CHAPTER 1

概要

Performance Monitor はブラウザベースのツールで、企業ネットワーク セキュリティに役立つサービスのヘルスとパフォーマンスを、モニタおよびトラブルシューティングします。サポートされているサービスのタイプは、リモートアクセス VPN、サイト間 VPN、ファイアウォール、Web サーバ ロード バランシング、およびプロキシ SSL です。

ヒント 重要なセキュリティの概念、テクノロジー、およびサービス タイプの詳細については、Cisco.com を参照してください。

ここでは、Performance Monitor の概要について説明します。

Performance Monitor とは

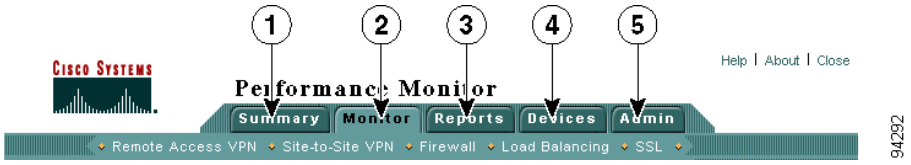
Performance Monitor は Cisco Security Management Suite のコンポーネントの 1 つです。ネットワーク内で重要なイベントが発生したときに、それらのイベントを分離し、分析してトラブルシューティングすることにより、サービスの可用性を向上できます。Performance Monitor は、必要なサーバ側のコンポーネントを提供し、Performance Monitor の代わりにいくつかの機能を管理する、CiscoWorks Common Services 上で実行されます。詳細については、Common Services のオンライン ヘルプを参照してください。

次の表に、Performance Monitor のスケーラビリティを示します。

- **デバイス数**：セキュリティ コンテキストを含めて、最大で 500 のデバイスをサポートします。
- **ユーザ数**：最大で 5 人のユーザを同時にサポートします。
- **VPN の制約**：モニタ対象のハブアンドスポーク VPN では、スポークではなくハブだけをモニタすることを推奨します。モニタするトンネルの数が 5,000 を超えないようにしてください。

次の図は、Performance Monitor のすべての機能にアクセスするためのタブを示します。

図 1-1　　タブ



1	[Summary] タブ オプションでは、次のことができます。 • ネットワーク内の既知のクリティカルな問題（P1 および P2）のリストや、ネットワーク内でサポートされているすべてのサービスのヘルスとパフォーマンスを要約したグラフとチャートを表示する。 • *ダッシュボード*（コンパクトな要約）を開いたり、フィルタを設定せずに*イベント ブラウザ*を開く。 **（注）**　ダッシュボードおよびイベント ブラウザの詳細については、「基本概念について」（P.1-3）を参照してください。
2	[Monitor] タブ オプションには、サポートされているデバイス上で、次のサポート対象のサービスをリアルタイムにモニタする機能があります。 • マルチコンテキスト（仮想ファイアウォール）を含めた、VPN（RAS またはサイト間）およびファイアウォール デバイスとサービス。 • コンテンツ スイッチング サービス モジュールのロードバランシング サービス。 • SSL プロキシ サービス。 サポートされるデバイスのリストについては、『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください。
3	[Reports] タブのオプションでは、次のことができます。 • 使用、スループット、パフォーマンスおよび障害に関するレポートを設定、生成、および参照する。 • レポートの自動作成および E メール配布をスケジュールする。 • 任意のユーザ、またはすべてのユーザのリモートアクセス VPN セッションに関するレポートを表示する。 • データ ポイントが時間、日、週、または月の間隔で発生しているレポート データを、最大 1 年分確認する。 • レポート データを CSV、XML、または PDF 形式でエクスポートする。
4	[Devices] タブ オプションでは、次のことができます。 • デバイスの属性を手動で、または CSV ファイルからインポートおよび検証する。 • デバイスのハードウェア、ソフトウェア、およびネットワークの説明を表示する。 • Performance Monitor が [Monitor] タブで最後にテーブルおよびグラフを更新したタイミング、および更新の対象範囲を知る。 • デバイスの SNMP 設定を編集する。 • デバイスのポーリングをイネーブルまたはディセーブルにする。 • デバイス グループ（システム定義またはユーザ定義）にナビゲートし、それらのプロパティを表示する。 • デバイス グループを作成し、それらのプロパティを編集する。 • ユーザ定義のデバイス グループを削除し、特定のデバイスへの参照を削除する。

5	[Admin] タブ オプションでは、イベント管理の設定、システム パラメータの設定、ログの確認、組織に対してカスタマイズしたオンライン ヘルプ コンテンツの作成、およびデフォルト ページの指定を行えます。 • イベント管理のオプションでは、次のことができます。 – SNMP トラップ、Syslog データ、または超過したしきい値に基づいてイベントを生成する。 – デフォルトまたはユーザ設定可能なしきい値を使用する。 – E メール、SNMP トラップ、および Syslog で通知を設定する。 システム パラメータの設定により、ポーリング間隔、トランケーション間隔、および Performance Monitor が履歴データのレコードを削除するまでの期間が制御されます。

基本概念について

Performance Monitor を正しく使用するうえで理解しておく必要がある基本概念を次の表に示します。

表 1-1　Performance Monitor の概念

概念	説明
クリティカルな問題	クリティカルな問題とは、システム コンポーネントがパフォーマンスのしきい値を超えた場合、または正常に機能していない場合に発生する異常な（P1 または P2 の）状態です。クリティカルな問題により、ネットワーク サービスが中断および停止することがあります。
ダッシュボード	ダッシュボードは小さなブラウザ ウィンドウで、この中で、サポートされている 1 つ以上のサービスの要約グラフを分離します。このグラフは、ユーザが指定した間隔でリフレッシュされ、選択した数のサービスのパフォーマンスを要約したものです。複数のサービスを選択すると、ダッシュボードはそれらのサービスを順番に循環し、ダッシュボードの表示がリフレッシュされるたびに、一度に 1 つのサービスのグラフを表示します。 [Summary] タブのページで分離アイコン（図 3-2（P.3-5）を参照）をクリックすると、ダッシュボードが開きます。
イベント	イベントは、管理対象のデバイスまたはコンポーネントが異常な状態になったことを通知するものです。モニタ対象の 1 つのデバイスまたはサービス モジュールで、複数のイベントが同時に発生することがあります。イベントの表示には、イベント ブラウザを開きます。
イベント ブラウザ	イベント ブラウザは、イベントを次の 2 つのイベント クラスに整理します。 • 障害 : モニタ対象のコンポーネントまたはサービスが失敗して、予想どおりに機能しなかったイベントを表示します。 • パフォーマンス : モニタ対象のコンポーネントまたはサービスが、許容されているしきい値を超えたイベントを表示します。 イベント ブラウザを使用すると、イベント全体を見たり、タイプごとに見たりすることも、選択した基準によってイベントをソートすることもできます。イベントは、イベント クラス、サービス タイプ、デバイス タイプ、重大度、状態、または説明によってフィルタすることも、割り当てられたイベント ID 番号で検索することもできます。表示されたイベントを解決する役割を担うこともできます。 モニタ対象のそれぞれのサービスには、専用のイベント ブラウザがあります。イベント ブラウザ内の情報は通常、ユーザ自身が開始したサービスだけが該当します。あるサービスのイベントだけを表示するには、該当するイベント ブラウザを開く必要があります。 **ヒント** すべてのサービスに関して、全タイプのフィルタされていないイベントを表示するイベント ブラウザを開くには、[Summary] > [Event Browser] を選択します。

表 1-1　Performance Monitor の概念（続き）

概念	説明
要約	要約グラフおよびテーブルは、設定可能な間隔で繰り返し行われるポーリングに基づいて、最近の 8 時間のサービス アクティビティを示します。詳細な情報を表示するには、ハイパーリンクされたグラフおよびテーブルのエントリをクリックします。

Performance Monitor と FCAPS

ネットワークを安全かつ効率よく実行するための明確な対象および戦略を提供するために、International Organization for Standardization（ISO; 国際標準化機構）は、*FCAPS* モデルと呼ばれるネットワーク管理モデルを開発しました。このモデルは、ネットワーク管理の 5 つの主要な分野である、障害管理、構成管理、アカウンティング、性能管理、およびセキュリティを識別するものです。

- 障害管理は、ネットワークおよびシステムの障害（停止や低下）の検出、診断、および修正に関係しています。障害管理の製品には通常、アラート処理やイベント管理機能が用意されており、障害を切り離して是正措置または選択的措置を容易にするために必要な、診断ツールが含まれているものもあります。
- 構成管理は、インストール、識別、インベントリの削除、（カード、モジュール、メモリ、ソフトウェアなどのコンポーネントも含めた）ハードウェア、ソフトウェア、ファームウェア、およびサービスの構成に関係しています。構成管理では、デバイスの展開ステータスのモニタリングおよび管理も提供します。構成管理の機能領域には、ソフトウェア管理、変更制御、およびインベントリ管理が含まれています。
- アカウンティング管理は、ネットワーク内のリソース使用の追跡に関係しています。たとえば、サービス プロバイダーが提示する時間とサービスの両方に対する課金コストの配分などです。アカウンティング管理では、通信およびコンピュータ設備の使用に対する課金だけでなく、ネットワークに対するユーザ アクセス、およびそれらのユーザによってアクセスされるリソースの追跡も行います。アカウンティング管理システムには通常、料金体系の知識が含まれています。
- 性能管理は、使用率、応答時間、アベイラビリティ、およびエラー率に関する短期間および長期間のネットワークとシステムの両方の統計の測定、および分析に関係しています。ネットワーク上で停止している箇所があるかどうかを判断する場合にも、性能管理を使用します。理想的には、パフォーマンス データを使用すると、キャパシティ使用率などの問題がユーザやサービスに影響を与える前に、ネットワーク プランナーがこれらの問題を示す傾向を識別しやすくなり、将来の障害を防止できます。性能管理ツールは、ネットワークおよびシステムの効率を改善するために、計画、設計、およびパフォーマンスチューニングをサポートする場合にも使用します。
- セキュリティ管理は、ネットワーク リソースへのアクセス制御、およびネットワークの不正使用または改ざんの防止に関係しています。セキュリティ管理ツールは、ユーザのアクセス権、データの機密性、セキュリティ攻撃や侵害の警告と監査証跡、セキュリティ対策の管理、およびパスワードの配布に対処できます。

次の表の太字で示すように、Performance Monitor アプリケーションの機能は、障害管理と性能管理のカテゴリに含まれています。

表 1-2　FCAPS モデルの構成

障害管理	構成管理	アカウンティング管理	性能管理	セキュリティ管理
アラームの処理	システムの調査	サービス使用の追跡	**データの収集**	ネットワーク エレメント（NE）アクセスの制御
問題の検出	プロビジョニング	サービスへの課金請求	**レポートの生成**	NE 機能の有効化
問題の修正	自動検出	サービス レベル契約	**データ分析**	アクセス ログ
テストと承認	バックアップと復元		**パフォーマンス モニタ**	
ネットワークの回復	データベース処理			
アラームの転送	インベントリの管理			
フィルタリング				

モニタリングおよびレポートでサポートされるサービスとプラットフォーム

次の表は、サポート対象のそれぞれの Cisco プラットフォームごとに、Performance Monitor がモニタできるサービス、およびレポートを発行できるサービスを示しています。表の後で、詳細に説明します。

表 1-3　モニタリングでサポートされるサービスとプラットフォーム

		モニタ対象のサービス タイプ							
		VPN				ファイアウォール		その他	
プラットフォーム		DMVPN	Easy VPN	リモート アクセス	サイト間	ファイアウォール	マルチコンテキスト	ロード バランシング	SSL
適応型セキュリティ アプライアンス 5500 シリーズ		×	○	○	○	○	○	×	×
Catalyst 6500 シリーズ スイッチ	コンテンツ スイッチング サービス モジュール	×	×	×	×	×	×		×
	ファイアウォール サービス モジュール	×	○	○	○	○	○	×	×
	SSL サービス モジュール	×	×	×	×	×	×	×	○
	VPNSM	○	×	—	○	—	×	×	×
	VPN SPA	○	×	—	○	—	×	×	×
	VSPA	○	×	—	○	—	×	×	×
Cisco IOS ルータ		○	○	○	○	○	×	×	×
PIX ファイアウォール		×	○	○	○	○	○	×	×
VPN 3000 コンセントレータ シリーズ		×	○	○	○	×	×	×	×

この表を検討する際は、次の点に注意してください。

- この表の見方は次のとおりです。
  - ×は、指定のプラットフォーム上で提供していないサービスを表します。
  - ○は、指定のプラットフォーム上で Performance Monitor がサポートしているサービスを表します。
  - ダッシュ（—）は、指定のプラットフォーム上で Performance Monitor がモニタしていないサービスを表します。
- 次のサービスのサポートは、ソフトウェアまたはデバイスのバージョンによって異なります。
  - PIX OS 7.0 以降は Easy VPN サービスをサポートしていますが、Easy VPN の RAS クラスタリングはサポートしていません。
  - PIX OS 7.0 以降は Easy VPN、RAS VPN、サイト間 VPN、および仮想（マルチコンテキスト）ファイアウォール サービスをサポートしています。
  - PIX OS 7.0 以降は、ルートされているシングル コンテキスト モードでのみ、RAS VPN およびサイト間 VPN サービスをサポートしています。
  - FWSM バージョン 2.2 以降は、仮想（マルチコンテキスト）ファイアウォール サービスをサポートしています。
  - FWSM バージョン 3.1 以降は、ルートされているシングル コンテキスト モードでのみ、RAS VPN およびサイト間 VPN サービスをサポートしています。
  - Cisco ASA Software Version 7.0 以降は、Easy VPN、RAS VPN、サイト間 VPN、および仮想（マルチコンテキスト）ファイアウォール サービスをサポートしています。
- Performance Monitor は、Cisco VPN 3000 コンセントレータ、または仮想クラスタ内に編成しているサポート対象の ASA アプライアンスのロード バランシングに対して、モニタおよびレポートの提供はしません。この表の *ロード バランシング* カラムは、Catalyst 6500 シリーズ スイッチのサポートされるコンテンツ スイッチング サービス モジュールに関連付けられた、Web サーバのロード バランシング サービスとは、排他的であることを示しています。