表示されます。
- *監査ログ*は、ACE Web Application Firewall Manager Web コンソールでのユーザ アクティビティを示します。

負荷が高いシステムで情報をログに記録する場合は、アプライアンスで大量のディスク容量が使用されることがあります。リソースの枯渇を防ぐために、アプライアンス上のログ ファイルが特定のディスク容量を使用する場合は、空き領域を増やすために古いログ ファイルが自動的に削除されます。この機能の目的は、アプライアンスの予期しないシャットダウンを防ぐことです。ただし、ログファイルを管理されたプロセスを使用して定期的にバックアップ ストレージにコピーして、アプライアンスから削除することをお勧めします。こうして、ログに記録された情報は必要に応じて復元できるようになります。このために、ファイルをアプライアンスから定期的に移動するシェル スクリプトを設定できます。ディスク管理の詳細については、『*Cisco ACE Web Application Firewall Administration Guide*』を参照してください。

イベント ロギング

イベント ログは、ACE Web Application Firewall と Manager のアクティビティに関する詳細な情報を提供します。イベント ログは、トラフィック処理アクティビティと、ACE Web Application Firewall Manager および ACE Web Application Firewall の内部的な操作に関する情報を示します。これらのイベントとしては、管理イベント（ポリシー導入など）、エラー通知、システムの操作に重要なその他のイベントなどがあります。この情報を使用すると、システムのポリシーまたはネットワーク設定で問題を容易に診断できるようになります。

システムは、イベントへの書き込みを複数の詳細レベルで行うことができます。詳細レベルが 1 つ上がるごとに、より多くの情報が記録されます。ロギング レベルは次のとおりです。

表 14-1　　イベント ロギング レベル

レベル	説明
アラート	システム障害を防ぐために早急な対応が必要な危機的なシステム状況。
エラー	正しくない結果や異常なシステム動作をもたらすエラー状況。
警告	異常な状態にあるようにみえる、予期しないシステム動作や他の不適切な結果をもたらす可能性がある状況。
通知	メッセージの受信や送信などの正常だが重要な状況。このレベルの報告では、正常な状況で処理される各メッセージに対して 1 行の出力が生成されます。
情報	メッセージ トラフィックの正常な処理での重要な処理ステージ。このレベルでは、処理された各メッセージが複数の行の出力を生成します。
デバッグ	ACE Web Application Firewall または Manager が報告できるすべての情報。1 つの例として、このレベルでは、ACE Web Application Firewall が処理する各メッセージの本文が記録されます。 メッセージに対して示されたデバッグレベルの情報には、要求で渡されたパスワードなどの機密情報が含まれることがあることに注意してください。一般的に、このレベルのロギングは、テストやトラブルシューティングの場合にだけ使用してください。

負荷が高い ACE Web Application Firewall は大量のイベント ログ レコードを生成することがあることに注意してください。イベント情報は Syslog を経由して Manager に渡されます（Syslog は UDP プロトコルとしてベストエフォート型の送信だけを行います）。負荷が非常に高いシステムの場合やストレステスト シナリオの場合は、イベント ログ情報が失われることがあります。

高い詳細レベル（通知、情報、デバッグ）では、システムが大量の情報を記録するため、ACE Web Application Firewall のパフォーマンスに影響が出ることがあります。これらのロギング レベルは問題を調査するときに有用ですが、実稼動システムで継続的に使用することは避けてください。

イベント ロギングの設定

イベント ログ項目は、ACE Web Application Firewall と Manager の両方によって生成されます。生成されるイベントの種類は次のとおりです。

- ACE Web Application Firewall イベント ログは、主にシステムのメッセージ処理アクティビティに関する情報を提供します。
- ACE Web Application Firewall Manager イベント ログは、システムの管理アクティビティに関する情報を提供します。

一般的に、ACE Web Application Firewall Manager イベント ログはシステム管理者にとって有用であり、ACE Web Application Firewall ログはポリシーのサービス定義を作成およびテストする管理者と開発者の両方にとって有用です。

イベントが記録されるログ レベルは、Firewall と Manager で別々に設定できます。

（注） Manager が複数のクラスタを管理する場合、イベント ログには現在のクラスタの Firewall に対する Firewall イベントだけが示されます。Manager イベントはすべてのクラスタに対して示されます。Manager イベントの場合、ログ説明はイベントにより影響を受けたクラスタをクラスタ名で示します。詳細については、第 16 章「Firewall クラスタの管理」を参照してください。

イベント ロギング レベルを設定するには、次の手順に従います。

ステップ 1　Web コンソールに `Administrator` ユーザまたは `Operations` ロールを持つ `Privileged` ユーザとしてログインします。

ステップ 2　次のいずれかの方法で [System Management] ページを表示します。

- 操作メニューで [System Management] リンクをクリックします。
- [Event Log] ページがすでに表示されている場合は、[Current ... Event Logging] ペインの右側にある編集リンクのいずれかをクリックします。

ACE Web Application Firewall Manager が [System Management] ページを表示します。

ステップ 3　Manager ロギングの場合は [Log all Manager events of type] メニューから、Firewall ロギングの場合は [Log all Manager events of type] メニューから値を選択します。

ステップ 4　メニューの隣にある [Set Log Level] ボタンをクリックして新しい設定を確認します。

新しい設定がすぐに反映されます。

クライアント IP ロギング

[Global Policy Settings] メニュー項目の下に表示される [Client IP] オプションを使用すると、Manager がロギングおよび報告のために HTTP 要求ヘッダーの値をソース クライアント IP として使用するよう指定できます。このオプションは、ACE Web Application Firewall が、クライアントの実際の IP アドレスを HTTP ヘッダー（たとえば、X-Forwarded-For ヘッダー）として送信するよう設定されたロード バランサの背後に導入された場合に役に立ちます。

オプションが有効な場合、イベント ログにはロード バランサの IP アドレス以外に HTTP ヘッダーから抽出された IP アドレスが含まれます。

このオプションを有効にするには、[Global Policy Settings] ページで [edit] をクリックし、[Use specified HTTP header value as the client IP] チェックボックスをオンにします。

クライアント IP に使用される HTTP ヘッダーのデフォルト名は X-Forwarded-For です。ロード バランサが異なる名前のヘッダーにクライアント IP 値を挿入する場合は、HTTP ヘッダーの名前を変更できます。

イベント ログの参照

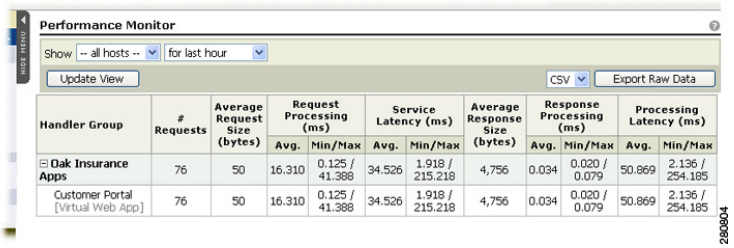
イベント ログを参照するには、操作メニューの [Reports & Tools] セクションにある [Event Log] リンクをクリックします。デフォルトでは、ACE Web Application Firewall Manager は過去 1 時間のイベントを表示します。[Event Log Viewer] の上部にある検索およびフィルタ ツールを使用すると、表示されたログをフィルタ処理できます。たとえば、特定の ACE Web Application Firewall インスタンスに対して生成されたイベントだけを表示することを選択できます。また、ACE Web Application Firewall によってメッセージ トランザクションに割り当てられたメッセージ Globally Unique Identifier（GUID）を使用して検索することもできます。この場合、[Event Log Viewer] には、その ID を持つ要求または応答に関連付けられたイベントだけが表示されます。

パフォーマンス監視

Performance Monitor は、メッセージの数、サイズ、処理時間などの、システムの広範なパフォーマンス情報を提供します。Performance Monitor を使用すると、システムのボトルネックを特定し、ACE Web Application Firewall とバックエンド インフラストラクチャでのパフォーマンスを最適化できます。

情報は、ハンドラ グループおよびエンドポイント別にページに表示されます。各項目に対して、さまざまなパフォーマンス統計情報が表示されます。各統計情報のカテゴリについては、[Performance Monitor] ページからアクセスできるオンライン ヘルプを参照してください。

図 14-1　　パフォーマンス情報



（注）　モニタに表示された一部の統計情報は概算値であることに注意してください。特に、メッセージで特定の種類のエラーが発生した場合、統計情報が期待されたように増加しないことがあります。

パフォーマンス データの時間別処理

Performance Monitor には、時間別にさまざまな方法で情報をフィルタ処理できるコントロールが含まれます。時間フィルタ処理により、コンソール ビューと、ファイルにエクスポートする情報が影響を受けます。統計情報は、次の時間で表示できます。

- 現在時間を終わりとした特定の時間（過去 1 時間や過去 7 日間など）。
- 特定の時間（午前 10 時など）を始まりとし、現在時間を終わりとする時間。
- 過去の特定の時間（ある日付の午前 10 時から午後 8 時など）。

パフォーマンス データを分析するときは、パフォーマンス情報に関する Manager の物理的な容量が無制限ではないことに注意してください。Manager のパフォーマンス データ容量に到達した場合は、古いものからパフォーマンス情報が失われます。容量を節約してこの影響を最小化するために、Manager は時間とともに小さいタイム フレームの情報を大きなタイム フレームに統合します。結果として、実際にはパフォーマンス データが古くなるにつれて解決可能性が低下します。したがって、比較的古い時期の操作から、短い期間の Manager パフォーマンス情報を問い合わせることはできますが、返されたデータは実際には要求されたものよりも長い期間を表している場合があります。この場合は、指定された解決が利用できないことがページ上部の通知に示されます。また、実際の値が、ページ上部の時間フィルタ フィールドに反映されます。

このデータの統合または損失が起こる頻度は、システムのトラフィックの性質によって異なります。パフォーマンス容量の到達に関して最も重要な要因は、Firewall でのトラフィック量よりも独立した仮想サービスの数と特に ID 報告の使用です。

簡単なガイドラインとして、約 100 個の仮想サービスがあり、各仮想サービスは頻繁にトラフィック フローを受け取り（およそ 10 秒ごとに 1 つの要求）、ID トラッキングが無効なポリシーの場合、Manager は 7 ～ 8 か月間でパフォーマンス データの容量に到達すると予想されます。仮想サービスが 10 個だけで、ID トラッキングがないポリシーの場合、Manager は数年間データを失わずにパフォーマンス データを保持できることがあります。

その一方で、データの統合は、数時間後に行われることがあります。10 個の仮想サービスが 10 秒ごとにそれぞれメッセージを受け取る場合、データは約 6 時間 30 分後に 5 分間のタイム フレームに統合されます。8 日後、5 分間のタイム フレームのデータは、単一の 1 時間のタイム フレームに統合されます（このように時間が経過するごとにタイム フレームが長くなります）。

Performance Monitor でデータが利用できない解決の時間の情報を要求した場合、インターフェイスは利用可能な最も近い時間範囲を提示し、ページの上部にその時間範囲が示されます。

過去のパフォーマンス情報の保持が重要な場合は、定期的にパフォーマンス データをファイルにエクスポートしてください。Manager は、CSV 形式と XML 形式でのパフォーマンス データのエクスポートをサポートします。

Manager がパフォーマンス情報を 1 日間に相当するレコードに統合する場合は、GMT で決められた日付境界に従って処理されます。

パフォーマンス情報の参照

パフォーマンス情報を参照にするには、次の手順に従います。

ステップ 1　Web コンソールに `Administrator` ユーザ、`Privileged` ユーザ、または `Policy View` ユーザとしてログインします。

ステップ 2　操作メニューの [Reports & Tools] セクションにある [Performance Monitor] リンクをクリックします。

[Performance Monitor] ページで、ハンドラ グループ別にソートされたポリシーのサービス定義に関するパフォーマンス統計情報が一覧表示されます。デフォルトでは、このページには、ポリシーのすべての仮想サービスに関する統計情報が表示されます。

ハンドラ グループの行には、そのグループのすべての仮想サービスに関する統計情報が表示されます。グループ名の下に、各サービス別の統計情報が詳細に表示されます。

（注）　複数処理の仮想サービスの場合、統計情報は仮想サービスの各処理に対してではなく、仮想サービス全体に対してだけ利用できます。

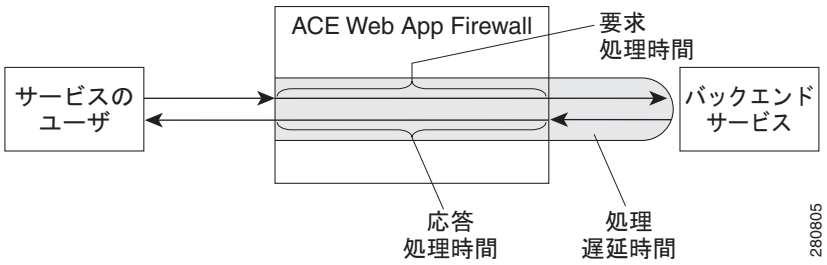
ページの上部にあるコントロールを使用すると、さまざまな方法（Firewall 別または時間別）で表示する情報をフィルタ処理できます。

これらの統計情報については注意すべきいくつかの点があります。

- [Request Processing] 時間と [Response Processing] 時間は、ACE Web Application Firewall が検証、ユーザ認証、変換、およびメッセージに関するポリシーにより指定されたその他のすべての処理を実行するのにかかる時間を表します。
- [Service Latency] カラムは、ACE Web Application Firewall がバックエンド サーバに要求を送信してから応答を受信するまでにかかる時間を示します。これには、ACE Web Application Firewall がメッセージの処理に費やす時間は含まれません。
- メッセージ処理（要求処理、応答処理、およびサービス ラウンド トリップを含む）にかかる時間の合計は [Processing Latency] カラムに示されます。

これらのカテゴリは図 14-2 に示されています。

図 14-2　パフォーマンス統計情報のカテゴリ



Performance Monitor に示された時間は、Time-To-First-Byte に基づいています。つまり、タイマーは、メッセージの最初のバイトを Firewall が受信したときに開始し、最初のバイトが Firewall からネットワークに送信されたときに終了します。したがって、これらの値はネットワークの状況によって影響されることがあります（特に、メッセージが複数のパケットから構成される場合）。

各パフォーマンス カテゴリについては、[Performance Monitor] ページのオンライン ヘルプを参照してください。

ファイルへのパフォーマンス情報のエクスポート

負荷が高い ACE Web Application Firewall システムの ACE Web Application Firewall Manager に保持されたパフォーマンス データは結果的に失われます。パフォーマンス データの量が Manager の容量に達すると、新しい情報を格納する領域を作成するために最も古い情報が削除されます。情報を永久的に保持する必要がある場合は、パフォーマンス情報をファイルにエクスポートできます。

パフォーマンス データを永久的に保存するメカニズムを提供する以外に、パフォーマンス データ エクスポート機能ではメッセージ処理時間に関する統計情報カテゴリが追加され、Performance Monitor インターフェイスで提供される情報よりもさらに豊富な情報にアクセスできます。

パフォーマンス データは XML データまたは Comma-Separated Value（CSV）形式のファイルとしてエクスポートできます。Performance Monitor の場合と同様に、エクスポートされたファイルの統計情報はハンドラ別に分けられます。

（注） Performance Monitor を参照する場合は、サブポリシー間を移動したハンドラが、ハンドラ名ではなく、移動元のサブポリシーのアクティビティに対する内部オブジェクト番号によって識別されます。

エクスポートされたファイルの情報は Performance Monitor の場合とは異なって示されることに注意してください。エクスポートされたパフォーマンス情報は、人が読むことができるよう処理または整理されていないため、ロー データと見なされます。

エクスポートされたデータと Performance Monitor との間には次の違いがあることに注意してください。

- 選択されたタイム フレームでトラフィックを受け取った仮想サービスはファイルに一覧表示されます。要求を受け取らなかった仮想サービスは生成されたファイルに表示されません。
- Prformance Monitor は、各ハンドラ グループに対するメッセージ処理の合計値を示します。エクスポートされたファイルは同じように合計値を示しませんが、代わりに各仮想サービスのレコードを含みます。ID 報告が有効な場合、ファイルには、サービスにアクセスした各 ID のレコードがその ID の要求数とともに含まれます。
- エクスポートされたデータ ファイルには、エラーのために処理されなかった要求のレコードが含まれます。これらは、1 よりも大きい値が指定されたエラー数フィールドによって示されます。
- Performance Monitor に示された Time-To-First-Byte 測定以外に、エクスポートされたファイルは各要求と応答の Time-To-Last-Byte 測定を示します。

パフォーマンス データを XML または CSV ファイルにエクスポートするには、次の手順に従います。

ステップ 1　Web コンソールに `Administrator` ユーザ、`Privileged` ユーザ、または `Policy View` ユーザとしてログインした状態で、操作メニューの [Reports & Tools] セクションにある [Performance Monitor] リンクをクリックします。

ステップ 2　Firewall と時間コントロールを使用して、エクスポートされたファイルにエクスポートする情報をフィルタ処理します。

Performance Monitor のビューに影響を与える以外に、フィルタ コントロール（タイム スパンなど）はファイルにエクスポートする情報を制御します。

ステップ 3　[Update View] をクリックします。

ステップ 4　次のいずれかの出力ファイル形式を選択します。

- XML（XML 形式ファイル）
- CSV（カンマ区切りのファイル）

この選択はファイル形式だけに関係し、生成される情報は影響を受けません。

ステップ 5　[Export Raw Data] をクリックします。

ステップ 6　[File Save] ダイアログで、ファイルの場所と、エクスポート ファイルを保存する名前を選択します。

保存後に、ファイルが生成され、指定したファイルの場所にダウンロードされます。

エクスポートされたファイルには、Performance Monitor に示されたすべての情報といくつかの追加の統計情報カテゴリが含まれます。この情報には、メッセージ エラー数（アクセス失敗数など）とメッセージ サイズに関する情報が含まれます。

XML ファイルは、`Report` 要素を持つファイルのデータによって表されるタイム フレームを示します。この要素は、ファイルに対してパフォーマンス データが取得されたタイム フレームを示す `queryStartTime` 属性および `queryEndTime` 属性を持ちます。

このファイルは、時間ベースのパフォーマンス測定に関する広範な詳細情報を提供します。このパフォーマンス データについては次の点に注意してください。

- メッセージのタイミングはマイクロ秒単位で示されます（Performance Monitor は時間をミリ秒単位で示します）。
- 時間測定には次の統計情報が含まれます。
  - Time-To-First Byte（TTFirst）は、Firewall がネットワークからメッセージの最初のバイトを受信してからメッセージの最初のバイトを送信するまでの時間です。Performance Monitor に示された時間は、Time-To-First Byte です。
  - Time-To-Last Byte（TTLast）は、Firewall がメッセージの最後のバイトを受信してからメッセージの最後のバイトを送信するまでの時間です。

統計情報カテゴリを使用すると、次の ID で測定されたメッセージ処理ステージを調べることができます。

- `Req` は要求処理時間であり、ACE Web Application Firewall がユーザ要求の処理に費やした時間です。たとえば、`MinReqTTFirst` です。
- `Resp` は応答処理時間であり、ACE Web Application Firewall がバックエンド サービスからの応答の処理に費やした時間です。たとえば、`MinRespTTFirst` です。
- `Source` はバックエンド メッセージ ラウンドトリップ時間であり、送信要求がサービスに送信されてからサービスからの応答を受信するまでの時間です。たとえば、`MinSourceTTFirst` です。
- `Roundtrip` は、要求処理、応答処理、およびバックエンド サービスへのラウンドトリップを含む全体的なメッセージの処理時間です。たとえば、`MinRoundtripTTFirst` です。

各統計情報カテゴリの説明については、Web コンソールのオンライン ヘルプを参照してください。