CHAPTER 32

システム ステータスの監視

この章では、システムの状態およびアクティビティを監視する方法について説明します。内容は次のとおりです。

ログ情報について

ACE XML Gateway および Manager には、システムのアクティビティを監視するためのさまざまな機能が用意されています。これらの機能には、ダイナミック トラフィック統計情報の表示をカスタマイズできる Manager Dashboard、パフォーマンス モニタ、広範なエラー ロギング、Manager にポリシーの変更を表示する監査ログ、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 コンソールで使用できる監視ツールについて説明します。Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）や syslog などのシステムを監視するための外部ツールの使用方法については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。

ログにはネットワークを通過する悪意のある可能性があるトラフィックに関する情報が提供されるので、ログを利用してシステムのセキュリティを強化できます。ログは、SQL 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と一致することを意図した署名など、さまざまな攻撃署名と一致する要求を識別します。また、ログにはサーバ処理エラーが収集、報告されるため、ログを使用してバックエンド インフラストラクチャに関する問題を特定できます。パフォーマンス レポート ツールは、ベスト パフォーマンスを実現するためにシステムを調整する際に役立ちます。

Manager Dashboard には、ログで提供される情報の概要が表示されます。ログイン後に最初に表示されるページとして、攻撃の疑いなど、注意が必要な場合がある状態を警告します。また、必要なグラフを表示するようにカスタマイズできます。サービス定義ごとにトランザクション レート、エラー、および遅延を表示するグラフを使用できます。

ACE XML Gateway システムには次のログ タイプがあります。

- *イベント ログ*は、ACE XML Gateway および Manager の処理および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には、メッセージ トランザクション、システムの起動およびシャットダウン、Web コンソール ユーザの認証、ポリシーの配布、さまざまなエラーやその他のアクティビティなどがあります。
- *パフォーマンス ログ*は、パフォーマンス分析に役立つ、システム内のトラフィックに関する各種統計情報を保持します。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、さまざまな情報を提供します。この情報は、パフォーマンス モニタ、および 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 XML Manager Web コンソールのユーザ アクティビティを表示します。
- *メッセージ トラフィック ログ*は、要求および応答メッセージに関する情報を記録します。ロギング設定に応じて、このログにはメッセージ トラフィックに関する統計情報、すべてのメッセージの完全なコピー、または統計情報とメッセージの両方が記録されます。

ビジー システムのログ情報は、アプライアンスのディスク容量を大量に使用することがあります。リソースを使い果たさないために、アプライアンスのログ ファイルが使用するディスク容量が一定量に達すると、古いログ ファイルは自動的に削除されてディスク容量を増やします。この機能は、アプライアンスに不測のシャットダウンが発生しないようにするためのものです。管理プロセスを使用して定期的にログ ファイルをバックアップ 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推奨します。それにより、ログ情報は必要に応じて復元できます。そのために、ファイルを定期的にアプライアンスから移動する Shell 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 XML Gateway Administration Guide*』を参照してください。

イベント ロギング

イベント ログには、ACE XML Gateway および Manager のアクティビティに関する詳細な情報が記録されます。ACE XML Manager および ACE XML Gateway の内部動作だけでなく、トラフィック処理アクティビティに関する情報も表示されます。これらのイベントには、制御イベント（ポリシーの配布など）、エラー通知、システムの運用に重要なその他のイベントがあります。この情報は、システムのポリシーやネットワーク設定における問題の診断に役立ちます。

イベント ログにはいくつかの詳細レベルがあります。レベルが高くなるに従い、より詳細な情報が記録されます。ログレベルは次のとおりです。

表 32-1　イベント ログレベル

レベル	説明
アラート	システムがきわめて危険な状態にあり、システム障害を防ぐために早急な対応が必要。
エラー	不適切な結果や、システムの不適切な動作につながるエラー状態。
警告	不適切と思われる状態にあり、予期しない動作や望ましくない結果につながる可能性がある。
通知	正常であるが注意が必要な状態（メッセージの受信や配信など）。この報告レベルでは、通常の状態で処理される各メッセージに対して出力が 1 行生成されます。

レベル	説明
情報	メッセージ トラフィックの通常処理において重要な処理段階。このレベルでは、処理される各メッセージに対して数行の出力が生成されます。
デバッグ	ACE XML Gateway または Manager で報告可能なすべての情報。このレベルでは、ACE XML Gateway が処理するすべてのメッセージの本文が記録されます。 メッセージに対して表示されるデバッグ レベルの情報には、要求内で渡される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。一般に、このレベルのロギングはテストまたはトラブルシューティング目的に限り使用します。

ビジー状態の ACE XML Gateway では大量のイベント ログ記録が生成されることを考慮することが重要です。イベント情報は、syslog 経由で 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配送だけを提供します。非常にビジー状態のシステムやストレス テストの場合、イベント ログ情報が失われる可能性があります。

高い詳細レベル（通知、情報、デバッグ）では、大量の情報が記録されるので ACE XML Gateway のパフォーマンスに影響を及ぼすことがあります。これらのログレベルは問題を調べる場合に便利ですが、実稼動システムでは継続して使用しないようにしてください。

イベント ロギングの設定

イベント ログ項目は、ACE XML Gateway および Manager によって生成されます。生成されるイベントのタイプは次のとおりです。

- ACE XML Gateway のイベント ログには、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が記録されます。
- ACE XML Manager のイベント ログには、システムの管理アクティビティに関する情報が記録されます。

一般に、ACE XML Manager のイベント ログはシステム管理者にとって有用であるのに対して、ACE XML Gateway のログは、管理者およびポリシーのサービス定義を作成およびテストする開発者の両方にとって有用です。

イベントを記録するログレベルは、Gateway および Manager について別々に設定できます。

（注） Manager が複数のクラスタを制御する場合、イベント ログには現在のクラスタ内の Gateway の Gateway イベントだけが表示されます。Manager イベントはすべてのクラスタについて表示されます。Manager イベントの場合、ログの説明にイベントによって影響を受けるクラスタがクラスタ名ごとに表示されます。詳細については、第 34 章「Gateway クラスタの管理」を参照してください。

イベント ログレベルを設定する手順は、次のとおりです。

ステップ 1　Web コンソールに `Administrator` ユーザまたは `Operations` のロールを持つ `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。

- 操作メニューの [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] ペインの右端にある編集リンクのいずれかをクリックします。

ACE XML Manager に [System Management] ページが表示されます。

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、Gateway 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　メニューの横の [Set Log Level] ボタンをクリックして新しい設定を確認します。

新しい設定はただちに有効になります。

クライアント IP ロギング

[Global Policy Settings] メニューに表示される [Client IP] オプションを使用して、ロギングおよび報告用にソース クライアント IP として HTTP 要求ヘッダーの値を Manager で使用できます。このオプションは、たとえば X-Forwarded-For ヘッダー内の HTTP ヘッダーとしてクライアントの実際の IP アドレスを送信するように設定されているロード バランサの後ろ側に ACE XML Gateway を配置する場合に有用です。

この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 アドレスに加えて HTTP ヘッダーから抽出された IP アドレスが含まれます。

（注）　現在、[Global Policy Settings] を使用してクライアント ソース IP アドレスをログに表示できます。この設定は、仮想 Web アプリケーションおよび Reactor プロセッサによって処理される仮想サービスだけに適用され、Flex Path プロセッサを使用する仮想サービスには適用されません。

このオプションを有効にするには、[Global Policy Settings] ページで [edit] をクリックして、[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 バランサによってクライアント IP 値が別の名前のヘッダーに挿入された場合、HTTP ヘッダーの名前を変更できます。

イベント ログの表示

イベント ログを表示するには、操作メニューの [Reports & Tools] セクションで [Event Log] リンクをクリックします。デフォルトでは、ACE XML Manager に直前 1 時間のイベントが表示されます。[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、表示されているログをフィルタリングできます。たとえば、特定の ACE XML Gateway インスタンスに関して生成されたイベントだけを表示するように選択できます。また、ACE XML Gateway によって特定のメッセージ トランザクションに割り当てられたグローバルに一意の ID であるメッセージ 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 を使用した要求または応答に関連するイベントだけが表示されます。

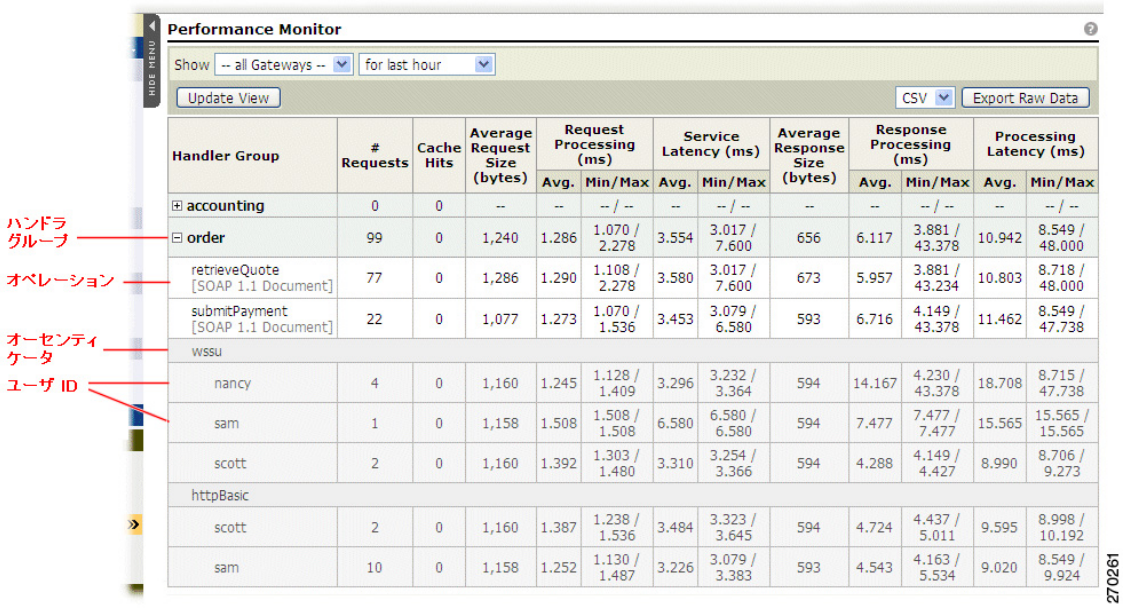
パフォーマンスの監視

パフォーマンス モニタには、メッセージの数、サイズ、処理時間を含む、システムの広範なパフォーマンス情報が表示されます。パフォーマンス モニタは、システム内のボトルネックを特定し、ACE XML Gateway およびバックエンド インフラストラクチャにおけるパフォーマンスを最適にするのに役立ちます。

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。各項目について、さまざまなパフォーマンス統計情報が表示されます。統計情報の各カテゴリについては、[Performance Monitor] ページから呼び出すオンライン ヘルプを参照してください。

ID 報告機能が有効な場合、モニタにサービスにアクセスするユーザの ID ごとの情報が表示されます。モニタに ID 固有の情報を表示するには、サービスに関連付けられているオーセンティケータに対して ID 追跡機能を有効にする必要があります（ID 追跡機能の有効化については、「ID 報告機能のイネーブル化」（P.6-94）を参照してください）。

図 32-1　　パフォーマンス情報



Performance Monitor

Show -- all Gateways -- for last hour

Update View　CSV　Export Raw Data

Handler Group	# Requests	Cache Hits	Average Request Size (bytes)	Request Processing (ms)		Service Latency (ms)		Average Response Size (bytes)	Response Processing (ms)		Processing Latency (ms)	
				Avg.	Min/Max	Avg.	Min/Max		Avg.	Min/Max	Avg.	Min/Max
⊞ accounting	0	0	--	--	-- / --	--	-- / --	--	--	-- / --	--	-- / --
⊟ order	99	0	1,240	1.286	1.070 / 2.278	3.554	3.017 / 7.600	656	6.117	3.881 / 43.378	10.942	8.549 / 48.000
retrieveQuote [SOAP 1.1 Document]	77	0	1,286	1.290	1.108 / 2.278	3.580	3.017 / 7.600	673	5.957	3.881 / 43.234	10.803	8.718 / 48.000
submitPayment [SOAP 1.1 Document]	22	0	1,077	1.273	1.070 / 1.536	3.453	3.079 / 6.580	593	6.716	4.149 / 43.378	11.462	8.549 / 47.738
wssu												
nancy	4	0	1,160	1.245	1.128 / 1.409	3.296	3.232 / 3.364	594	14.167	4.230 / 43.378	18.708	8.715 / 47.738
sam	1	0	1,158	1.508	1.508 / 1.508	6.580	6.580 / 6.580	594	7.477	7.477 / 7.477	15.565	15.565 / 15.565
scott	2	0	1,160	1.392	1.303 / 1.480	3.310	3.254 / 3.366	594	4.288	4.149 / 4.427	8.990	8.706 / 9.273
httpBasic												
scott	2	0	1,160	1.387	1.238 / 1.536	3.484	3.323 / 3.645	594	4.724	4.437 / 5.011	9.595	8.998 / 10.192
sam	10	0	1,158	1.252	1.130 / 1.487	3.226	3.079 / 3.383	593	4.543	4.163 / 5.534	9.020	8.549 / 9.924

（注） モニタに表示される統計情報は、概算値と見なす必要がある場合があります。特に、あるタイプのエラーになるメッセージは予想したように関連する統計情報を増加させないことがあります。また、この問題の発生状況はメッセージを処理するのが Reactor か Flex Path かによってさまざまです。たとえば、検証エラーを発生される Reactor によって処理される応答は予想どおりに BackendCount 統計情報を増加させません。同様に、Flex Path 上のメッセージのバックエンド サービス エラー（要求に対して 500 SOAP エラーを返します）は予想どおりに ErrorCount 統計情報を増加させません。

時間ごとのパフォーマンス データのフィルタリング

パフォーマンス モニタには、さまざまな方法で時間ごとに情報をフィルタリングできるコントロールが含まれています。時間フィルタリングは、コンソールの表示およびファイルにエクスポートする情報に影響を及ぼします。統計情報は次の時間で表示できます。

- 現在の時刻に終了する時間（直前 1 時間、過去 7 日間など）
- 設定時刻に開始する時間（午前 10 時に開始して現在の時刻に終了する時間など）
- 過ぎた時刻に終了する時間（特定の日の午前 10 時から午後 8 時までなど）

パフォーマンス データを分析する際には、Manager のパフォーマンス情報の物理的な容量には制限があることを考慮することが重要です。Manager のパフォーマンス データ容量がいっぱいになると、最も古いパフォーマンス情報が削除されます。情報をできるだけ削除されないように容量を保持するために、Manager は時間とともに短いタイム フレームから長いタイム フレームに情報を統合します。実際にはパフォーマンス データが古くなるとその詳細度を下げます。そのため、比較的長いオペレーション期間の情報の中から、短い時間の Manager のパフォーマンス情報のクエリーが可能ですが、返されるデータは実際に要求したよりも長い期間のデータであることがあります。この場合、ページ上部の通知には指定された詳細度が使用できないことが示されます。また、実際の値がページ上部にある時間フィルタ欄に反映されます。

このデータ統合またはデータ損失が発生する速度は、システム内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がいっぱいになる最も重要な要因は、さまざまな仮想サービスの数、特に Gateway でのトラフィックの量ではなく、ID 報告機能の使用です。

おおまかなガイドラインとして、約 100 個の仮想サービスを持つポリシーでは、それぞれのトラフィック フローが一定で（約 10 秒ごとに 1 つの要求）、ID 追跡機能が無効な場合は、Manager のパフォーマンス データ容量は 7 ～ 8 か月でいっぱいになると予想されます。ポリシーの仮想サービスが 10 個程度で ID 追跡機能が無効な場合、Manager は数年間パフォーマンス データを失うことなく保持できる場合もあります。

データ統合は数時間後に行われることがあります。仮想サービスが 10 個あり、それぞれが 10 秒ごとにメッセージを受信する場合、データは約 6.5 時間後に 5 分間のタイム フレームに統合されます。8 日後、複数の 5 分間のタイム フレームのデータは 1 時間のタイム フレーム 1 つに統合され、以後同様に統合されます。

パフォーマンス モニタでデータが使用できない詳細度で、ある時間間隔の情報を要求すると、使用可能な最も近い時間範囲がインターフェイスに表示され、ページ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を保持する場合は、パフォーマンス データを定期的にファイルにエクスポートする必要があります。Manager では、パフォーマンス データの Comma-Separated Values（CSV; カンマ区切り形式）および Extensible Markup Language（XML; 拡張マークアップ言語）形式でのエクスポートがサポートされます。

Manager がパフォーマンス情報を 1 日に対応するレコードに統合する場合、Greenwich Mean Time（GMT; グリニッジ標準時）で指定された日付境界線に沿って行います。または、Manager で GMT を基準とした特定の時間帯で 1 日のレコード境界線を引くことも可能です。そのためには、Manager の [Gateway Settings] ページにある [Message statistics "day" boundary] 欄を設定します。

パフォーマンス情報の表示

パフォーマンス情報を表示する手順は、次のとおりです。

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] セクションで [Performance Monitor] リンクをクリックします。

[Performance Monitor] ページに、ハンドラ グループごと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 グループ行には、そのグループのすべての仮想サービスに関する合計統計情報が表示されます。グループ名の下に、統計情報がサービスごとに分類されます。

（注）　マルチ オペレーション仮想サービスでは、仮想サービスの各オペレーションに関する統計情報はなく、仮想サービス全体の統計情報だけになります。

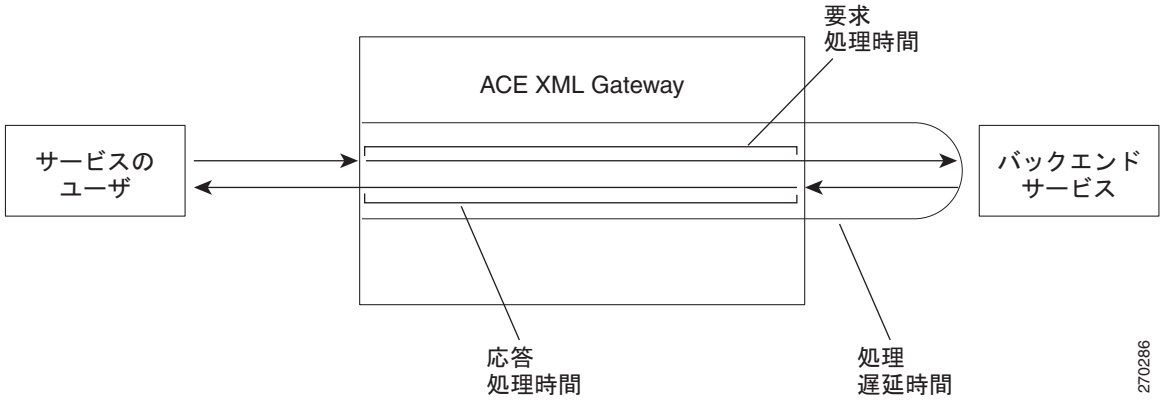
ページの上部にあるコントロールを使用すると、Gateway ごと、時間ごとなどのさまざまな方法で表示する情報をフィルタリングできます。

こうした統計情報に関して注意すべき点がいくつかあります。

- **Request Processing** および **Response Processing** 時間は、ACE XML Gateway が検証、ユーザ認証、変換、またはメッセージのポリシーで指定されたその他の処理手順を行うのに要する時間を表します。
- [Service Latency] カラムには、ACE XML Gateway がバックエンド サービスに要求を送信した時点から応答を受信するまでにかかった時間が表示されます。ACE XML Gateway がメッセージの処理に費やす時間は含まれません。
- メッセージ処理にかかる合計時間（要求処理、応答処理、サービス ラウンドトリップを含む）は、[Processing Latency] カラムに表示されます。

図 32-2 に、統計情報のカテゴリを示します。

図 32-2　パフォーマンス統計情報のカテゴリ



パフォーマンス モニタに表示される時間は 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が Gateway によって受信された時点で開始し、最初のバイトが Gateway からネットワークに転送された時点で終了します。そのため、特にメッセージが複数のパケットで構成されている場合、この値はネットワークの状態によって影響を受けることがあります。

パフォーマンス情報の各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。

パフォーマンス情報のファイルへのエクスポート

パフォーマンス データがビジー状態の ACE XML Gateway システムの ACE XML Manager に残されている場合、最終的にデータは失われます。パフォーマンス データ量が Manager の最大容量に達すると、最も古い情報が削除されて新しい情報のための容量が作成されます。パフォーマンス情報を無期限に保持する必要がある場合、ファイルにエクスポートできます。

パフォーマンス データのエクスポート機能は、パフォーマンス データを無期限に保存するためのメカニズムを提供するだけでなく、パフォーマンス モニタ インターフェイスで提供される情報より豊富な情報を利用できるようにします。また、メッセージ処理時間に関する統計情報のカテゴリも追加されます。

パフォーマンス データは、XML データとして、またはカンマ区切り形式（CSV）ファイルにエクスポートできます。パフォーマンス モニタの場合と同様に、エクスポートされたファイルの統計情報はハンドラごとにグループ分けされます。

（注）　パフォーマンス モニタを表示する場合、サブポリシー間で移動されたハンドラは、ハンドラ名ではなく、以前のサブポリシーにおけるアクティビティの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、パフォーマンス モニタとは異なって表示されます。エクスポートされたパフォーマンス情報は、人間が読めるように処理または構成されていない未加工のデータとして見なす必要があります。

エクスポートされたデータとパフォーマンス モニタには次のような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信した仮想サービスはファイルに一覧表示されます。要求を受信し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。
- パフォーマンス モニタには、各ハンドラ グループのメッセージ処理についての合計値が表示されます。エクスポートされたファイルには、同じような合計値は表示されません。代わりに各仮想サービスのレコードが含まれます。ID 報告機能が有効な場合、サービスにアクセスした各 ID のレコードおよびその ID の要求数が含まれます。
- 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ていない要求のレコードが含まれます。これらは、エラー数欄に 1 より大きい値で表示されます。
- パフォーマンス モニタに表示される Time-To-First-Byte 測定値に加えて、エクスポートされたファイルには各要求および応答の Time-To-Last-Byte 測定値が表示されます。

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手順は、次のとおりです。

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て、操作メニューの [Reports & Tools] セクションで [Performance Monitor] リンクをクリックします。

ステップ 2　Gateway および時間コントロールを使用してエクスポート ファイルにエクスポートする情報をフィルタリングします。

期間などのフィルタ コントロールは、パフォーマンス モニタの表示に影響を与える以外に、ファイルにエクスポートされ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　出力ファイル形式を次から選択します。

- XML（XML 形式ファイル）
- CSV（カンマ区切りファイル）

この選択が影響を及ぼすのは、生成される情報ではなくその形式だけです。

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、エクスポート ファイルを保存するためのファイルの場所と名前を選択します。

保存すると、ファイルが生成されて指定した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、パフォーマンス モニタに表示されるすべての情報に加えてその他の統計情報カテゴリも含まれます。この情報には、アクセス障害などのメッセージ エラー数とメッセージ サイズに関する情報が含まれます。

XML ファイルでは、ファイル内のデータによって表されるタイム フレームが `Report` 要素で示されます。この要素には `queryStartTime` および `queryEndTime` アトリビュートがあり、パフォーマンス データがファイルに取り込まれた時間を示します。

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 データに関して次の点に注意してください。

- メッセージ タイミングはマイクロ秒で表示されます（パフォーマンス モニタでは時間はミリ秒で表示されます）。
- 時間測定値には次の統計情報が含まれます。
  - Time-To-First-Byte（TTFirst）は、Gateway 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の送信を開始するまでの時間です。パフォーマンス モニタに表示される時間は Time-To-First-Byte です。
  - Time-To-Last-Byte（TTLast）は、Gateway 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。

統計情報のカテゴリ名では、次の識別子によって測定されるメッセージ処理段階を確認できます。

- `Req` は要求処理時間（ACE XML Gateway がユーザ要求の処理に費やす時間）です。例：`MinReqTTFirst`
- `Resp` は応答処理時間（ACE XML Gateway がバックエンド サービスからの応答の処理に費やす時間）です。例：`MinRespTTFirst`
- `Source` は、発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が受信されるまでのバックエンド メッセージ ラウンドトリップ時間です。例：`MinSourceTTFirst`
- `Roundtrip` は、要求処理、応答処理、バックエンド サービスへのラウンドトリップを含むメッセージ処理合計時間です。例：`MinRoundtripTTFirst`

統計情報の各カテゴリについては、Web コンソールのオンライン ヘルプを参照してください。

サービスの状態

ACE XML Manager は、ポリシー内のすべてのサービス定義のステータスの概要を表示します。このステータス表示を確認すると、各ハンドラの負荷状態および ACE XML Gateway がいずれかのハンドラに関してエラーを報告しているかどうかをすぐに把握できます。[Service Health] ページでは、簡単に特定のハンドラを見つけてそのステータスを表示できます。

ハンドラのステータスを表示する手順は、次のとおりです。

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] セクションで [Service Health] リンクをクリックします。

[Service Health] ページには、ハンドラ グループごとにまとめられたポリシーの各ハンドラおよびそれぞれのステータスの概要が表示されます。デフォルトでは、定義済みのすべてのハンドラのステータスが表示されます。

ページの上部にあるフィルタ コントロールを使用して、表示項目を特定の Gateway アプライアンス、または指定間隔で処理されるトラフィックだけに絞り込むことができます。

[Status] カラムには、仮想サービスが正常にエラーなしで稼動しているかどうかが表示されるので（正常に動作している場合は[OK]）、問題を迅速に特定できます。

[Error Summary] カラムには、各ハンドラに対して記録されたエラー メッセージの簡単な概要が表示されます。その他のカラムには、ハンドラの現在のログレベルおよび処理されたメッセージの数が表示されます。

[Message Logging] カラムで現在のログレベルを確認できます。Gateway 内の Flex Path I/O プロセッサのハンドラでは、このカラムのメニューを使用してログレベルを変更できます。

（注）　この場合、統計情報のロギングだけがサポートされるため、Flex Path にないハンドラにはこのオプションはありません。

メッセージ ロギング

ACE XML Gateway は、処理する各メッセージに関する情報を記録します。記録された情報は message-traffic ログに格納されます。ACE XML Manager の [Message Traffic Log] ページで、記録された情報を表示、フィルタリング、検索できます。

メッセージ トラフィックの場合は、ACE XML Gateway は次の 3 つのレベルのいずれかで情報を記録します。

- 統計情報のみ
- 発信メッセージのログ メッセージ本文
- 着信および発信メッセージのログ メッセージ本文

統計情報だけをログに記録するように設定された仮想サービスは、メッセージのサイズおよびそのメッセージの処理にかかった時間を示す累積合計値だけを記録します。発信メッセージ用に設定された仮想サービスは、処理された各発信メッセージの完全なコピーを記録します。着信および発信メッセージ用に設定された仮想サービスは、着信および発信メッセージのメッセージ本文の完全なコピーを記録します。

異なるログレベルに異なるハンドラが設定されていることがあるため、メッセージ ログ エントリに記録されている情報は統一されていません。記録されたメッセージ データを調べるときは、ハンドラによって作成されるエントリのログレベルは異なることに留意してください。

記録される情報は、各ハンドラの設定によって決まります。各ハンドラの情報ページから利用できるエディタを使用して、処理するメッセージに関する情報を異なる詳細度で記録するようにハンドラを設定できます。最も詳細に記録する設定では、ハンドラはメッセージ自体の完全なコピーを含む、各メッセージに関してハンドラが認識しているすべての情報を記録します。この最も詳細な設定には注意が必要です。多数の大きなメッセージの完全なコピーを記録すると、ディスク容量がすぐにいっぱいになってしまう可能性があるからです。

または、処理されたメッセージの数、サイズ、処理時間などの処理に関する統計情報だけを記録するようにハンドラを設定することもできます。この統計情報だけの設定はメッセージ全体を記録する場合より速くなりますが、問題のデバッグ時に重要になる個別メッセージに関する情報が少なくなります。

一般に、パフォーマンスを重要視する場合は実稼動システムには統計情報だけのロギング、ポリシーのテストおよび作成にはより詳細なメッセージ ロギングを推奨します。

メッセージ ロギングの設定

ポリシー内のメッセージ ログレベルは仮想サービスのプロパティです。次の手順で、オブジェクト作成時にメッセージ ロギングを設定、または変更します。

ステップ 1　ACE XML Manager 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て、[Virtual Services] ブラウザを開きます。

メッセージ ロギングは、個々のサービス定義オブジェクトごとに有効にすることも、ハンドラ グループごとに複数のサービス定義を 1 度に有効にすることも可能です。

ステップ 2　1 つのサービス定義のメッセージ ロギングを設定する手順は次のとおりです。

a. メッセージ ロギングを有効にする仮想サービス オブジェクトまたはメッセージを処理するハンドラをクリックします。

b. [General settings] という見出しの横の [Edit] リンクをクリックします。

c. [Default Message Logging] メニューから [log bodies of inbound and outbound messages] を選択します。

ステップ 3　ハンドラ グループごとにメッセージ ロギングを設定する手順は次のとおりです。

a. [Virtual Services] ブラウザで、ハンドラ グループ名をクリックします。

b. [Set message logging levels for all members to] メニューから [log bodies of inbound and outbound messages] を選択します。

ステップ 4　[Save Changes] をクリックし、ポリシーを配布して変更を有効にします。

アクティブなシステムのメッセージ ロギングは、アプライアンスのディスク容量を大量に使用することがあります。[System Management] > [Gateway Settings] ページから、メッセージ ロギングによって使用される容量を制限できます。[Delete old log files when total message log disk usage exceeds] オプションを使用して制限を設定します。

メッセージ トラフィック ログの表示

メッセージ トラフィック ログを表示する手順は、次のとおりです。

ステップ 1　ACE XML Manager Web コンソールに `Message Traffic Log` ロールを持つ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] セクションで [Message Traffic Log] リンクをクリックします。

[Message Traffic Log] ページが表示されます。

ステップ 3　ログで必要なメッセージを検索します。

- ユーザ、ハンドラ、サービス GUID、およびその他のさまざまな条件で検索結果をフィルタリングするコントロールを設定します。

  詳細については、この項の以降の説明を参照してください。
- [Update View] ボタンをクリックします。

  [Search Results] ペインに検索条件に適合するログ エントリが表示されます。

ACE XML Manager の [Message Traffic Log] ページにはメッセージ ログの内容が表示されます。このページには、エントリをフィルタリングおよび検索するためのツールが用意されています。デフォルトでは、[Message Traffic Log] ページにログのすべてのエントリが表示されます。

ビジー状態の Gateway のログはかなり大きくなることがあり、大量のエントリがトラブルシューティングを妨げる場合があります。ページの上部にある検索タブを使用して、クエリーに適合するログ エントリだけを表示するクエリーを作成できます。

次の検索タブがあります。

- [Simple Search] はデフォルトで表示されるタブで、最もよく使用される検索オプションがあります。
- [Advanced Search] には、サービス、ユーザ、または要求や応答アトリビュートによる検索など、詳細検索オプションがあります。
- [GUID Search] では、ACE XML Gateway によってメッセージに割り当てられた Globally Unique Identifier（GUID）がわかっている場合に特定のメッセージを検索できます。[GUID Search] オプションは、ログを調べて特定したメッセージの ACE XML Gateway による処理を追跡する場合に最も便利です。
- [User Search] ではユーザ ID で検索できます。このオプションを使用する場合、特定のオーセンティケータに対してユーザ ID 機能を有効にしておく必要があります。ログのユーザ情報の有効化については、「ID 報告」（P.6-93）を参照してください。

ページにはリスト内のログ エントリに関する情報が表示されますが、表示されるエントリの数は検索ツールで設定した数に制限されます。デフォルトでは、ページ当たり 25 のログ エントリが表示されます。各エントリには、エントリが作成された時刻のほかに、エントリを記録した特定の Gateway アプライアンスの IP アドレス、メッセージ タイプ、ハンドラ、要求を受信したオーセンティケータなどのエントリに関する情報が表示されます。表示される情報は、エントリが作成された時点の記録するハンドラのロギング設定によって決まります。

特定のエントリに関する詳細を表示するには、そのエントリの行の右端にある [Details] リンクをクリックします。

準拠性レポート

Sarbanes-Oxley Act（SOX; 米国企業改革法）などの標準会計要件に準拠するために、企業は発生したビジネス プロセス トランザクションを調査および報告できる必要があります。ビジネス プロセスに適用されるポリシーの変更について説明できることも重要です。

こうしたポリシーの作成および適用ポイントとして、ACE XML Gateway は、該当する要件の対象となるトラフィックのタイプの Gateway としてだけではなく、準拠性要件に対応するために必要な情報の収集および報告にも適しています。

ACE XML Gateway は、ここで説明されているようなポリシー オブジェクトのログレベル設定および準拠性レポート生成のツールなど、準拠性要件に適合するためのツールを備えています。

準拠性ロギングの表示と有効化

ほとんどの場合、準拠性についての報告要件に従うにはビジネス プロセス間のトランザクションを監査する機能が必要です。そのため、こうした要件に準拠するために ACE XML Gateway ポリシーの該当するトラフィック ハンドラで何らかの形でメッセージ ロギングを有効にする必要があります。

[Compliance Report] ページには、現在導入されているポリシーの各サービス ポリシー オブジェクト（ハンドラおよびサービス記述子）のロギング設定の概要が表示されます。

ポリシーのロギング ステータスを表示する手順は、次のとおりです。

ステップ 1　操作メニューの [Reports & Tools] セクションで [Compliance Report] リンクをクリックします。

[Compliance Report] というタブが付いたペインが表示されます。[Logging Settings] タブには、現在のポリシーでハンドラおよびサービス記述子に対してロギングが有効になっているかが表示されます。

ロギング オプションは次のいずれかに設定できます。

- **enabled**：ハンドラまたはサービス記述子の **Default Message Logging** プロパティは [log headers of outbound messages] に設定されます。これは準拠性レポート作成に適したレベルです。
- **disabled**：ハンドラまたはサービス記述子の **Default Message Logging** プロパティは [log statistics only (no message content)] に設定されます。これは準拠性レポートを作成するために適したレベルではありません。

ステップ 2　特定の仮想サービスの準拠性ロギングのステータスを変更するには、その仮想サービスの [Compliance Logging] カラムにある [edit] リンクをクリックします。

[General Information] 編集ページが表示されます。

ステップ 3　[Default Message Logging] メニューから次のいずれかのログレベルを選択します。

- **[log headers of outbound messages]**
- **[log bodies of outbound messages]**
- **[log bodies of inbound and outbound messages]**

ステップ 4　[Save Changes] をクリックします。

ハンドラの情報ページが表示されます。

ステップ 5　[Compliance Report] ページに戻るには、操作メニューの [Compliance Report] リンクをクリックします。

ハンドラのステータスは、ポリシーを配布するまで元の状態のままであることに注意してください。

設定が完了すると、ACE XML Gateway は、設定した仮想サービスによって処理されたトラフィックのトランザクション情報をログに記録します。この後に生成する準拠性レポートに情報が表示されます（「準拠性レポートの生成」（P.32-347）を参照）。

準拠性レポートの生成

準拠性レポートの生成手順は、次のとおりです。

ステップ 1　操作メニューの [Reports & Tools] セクションで [Compliance Report] リンクをクリックします。

[Compliance Report] というタブが付いたペインが表示されます。このタブには、ポリシー内のサービス オブジェクトのロギング ステータスがハンドラごとに表示されます。準拠性ロギングの設定および詳細については、「準拠性レポートの生成」（P.32-347）を参照してください。

[Compliance Report] ページにはそのほかに次のようなタブがあります。

- [Test Messages]。ACE XML Manager Web コンソール内のテスト ブラウザから発信されたトラフィックに関する情報が表示されます。
- [Message Traffic]。Web コンソール内のテスト ブラウザから発信されたトラフィックに関する情報が表示されます。

- [Policy Changes]。ACE XML Gateway の管理者に関連付けられたアクティビティ、特に ACE XML Gateway ポリシーの変更が表示されます。
- [Event Log]。イベント ログが表示されます。

ステップ 2　ログ レポート ペインに表示されるメッセージの期間を変更する手順は、次のとおりです（どのメッセージが生成されるレポートに含まれるかにも影響を及ぼします）。

a. [Show] ペインから新しい期間を選択します。直近 7 日間、30 日間、または 60 日間に生成されたメッセージを表示するように選択するか、または [date range] オプションを選択して日付範囲を指定します。

b. [Update View] をクリックします。

ステップ 3　すべてのアクティビティの XML 形式レポートを生成するには、[Export as XML] ボタンをクリックします。

生成されたログ ファイルがポップアップ ブラウザ ウィンドウに表示されます。ログ ファイルには、前の手順で指定したタイム フレームが反映されます。また、ACE XML Manager は複合ログ ファイルも生成します。このファイルには、メッセージ トラフィック、テスト アクティビティ、管理アクティビティ、およびイベントが XML 形式データとして格納されます。