Cisco Performance Monitor 4.0 ユーザ ガイド

User Guide for Cisco Performance Monitor 4.0

Text Part Number: OL-21886-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Performance Monitor 4.0 ユーザ ガイド

CONTENTS

はじめに

Cisco Security Manager（Security Manager）を購入すると、ライセンスによって、Cisco Performance Monitor（Performance Monitor）をダウンロードおよびインストールし、適切なバージョンを使用する権限が得られます。

Performance Monitor は、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。これによりユーザは、ネットワークでイベントが発生したときに、イベントを分離、分析、およびトラブルシューティングして、サービスのアベイラビリティを向上できます。

このマニュアルでは、Performance Monitor アプリケーションの機能、およびこれらの機能の使用方法について説明します。

ヒント SAFE はセキュアなネットワークを設計、実装、および保守するためのシスコのストラテジです。シスコでは、Security Manager、または Security Manager に関連する何らかのコンポーネント アプリケーションをインストールする前に、Cisco SAFE の詳細計画におけるベスト プラクティスを実装することを推奨します。SAFE の詳細については、http://www.cisco.com/go/safe を参照してください。

対象読者

このマニュアルは、エンド ユーザのサポート、ネットワーク運用の管理、またはネットワーク キャパシティの計画を行っているネットワークおよびセキュリティの担当者を対象にしています。

表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	**太字**
ユーザが値を指定する変数	*イタリック体*
セッション情報およびシステム情報の表示出力	`Screen フォント`
ユーザが入力する情報	太字の **`screen`** フォント
ユーザが入力する変数	*イタリック体の `screen` フォント*

項目	表記法
メニュー項目およびボタン名	太字
本文中のメニュー項目の選択	**[Option] > [Network Preferences]**
表中のメニュー項目の選択	[Option] > [Network Preferences]

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ヒント 「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイント アドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

Performance Monitor のマニュアル

Performance Monitor のマニュアルの完全なリストについては、次の URL にある、このバージョンの製品のマニュアル ロードマップを参照してください。
http://www.cisco.com/en/US/products/ps6498/products_documentation_roadmaps_list.html

http://www.cisco.com/go/csmanager も参照してください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

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

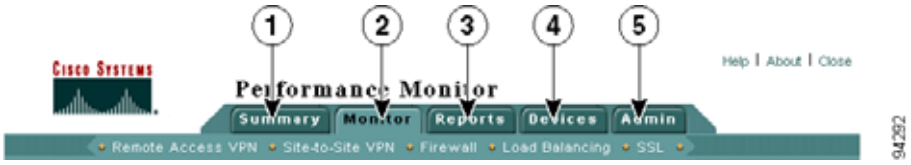
Performance Monitor は Cisco Security Management Suite のコンポーネントの 1 つです。ネットワーク内で重要なイベントが発生したときに、それらのイベントを分離し、分析してトラブルシューティングすることにより、サービスの可用性を向上できます。Performance Monitor は、必要なサーバ側のコンポーネントを提供し、Performance Monitor の代わりにいくつかの機能を管理する、CiscoWorks Common Services 上で実行されます。詳細については、Common Services のオンライン ヘルプを参照し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

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。

CHAPTER 2

始める前に

お使いのサーバやネットワーク内で特定のオプションや機能が設定されていない場合は、Performance Monitor が設計どおりに動作できません。この章では、Performance Monitor で提供されるすべての機能を使用できるように、行う必要がある作業、推奨する作業について説明します。

表 2-1　高レベルのタスク

	タスク
ステップ 1	**アクセス用にサポートされているデバイスを設定します。**Performance Monitor で検証、ポーリング、およびモニタできるようにデバイスを設定する必要があります。「デバイスのブートストラップ」（P.2-2）を参照してください。
ステップ 2	**デバイスをインポートまたは追加します。**重要なデバイス アトリビュートのローカル レコードが作成されるまで、Performance Monitor でデバイスをモニタできません。「Importing Devices ウィザードを使用したデバイスのインポートまたは追加」（P.2-9）を参照してください。
ステップ 3	**デバイスを検証します。**「デバイスの検証」（P.2-13）を参照してください。 **（注）** デフォルトでは、デバイスの検証中に Performance Monitor ですべての検証対象のデバイスが管理対象状態に設定されます（ポーリングがイネーブルになります）。デバイスを管理対象外の状態に移行するように選択した場合、そのデバイスのヘルスやパフォーマンスをモニタできるようにするには、手動で管理対象状態に戻す必要があります。デバイスを管理対象状態に設定するには、「デバイス モニタリングのイネーブル化またはディセーブル化」（P.11-6）を参照してください。
ステップ 4	**E メールを設定します。**お使いのサーバで設定するまでは、E メールによってイベントの通知を送信したり、スケジュールされたレポートを配布したりはできません。「E メール使用のための Common Services の設定」（P.2-16）を参照してください。
ステップ 5	**SNMP を設定します。**「SNMP トラップの受信」（P.2-17）を参照してください。
ステップ 6	**ポーリングのタイム アウトを設定します。**1 つでもデバイスがポーリングのタイム アウトまでに応答できなかった場合、Performance Monitor はすべてのデバイスのポーリングを停止します。タイム アウトのデフォルトは 30 秒です。低速の WAN リンク経由でポーリングを行う場合は、この値を大きくする必要があります。「ポーリングのタイム アウトの設定」（P.2-18）を参照してください。

必要な高レベルのタスクを完了すると、デバイスをモニタしたり、デバイスの操作を実行したりできるようになります。たとえば、次のことを実行できます。

- グループ内のデバイスを整理する。「デバイス グループの管理」（P.11-8）を参照してください。
- 読み込まれたレポートを表示する。第 10 章「トレンド レポートの使用」を参照してください。

ヒント　SNMP などの保護されていないプロトコルをイネーブルにしたときにネットワークを保護するように、ファイアウォール フィルタを設定することを推奨します。

デバイスのブートストラップ

ここで説明するように、Performance Monitor で検証、ポーリング、およびモニタリングできるようにデバイスをセットアップする必要があります。

SSL サービス モジュールのセットアップ

次の表に、SSL サービス モジュールに必要なセットアップ手順を示します。Catalyst 6500 スイッチおよび SSL サービス モジュールの詳細な資料については、Cisco.com を参照してください。

表 2-2　SSL サービス モジュールのセットアップ手順

	タスク
ステップ 1	**RSA キーを生成し、サービス モジュールで SSH をイネーブルにします。** • SSL モジュールに管理ユーザ アカウントが存在していることを確認します。 • SSL モジュールでイネーブル パスワードを設定します。 • RSA キー ペアを生成し、SSH をイネーブルにするには、次のコマンドを使用します。 – **ssl-proxy(config) # ip ssh rsa keypair-name** *ssh-key* – **ssl-proxy(config) # crypto key generate rsa general-keys** *ssh-key* • SSH が正しく設定されていることを確認するには、次のように入力します。 **ssl-proxy# show ip ssh** 次のメッセージが表示されます。 **SSH Enabled - version 1.5**

ルータのセットアップ

次の表に、サポートされる Cisco ルータに必要なセットアップ手順を示します。Cisco ルータの詳細な資料については、Cisco.com を参照してください。

表 2-3　ルータのセットアップ手順

	タスク
ステップ 1	**SNMP をイネーブルにして、コミュニティ ストリングをセットアップします。**SNMP は検証、ポーリング、およびモニタリングに必要です。 コンフィギュレーション モードに切り替えて、**snmp community** *community_string* **ro** と入力します。*community_string* は割り当てるコミュニティ ストリング（読み取り専用）です。 **注意**　SNMP はセキュアなプロトコルではありません。SNMP トラフィックを保護するため、ファイアウォール フィルタを作成することを推奨します。
ステップ 2	（任意）**システム名、連絡先、場所の変数を設定します。**Performance Monitor で、これらの変数が [View Device Detail] ウィンドウに表示されます。コンフィギュレーション モードに切り替えて、次のコマンドを使用します。 • システム名を設定するには、**hostname** *name* と入力します。 • システムの連絡先を設定するには、**snmp contact** *contact* と入力します。 • 場所を設定するには、**snmp location** *location* と入力します。
ステップ 3	**SNMP トラップをイネーブルにします。**コンフィギュレーション モードに切り替えて、次のコマンドを使用します。 **snmp-server host** *ip_address* **version 2c public ipsec isakmp snmp** *ip_address* は Performance Monitor をインストールしたサーバの実際の IP アドレスです。 **snmp-server enable traps snmp linkdown linkup** **snmp-server enable traps isakmp policy add** **snmp-server enable traps isakmp policy delete** **snmp-server enable traps ipsec cryptomap add** **snmp-server enable traps ipsec cryptomap delete** **snmp-server enable traps ipsec cryptomap attach** **snmp-server enable traps ipsec cryptomap detach** **snmp-server enable traps ipsec tunnel start** **snmp-server enable traps ipsec tunnel stop**
ステップ 4	**HTTPS をイネーブルにします。**コンフィギュレーション モードに切り替えて、**ip http secure-server** と入力します。 HTTPS をイネーブルにしている場合に限り、Performance Monitor で Easy VPN および DMVPN のセッションをモニタできます。

Catalyst 6500 スイッチのセットアップ

次の表に、IPSec VPN サービス モジュールまたは CSM サービス モジュールが動作している Catalyst 6500 スイッチに必要なセットアップ手順を示します。Catalyst 6500 スイッチおよび IPSec VPN サービス モジュールまたは CSM サービス モジュールの詳細な資料については、Cisco.com を参照してください。

表 2-4　Catalyst 6500 スイッチのセットアップ手順

	タスク
ステップ 1	**SNMP をイネーブルにして、コミュニティ ストリングをセットアップします。**SNMP はポーリング、およびモニタリングに必要です。 コンフィギュレーション モードに切り替えて、**snmp community** *community_string* **ro** と入力します。*community_string* は割り当てるコミュニティ ストリング（読み取り専用）です。 **注意**　SNMP はセキュアなプロトコルではありません。SNMP トラフィックを保護するため、ファイアウォール フィルタを作成することを推奨します。
ステップ 2	（任意）**システム名、連絡先、場所の変数を設定します。**Performance Monitor で、これらの変数が [View Device Detail] ウィンドウに表示されます。コンフィギュレーション モードに切り替えて、次のコマンドを使用します。 • システム名を設定するには、**hostname** *name* と入力します。 • システムの連絡先を設定するには、**snmp contact** *contact* と入力します。 • 場所を設定するには、**snmp location** *location* と入力します。
ステップ 3	**CSM サービス モジュールの SNMP トラップをイネーブルにします。**コンフィギュレーション モードに切り替えて、次のコマンドを使用します。 **snmp-server enable traps slb real.** **snmp-server enable traps snmp.** **snmp-server host** *ip_address* **traps version 2 public casa slb snmp,** *ip_address* は Performance Monitor をインストールしたサーバの実際の IP アドレスです。
ステップ 4	**IPSec VPN サービス モジュールの SNMP トラップをイネーブルにします。**コンフィギュレーション モードに切り替えて、次のコマンドを使用します。 **snmp-server host** *ip_address* **version 2c** *community_string* **ipsec isakmp snmp** *ip_address* は Performance Monitor をインストールしたサーバの実際の IP アドレスで、*community_string* は割り当て済みのコミュニティ ストリング（読み取り専用）です。 **snmp-server enable traps snmp linkdown linkup** **snmp-server enable traps isakmp policy add** **snmp-server enable traps isakmp policy delete** **snmp-server enable traps ipsec cryptomap add** **snmp-server enable traps ipsec cryptomap delete** **snmp-server enable traps ipsec cryptomap attach** **snmp-server enable traps ipsec cryptomap detach** **snmp-server enable traps ipsec tunnel start** **snmp-server enable traps ipsec tunnel stop**

ASA アプライアンス、PIX デバイス、およびファイアウォール サービス モジュールのセットアップ

次の表に、ASA アプライアンスと PIX ファイアウォール、ファイアウォール サービス モジュールが動作している Catalyst 6500 スイッチに必要なセットアップ手順を示します。これらのデバイスおよび技術の詳細な資料については、Cisco.com を参照してください。

表 2-5　ファイアウォールのセットアップ手順

	タスク
ステップ 1	**Performance Monitor サーバをファイアウォール アプライアンス、デバイス、およびモジュールの SNMP ホストとして指定します。**ファイアウォール コマンドラインで **snmp-server host inside** *ip_address* コマンドを入力します。*ip_address* は Performance Monitor をインストールしたサーバの実際の IP アドレスです。 **注意**　SNMP はセキュアなプロトコルではありません。SNMP トラフィックを保護するため、ファイアウォール フィルタを作成することを推奨します。
ステップ 2	**Performance Monitor サーバをポーリング対象の HTTP ホストとして指定します。**ファイアウォール コマンドラインで **http** *ip_address netmask if_name* と入力します。 • *ip_address* は Performance Monitor をインストールしたサーバの IP アドレスです。 • *netmask* は、サブネット アドレスに使用される IP アドレスのビット数を示すために IP で使用される、32 ビットのアドレス マスクです。 • *if_name* はインターフェイスの名前です（**inside** など）。 netmask を使用すると、サブネット全体を HTTP ホストとして指定できます。たとえば、HTTP ホストとして 171.69.74.0 を指定するには、**http: 171.69.74.0 255.255.255.0 inside** と入力します。
ステップ 3	**HTTPS ポーリングをイネーブルにします。**ファイアウォール コマンドラインで **http server enable** と入力します。 **（注）**　**http server enable** コマンドを使用しても、このデバイスでセキュアな HTTPS サーバをイネーブルにできます。

表 2-5　ファイアウォールのセットアップ手順（続き）

タスク
ステップ 4　**Syslog を設定します。**メッセージがすべての設定済みサーバ ホストに送信されます。エラーは実稼動環境だけで記録することを推奨します。ファイアウォール コマンドラインから Syslog ロギングをディセーブルにするには、**no logging on** と入力します。 • ファイアウォール コマンドラインから Syslog ロギングをイネーブルにするには、**logging on** と入力します。 • ファイアウォールでクロックを設定するには、**clock set** *hh:mm:ss* {*day month* | *month day*} *year* と入力します。 • Syslog メッセージでタイムスタンプをイネーブルにするには、**logging timestamp** と入力します。 • ログレベルを設定するには、**logging trap** *level* と入力します。*level* は、該当する最も低い重大度レベルです。たとえば、**logging trap error** と入力すると、重大度レベルが error（レベル 3）から emergency（レベル 0）の間のすべてのメッセージが記録されます（Syslog メッセージには、次の重大度レベルがあります。0 : Emergency、1 : Alert、2 : Critical、3 : Error、4 : Warning、5 : Notification、6 : Informational、7 : Debugging)。 **（注）** ログレベルを低く設定しすぎると、多数のメッセージがトリガーされるため、ファイアウォールのパフォーマンスが低下する可能性があります。*error* 重大度レベルを使用することを推奨します。 • Performance Monitor をインストールしたサーバとして Syslog サーバ ホストを設定するには、**logging host** *if_name ip_address* と入力します。*if_name* はインターフェイス名で（たとえば、**dmz**）、*ip_address* は Performance Monitor をインストールしたサーバの IP アドレス（たとえば、**logging host dmz 10.1.20.111**）です。複数の Syslog のサーバ ホストを設定できます。

VPN 3000 コンセントレータのセットアップ

次の表に、VPN 3000 コンセントレータに必要なセットアップ手順を示します。

VPN 3000 コンセントレータの詳細な資料については、Cisco.com を参照してください。VPN 3000 Concentrator Series Manager アプリケーションの詳細マニュアルは、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』および『*VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*』を参照してください。

表 2-6　VPN 3000 コンセントレータのセットアップ手順

	タスク
ステップ 1	**VPN 3000 Concentrator Series Manager（4.01 以前のリリース）の HTTPS をイネーブルにします。** VPN 3000 Concentrator Series Manager では HTTP 接続と HTTPS 接続の両方がサポートされますが、ベスト プラクティスとして HTTPS の使用を推奨します。HTTPS 接続には SSL 認証が必要です。 1. VPN コンセントレータと同じプライベート ネットワーク内の、PC またはワークステーションでブラウザを開きます。 2. ブラウザの [Address] または [Location] フィールドで、**https://***address* と入力します。*address* はコンセントレータのプライベート インターフェイスの IP アドレス（たとえば、https://10.10.147.2）です。次に、Enter を押します。 3. ブラウザに VPN 3000 Concentrator Series Manager のログイン プロンプトが表示されない場合は、コンセントレータに telnet で接続（または直接アクセス）してください。CLI メニューから、[Configuration] > [System] > [Management Protocols] > [HTTP/HTTPS] を選択します。[Enable HTTPS] を選択します。変更を保存して適用します。
ステップ 2	**VPN 3000 Concentrator Series Manager（4.1 以降のリリース）の HTTPS をイネーブルにします。**ブラウザまたはコンセントレータ CLI のいずれかを使用して、コンセントレータで HTTPS をイネーブルにできます。HTTPS 接続には SSL 認証が必要です。 • ブラウザから HTTPS をイネーブルにするには、標準 HTTP セッションから VPN 3000 Concentrator Series Manager にログインし、[Configuration] > [Tunneling and Security] > [SSL] > [HTTPS] を選択します。[Enable] チェックボックスをオンにして、[Apply] をクリックします。 • CLI から HTTPS をイネーブルにするには、コンセントレータに telnet 接続（または直接アクセス）し、CLI メニューから [Configuration] > [Tunneling and Security] > [SSL] > [HTTPS] > [Enable/Disable HTTPS] を選択します。次に、[Enable HTTPS] を選択し、変更を保存します。

表 2-6　VPN 3000 コンセントレータのセットアップ手順（続き）

	タスク
ステップ 3	**VPN 3000 Concentrator Series Manager（4.1 以降のリリース）の HTTPS 管理セッションをイネーブルにします。** 1. VPN コンセントレータと同じプライベート ネットワーク内の、PC またはワークステーションでブラウザを開きます。 2. ブラウザの [Address] または [Location] フィールドで、**https://***address*/**admin** と入力します。*address* はコンセントレータの IP アドレスです。次に、Enter を押します。 3. VPN 3000 Concentrator Series Manager のログイン プロンプトが表示される場合、管理ユーザのユーザ名と大文字と小文字が区別されるパスワード（一連のアスタリスクとして表示される）を入力し、[Login] をクリックします。 4. [Configuration] > [Interfaces] を選択し、インターフェイス名をクリックします。 5. 選択するインターフェイスは、[Importing Devices] ウィザードで IP アドレスを入力するインターフェイスにする必要があります。「Importing Devices ウィザードを使用したデバイスのインポートまたは追加」（P.2-9）を参照してください。 6. [WebVPN] タブをクリックし、[Allow Management HTTPS Sessions] チェックボックスをオンにします。 7. [Apply] をクリックします。
ステップ 4	**SNMP をイネーブルにします。** 1. この表の説明のとおり、VPN 3000 Concentrator Series Manager にログインします。 2. （任意）コミュニティ ストリングが設定されていない場合は、[Configuration] > [System] > [Management Protocols] > [SNMP Communities] を選択し、[Add] をクリックします。 3. コミュニティ ストリングを入力し、[Add] をクリックして、[Save Needed] をクリックします。 4. [Configuration] > [System] > [Management Protocols] > [SNMP] を選択します。 5. [Enable] チェックボックスをオンにして、[Apply] をクリックします。 **注意**　SNMP はセキュアなプロトコルではありません。SNMP トラフィックを保護するため、ファイアウォール フィルタを作成することを推奨します。
ステップ 5	**XML インターフェイスをイネーブルにします。** すべてのリモート アクセス VPN クラスタ内で少なくとも 1 つの VPN コンセントレータに対して、XML インターフェイスをイネーブルにする必要があります。クラスタに含まれないコンセントレータでは、XML インターフェイスをイネーブルにする必要はありません。 1. この表の説明のとおり、VPN 3000 Concentrator Series Manager にログインし、[Configuration] > [System] > [Management Protocols] > [XML] を選択します。 2. [Enable] チェックボックスをオンにして、[Apply] をクリックします。
ステップ 6	**linkup トラップと linkdown トラップを設定します。** 1. この表の説明のとおり、VPN 3000 Concentrator Series Manager にログインし、[Configuration] > [System] > [Events] > [Classes] を選択して、[Add] をクリックします。 2. [Class Name] リストから [IP] を選択します。 3. [Severity to Trap] リストから [1-3] を選択し、[Add] をクリックします。 4. [Configuration] > [System] > [Events] > [Trap Destinations] を選択し、[Add] をクリックします。 5. [Destination] フィールドで、Performance Monitor をインストールしたサーバの IP アドレスを入力します。 6. [SNMP Version] リストから [SNMPv2] を選択し、[Add] をクリックします。

表 2-6　VPN 3000 コンセントレータのセットアップ手順（続き）

	タスク
ステップ 7	**Syslog を設定します。** [Reports] タブの User Session Report 機能は、VPN コンセントレータで Syslog をイネーブルにしている場合にだけ動作します。 1. この表の説明のとおり、VPN 3000 Concentrator Series Manager にログインし、[Configuration] > [System] > [Events] > [Classes] を選択して、[Add] をクリックします。 2. [Class Name] リストから [AUTH] を選択し、[Enable] チェックボックスをオンにします。 3. [Severity to Syslog] リストから [1-5] を選択し、[Add] を 2 回クリックします。 4. [Class Name] リストから [IKE] を選択し、[Enable] チェックボックスをオンにします。 5. [Severity to Syslog] リストから [1-5] を選択し、[Add] をクリックします。 6. [Save Needed] をクリックし、[OK] をクリックします。 7. [Configuration] > [System] > [Events] > [Syslog Servers] を選択し、[Add] をクリックします。 8. [Syslog Server] フィールドで、Performance Monitor をインストールしたサーバの IP アドレスを入力し、[Add] をクリックします。 9. （任意）Performance Monitor がコンセントレータで Syslog メッセージを送信する唯一のアプリケーションである場合、このアプリケーション自体のパフォーマンスを向上するには、[Configuration] > [System] > [Events] > [General] を選択し、[Severity to Syslog] リストから [None] を選択して、[Apply] をクリックします。 10. [Enable] チェックボックスをオンにして、[Apply] をクリックします。

IPSec VPN 共有ポート アダプタ（VPN SPA）のセットアップ

次の表に、VPN SPA に必要なセットアップ手順を示します。

表 2-7　VPN SPA のセットアップ手順

	タスク
ステップ 1	**HTTPS をイネーブルにします。**`ip http secure server` と入力します。

Importing Devices ウィザードを使用したデバイスのインポートまたは追加

Performance Monitor ではデバイスとの通信のために、そのデバイスについての情報が必要です。Importing Devices ウィザードを使用してデバイスをインポートするか、または手動でネットワークでサポートされるデバイスの IP アドレス、ホスト名、および読み取り専用のコミュニティ ストリングを入力します。インポートは、デバイス アトリビュートの説明リスト（デバイス グループのメンバシップ リストの場合もある）をインベントリ外から Performance Monitor に転送するためのメカニズムです。

Importing Devices ウィザードのオプションを使用すると、Common Services ベースのサーバ上のカンマ区切り（CSV）ファイルまたは Device Credentials Repository（DCR）からデバイス アトリビュートをインポートできます。また、手動でデバイス アトリビュートを追加することもできます。ウィザードの使用の一般情報については、「ウィザードの使用方法」（P.3-10）を参照してください。

次については、追加、インポート、検証ができません。

- サポートされていないデバイス タイプ。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。
- MCP プロセスが停止しているときは、すべてのデバイス。「MCP プロセスのメンテナンス」（P.3-16）を参照してください。
- ダイナミック IP アドレスを使用するデバイスや、SNMP 値が設定されていないデバイス。
- 正しい SNMP および XML のクレデンシャルが指定され、HTTPS がイネーブルになり、VPN 3000 Concentrator Series Manager が動作している場合を除き、VPN 3000 シリーズ コンセントレータ。

始める前に

デバイスをインポートまたは追加するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Importing Devices] を選択し、[Import] をクリックします。

ステップ 2　次のいずれかの方法を選択してデバイスを追加し、[Next] をクリックします。

- [From CSV File] では、デバイスが含まれるカンマ区切り（CSV）ファイルを使用します。

  デバイス アトリビュートをインポートできるのは、CSV 2.0 形式のカンマ区切り（CSV）ファイルからのみです。有効な CSV の例を表示するには、次のステップで [See sample CSV file] をクリックしてください。Performance Monitor では、CSV ファイルから SSL サービス モジュール アトリビュートをインポートおよび検証できません。

  CSV ファイルからデバイスをインポートできるようにするには、デバイス アトリビュート情報の CSV ファイルを検索するか生成し、Performance Monitor をインストールしたサーバにアップロードする必要があります。多数のエレメント マネジメント システムで、デバイスのインベントリ情報をエクスポートできます。CSV ファイルのインベントリ情報をエクスポートする方法については、お使いの EMS ソフトウェアのマニュアルを参照してください。Performance Monitor にはデフォルトのアップロード ディレクトリまたは設定ディレクトリがありません。
- [Manually Add New Devices] では、特定のデバイス情報を直接入力します。
- [From Device Credentials Repository] では、Common Services の Device Credentials Repository（DCR）からデバイスをインポートします。デバイスをインポートするには、このサーバまたは別のサーバにあらかじめ DCR が配置されている必要があります。また、DCR サーバがマスター サーバとして設定されている必要があります。マスター DCR サーバを設定する方法については、Common Services のオンライン ヘルプを参照してください。

ステップ 3　[From CSV File] を選択した場合は、次の手順に従います。そうでない場合は、次のステップに進みます。

a. アップロードする CSV ファイルの完全なローカル（使用するサーバ上の）パス名を入力し、[Next] をクリックします。

たとえば、c:¥temp¥devicelist.csv と入力します。CSV ファイルで見つけたデバイスの組み合わせを含めるか、除外することができます。

b. 1 つまたは複数のデバイスのチェックボックスをオンにして、インポートするデバイス アトリビュートをマークします。すべてのデバイスを選択するには、カラム見出し行のチェックボックスをオンにします。

c. 選択内容を保存するには、[Next] をクリックします。

d. アトリビュートを選択したデバイスのリストを確認するには、[Next] をクリックします。

ステップ 4　[Manually Add New Devices] を選択した場合は、次の手順に従います。そうでない場合は、次のステップに進みます。

a. [Device Type] リストから、関連するデバイス タイプを選択します。

複数のデバイスを同時に追加する場合、すべてを同じデバイス タイプにする必要があります。そうしないと、Performance Monitor によるポーリング中の問い合わせが不適切になり、ポーリングの結果が信頼できなくなります。別の種類のデバイスを手動で追加するたびに、このステップを実行する必要があります。

b. 追加するデバイスの IP アドレスまたは DNS 名を指定するには、[Device Names/IP Addresses] テキスト ボックスに 1 つまたは複数の IP アドレスまたは DNS 名を入力します。複数のアドレスのエントリは、スペースまたはカンマで区切ります。

c. [Next] をクリックします。

追加するデバイスの SNMP の情報および Telnet ログイン クレデンシャル（該当する場合）を指定できますが、SNMP の再試行回数または SNMP タイムアウト時間がデフォルトよりも多い場合、デバイスの検証およびポーリングに時間がかかります。

d. [Read Community] テキスト ボックスに、read コミュニティ ストリングを指定します。

read コミュニティ ストリングは、指定されたデバイスへの読み取り専用アクセスを可能にするためのパスワードです。すべての read コミュニティ ストリングがすべてのデバイスで同一である場合、[Read Community] テキスト ボックスの 1 つのエントリを複数のデバイスに適用できます。ほとんどのデバイスおよび Performance Monitor のデフォルト エントリは *public* です。お使いのデバイスのコミュニティ ストリングがデフォルトとは異なる場合、検証を開始たり、デバイスを設定したりできるようにするには、正しいコミュニティ ストリングを指定する必要があります。

e. [SNMP Timeout] リストから値を選択します。

これは Performance Monitor で応答を再び促す前にデバイスからの応答を待機する秒数です。最小は 1 秒、最大は 60 秒です。デフォルトは 3 秒です。

f. [SNMP Retries] リストから値を選択します。

これは、Performance Monitor でデバイスがタイムアウトしたと宣言する前に、デバイスとの通信を行う試行回数です。デフォルトは 1 です。

g. 次のいずれかを実行します。

- デバイス上のローカル ユーザ名または TACACS などの外部 AAA サーバを使用する場合、[Username] フィールドに管理ユーザのユーザ名を入力します。ユーザ名を入力すると、その下のフィールドのラベルがそれぞれ [User Password] および [Confirm User Password] に変わります。[User Password] フィールド、[Confirm User Password] フィールドに管理者のパスワードを順に入力します。

（注） ローカル データベースまたは外部 AAA サーバ、またはイネーブル パスワードのどの認証を使用するかに応じて、[User Password] および [Confirm User Password] フィールドは、[Enable Password] および [Confirm Enable Password] フィールドに切り替わります。

- パスワード認証のイネーブルを使用する場合、ユーザ名を空白のままにして、[Enable Password] テキスト ボックスにイネーブル パスワードを入力し、[Confirm Enable Password] フィールドで確認します。

  リモート Telnet 接続を介してデバイスにアクセスする場合、イネーブル パスワードにより、デバイスで特権 *イネーブル モード*がアクティブになります。特定の特権の操作は、デバイスがイネーブル モードで動作している場合だけ実行できます。

h. デバイスで Performance Monitor との安全な通信のために使用できる HTTPS ポート番号を入力します。ポート番号を変更していない場合、このフィールドにデフォルトのポート 443 が表示されます。

セキュリティ アプライアンスでは、同じインターフェイス上で Performance Monitor セッションのために SSL VPN 接続と HTTPS 接続の両方を同時にサポートできます。デフォルトでは HTTPS と SSL VPN の両方でポート 443 を使用します。したがって、同じインターフェイス上で HTTPS と SSL VPN の両方をイネーブルにするには、HTTPS または WebVPN のいずれかに別のポート番号を指定する必要があります。または、別のインターフェイス上で SSL VPN および HTTPS を設定します。

i. 選択内容を保存して次のステップに進むには、[Next] をクリックします。

Performance Monitor に、アトリビュートを追加したデバイスが表示されるため、検証が実行される前にエントリを確認できます。

ステップ 5　[From Device Credentials Repository] を選択した場合、次の手順に従います。そうでない場合は、次のステップに進みます。

a. 次の必要な情報を入力します。

- [Host] : DCR サーバの IP アドレスまたはホスト名。Performance Monitor と同じサーバに DCR インベントリが読み込まれている場合、ループバック IP アドレス 127.0.0.1 を使用できます。
- [Port] : DCR サーバが HTTPS 要求を受信するポート番号。デフォルトのポートは 443 です。
- [Username] : デバイスのエクスポートおよびインポートのための権限を持つユーザのユーザ名。
- [Password] : ユーザ名に関連付けられたパスワード。

b. [Next] をクリックします。

c. 1 つまたは複数のデバイスのチェックボックスをオンにして、インポートするデバイス アトリビュートをマークします。すべてのデバイスを選択するには、カラム見出し行のチェックボックスをオンにします。

d. 選択内容を保存し、アトリビュートを選択したデバイスのリストを確認するには、[Next] をクリックします。

Performance Monitor にデバイスが表示されるため、検証が実行される前にエントリを確認できます。

ステップ 6　このプロセスを完了するには、[Finish] をクリックします。デバイスを追加またはインポートすると、ただちにワンタイム認証ジョブが開始されます。検証については、「デバイスの検証」（P.2-13）を参照してください。

ヒント　CSV ファイルからデバイス アトリビュートをインポートした場合、ここでそのファイルを削除して、ファイルに含まれている機密情報の不法な使用を防ぎます。暗号化されていないファイルに重要なデバイス クレデンシャルが含まれています。このアベイラビリティにより、ネットワークのセキュリティにリスクが生じます。

デバイスの検証

どのような種類のデバイスを検証する場合も、そのデバイスが存在していて到達可能であり、必要な機能やインターフェイスがイネーブルになっていて、適切なクレデンシャルがあり、スタティック（ダイナミックではない）IP アドレスを使用していて、SNMP 値が設定されていることを確認します。デバイスの検証では、VPN 3000 シリーズ コンセントレータで正しい XML クレデンシャルを使用していて、HTTPS がイネーブルになっていて、VPN 3000 コンセントレータ シリーズの Manager がイネーブルになっていることも確認します。

デフォルトでは、デバイスの検証中に Performance Monitor ですべての検証対象のデバイスが管理対象状態に設定されます（ポーリングがイネーブルになります）。デバイスを管理対象外の状態に移行するように選択した場合、そのデバイスのヘルスやパフォーマンスをモニタできるようにするには、再検証する必要があります。

デフォルトでは、デバイスの検証が 1 日に一度、深夜に自動的に実行されます。また、指定した他の時間や間隔で実行することもできます。即時ワンタイム検証はいつでも実行できます。

Performance Monitor では、次のことは検証できません。

- サポートされていないデバイス タイプ。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。
- MCP プロセスが停止しているときは、すべてのデバイス。「MCP プロセスのメンテナンス」（P.3-16）を参照してください。
- ダイナミック IP アドレスを使用するデバイスや、SNMP 値が設定されていないデバイス。
- 正しい SNMP および XML のクレデンシャルが指定され、HTTPS がイネーブルになり、VPN 3000 Concentrator Series Manager が動作している場合を除き、VPN 3000 シリーズ コンセントレータ。

ここでは、デバイス検証のスケジュール方法、完了した検証タスクの結果の確認方法、およびスケジュールされていない検証の実行方法などについて説明します。

- 「デバイス検証のスケジューリング」（P.2-13）
- 「検証タスクの履歴の表示」（P.2-14）

デバイス検証のスケジューリング

選択した時刻にデバイス検証タスクを実行したり、選択した間隔で繰り返すように指定できます。また、即時ワンタイム検証を実行することもできます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Importing Devices] を選択します。

ステップ 2　[Device Validation Tasks] ページで [Revalidate] をクリックし、[Start Time] 領域のリストからオプションを選択します。

ヒント　[Start Time] リストに、[Month]、[calendar date]、[year]、[hour]、および [minute] の値を左から右の順に表示します。

ステップ 3　（任意）特定の間隔で検証を繰り返すには、次の手順に従います。

a. [Repeat] チェックボックスをオンにします。

b. [Every] テキスト ボックスに数値を入力します。

c. リストから、間隔のタイプ（たとえば、[hours]）を選択します。

ステップ 4　次のいずれかを実行します。

- 変更を保存して実装するには、[Apply] をクリックします。
- 変更を破棄するには、[Schedule Validation Task] ページを閉じて、[Device Validation Tasks] ページに戻り、[Cancel] をクリックします。

ヒント　スケジュールされていない検証をすぐに 1 回実行するには、[Run Now] をクリックします。

検証タスクの履歴の表示

過去のデバイス検証の結果を表示できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Importing Devices] を選択します。

Performance Monitor では最近の 15 回分の検証タスクが表示され、それらのステータスが説明されます。

ステップ 2　[Device Validation Tasks] リストでオプション ボタンをクリックし、[Details] をクリックします。

[Validation Task Details] ウィンドウに検証結果の履歴が表示されます。

ステップ 3　次のいずれかを実行します。

- 表示された値が最新のものではないと思われる場合、[Validation Task Details] ウィンドウを更新するには、[Refresh] をクリックします。
- [Validation Task Details] ウィンドウを閉じるには、[OK] をクリックします。

検証ステータス

タスク ステータスの履歴は次のように表示されます。

タスクのステータス メッセージ	注意事項
Success: The task was completed in *t* sec.	変数は次の内容を表します。 • *t* : 指定された検証にかかった秒数。 • *x* : Performance Monitor で検証できなかったデバイスの数。この数には部分的に成功した検証は含まれていません。 • *y* : Performance Monitor で検証を試行したデバイスの数。
Failed: *x* of *y* devices were not imported.The task was completed in *t* sec.	
Partial Success: Some of the VPN 3000 Series Concentrator clusters failed to be validated.The task was completed in *t* sec.	部分的に成功した検証では、Performance Monitor で 1 つまたは複数のデバイスのクラスタ情報を収集できません。これは、Performance Monitor で XML クレデンシャルが正しく入力されなかった場合や、デバイスで XML インターフェイスがディセーブルになっている場合に発生します。

検証の詳細

成功した検証のタスクの詳細メッセージは次の 1 種類だけです。
The device *DNS name* | *IP address* was imported successfully.

このメッセージはサービス タイプやデバイス タイプに関係なく、成功したすべての検証に適用されます。

失敗した検証の検証タスクの詳細メッセージの履歴は、サービス タスクごとに異なります。検証の失敗メッセージは次のように表示されます（汎用メッセージはこの表内のサービスのタイプやデバイス名、またはサポートされるその他のデバイスと IPSec VPN サービス モジュールや CSM サービス モジュールによって提供されるロード バランシング サービスなどのサービスに適用されます）。

サービス タイプ	メッセージ
（全般）	The device *DNS name* | *IP address* could not be imported because the SNMP request timed out.
	The device *DNS name* | *IP address* could not be imported because the object identifier is not supported.
	The device *DNS name* | *IP address* could not be imported.Either HTTPS was not enabled or the credentials are not correct.
	The device *DNS name* | *IP address* could not be imported.The device name could not be resolved into an IP address. **ヒント** デバイスにスタティック IP アドレスが割り当てられていることを確認します。Performance Monitor はダイナミック IP アドレス指定をサポートしていません。
	The device *DNS name* | *IP address* could not be imported.The chassis does not contain any supported services modules. **（注）** Performance Monitor では、スイッチに少なくとも 1 つの サポートされるサービス モジュールが含まれていない場合は、Catalyst 6500 スイッチを検証できません。

サービス タイプ	メッセージ
SSL	The device *DNS name* | *IP address* could not be imported.Either the version of SSL is not supported or the IP address is not for an SSL module.
	The device *DNS name* | *IP address* could not be imported because the SSL module credentials are unknown.
	The device *DNS name* | *IP address* could not be imported because Performance Monitor could not communicate with the SSL module.
	The device *DNS name* | *IP address* could not be imported because the SSL login credentials are not correct.
ファイアウォール	The device *DNS name* | *IP address* could not be imported.Either the firewall HTTPS interface was not enabled or the credentials are not correct.
	The device *DNS name* | *IP address* could not be imported.The device must be imported using the Admin context IP address or DNS name.
ルータ	The device *DNS name* | *IP address* could not be imported because this router does not support the IPSec MIB.
RAS VPN	The device *DNS name* | *IP address* import was partially successful.To monitor the cluster *clustername*, you must import the device *IP address*.
	The device *DNS name* | *IP address* import was partially successful.To monitor the cluster, you must enable the XML interface or enter the correct login credentials. **（注）**　その後、メッセージ「An error occurred when the Router MC group was being created.」が表示されることがあります。
	The device *DNS name* | *IP address* could not be imported.Performance Monitor cannot establish an HTTPS connection with the VPN 3000 Concentrator Series Manager.Please verify that HTTPS is enabled.
	The device *DNS name* | *IP address* could not be imported.Performance Monitor cannot validate the device credentials against the VPN 3000 Concentrator Series Manager.Please verify that you entered the correct device credentials.
	The device *DNS name* | *IP address* could not be imported.Performance Monitor cannot establish an HTTPS connection with the VPN 3000 Concentrator Series Manager: HTTP <*HTTPCode*> - <*HTTPResponse*>.Please verify that Management HTTPS sessions are allowed.
適応型セキュリティ アプライアンス	Some of the ASA Series clusters failed to be validated. **（注）**　ASA クラスタ処理を使用していない場合、このメッセージは表示されません。

Performance Monitor では、少なくとも 1 つのデバイスが検証された場合や、少なくとも 1 つのクラスタが検証されていない場合、次の RAS VPN 検証の詳細が表示されます。

- *x* devices were imported successfully.
- Some of the VPN 3000 Series Concentrator clusters failed to be validated. すべてのリモート アクセス VPN クラスタ内で少なくとも 1 つの VPN コンセントレータに対して、XML インターフェイスをイネーブルにする必要があります。「デバイスのブートストラップ」（P.2-2）を参照してください。
- *y* devices failed to be imported. これらのデバイスをモニタするには、インポートし直す必要があります。

E メール使用のための Common Services の設定

Performance Monitor で E メールによってイベントの通知を送信したり、スケジュールされたレポートを配布できるようにするには、E メール サーバを使用するように Common Services を設定する必要があります。

始める前に

この手順を完了するには、ユーザ ロールが System Administrator または Network Administrator である必要があります。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　Performance Monitor をインストールしたサーバで **https://**<*server_name*>**/cwhp/cwhp.applications.do** ページから [Common Services] > [Server] > [Admin] を選択します。

Common Services の [Admin] ページに新しいブラウザ ウィンドウが開きます。

ステップ 2　TOC で [System Preferences] をクリックし、次の手順を実行します。

a. [SMTP Server] フィールドで **localhost** と入力するか、または IP アドレスを指定するか、あるいは **mailserver.example.com** のように使用する別の E メール サーバの完全修飾 DNS 名を指定します。

b. [CiscoWorks Email ID] フィールドで、**admin@example.com** のように完全修飾された E メールの返信アドレスを入力します。

ステップ 3　[Apply] をクリックします。

SNMP トラップの受信

（注）　Performance Monitor で処理できる SNMP のリストについては、「通知の操作」（P.12-1）を参照してください。

サーバ上の他のアプリケーションが UDP ポート 162 から SNMP トラップを受信している場合は、インストールされた Performance Monitor では SNMP トラップが受信されず、SNMP トラップに基づくイベントに関する情報が表示されません。このような場合、トラップを別のポートに転送するように競合するアプリケーションを設定し、Performance Monitor が別のポートでトラップを受信するように設定する必要があります。

手順

ステップ 1　DOS プロンプト ウィンドウを開くには、[Start] > [Run] を選択し、**cmd** と入力して、[OK] をクリックします。

ステップ 2　コマンドラインに次のように入力します。*$NMSROOT*`¥bin¥perl.exe`
$NMSROOT`¥mcp¥bin¥modifyTrapReceiverPort.pl` *port*

port は Performance Monitor で SNMP トラップを受信する UDP ポートの識別番号で、*$NMSROOT* は Performance Monitor をインストールしたディレクトリ（たとえば、**C:¥Program Files¥CSCOpx**）です。

ステップ 3　Enter を押します。

ポーリングのタイム アウトの設定

1 つのデバイスで結果を返すまでに 30 秒以上かかっただけでも、Performance Monitor はモニタリングがイネーブルになっているすべてのデバイスのポーリングを停止します。Performance Monitor で HTTPS を使用するデバイスからの **show** コマンドの出力を受信しようとすると、デバイス上で 1 つの **show** コマンドの取得に 30 秒以上かかる場合があり、ポーリングが停止してしまいます。この問題は、非常に低速な WAN リンクを通じて Performance Monitor でデバイスのポーリングを行う場合に発生する可能性があります。

CLI コマンドのポーリング タイムアウト期間は、*NMSROOT*¥mcp¥conf¥devices ディレクトリにある device.properties ファイルによって、デフォルトで 30 秒に設定されます。*NMSROOT* は Performance Monitor をインストールしたディレクトリ名です。デバイスのポーリングに長い時間がかかる場合は、device.properties ファイルの次の行を修正して、タイムアウト値を変更してください。

Polling.CLIQuery.Timeout=*timeout_value*

timeout_value はポーリング タイムアウト期間です（秒単位）。

CHAPTER 3

スタートアップ ガイド

ここでは、Performance Monitor の使用を開始するにあたって役に立つ内容を記載します。

自動アップデート サーバへのログインと終了

Cisco Security Management Suite のホームページを使用して、Performance Monitor にログインします。また、このホームページを使用すると、Security Manager クライアントをインストールしたり、Common Services、Auto Update Server、RME、および Common Services にインストールされている他のソフトウェアにアクセスすることもできます。

手順

ステップ 1 Web ブラウザで、次のいずれかの URL を開きます。ここで *PMServer* は、Performance Monitor がインストールされているコンピュータの名前です。[Security Alert] ウィンドウではすべて [Yes] をクリックします。

- SSL を使用しない場合は、http://*PMServer*:1741
- SSL を使用する場合は、https://*PMServer*:443

Cisco Security Management Suite のログイン画面が表示されます。このページで、JavaScript とクッキーがイネーブルになっていることと、使用している Web ブラウザがサポート対象のバージョンであることを確認します。Security Manager を実行するためのブラウザの設定方法については、『*Installation Guide for Cisco Security Manager*』を参照してください。

（注） セキュリティを確保するためには SSL の使用を推奨します。

ステップ 2 Cisco Security Management Suite サーバに、自分のユーザ名とパスワードでログインします。最初にサーバをインストールしたときは、ユーザ名 **admin** と、製品のインストール時に定義したパスワードを使用します。

ステップ 3　ログインすると Cisco Security Management Suite のホームページが開きます。このホームページには、サーバにインストールされているスイートのアプリケーションがリストされます。Performance Monitor を実行しているサーバの、少なくとも次の機能にアクセスできます。製品のインストール内容によっては、他の機能も使用できる場合があります。

- Performance Monitor：この項目をクリックすると、Performance Monitor インターフェイスが開きます。
- Server Administration：この項目をクリックすると、CiscoWorks Common Services Server のページが開きます。CiscoWorks Common Services は、サーバ管理の基礎となるソフトウェアです。これを使用して、サーバの保守とトラブルシューティング、ローカル ユーザの定義など、バックエンド サーバ機能の設定および管理を行います。
- CiscoWorks リンク（ページ右上）：このリンクをクリックすると、CiscoWorks Common Services のホームページが開きます。このページから Performance Monitor にアクセスすることもできます。

ステップ 4　アプリケーションを終了するには、画面右上隅の [Logout] をクリックします。サーバのいずれかのウィンドウ（[Performance Monitor] ウィンドウ、Security Manager のホームページなど）からログアウトすると、すべてのウィンドウからログアウトしたことになります。

ログイン セッションは、非アクティブな状態が 2 時間続くとタイムアウトになります。

ユーザの権限について

サーバは、ログインするユーザごとにユーザ名とパスワードを認証します。Performance Monitor を起動すると、Common Services が、ユーザに割り当てられているロールに基づいて、ユーザに実行が許可されているタスクと操作を識別します。タスクおよび関連するインターフェイス エレメントの一部は、許可されていないユーザには表示されません。システム管理権限を持つユーザはすべての機能にアクセスできますが、他のユーザには一部の機能しか表示されません。たとえば、システム管理者は、スケジュールされている E メール レポート ジョブを、ジョブの作成者が誰かにかかわらずすべて表示できますが、他のユーザは、自分が作成した E メール ジョブだけを表示できます。

Performance Monitor のユーザ認証と権限付与は、Common Services で行われます。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。

（注）　Cisco ACS を使用してサーバでユーザ アカウントを管理するように、Common Services を設定することができます。Common Services オンライン ヘルプの「Configuring CiscoWorks Common Services to use Cisco Secure ACS Authorization and Authentication」の項を参照してください。

Common Services には、7 つのユーザ ロールが用意されています。次の表に、これらのロールと、Performance Monitor のタスクおよびインターフェイス エレメントの対応関係を示します。

表 3-1　Common Services のユーザ ロールと Performance Monitor ユーザ権限の対応

Common Services のロール	許可されるタスク	表示されるインターフェイス タブ
System Administrator	すべてのタスク（読み取り / 書き込み）。	すべてのタブとすべてのオプション。
Network Administrator（キャパシティ プランナー）	Network Operator のすべての権限、および RAS ユーザ セッションの終了権限。	すべてのタブ。 ただし、[Admin] タブのすべてのオプションは、[My Profile] オプションを除き、このユーザ ロールには表示されません。

表 3-1　Common Services のユーザ ロールと Performance Monitor ユーザ権限の対応（続き）

Common Services のロール	許可されるタスク	表示されるインターフェイス タブ
Network Operator	• リアルタイム モニタリング。 • インベントリ（読み取り / 書き込み）。 • ポーリング ポリシー（読み取り / 書き込み）。 • 障害管理（読み取り / 書き込み）。 • 履歴レポートのスケジューリング（読み取り / 書き込み）。 • 履歴レポートの表示（読み取り専用）。	すべてのタブ。 ただし、[Admin] タブのすべてのオプションは、[My Profile] オプションを除き、このユーザ ロールには表示されません。
Approver	• リアルタイム モニタリング。 • インベントリ（読み取り / 書き込み）。 • ポーリング ポリシー（読み取り / 書き込み）。 • 障害管理（読み取り / 書き込み）。 • 履歴レポートのスケジューリング（読み取り / 書き込み）。 • 履歴レポートの表示（読み取り専用）。	[Summary]、[Monitor]、[Reports]、および [Admin]。 ただし、[Admin] タブのすべてのオプションは、[My Profile] オプションを除き、このユーザ ロールには表示されません。
Help Desk	• リアルタイム モニタリング。 • インベントリ（読み取り専用）。 • ポーリング ポリシー（読み取り専用）。 • 障害管理（読み取り専用）。	[Summary]、[Monitor]、および [Admin]。 ただし、[Admin] タブのすべてのオプションは、[My Profile] オプションを除き、このユーザ ロールには表示されません。
Export Data Developer	（注）　これらの Common Services のユーザ ロールは、Performance Monitor のタスクと直接対応していません。デフォルトでは、これらのロールのユーザは、ヘルプ デスクのスタッフと見なされます。	

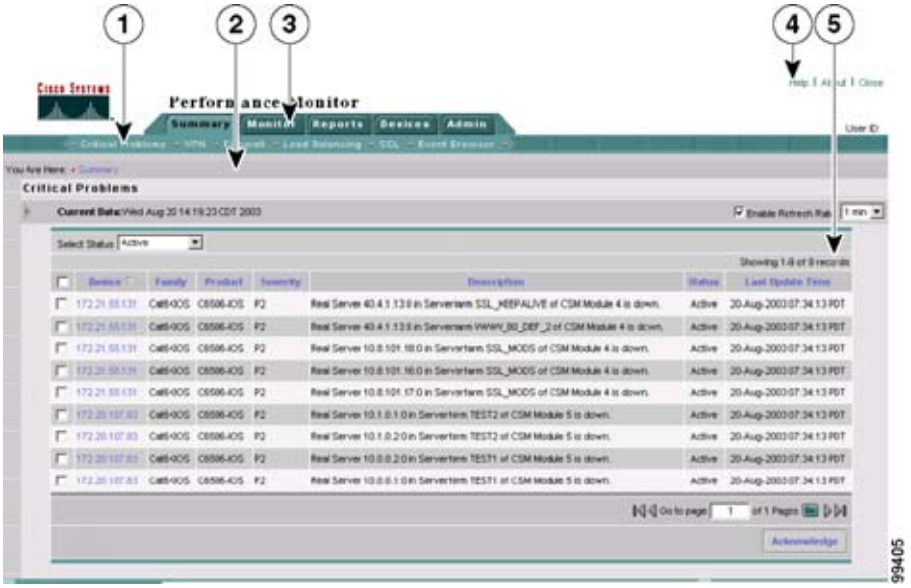
Performance Monitor インターフェイスの使用方法

Performance Monitor は、非アクティブな状態が 2 時間続くとタイムアウトになります。タイムアウトになった場合は、再度ログインする必要があります。このタイムアウトは設定できません。ここでは、よく使用するインターフェイス エレメントについて説明します。

ユーザ インターフェイスについて

次の図に、Performance Monitor のインターフェイスに含まれる一般的なエレメントを示します。

図 3-1　Performance Monitor の一般的なインターフェイス エレメント



1	*オプション バー*: 選択されているタブで使用できるオプションが表示されます。
2	パス バー: たとえば [You Are Here] の次に、選択されているタブ、オプション、およびページ（該当する場合）がリストされます。

3	タブ: ここから Performance Monitor の各機能へアクセスできます。タブをクリックすると、そのタブのオプションが表示されます。 • [Summary] : クリティカル エラー（P1 および P2）を表示したり、サポート対象のサービスに関して要約したグラフおよび表を表示したり、または、プリセット フィルタがないイベント ブラウザを開いたりします。 • [Monitor] : リモート アクセス VPN、サイト間 VPN、ファイアウォール サービス、ロード バランシング サービス、および SSL プロキシ サービスの状態をモニタします。 • [Reports] : VPN、ファイアウォール サービス、ロード バランシング サービス、および SSL プロキシ サービスに関する履歴レポートの設定および生成を行います。 • [Devices] : デバイスの検証およびグループ化を管理します。 • [Admin] : モニタ対象のサービスで、障害またはしきい値超過が発生した場合の自動通知を設定します。しきい値および間隔を設定します。ログ ファイルの表示および設定を行います。デフォルト ページを設定します。
4	ツール バー: [Close]、[Help]、および [About] リンクが含まれています。 • [Help] : アクティブなページに関する状況依存ヘルプが表示されます。また、ここから他のヘルプ トピックにアクセスすることもできます。 • [About] : Performance Monitor のバージョンおよび著作権情報が表示されます。 • [Close] : すべての Performance Monitor ウィンドウを閉じます。
5	ページ: Performance Monitor から提供された情報をユーザが確認するための表示領域です。また、この領域ではアプリケーション タスクを実行します。

インターフェイスのアイコンについて

図 3-2 に、次の特殊アイコン以外のすべての Performance Monitor インターフェイス アイコンを示します。また、各アイコンの用途および正しい使用方法についても説明します。

- 特定の種類のデバイスを示すアイコン（図 3-3（P.3-6）を参照）。
- 相互関係のある、特定の範囲のページ間を移動できるようにするアイコン（図 3-5（P.3-8）を参照）。

図 3-2　一般的なアイコン

1	アラート（アクティブ）: 2 つの場所の、どちらかに表示されます。重大な問題または障害を示します。このアイコンをクリックすると、次のようになります。 • 説明の表の [Alert] カラムにあるアイコンの場合、関連するサービス、デバイス、またはモジュールのイベント ブラウザが開きます。「イベント ブラウザの操作」（P.3-12）を参照してください。 • [Summary] タブのグラフまたはチャートの行の上にあるアイコンの場合、[Critical Problems] の要約が表示されます。「クリティカルな問題の要約の操作」（P.4-2）を参照してください。 **ヒント** 特定のアラート アイコンをクリックした場合にどちらの動作になるかわからないときは、クリックする前に、そのアイコンの上にポインタを移動してください。[Critical Problems] の要約が表示されるアイコンの場合、ツールチップに [Critical Problems] と表示されます。 **（注）** イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページまたはイベント ブラウザ ウィンドウに表示され続けます。
2	アラート（非アクティブ）: [Summary] タブのグラフまたはチャートの行の上に表示されます。重大な問題または障害がないことを示します。このアイコンをクリックすると [Critical Problems] の要約が表示されます。
3	分離 : [Summary] タブのページ内のグラフの行の上に表示されます。*ダッシュボード*（「基本概念について」（P.1-3）を参照）などの関連するグラフを個別に分離できることを示します。このアイコンをクリックするとダッシュボードが開きます。
4	レポートの印刷 : 履歴のトレンドまたはユーザ セッションに関して生成されたレポート内に表示されます。このアイコンをクリックするとレポートが印刷されます。
5	レポートのヘルプ : 履歴のトレンドまたはユーザ セッションに関して生成されたレポート内に表示されます。このアイコンをクリックするとオンライン ヘルプが表示されます。

デバイス アイコンについて

一部のページでは、Performance Monitor は、アイコンを使用してネットワーク内の検証済みデバイスを表します（図 3-3）。

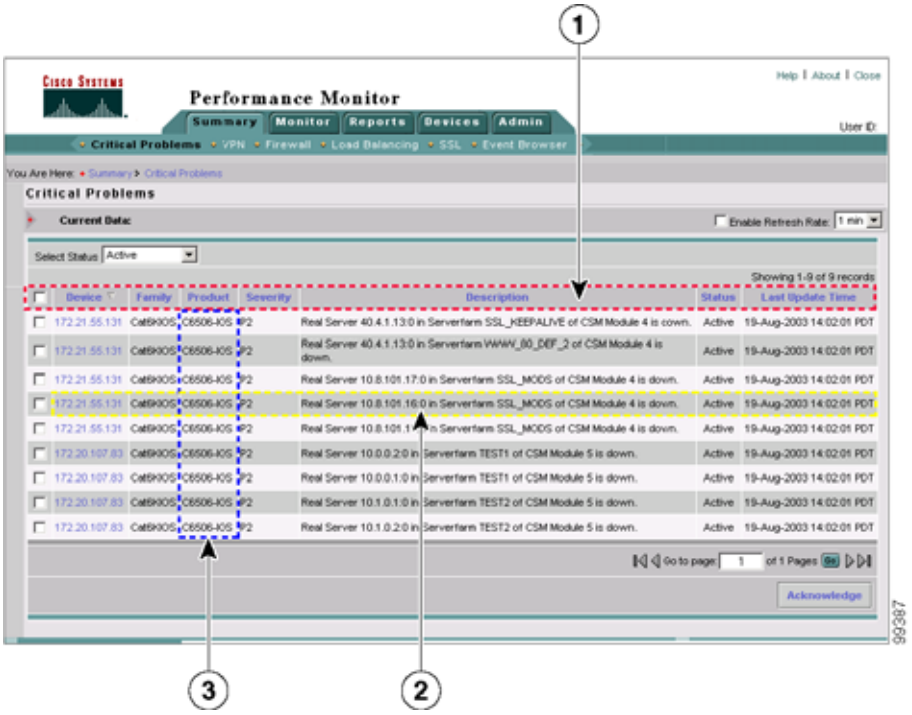
図 3-3　デバイス アイコン

1	ルータ。	5	SSL サービス モジュール。
2	VPN コンセントレータ。	6	到達不能なデバイス。
3	ファイアウォール（PIX、ASA、またはサービス モジュール）。	7	モニタリングがディセーブルになっているデバイス。
4	コンテンツ スイッチング サービス モジュール。		

Performance Monitor テーブルの使用方法

テーブルには、デバイスや重大な問題などの項目が含まれており、テーブルのあるページでは、ほとんどの場合、特定のタスクをオプションで実行することができます。一般的に Performance Monitor のテーブルには、他のアプリケーションで使用するテーブルとはいろいろと異なる点があります。また、場合によっては、ネットワーク デバイスおよびサービスに関するトラブルシューティング機能などの見慣れない内容が含まれていることがあります。また、複数ページにまたがるテーブルもあります。

図 3-4　　テーブルの例



1	カラム見出し : カラム見出しは、テーブル データの上に、テーブルの幅全体に表示されます。各カラム見出しは、それぞれのカラムにある情報の種類を示しています。通常、カラム見出しをクリックすると、そのカラムの内容でテーブル全体をソートし直すことができます。
2	行 : 1 つの行に 1 つの項目についての記述があり、各行には項目に関する複数の情報が入っています。たとえば、単一のデバイスに関する 1 行には、そのデバイスの IP アドレス、デバイス ファミリ（VPN 3000 コンセントレータなど）、およびアラーム状態がリストされます。
3	カラム : カラムには、複数の項目に同じように該当する、単一のカテゴリの情報が示されます。たとえば、あるカラムには、リストされている全デバイスの IP アドレス情報やアラーム状態がリストされます。カラム内の情報が測定値である場合、ほとんど必ず次のいずれかによって示されます。 • デルタ : あるポーリング サイクルと次のポーリング サイクルとの間の差。 • 整数値 : カウント値（デバイス上のアクティブな VPN トンネルの数、ユーザ セッションの正確な所要時間など）。

複数ページにまたがるテーブル

すべての関連データを単一ページに表示するには行数が足りないという場合に、単一のテーブルが複数ページにまたがることがあります。ほとんどの場合、テーブルが複数ページにまたがる理由は次のいずれかです。

- [Rows per page] リストで選択した行数が少なすぎた。
- [Rows per page] リストの最大値（40 行）を使用しても、テーブル全体が 1 ページに収まらない。

このような場合は、テーブルの下のナビゲーション ボタン（図 3-5（P.3-8））を使用するか、または [Go to page] テキスト ボックスにテーブルのページ番号を入力し、[Go] をクリックします。

図 3-5　テーブルのナビゲーション ボタン

1	クリックすると、複数ページあるテーブルの最初のページが表示されます。
2	クリックすると、複数ページあるテーブルの前のページが表示されます。
3	クリックすると、複数ページあるテーブルの次のページが表示されます。
4	クリックすると、複数ページあるテーブルの最後のページが表示されます。

テーブルのチェックボックス

編集できる項目またはアクションを実行できる項目に関する行には、チェックボックスが表示されます。項目を行単位で選択することも、カラム見出し内のチェックボックスを選択して全項目を選択することもできます。

テーブルのアクション

テーブル内の項目を編集する場合は、その項目のチェックボックスを選択し、適切なアクション ボタンをクリックします。選択されている項目と関係のないボタン、または権限のないボタンはグレー表示されます。

テーブルの一般エレメント

表 3-2 に、Performance Monitor のほとんどのテーブルでよく使用されるエレメントを示します。

表 3-2　Performance Monitor テーブルの一般エレメント

エレメント	用途または使用手順
[Current Data] のタイムスタンプ	この [Current Data] のタイムスタンプを確認して、表示内容が最新かどうかを判別します。タイムスタンプが新しいほど、精度が高いと見なせます。 CiscoWorks Server の場所にかかわらず、ユーザの場所の時刻とタイムゾーンの省略名が表示されます。
[Enable Refresh Rate] チェックボックス	次のいずれかを実行します。 • 画面の自動リフレッシュを Performance Monitor でグローバルにイネーブルにするには、このチェックボックスを選択します。 • 画面の自動リフレッシュをディセーブルにするには、このチェックボックスを選択解除します。

表 3-2　Performance Monitor テーブルの一般エレメント（続き）

エレメント	用途または使用手順
分のリスト	画面の自動リフレッシュをイネーブルにした場合に、そのリフレッシュの頻度を変更するには、この分のリストから間隔を選択します。 最高頻度は 1 分間隔です。最低頻度は 5 分間隔です。
カラム見出し	カラム見出し内の語をクリックすると、そのカラムでテーブルがソートされます。たとえば、[Device] カラムのあるテーブルで、[Device] カラム見出しをクリックすると、デバイス名または IP アドレスでテーブルがソートされます。 カラム見出し内に三角のイメージがある場合は、その三角をクリックすると、ソート順が逆転します。 **（注）** ハイパーリンクされていないカラム見出しもあります。そのようなカラムの値ではテーブルをソートできません。
[Rows per page] リスト	このリストから行数を選択して、1 ページ内に表示されるテーブルの行の最大数を変更します。選択すると、画面の自動リフレッシュが実行されます。
チェックボックス	アクションの適用対象のエントリを 1 つまたは複数選択します。エントリを個別に選択したり、または全エントリを一括で選択したりできます。 • カラム見出し行内にあるチェックボックスを使用すると、全エントリを一括で選択または選択解除できます（2 ページ以上続くテーブルの場合、アクティブなページにあるエントリだけが選択されます）。 • 1 つのエントリに関する行のチェックボックスを使用すると、そのエントリを個別に選択することができます。 **（注）** アクションを実行する前に、そのアクションの適用対象となるエントリを選択する必要があります。
[Troubleshoot] ボタン	シスコシステムズが開発したトラブルシューティングの情報が、Performance Monitor アプリケーションに組み込まれています。この対話形式のトラブルシューティング ツールは、次の 2 つの方法で、オンラインに限り利用できます。 • [Troubleshoot] ボタン。インターフェイスに表示されている場合（[Troubleshoot] ボタンがないページもあります）。 • Performance Monitor オンライン ヘルプの目次。
[Refresh] ボタン	アクティブなページを手動で 1 回リフレッシュする場合に、[Refresh] をクリックします。 リフレッシュされたページに表示される値は、最新のポーリング サイクルで収集されたデータか、あるいは、デバイスのインターフェイス、実サーバ、またはサイト間 VPN トンネルの状況に関してデバイスから受信されたトラップ情報に基づいています。

Performance Monitor テーブルのオプション タスク

表 3-3 に、多数のテーブル ページにあるオプション タスクを示します。

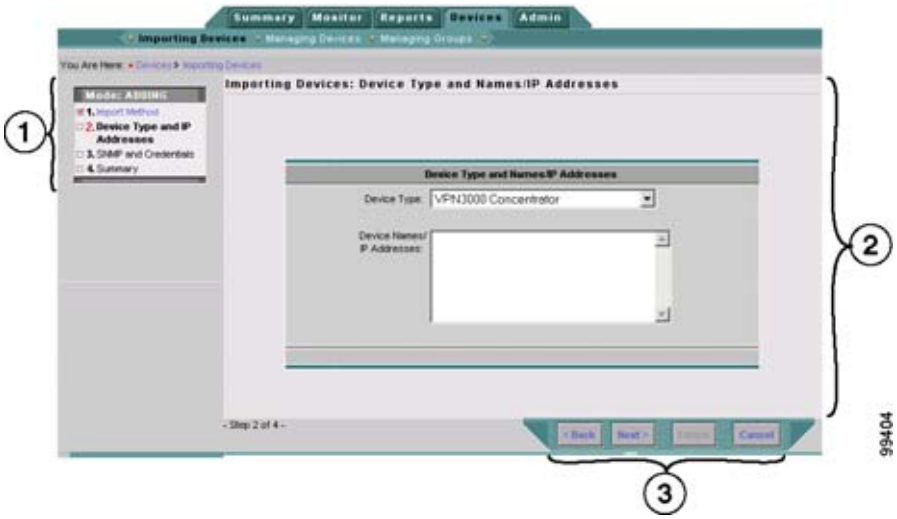
表 3-3　Performance Monitor テーブルのオプション タスク

オプション タスク	手順
カラム内の値に従ってテーブルをソートする。	カラム見出し内の語をクリックすると、そのカラムでテーブルがソートされます。カラム見出し内に三角のイメージがある場合は、その三角をクリックすると、ソート順が逆転します。 （注）　ハイパーリンクされていないカラム見出しもあります。そのようなカラムの値ではテーブルをソートできません。
Performance Monitor 画面のリフレッシュ設定をグローバルに変更、またはアクティブな表示をリフレッシュする。	次のいずれかを実行します。 • 画面の自動リフレッシュをイネーブルにするには、[Enable Refresh Rate] チェックボックスを選択します。 • 画面の自動リフレッシュをディセーブルにするには、[Enable Refresh Rate] チェックボックスを選択解除します。 • 画面の自動リフレッシュがイネーブルになっている場合に、そのリフレッシュの頻度を変更するには、分のリストから間隔を選択します。 • 画面の自動リフレッシュをディセーブルにした場合でも、[Refresh] をクリックすると、画面が 1 回リフレッシュされます。
値表示のタイミングを評価する。	[Current Data] のタイムスタンプを確認して、表示されている値が最新かどうかを判別します。タイムスタンプが新しいほど、精度が高いと見なせます。 CiscoWorks Server の場所にかかわらず、ユーザの場所の時刻とタイムゾーンの省略名が表示されます。

ウィザードの使用方法

ウィザードは、デバイスのインポートや追加などの複雑なタスクの手順を 1 つずつ説明しながら、ユーザが実行できるようにします。図 3-6 に、[Importing Devices] ウィザードの代表的なページを示します。このウィザードのエレメントは、次のとおりです。

図 3-6　ウィザード ページの例



1. ウィザードの手順をリストした目次

2. ウィザードのページ
3. ウィザードのアクション ボタン

目次には、このウィザードに含まれている手順がリストされます。また、完了済みの手順の目次エントリは、特定の手順またはフィールドに素早く戻れるようにリンクされています。ウィザードで作業するときには、順序どおりに手順を完了させる必要があります。順序を変えたり、またはウィザードを途中で終了しようとすると、エラー メッセージが表示され、その操作は拒否されます。ウィザードのアクション ボタンは、選択した手順に応じて変化します。

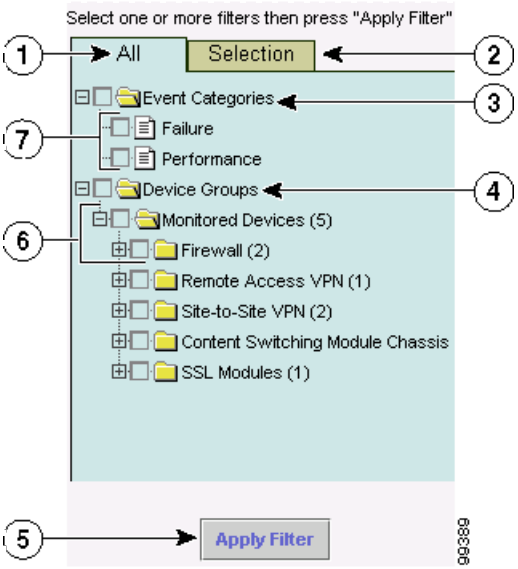
- 最初と最後の手順では、それぞれ [Back] ボタンおよび [Next] ボタンがグレー表示されます。
- 変更を保存しないでウィザードを終了するには、[Cancel] をクリックします。
- 変更を確定してウィザードを終了するには、[Finish] をクリックします。

[Finish] をクリックするまで、Performance Monitor は、ユーザによる選択内容を一切適用しません。[Finish] をクリックしても、ウィザードで設定しなかった手順はすべてスキップされます。ほとんどのウィザードにはデフォルト値が設定されており、スキップした手順にも適用されます。

オブジェクト セレクタの使用方法

オブジェクト セレクタは、フォルダ、サブフォルダ、およびその内容といったフレームワークに基づいており、Performance Monitor のさまざまなページに表示されます。オブジェクト セレクタ内のエレメントは、オブジェクト セレクタの用途に応じて、若干異なります。通常、オブジェクト セレクタには、デバイス グループ、デバイス、および（場合によっては）イベントがネストされたツリーが示され、フィルタリング基準としてデバイスおよびイベントをユーザが選択できるようになっています。

図 3-7　　オブジェクト セレクタのエレメント



1	[All] タブ : このタブで、表示して選択できるものは次のとおりです。 • イベント カテゴリ、デバイス グループ、および個々のデバイス。これによって、イベント ブラウザ ウィンドウに表示される結果をフィルタすることができます。 • デバイス グループ（システム定義またはユーザ定義のもの）および個々のデバイス。次のことを実行できます。 – 設定するレポートの範囲を制限する。 – SNMP 設定およびポーリング用のクレデンシャルを編集する。 – ポーリングをイネーブルまたはディセーブルにする。 – デバイスのプロパティを表示する。 – デバイスを削除する。 • ユーザ定義デバイス グループおよび個々のデバイス。次のことを実行できます。 – ユーザ定義デバイス グループを作成、編集、または削除する。 – デバイス グループの詳細を表示する。
2	[Selection] タブ : [All] タブで選択した全オブジェクトのリストを抜き出して表示できます。選択リストからオブジェクトを削除するには、関連するチェックボックスを選択解除します。
3	Event Categories フォルダ : 選択できるイベントが含まれています。イベント ブラウザ ウィンドウの左側のペインにある Event Categories フォルダの場合、このフォルダをクリックすると、すべてのイベントを選択できます。または、フォルダを展開し、フォルダ内の次のイベント カテゴリのいずれか、または両方を選択することもできます。 • Failure : 状態イベントとも呼ばれる障害イベントは、*Up* と *Down* のように、極端な値だけが存在する状況に関するイベントです。 • Performance : 範囲イベントとも呼ばれるパフォーマンス イベントは、*OK*、*Degraded*、*Overloaded* のように、ある範囲の値が存在する状況に関するイベントです。
4	Device Groups フォルダ : ルート レベルに Monitored Devices フォルダがあります。また、Monitored Devices フォルダ内には、さらにネストされたサブフォルダがあり、これによって、ネットワーク内のさまざまなタイプのモニタ対象デバイスが分類されています。これらのサブフォルダ内には、システム定義のデバイス グループが含まれますが、ユーザ定義のデバイス グループが含まれる場合もあります。デバイスを個別に選択したり、デバイス グループを個別に選択したり、または全デバイス グループを選択したりできます。
5	[Apply Filter] ボタン : 選択内容を適用するには、[Apply Filter] ボタンをクリックします。 **（注）** [Apply Filter] ボタンが表示されないオブジェクト セレクタもあります。その場合は、選択するとすぐに反映されます。
6	[Selection] ツリー内のフォルダまたはサブフォルダの左に、+ 記号または – 記号が表示されることがあります。+ 記号をクリックするとツリー内の該当するレベルが展開し、– 記号をクリックすると縮小します。
7	オブジェクトの横のチェックボックスを選択すると、そのオブジェクトと、その階層内のすべての子ノードが選択されます。オブジェクトを選択解除するには、再度クリックします。 **（注）** アクション ボタンをクリックする前に、オブジェクト セレクタで、少なくとも 1 つのチェックボックスを選択する必要があります。たとえば、レポートを設定する場合、チェックボックスを選択して、レポート対象のデバイスまたはグループを指定する必要があります。

イベント ブラウザの操作

イベントとは、モニタ対象のデバイスまたはコンポーネントに異常な状態が発生し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 ブラウザ ウィンドウを使用すると、イベントを表示し、選択した基準によってイベントをソートしたりフィルタしたりできます。Performance Monitor では、フィルタされたイベント ブラウザおよびフィルタされていないイベント ブラウザのどちらも利用できます。

イベント ブラウザ ウィンドウを開くには、次のいずれかを実行します。

- [Summary] タブで、[Event Browser] オプションを選択します。開いたイベント ブラウザには、サービス タイプまたはイベントが発生したデバイスにかかわらず、ネットワーク内でモニタされたすべてのイベントが表示されます。
- [Summary] タブの [Critical Problems] テーブルで、リンクされているエントリのいずれかをクリックします。開いたイベント ブラウザには、関連するデバイスのイベントだけが表示されます。
- [Monitor] タブのいずれかの目次で、[Event Browser] をクリックします。開いたイベント ブラウザには、関連するサービスに影響するイベントだけが表示されます。
- [Monitor] タブで、[Alert] カラムを含むテーブルにある、ハイパーリンクされたアラート アイコンのいずれかをクリックします。開いたイベント ブラウザには、関連デバイスの関連サービスに影響するイベントだけが表示されます。

イベント ブラウザ ウィンドウを開くと、左側のペインにオブジェクト セレクタがあります。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

次の表に、イベント ブラウザで実行可能な代表的タスクを示します。他のタスクについては、「Performance Monitor テーブルのオプション タスク」（P.3-9）に説明があります。イベント ブラウザ ウィンドウのエレメントの概要については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。

表 3-4　イベント ブラウザ ウィンドウでの代表的なタスク

タスク	手順
イベント カテゴリを使用してイベント リストをフィルタする。	左側のペインでイベント タイプを表示して選択すると、右側のペインの結果をフィルタできます。 **1.** Event Categories フォルダが閉じている場合は、フォルダの左の + 記号をクリックします。 フォルダが展開されます。フォルダには、個別に選択できるイベント カテゴリが含まれています。 **2.** イベント カテゴリの左のチェックボックスを選択して、そのカテゴリを選択します。または、フォルダの左のチェックボックスを選択して、すべてのイベント カテゴリを選択します。 **3.** [Apply Filter] をクリックします。 リフレッシュ後の表示には、選択したカテゴリ（1 つまたは複数）のイベントだけが示されます。
デバイスまたはデバイス グループを使用してイベント リストをフィルタする。	左側のペインでデバイス グループまたは個々のデバイスを表示して選択すると、右側のペインの結果をフィルタすることができます。 **1.** Device Groups フォルダが閉じている場合は、フォルダの左の + 記号をクリックします。 フォルダが展開されます。ネストされたサブフォルダをさらに展開して、デバイス カテゴリや、最終的には個々のデバイスを表示することもできます。 **2.** フォルダの左のチェックボックスを選択して、そのフォルダとすべての子ノードを選択します。または、デバイスの左のチェックボックスを選択して、そのデバイスだけを選択します。 **3.** [Apply Filter] をクリックします。 リフレッシュ後の表示には、選択したデバイスのイベントだけが示されます。
重大度レベルを使用してイベント リストをフィルタする。	重大度レベルの範囲（P1 が最高の重大度で、P5 が最低の重大度）を指定するには、[Select Severity] リストで関連するオプションを選択します。 Performance Monitor はこのフィルタをすぐに適用し、イベント ブラウザが自動リフレッシュされ、フィルタされた結果が表示されます。リフレッシュ後の表示には、指定された範囲の重大度のイベントだけが示されます。

表 3-4　イベント ブラウザ ウィンドウでの代表的なタスク（続き）

タスク	手順
アラーム状態を使用してイベント リストをフィルタする。	アラーム状態を指定するには、[Alarm Status] リストで関連するオプションを選択します。 Performance Monitor はこのフィルタをすぐに適用し、イベント ブラウザが自動リフレッシュされ、フィルタされた結果が表示されます。リフレッシュ後の表示には、指定した 1 つのアラーム状態（[All] を選択した場合は複数のアラーム状態）のイベントだけが示されます。 **（注）** フィルタリングに使用するために、[Alarm Status] リストで選択した内容を、[Event State] リストで選択した内容と組み合わせることはできません。両方のリストで選択した場合、2 番目に選択した内容によって、最初に選択した内容はクリアされて上書きされます。
イベント状態を使用してイベント リストをフィルタする。	右側のペインの [Event State] リストから値を選択します。[Event State] リストで使用できるオプションには、次のような種類があります。 • [Generic]：取り得るすべての状態のスーパーセットがオプションとしてリストされます。 • [Service]：指定されたサービスに関するもの（たとえばサイト間 VPN などで取り得る状態）だけがオプションとしてリストされます。 • [Device]：指定されたデバイスに関するもの（たとえば VPN 3000 コンセントレータなどで取り得る状態）だけがオプションとしてリストされます。 • [Combined Device and Service]：指定のサービスおよび指定のデバイス タイプの両方について、取り得るすべての状態のスーパーセットがオプションとしてリストされます。 **（注）** フィルタリングに使用するために、[Event State] リストで選択した内容を、[Alarm Status] リストで選択した内容と組み合わせることはできません。両方のリストで選択した場合、2 番目に選択した内容によって、最初に選択した内容はクリアされて上書きされます。 Performance Monitor はこのフィルタをすぐに適用し、イベント ブラウザが自動リフレッシュされ、フィルタされた結果が表示されます。
時間範囲を使用してイベント リストをフィルタする。	右側のペインの [Time] リストから値を選択します。 Performance Monitor はこのフィルタをすぐに適用し、イベント ブラウザが自動リフレッシュされ、フィルタされた結果が表示されます。
イベント ID を使用し、単一のイベントを分離して表示する。	Performance Monitor が E メール メッセージを送信して、ユーザにイベントを通知するときに、そのイベントに自動的に割り当てられた連番の ID 番号がユーザに示されます。 イベントの詳細を表示するには、その ID 番号を [Event ID] テキスト ボックスに入力し、[Find] をクリックします。 **（注）** [Event ID] の検索は、それまでのフィルタリングとは関係なく機能します。
検索キーワードまたは用語を使用して、ある説明と一致するイベントを表示する。	Performance Monitor でイベントの説明に使用される、あるテキスト文字列と一致するイベントだけを、個別に表示できます。たとえば、*not accessible*、*failure*、*inbound* などの文字列を説明に含むイベントだけを表示できます。 [Description] テキスト ボックスに文字列を入力します。次に、[Search] をクリックすると、その文字列を説明に含むイベントだけが表示されます。 クエリーでは、大文字と小文字が区別されません。 **（注）** 説明の検索は、それまでのフィルタリングとは関係なく機能します。

イベント ブラウザ ウィンドウ

次の表に、イベント ブラウザ ウィンドウのエレメントを示します。

表 3-5　イベント ブラウザ ウィンドウのリファレンス

エレメント	説明
オブジェクト セレクタ	左側のペインにオブジェクト セレクタがあります。これについては、「オブジェクト セレクタの使用方法」（P.3-11）に説明があります。
[Select Severity] リスト	重大度のレベルまたは範囲を選択できます。リフレッシュ後の表示には、選択内容と一致するイベントだけが示されます。P1 が最高の重大度で、P5 が最低の重大度です。 [All] オプションを選択すると、P1 から P5 までの問題、および重大度がすでに OK に設定された解決済みの問題が表示されます。
[Select Time] リスト	特定の時間枠内で発生したイベントだけに表示を制限できます。
[Event State] リスト	値を選択できます。リフレッシュ後の画面には、特定のイベント状態によってトリガーされたイベントだけが表示されます。 [Event State] カラムまたは [Event State] リスト内のイベント トリガー値は、[Administration] タブのイベント固有のしきい値設定で定義または編集した、次の値と同じです。 • *Up* と *Down* のような対極の値が、障害イベントに適用されます。 • *OK*、*Degraded*、*Overloaded* のようなある範囲内の値が、パフォーマンス イベントに適用されます。 **（注）** [Event State] リスト内の値は、正確には、表示されたイベントの対象であるサービス（1 つまたは複数）によって異なります。[Summary] > [Event Browser] の順に選択した場合、[Event State] リストには、取り得るすべての値が含まれます。それ以外の場合は、関連するサービスに適用される状態だけが表示されます。
[Alarm Status] リスト	アラーム状態を選択できます。リフレッシュ後の表示には、指定したアラーム状態のイベントだけが示されます。リストされる状態は、[All]、[Active]、[Cleared]、および [Acknowledged] です。
[Event ID] テキスト ボックス	Performance Monitor から送信されたイベント通知の詳細情報を表示できます。 既知のイベント ID 番号をテキスト ボックスに入力し、[Find] をクリックします。 **（注）** [Event ID] の検索は、それまでのフィルタリングとは関係なく機能します。
[Description] テキスト ボックス	特定のテキスト文字列を説明に含むイベントだけを表示するための、クエリーを定義できます。 キーワードまたは用語を入力して、クエリーのパラメータを定義します。有効なパラメータは、Performance Monitor の [Description] カラムに表示される可能性のある単語または用語に限定されます。 入力した文字列を説明に含むイベントだけを表示するには、[Search] をクリックします。 **（注）** 説明の検索は、それまでのフィルタリングとは関係なく機能します。
[Device] カラム	関連するモニタ対象サービスを提供するデバイスの DNS 名が表示されます。 表示されるエントリは、開いているイベント ブラウザ ウィンドウの種類に応じて異なります。たとえば [Firewall Event Browser] の [Device] カラムには、ファイアウォール デバイスの DNS 名と、1 つまたは複数のファイアウォール サービス モジュールを含むスイッチの DNS 名がリストされます。
[Severity] カラム	重大度レベルが表示されます。最高の重大度は P1 で、最低の重大度は P5 です。

表 3-5　イベント ブラウザ ウィンドウのリファレンス（続き）

エレメント	説明
[Type] カラム	関連サービスがインスタンス内でしきい値を超過した、というイベントの種類が表示されます。このカラムに表示されるエントリは、関連するモニタ対象サービスに対して、イベント固有のしきい値を定義するときに表示されるオプションと同じです。 サービスの全イベント タイプのリストを表示するには、[Administration] > [Notifications] の順に選択し、選択ツリー内でサービス フォルダを展開します。
[Description] カラム	イベントがサービスに与える影響が表示されます。たとえば、帯域幅が低下する、VPN がダウンする、などの情報があります。 特定の説明と一致するイベントだけを個別に表示する方法については、このテーブルの *[Description] テキスト ボックス*行を参照してください。
[Event ID] カラム	Performance Monitor によって管理者に通知するために対象イベントに関連付けられた数値 ID が表示されます。 Performance Monitor によって割り当てられる ID 番号は長期間にわたる連番であるため、新しいイベントの数値 ID は、古いイベントの ID よりも大きい値となります。[Event ID] カラムの値でテーブルをソートすると、時系列順に並べられます。 Performance Monitor の通知オプションについては、「通知の操作」（P.12-1）を参照してください。
[Event State] カラム	関連イベントをトリガーしたイベント状態値が表示されます。 詳細については、このテーブルの *[Event State] リスト*行を参照してください。
[Alarm Status] カラム	関連イベントのアラーム状態（[Acknowledged]、[Active]、または [Cleared] のいずれか）が表示されます。
[Product] カラム	汎用デバイス タイプが表示されます。 **ヒント** 特定のデバイスに関する詳細情報を参照するには、オブジェクト セレクタ内に表示されるデバイス名の上にポインタを移動してください。
[Occur Time] カラム	このイベントがポーリングによって記録された時刻が表示されます。 ユーザの場所にかかわらず、CiscoWorks Server の時刻とタイムゾーンの省略名が表示されます。
[Clear Event]	選択されているイベントをクリアします。イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ウィンドウに表示され続けます。

（注） [Event State] リストまたは [Alarm Status] リストのどちらかで、オプションを選択できます。どちらかのリストでオプションを選択すると、もう一方のリストの選択内容が「All」にリセットされます。

関連トピック

- 「イベント ブラウザの操作」（P.3-12）

MCP プロセスのメンテナンス

Performance Monitor は、多数のデバイスに対して頻繁にポーリングを行います。このためには、*MCP* と呼ばれるサーバ プロセスが必要です。サーバのパフォーマンスを全体的に向上させるため、*restartMCP.pl* と呼ばれるスケジュールされたジョブによって、MCP プロセスは、週に一度、日曜の午前 3:30 に停止して再起動されます。このスクリプトは、**pdterm MCP** コマンドを実行し、1 分間待機した後に **pdexec MCP** コマンドを実行します。

（注）
- また、*restartMCP.pl* ジョブは、McpDbEngine プロセスの停止と再起動も行います。
- restartMCP.pl ジョブのスケジュール間隔は、Performance Monitor がインストールされているサーバの現地時間に基づきます。

ヒント
- スケジュールされたジョブのリストを表示するには、Windows コマンドラインにアクセスし、**at** と入力して Enter を押します。
- *restartMCP.pl* スクリプトのエントリを編集すると、スケジュールを変更できます。

MCP プロセスが再起動されるまでは、次の状態が続きます。

- デバイスのポーリングは行われない。
- 新規または反復される検証タスクは実行されない。
- Performance Monitor は、モニタ対象デバイスから送信されたすべての SNMP トラップ情報を失う。
- 新規デバイスを追加またはインポートできない。

Performance Monitor インターフェイスに影響はないため、保管されているデータを使用して作業できます。ただし、表示されるデータの一部は、ネットワーク内のデバイスおよびサービスの現在の状況と一致していない可能性があります。また、履歴レポートを実行したときに、表示されたグラフで、MCP プロセスが実行していなかった期間のデータが落ち込んでいることがあります。

MCP プロセスのシャットダウンおよび再起動は、通常 5 分未満で済みます。

Performance Monitor の動作順序

設定されてユーザの意図どおりに動作するようになった Performance Monitor は、特定の操作を次の順序で自動的に実行します。

1. スケジュールされた検証を実行し、デバイスが存在して到達可能であることを確認します。この検証では、指定されたデバイスのクレデンシャルが正しく、必要な機能および必要なインターフェイスはイネーブルになっていることが前提になっています。

   VPN 3000 シリーズのコンセントレータの場合は、検証によって、関連するコンセントレータが正しい XML クレデンシャルを使用しているか、HTTPS がイネーブルになっているか、および VPN 3000 Concentrator Series Manager が稼動しているかどうかも確認されます。
2. ポーリングするデバイスのリストを、スケジュールされた検証の結果に基づいて更新します。
3. 到達可能なデバイスをポーリングして、それらのデバイスの現在のステータスを調べます。そして、デバイスのステータス情報を、パフォーマンスしきい値および障害しきい値と比較し、必要に応じて、パフォーマンス イベントと障害イベントの生成、イベント通知の送信、およびテーブルとグラフの値の更新を行います。

   （注）　タイムアウト期間内にデバイスがポーリングに応答しなかった場合は、すべてのデバイスに対するポーリングが停止します。詳細については、「ポーリングのタイム アウトの設定」（P.2-18）を参照してください。

4. ログを（継続的に）更新します。
5. スケジュールされたジョブおよび反復ジョブを実行します。

CHAPTER 4

要約の使用方法

要約グラフとテーブルは、帯域幅の使用量、接続失敗、使用状況のレベル、クリティカルな問題など、パフォーマンス メトリックのあまり詳細でない表現を提供します。

要約グラフおよびいくつかのテーブルには、関連する項目またはカテゴリの追加詳細へのリンクがあります。

（注） 「基本概念について」（P.1-3）の説明に従って、分離可能なダッシュボードに特定の種類の要約情報を表示できます。

次の表に、[Summary] タブのオプションを示します。

表 4-1　Performance Monitor の要約オプション

オプション	説明
[Critical Problems]	次の場合に、[Critical Problems] オプションを選択します。 • 既知のクリティカルな問題のテーブルを表示する。 • 問題の状態で、問題をフィルタリングする。 • ネットワークで Performance Monitor が検出した問題を確認する。 「クリティカルな問題の要約の操作」（P.4-2）を参照してください。
[VPN]	[VPN] オプションを選択すると、VPN サービスのパフォーマンス要約グラフが表示されます。「VPN サービスの要約の操作」（P.4-3）を参照してください。
[Firewall]	[Firewall] オプションを選択すると、ファイアウォール サービスのパフォーマンス要約グラフが表示されます。「ファイアウォール サービス要約の操作」（P.4-5）を参照してください。
[Load Balancing]	[Load Balancing] オプションを選択すると、コンテンツ スイッチング サービスのパフォーマンス要約グラフが表示されます。「ロード バランシング要約の操作」（P.4-6）を参照してください。
[SSL]	[SSL] オプションを選択すると、SSL プロキシ サービスのパフォーマンス要約グラフが表示されます。「SSL サービス要約の操作」（P.4-7）を参照してください。
[Event Browser]	[Event Browser] オプションを選択すると、プリセット フィルタなしで [Event Browser] ウィンドウが開きます。「イベント ブラウザの操作」（P.3-12）を参照してください。

クリティカルな問題の要約の操作

クリティカルな問題は、重大度が P1 または P2 です。ネットワーク上でモニタされているすべてのサービスの既知のクリティカルな問題を表示できます。クリティカルな問題を確認すると、問題に対処中であることを示すことができます。このような問題のステータスは、Active から Acknowledged に変更されます。問題が解決した後、イベント ブラウザからイベントをクリアできます。確認またはクリアされたイベントは、問題が次のポーリング サイクルの前に解決されていなかった場合、また報告されます。問題が次のポーリング サイクルの前に解決された場合、イベントはステータスにかかわらずクリアされます。

手順

ステップ 1　[Summary] > [Critical Problems] を選択します。テーブルのカラムの説明については、表 4-2 を参照してください。

ヒント　最初に、すべてのアクティブな問題がテーブルに表示されます。この表示は、[Select Status] リストで希望するオプションを選択することによって、確認された問題だけ、またはすべての問題（アクティブまたは確認済み）を表示するように変更できます。リフレッシュされたリストには、指定された状態のモニタ対象の問題だけが表示されます。指定された状態と一致する問題がない場合、リフレッシュされたリストにレコードが表示されません。

ステップ 2　アクティブな問題に対して、次のことができます。

- [Event Browser] ウィンドウを開き、特定のデバイスのすべてのイベントを表示するフィルタ処理されたリストを表示する。[Description] カラムで、ハイパーリンク付きの項目をクリックします。

  イベント ブラウザの表示は、[Critical Problems] ページと異なり、P1 および P2 の重大度に制限されません。そのため、イベント ブラウザには、指定したデバイスの任意の重大度、またはすべての重大度のイベントを表示できます。

- クリティカルな問題を確認する。解決する問題が記述された行のチェックボックスをオンにし、[Acknowledge] をクリックします。一度に複数のボックスを選択できます。また、見出し行のボックスをクリックすると、すべての問題を選択できます。

  クリティカルな問題を確認すると、問題に対処中であることを示すことができます。特定の問題を確認できるユーザは、1 人だけです。問題が解決した後、イベント ブラウザからイベントをクリアできます。確認を取り消す方法がないことに注意してください。

参考

表 4-2　クリティカルな問題の要約

要素	説明
[Device] カラム	DNS 名または IP アドレスで、モニタされている問題が発生したデバイスを識別します。
[Family] カラム	VPN ルータ、コンセントレータ、またはサービス モジュールが搭載されたスイッチとして、デバイスを識別します。
[Product] カラム	関連する製品の型番が表示されます。
[Severity] カラム	P1 から P5 の値が表示されます。P1 が、最も重大度が高い問題で、P5 が、最も重大度が低い問題です。
[Description] カラム	クリティカルな問題に関する簡単な説明が表示されます。

表 4-2　クリティカルな問題の要約（続き）

要素	説明
[Status] カラム	問題のステータス ラベルが表示されます。[Select Status] リストのオプションと同じです。
[Last Update Time] カラム	クリティカルな問題を報告した、Performance Monitor のポーリングの最新の時刻が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

VPN サービスの要約の操作

Performance Monitor は、ネットワーク上のリモート アクセスおよびサイト間 VPN サービスの状態を要約するグラフを提供します。

（注） 特に指定されたものを除き、Performance Monitor のすべての要約グラフは、デルタ値（ポーリング サイクル間で測定された差）を示します。

手順

ステップ 1　[Summary] > [VPN] を選択します。

[VPN] ページに、リアルタイム モニタリングの結果を示すグラフが表示されます（表 4-3）。[Enable Refresh Rate] チェックボックスがオンになっている場合、表示は常に最新です。そうでない場合、[Refresh] ボタンをクリックすると、表示がリフレッシュされます。

ヒント [Critical Problems] ボタンは、少なくとも 1 つのクリティカルな問題がネットワークに存在する場合、赤くなります。そうでない場合、ボタンはグレーです。ボタンをクリックすると、すべてのクリティカルな問題（P1 および P2）のテーブルが表示されます。（「インターフェイスのアイコンについて」（P.3-5）を参照）。

ステップ 2　グラフをクリックすると、追加の詳細が表示されます。「ダッシュボード」のグラフを分離するには、分離アイコンをクリックします。

VPN 要約グラフの種類

表 4-3　VPN 要約のグラフ

グラフの種類	説明
リモート アクセス グラフ	
RAS 要約グラフは、VPN コンセントレータのパブリック インターフェイスから受信した情報を示します。	
[Top 3 Throughput (RAS)]	スループット レベルが最も高い 3 台の VPN コンセントレータについて、リアルタイムのスループット レベルを Kbps 単位で示します。ネットワークにある VPN コンセントレータが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの VPN コンセントレータにもスループットがない場合、グラフは空です。 クリックすると [Remote Access Devices] ページが表示され、RAS デバイスのパフォーマンス統計情報が個別に表示されます（「RAS デバイスの使用状況とアクティビティのモニタリング」（P.5-6）を参照）。
[Top 3 Connection Failures % (RAS)]	接続失敗が最も多い 3 台の VPN コンセントレータについて、リアルタイムの接続失敗の割合を示します。ネットワークにある VPN コンセントレータが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの VPN コンセントレータでも接続が失敗していない場合、グラフは空です。 クリックするとイベント ブラウザが開き、重大な RAS エラーだけが表示されます（「イベント ブラウザ ウィンドウ」（P.3-15）を参照）。
[Top 3 User Session Count (RAS)]	最もユーザ セッションが多い 3 台のデバイスについて、リアルタイムのセッション数を示します。ユーザ セッションが存在するデバイスが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの RAS デバイスにもユーザ セッションがない場合、グラフは空です。 クリックすると [Remote Access Devices] ページが表示され、RAS デバイスのパフォーマンス統計情報が個別に表示されます（「RAS デバイスの使用状況とアクティビティのモニタリング」（P.5-6）を参照）。
サイト間グラフ	
サイト間要約グラフは、インターフェイスから受信したクリプト マップが添付されている情報を示します。	
[Top 3 Throughput (Site-to-Site)]	スループット レベルが最も高い 3 台のサイト間デバイスについて、リアルタイムのスループット レベルを Kbps 単位で示します。ネットワークにあるサイト間デバイスが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どのサイト間デバイスにもスループットがない場合、グラフは空です。 クリックすると [Site-to-Site Devices] ページが表示され、サイト間デバイスのパフォーマンス統計情報が個別に表示されます（「サイト間デバイスの使用とアクティビティのモニタリング」（P.6-3）を参照）。
[Top 3 Connection Failures % (Site-to-Site)]	接続失敗が最も多い 3 台のサイト間デバイスについて、リアルタイムの接続失敗を示します。ネットワークにあるサイト間デバイスが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どのサイト間デバイスでも接続が失敗していない場合、グラフは空です。 クリックするとイベント ブラウザが開き、重大なサイト間エラーだけが表示されます（「イベント ブラウザ ウィンドウ」（P.3-15）を参照）。
[Top 3 Tunnel Count (Site-to-Site)]	最もトンネルが多い 3 台のデバイスについて、リアルタイムのトンネル数を示します。ネットワークにあるサイト間デバイスが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どのサイト間デバイスにもトンネルがない場合、グラフは空です。 クリックすると [Site-to-Site Devices] ページが表示され、サイト間デバイスのパフォーマンス統計情報が個別に表示されます（「サイト間デバイスの使用とアクティビティのモニタリング」（P.6-3）を参照）。

ファイアウォール サービス要約の操作

Performance Monitor は、ネットワーク上にあるファイアウォール サービスの現在の状態を要約するグラフを提供します。

（注） 特に指定されたものを除き、Performance Monitor のすべての要約グラフは、デルタ値（ポーリング サイクル間で測定された差）を示します。

手順

ステップ 1　[Summary] > [Firewall] を選択します。

[Firewall] ページに、リアルタイム モニタリングの結果を示すグラフが表示されます（表 4-4）。[Enable Refresh Rate] チェックボックスがオンになっている場合、表示は常に最新です。そうでない場合、[Refresh] ボタンをクリックすると、表示がリフレッシュされます。

ヒント [Critical Problems] ボタンは、少なくとも 1 つのクリティカルな問題がネットワークに存在する場合、赤くなります。そうでない場合、ボタンはグレーです。ボタンをクリックすると、すべてのクリティカルな問題（P1 および P2）のテーブルが表示されます。（「インターフェイスのアイコンについて」（P.3-5）を参照）。

ステップ 2　グラフをクリックすると、追加の詳細が表示されます。「ダッシュボード」のグラフを分離するには、分離アイコンをクリックします。

ファイアウォール要約グラフの種類

表 4-4　ファイアウォール要約のグラフ

グラフの種類	説明
[Top 3 Interface Bandwidth Consumption %]	帯域幅を最も消費している 3 つの PIX ファイアウォール デバイス インターフェイスについて、リアルタイムの帯域幅の使用量の割合を示します。どの PIX インターフェイスも帯域幅を使用していない場合、グラフは空です。 **（注）** インターフェイスの帯域幅の使用量の計算には、ファイアウォール サービス モジュールのインターフェイスは含まれません。ただし、検査ポリシーが設定されている IOS ルータのインターフェイスは、計算に使用されます。 クリックすると [Firewalls] ページが表示され、すべてのファイアウォール デバイスおよびモジュールの使用状況およびアクティビティ統計情報が表示されます（「ファイアウォール デバイス テーブルの操作」（P.7-1）を参照）。
[Top 3 Interface Errors]	最も多くのエラーが発生している 3 つのファイアウォール デバイス インターフェイスについて、リアルタイムのエラー数が表示されます。エラーが発生したインターフェイスが 3 つ未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どのファイアウォール インターフェイスでもエラーが発生していない場合、グラフは空です。 クリックするとイベント ブラウザが開き、重大なファイアウォール イベントだけが表示されます（「イベント ブラウザ ウィンドウ」（P.3-15）を参照）。

表 4-4　ファイアウォール要約のグラフ（続き）

グラフの種類	説明
[Top 3 Connections]	最も接続が多い 3 台のファイアウォール デバイスについて、リアルタイムの接続数を示します。接続が存在するデバイスが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どのファイアウォール デバイスにも接続がない場合、グラフは空です。 クリックすると [Firewalls] ページが表示され、すべてのファイアウォール デバイスの使用状況およびアクティビティ統計情報が表示されます（「ファイアウォール デバイス テーブルの操作」（P.7-1）を参照）。

ロード バランシング要約の操作

Performance Monitor は、ネットワークで Web サーバのロード バランシング サービスを提供する、有効な Content-Switching Service Module（CSM; コンテンツ スイッチング サービス モジュール）の現在の状態の要約を提供します。

（注）　特に指定されたものを除き、Performance Monitor のすべての要約グラフは、デルタ値（ポーリング サイクル間で測定された差）を示します。

手順

ステップ 1　[Summary] > [Load Balancing] を選択します。

[Load Balancing] ページに、リアルタイム モニタリングの結果を示す棒グラフが表示されます（表 4-5）。[Enable Refresh Rate] チェックボックスがオンになっている場合、表示は常に最新です。そうでない場合、[Refresh] ボタンをクリックすると、表示がリフレッシュされます。

ヒント　[Critical Problems] ボタンは、少なくとも 1 つのクリティカルな問題がネットワークに存在する場合、赤くなります。そうでない場合、ボタンはグレーです。ボタンをクリックすると、すべてのクリティカルな問題（P1 および P2）のテーブルが表示されます。（「インターフェイスのアイコンについて」（P.3-5）を参照）。

ステップ 2　グラフをクリックすると、追加の詳細が表示されます。「ダッシュボード」のグラフを分離するには、分離アイコンをクリックします。

ロード バランシング要約グラフの種類

表 4-5　ロード バランシング要約のグラフ

グラフの種類	説明
[Top 3 Current Connections]	最も接続が多い 3 つの CSM モジュールについて、リアルタイムの接続数を示します。接続が存在するモジュールが 3 つ未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの CSM モジュールにも接続がない場合、グラフは空です。 クリックすると [Load Balancing Modules] ページが表示され、すべての CSM モジュールの使用状況およびアクティビティ統計情報が表示されます（「CSM の使用とアクティビティ統計情報の表示」（P.8-2））。
[Top 3 Connection Failures %]	最も接続失敗が多い 3 つの CSM モジュールについて、リアルタイムの接続失敗の割合を示します。接続に失敗したモジュールが 3 つ未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの CSM モジュールでも接続が失敗していない場合、グラフは空です。 クリックするとイベント ブラウザが開き、重大な CSM エラーだけが表示されます（「イベント ブラウザ ウィンドウ」（P.3-15）を参照）。
[Top 3 Virtual Server Connections]	最も接続が多い 3 つの仮想サーバについて、リアルタイムの接続数を示します。接続が存在する仮想サーバが 3 台未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの仮想サーバにも接続がない場合、グラフは空です。 クリックすると [Load Balancing Modules] ページが表示され、すべての CSM モジュールの使用状況およびアクティビティ統計情報が個別に表示されます（「CSM の使用とアクティビティ統計情報の表示」（P.8-2））。

SSL サービス要約の操作

Performance Monitor は、ネットワーク上にある SSL プロキシ サービスの現在の状態を要約するグラフを提供します。

（注） 特に指定されたものを除き、Performance Monitor のすべての要約グラフは、デルタ値（ポーリング サイクル間で測定された差）を示します。

手順

ステップ 1　[Summary] > [SSL] を選択します。

[SSL Summary] ページに、リアルタイム モニタリングの結果を示す棒グラフが表示されます（表 4-6）。[Enable Refresh Rate] チェックボックスがオンになっている場合、表示は常に最新です。そうでない場合、[Refresh] ボタンをクリックすると、表示がリフレッシュされます。

ヒント [Critical Problems] ボタンは、少なくとも 1 つのクリティカルな問題がネットワークに存在する場合、赤くなります。そうでない場合、ボタンはグレーです。ボタンをクリックすると、すべてのクリティカルな問題（P1 および P2）のテーブルが表示されます。（「インターフェイスのアイコンについて」（P.3-5）を参照）。

ステップ 2　グラフをクリックすると、追加の詳細が表示されます。「ダッシュボード」のグラフを分離するには、分離アイコンをクリックします。

SSL 要約グラフの種類

表 4-6　SSL 要約のグラフ

グラフの種類	説明
[Top 3 Connections]	最も接続が多い 3 つの SSL モジュールについて、リアルタイムの接続数を示します。接続が存在するモジュールが 3 つ未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの SSL モジュールにも接続がない場合、グラフは空です。 クリックすると [SSL Modules] ページが表示され、すべての SSL モジュールの使用状況およびアクティビティ統計情報が表示されます（「SSL 使用状況およびアクティビティ統計情報の操作」（P.9-2）を参照）。
[Top 3 Error]	最もエラーが多い 3 つの SSL モジュールについて、リアルタイムのエラー数を示します。エラーが発生したモジュールが 3 つ未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの SSL モジュールでもエラーが発生していない場合、グラフは空です。 クリックするとイベント ブラウザが開き、重大な SSL エラーだけが表示されます（「イベント ブラウザ ウィンドウ」（P.3-15）を参照）。
[Top 3 Module Throughput]	最もスループットが高い 3 つの SSL モジュールについて、リアルタイムのスループット レベルをバイト単位で示します。測定可能なスループットがあるモジュールが 3 つ未満の場合は、グラフに表示されるバーが 3 本よりも少なくなります。どの SSL モジュールにも測定可能なスループットがない場合、グラフは空です。 クリックすると [SSL Modules] ページが表示され、すべての SSL モジュールの使用状況およびアクティビティ統計情報が個別に表示されます（「SSL 使用状況およびアクティビティ統計情報の操作」（P.9-2）を参照）。

CHAPTER 5

リモート アクセス VPN サービスのモニタリング

Remote Access Service（RAS; リモート アクセス サービス）VPN は、モバイル ユーザや在宅勤務者などのリモート ユーザへの接続の安全性を保護します。RAS VPN のモニタリングは、クラスタ、コンセントレータ、およびユーザ セッション パフォーマンスの最も重要なすべての指標を、ひと目でわかるように提示します。

Performance Monitor により、RAS VPN の問題が存在しているか、どこに問題があるかを、すばやく判断することができます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。

オプションとして、一度に 1 人の RAS ユーザをログアウトできます。

ヒント RAS VPN サービスの一般的な問題をトラブルシューティングするには、付録のトラブルシューティングを参照してください。

ここでは、RAS VPN のモニタリング機能について説明します。

RAS 仮想クラスタについて

（注）

- Performance Monitor およびマニュアルにおける *ロード バランシング サービス*は、コンテンツ スイッチング サービス モジュールの Web サーバ ロードバランシング機能だけを表しています。Performance Monitor は、仮想クラスタ内で組み合わせたコンセントレータまたはアプリケーションのロード バランシングはモニタしません。
- PIX OS および Easy VPN は RAS VPN の使用をサポートしていますが、これらの 2 つのテクノロジーは、両方とも仮想クラスタの使用をサポートしていません。

RAS VPN では、リモート ユーザが、ダイヤルアップ、ISDN、DSL、ケーブル、その他のテクノロジーによって接続し、共有しているパブリック インフラストラクチャを介してプライベート ネットワークに参加することができます。

Performance Monitor は、複数の種類の異なるデバイスで生じた RAS VPN サービスをモニタしますが、Cisco VPN 3000 シリーズ コンセントレータおよび ASA 5520 または 5550 アプライアンスに対しては特別な考慮が必要です。これらのものはロードバランシングに対して単独で、または*仮想クラスタ*内で組み合わせてモニタすることが可能なためです。仮想クラスタでは、コンセントレータのコレクション、またはアプライアンスのコレクションを 1 つのエンティティとして機能させることができます。

クラスタは、1 つの IP アドレスによって外部のクライアント スペースに認識されます。仮想 IP アドレスはルーティング可能なアドレス、つまり他のデバイスがパケットを送信できる有効なアドレスにする必要があります。そうしないと、受信パケットがクラスタに到達できません。

この仮想 IP アドレスは、VPN クラスタ内の特定のデバイスには関連付けられません。これは、*仮想クラスタ マスター*によってサービスされます。仮想クラスタ マスタ コンセントレータは、特定のクラスタ内のすべてのセカンダリ コンセントレータまたはアプライアンスからのロード情報を保持しています。各セカンダリ コンセントレータは、KeepAlive 負荷情報をマスターに送信します。

- VPN 3000 シリーズには、6 つの異なったコンセントレータ モデルがあります。これらのモデルの使用および機能については、http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/index.html を参照してください。モニタしているコンセントレータが正常に機能しているかどうかを判断するうえで役に立ちます。
- ASA 5520 および 5550 アプライアンスの使用および機能については、http://www.cisco.com/en/US/products/ps6120/index.html を参照してください。

Easy VPN について

Cisco Easy VPN は、いくつかの種類のシスコ デバイスに対するソフトウェアの機能で、リモート オフィスおよびテレワーカーに対する VPN の展開を簡潔にするものです。Easy VPN では、多数のデバイスにおける VPN 管理が一元化されるため、VPN 展開の複雑さが軽減します。Easy VPN の実装では、サポートされているデバイス内で Cisco Easy VPN Server と Cisco Easy VPN Remote 機能の両方を使用する必要があります。

Easy VPN を使用すると、サポートされているルータ、アプライアンス、ファイアウォール、およびコンセントレータはリモート VPN クライアントのように機能します。したがって、これらのデバイスは Easy VPN サーバからセキュリティ ポリシーを受け取ることが可能になり、これにより組織内の遠隔地における VPN 構成の要件が最小になります。

また、Cisco Easy VPN Server に対応しているデバイスは、自身の PC 上で Cisco VPN クライアント ソフトウェアを実行しているモバイル リモート ワーカーによって開始された VPN トンネルを終了することができます。

Performance Monitor では、ある Easy VPN サーバで、サイト間 VPN またはリモートアクセス VPN のいずれかで、サポートされているルータ、アプライアンス、ファイアウォール、およびコンセントレータが VPN ヘッドエンド デバイスのように機能することが可能であっても、すべての Easy VPN セッションが RAS VPN セッションのように示されます。

Easy VPN の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html

（注）

- Easy VPN は RAS クラスタの使用をサポートしていません。
- Performance Monitor は Easy VPN セッションのユーザ名を表示しません。また、ユーザ名を特別な Easy VPN セッションに関連付けません。
- Performance Monitor の User Session Report 機能は、Easy VPN をサポートしていません。

RAS クラスタ テーブルの操作

Performance Monitor では、すべてのリモート アクセス クラスタの概要を表示できます。この概要を使用して、ユーザ データとコンセントレータ データを分離し、有効なクラスタ統計情報のサブセットを表示します。

ヒント　Performance Monitor は、1 日に 1 回、クラスタ メンバシップのレコードを自動的に更新します。クラスタ内で VPN コンセントレータを追加または削除した場合、またはクラスタ間でコンセントレータを移動した場合は、[Devices] > [Importing Devices] を選択し、[Revalidate] をクリックする必要があります。このようにしないと、次の自動更新まで、対象のクラスタについて誤った情報が表示されます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Clusters] を選択します。テーブルのカラムの説明については、表 5-1 を参照してください。

Performance Monitor は、VPN コンセントレータのヘルスとパフォーマンスの測定値を平均して、ネットワーク内のクラスタについて表示する概要レベルの統計情報を作成します。

ステップ 2　次のいずれかを実行して、リストを調整したり、さらに詳細な情報を取得することができます。

- リスト内でデバイスを見つけるには、[Find Device] フィールドでデバイスの IP アドレスまたは DNS 名を入力し、[Find] をクリックします。デバイスが見つかると、[Remote Access Device Graphs] ページに、指定されたコンセントレータの情報が表示されます。グラフの種類については、「RAS デバイスの詳細グラフの表示」（P.5-5）を参照してください。
- RAS クラスタのドロップしたパケットのグラフを表示するには、[Packet Drop %] カラムの対象エントリをクリックします。
- RAS クラスタのスループット グラフを表示するには、[Throughput (kbps)] カラムの対象エントリをクリックします。
- RAS クラスタの帯域幅使用率のグラフを表示するには、[Bandwidth Usage %] カラムの対象エントリをクリックします。

参考

表 5-1　[Remote Access Clusters] ページ

エレメント	説明
[Cluster] カラム	仮想クラスタ マスターの DNS 名が表示されます。
[Devices] カラム	クラスタ内のデバイスの合計数が表示されます。

表 5-1　[Remote Access Clusters] ページ（続き）

エレメント	説明
[Master Device] カラム	指定したクラスタ上のマスター デバイスの IP アドレスが表示されます。 仮想クラスタ マスター コンセントレータは、クラスタ内のすべてのセカンダリ コンセントレータのロード情報を保持しています。各セカンダリは、KeepAlive メッセージ交換のロード情報をマスターへ送信します。
[# of Users] カラム	すべての RAS デバイス上のアクティブ セッションについて、集約した合計数が表示されます。 （注）　いずれかのユーザが RAS ユーザからログアウトすると、次に表示がリフレッシュしたときに、この値が異なる場合があります。
[Load Variance] カラム	最も高負荷のデバイスと、最も低負荷のデバイス間の差異を測定して計算されたスキューを示します。 デバイスの負荷は、現在のアクティブなセッションの数を、設定した最大許容接続数で除算した割合（パーセンテージ）として計算されます。
[Packet Drop %] カラム	IPSec フェーズ 1（IKE）トンネルおよびフェーズ 2（IPSec）トンネルでドロップしたパケットの計算結果を、すべての RAS デバイス上のすべての受信および送信パケットの割合（パーセンテージ）として表示します。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Packets Drop] カラムでハイパーリンクされているエントリをクリックします。
[Throughput (kbps)] カラム	すべての RAS デバイス上のパブリック インターフェイス間の送信および受信オクテットの合計が表示されます。 新しいブラウザを開いてグラフとして選択した内容を表示するには、[Throughput (kbps)] カラムでハイパーリンクされているエントリをクリックします。
[Bandwidth Usage %] カラム	すべての RAS デバイスで使用されている帯域幅を、すべての RAS デバイスで使用できる帯域幅で除算した平均（パーセンテージ）が表示されます。 新しいブラウザを開いてグラフとして選択した内容を表示するには、[Bandwidth Usage %] カラムでハイパーリンクされているエントリをクリックします。
[Inbound Connection Failure %] カラム	すべての受信接続の試行において、受信のフェーズ 1（IKE）およびフェーズ 2（IPSec）接続の中で、リモートで開始されて失敗したものの平均（パーセンテージ）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS デバイスの操作

検証済みの VPN コンセントレータのステータスを説明している情報を分離してモニタする方法については、次のトピックを参照してください。

- 「RAS デバイスの詳細グラフの表示」（P.5-5）
- 「RAS デバイスの使用状況とアクティビティのモニタリング」（P.5-6）
- 「RAS デバイス障害のモニタリング」（P.5-8）
- 「RAS デバイスの暗号化アクティビティのモニタリング」（P.5-9）

- 「RAS デバイスの暗号化アクセラレータ カード データの表示」（P.5-10）
- 「リモート アクセス インターフェイス テーブルの表示」（P.5-11）

RAS デバイスの詳細グラフの表示

ネットワーク内で検証済みの VPN 3000 シリーズ コンセントレータの情報を分離し、そのヘルスとパフォーマンスを示す詳細グラフを表示することができます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] を選択します。

デフォルトでは、[Remote Access Device Graphs] ページに、IP アドレスとして最も小さい数を使用しているデバイスのヘルスとパフォーマンスを表すグラフが表示されます。グラフの説明については、表 5-2 を参照してください。

（注）　2 つの縦（Y）軸を使用するグラフを解釈するときに、既知の問題が発生することがあります。最初の Y 軸は常にゼロで始まるのに対し、2 番目の Y 軸は、指定された時間範囲の最も低い値がゼロよりも大きい場合でも、その値で始まります。そのため、2 つの Y 軸を直接比較できないことがあります。

ステップ 2　[Select Device] リストから、グラフを表示するデバイスを選択します。

RAS グラフの種類

表 5-2　RAS グラフの種類

グラフの種類	説明
[Bandwidth Utilization]	パブリック インターフェイスで使用されているデバイスの帯域幅容量の割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で使用されている帯域幅容量の平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[CPU Usage]	使用されたデバイスの CPU 能力の割合を示します。 • 縦軸は、特定のポーリング サイクル内で使用されている CPU 能力の平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Inbound Connect Failures]	長期にわたる受信接続失敗のトレンドを示します。 • 縦軸は、特定のポーリング サイクル内での失敗の平均数を表します。 • 横軸は、ポーリング サイクルの時刻を示します。

表 5-2　RAS グラフの種類（続き）

グラフの種類	説明
[Throughput vs. Session]	一定期間のスループットの傾向を VPN セッション数の傾向と比較するうえで有用な折れ線グラフが表示されます。 • 2 種類の情報を表示するため、2 つの縦軸を使用します。 – 左の（オレンジの）縦軸は、特定のポーリング サイクル内の平均スループットをバイト単位で示します。 – 右の（青色の）縦軸は、特定のポーリング サイクル内の平均セッション数を示します。 • 横軸は、Performance Monitor がそれぞれの縦軸のトレンドを計算した時刻を示します。
[IKE Phase 1 Connection Failures]	フェーズ 1（IKE）接続で失敗した割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で失敗した接続の平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[IPSec Phase 2 Connection Failures]	フェーズ 2（IPSec）接続で失敗した割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で失敗した接続の平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。

RAS デバイスの使用状況とアクティビティのモニタリング

Performance Monitor では、ネットワーク内のクラスタで RAS VPN サービスを提供している検証済みのすべての Cisco VPN 3000 シリーズ コンセントレータについて、概要を参照できます。この概要を使用すると、次のことができます。

- VPN コンセントレータの使用およびアクティビティ、コンセントレータの障害、およびコンセントレータの暗号化アクティビティを表しているデータを分離します。
- VPN コンセントレータの状態を要約しているテーブルおよびグラフを表示します。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Devices] を選択します。テーブルのカラムの説明については、表 5-3 を参照してください。

[Remote Access Devices] ページに、コンセントレータの使用およびアクティビティの統計情報のテーブルが表示されます。このページ上のすべての測定値は、*デルタ*として計算されます（あるポーリング サイクルから次のサイクルまでの差の範囲を示します）。ただし、現在のユーザ数は整数です。

（注）　いずれかのユーザが RAS ユーザからログアウトすると、次に表示がリフレッシュされたときに、現在のユーザ数の整数値が異なる場合があります。

ステップ 2　次のいずれかを実行して、リストを調整したり、さらに詳細な情報を取得することができます。

- 特定のクラスタ内でこれらのデバイスだけをリストに表示するには、[Select Cluster] リストでクラスタを選択します。Easy VPN は、RAS クラスタの使用をサポートしていないことに注意してください。
- 特定のコンセントレータについて詳細グラフを表示するには、[Device] カラムで IP アドレスまたは DNS 名をクリックします。

- コンセントレータのドロップしたパケットのグラフを表示するには、[Packet Drop %] カラムの対象エントリをクリックします。
- コンセントレータのスループット グラフを表示するには、[Throughput (kbps)] カラムの対象エントリをクリックします。
- コンセントレータの帯域幅使用のグラフを表示するには、[Bandwidth Usage %] カラムの対象エントリをクリックします。

参考

表 5-3　[Remote Access Devices]

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な RAS エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。 **（注）** イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページに表示され続けます。
[Device] カラム	デバイスの IP アドレスまたは DNS 名が表示されます。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Device] カラムでハイパーリンクされているエントリをクリックします。
[Cluster] カラム	仮想クラスタ マスターの DNS 名が表示されます。
[Model] カラム	シスコ デバイスのモデル名と番号が表示されます。
[# Of Users] カラム	アクティブ セッションの数が表示されます。 **（注）** いずれかのユーザが RAS ユーザからログアウトすると、次に表示がリフレッシュしたときに、この値が異なる場合があります。
[Packet Drop %] カラム	フェーズ 1（IKE）トンネルおよびフェーズ 2（IPSec）トンネルでドロップしたパケットの計算結果を、すべての受信および送信パケットの割合（パーセンテージ）として表示します。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Packet Drop %] カラムでハイパーリンクされているエントリをクリックします。
[Packets In] カラム	受信パケットの数が表示されます。
[Packets Out] カラム	送信パケットの数が表示されます。
[Throughput (kbps)] カラム	指定した RAS デバイス上のパブリック インターフェイスを介した送信および受信の合計オクテットが表示されます。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Throughput (kbps)] カラムでハイパーリンクされているエントリをクリックします。
[Bandwidth Usage %] カラム	指定した RAS デバイスで使用されている帯域幅を、そのデバイスで使用できる帯域幅で除算した割合（パーセンテージ）が表示されます。 新しいブラウザを開いて、グラフとして選択した内容を表示するには、[Bandwidth Usage] カラムでハイパーリンクされているエントリをクリックします。
[Last Updated] カラム	Performance Monitor がデバイスを最後にポーリングした日付と時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS デバイス障害のモニタリング

検証済みの VPN コンセントレータの操作における障害が記載されているテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Devices] > [Failures] を選択します。テーブルのカラムの説明については、表 5-4 を参照してください。

[Remote Access Failures] ページ上のすべての測定値は、デルタとして計算されます。

ステップ 2　リストを絞り込んで、より詳細な情報を表示することができます。

- 特定のクラスタ内でこれらのデバイスだけをリストに表示するには、[Select Cluster] リストでクラスタを選択します。Easy VPN は、RAS クラスタの使用をサポートしていないことに注意してください。
- 特定の VPN コンセントレータについて詳細な統計情報を表示するには、[Device] カラムで IP アドレスまたは DNS 名をクリックします。「RAS デバイスの操作」（P.5-4）を参照してください。

参考

表 5-4　[Remote Access Failures]

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な RAS エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Device] カラム	デバイスの DNS 名または IP アドレスが表示されます。 選択したデバイスのパフォーマンスのサマリー グラフを表示するには、[Device] カラムでいずれかのエントリをクリックします。
[Inbound Connect Failure %] カラム	リモートで開始され、フェーズ 1（IKE）またはフェーズ 2（IPSec）で失敗したすべての受信接続試行の割合（パーセンテージ）が表示されます。
[IKE Phase 1 Failure %] カラム	ローカルに開始され、有効化することに失敗したフェーズ 1（IKE）トンネルの割合（パーセンテージ）が表示されます。
[IPSec Phase 2 Failure %] カラム	フェーズ 2（IPSec）で受け取った交換で、無効なために拒否された割合（パーセンテージ）が表示されます。
[Replays] カラム	現在のトンネル、および前のフェーズ 2（IPSec）トンネルのすべてにおいて（アンチリプレイ処理のために）ドロップした受信パケットの合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS デバイスの暗号化アクティビティのモニタリング

検証済みの VPN コンセントレータについて、暗号化アクティビティ データの概要テーブルを表示および操作できます。

（注）　表示される結果には、VPN 3005 コンセントレータまたは VPN 3015 コンセントレータは含まれていません。これらのデバイスは、Scalable Encryption Processor（SEP）カードの代わりにソフトウェアの暗号化を使用します。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Devices] > [Cryptos] を選択します。テーブルのカラムの説明については、表 5-5 を参照してください。

[Remote Access Cryptos] ページ上のすべての測定値は、SEP カード数の整数値を除いて、デルタとして計算されます。

ステップ 2　リストを絞り込んで、より詳細な情報を表示することができます。

- 特定のクラスタ内でこれらのデバイスだけをリストに表示するには、[Select Cluster] リストでクラスタを選択します。Easy VPN は、RAS クラスタの使用をサポートしていないことに注意してください。
- 特定の VPN コンセントレータについて詳細な統計情報を表示するには、[Device] カラムで IP アドレスまたは DNS 名をクリックします。「RAS デバイスの操作」（P.5-4）を参照してください。

参考

表 5-5　[Remote Access Device Cryptos]

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な RAS エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Device] カラム	デバイスの IP アドレスまたは DNS 名が表示されます。 選択したデバイスのパフォーマンス グラフを表示するには、[Device] カラムでいずれかのエントリをクリックします。
[No.Cards] カラム	モニタ対象のデバイスにインストールされている SEP カードの合計数が表示されます。
[Encryption Failure %] カラム	すべての SEP カードにおいて、現在アクティブなフェーズ 2（IPSec）の全トンネルで失敗した送信の暗号化の割合（パーセンテージ）が表示されます。

表 5-5　[Remote Access Device Cryptos]（続き）

エレメント	説明
[Decryption Failure %] カラム	すべての SEP カードにおいて、現在アクティブなフェーズ 2（IPSec）の全トンネルで失敗した受信の復号化の割合（パーセンテージ）が表示されます。
[Packet Drop %] カラム	すべての SEP カードにおいて、フェーズ 1（IKE）およびフェーズ 2（IPSec）のトンネルでドロップしたパケットの割合（パーセンテージ）が表示されます。
[Encrypted Packets] カラム	すべての SEP カードにおいて、暗号化された送信パケットの集約数が表示されます。
[Decrypted Packets] カラム	すべての SEP カードにおいて、復号化された受信パケットの集約数が表示されます。
[Throughput (Kbps)] カラム	すべての SEP カードにおいて、送信（暗号化）および受信（復号化）されたオクテットの集約数（Kbps）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS デバイスの暗号化アクセラレータ カード データの表示

検証済みの VPN コンセントレータについて、暗号化アクセラレータ カード データのテーブルを表示および操作できます。

（注）　表示される結果には、VPN 3005 コンセントレータまたは VPN 3015 コンセントレータは含まれていません。これらのデバイスは、SEP カードの代わりにソフトウェアの暗号化を使用します。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] > [Crypto Status] を選択します。テーブルのカラムの説明については、表 5-6 を参照してください。

[Remote Access Cryptos] ページ上のすべての測定値は、デルタとして計算されます。

ステップ 2　[Select Device] リストから、表示するデバイスを選択します。

参考

表 5-6　[Remote Access Cryptos]

エレメント	説明
[Slot] カラム	SEP カードがインストールされている VPN コンセントレータ内のスロットの数を識別します。
[Status] カラム	SEP カードの機能状態を表すメッセージが表示されます。
[Packets In] カラム	SEP カードの復号化された受信パケットの数が表示されます。
[Packets Out] カラム	SEP カードの暗号化された送信パケットの数が表示されます。

表 5-6　[Remote Access Cryptos]（続き）

エレメント	説明
[Packet Drop %] カラム	フェーズ 1（IKE）トンネルおよびフェーズ 2（IPSec）トンネルでドロップしたパケットの数を、復号化された受信パケットおよび暗号化された送信パケットの割合（パーセンテージ）として表示します。
[Throughput (Kbps)] カラム	SEP カードにおいて、一定期間に暗号化された送信オクテットおよび復号化された受信オクテットの合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

リモート アクセス インターフェイス テーブルの表示

検証済みの VPN コンセントレータについて、インターフェイス ステータス データのテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] > [Interfaces] を選択します。テーブルのカラムの説明については、表 5-7 を参照してください。

[Remote Access Interfaces] ページには、*パブリック インターフェイス*および*プライベート インターフェイス*の情報が表示されます。パブリック（外部）インターフェイスは、パブリック IP アドレスを使用して、外部ネットワークに接続します。プライベート（内部）インターフェイスは、プライベート IP アドレスを使用し、外部ネットワークからは見えません。

[Remote Access Interfaces] ページ上のすべての測定値は、デルタとして計算されます。

ステップ 2　[Select Device] リストから、表示するデバイスを選択します。

参考

表 5-7　[Remote Access Interfaces] ページ

エレメント	説明
[Description] カラム	物理インターフェイスの具体的な説明（DEC 21143A PCI Fast Ethernet など）が示されます。
[Address] カラム	インターフェイスの MAC アドレスが表示されます。
[Type] カラム	TCP/IP がバインドされているフレーム タイプが表示されます。たとえば、表示されたタイプ iso88023-csmacd は、Carrier Sense Multiple Access/Collision Detection（CSMACD; 搬送波感知多重アクセス/衝突検出）に適用される、100 Mb/s ファースト イーサネットのフレーム タイプを示します。
[Access] カラム	[Public] または [Private] のいずれかが表示されます。
[Admin Status] カラム	[Up] または [Down] が表示されます。
[Oper Status] カラム	[Up] または [Down] が表示されます。
[Speed (Kbps)] カラム	インターフェイスの速度（Kbps）が表示されます。

表 5-7　[Remote Access Interfaces] ページ（続き）

エレメント	説明
[Packets In] カラム	前回のポーリング サイクル以降の受信パケットの合計数が表示されます。
[Packets Out] カラム	前回のポーリング サイクル以降の送信パケットの合計数が表示されます。
[Packet Drop %] カラム	前回のポーリング サイクル以降にドロップしたパケットの割合（パーセンテージ）が表示されます。
[Throughput (Kbps)] カラム	インターフェイスにおいて、一定期間に暗号化された送信オクテットおよび復号化された受信オクテットの合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS ユーザの操作

ここでは、RAS ユーザをモニタする次の機能について説明します。

- 「RAS ユーザの詳細の表示」（P.5-12）
- 「RAS デバイスの上位 10 ユーザの識別」（P.5-13）
- 「RAS クラスタの上位 10 ユーザの識別」（P.5-15）

RAS ユーザの詳細の表示

現在の 1 人の RAS VPN ユーザに関して、最新の詳しい接続情報を分離および表示できます。オプションで、検索したユーザをログアウトすることができます。

（注） 対象の RAS VPN コンセントレータに多数のアクティブ セッションがある場合、ユーザ セッションの検索時間が 1 分を超えることがあります。

ヒント 次の内容について、レポートを表示することもできます。

- 選択した傾向タイプに従った、指定した期間における RAS VPN ユーザの上位 10 人のランク。「RAS VPN の上位 10 ユーザ レポートの表示」（P.10-8）を参照してください。
- 指定した期間における、1 人以上の RAS VPN ユーザの VPN セッションの説明。「RAS VPN ユーザ セッション レポートの表示」（P.10-9）を参照してください。

始める前に

ユーザのログアウト機能は、次の場合だけ有効です。

- 自分の CiscoWorks ユーザ ロールが System Administrator または Network Administrator の場合。「ユーザの権限について」（P.3-2）を参照してください。

- 対象の VPN コンセントレータで VPN 3000 Concentrator Series Manager がイネーブルになっており、Performance Monitor が対象のコンセントレータについて、正しい認証クレデンシャルのレコードを持っている場合。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [User Lookup] を選択します。

ステップ 2　次のユーザの詳細情報を入力します。

- [Find User]：ユーザの IP アドレスまたはユーザ名を入力します。
- [Search In]：必要な場合は、1 つのデバイスまたは 1 つのクラスタのいずれかに制限して検索し、その名前または IP アドレスを選択することで検索の対象を特定できます。特定のデバイスまたはクラスタに関する検索を制限しない場合は、[Devices All] を選択します。

ステップ 3　[Go] をクリックします。ユーザが見つかった場合は、次のユーザ セッションの詳細が表示されます。

- [User Name]：ユーザのログイン名。
- [Group Name]：ユーザが属しているユーザ グループ。
- [Cluster Name]：VPN コンセントレータがクラスタ メンバの場合、名前または IP アドレスによってクラスタを識別します。
- [Device Name]：名前または IP アドレスによって VPN コンセントレータを識別します。
- [Client IP Address]：ユーザの IP アドレス。
- [Protocol]：ユーザの接続プロトコル（IPSec over UDP など）。
- [Throughput (Kbps)]：ユーザの平均スループット / 秒。
- [Connection Duration]：日、時間、分、および秒で測定されます。
- [Octet In]：トンネルの開始以降の受信オクテットの合計数。
- [Octet Out]：トンネルの開始以降の送信オクテットの合計数。

ステップ 4　（任意）ユーザ セッションを終了するには、[Logout] をクリックします。

ログアウトが正常に終了すると、指定したユーザがログアウトされ、そのユーザの IP アドレスは、アクティブな RAS セッションを表すテーブルに表示されなくなります。「The user <username> was logged out successfully」というシステム メッセージが表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS デバイスの上位 10 ユーザの識別

Performance Monitor は、検証済みのすべての VPN コンセントレータに接続した、または 1 つのクラスタ内で検証済みのコンセントレータに接続されている上位 10 人のユーザをランキングすることができます。ランキングの値はスループット、接続期間、または 1 ユーザあたりのトラフィック数によって判断されます。

（注）　Performance Monitor は、各 VPN コンセントレータの上位 10 人のユーザをランキングします。次に、全体の上位 10 人のユーザを算出するときに、それらの 10 人のみを対象として互いにランクを決めます。あるコンセントレータに対して上位 10 人に入らないユーザは、（個別のコンセントレータについて 1 位のユーザが持っているスループットまたは帯域幅の要件が、除外されるユーザよりも低い場合でも）全体のランキングから除外されます。したがって、上位 10 人のランキングはおよそのランキングです。

始める前に

ユーザのログアウト機能は、次の場合だけ有効です。

- 自分の CiscoWorks ユーザ ロールが System Administrator または Network Administrator の場合。「ユーザの権限について」（P.3-2）を参照してください。
- 対象の VPN コンセントレータで VPN 3000 Concentrator Series Manager がイネーブルになっており、Performance Monitor が対象のコンセントレータについて、正しい認証クレデンシャルのレコードを持っている場合。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Device Details] > [Top 10 Device Users] を選択します。

[Top 10 Device Users] ページ上のすべての測定値は、デルタではなく整数です。テーブルのカラムについては、表 5-8 を参照してください。

ステップ 2　[Select Device] リストから、表示するデバイスを選択します。

ステップ 3　上位ユーザを算出するランキング基準を、[Compute Using] リストから選択します。次のオプションがあります。

- [Throughput] : kbps 単位で測定されたスループットに従ってユーザをランキングします。
- [Connect Duration] : 現在のセッションの期間（日、時間、分、および秒）に従ってユーザをランキングします。
- [Total Traffic] : 受信および送信パケットの合計に従ってユーザをランキングします。

ステップ 4　必要な場合は、ユーザを切断できます。対象の RAS VPN コンセントレータに多数のアクティブ セッションがある場合、ユーザ セッションを終了するための時間が 1 分を超えることがあります。

ユーザをログアウトするには、対象ユーザのオプション ボタンをクリックし、[Logout] をクリックします。ログアウトが正常に終了すると、対象ユーザがログアウトされ、そのユーザの IP アドレスは、アクティブな RAS セッションを表すテーブルに表示されなくなります。

参考

表 5-8　[Top 10 Device Users]

エレメント	説明
[User] カラム	現在のセッションに関連付けられているユーザ名が表示されます。 **（注）** EzVPN セッションはこの機能をサポートしていません。
[Group] カラム	ユーザ名に関連付けられているユーザ グループ名が表示されます。 ユーザ セッションが Easy VPN サーバとして設定されているルータに関連付けられている場合は、そのグループ名がハイパーリンクされています。このような場合は、リンクをクリックして [Details of the Group Policy] ウィンドウを開きます。「グループ ポリシーの詳細」（P.5-17）を参照してください。
[Public IP Address] カラム	ユーザの IP アドレスが表示されます。
[Protocol] カラム	記載されている VPN セッションで使用中のプロトコルを識別します。
[Traffic In] カラム	受信パケットの合計数が表示されます。
[Traffic Out] カラム	送信パケットの合計数が表示されます。
[Total Traffic] カラム	受信オクテットと送信オクテットを組み合わせた数が表示されます。
[Connect Duration] カラム	ユーザが現在のセッションを確立してから経過した日数、時間、分、および秒が表示されます。
[Throughput (Kbps)] カラム	1 つのユーザ セッションあたりの一定期間の暗号化された送信オクテットおよび復号化された受信オクテットの合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS クラスタの上位 10 ユーザの識別

1 つのクラスタに接続されているすべてのユーザをランキングすることも、すべてのクラスタ間で（Easy VPN ユーザを除く）ユーザをランキングすることもできます。Easy VPN は RAS クラスタの使用をサポートしていません。

Easy VPN ユーザを除いて、一度に 1 人のユーザをログアウトすることができます。

始める前に

ユーザのログアウト機能は、次の場合だけ有効です。

- 自分の CiscoWorks ユーザ ロールが System Administrator または Network Administrator の場合。「ユーザの権限について」（P.3-2）を参照してください。
- 対象の VPN コンセントレータで VPN 3000 Concentrator Series Manager がイネーブルになっており、Performance Monitor が対象のコンセントレータについて、正しい認証クレデンシャルのレコードを持っている場合。

手順

ステップ 1　[Monitor] > [Remote Access VPN] > [Top 10 Cluster Users] を選択します。

[Top 10 Cluster Users] ページ上のすべての測定値は、デルタではなく整数です。

ステップ 2　表示するクラスタを、[Select Cluster] リストから選択します。レポートの対象を特定のクラスタに制限しない場合は、[All] を選択します。

ステップ 3　上位ユーザを算出するランキング基準を、[Compute Using] リストから選択します。次のオプションがあります。

- [Throughput] : kbps 単位で測定されたスループットに従ってユーザをランキングします。
- [Connect Duration] : 現在のセッションの期間（日、時間、分、および秒）に従ってユーザをランキングします。
- [Total Traffic] : 受信および送信パケットの合計に従ってユーザをランキングします。

ステップ 4　必要な場合は、ユーザを切断できます。対象の RAS VPN コンセントレータに多数のアクティブ セッションがある場合、ユーザ セッションを終了するための時間が 1 分を超えることがあります。

ユーザをログアウトするには、対象ユーザのオプション ボタンをクリックし、[Logout] をクリックします。ログアウトが正常に終了すると、対象ユーザがログアウトされ、そのユーザの IP アドレスは、アクティブな RAS セッションを表すテーブルに表示されなくなります。

参考

表 5-9　[Top 10 Cluster Users]

エレメント	説明
[User] カラム	現在のセッションに対して認証されているユーザ名が表示されます。
[Group] カラム	指名ユーザに関連付けられているユーザ グループ名のエントリが表示されます。 ユーザ セッションが Easy VPN サーバとして設定されているルータに関連付けられている場合は、そのグループ名がハイパーリンクされています。このような場合は、リンクをクリックして [Details of the Group Policy] ウィンドウを開きます。「グループ ポリシーの詳細」（P.5-17）を参照してください。 **（注）**　ユーザ セッションが、PIX ファイアウォールまたは VPN 3000 コンセントレータ上の Easy VPN サーバに関連付けられている場合は、グループ名はハイパーリンクされません。
[Public IP] カラム	ユーザのパブリック IP アドレスが表示されます。
[Protocol] カラム	この VPN セッションに対して、IPSec、L2TP、または PPTP のどのレイヤ 2 プロトコルが使用されているかを識別します。
[Traffic In] カラム	受信パケットの数が表示されます。
[Traffic Out] カラム	送信パケットの数が表示されます。
[Total Traffic] カラム	受信オクテットと送信オクテットを組み合わせた数が表示されます。
[Connect Duration] カラム	アクティブなセッションが開始されてから経過した秒数が表示されます。
[Throughput (kbps)] カラム	ユーザ セッションあたりに、受信オクテットに追加された送信オクテットの数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

グループ ポリシーの詳細

次の表は、セッションが、Easy VPN サーバとして設定されているルータに関連付けられている場合に、ユーザ セッションに割り当てられているグループ ポリシーのフィールドについて説明しています。このウィンドウを開く方法については、「RAS デバイスの上位 10 ユーザの識別」（P.5-13）または「RAS クラスタの上位 10 ユーザの識別」（P.5-15）を参照してください。

（注） PIX Security Appliances からの Easy VPN セッションに対しては、同等の情報がありません。

表 5-10　[Details of the Group Policy] ウィンドウ

エレメント	説明
[Group Name] 行	対象のセッション内のユーザ名に関連付けられているユーザ グループ名が表示されます。
[Pool Name] 行	IP ローカル プール アドレスの名前が表示されます。この名前によって、内部 IP アドレスをクライアントへ割り当てるアドレス範囲を定義します。ユーザは少なくとも 1 つのプール名を定義する必要がありますが、各グループ ポリシーに対して別のプールを定義することもできます。この属性は必ず定義し、有効な IP ローカル プール アドレスを参照するようにします。そのようにしないと、クライアントの接続が失敗します。
[DNS Servers] 行	指定されたグループを使用しているすべての DNS サーバについて、IP アドレスのリストをカンマ区切り形式で表示します。
[WINS Servers] 行	指定されたグループを使用しているすべての WINS サーバについて、IP アドレスのリストをカンマ区切り形式で表示します。
[Domain Name] 行	グループが使用している、DNS 解決可能なドメイン名（cisco.com など）が表示されます。
[ACL] 行	どのトラフィックが暗号化されるかを定義する ACL の名前が表示されます。ACL 名は、対象グループに対してスプリットトンネリングが設定されている場合のみ表示されます。
[Backup Gateway] 行	プライマリ Easy VPN サーバへの接続が失敗した場合に、最初に試行するようルータで設定されているバックアップ ゲートウェイの IP アドレスまたはホスト名が表示されます。
[Firewall Are-U-There] 行	VPN セッションが Black Ice または Zone Alarm パーソナル ファイアウォールを通過することを示すように、クライアントがサーバ グループに対してシグナルを送信したかどうかを示します。
[Include-local-lan] 行	（スプリットトンネリングを使用せずに）クライアントおよびローカル ネットワークへの同時接続をサポートしているグループに対して、属性が設定されているかどうかを示します。これは「スタブ」ネットワークと呼ばれることもあり、デフォルトのルート 0.0.0.0/0 上ですべての非ローカル トラフィックを送信します。
[Group Lock] 行	preshred キー認証で IKE を使用する場合に、ユーザが Xauth ユーザ名（グループ名など）を提供できるよう、サーバ グループに対して属性が設定されているかどうかを示します。 **（注）** シスコでは、証明書などの RSA シグニチャ認証メカニズムを使用するクライアントでは、Group-Lock 属性を使用しないことを推奨します。代わりに、このようなクライアントは User-VPN-Group 属性を使用してください。
[Save Password] 行	サーバ グループに対して、クライアント PC 上でユーザが XAuth 証明書をローカルに保存できるようにするオプションがイネーブルになっているかどうかを示します。

CHAPTER 6

サイト間 VPN サービスのモニタリング

サイト間 VPN のモニタリングでは、デバイスおよびトンネルのパフォーマンスの最も重要なすべての指標が、ひと目でわかるように示されます。Performance Monitor では、サイト間の問題が存在しているか、どこに問題があるかを、すぐに判断することもできます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。

サイト間 VPN では、次の間の接続が可能です。

- 組織の本社、遠隔オフィス、および支社。
- 組織のイントラネットおよび信頼できるパートナー、仕入先、顧客、または持ち株会社。

Performance Monitor は、次の場所でサイト間 VPN サービスをモニタします。

- Cisco IOS VPN ルータ。
- サポートされている 1 つ以上のサービス モジュールがインストールされた Cisco Catalyst 6500 シリーズ スイッチ。
- Cisco VPN 3000 シリーズ コンセントレータ。
- 適応型セキュリティ アプライアンス。
- PIX Security Appliances（PIX ファイアウォールとも呼ばれる）。

（注） Performance Monitor では、ある Easy VPN サーバで、サイト間 VPN *または*リモートアクセス VPN の*いずれか*で、サポートされているルータ、アプライアンス、ファイアウォール、およびコンセントレータが VPN ヘッドエンド デバイスのように機能することが可能であっても、すべての Easy VPN セッションが RAS VPN セッションのように示されます。「Easy VPN について」（P.5-2）を参照してください。

ヒント サイト間 VPN サービスの一般的な問題をトラブルシューティングするには、付録のトラブルシューティングを参照してください。

ここでは、サイト間 VPN のモニタリング機能について説明します。

DMVPN について

Cisco IOS ルータの Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）機能は、GRE トンネル、IPSec 暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせて、大規模および小規模の IPsec VPN を作成するための簡潔で拡張性のある方法を提供します。NHRP では、ハブがすべてのスポークに関するパブリック IP アドレスのデータベースを保持しています。DMVPN ネットワークのスポークは、ブート セッション中に自身のパブリック IP アドレスをハブに登録します。ソース スポークはハブ上の NHRP データベースに問い合わせて、宛先スポークのパブリック IP アドレスを取得します。マルチポイント GRE トンネル インターフェイスでは、単一の GRE トンネルが複数の IPSec トンネルをサポートできます。これにより、複雑さが軽減します。

DMVPN は、*ハブツースポーク*、および*スポークツースポーク*の 2 つのコンフィギュレーションをサポートしています。

- ハブツースポーク展開の利点には、次のものがあります。
  - ハブ アンド スポークに対して設定が簡潔で小さくなる。
  - VPN に新しいスポークを追加するためのゼロタッチ プロビジョニング。
  - 動的にアドレス指定されたスポークのサポート。
  - ハブツースポークからのマルチキャスト トラフィックのサポート。
- スポークツースポーク展開の利点には、ハブ アンド スポーク展開のすべての利点が含まれ、さらに次の利点もあります。
  - ダイナミック スポークツースポーク トンネルの方向付け。
  - 仮想フル メッシュへの、小さいスポークによる参加のサポート。

また、Performance Monitor では、第 3 のオプションとして*スポークツーハブ*を選択できます。スポークツーハブは、実際にはユーザが展開できる設定ではありません。Performance Monitor の便利な点は、スポークを選択し、それに関連するハブを簡単に識別できることです。

Performance Monitor では、[Tunnels] ページに DMVPN の使用が表示されます。ここでは、表示されたすべての結果は、[Select Tunnel Type] リストから選択した内容によって制約されています。「サイト間デバイス トンネル テーブルの表示」（P.6-9）を参照してください。

（注）　次の*すべて*を実行した場合、DMVPN スポークツースポーク トンネルに関する大量の E メールを受信する可能性があります。

- スポーク間セッションをサポートするフル メッシュ トポロジを使用するように、DMVPN を設定する。
- サイト間 VPN トンネル ダウン イベントのしきい値を設定する。
- これらのイベントの自動 E メール通知をスケジューリングする。

サイト間トンネルはダイナミックで、多数のトンネル ダウン イベントが含まれる設計により、存続期間が短くなります。この大量の E メールの問題が発生する場合は、E メールの通知をディセーブルにするか、ハブだけをモニタするように Performance Monitor を設定することを推奨します。

DMVPN と Easy VPN の比較

次の表は、DMVPN と Easy VPN の主な違いについてまとめています。Easy VPN の詳細、および Performance Monitor で Easy VPN がどのように表示されるかについては、「Easy VPN について」（P.5-2）を参照してください。

表 6-1　DMVPN と Easy VPN の比較

サービス / 機能名	DMVPN	Easy VPN
マルチキャスト トラフィックのサポート	あり。	—
スポークツースポーク通信	あり。	—
GRE/Quality of Service のサポート	あり。	—
ルーティング プロトコルのサポート	あり。	—
証明書のサポート	あり。	—
ステートフル フェールオーバー	回復用のルーティング プロトコルによって異なる。	あり。
ハブごとのスケーラビリティ	ルーティング プロトコルのため、DMVPN ハブは、1 つのハブでサポートするスポークが少ない。	1 つのハブで多数のスポークをサポートする。
すべてのスポークで同一設定	—	あり。
クロスプラットフォームのサポート	—	あり。
ソフトウェアまたはハードウェア クライアントのサポート	ハードウェア クライアントのみ。	あり。
ハブへのトンネルが常時稼動	あり。	不要。

サイト間デバイスの操作

ここでは、サイト間 VPN サービスを提供する個々のデバイスおよびモジュールのステータスを、どのようにモニタするかについて説明します。

- 「サイト間デバイスの使用とアクティビティのモニタリング」（P.6-3）
- 「サイト間デバイス障害のモニタリング」（P.6-5）
- 「サイト間デバイス暗号化アクティビティのモニタリング」（P.6-5）

サイト間デバイスの使用とアクティビティのモニタリング

ネットワーク内で検証済みのサイト間デバイスまたはサービス モジュールの使用、およびアクティビティ統計情報のテーブルを表示および作業できます。すべてのデバイスを表示することも、特定のグループ内のデバイスを表示することもできます。この概要を使用すると、次のことができます。

- デバイスの使用状況とアクティビティ、デバイス障害、およびデバイスの暗号化アクティビティの説明を分離します。
- サイト間 VPN サービスを提供するデバイスまたはモジュールの状態を要約したチャートおよびグラフを表示します。

サイト間デバイス テーブルを表示するには、[Monitor] > [Site-to-Site VPN] > [Devices] を選択します。このテーブルのカラムの説明については、表 6-2 を参照してください。

このテーブルを使用すると、たとえば次のことができます。

- ユーザ定義の 1 つのデバイス グループのデバイスのみを表示するか、またはすべてのデバイスを表示する。[Select Group] リストからグループ名を選択します。リフレッシュされたページには、指定されたグループのデバイスのみが表示されます。デフォルトでは、すべてのデバイスが表示されます。モニタしているデバイスの中には、ユーザ定義のデバイス グループに属していないものがあります。
- イベント ブラウザを開いて、特定のデバイスまたはサービス モジュールに関する重大なエラー（P1 または P2）のみを表示する。デバイスの [Alert] カラムでアラート アイコンをクリックします。

（注）　重大なエラーがないデバイスまたはモジュールでは、[Alert] カラムが空になっています。

- 1 つのデバイスまたはサービス モジュールの全体の状態を要約するチャートとグラフを表示する。[Device] カラムで DNS 名または IP アドレスをクリックします。
- 1 つのデバイスまたはサービス モジュールに対するスループット グラフを表示する。[Throughput (Kbps)] カラムでハイパーリンクされているエントリをクリックします。
- 1 つのデバイスまたはサービス モジュールに対して、ドロップしたパケットのグラフを表示する。[Packet Drop %] カラムでハイパーリンクされているエントリをクリックします。

表 6-2　[Site-to-Site Devices] テーブル

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。このアイコンをクリックしてイベント ブラウザを開いて、重大なサイト間 VPN エラーのみがフィルタされた内容を表示します。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。 （注）　イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページに表示され続けます。
[Device] カラム	デバイスの IP アドレスまたは DNS 名が表示されます。
[Model] カラム	シスコ デバイスのモデル名が表示されます。
[CPU Usage %] カラム	CPU の全能力に対する使用の平均パーセントが表示されます。
[Memory Usage %] カラム	前回のポーリング サイクル以降に使用したプロセッサの合計メモリ容量に対する、使用の平均パーセンテージが表示されます。
[Throughput (Bps)] カラム	前回のポーリング サイクル以降の、パブリック インターフェイスを介した受信および送信オクテットの合計（バイト）が表示されます。
[No.Tunnels] カラム	前回のポーリング サイクル以降の、アクティブなトンネルと非アクティブなトンネルを組み合わせた数が表示されます。
[Packets In] カラム	前回のポーリング サイクル以降に、アクティブなフェーズ 1（IKE）およびフェーズ 2（IPSec）のトンネルを介して受信したパケット数が表示されます。
[Packets Out] カラム	前回のポーリング サイクル以降に、アクティブなフェーズ 1（IKE）およびフェーズ 2（IPSec）のトンネルを介して送信したパケット数が表示されます。
[Packet Drop %] カラム	前回のポーリング サイクル以降に、フェーズ 1（IKE）トンネルおよびフェーズ 2（IPSec）トンネルでドロップしたパケットの数を、すべての受信および送信パケットの割合（パーセンテージ）として表示します。
[Last Updated] カラム	Performance Monitor がデバイスを最後にポーリングした日付と時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サイト間デバイス障害のモニタリング

検証済みのサイト間デバイスおよびサービス モジュールの操作における障害が記載されているテーブルを表示し、作業するには、[Monitor] > [Site-to-Site VPN] > [Devices] > [Failures] を選択します。

[Site-to-Site Failures] ページ上のすべての測定値は、デルタとして計算されます。カラムについては、表 6-3 を参照してください。

障害テーブルの 1 つのデバイスまたはサービス モジュールの全体の状態を要約するチャートとグラフを表示するには、[Device] カラムで対象の DNS 名または IP アドレスをクリックします。

表 6-3　[Site-to-Site Device Failures]

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。このアイコンをクリックしてイベント ブラウザを開いて、重大なサイト間 VPN エラーのみがフィルタされた内容を表示します。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Device] カラム	デバイスの DNS 名または IP アドレスが表示されます。
[Inbound Connection Failure %] カラム	受信のフェーズ 1（IKE）およびフェーズ 2（IPSec）の接続において、リモートで開始され、失敗したものを、すべての接続の試行（受信および送信）の割合（パーセンテージ）として表示します。
[Outbound Connection Failure %] カラム	送信のフェーズ 1（IKE）およびフェーズ 2（IPSec）の接続において、ローカルで開始され、失敗したものを、すべての送信接続の試行の割合（パーセンテージ）として表示します。
[Replay] カラム	現在のトンネル、および前のフェーズ 2（IPSec）トンネルのすべてにおいて（アンチリプレイ処理のために）ドロップした受信パケットの合計数が表示されます。
[Connection Failure %] カラム	すべての交換において、受信および送信の接続失敗の合計が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サイト間デバイス暗号化アクティビティのモニタリング

検証済みのサイト間デバイスの暗号化アクティビティに関するテーブルを表示し、作業するには、[Monitor] > [Site-to-Site VPN] > [Devices] > [Cryptos] を選択します。

[Site-to-Site Cryptos] ページには、VPN ルータおよび IPSec VPN サービス モジュールの暗号化および復号化アクティビティが示されます。[Site-to-Site Cryptos] ページ上のすべての測定値は、デルタとして計算されます。カラムについては、表 6-4 を参照してください。

暗号化アクティビティ テーブルの 1 つのデバイスまたはサービス モジュールの全体の状態を要約するチャートとグラフを表示するには、[Device] カラムで対象の DNS 名または IP アドレスをクリックします。

表 6-4　[Site-to-Site Cryptos] ページ

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。このアイコンをクリックしてイベント ブラウザを開いて、重大なサイト間 VPN エラーのみがフィルタされた内容を表示します。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Device] カラム	デバイスの DNS 名または IP アドレスが表示されます。
[Packet In] カラム	すべての SEP カードでの、受信パケットの集約数が表示されます。
[Packet Out] カラム	すべての SEP カードでの、送信パケットの集約数が表示されます。
[Packet Drop %] カラム	現在および以前のアクティブなフェーズ 1（IKE）およびフェーズ 2（IPSec）のトンネルでの、最終的に失敗した送信の暗号化の合計数の計算結果が表示されます。
[Encrypt Failure %] カラム	アクティブなフェーズ 2（IPSec）の全トンネルで、最終的に失敗した送信の暗号化の割合（パーセンテージ）が表示されます。
[Decrypt Failure %] カラム	アクティブなフェーズ 2（IPSec）の全トンネルで、最終的に失敗した受信の復号化の割合（パーセンテージ）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サイト間デバイスの詳細の操作

Performance Monitor では、必要なサイト間 VPN のデバイス情報の詳細を表示および作業できます。追加情報については、次のトピックを参照してください。

- 「サイト間デバイスの詳細グラフの表示と意味」（P.6-6）
- 「サイト間デバイス インターフェイス テーブルの表示」（P.6-8）
- 「サイト間デバイス トンネル テーブルの表示」（P.6-9）

サイト間デバイスの詳細グラフの表示と意味

サイト間 VPN で、検証済みデバイスのステータスのグラフィカルな表示を示すことができます。

手順

ステップ 1　[Monitor] > [Site-to-Site VPN] > [Device Details] を選択します。

Performance Monitor では最初に、IP アドレスとして最小の数値を使用しているデバイスのヘルスとパフォーマンスを表すグラフが表示されます。グラフの説明については、表 6-5 を参照してください。

（注）　2 つの縦（Y）軸を使用するグラフを解釈するときに、既知の問題が発生することがあります。最初の Y 軸は常にゼロで始まるのに対し、2 番目の Y 軸は、指定された時間範囲の最も低い値がゼロよりも大きい場合でも、その値で始まります。そのため、2 つの Y 軸を直接比較できないことがあります。

ステップ 2　[Select Device] リストから、グラフを表示するデバイスを選択します。

サイト間グラフの種類

表 6-5　サイト間デバイス グラフの種類

グラフの種類	説明
[CPU Usage]	使用されているデバイスの CPU 能力の割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で使用されている CPU 能力の平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Memory Usage]	使用されているデバイスのメモリ容量の割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内で使用されているメモリ容量の平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Packet Drops]	サイト間 VPN トンネルでドロップしたパケットの割合（パーセンテージ）を示します。 • 縦軸は、特定のポーリング サイクル内でドロップしたパケットの平均（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Throughput vs. No. Tunnels]	長期間のスループットの傾向を 使用中のトンネル数の傾向と比較するうえで有用な折れ線グラフが表示されます。 • 2 種類の情報を表示するため、2 つの縦軸を使用します。 – 左の（オレンジの）縦軸は、特定のポーリング サイクル内の平均スループットを 1 秒あたりのバイト単位で表します。 – 右の（青色の）縦軸は、特定のポーリング サイクル内の平均トンネル数を表します。 • 横軸は、Performance Monitor がそれぞれの縦軸のトレンドを計算した時刻を示します。
[Inbound Connection Failures]	長期にわたる受信接続失敗のトレンドを示します。 • 縦軸は、特定のポーリング サイクル内での失敗の平均数を表します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Outbound Connection Failures]	長期にわたる送信接続失敗のトレンドを示します。 • 縦軸は、特定のポーリング サイクル内での失敗の平均数を表します。 • 横軸は、ポーリング サイクルの時刻を示します。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サイト間デバイス インターフェイス テーブルの表示

サイト間デバイス インターフェイスのパフォーマンスおよびアクティビティ統計情報のテーブルを、表示および作業できます。

手順

ステップ 1　[Monitor] > [Site-to-Site VPN] > [Device Details] > [Interfaces] を選択します。テーブルのカラムの説明については、表 6-6 を参照してください。

[Site-to-Site Interfaces] ページには、クリプト マップにバインドされている、または Internet Assigned Number Authority（IANA）インターフェイス タイプ 131（トンネル）の一部になっているデバイス インターフェイスが示されます。

[Site-to-Site Interfaces] ページ上のすべての測定値は、デルタとして計算されます。

ステップ 2　[Select Device] リストから、表示するデバイスを選択します。

デフォルトでは、VPN インターフェイスのみがテーブルにリストされています。ただし、[Select Interfaces] リストから [All Interfaces] を選択して、デバイスに関するすべてのインターフェイスを表示することができます。

参考

表 6-6　[Site-to-Site Interfaces] ページ

エレメント	説明
[Descr] カラム	物理インターフェイスの特別な説明が示されます。例：DEC 21143A PCI Fast Ethernet。
[Address] カラム	インターフェイスの MAC アドレスが表示されます。
[Admin Status] カラム	[Up] または [Down] のいずれかが表示されます。
[Operation Status] カラム	[Up] または [Down] のいずれかが表示されます。
[Type] カラム	TCP/IP がバインドされているフレーム タイプが表示されます。たとえば、表示されたタイプ **iso88023-csmacd** は、Carrier Sense Multiple Access/Collision Detection（CSMACD; 搬送波感知多重アクセス/衝突検出）に適用される、100 MBits/s ファースト イーサネットのフレーム タイプを示します。
[Speed (Kbps)] カラム	インターフェイスの速度（Kbps）が表示されます。
[Packet In] カラム	前回のポーリング サイクル以降に、インターフェイス上で受信したパケットの合計数が表示されます。
[Packet Out] カラム	前回のポーリング サイクル以降に、インターフェイス上で送信したパケットの合計数が表示されます。
[Packet Drop %] カラム	前回のポーリング サイクル以降にドロップしたパケットの合計割合（パーセンテージ）が表示されます。
[Throughput (Bps)] カラム	インターフェイスの平均スループット率（バイト）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サイト間トンネルの操作

ここでは、サイト間 VPN でのトンネルの操作方法について説明します。

サイト間デバイス トンネル テーブルの表示

検証済みのすべてのサイト間デバイスで、VPN トンネルのテーブルを表示し、それを使用して作業することも、1 つのデバイスについてトンネルを表示することもできます。

トンネルのリストを表示するには、[Monitor] > [Site-to-Site VPN] > [Device Details] > [Tunnels] を選択します。

デフォルトでは、[Tunnels] ページに、検証済みのすべてのサイト間デバイスのトンネルが表示されます。表示される値は、トンネルの開始以降に計算された整数です。

上記のテーブルのドロップダウン リストを使用してリストをフィルタできます。

- [Select Device] : デバイスの IP アドレスを選択して、そのデバイスの VPN トンネルに関する情報を表示します。
- [Select Tunnel Type] : 表示する DMVPN トンネルのタイプを選択するか、またはすべてのサイト間トンネルを表示するか、またはデバイスがどのハブを使用しているかを調べます。
  - [All] : 選択したデバイスに対するすべての DMVPN トンネルが表示されます。
  - [DMVPN Hub-Spoke] : 選択したデバイスに対する、ハブツースポークの DMVPN トンネルだけが表示されます。
  - [DMVPN Spoke-Hub] : このオプションでは、Performance Monitor で、どのハブが、[Select device] リストで選択したスポークに関連付けられているかを簡単に識別できて便利です。
  - [DMVPN Spoke-Spoke] : スポークツースポークの DMVPN トンネルだけが表示されます。これらのトンネルは動的で、多数のトンネル アップ イベントおよびトンネル ダウン イベントを生成するライフタイムが非常に短いことがあります。

次の表に、トンネル テーブルのカラムを示します。

表 6-7　[Tunnels] ページ

エレメント	説明
[Local Endpoint] カラム	トンネルが終了したローカル エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。 DMVPN トンネルの場合は、ハイパーリンクされている IP アドレスをクリックして、リモート IP アドレス、およびトンネルの期限が切れる予定の時刻を表示できます。 **（注）** Performance Monitor の内部で、「ローカル」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。
[Remote Endpoint] カラム	トンネルが終了したリモート エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。 **（注）** Performance Monitor の内部で、「リモート」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。

表 6-7　[Tunnels] ページ（続き）

エレメント	説明
[Local Subnet] カラム	次の 3 つのカラムの値は全体として、1 つのトンネルのアクセス リストを定義しています。 • [Local Subnet]：ローカル エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Remote Subnet]：リモート エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Protocol]：トンネル プロトコルおよび使用したポート（TCP 80 など）が表示されます。
[Remote Subnet] カラム	
[Protocol] カラム	
[Status] カラム	[Up] または [Down] のいずれかが表示されます。
[Active Time] カラム	トンネルのライフタイムを時間、分、および秒単位で表示します。
[Auth Fail In] カラム	トンネルの開始以降の、受信パケットに対する認証失敗の数が表示されます。
[Auth Fail Out] カラム	トンネルの開始以降の、送信パケットに対する認証失敗の数が表示されます。
[Packets In] カラム	トンネル開始以降の受信パケットの数が表示されます。
[Packets Out] カラム	トンネル開始以降の送信パケットの数が表示されます。
[Packet Drop %] カラム	ドロップしたパケットが、トンネル開始以降の、受信および送信パケットのすべての割合（パーセンテージ）として表示されます。
[Throughput (Bps)] カラム	トンネルの開始以降の、トンネルを介した受信および送信オクテットの合計（バイト）が表示されます。
[Last Update] カラム	Performance Monitor がデバイスを最後にポーリングした日付と時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サイト間 VPN トンネルの検索

単一のトンネルを検索および分離し、プロパティを表示することができます。

手順

ステップ 1　[Monitor] > [Site-to-Site VPN] > [Tunnel Lookup] を選択します。

[Site-to-Site Tunnel Lookup] ページが表示されます。

ステップ 2　1 つのトンネルを識別するには、次の値を入力します。

- トンネルが終了した一方の終端の、エンドポイント デバイスのインターフェイスの IP アドレス。
- *同じ*トンネルが終了した*反対の終端*の、エンドポイント デバイスのインターフェイスの IP アドレス。

ステップ 3　[Go] をクリックします。トンネルが見つかると、そのトンネルの詳細がページに表示されます。カラムについては、「サイト間デバイス トンネル テーブルの表示」（P.6-9）を参照してください。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

CHAPTER 7

ファイアウォール サービスのモニタリング

Performance Monitor は、Cisco 適応型セキュリティ アプライアンス、Cisco Secure PIX Firewall デバイス、および Cisco Catalyst 6500 スイッチのファイアウォール サービス モジュール（FWSM）で提供されるファイアウォール サービスの状態を判別します。

ここでは、ファイアウォール モニタリング機能について説明します。

ヒント ファイアウォールの一般的な問題のトラブルシューティングについては、付録の「トラブルシューティング」を参照してください。

ファイアウォール デバイス テーブルの操作

Performance Monitor では、すべての有効なファイアウォール デバイス、モジュール、およびセキュリティ コンテキストが表形式で示され、ひと目で概要を確認できます。このテーブルを使用して、ステータス、使用状況、およびエラーの説明を分離できます。

手順

ステップ 1 [Monitor] > [Firewall] > [Devices] を選択します。テーブルのカラムの説明については、表 7-1 を参照してください。

ステップ 2 次のいずれかを実行して、リストを調整したり、さらに詳細な情報を取得することができます。

- 単一デバイスの仮想コンテキストだけを表示するようにリストを制限するには、[Select Admin Context] リストからデバイスの管理コンテキストを選択します。デフォルト設定では、すべてが表示されます（すべての仮想コンテキストを含む、すべてのファイアウォールがリストされます）。
- イベント ブラウザを開いて、重大なファイアウォール エラーだけを表示するには、[Alert] カラムにアラート アイコンが表示されたときに、このアイコンをクリックします。
- 単一のデバイス、モジュール、またはコンテキストの状態を要約するグラフを表示するには、デバイス、モジュール、またはコンテキストの IP アドレスまたは DNS 名が [Device] カラムに表示されたときに、これをクリックします。

参考

表 7-1　[Firewall Devices] ページ

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大なファイアウォール エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。 （注）　イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページに表示され続けます。
[Device] カラム	関連するファイアウォールの DNS 名または IP アドレスが表示されます。 （注）　ルータは、少なくとも 1 つのインターフェイスが検査ポリシーを使用して設定されている場合だけ、[Firewall Devices] ページに表示されます。
[Model] カラム	関連するアプライアンス、デバイス、またはサービス モジュールのハードウェア モデルを示しています。
[Version] カラム	関連するファイアウォールにインストールされている Cisco Firewall ソフトウェア リリース バージョンを示します。
[Memory Usage %] カラム	関連するファイアウォールが使用しているメモリのバイトの割合が表示されます。
[CPU Usage %] カラム	現在使用されている CPU 能力の割合が表示されます。これは、最近 5 秒間の平均です。
[No.Connections] カラム	関連するファイアウォールでアクティブな接続の合計数が表示されます。
[Xlates] カラム	関連するファイアウォールでアクティブな変換の数が表示されます。
[Packet Rate In] カラム	すべてのインターフェイスにわたる、受信パケットの現在のレートの合計が表示されます。
[Packet Rate Out] カラム	すべてのインターフェイスにわたる、送信パケットの現在のレートの合計が表示されます。
[No.Errors] カラム	前回のポーリング サイクル以降に発生した受信パケット エラーの数が、すべてのファイアウォール インターフェイスで集約されて表示されます。
[Throughput (Kbps)] カラム	前回のポーリング サイクル以降の関連するファイアウォールの 1 秒あたりの平均スループット速度が、すべてのインターフェイスで集約されて表示されます。
[Last Updated] カラム	表示された値がポーリングまたはトラップによって提供された時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

ファイアウォール デバイスの詳細の操作

ここでは、単一のファイアウォール デバイスまたはモジュール用のモニタリング機能について説明します。

- 「デバイスまたはモジュールの詳細グラフの表示と意味」（P.7-3）

- 「デバイスまたはモジュール インターフェイス テーブルの表示」（P.7-4）
- 「デバイスまたはモジュール ブロック テーブルの表示」（P.7-5）
- 「デバイスまたはモジュール接続テーブルの表示」（P.7-5）

デバイスまたはモジュールの詳細グラフの表示と意味

1 つの検証済みファイアウォール デバイスまたはモジュールの CPU 使用状況、メモリ使用状況、インターフェイス エラー、スループット、および接続を示すグラフを表示および操作できます。

ステップ 1　[Select Monitor] > [Firewall] > [Device Details] を選択します。

デフォルトでは、Performance Monitor は、IP アドレスとして最も低い番号を使用するデバイスまたはモジュールのヘルスとパフォーマンスを示すグラフを表示します。グラフの説明については、表 7-2 を参照してください。

（注）　2 つの縦（Y）軸を使用するグラフを解釈するときに、既知の問題が発生することがあります。最初の Y 軸は常にゼロで始まるのに対し、2 番目の Y 軸は、指定された時間範囲の最も低い値がゼロよりも大きい場合でも、その値で始まります。そのため、2 つの Y 軸を直接比較できないことがあります。

ステップ 2　[Select Device] リストから、グラフを表示するデバイスを選択します。

ファイアウォールのグラフの種類

表 7-2　ファイアウォール デバイスのグラフの種類

グラフの種類	説明
[CPU Usage]	使用されたデバイスまたはモジュールの CPU 能力の割合を示します。 • 縦軸は、関連するポーリング サイクルで使用された CPU 能力の割合の平均を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Memory Usage]	使用されたデバイスまたはモジュールのメモリ容量の割合を示します。 • 縦軸は、関連するポーリング サイクルで使用されたメモリ容量の割合の平均を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Throughput vs. Connection]	長期にわたるスループットのトレンドと接続のトレンドを比較するのに役立つ折れ線グラフが表示されます。 • 2 種類の情報を表示するため、2 つの縦軸を使用します。 – 左の（オレンジ色の）縦軸は、関連するポーリング サイクルでの平均スループットをバイト単位で示します。 – 右の（青の）縦軸は、関連するポーリング サイクルでのファイアウォール接続数の平均を示します。 • 横軸は、Performance Monitor がそれぞれの縦軸のトレンドを計算した時刻を示します。

表 7-2　ファイアウォール デバイスのグラフの種類（続き）

グラフの種類	説明
[Interface Error]	長期にわたるデバイスまたはモジュール インターフェイス エラーのトレンドを示します。 • 縦軸は、関連するポーリング サイクルで発生したエラーの平均数を示します。 • 横軸は、ポーリング サイクルの時刻を示します。

デバイスまたはモジュール インターフェイス テーブルの表示

1 つの検証済みのファイアウォール デバイスまたはモジュールのインターフェイス パフォーマンス統計情報テーブルを、表示および操作できます。

（注）　検査ポリシーが設定されているルータのインターフェイスが、[Firewall Interfaces] ページに表示されます。ただし、PIX、ASA、および FWSM デバイスの場合は、すべてのインターフェイスが表示されます。

手順

ステップ 1　[Monitor] > [Firewall] > [Device Details] > [Interfaces] を選択します。テーブルのカラムの説明については、表 7-3 を参照してください。

[Firewall Interfaces] ページのすべての測定値は、*デルタ*として計算されます。つまり、あるポーリング サイクルから次のポーリング サイクルまでの差の範囲を示します。

ステップ 2　[Select Device] リストから、詳細を表示するデバイスを選択します。

参考

表 7-3　[Firewall Interfaces] ページ

要素	説明
[Name] カラム	デバイスの DNS 名または IP アドレスが表示されます。
[Speed (Kbps)] カラム	関連するインターフェイスを通るトラフィック フローの平均速度（キロビット）が表示されます。
[Bytes In] カラム	前回のポーリング サイクル以降のインターフェイスでの受信バイトの合計数が表示されます。
[Bytes Out] カラム	前回のポーリング サイクル以降のインターフェイスでの送信バイトの合計数が表示されます。
[Packets In] カラム	前回のポーリング サイクル以降のインターフェイスでの受信パケットの合計数が表示されます。

表 7-3　[Firewall Interfaces] ページ（続き）

要素	説明
[Packets Out] カラム	前回のポーリング サイクル以降のインターフェイスでの送信パケットの合計数が表示されます。
[Packet Errors] カラム	前回のポーリング サイクル以降にインターフェイスで発生したパケット エラーの合計数が表示されます。
[Bandwidth Utilization %] カラム	デバイス タイプごとに異なる値が表示されます。 • PIX：使用中の帯域幅容量の割合が表示されます。 • ファイアウォール サービス モジュール：「N/A」と表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

デバイスまたはモジュール ブロック テーブルの表示

ブロックとは、パケットを処理する内部バッファです。[Firewall Blocks] テーブルに表示される値は、1 つの検証済みのファイアウォール デバイスまたはモジュールのブロックの状態を示しています。ファイアウォール ブロック統計情報テーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Firewall] > [Device Details] > [Blocks] を選択します。

デフォルトでは、[Firewall Blocks] ページには、IP アドレスとして最も低い番号を使用するデバイスまたはモジュールのブロック情報が表示されます。

ステップ 2　[Select Device] リストから、詳細を表示するデバイスを選択します。各カラムで、次の情報を示します。

- [Block Size]：ブロック サイズをバイト単位で表示します。
- [No.Available]：使用可能なブロックの数を表示します（関連するブロックのサイズ単位）。
- [No.In Use]：使用中のブロックの数を表示します（関連するブロックのサイズ単位）。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

デバイスまたはモジュール接続テーブルの表示

ファイアウォールは、接続要求の目的とプロトコルを調べてから、接続を許可または拒否します。1 つの検証済みのファイアウォール デバイスまたはモジュールの接続統計情報テーブルを、表示および操作できます。

手順

ステップ 1　[Monitor] > [Firewall] > [Device Details] > [Connections] を選択します。

各行には、記述されている値に関して 1 秒ごとに計算された変化のレートが表示されます（レートの種類は、測定値の各インスタンスで指定されます）。

Performance Monitor は、常に各値を再計算しているため、ある 1 秒間に関連する変化がなかった場合、行に値ゼロ（0）が表示されることがあります。

表示された値は累積値ではありません。値は、表示がリフレッシュされるときに増加したり減少したりすることがあります。

（注）　設定されていないファイアウォール機能については、常に値ゼロが表示されます。

ステップ 2　[Select Device] リストから、詳細を表示するデバイスを選択します。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

CHAPTER 8

ロードバランシング サービスのモニタリング

ロードバランシングは、ネットワーク トラフィックが複数のパスを通って指定の宛先へ到達できるようにするテクノロジーです。ロードバランシングは、ユーザに対して負荷分散が透過になるように、着信したサービス要求を複数のサーバへ均等に分散します。

コンテンツ スイッチングはサーバのロードバランシングの一種です。これは、サーバの負荷およびコンテンツのアベイラビリティに基づいて、Web サーバ間でトラフィックの負荷を均等にするものです。

Performance Monitor は、Cisco Catalyst 6500 シリーズ スイッチにインストールされている、検証済みの Content-Switching Service Module（CSM; コンテンツ スイッチング サービス モジュール）のモニタリングをサポートしています。

（注） Performance Monitor は、Cisco VPN 3000 コンセントレータのクラスタ ロード バランシング機能またはクラスタ ロード バランシング パフォーマンスはモニタしません。

ここでは、ネットワーク内の Web サーバのロード バランシング サービスを行う次の機能について説明します。

- 「コンテンツ スイッチングの概念」（P.8-1）
- 「モジュールの集合的モニタリング」（P.8-2）
- 「モジュールの個別モニタリング」（P.8-5）

ヒント ロードバランシング サービスの一般的な問題をトラブルシューティングするには、付録のトラブルシューティングを参照してください。

コンテンツ スイッチングの概念

コンテンツ スイッチは、Web コンテンツのアベイラビリティおよび Web サーバ上の負荷を分析します。コンテンツ スイッチは、この分析結果を使用してサーバ間でトラフィックの負荷を均等にし、Web サイトのエンドユーザにとって透過な方法で、Web コンテンツの配信を促進します。

コンテンツ スイッチが正しく設定されていると、次のようになります。

- Web サイトの応答性が改善される。
- 帯域幅の広いファイルを、きめ細かく効率よく配信する。
- ネットワークの輻輳が低減する。
- ネットワークおよびサーバ内でリソースの使用率が最適化される。

- Web アプリケーション プラットフォームのパフォーマンスとスケーラビリティが改善される。

コンテンツ スイッチング サービス モジュールの目的

コンテンツ スイッチング サービス モジュール（CSM）には、レイヤ 4 からレイヤ 7 のパケット情報に基づいて、ネットワーク デバイスと *サーバ ファーム*間に、高性能の接続を提供します。クライアントは、*仮想サーバ*に関連付けられている Virtual IP Address（VIP; 仮想 IP アドレス）を提供することで、CSM へ接続します。クライアントが仮想サーバへの接続を開始すると、CSM は、設定されているロードバランシング アルゴリズムおよびポリシーに基づいて、接続のための *実サーバ*を選択します。

仮想サーバ	仮想サーバは、CSM に設定されているポリシーを通じて、実サーバ ファームを使用します。
実サーバ	実サーバは、サーバ ファームに割り当てられている物理デバイスまたは仮想デバイスです。実サーバは、負荷が均等化されたサービスを提供します。サーバがクライアントの要求を受け取ると、サーバはディスクから一致する情報を引き出して、それがクライアントに転送されるよう、CSM に送信します。
サーバ ファーム	サーバ ファームまたはサーバ プールは、同じコンテンツを含んでいるサーバのコレクションです。サーバ ファームを設定し、それをサーバに追加する場合、および仮想サーバにサーバ ファームをバインドする場合には、サーバ ファームの名前を指定します。

Performance Monitor では CSM をモニタし、実サーバのネットワーク セッションおよびサーバの負荷状況を追跡して、セッションを最適なサーバに振り向けることができます。

モジュールの集合的モニタリング

ここでは、CSM モジュールを集合的にモニタする方法を説明します。

CSM の使用とアクティビティ統計情報の表示

ネットワーク上のすべての有効な CSM モジュールの使用状況およびアクティビティ統計情報を表示できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [ModulesSelect] を選択します。テーブルのカラムの説明については、表 8-1 を参照してください。

[Load Balancing Modules] ページのすべての測定値は、*デルタ*として計算されます（あるポーリング サイクルから次のポーリング サイクルまでの差の範囲を示します）。ただし、現在の接続数は整数です。

ステップ 2　1 つの CSM モジュールの詳細グラフを表示するには、[Chassis:Module] カラムで関連するエントリをクリックします。

参考

表 8-1　[Load Balancing Modules] ページ

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な CSM エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。 **（注）**　イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページに表示され続けます。
[Chassis:Module] カラム	対象の Catalyst 6500 スイッチの IP アドレス、および CSM モジュールがインストールされている番号付きのスロットが表示されます。
[No.Current Connections] カラム	CSM 接続の現在の数が表示されます。
[No.Created Connections] カラム	前回のポーリング サイクル以降に作成された CSM 接続の合計数が表示されます。
[No.Destroyed Connections] カラム	前回のポーリング サイクル以降に破棄された CSM 接続の合計数が表示されます。
[Last Updated] カラム	表示された値がポーリングまたはトラップによって提供された時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

ロード バランシングの障害統計情報の表示

検証済みの CSM モジュールの操作における障害が記載されているテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [Failures] を選択します。テーブルのカラムの説明については、表 8-2 を参照してください。

[Load Balancing Failures] ページのすべての測定値は、デルタとして計算されます。

ステップ 2　1 つの CSM モジュールの要約グラフを表示するには、[Chassis:Module] カラムで関連するエントリをクリックします。

参考

表 8-2　[Load Balancing Failures] ページ

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な CSM エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Chassis:Module] カラム	対象の Catalyst 6500 スイッチの IP アドレス、および CSM モジュールがインストールされている番号付きのスロットが表示されます。
[No.Failed Connections] カラム	失敗した接続の合計数が表示されます。
[Failed Connections %] カラム	結果として失敗した接続の割合（パーセンテージ）が表示されます。
[No.Dropped Connections] カラム	ドロップした接続の合計数が表示されます。
[Dropped Connections %] カラム	全接続に対するドロップした接続の割合（パーセンテージ）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

サーバおよびポリシーの拒否統計情報の表示

検証済みの CSM モジュールに関する拒否統計情報のテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [Rejects] を選択します。テーブルのカラムの説明については、表 8-3 を参照してください。

[Load Balancing Rejects] ページのすべての測定値は、デルタとして計算されます。

ステップ 2　1 つの CSM モジュールの要約グラフを表示するには、[Chassis:Module] カラムで関連するエントリをクリックします。

参考

表 8-3　[Load Balancing Rejects] ページ

エレメント	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な CSM エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Chassis:Module] カラム	対象の Catalyst 6500 スイッチの IP アドレス、および CSM モジュールがインストールされている番号付きのスロットが表示されます。
[No.of No Active Server Rejects] カラム	対象のサーバ ファームにアクティブなサーバがなかったために拒否された接続の数が表示されます。
[No.of No Match Policy Rejects] カラム	設定されているいずれのポリシーとも一致しなかったために拒否された接続の数が表示されます。
[No.of No Config Policy Rejects] カラム	一致する仮想サーバが、いずれかのポリシーで設定されていなかったために拒否された接続の数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

モジュールの個別モニタリング

ここでは、CSM モジュールを個別にモニタする方法を説明します。

- 「モジュールの詳細グラフの表示と意味」（P.8-5）
- 「仮想サーバ テーブルの表示」（P.8-6）
- 「実サーバ テーブルの表示」（P.8-7）
- 「インターフェイス テーブルの表示」（P.8-8）

モジュールの詳細グラフの表示と意味

1 つの検証済みの CSM モジュールの詳細グラフのページを、表示および操作できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [Module Details] を選択します。

デフォルトでは、Performance Monitor は、IP アドレスとして最も低い番号を使用するモジュールのヘルスとパフォーマンスを説明するグラフを表示します。グラフの説明については、表 8-4 を参照してください。

ステップ 2　[Select Chassis:Module] リストから、表示する CSM モジュールの IP アドレスとスロット番号を選択します。

ロード バランシング グラフの種類

表 8-4　ロード バランシング モジュール グラフの意味

ラベル	説明
[Connection Failures]	長期にわたるモジュールの接続失敗のトレンドを示します。 • 縦軸は、特定のポーリング サイクル内での障害の割合（パーセンテージ）を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Dropped Connection]	長期にわたるドロップされた接続のトレンドを示します。 • 縦軸は、特定のポーリング サイクル内でドロップした接続の平均数を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Current Connections]	長期間にわたる成功した接続のトレンドを示します。 • 縦軸は、特定のポーリング サイクル内で成功した接続の平均数を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Total Rejects]	長期間にわたる拒否された接続のトレンドを示します。 • 縦軸は、次の値の一定期間の合計平均を示します。 – 対象のサーバ ファームにアクティブなサーバがなかったために拒否された接続の数。 – 設定されているいずれのポリシーとも一致しなかったために拒否された接続の数。 – 一致する仮想サーバが、いずれかのポリシーで設定されていなかったために拒否された接続の数。 • 横軸は、ポーリング サイクルの時刻を示します。

仮想サーバ テーブルの表示

1 つの検証済みの CSM モジュールに関する仮想サーバ統計情報のテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [Virtual Servers] を選択します。テーブルのカラムの説明については、表 8-5 を参照してください。

[Load Balancing Virtual Servers] ページには、特定の CSM モジュールに関連付けられているすべての仮想サーバの情報が表示されます。

ステップ 2　[Select Chassis:Module] リストから、表示する CSM モジュールの IP アドレスとスロット番号を選択します。

参考

表 8-5　[Load Balancing Virtual Servers] ページ

エレメント	説明
[Name] カラム	CSM 上に設定されている仮想サーバの名前が表示されます。
[Address] カラム	対象の仮想サーバの IP アドレスが表示されます。
[Port] カラム	対象のコンテンツ タイプを管理する仮想サーバの論理ポートが表示されます。
[State] カラム	仮想サーバの機能状態が表示されます。
[No.Current Connections] カラム	アクティブな接続の数が表示されます。
[No.Total Connections] カラム	前のポーリング サイクル以降の接続の合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

実サーバ テーブルの表示

1 つの検証済みの CSM モジュールに関する実サーバ統計情報のテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [Real Servers] を選択します。テーブルのカラムの説明については、表 8-6 を参照してください。

[Load Balancing Real Servers] ページには、特定の CSM モジュールに関連付けられているすべての実サーバの情報が表示されます。

ステップ 2　[Select Chassis:Module] リストから、表示する CSM モジュールの IP アドレスとスロット番号を選択します。

参考

表 8-6　[Load Balancing Real Servers]

エレメント	説明
[Server Farm] カラム	サーバ ファームの名前が表示されます。
[Address] カラム	実サーバの IP アドレスが表示されます。
[Port] カラム	実サーバのポート番号が表示されます。
[State] カラム	実サーバの状態が表示されます。
[No.Current Connections] カラム	アクティブな接続の数が表示されます。
[No.Total Connections] カラム	前のポーリング サイクル以降の接続の合計数が表示されます。
[No.Total Failed Connections] カラム	前回のポーリング サイクル以降に失敗した接続の合計数が表示されます。
[Connection Failed %] カラム	前回のポーリング サイクル以降に失敗した接続の割合（パーセンテージ）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

インターフェイス テーブルの表示

1 つの検証済みの CSM モジュールに関するインターフェイス統計情報のテーブルを表示および操作できます。

手順

ステップ 1　[Monitor] > [Load Balancing] > [Interfaces] を選択します。テーブルのカラムの説明については、表 8-7 を参照してください。

[Load Balancing Interfaces] ページの統計情報には、CSM モジュール インターフェイスに関連付けられた、経路設定済み VLAN が示されます。

[Load Balancing Interfaces] ページ上のすべての測定値は、デルタとして計算されます。

ステップ 2　[Select Chassis:Module] リストから、表示する CSM モジュールの IP アドレスとスロット番号を選択します。

参考

表 8-7　[Load Balancing Interfaces]

エレメント	説明
[Descr] カラム	物理インターフェイスの特別な説明が示されます。例：`DEC 21143A PCI Fast Ethernet`。
[Address] カラム	インターフェイスの MAC アドレスが表示されます。
[Admin Status] カラム	管理ステータスが表示されます。
[Operation Status] カラム	動作状態が表示されます。
[Type] カラム	TCP/IP がバインドされているフレーム タイプが表示されます。たとえば、表示されたタイプ **iso88023-csmacd** は、Carrier Sense Multiple Access/Collision Detection（CSMACD; 搬送波感知多重アクセス / 衝突検出）に適用される、100 MBits/s ファースト イーサネットのフレーム タイプを示します。
[Speed (Kbps)] カラム	インターフェイスの速度（Kbps）が表示されます。
[Packets In] カラム	前回のポーリング サイクル以降のインターフェイスでの受信パケットの合計数が表示されます。
[Packets Out] カラム	前回のポーリング サイクル以降のインターフェイスでの送信パケットの合計数が表示されます。
[Packet Drop %] カラム	前回のポーリング サイクル以降にドロップしたパケットの合計数が表示されます。
[Throughput (Kbps)] カラム	前回のポーリング サイクル以降の、インターフェイスを通じた受信および送信オクテットの合計（Kbps）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

CHAPTER 9

SSL サービスのモニタリング

Performance Monitor 機能を使用すると、Secure Socket Layer（SSL）モジュールの動作およびパフォーマンスの重要な点を、リアルタイムでモニタおよび解釈できます。

ここでは、SSL モジュール モニタリング機能について説明します。

SSL の概念

Secure Socket Layer（SSL）は、プライバシー、認証、およびデータ整合性によってデータの安全な転送を可能にするプロトコルです。SSL では証明書、公開キー、および秘密キーを使用します。

ここでは、SSL モニタリングを理解するために必要な情報を示します。

SSL モジュールの目的

SSL サービス モジュールは、Cisco Catalyst 6500 シリーズ スイッチの統合型モジュールです。Series 6500 スイッチの任意のポートがネットワーク上の Web サーバのプロキシ SSL ポートである場合、このサーバから、リソースを大量に消費する SSL 機能をオフロードできます。1 つの SSL モジュールが複数の Web サーバのプロキシとして動作できます。

SSL モジュールは、暗号化された Web トラフィックの配送を高速化し、すべての SSL 関連タスクを実行します（Web 対応アプリケーションの配送を含みます）。そのため、Web サーバは、独自の SSL 機能を実行するよりも高速かつ大量に、暗号化されていない Web コンテンツを配送できます。

適切に設定された SSL モジュールは、次のように機能します。

- Web サイトがサポートするセキュア接続の数を増やします。
- Web サーバがより多くのコンテンツ要求を処理できるようにします。
- サーバのロード バランシングを提供します。

SSL モジュールのパフォーマンス

Catalyst 6500 スイッチのシャーシには、最大 4 台の SSL モジュールを搭載できます。最適化された状況下では、各 SSL モジュールが以下を提供します。

- 1 秒あたり最大 2,500 の接続セットアップ。4 台のモジュールが設置されている場合、1 シャーシあたり 10,000。
- 最大 300 Mbps のバルク暗号化スループット。4 台のモジュールが設置されている場合、1 シャーシあたり 12.2 Gbps。
- 最大 60,000 の同時接続。4 台のモジュールが設置されている場合、1 シャーシあたり 240,000。

各 SSL モジュールは、独自の CPU と独自の IP アドレスを持ちます。

SSL モジュールが正しく設定されていない場合、または正しく動作していない場合、ネットワーク上の暗号化された Web サービス、および暗号化されていない Web サービスが低下することがあります。

ネットワーク上の SSL モジュールで提供されるサービス レベルが、指定されている性能を下回っていると判断される場合は、ネットワーク管理ツールで原因を切り分け、修正アクションを実行できます。

モジュールの集合的モニタリング

ここでは、SSL モジュールを集合的にモニタする方法を説明します。

- 「SSL 使用状況およびアクティビティ統計情報の操作」（P.9-2）
- 「SSL 統計情報の操作」（P.9-3）
- 「TCP 接続統計情報の操作」（P.9-4）

SSL 使用状況およびアクティビティ統計情報の操作

ネットワーク上のすべての有効な SSL モジュールの使用状況およびアクティビティ統計情報を表示できます。

手順

ステップ 1　[Monitor] > [SSL] > [Modules] を選択します。テーブルのカラムの説明については、表 9-1 を参照してください。

ステップ 2　1 つの SSL モジュールの詳細グラフを表示するには、[Module] カラムで、関連する IP アドレスをクリックします。

参考

表 9-1　[SSL Modules] ページ

要素	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な SSL エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。 **（注）** イベントをクリアした後、1 分経過するか、ページがリフレッシュされるかのいずれか早い方まで、アラート アイコンはデバイス モニタリング ページに表示され続けます。
[Module] カラム	SSL モジュールの IP アドレスが表示されます。
[Version] カラム	SSL モジュールのソフトウェア バージョンが表示されます。
[Memory Usage %] カラム	関連する SSL モジュールが使用しているメモリのバイトの割合が表示されます。
[CPU Usage %] カラム	現在使用されている SSL モジュールの CPU 能力の割合が表示されます。これは、最近 5 秒間の平均です。
[No.Active Sessions] カラム	SSL モジュールでアクティブなセッションの数が表示されます。
[Last Updated] カラム	表示された値がポーリングまたはトラップによって提供された時間が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

SSL 統計情報の操作

すべての有効な SSL モジュールの SSL アクティビティ統計情報のテーブルを、表示および操作できます。

ステップ 1　[Monitor] > [SSL] > [Statistics] を選択します。テーブルのカラムの説明については、表 9-2 を参照してください。

[SSL Statistics] ページのすべての測定値は、*デルタ*として計算されます（あるポーリング サイクルから次のポーリング サイクルまでの差の範囲を示します）。ただし、アクティブ セッションおよびアクティブ接続の数は整数です。

ステップ 2　1 つの SSL モジュールの要約グラフを表示するには、[Module] カラムで、関連する IP アドレスまたは DNS 名をクリックします。

参考

表 9-2　[SSL Statistics] ページ

要素	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な SSL エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。
[Module] カラム	モジュールの IP アドレスが表示されます。
[Connects Attempted] カラム	前回のポーリング サイクル以降に試行された SSL 接続の合計数が表示されます。
[Connects Completed] カラム	前回のポーリング サイクル以降に正常に完了した SSL 接続の合計数が表示されます。
[Connects Active] カラム	アクティブな SSL 接続の数が表示されます。
[Active Sessions] カラム	アクティブな SSL セッションの合計数が表示されます。
[Handshake Failures] カラム	前回のポーリング サイクル以降に発生したハンドシェイク失敗の数が表示されます。
[Data Failures] カラム	前回のポーリング サイクル以降に発生したデータ障害の数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

TCP 接続統計情報の操作

すべての有効な SSL モジュールの TCP 接続統計情報のテーブルを、表示および操作できます。

ステップ 1　[Monitor] > [SSL] > [TCP Connections] を選択します。テーブルのカラムの説明については、表 9-3 を参照してください。

[SSL TCP Statistics] ページのすべての測定値は、デルタとして計算されます。

ステップ 2　1 つの SSL モジュールの要約グラフを表示するには、[Module] カラムで、関連する IP アドレスまたは DNS 名をクリックします。

参考

表 9-3　[SSL TCP Connections] ページ

要素	説明
[Alert] カラム	重大度が高い問題または障害が発生した場合に、アラート アイコンが表示されます。アイコンをクリックすると、イベント ブラウザが開き、重大な SSL エラーだけが表示されるようにフィルタ処理された画面が表示されます。「インターフェイスのアイコンについて」（P.3-5）を参照してください。 イベント ブラウザ要素のリファレンス情報については、「イベント ブラウザ ウィンドウ」（P.3-15）を参照してください。

表 9-3　[SSL TCP Connections] ページ（続き）

要素	説明
[Module] カラム	モジュールの IP アドレスが表示されます。
[Connects Init] カラム	前回のポーリング サイクル以降に開始された TCP 接続の数が表示されます。
[Connects Established] カラム	前回のポーリング サイクル以降に確立された TCP 接続の数が表示されます。
[Connects Accepted] カラム	前回のポーリング サイクル以降に受け入れられた TCP 接続の数が表示されます。
[Connects Dropped] カラム	前回のポーリング サイクル以降にドロップされた TCP 接続の数が表示されます。
[Connects Closed] カラム	前回のポーリング サイクル以降に終了された TCP 接続の数が表示されます。
[Packet Sent] カラム	前回のポーリング サイクル以降に送信されたパケットの合計数が表示されます。
[Packet Received] カラム	前回のポーリング サイクル以降に受信されたパケットの合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

モジュールの個別モニタリング

ここでは、有効な SSL モジュールを個別にモニタする方法を説明します。

- 「モジュールの詳細グラフの表示と意味」（P.9-5）
- 「SSL プロキシ統計情報テーブルの表示」（P.9-6）
- 「SSL プロキシ エラー テーブルの表示」（P.9-7）

モジュールの詳細グラフの表示と意味

1 つの検証済みの SSL モジュールの詳細グラフのページを、表示および操作できます。

手順

ステップ 1　[Monitor] > [SSL] > [Module Details] を選択します。

デフォルトでは、Performance Monitor は、IP アドレスとして最も低い番号を使用するモジュールのヘルスとパフォーマンスを説明するグラフを表示します。グラフの説明については、表 9-4 を参照してください。

（注）　2 つの縦（Y）軸を使用するグラフを解釈するときに、既知の問題が発生することがあります。最初の Y 軸は常にゼロで始まるのに対し、2 番目の Y 軸は、指定された時間範囲の最も低い値がゼロよりも大きい場合でも、その値で始まります。そのため、2 つの Y 軸を直接比較できないことがあります。

ステップ 2　[Select Device] リストから、グラフを表示するデバイスを選択します。

SSL モジュール グラフの種類

表 9-4　SSL モジュール グラフの意味

ラベル	説明
[CPU Usage]	使用されたモジュールの CPU 能力の割合を示します。 • 縦軸は、関連するポーリング サイクルで使用された CPU 能力の割合の平均を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Memory Usage]	使用されたモジュールのメモリ容量の割合を示します。 • 縦軸は、関連するポーリング サイクルで使用されたメモリ容量の割合の平均を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Error Rate]	長期にわたるモジュール インターフェイス エラーのトレンドを示します。 • 縦軸は、関連するポーリング サイクルで発生したエラーの平均数を示します。 • 横軸は、ポーリング サイクルの時刻を示します。
[Throughput vs. Connections]	長期にわたるスループットのトレンドと接続のトレンドを比較するのに役立つ折れ線グラフが表示されます。 • 2 種類の情報を表示するため、2 つの縦軸を使用します。 – 左の（青の）縦軸は、関連するポーリング サイクルでの平均スループットをバイト単位で示します。 – 右の（赤の）縦軸は、関連する時間での SSL 接続数の平均を示します。 • 横軸は、Performance Monitor がそれぞれの縦軸のトレンドを計算した時刻を示します。

SSL プロキシ統計情報テーブルの表示

1 つの検証済みの SSL モジュールのプロキシ統計情報のテーブルを、表示および操作できます。

手順

ステップ 1　[Monitor] > [SSL] > [Proxy Statistics] を選択します。テーブルのカラムの説明については、表 9-5 を参照してください。

[SSL Proxy Statistics] ページのすべての測定値は、デルタとして計算されます。

ステップ 2　[Select Device] リストから、表示するデバイスを選択します。

参考

表 9-5　[SSL Proxy Statistics]

要素	説明
[Proxy] カラム	プロキシ サービス名が表示されます。
[Connects Attempted] カラム	前回のポーリング サイクル以降に試行された、関連するプロキシ サービスの接続の合計数が表示されます。
[Connects Completed] カラム	前回のポーリング サイクル以降に正常に完了した、関連するプロキシ サービスの接続の合計数が表示されます。

表 9-5　[SSL Proxy Statistics]（続き）

要素	説明
[Connects in Handshake] カラム	関連するプロキシ サービスの、ハンドシェイク状態の接続数が表示されます。
[Connects in Data] カラム	関連するプロキシ サービスの、データ状態の接続数が表示されます。
[Connects in Reneg] カラム	関連するプロキシ サービスの、再ネゴシエート状態の接続数が表示されます。
[Bytes Encrypted] カラム	前回のポーリング サイクル以降の、関連するプロキシ サービスの暗号化された送信バイトの合計数が表示されます。
[Bytes Decrypted] カラム	前回のポーリング サイクル以降の、関連するプロキシ サービスの復号化された受信バイトの合計数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

SSL プロキシ エラー テーブルの表示

1 つの検証済みの SSL モジュールのプロキシ エラーのテーブルを、表示および操作できます。

手順

ステップ 1　[Monitor] > [SSL] > [Proxy Errors] を選択します。テーブルのカラムの説明については、表 9-6 を参照してください。

[SSL Proxy Errors] ページのすべての測定値は、デルタとして計算されます。

ステップ 2　[Select Device] リストから、表示するデバイスを選択します。

参考

表 9-6　[SSL Proxy Errors]

要素	説明
[Proxy] カラム	プロキシ サービス名が表示されます。
[Handshake Failures] カラム	ハンドシェイク状態で発生した、関連するプロキシ サービスの SSL 失敗数が表示されます。
[Data Failures] カラム	データ状態で発生した、関連するプロキシ サービスの SSL 失敗数が表示されます。
[MAC Errors] カラム	前回のポーリング サイクル以降に発生した、関連するプロキシ サービスの Machine Authentication Code（MAC）検証エラーの数が表示されます。
[Version Mismatch] カラム	前回のポーリング サイクル以降に発生した、関連するプロキシ サービスの SSL バージョン不一致エラーの数が表示されます。
[No Compress] カラム	圧縮アルゴリズムがサポートされていない前回のポーリング サイクル以降に発生した、関連するプロキシ サービスのエラーの数が表示されます。
[No Cipher] カラム	SSL 暗号化に互換性がない前回のポーリング サイクル以降に発生した、関連するプロキシ サービスのエラーの数が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

CHAPTER 10

トレンド レポートの使用

（注） サポートされるサービスおよびプラットフォームの詳細については、「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」（P.1-5）を参照してください。

ここでは、Performance Monitor で使用できるレポートの機能について、および生成した履歴トレンド レポートを使用および保存する方法について説明します。

レポートのオプションについて

サポートされているすべてのサービス タイプについて、レポートを設定および生成できます。レポートは、4 つの広義のカテゴリ、および 30 を超える狭義のサブカテゴリに分類されます。

（注） RAS VPN サービスとサイト間 VPN サービスのみ、4 つの広義のレポート カテゴリをすべてサポートしています。ほとんどの場合、サブカテゴリはサービスに特有です。

サブカテゴリは、検証済みのデバイスについて、またはサポートされているデバイスにおける狭い範囲の条件について、長期間のトレンドを測定します。Failure（障害）カテゴリの中のサブカテゴリは、障害の中の特別な種類を表す、というように、サブカテゴリはカテゴリに特有です。1 つのレポートに対して選択できるサブカテゴリの数は、1 ～ 4 で、選択するサブカテゴリによって異なります。

レポートのカテゴリには次のものがあります。

カテゴリ名	参考
Failure	「障害レポートのサブカテゴリについて」（P.10-2）を参照してください。
Performance	「パフォーマンス レポートのサブカテゴリについて」（P.10-3）を参照してください。
Throughput	「スループット レポートのサブカテゴリについて」（P.10-4）を参照してください。
Usage	「使用状況レポートのサブカテゴリについて」（P.10-5）を参照してください。

障害レポートのサブカテゴリについて

障害レポートで生成されるそれぞれの折れ線グラフには、表 10-1 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- 障害レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- 障害レポートに表示されるグラフについて説明します。

（注） 履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-16）を参照してください。

表 10-1　障害レポートの設定サブカテゴリ

障害レポートのサブカテゴリ	該当するサービス	説明
（注） 障害レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイルまたはカウントのいずれかを表します。		
[% of Inbound Conn Failures]	リモート アクセス VPN	グラフは、失敗した受信接続の長期間のトレンドを、リモート アクセス VPN の全デバイスに対するすべての受信接続の割合（パーセンテージ）として示します。
[% of Phase 1 Conn Failures]	リモート アクセス VPN	グラフは、失敗したフェーズ 1（IKE）接続の長期間のトレンドを、フェーズ 1 の全接続の割合（パーセンテージ）として示します。
[% of Phase 2 Conn Failures]	リモート アクセス VPN	グラフは、失敗したフェーズ 2（IPSec）接続の長期間のトレンドを、フェーズ 2 の全接続の割合（パーセンテージ）として示します。
[% Of Conns Dropped By All Virtual Servers]	ロード バランシング	グラフは、ドロップした仮想サーバ接続の長期間のトレンドを、全接続の割合（パーセンテージ）として示します。
[% Of Failed Conns Per Module]	ロード バランシング	グラフは、失敗したロードバランシング接続の長期間のトレンドを、CSM サービス モジュールの全接続の割合（パーセンテージ）として示します。
[% Of Inbound Conn Failures]	サイト間 VPN	グラフは、失敗した受信フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルの長期間のトレンドを、すべての受信交換の割合（パーセンテージ）として示します。
[% Of Outbound Conn Failures]	サイト間 VPN	グラフは、失敗した送信フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルの長期間のトレンドを、すべての送信交換の割合（パーセンテージ）として示します。
[% of Total Conn Failures]	サイト間 VPN	グラフは、失敗したフェーズ 1（IKE）およびフェーズ 2（IPSec）接続の長期間のトレンドを、すべての受信および送信交換の割合（パーセンテージ）として示します。
（注） 少数のデータ ポイントをベースにする場合には、通常、トレンド レポートはあまり有用ではありません。日付の範囲およびトレンドのタイプによって、データ ポイントの数が決まります。たとえば、期間が 2 日に満たないデータに対して Daily のトレンド タイプを適用した場合、データ ポイントは 1 つだけになります。1 つのデータ ポイントのみからトレンドをグラフ化することはできません。		

パフォーマンス レポートのサブカテゴリについて

パフォーマンス レポートで生成されるそれぞれの折れ線グラフには、表 10-2 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- パフォーマンス レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- パフォーマンス レポートに表示されるグラフについて説明します。

（注） 履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-16）を参照してください。

表 10-2　パフォーマンス レポートの設定サブカテゴリ

パフォーマンス レポート のサブカテゴリ	該当するサービス	説明
（注） パフォーマンス レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイル値またはカウントのいずれかを表します。		
[Bandwidth Usage]	リモート アクセス VPN	グラフは、使用された全帯域幅容量の平均パーセンテージに関する長期間のトレンドを示します。これは、インターフェイス速度を係数とし、受信および送信パケットの合計として計算されます。
[CPU Usage]	• ファイアウォール • リモート アクセス VPN • サイト間 VPN • SSL	グラフは、使用された全 CPU 能力の平均パーセンテージに関する長期間のトレンドを示します。
[CPU Usage Rev]	サイト間 VPN	グラフは、使用された全 CPU 能力の平均パーセンテージに関する長期間のトレンドを示します。 **（注）** [CPU Usage Rev] サブカテゴリを選択したときにレポートに何も示されない場合は、代わりに [CPU Usage] サブカテゴリを使用してください。
[FTP Fixup]	ファイアウォール	グラフは、[FTP Fixup]（FTP トラフィックに適用される、PIX OS のインスペクション機能）に対する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[HTTP Fixup]	ファイアウォール	グラフは、[HTTP Fixup]（HTTP トラフィックに適用される、PIX OS のインスペクション機能）に対する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[Memory Usage]	• ファイアウォール • サイト間 VPN • SSL	グラフは、使用されたプロセッサ メモリ容量の平均パーセンテージに関する長期間のトレンドを示します。
[SSL Connections]	SSL	グラフは、アクティブな SSL 接続の合計数に関する長期間のトレンドを示します。

表 10-2　パフォーマンス レポートの設定サブカテゴリ（続き）

パフォーマンス レポート のサブカテゴリ	該当するサービス	説明
[TCP Fixup]	ファイアウォール	グラフは、[TCP Fixup]（TCP トラフィックに適用される、PIX OS のインスペクション機能）に対する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[TCP Intercept]	ファイアウォール	グラフは、[TCP Intercept]（TCP サービスに対する Denial-Of-Service（DOS; サービス妨害）攻撃を回避する PIX OS の機能）に関する 1 秒あたりの平均アクティビティおよび変化率の長期間のトレンドを示します。
[Throughput]	SSL	グラフは、インターフェイス速度を係数として、全パブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを示します。
[Total IfErrors]	ファイアウォール	グラフは、ファイアウォールのインターフェイス エラーの数について長期間のトレンドを示します。
[Total Throughput]	ファイアウォール	グラフは、インターフェイス速度を係数として、全パブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを示します。
[URL Access]	ファイアウォール	グラフは、PIX OS の **show perfmon** コマンドの出力に基づいて、1 秒あたりに URL（Web サイト）がアクセスされた平均回数の長期間のトレンドを示します。
[URL Request]	ファイアウォール	グラフは、PIX OS の **show perfmon** コマンドの出力に基づいて、1 秒あたりに URL（Web サイト）が要求された平均回数の長期間のトレンドを示します。
[Xlates]	ファイアウォール	グラフは、ファイアウォールを介して 1 秒あたりに行われた TCP および UDP NAT 変換の平均回数の長期間のトレンドを示します。 **（注）** 変換は、内部アドレスから外部アドレスへのマッピングで、NAT では 1 対 1、PAT では多対 1 にすることができます。1 つのホストで、さまざまな宛先に対して複数の接続を持つことができますが、変換は 1 つだけです。xlate のカウント数が、内部ネットワーク上のホスト数よりもかなり多くなっていることに気付いた場合は、内部ホストのいずれか 1 つが侵害されている可能性があります。

（注） 少数のデータ ポイントをベースにする場合には、通常、トレンド レポートはあまり有用ではありません。日付の範囲およびトレンドのタイプによって、データ ポイントの数が決まります。たとえば、期間が 2 日に満たないデータに対して Daily のトレンド タイプを適用した場合、データ ポイントは 1 つだけになります。1 つのデータ ポイントのみからトレンドをグラフ化することはできません。

スループット レポートのサブカテゴリについて

スループット レポートで生成されるそれぞれの折れ線グラフには、表 10-3 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- スループット レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- スループット レポートに表示されるグラフについて説明します。

（注）　履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-16）を参照してください。

表 10-3　スループット レポートの設定サブカテゴリ

スループット レポートのサブカテゴリ	該当するサービス	説明
（注）　スループット レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイル値またはカウントのいずれかを表します。		
[Throughput]	• リモート アクセス VPN • サイト間 VPN	グラフは、インターフェイス速度を係数として、全パブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを示します。
[Throughput Per Accelerator]	リモート アクセス VPN	グラフは、Scalable Encryption Processor（SEP）アクセラレータ カードでの受信および送信オクテットの合計（kbps）の長期間のトレンドを、SEP カードの速度を係数として示します。 （注）　グラフの各線は、個別の SEP カードを表します。VPN 3005 コンセントレータまたは VPN 3015 コンセントレータには SEP カードがないため、このレポートではこれらのデバイスは対象外になります。[Throughput Per Accelerator] を選択した場合は、他のレポート サブカテゴリを選択できません。
[Throughput Per Interface]	• リモート アクセス VPN • サイト間 VPN	グラフは、1 つのデバイスのパブリック インターフェイスを介した受信および送信オクテットの合計（kbps）の長期間のトレンドを、インターフェイス速度を係数として示します。 （注）　グラフの各線は、個別のインターフェイスを表します。[Throughput Per Interface] を選択した場合は、他のレポート サブカテゴリを選択できません。
[% Of Crypto Packet Drop]	サイト間 VPN	グラフは、ドロップした暗号化パケットの長期間のトレンドを、暗号化および復号化された全パケットの割合（パーセンテージ）として示します。
[% Of Crypto Packet Errors]	リモート アクセス VPN	グラフは、フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルでエラーとなった暗号化パケットの長期間のトレンドを、暗号化された全パケットの割合（パーセンテージ）として示します。
[% Of Packets Dropped]	• リモート アクセス VPN • サイト間 VPN	グラフは、フェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルでドロップしたパケットの長期間のトレンドを、すべての受信および送信パケットの割合（パーセンテージ）として示します。

使用状況レポートのサブカテゴリについて

使用状況レポートで生成されるそれぞれの折れ線グラフには、表 10-4 で説明するように、選択したサービス タイプおよびサブカテゴリによって、デバイス、サービス モジュール、または仮想サーバに関する結果が表示されます。

- 使用状況レポートを設定するためのすべてのサブカテゴリをリストします。
- どのサービスがサブカテゴリをサポートしているかを指定します。
- 使用状況レポートに表示されるグラフについて説明します。

（注）　履歴レポートを実行すると、CiscoWorks Server 上で MCP プロセスが実行されていなかった期間に、グラフで降下している箇所が示されることがあります。「MCP プロセスのメンテナンス」（P.3-16）を参照してください。

表 10-4　使用状況レポートの設定サブカテゴリ

使用状況レポートのサブカテゴリ	該当するサービス	説明
（注）　使用状況レポートのすべてのグラフでは、横軸が時間を表します。縦軸は、レポートによって、パーセンタイルまたはカウントのいずれかを表します。		
[Number of Tunnels]	サイト間 VPN	グラフは、サイト間 VPN に対してフェーズ 1（IKE）およびフェーズ 2（IPSec）トンネルを組み合わせた数の長期間のトレンドを示します。
[Number of Users]	リモート アクセス VPN	グラフは、すべての RAS デバイスにおけるアクティブなセッションの集約数について、長期間のトレンドを示します。
[# Of Conns Per Module]	ロード バランシング	グラフは、特定のシャーシ内の各 CSM モジュールに対して、接続の平均数に関する長期間のトレンドを示します。 （注）　グラフの各線は、個別のサービス モジュールを表します。[# Of Conns Per Module] を選択した場合は、他のレポート サブカテゴリを選択できません。
[# Of Conns Per Virtual Server]	ロード バランシング	グラフは、特定のシャーシに関連付けられている各仮想サーバに対して、接続数の長期間のトレンドを示します。 （注）　グラフの各線は、個別の仮想サーバを表します。[# Of Conns Per Virtual Server] を選択した場合は、他のレポート サブカテゴリを選択できません。
（注）　少数のデータ ポイントをベースにする場合には、通常、トレンド レポートはあまり有用ではありません。日付の範囲およびトレンドのタイプによって、データ ポイントの数が決まります。たとえば、期間が 2 日に満たないデータに対して Daily のトレンド タイプを適用した場合、データ ポイントは 1 つだけになります。1 つのデータ ポイントのみからトレンドをグラフ化することはできません。		

レポートの設定と生成

ネットワーク内でサポートされているサービスに対して、履歴レポートを設定および生成することができます。

手順

ステップ 1　[Report] > [Service Type] > [Configure Report] を選択します。[Service Type] は、オプション バーで選択するサービスです。

[Configure Report] ページには、オブジェクト セレクタ、選択したサービスに適用されるアクション ボタン、リスト、およびレポートのカテゴリが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　[All] タブがアクティブになっていない場合は、このタブをクリックして、選択ツリー内のデバイス グループおよび個々のデバイスのリストを表示します。レポートの対象にする情報が定義されているデバイスを選択します。1 つのデバイス グループをすると、そのグループ内のすべてのデバイス、および階層内でのそのグループの下位グループが選択されます。

レポートを設定する前に、少なくとも 1 つのデバイスをツリーから選択する必要があります。次のレポート サブカテゴリで選択が必要なデバイスは *1 つだけ*です。

- [Remote Access] : [Throughput] : [Throughput Per Accelerator]
- [Remote Access] : [Throughput] : [Throughput Per Interface]
- [Site-To-Site] : [Throughput] : [Throughput Per Interface]
- [Load Balancing] : [Usage] : [# Of Conns Per Virtual Server]
- [Load Balancing] : [Usage] : [# Of Conns Per Module]
- [Load Balancing] : [Failure] : [% Of Conns Dropped By All Virtual Servers]
- [Load Balancing] : [Failure] : [% Of Failed Conns Per Module]

ステップ 3　レポート カテゴリを選択し、サブカテゴリを選択してから [>>]（追加）をクリックして、[Selected List] に移動します。誤ったサブカテゴリを選択してしまった場合は、[<<]（削除）をクリックします。

次のルールに従って、複数のレポート タイプを選択できます。

- いずれのレポートについても、4 つを超えるサブカテゴリは選択できません。
- 1 つのレポートに対して 2 つを超えるサブカテゴリは選択できません（ただし、選択したすべてのサブカテゴリがパーセント単位で測定している場合は除きます）。このような場合は、最大 4 つのサブカテゴリを選択できます。
- 選択したサブカテゴリのうち、いずれか 1 つがパーセント単位で測定している場合は、2 つを超えるサブカテゴリは選択できません。
- 「レポートのオプションについて」（P.10-1）およびその各項に説明があるとおり、サブカテゴリを 1 つしか選択できない場合があります。

レポートには 30 を超えるサブカテゴリがあります。レポート タイプの説明については、次の各項を参照してください。

- 「障害レポートのサブカテゴリについて」（P.10-2）
- 「パフォーマンス レポートのサブカテゴリについて」（P.10-3）
- 「スループット レポートのサブカテゴリについて」（P.10-4）
- 「使用状況レポートのサブカテゴリについて」（P.10-5）

ステップ 4　[Trending Type] リストから間隔を選択します。トレンドのオプションには、次のものがあります。

- [Hourly]：レポートは、指定したカレンダー日付の範囲に対して、1 時間間隔でモニタした値を示します。
- [Daily]：レポートは、指定したカレンダー日付の範囲に対して、1 日間隔でモニタした値を示します。
- [Weekly]：レポートは、指定したカレンダー日付の範囲に対して、1 週間間隔でモニタした値を示します。
- [Monthly]：レポートは、指定したカレンダー日付の範囲に対して、1 か月間隔でモニタした値を示します。

ステップ 5　レポートの対象とするデータについて、開始（[From]）と終了（[To]）の日付を選択します。

ステップ 6　次のいずれかを実行します。

- レポートを生成して新しいブラウザ ウィンドウで表示するには、[View] をクリックします。
- レポートを生成し、1 回または繰り返しの E メール配信オプションを設定するには、[Email] をクリックします。繰り返しの E メール ジョブを設定する場合は、レポートに何時間分のデータを含めるかを指定できます。

- レポートを生成してそれをファイルに保存するには、ファイル形式を選択して [Export] をクリックします。使用できる形式には、次のものがあります。
  - CSV：データをカンマ区切りの ASCII リストでエクスポートします。ほとんどのスプレッドシート アプリケーションは、CSV を表形式で表示できます。
  - XML：データを Extensible Markup Language（XML）でエクスポートします。XML は、Web ブラウザ、ワード プロセッサ、または XML ファイルを表示する他のアプリケーションで確認できます。
  - PDF：データを Portable Document Format（PDF）形式でエクスポートします。PDF は、Adobe Acrobat Reader アプリケーション、または PDF ファイルを表示する他のアプリケーションで確認できます。

履歴レポートについて

生成したレポートには、選択したサブカテゴリの履歴トレンドを示すグラフが表示されます。Performance Monitor はレポートに対して、指定したトレンド タイプおよび日付範囲を適用します。特定のグラフの詳細については、「レポートのオプションについて」（P.10-1）およびその各項を参照してください。

[Performance Monitor Report] ページの [Details] エリアには、対象レポートのユーザ名、トレンド タイプ、および日付範囲が表示されます。

関連トピック

- 「レポートの設定と生成」（P.10-6）

RAS VPN の上位 10 ユーザ レポートの表示

すべての RAS デバイス間で、ネットワーク内の RAS VPN の上位 10 ユーザの履歴レポートを表示できます。

（注）　Performance Monitor は、Easy VPN RAS セッションについてこの情報を表示できません。

手順

ステップ 1　[Reports] > [Remote Access] > [Top 10 Users] を選択します。

デフォルトでは、[Top 10 Users] ページに、スループット レベルが最も高い RAS ユーザが 10 人表示され、最近 24 時間の時間ごとのデータ ポイントが示されます。対象の 24 時間で RAS VPN に接続していたユーザが 10 人未満の場合は、10 人よりも少ない人数が表示されます。

レポートの情報は、デバイスごとのユーザ アクティビティ ランキングをベースにしています。

ステップ 2　必要な場合はレポート基準を修正し、[Go] をクリックして結果を確認してください。次のいずれかの方法で実行できます。

- トレンド タイプを変更します。次のいずれかを選択します。
  - [Hourly]：モニタされた値を 1 時間間隔で表示します。
  - [Daily]：モニタされた値を 1 日間隔で表示します。
  - [Weekly]：モニタされた値を 1 週間間隔で表示します。

  - [Monthly]：モニタされた値を 1 か月間隔で表示します。
- [From] フィールドと [To] フィールドに異なる日付を入力し、レポート日付の別の範囲を指定します。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

RAS VPN ユーザ セッション レポートの表示

指定した複数のユーザ、または 1 人のユーザについて、VPN セッションへの長期間のリモート アクセスを表すレポートを表示できます。

ヒント　いくつかのマルチユーザ セッションのクエリーでは、結果として大きい値が返されることがあります。クエリーの結果として 10,000 を超える値が返される場合は、[User Session Report] ページでブラウザをロードするために数分かかります。このような遅延が問題となる場合は、特定のデバイスを選択し、クエリーを発行する前に開始時間と終了時間を調整することを推奨します。

始める前に

この機能では、Syslog メッセージを Performance Monitor へ送信するよう、VPN 3000 コンセントレータ、ASA および PIX デバイスを設定する必要があります。

- アプライアンスおよびファイアウォールの設定については、「ASA アプライアンス、PIX デバイス、およびファイアウォール サービス モジュールのセットアップ」（P.2-5）を参照してください。
- VPN コンセントレータの設定については、「VPN 3000 コンセントレータのセットアップ」（P.2-7）を参照してください。
- Performance Monitor が処理可能な Syslog メッセージのリストについては、「通知の操作」（P.12-1）を参照してください。

手順

ステップ 1　[Reports] > [Remote Access] > [User Session Report] を選択します。

[User Session Report] ページにはオブジェクト セレクタがあります。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　複数のユーザ、または 1 人のユーザのどちらに対してセッション レポートを表示するかを決定し、次のいずれかを実行します。

- すべてのユーザのセッションが含まれている情報を表示するには、[Search All Users] を選択します。
- ユーザ セッションの検索対象を 1 人のユーザに制限するには、ツリーでクラスタ ペアレントを選択します。
- ユーザ セッションの検索対象を 1 つのデバイスに制限するには、ツリーでデバイスを選択します。
- 検索対象を 1 人のユーザのセッションに制限するには、[User Name] テキスト ボックスにユーザ名を入力します。

ステップ 3　Performance Monitor がセッションを検索する間隔を定義するには、次の両方を実行します。

- [Start Time] エリアで、カレンダー日付を選択し、HH:MM:SS 形式で時間を入力します。[Start Time] エリアの値は、Performance Monitor がセッション情報を検索する間隔の始まりを定義します。
- [End Time] エリアで、カレンダー日付を選択し、HH:MM:SS 形式で時間を入力します。[End Time] エリアの値は、Performance Monitor がセッション情報を検索する間隔の終わりを定義します。

ステップ 4　次のいずれか、または両方を実行します。

- 新しいブラウザ ウィンドウにレポートを表示するには、[View] をクリックします。
- レポートをエクスポートするには、ファイル形式（CSV または XML）を選択して [Export] をクリックします。

  CSV を選択すると、以前にサーバを「信頼できるソース」として指定していない場合には、Performance Monitor で、CiscoWorks Server の証明書を承認するよう要求されることがあります。この証明書を承認すると、Performance Monitor は、デフォルトのスプレッドシート アプリケーションにエクスポートされた CSV データを表示します。証明書を承認しなかった場合は、CSV ファイルをローカルに保存するためのファイル名とパスの指定を、Performance Monitor から求められます。

  XML を選択すると、XML のエクスポートによって新しいブラウザ ウィンドウが開きます。このウィンドウから、表示された結果を保存できます。エクスポートしたレポートのローカル コピーを保存するには、[File] > [Save As] を選択します。

レポートの内容について、表 10-5 に示します。

ユーザ セッション レポートの形式

表 10-5　ユーザ セッション レポートの形式

エレメント	説明
[Username] カラム	1 人のユーザを検索し、一致したユーザ名が見つかった場合には、検索クエリーとして入力した認証済みのユーザ名が表示されます。 特定の期間におけるすべてのユーザのセッションを検索した場合は、[Username] カラムに、その期間のすべてのセッションに関連付けられている認証済みのすべてのユーザ名が含まれていることがあります。
[IP Address] カラム	対象のセッションに関連付けられているユーザの IP アドレスが表示されます。特定のユーザの IP アドレスは、特にダイナミック アドレッシングを使用しているネットワークでは、セッションによって変わることがあります。
[State] カラム	対象のユーザ セッションの最も新しいステータス（Active または Completed）が表示されます。
[VPN Device Name] カラム	対象のセッションが実行された（またはアクティブなセッションの場合は、実行している）VPN コンセントレータの DNS 名が表示されます。
[Start Time] カラム	対象のセッションが開始された日付と時間が、MM/DD/YYYY HH:MM:SS の形式で表示されます。
[End Time] カラム	対象のセッションが終了した日付と時間が、MM/DD/YYYY HH:MM:SS の形式で表示されます。 [End Time] の値が赤の場合は、正確な終了時刻が不明です。このような場合に表示された値は、Performance Monitor のポーリングでセッションがアクティブでなくなったと判断された時刻です。

表 10-5　ユーザ セッション レポートの形式（続き）

エレメント	説明
[Duration] カラム	セッションの期間が、日、時間、分、および秒で表示されます。 正確な終了時刻がわからない場合は、[Duration] カラムの値が赤になります。このような場合に表示された値は、Performance Monitor のポーリングでセッションがアクティブでなくなったと判断された期間です。
[Last Verified] カラム	デバイスのポーリングで、対象のセッションに対して最後に情報を提供した時刻が、MM/DD/YYYY HH:MM:SS 形式で表示されます。
[Bytes In] カラム	ユーザが対象セッションでネットワークを介して受信した、トンネリングされたバイト数の合計数が表示されます。
[Bytes Out] カラム	ユーザが対象セッションでネットワークを介して送信した、トンネリングされたバイト数の合計数が表示されます。

サイト間 VPN の上位 10 トンネル レポートの表示

すべてのデバイス間で、ネットワーク内のサイト間 VPN の上位 10 トンネルの履歴レポートを表示できます。

手順

ステップ 1　[Reports] > [Site-to-Site] > [Top 10 Tunnels] を選択します。

デフォルトでは、[Top 10 Tunnels] ページに、スループット レベルが最も高いトンネルが 10 個表示され、最近 24 時間の時間ごとのデータ ポイントが示されます。対象の 24 時間で、スループットを測定できたトンネルが 10 個未満の場合は、10 個よりも少ない数が表示されます。

テーブルのカラムの説明については、表 10-6 を参照してください。

ステップ 2　必要な場合はレポート基準を修正し、[Go] をクリックして結果を確認してください。次のいずれかの方法で実行できます。

- トレンド タイプを変更します。次のいずれかを選択します。
  - [Hourly]：モニタされた値を 1 時間間隔で表示します。
  - [Daily]：モニタされた値を 1 日間隔で表示します。
  - [Weekly]：モニタされた値を 1 週間間隔で表示します。
  - [Monthly]：モニタされた値を 1 か月間隔で表示します。
- [From] フィールドと [To] フィールドに異なる日付を入力し、レポート日付の別の範囲を指定します。

参考

表 10-6　[Top 10 Tunnels] ページ

エレメント	説明
[Device Name] カラム	対象デバイスの DNS 名または IP アドレスが表示されます。
[Local Endpoint] カラム	トンネルが終了したローカル エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。 （注）　Performance Monitor の内部で、「ローカル」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。
[Remote Endpoint] カラム	トンネルが終了したリモート エンドポイント デバイスのインターフェイスの IP アドレスが表示されます。 （注）　Performance Monitor の内部で、「リモート」エンドポイント デバイスの ID が変化することがあります。これは、このようなデバイスの ID は常に、モニタしているデバイスに対して相対的に定義されるからです。
[Local Subnet] カラム [Remote Subnet] カラム [Protocol] カラム	次の 3 つのカラムの値は全体として、1 つのトンネルのアクセス リストを定義しています。 • [Local Subnet] : ローカル エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Remote Subnet] : リモート エンドポイント デバイス上のトンネル サブネットおよびマスクが表示されます。 • [Protocol] : トンネル プロトコルおよび使用したポート（TCP 80 など）が表示されます。
[Throughput (Kbps)] カラム	トンネルの開始以降の、トンネルを介した受信および送信オクテットの合計（kbps）が表示されます。

関連トピック

- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

スケジュールされた E メール ジョブの操作

スケジュールされた E メール ジョブを表示および削除できます。Performance Monitor は、これらのジョブによって履歴レポートを配信します。

手順

ステップ 1　[Reports] > [Service Type] > [Scheduled Email Jobs] を選択します。[Service Type] は、オプション バーで選択するサービスです。

ステップ 2　リストから 1 つのジョブを選択します。

ステップ 3　次のいずれかを実行します。

- [Email Job Details] ウィンドウでジョブを表示するには、[View] をクリックします。
- ジョブを削除するには、[Delete] をクリックします。ジョブを削除すると、元に戻すことはできません。

参考

表 10-7　　E メール ジョブ

エレメント	説明
[Job Name] カラム	ジョブの名前が表示されます。名前は次の要素で構成されます。 • CiscoWorks のユーザ名：Admin など。 • 特定のサービス タイプ：RAS など。 • [Schedule Email Report] ウィンドウの [Job Name] フィールドで入力した値。
[Recurring] カラム	次のいずれかが表示されます。 • [Yes]：ジョブが繰り返しスケジュールされます。 • [No]：ジョブは 1 回だけスケジュールされます。
[Next Schedule] カラム	繰り返しスケジュールされるジョブだけに、ジョブが次回実行される日付と時間が表示されます。
[Last Run Status] カラム	E メールが正常に送信されたか、配信に失敗したかを示すメッセージが表示されます。
[Last Run Time] カラム	スケジュールされていた対象の E メール ジョブが最後に実行された時刻が、MM/DD/YYYY HH:MM:SS 形式で表示されます。

関連トピック

- 「レポートの設定と生成」（P.10-6）
- 「Performance Monitor テーブルのオプション タスク」（P.3-9）
- 「テーブルの一般エレメント」（P.3-8）

CHAPTER 11

デバイスの管理とグループ化

Performance Monitor では、デバイスとはネットワーク内の物理ノード、または物理ノードで定義される仮想ノードです。いずれの場合も、デバイスは IP アドレス指定可能な必要があります。

たとえば、*マルチコンテキスト モード*を使用して、1 つのファイアウォールをセキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化することができます。マルチコンテキスト モードで動作しているファイアウォールには、セキュリティ ポリシー、インターフェイス、およびその他のオプションを定義するための各コンテキストが設定されています。これは物理デバイス上で同等のオプションを設定することと同じです。

システム管理者はシステム設定でコンテキストを追加および管理します。システム設定では、基本的なファイアウォール設定を識別しますが、ネットワーク インターフェイスやネットワーク設定自体は含まれず、代わりに*管理コンテキスト*として指定されたコンテキストを使用します。

管理コンテキストは、管理コンテキストにログインしたユーザがシステム全体およびその他のすべてのコンテキストに対する管理者権限を持つことを除いて、他のセキュリティ コンテキストと同じです。Performance Monitor では、物理デバイス上で設定されたすべてのコンテキストをモニタする場合、デバイスから管理コンテキストだけをインポートします。同様に、Performance Monitor で管理コンテキストを削除すると、関連する物理デバイス上のコンテキストごとに Performance Monitor が維持するレコードを、同時に削除することになります。

リスト、メニュー、グラフ、レポート、ログ、またはその他の場所に、Performance Monitor で特定のセキュリティ コンテキストを表示する場合は、次の 2 種類の動作の可能性があります。

- 管理コンテキストの IP アドレスは、*<IP_address_of_admin_context>:<context_name>* のように、コンテキスト名のプレフィクスとして表示されます。これは、Performance Monitor がデフォルトで管理コンテキスト IP アドレスおよびクレデンシャルを使用して、検証されたデバイス上でセキュリティ コンテキストのポーリングおよびモニタを行う場合に発生します。

  （注） Performance Monitor では、管理コンテキストをインポートすると、すべてのセキュリティ コンテキストが自動的に検出されます。また（必要に応じて）、管理コンテキストの IP アドレスおよびクレデンシャル情報を使用して、デバイス上のその他のコンテキストのポーリングおよびモニタを行います。ただし、Performance Monitor が管理コンテキスト IP アドレスを使用して、デバイス上でセキュリティ コンテキストのポーリングおよびモニタを行う場合、モニタできるコンテキストは 5 つまでです。お使いのデバイスに 6 つ以上のコンテキストが含まれている場合、検出後にいつでもあらゆるコンテキストの IP アドレスおよびクレデンシャルを手動で入力できます。

- セキュリティ コンテキストの IP アドレスはプレフィクスなしで表示されます。これは、デフォルトで *<IP_address_of_admin_context>:<context_name>* のように表示されていたコンテキストのクレデンシャルを手動で編集した後に発生します。

Performance Monitor のデバイス グループはフォルダと似ています。一部のデバイス グループはシステム定義グループで、その他のデバイス グループはユーザ定義グループです。

- システム定義デバイス グループでは、物理デバイスおよびセキュリティ コンテキストがデバイス タイプまたはサービス タイプごとに自動的にソートされます。システム定義デバイス グループは、一貫性があって論理的です。
- Performance Monitor のユーザ定義デバイス グループにより、組織内でデバイス、セキュリティ コンテキスト、その他のデバイス グループの組み合わせを収集できます。デバイスを一貫した方法で整理していない場合は、ユーザ定義グループ内のデバイスに物理的、論理的、またはトポロジの関係が想定されません。

（注）　第 2 章「始める前に」で、[Devices] タブのデバイス インポート機能およびデバイス検証機能について説明します。

ここでは、[Devices] タブにある次のオプションについて説明します。

- 「デバイスの管理」（P.11-2）
- 「デバイス グループの管理」（P.11-8）

デバイスの管理

[Devices] > [Managing Devices] を選択すると、Performance Monitor でデバイスを管理できるようにするためのオブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ヒント　最近インポートしたか、追加したデバイスがまだ表示されていない場合、[Refresh] をクリックして、[Managing Devices] のオブジェクト セレクタでデバイス リストを更新します。デバイス アイコンについては、「デバイス アイコンについて」（P.3-6）を参照してください。

ここでは、デバイス管理オプションについて説明します。

- デバイス アトリビュートおよび [View] ボタンについては、「デバイス アトリビュートの表示」（P.11-2）を参照してください。
- 設定可能なデバイス プロパティおよび [Edit] ボタンについては、「デバイスの編集」（P.11-3）を参照してください。
- [Enable Monitoring] ボタンおよび [Disable Monitoring] ボタンについては、「デバイス モニタリングのイネーブル化またはディセーブル化」（P.11-6）を参照してください。
- デバイス モニタリング操作の概要および [Report] ボタンについては、「デバイス モニタリングの概要の表示」（P.11-7）を参照してください。
- [Delete] ボタンの使用および効果については、「デバイス、グループ、またはコンテキストの削除」（P.11-7）を参照してください。

デバイス アトリビュートの表示

検証されたデバイスのアトリビュートを表示できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Devices] を選択します。

[Managing Devices] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　選択ツリーからデバイスまたはデバイス グループを選択し、[View] をクリックします。

[View Device Detail] ウィンドウに、デバイス アトリビュートが表示されます（表 11-1）。

（注）　デバイスで対応するパラメータが設定されていない場合、[View Device Detail] ウィンドウに、パラメータの詳細が表示されません。

参考

表 11-1　[View Device Detail] ウィンドウ

パラメータ	表示される値
[Polling Enabled]	[Yes] または [No]。
[Name]	ホスト名、IP アドレス、または SNMP システム名。
[IP Address]	デバイスの IP アドレス。
[SysName]	システム名。
[SysOid]	デバイス タイプの一意の識別子。
[Product]	特定の製品のリビジョン。
[Family]	デバイス タイプ。
[Version]	デバイスにインストールされたソフトウェアのバージョン。
[Description]	デバイスの詳細な説明。
[Contact]	このデバイスが故障しているか、設定に誤りがある場合に連絡先となる担当者。
[Location]	デバイスの物理的な場所。

デバイスの編集

Performance Monitor で検証またはポーリングのためにデバイスと通信する場合に使用する、SNMP 設定およびデバイス クレデンシャルを編集できます。

編集するセキュリティ コンテキストを選択した場合は、Performance Monitor がそのコンテキストに関連付けた IP アドレスを変更すると、Performance Monitor でそのコンテキストをリスト、メニュー、グラフ、レポート、ログ、またはその他の場所に表示する方法を変更できるため、特別な注意が必要です。

（注）
- SNMP の再試行回数または SNMP タイムアウト時間がデフォルトよりも多い場合、デバイスの検証およびポーリングに時間がかかります。
- Performance Monitor のデフォルトで *<IP_address_of_admin_context>:<context_name>* のように表示されていたセキュリティ コンテキストのクレデンシャルを手動で編集した場合は、セキュリティ コンテキストが独自の IP アドレスによって表示されます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Devices] を選択します。

[Managing Devices] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　選択ツリーからデバイスまたはデバイス グループを選択し、[Edit] をクリックします。

ヒント　複数のデバイスを同時に選択できます。ただし、選択できるデバイスは同じタイプのデバイスに制限されます。

ステップ 3　[Edit Devices] ウィンドウで、要件を満たすオプション タスクを実行します（表 11-2）。

更新されたディスプレイに、実行したオプション タスクの結果が表示されます。

ステップ 4　（**任意**）変更を保存して実装する場合、[Validate edited devices] チェックボックスをオンにして [Apply] をクリックすると、編集済みのデバイスまたはデバイス グループが自動的に再検証できます。

ステップ 5　次のいずれかを実行します。
- 選択内容を破棄して [Edit Devices] ウィンドウを閉じるには、[Cancel] をクリックします。
- 変更を保存して実装するには、[Apply] をクリックします。

参考

表 11-2　[Edit Devices] ウィンドウのタスク

オプション タスク	手順	追加情報
SNMP の read コミュニティ ストリングを指定する。	[Read Community]（または [Chassis Read Community]）テキスト ボックスで、ストリングを上書きします。	read コミュニティ ストリングは、指定されたデバイスまたはセキュリティ コンテキストへの読み取り専用アクセスを可能にするためのパスワードです。デフォルトは *public* です。お使いのデバイス（複数のデバイスを選択することもできる）のコミュニティ ストリングがデフォルトとは異なる場合、検証を開始たり、デバイスをモニタしたりできるようにするには、正しいコミュニティ ストリングを指定する必要があります。 すべてのデバイスで同一のストリングを使用する場合、1 つの Read Community エントリを選択したすべてのデバイスに適用できます。 セキュリティ コンテキストの場合、使用する正しい read コミュニティ ストリングが Performance Monitor でコンテキストのポーリングやモニタに使用する IP アドレスに関連付けられます。
異なる SNMP タイムアウト設定を指定する。	[SNMP Timeout] リストから値を選択します。	この値は Performance Monitor で応答を再び促す前にデバイスからの応答を待機する秒数です。最小期間は 1 秒、最大期間は 60 秒です。デフォルトは 10 秒です。
SNMP の別の再試行回数を指定する。	[SNMP Retries] リストから値を選択します。	この値は、Performance Monitor でデバイスがタイムアウトしたと宣言する前に、デバイスとの通信を行う試行回数です。デフォルトは 1 回です。
別の管理者ユーザ名を使用する。	Performance Monitor で [Username] テキスト ボックスが表示された場合は、既存のユーザ名を上書きします。	Performance Monitor で Telnet 接続をサポートするデバイスおよびセキュリティ コンテキストの [Username] テキスト ボックスが表示されます。 セキュリティ コンテキストの場合、使用する正しいユーザ名が Performance Monitor でコンテキストのポーリングやモニタリングに使用する IP アドレスに関連付けられます。
別の管理者パスワードを使用する。	Performance Monitor で [Password] テキスト ボックスと [Confirm Password] テキスト ボックスが表示された場合は、既存のパスワードを上書きします。	Performance Monitor で Telnet 接続をサポートするデバイスの [Password] テキスト ボックスと [Confirm Password] テキスト ボックスが表示されます。
別のイネーブル パスワードを使用する。	Performance Monitor で [Enable Password] テキスト ボックスと [Confirm Enable Password] テキスト ボックスが表示された場合は、既存のイネーブル パスワードを上書きします。	Performance Monitor で Telnet 接続をサポートするデバイスおよびセキュリティ コンテキストの [Enable Password] テキスト ボックスと [Confirm Enable Password] テキスト ボックスが表示されます。 リモート Telnet 接続を介してデバイスにアクセスする場合、イネーブル パスワードにより、Cisco IOS デバイスで特権*イネーブル モード*がアクティブになります。特定の特権の操作は、デバイスがイネーブル モードの場合だけ実行できます。 セキュリティ コンテキストの場合、使用する正しいイネーブル パスワードが Performance Monitor でコンテキストのポーリングやモニタリングに使用する IP アドレスに関連付けられます。

表 11-2　[Edit Devices] ウィンドウのタスク（続き）

オプション タスク	手順	追加情報
セキュリティ コンテキストをポーリングするときに使用する、別の IP アドレスを指定する。	リストから、コンテキストに特別に割り当てられる IP アドレスを選択するか、または [Admin Context IP] を選択します。	このオプション タスクは、セキュリティ コンテキストのアトリビュートを編集するときだけ使用できます。 あらゆるコンテキストが独自のクレデンシャルを持っている可能性があるため、リストからの選択内容によっては、Performance Monitor でコンテキストのポーリングに使用するよう設定したクレデンシャルが、無効化されることがあります。 リストから IP アドレスを選択する場合は、その他のすべての値が正しいことを確認し、そうでない場合はここで編集します。
デバイスを検証し、編集済みのアトリビュートが正しいことを確認する。	チェックボックスをオンにします。	ワンタイム検証を開始します。

関連トピック

- 「デバイスの管理」（P.11-2）

デバイス モニタリングのイネーブル化またはディセーブル化

テーブル、グラフ、およびレポートには、モニタリングがイネーブルになっている検証済みのデバイスに関する情報だけが含まれています。Performance Monitor では、デバイス検証に成功した後にモニタリングが自動的にイネーブルになり、次のポーリング サイクルで自動的にポーリングが実行されます。

ポーリングからデバイスを除外する場合は、そのデバイスのモニタリングをディセーブルにできます。その後、ユーザの判断で、手動でモニタリングを再イネーブル化することもできます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Devices] を選択します。

[Managing Devices] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　選択ツリーからデバイスまたはデバイス グループを選択し、次のいずれかを実行します。

- [Enable Monitoring] をクリックして、すべてのポーリング サイクルで、選択したデバイスをポーリングします。
- [Disable Monitoring] をクリックして、デバイスのポーリングを停止します。

ステップ 3　（任意）選択ツリーからデバイスを選択し、[View] をクリックして、そのデバイスのモニタリングがイネーブルかディセーブルかを確認します。

[Info] ウィンドウに、デバイスを説明するテキストが表示されます（表 11-1）。テキストの 1 行目に、[Polling Enabled] が [Yes] または [No] と表示されます。

関連トピック

- 「デバイスの管理」（P.11-2）
- 「デバイス アトリビュートの表示」（P.11-2）

デバイス モニタリングの概要の表示

[Monitor] タブのテーブルとグラフに使用する情報が Performance Monitor で最後に更新されたのはいつか、およびその情報が更新された範囲に関する、操作の概要を表示できます。

手順

ステップ 1　[Devices] > [Managing Devices] を選択します。

（注）　モニタリングの概要を表示する場合は、[Managing Devices] 選択ツリーから何も選択する必要がありません。選択を行っても、表示される結果には影響がありません。

ステップ 2　[Report] をクリックします。概要レポートの説明については、表 11-3 を参照してください。

参考

表 11-3　モニタリングの概要レポート

カラム	説明
[Polling Unit]	モニタ対象の値が更新された情報のカテゴリを識別します。
[Last Polling Update]	ポーリングが最後に実行された時刻と日付を HH:MM:SS *CiscoWorks_Server_timezone* YYYY/MM/DD の形式で表示します。
[No.Records Updated]	関連するポーリング単位の更新されたレコード数を表示します。
[No.Records]	関連するポーリング単位に Performance Monitor で保存されたレコードの合計数を表示します。
[Time Taken]	Performance Monitor での関連するポーリング単位の更新に必要な時間数を表示します。

関連トピック

- 「デバイスの管理」（P.11-2）

デバイス、グループ、またはコンテキストの削除

Performance Monitor では、検証されたデバイスまたはデバイス グループ内のすべてのデバイスのレコードを削除できます。また、検証された管理コンテキストのレコードを削除することもできます。管理コンテキストを削除する場合は、その管理コンテキストに関連付けられたすべての仮想コンテキストも削除することになります。仮想コンテキストを直接削除することはできません。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Devices] を選択します。

[Managing Devices] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　選択ツリーから少なくとも 1 つのオブジェクトを選択し、[Delete] をクリックします。

- 選択内容にデバイスが含まれている場合、そのデバイスはシステム定義グループおよびユーザ定義グループから削除されます。Performance Monitor でデバイスのポーリングが実行されなくなります。
- 選択内容に仮想コンテキストが含まれる場合、Performance Monitor でそのレコードが削除され、その仮想コンテキストのポーリングが停止されます。
- 選択内容にデバイス グループが含まれている場合、そのすべてのメンバー デバイスがシステム定義グループおよびユーザ定義グループから削除されます。Performance Monitor で、それらのすべてのデバイスのポーリングが実行されなくなります。
- 選択内容に管理コンテキストが含まれる場合、Performance Monitor でその管理コンテキストのレコードと、同じ物理デバイス上のすべての仮想コンテキストのレコードが削除されます。Performance Monitor で、関連デバイスのすべてのコンテキストのポーリングが実行されなくなります。

選択したデバイス、仮想コンテキスト、デバイス グループ、または管理コンテキストについての情報が Performance Monitor のテーブル、グラフ、またはレポートに表示されなくなります。

関連トピック

- 「デバイスの管理」（P.11-2）

デバイス グループの管理

デバイス グループを使用すると、1 回の操作で複数のデバイスを操作できます。デバイス グループは、デバイス、他のグループ、またはデバイスとグループの組み合わせを含めることができる名前付きのエンティティです。グループは概念的にフォルダと同じです。

[Devices] > [Managing Groups] を選択すると、既存のデバイス グループを表示したり、新しいグループまたは既存のグループにデバイスを割り当てたりできます。

ヒント　[Refresh] をクリックすると、選択ツリーでデバイス グループ リストが更新されます。

[Managing Groups] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

Performance Monitor で認識されているすべてのデバイスが 1 つまたは複数の *システム定義グループ*に表示され、*ユーザ定義グループ*にも表示できます。

システム定義グループ	システム定義グループは、Performance Monitor をインストールした直後からデフォルトで存在しています。 • Device Types フォルダでは、すべてのデバイスがデバイス タイプごとに整理され、一時的にモニタリングをディセーブルにした検証済みのデバイスも表示されます。 • Monitored Devices フォルダでは、開始されるデバイスがデバイス タイプごとに整理されます。モニタリングがイネーブルになっている検証済みのデバイスだけの情報が表示されます。 システム定義グループは編集したり、削除したりできません。Performance Monitor では、ポーリング中に読み取られた情報に基づいて、システム定義グループが自動的に読み込まれます。デバイスのモニタリングのイネーブル化またはディセーブル化の詳細については、「デバイス モニタリングのイネーブル化またはディセーブル化」（P.11-6）を参照してください。 **（注）** Performance Monitor で次のポーリング サイクルが完了した後にだけ、デバイスやネットワークの変更がシステム定義グループに反映されます。ポーリング間隔の設定については、「システム パラメータの操作」（P.12-9）を参照してください。
ユーザ定義グループ	ユーザ定義グループは、システム定義グループでは満たすことができない要件を満たすためにユーザが作成するグループです。たとえば、地理的地域や企業の部門ごとにネットワーク資産を分割するグループを作成できます。 任意の数のグループを定義できます。すべてのグループに、指定したサブグループや組織の階層内のデバイスの組み合わせを含めることができます。

関連トピック

- 「グループの作成」（P.11-9）
- 「グループの編集」（P.11-10）
- 「グループの削除」（P.11-12）

グループの作成

ユーザ定義デバイス グループを作成できます。

（注） 有効なグループ名および有効なグループの説明の要件の詳細については、「命名のガイドライン」（P.11-10）を参照してください。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Groups] を選択します。

[Managing Groups] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　Device Groups フォルダまたはユーザ定義グループをクリックします。

選択内容によって、作成するグループの親が定義されます。

ステップ 3　新しいデバイス グループを設定するには、[Add] をクリックします。

（注）　新しいグループを作成できるのは、最初に親を選択した場合だけです。システム定義グループにサブグループを追加することはできません。

[Add Group] ページに、オブジェクト セレクタ、テキスト ボックス、およびアクション ボタンが表示されます。

ステップ 4　[Name] テキスト ボックスに、新しいグループの有効な名前を入力します。

ステップ 5　（任意）[Description] テキスト ボックスに、新しいグループの有効な説明を入力します。

ステップ 6　選択ツリーで、1 つまたは複数のデバイスまたはデバイス グループを選択します（すべてのサブグループおよびそれに含まれるデバイスを選択します）。

ステップ 7　選択したデバイスを新しいグループに追加するには、[Add] をクリックします。

追加されたデバイスは、[Group] リストの [Devices] に表示されます。

ステップ 8　（任意）グループからデバイスを削除するには、[Group] リストの [Devices] から選択し、[Remove] をクリックします。

ステップ 9　変更を保存するか破棄して、[Managing Groups] ページに戻ります。

- 新しいグループを保存するには、[Save] をクリックします。

  新しいグループが表示され、オブジェクト セレクタに追加されます。
- 変更を破棄するには、[Cancel] をクリックします。

関連トピック

- 「デバイス グループの管理」（P.11-8）

命名のガイドライン

Performance Monitor では、ユーザ定義グループの名前および説明に次の制限があります。

- デバイス グループ名は 64 文字以下に制限されます。
- デバイス グループの説明は 256 文字以下に制限されます。
- デバイス グループの名前および説明には、a123b や A123B のようなスペースと英数字（大文字と小文字）以外に、Performance Monitor では次の文字だけを使用できます。
  `!#%()*+/-:;=?_[]\{}~$,.`
- 次の文字はグループの名前および説明に使用できません。
  `" ' ‘ ” ` @ ^ & < > |`

グループの編集

ユーザ定義グループの名前、説明、および構造を編集できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Groups] を選択します。

[Managing Groups] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　ユーザ定義のデバイス グループをクリックします。

ステップ 3　デバイス グループを変更するには、[Edit] をクリックします。

（注）　システム定義グループは編集できません。

[Edit Group] ページに、オブジェクト セレクタ、テキスト ボックス、およびアクション ボタンが表示されます。

ステップ 4　要件を満たすタスクを実行します（表 11-4）。

更新されたディスプレイに、実行したタスクの結果が表示されます。

ステップ 5　変更を保存するか破棄して、[Managing Groups] ページに戻ります。

- 新しいグループを保存するには、[Save] をクリックします。

  新しいグループが表示され、オブジェクト セレクタに追加されます。
- 変更を破棄するには、[Cancel] をクリックします。

参考

表 11-4　[Edit Group] ページのタスク

オプション タスク	手順
デバイス グループ名を変更する。	[Name] テキスト ボックスで、デバイス グループ名を変更します。「命名のガイドライン」（P.11-10）を参照してください。
デバイス グループの説明を入力または変更する。	[Description] テキスト ボックスで、デバイス グループの新しい説明を入力するか、変更します。「命名のガイドライン」（P.11-10）を参照してください。
編集したグループにデバイスを個別に追加する。	1. 選択ツリーから 1 つ以上のデバイスを選択します。 2. 選択したデバイスを編集したグループに追加するには、[Add] をクリックします。 追加されたデバイスは、[Group] リストの [Devices] に表示されます。
1 つまたは複数のグループから、編集したグループにデバイスを追加する。	1. 1 つまたは複数のデバイスまたはデバイス グループを選択します（すべてのサブグループおよびそれに含まれるデバイスを選択します）。 2. 選択したデバイスを編集したグループに追加するには、[Add] をクリックします。 追加されたデバイスは、[Group] リストの [Devices] に表示されます。
編集したグループからデバイスを削除する。	[Group] リストからデバイスを選択し、[Remove] をクリックします。

関連トピック

- 「デバイス グループの管理」（P.11-8）

グループの削除

ユーザ定義デバイス グループを削除できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Devices] > [Managing Groups] を選択します。

[Managing Groups] ページに、オブジェクト セレクタとアクション ボタンが表示されます。「オブジェクト セレクタの使用方法」（P.3-11）を参照してください。

ステップ 2　ユーザ定義のデバイス グループをクリックします。

ステップ 3　デバイス グループを削除するには、[Delete] をクリックします。

（注）　システム定義グループは削除できません。

ステップ 4　[OK] をクリックします。

ユーザ定義グループを削除しても、そのグループ内のデバイスは削除されません。メンバーになっているシステム定義グループから、関連するデバイスに引き続きアクセスできます。

関連トピック

- 「デバイス グループの管理」（P.11-8）

CHAPTER 12

Performance Monitor の管理

ネットワークを効果的に管理するには、ミッションクリティカルなシステムで発生するイベントをできるだけ迅速に識別し、解決する必要があります。

Performance Monitor の管理オプションでは、イベント検出を設定し、公式に基づくしきい値とユーザ設定しきい値に従って、イベントを事前に識別して表示し、ログに記録できます。

次の表に、Performance Monitor からアクセスする管理オプションを示します。

表 12-1　Performance Monitor の管理オプション

オプション	説明
Notifications	パフォーマンス イベントまたは障害が発生した場合の SNMP トラップ、Syslog エントリ、または E メールからのモニタ対象サービスの通知を設定し、イネーブルにします。「通知の操作」（P.12-1）を参照してください。
Events	あらゆる優先順位のパフォーマンス イベントまたは障害イベントを生成するためのしきい値を設定し、イネーブルにします。「イベントしきい値の操作」（P.12-7）を参照してください。
System Parameters	使用できるデータ タイプのポーリング間隔とトランケーション間隔を設定し、イネーブルにします。「システム パラメータの操作」（P.12-9）を参照してください。
Logs	デバッグ ログ ファイルを表示してエクスポートしたり、切断された RAS ユーザ セクションの概要を表示します。「ログの操作」（P.12-10）を参照してください。
My Profile	Performance Monitor の起動時にデフォルトで表示されるページを選択します。「デフォルト ページの選択」（P.12-12）を参照してください。

通知の操作

Performance Monitor では、重要な条件がグローバルに、または特定のサービスに対して定義したパフォーマンス パラメータに達するか、または超えた場合に、自動的に通知できます。
Performance Monitor では、設定した各通知タイプに個別の通知を送信します。

ここでは、通知およびその設定方法について説明します。

サポートされる SNMP トラップと Syslog メッセージについて

通知のためには、SNMP トラップ、Syslog メッセージ、およびデバイス ポーリングによって情報を提供するモニタ対象デバイスから、Performance Monitor が重要な情報を受信する必要があります。詳細については、「SNMP トラップの受信」（P.2-17）を参照してください。

Performance Monitor では、次の種類の SNMP トラップを処理できます。

ソース デバイス	サポートされる SNMP トラップと Syslog メッセージ
ASA デバイス	• ASA-4-113019 • ASA-7-713052
CSM サービス モジュール	• 実サーバの状態遷移 • インターフェイスの運用状態
VPN サービス モジュール	• 追加されたポリシー • 削除されたポリシー • 追加されたクリプト マップ • 削除されたクリプト マップ • 接続されたクリプト マップ • 接続解除されたクリプト マップ • トンネルの開始 • トンネルの停止 • インターフェイスの運用状態
VPN ルータ	• 追加されたポリシー • 削除されたポリシー • 追加されたクリプト マップ • 削除されたクリプト マップ • 接続されたクリプト マップ • 接続解除されたクリプト マップ • トンネルの開始 • トンネルの停止 • インターフェイスの運用状態

Performance Monitor では、次の種類の Syslog メッセージを処理できます。

ソース デバイス	サポートされる Syslog メッセージのタイプ
VPN 3000 コンセントレータ	• IKE-5-120 • AUTH-5-28
PIX ファイアウォール	• PIX-1-104001 • PIX-1-105006 • PIX-1-105007 • PIX-1-101001 • PIX-1-1011002 • PIX-1-101004 • PIX-2-709007 • PIX-3-201008 • PIX-3-202001 • PIX-4-113019 • PIX-7-713052
ファイアウォール サービス モジュール	• PIX-1-105006 • PIX-1-105007 • PIX-1-101001 • PIX-1-1011002 • PIX-1-101004 • PIX-2-709007 • PIX-3-201008 • PIX-3-202001 • FWSM-4-113019 • FWSM-7-713052

通知の設定

Performance Monitor では、重要な条件がグローバルに、または特定のサービスに対して定義したパフォーマンス パラメータに達するか、または超えた場合に、自動的に通知できます。
Performance Monitor では、設定した各通知タイプに個別の通知を送信します。

次の 3 つの通知レベルがあります。

- Global：すべてのサービス タイプのすべてのイベント。
- Service：1 つのサービス タイプのすべてのイベント。
- Event：特定のサービス タイプの特定のイベント。

（注）　グローバルに通知を設定し、サービス レベルまたはイベント レベルで重複している場合は、通知を重複して受信します。また、イベントレベルで通知を設定し、それがサービス レベルで設定した通知設定と重複している場合も、通知を重複して受信します。

始める前に

- CiscoWorks Common Services で E メール サーバを使用するように設定していることを確認します。「E メール使用のための Common Services の設定」（P.2-16）を参照してください。
- 通知を設定するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [Notifications] を選択します。

ステップ 2　設定する通知のタイプをツリーで選択します。

- [Global]：Global 通知を設定します。
- サービス タイプ（[Firewall]、[Load Balancing]、[Remote Access VPN]、[SSL]、[Site-to-Site VPN]）：サービスのすべてのイベント タイプに対して通知を設定します。
- サービス タイプ内のイベント タイプ（ツリーの一番下のノード、たとえば、[CPU Usage]）：特定のイベント タイプだけの通知を設定します。「通知がサポートされるイベント タイプについて」（P.12-5）を参照してください。

ヒント　ツリーでの選択内容で画面が更新されますが、選択内容はツリーで維持されません。設定する通知の種類を確認するには、[Email Recipients] リストの上にある右側のペインでタイトルを確認する必要があります。このタイトルには、[Global Notifications]、[Service Notifications: *Service Type*]、[Event Notifications: *Event Type*] などと表示されます。

ステップ 3　表 12-2 に示すいずれかのタスクを実行します。

通知の設定手順

表 12-2　通知の設定手順

タスク	手順
E メールの受信者を追加する。	1. [Email Recipients] 領域で、[Add] をクリックします。 2. [Edit Email Recipients] ウィンドウで、[Email Address] テキスト ボックスに E メール アドレスを 1 つ入力します。 3. E メール メッセージを送信するイベントの重大度の範囲を定義します。[From Priority] リストと [To Priority] リストでオプションを選択します。[P1] は重大度が高い問題、[P5] は重大度が低い問題で、[OK] は解決した問題です。[From] 領域での重大度レベルの選択は、[To] 領域でのレベル選択よりも低くする必要があります。 4. [Apply] をクリックします。[Edit Email Recipients] ウィンドウが閉じます。[Notifications] ページが更新され、定義した受信者が [Email Recipients] リストに表示されます。

表 12-2　通知の設定手順（続き）

タスク	手順
SNMP トラップの受信者を追加する。	1. [Trap Recipients] 領域で、[Add] をクリックします。 2. [Edit Trap Recipients] ウィンドウで、[Host] テキスト ボックスに管理対象のデバイス IP アドレスまたは DNS ホスト名を入力します。 3. [Port] テキスト ボックスに、デバイスの [SNMP] ポート番号を指定します。 4. [Community] テキスト ボックスに、デバイスの read コミュニティ ストリングを指定します。 5. [Apply] をクリックします。[Edit Trap Recipients] ウィンドウが閉じます。[Notifications] ページが更新され、定義した受信者が [Trap Recipients] リストに表示されます。
Syslog の受信者を追加する。	1. [Syslog Recipients] 領域で、[Add] をクリックします。 2. [Edit Syslog Recipients] ウィンドウで、[Host] テキスト ボックスに Syslog ホスト名または IP アドレスを 1 つ入力します。 3. [Port] テキスト ボックスに、デバイスのポート番号を指定します。 4. [Apply] をクリックします。[Edit Syslog Recipients] ウィンドウが閉じます。[Notifications] ページが更新され、定義した受信者が [Syslog Recipients] リストに表示されます。
受信者を編集する。	1. 編集する受信者を選択し、その領域の [Edit] ボタンをクリックします。 2. 必要に応じて設定を変更し、[Apply] をクリックします。
受信者を削除する（通知をディセーブル）。	削除する受信者を選択し、その領域の [Delete] ボタンをクリックします。 **（注）**　削除はすぐに反映されます。元に戻す機能はありません。
イベント タイプごとのしきい値を設定する。	特定のイベント タイプを選択すると、受信者リストの下にある [Threshold] ボタンをクリックして、イベントの通知のしきい値を設定できます。しきい値の設定の詳細については、「イベントしきい値の操作」（P.12-7）を参照してください。

通知がサポートされるイベント タイプについて

通知では 40 種類を超えるイベント タイプがサポートされ、サービス タイプごとに分類されます（表 12-3 を参照してください）。

表 12-3　通知のイベント タイプ

モニタ対象のサービス	サポートされるイベント タイプ
ファイアウォール	CPU Usage
	Command Replication
	Device Accessible via Https
	Device Accessible via Snmp
	Failover
	Failover Cable
	Fragment Size
	HA Other
	Interface State
	Memory Usage
	New Connections
	Regular Translation
	Translation Slot
ロード バランシング	Connection Failure
	Created Connection Rate
	Dropped Connection
	Interface Status
	Real Server Status
リモート アクセス VPN	Bandwidth Usage
	CPU Usage
	Device Accessible via Snmp
	Device Load
	Inbound Connection Failures
	Interface Status
	Packet Drop
	SEP Module Packet Drop
	SEP Module Status
SSL	CPU Usage
	Device Accessible via Https
	Memory Usage
	SSL Errors

表 12-3　通知のイベント タイプ（続き）

モニタ対象のサービス	サポートされるイベント タイプ
サイト間 VPN	CPU Usage Connection Failures Crypto Map Binding Crypto Map Change Crypto Packet Drops Device Accessible via Https Device Accessible via Snmp ISAKMP Policy Change Interface Status Memory Usage Packet Drop Tunnel Status 次のすべてを実行した場合、DMVPN スポークツースポーク トンネルに関する大量の E メールを受信する可能性があります。 • スポーク間セッションをサポートするフル メッシュ トポロジを使用するように、DMVPN を設定する。 • サイト間 VPN トンネル ダウン イベントのしきい値を設定する。 • これらのイベントの自動 E メール通知をスケジューリングする。 サイト間トンネルはダイナミックで、多数のトンネル ダウン イベントが含まれる設計により、存続期間が短くなります。この大量の E メールの問題が発生する場合は、E メールの通知をディセーブルにするか、ハブだけをモニタするように Performance Monitor を設定することを推奨します。

イベントしきい値の操作

しきい値を作成するには、次のことを実行します。

- 特定のサービスのパフォーマンス メトリックまたは障害のメトリックに動作状態の境界（OK、Degraded、Overloaded など）を定義します。
- レコードが更新される前に動作状態が再帰する必要がある連続ポーリング サイクルの数を指定します。
- 特定のメトリックに対して可能性のあるそれぞれの動作状態に優先度レベルを関連付けます（表示およびユーザ通知のため）。

定義したしきい値でさまざまなサービス、メトリック、および状態を使用しますが、すべてのしきい値の定義で同じ基本ワークフローに従います。

ヒント　状態が定義したしきい値を超えるか下回ると、Performance Monitor でアラームが記録されます。アラームは対応するイベント ブラウザで表示および解釈できます。場合によっては、[Critical Problems] の要約で重大な問題も表示できます。「イベント ブラウザの操作」（P.3-12）および「クリティカルな問題の要約の操作」（P.4-2）を参照してください。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [Events] を選択します。

ステップ 2　TOC からサービスを選択します。

（注）　インスペクション ポリシーで設定されている場合、[Firewall Devices] ページに IOS ルータが表示されますが、[Admin] > [Events] からサイト間 VPN を選択して、ルータのイベントしきい値を設定する必要があります。[Threshold Configuration] ページからファイアウォール サービスのイベントしきい値を設定しても、ルータに適用されません。

ステップ 3　しきい値を設定するパフォーマンス メトリックまたは障害のメトリックが見つかるまで、[Events] リストのエントリをスキャンし、対応する行のオプション ボタンを選択します。

ステップ 4　[Threshold] をクリックします。

ヒント　また、[Admin] > [Notifications] を選択し、イベントを選択して [Threshold] をクリックすると、イベントのしきい値を設定することもできます。

[Threshold Configuration] ページが表示されます。

- 障害のメトリックを選択した場合、[Threshold Configuration] ページに 2 つの相反する [State Name] 値（たとえば、[Up] と [Down]）が表示されます。または、1 つの極端な状態値（[OK] など）の後に、複数の中間のステータスが続きます。
- パフォーマンス メトリックを選択した場合、[State Name] 値の範囲（[OK]、[Medium]、[High] など）が [Threshold Configuration] ページに表示されます。各値は範囲内の上限のパーセンテージと下限のパーセンテージに関連付けられます。

ステップ 5　[Enable] チェックボックスをオンにします。

[Enable] チェックボックスをオンにする必要があります。そうしないと、[Threshold Configuration] ページで値を定義できません。

ステップ 6　次のいずれかを実行します。

- [State Name] 領域に 2 つの相反する値（たとえば、良好な [Up] と、問題がある [Down]）が表示される場合、次の内容を指定します。
  - 問題がある状態のイベントの優先度レベル。
  - トリガーするポーリング間隔の失敗数、クリアする成功の回数、[Repetitions before State Change] フィールドの問題のある状態に関連付けられたイベント。
- [State Name] 領域に 3 つの値の範囲が表示された場合は、上限と下限のしきい値パーセンテージ、ポーリング間隔の回数、範囲内の 3 つの値のそれぞれの優先度レベルを指定します。たとえば、中間の状態の下限のしきい値の境界として 10% を選択します（この場合、選択内容が開始状態の上限しきい値パーセンテージとして自動的に適用されます）。

（注）　パフォーマンス メトリックのしきい値を設定する場合、開始状態の下限しきい値パーセンテージは常にゼロ（0%）で、優先度は常に [OK] です。問題のある状態の上限のしきい値パーセンテージは常に 100% です。これらの値は変更できません。

ステップ 7　次のいずれかを実行します。

- 選択内容を破棄して [Events] ページに戻るには、[Cancel] をクリックします。
- 選択内容を保存して実装するには、[Apply] をクリックします。
- すべての値をデフォルト設定にリセットし、[Threshold Configuration] ページを表示したままにするには、[Default] をクリックします。

システム パラメータの操作

ポーリング間隔、トランケーション間隔、およびユーザ セッション データの保存を設定できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [System Parameters] を選択します。

ステップ 2　表 12-4 に示すように、必要な設定を行います。次の表に、各設定で許可された最小値と最大値、設定のデフォルトを示します。すべての値をデフォルトに戻すには、[Default] ボタンをクリックします。

システム パラメータ

表 12-4　システム パラメータの設定

行の名前	オプション タスク	手順
Polling Interval (mins)	ポーリング間隔を設定します。	ポーリング間隔を分単位で指定するオプションをリストから選択し、[Apply] をクリックします。
Hourly aggregated data is kept for (days)	時間ごとのデータのトランケーション間隔を設定します。	時間ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Daily aggregated data is kept for (days)	日ごとのデータのトランケーション間隔を設定します。	日ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Weekly aggregated data is kept for (days)	週ごとのデータのトランケーション間隔を設定します。	週ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Monthly aggregated data is kept for (days)	月ごとのデータのトランケーション間隔を設定します。	月ごとのデータを保持する日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Event data is kept for (days)	イベントの履歴データのトランケーション間隔を設定します。	イベント履歴のトランケーション（切り捨て）が実行されるまでの日数を指定するオプションをリストから選択し、[Apply] をクリックします。

表 12-4　システム パラメータの設定（続き）

行の名前	オプション タスク	手順
Task data is kept for (days)	タスクの履歴データのトランケーション間隔を設定します。	タスク履歴のトランケーション（切り捨て）が実行されるまでの日数を指定するオプションをリストから選択し、[Apply] をクリックします。
User Session Polling Interval (hours)	ユーザ セッションのポーリング間隔を設定します。	ポーリング間隔を時間単位で指定するオプションをリストから選択し、[Apply] をクリックします。
User Session Report data is kept for (days)	ユーザ セッション データのトランケーション間隔を設定します。	ユーザ セッション レポートのトランケーション（切り捨て）が実行されるまでの日数を指定するオプションをリストから選択し、[Apply] をクリックします。
Logout User Audit Trail data is kept for (months)	ユーザ監査証跡データのトランケーション間隔を設定します。	ユーザ監査証跡のトランケーション（切り捨て）が実行されるまでの月数を指定するオプションをリストから選択し、[Apply] をクリックします。

ログの操作

Performance Monitor 自体に問題があるという例外的なイベントでは、Performance Monitor のデバッグ ログ ファイルを表示またはダウンロードして、問題の解決のために TAC を利用できます。

また、ログ アウトしたすべての RAS ユーザの VPN セッションを説明している監査証跡も表示できます。

始める前に

このオプションを使用するための適切な権限を持っていることを確認します。ユーザ セッションを終了するには、システム管理者またはネットワーク管理者の必要があります。「ユーザの権限について」（P.3-2）を参照してください。

手順

ステップ 1　[Admin] > [Logs] を選択します。

ステップ 2　TOC からオプションを選択します。

- [Debugging Log Files] をクリックして、Performance Monitor のトラブルシューティングで使用されるログのリストを表示します。このログにはサーバ上の場所や現在のサイズが含まれています。次のデバッグ ログを利用できます。
  - faults.log : *Faults Log* には、障害の履歴データが表示されます。
  - job.log : *Job Log* には、Performance Monitor ジョブの履歴が表示されます。
  - polling.log : *Polling Log* には、displays historical デバイス ポーリング データの履歴が表示されます。
  - validation.log : *Validation Log* には、デバイス ポーリング データの履歴が表示されます。
  - mcpui.log : *Monitoring Center for Performance User Interface Log* には、最近のユーザ インターフェイスのオペレーションが表示されます。
- [Logout User Audit Trail] をクリックすると、ログアウトした RAS VPN ユーザの統計情報が表示されます。表 12-5 に、終了したユーザ セッションを示します。

（注）　ユーザ ログアウト機能については、第 5 章「リモート アクセス VPN サービスのモニタリング」に説明があります。

ステップ 3　（任意）TOC から [Debugging Log Files] を選択した場合、オプション ボタンをクリックしてログを選択し、次のいずれかを実行します。

- HTML バージョンのログを表示するには、[View] をクリックします。
- ログのローカル コピーを保存するには、[Download] をクリックし、表示されたウィンドウで [File] > [Save As] を選択してログをテキスト ファイルまたは HTML ファイルとして保存します。

ログの表示中に [Refresh] をクリックして、最新のポーリング サイクルから情報を表示できます。

参考

表 12-5　[Logout User Audit Trail]

エレメント	説明
[Administrator Name] カラム	記述された VPN セッションを終了した（または終了しようとした）ユーザの CiscoWorks ユーザ名を表示します。 （注）　ユーザ セッションを終了するには、システム管理者またはネットワーク管理者の必要があります。「ユーザの権限について」（P.3-2）を参照してください。
[Status] カラム	強制的なログアウトに成功したか、失敗したかを示します。
[Error Message] カラム	失敗した場合、関連するエラー メッセージを表示します。 （注）　一部の障害は不明なエラーの結果として発生します。このような場合、Performance Monitor でこのカラムにテキストが表示されません。
[Time] カラム	説明した VPN セッションがいつ終了したかを示すタイムスタンプを表示します。
[Logged Out User] カラム	終了した VPN セッションのユーザ名を表示します。
[User Group] カラム	セッションが終了した RAS ユーザに関連付けられた VPN 3000 ユーザ グループの名前を示します。
[Client IP Addr] カラム	VPN に接続されている、説明した RAS ユーザからの IP アドレスを表示します。
[Protocol] カラム	説明した VPN セッションのプロトコルを識別します。
[VPN3K Device] カラム	RAS ユーザが切断された VPN 3000 コンセントレータの DNS 名または IP アドレスを表示します。
[Traffic In] カラム	インバンド バイト数を表示します。
[Traffic Out] カラム	アウトバウンド バイト数を表示します。
[Connection Duration] カラム	VPN トンネルが切断されるまでの合計期間（秒単位）を表示します。
[Throughput (kbps)] カラム	VPN トンネルが切断されるまでの平均スループット速度を表示します。

デフォルト ページの選択

Performance Monitor の起動時にデフォルトで表示されるページを選択できます。デフォルトは [Summary] > [Critical Problems] です。

手順

ステップ 1　[Admin] > [My Profile] を選択します。

ステップ 2　選択ツリーでページ名をクリックし、[Apply] をクリックします。

選択したページは、次回 Performance Monitor を起動したときに最初に表示されます。

APPENDIX A

Performance Monitor についての FAQ

ここでは、Performance monitor についての一般的な質問に対する回答と、トラブルシューティングのヒントを示します。

インストール

ブラウザに Performance Monitor を読み込めない原因は何ですか。

サーバの起動時または再起動時に、必要なプロセスを初期化するために約 5 分かかります。このようなプロセスの初期化中にブラウザに Performance Monitor を読み込もうとすると、次のようなエラーメッセージが表示されます。

- Could not connect to JRun Connector Proxy
- Internal Server Error
  The server encountered an internal error or misconfiguration and was unable to complete your request.

このようなメッセージが表示された場合は、数分待ってから Performance Monitor をもう一度起動してみてください。それでも起動できない場合は、システム管理者に連絡してください。

Performance Monitor を起動しようとすると、エラー 500 が表示されるのはなぜですか。

Performance Monitor を起動しようとしたときに次のエラー メッセージが表示される場合は、認証と認可（AAA）に Cisco Secure ACS サーバ（ACS）を使用していることが考えられます。

```
Error: 500
Location: /mcp/goHome.do
Internal Servlet Error:
java.lang.ArrayIndexOutOfBoundsException: 0 >= 0
```

AAA に ACS を使用する場合、次の手順を実行して、ACS および Performance Monitor が一緒に動作するように適切に設定されていることを確認してください。

ステップ 1　Performance Monitor サーバが AAA に ACS サーバを使用するように設定されていることを確認します。

a. ブラウザから、Performance Monitor サーバにログインします。

b. URL を **https://***server_name*/**cwhp/loginModule.do** に変更します。*server_name* は Performance Monitor サーバの DNS 名または IP アドレスです。

[AAA Server Information] ページで [ACS] オプション ボタンを選択し、必要なクレデンシャルが存在している必要があります。

ステップ 2　ACS サーバが Performance Monitor と連動するように設定されていることを確認します。すべての Performance Monitor ユーザ名に対して、対応する ACS ユーザ名が存在している必要があります。

a. Performance Monitor にアクセスするすべての ACS ユーザが、Performance Monitor へのアクセスを許可されたグループに属していることを確認します。詳細については、Cisco Secure ACS のユーザ ガイドを参照してください。

b. Performance Monitor ユーザが属している ACS グループを編集します。[MCP] チェックボックスおよび [Assign Performance Monitor for Any Network Device] オプション ボタンがオンになっていることを確認します。詳細については、Cisco Secure ACS のユーザ ガイドを参照してください。

Performance Monitor が正常に動作していることを確認するにはどうすればいいですか。

Performance Monitor は、必要なサーバ プロセスも実行している場合にだけ正常に動作します。

ステップ 1　ブラウザから、Performance Monitor サーバにログインします。

ステップ 2　[Common Services] で、[Server] > [Admin] > [Processes] を選択します。

ステップ 3　次のプロセスが実行されていることを確認します。

- Apache
- Tomcat
- MCP
- McpDbEngine

ステップ 4　必要なプロセスが実行されていない場合は、プロセスを開始してください。「Performance Monitor プロセスのステータスを変更するにはどうすればよいですか。」を参照してください。

Performance Monitor プロセスのステータスを変更するにはどうすればよいですか。

いずれかのプロセスを実行していない場合、プロセスを起動するか、またはすべてのプロセスを停止してから再起動します（すべてのプロセスを適切な順序で開始します）。

ステップ 1　特定のプロセスを再起動するには、次のいずれかを実行します。

- Performance Monitor のブラウザ セッションで、[Common Services] で、[Server] > [Admin] > [Processes] を選択し、プロセスを選択して [Start] または [Stop] をクリックします。
- サーバで、Windows コマンド ウィンドウの *NMSROOT*¥bin から、プロンプトで **pdexec** <*Process Name*> と入力します（プロセス名では、大文字と小文字が区別されます）。

（注）　特定のプロセスを選択する場合、そのプロセスの依存関係は自動的に開始されません。

プロセスが起動するまで 5 分お待ちください。

ステップ 2　問題が続く場合は、サーバからすべてのプロセスを再起動してください。ブラウザ セッションからログアウトし、サーバにログインして、Windows のコマンドラインを開いてください。ディレクトリを *NMSROOT*¥bin に移動し、次のコマンドを入力して、すべてのプロセスを停止してから再起動してください。

a. プロセスを停止するには、**net stop crmdmgtd** と入力します。

b. プロセスを起動するには、**net start crmdmgtd** と入力します。

ポート 162 がすでに使用されている場合に、SNMP トラップを別のポートに転送するにはどうすればよいですか。

サーバ上の別のアプリケーションが UDP ポート 162 を使用して SNMP トラップを受信している場合、modifyTrapReceiverPort.pl スクリプトを使用して Performance Monitor で Fault.properties ファイルに別のポート番号を指定する必要があります。

ヒント　どのアプリケーションでサーバの UDP ポート 162 を使用しているかが不明な場合は（またはどのアプリケーションがそのポートを使用しているかがわかっている場合でも）、Windows のコマンド **netstat -o -p udp** を使用して、Process ID Number（PID; プロセス ID 番号）をそのポートに関連付け、タスク マネージャ（Ctrl-Shift-Esc）を使用して PID を名前付きのアプリケーションに関連付けることができます。

ステップ 1　CiscoWorks Server の Daemon Manager を停止するには、Windows のコマンドラインで **net stop crmdmgtd** と入力します。

ステップ 2　SNMP トラップを転送するアプリケーションを、選択した UDP ポートで Performance Monitor サーバに転送するように設定します。UDP ポート番号は 1024 よりも大きくする必要があります。

ステップ 3　コマンドラインで次のように入力して、Performance Monitor が UDP ポートで SNMP トラップを受信するように設定します。

NMSROOT¥mcp¥bin¥modifyTrapReceiverPort.pl **disable** *port_number*

NMSROOT は Common Services をインストールしたサブディレクトリのフル パス名で、*port_number* は Performance Monitor サーバが SNMP トラップを受信する実際の UDP ポート番号です。

ステップ 4　CiscoWorks Server の Daemon Manager を再起動するには、コマンドラインで **net start crmdmgtd** と入力します。

デバイスのインポート、検証、および管理

DCR からのインポートに失敗するのはなぜですか。

次の 2 つの可能性があります。

- デバイス クレデンシャルのインポートに失敗した DCR サーバで SSL がイネーブルになっていない場合、その DCR サーバで SSL をイネーブルにしてからインポートを再試行してください。
- DCR サーバに SNMP 設定およびデバイスで使用するログイン クレデンシャルに正しくないレコードが含まれている場合、DCR サーバでそのレコードを修正してからインポートを再試行してください。

CSV ファイルからの SSL サービス モジュールのインポートに失敗するのはなぜですか。

CSV ファイルから SSL サービス モジュールをインストールできませんが、Performance Monitor に手動で追加することはできます。SSL サービス モジュールに DNS 名が含まれている場合、Performance Monitor で DNS サーバが設定されていることを確認してください。これによって、Performance Monitor で DNS 名を IP アドレスに変換できます。

SSL サービス モジュールを手動で追加する方法については、「Importing Devices ウィザードを使用したデバイスのインポートまたは追加」（P.2-9）を参照してください。

CSV ファイルからのインポートに失敗するのはなぜですか。

正しくない CSV ファイル形式を使用している可能性があります。サポートされている形式を使用するサンプル CSV ファイルを参照するには、**https://**<*server_name*>**/mcp/device_CSV_sample.htm** にアクセスしてください。*server_name* は、お使いの Performance Monitor サーバの DNS 名または IP アドレスです。

Common Services の Device Credentials Repository（DCR）または RME から CSV ファイルを生成できます。Performance Monitor では CSV バージョン 3.0 だけがサポートされ、それ以前のバージョンはサポートされません。

インポートしたデバイスが [Device Validation Tasks] ページに表示されないのはなぜですか。

Importing Devices ウィザードで必要なすべての手順を実行した後に、新しいタスクが [Device Validation Tasks] ページ（[Devices] > [Importing Devices]）に表示されない場合、またはインポートするデバイスが他のインターフェイス ページに表示されない場合は、MCP プロセスが実行されていることを確認してください。MCP プロセスではデバイスの検証およびポーリングを実行します。このプロセスが実行されていない場合は、[Device Validation Tasks] ページに新しい検証タスクが表示されず、[Import Devices] ページに関連するエラー メッセージが表示されません。

ステップ 1　MCP プロセスが実行されているかどうかを確認するには、次の手順を実行します。

a. Performance Monitor サーバにログインします。

b. 次のいずれかを実行します。

- ブラウザで、[Common Services] > [Server] > [Admin] > [Processes] を選択します。
- サーバの CLI で、*NMSROOT*¥bin からプロンプトに **pdshow MCP** と入力します（MCP は大文字にする必要があります）。

ステップ 2　MCP プロセスが実行されていない場合は、次のいずれかを実行します。

- ブラウザで、[Common Services] > [Server] > [Admin] > [Processes] を選択し、[Start Process] ページから MCP プロセスを選択し、[Start] をクリックします。
- サーバの CLI で、*NMSROOT*¥bin からプロンプトに **pdexec MCP** と入力します（MCP は大文字にする必要があります）。

MCP プロセスが起動するまで 2 ～ 3 分お待ちください。

ステップ 3　Performance Monitor インターフェイスから、[Devices] > [Importing Devices] を選択します。

ステップ 4　[Refresh] をクリックします。

PIX Firewall デバイスをインポートしようとすると、エラー メッセージが表示されるのはなぜですか。

PIX Firewall デバイスのインポート時にユーザ パスワードではなく、イネーブル パスワードを使用すると、次のエラー メッセージが表示されます。

```
The Device <device name> could not be imported. Either the firewall HTTPS interface was
not enabled or the credentials are not correct. One device failed to be imported. To
monitor this device, you must import it again.
```

この問題を解決するには、イネーブル パスワードではなくユーザ パスワードを使用します。

PIX Firewall デバイスを Performance Monitor に追加できないのはなぜですか。

Microsoft Windows Certificate Services で PIX Firewall のクレデンシャルを生成した場合、クレデンシャルの不正な形式の URL または不正な形式の Microsoft Universal Naming Convention（UNC）名によって Performance Monitor で問題が発生する可能性があります。

次の例では、テキストの最後の行の UNC が file:// URL と誤って表示されています。この種のエラーによって、Performance Monitor で問題が発生する可能性があります。

```
[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://yourtest01/CertEnroll/TestConnect.crl
URL=file://¥¥yourtest01¥CertEnroll¥TestConnect.crl
```

このような問題を解決するには、PIX Firewall クレデンシャルを確認してください。不正な形式の URL または不正な UNC が含まれる場合、エラーが含まれていない新しいクレデンシャルを生成して、Performance Monitor にデバイスを追加してください。

[Monitor] タブにデバイスが表示されないのはなぜですか。

デバイスがモニタされていることを確認し、[Validation Task Details] ページでエラー メッセージを確認してください。

ステップ 1　[Devices] > [Managing Devices] を選択します。

[Managing Devices] ページにデバイスが表示され、モニタされていることを確認します。

ステップ 2　[Devices] > [Importing Devices] を選択します。

ステップ 3　[Device Validation Tasks] リストでデバイスのオプション ボタンをクリックし、[Details] をクリックします。

[Validation Task Details] ウィンドウに検証結果の履歴が表示されます。「検証タスクの履歴の表示」（P.2-14）を参照してください。

ステップ 4　[Validation Task Details] ウィンドウを更新するには、[Refresh] をクリックします。

Device Not Reachable というメッセージは何を意味していますか。

ポーラーがデバイスからすべての情報を取得できなかったため、一部のデバイス データを利用できない可能性があります。これは、次のような場合に発生します。

- **デバイスへの IP 接続が失われている。**IP 接続に影響を与えているネットワークの問題を探して解決してください。デバイスがビジーすぎて SNMP 要求に対応できない場合は、そのデバイスのマニュアルを参照して、問題の分析方法とデバイスの調整方法を調べてください。
- **デバイスのコミュニティ ストリングが変更された。**Performance Monitor で関連するエントリを修正してから、デバイスのポーリングを再試行してください。
- **デバイスの MIB 変数によってアクセスが制限されている。**インストールされている OS バージョンで、Performance Monitor で使用している MIB がサポートされているかどうかを確認してください。デバイスに新しい OS バージョンを使用できる場合は、最新の OS バージョンにアップグレードすることを検討してください。

SNMP Timeout エラー メッセージやイベントが表示される場合はどうすればよいですか。

SNMP Timeout パラメータを大きくするには、次のいずれかを実行します。

- [Devices] > [Importing Devices] でデバイスのインポート時に、パラメータを変更します。「Importing Devices ウィザードを使用したデバイスのインポートまたは追加」（P.2-9）を参照してください。
- [Devices] > [Managing Devices] でデバイスを編集します。「デバイスの編集」（P.11-3）を参照してください。

[SNMP Retries] は再試行の最大回数を示しています。再試行は、デバイスの SNMP エージェントとの通信に失敗したことを意味します。したがって、Performance Monitor で再度要求されます。

[SNMP Timeout] はデバイスが要求を待機する間隔を示します。その後の再試行間隔は、以前のタイムアウト値の 2 倍になるという再試行ポリシーのロジックを使用して計算されます。たとえば、初期タイムアウトが 3 秒で、再試行回数が 3 回の場合、各再試行間のタイムアウト値は 3、6、12 となり、合計 21 秒です。

すべてのデバイス ポーリングが停止したのはなぜですか。

1 つでもデバイスがタイムアウト期間内に Performance Monitor のポーリングに応答しなかった場合は、すべてのデバイスのポーリングが停止します。ポーリング タイムアウト期間を長くしてください。詳細については、「ポーリングのタイム アウトの設定」（P.2-18）を参照してください。

管理

- 「通知を受信できないのはなぜですか。」
- 「通知をディセーブルにするにはどうすればよいですか。」

- 「ポーリング情報がディスクに保存されないようにするにはどうすればよいですか。」
- 「SNMP トラップでイベントが生成されないのはなぜですか。」
- 「Performance Monitor データベースのバックアップと復元を行うにはどうすればよいですか。」

通知を受信できないのはなぜですか。

通知が適切に設定されていない可能性があります。

ステップ 1　[Admin] > [Notifications] を選択します。

ステップ 2　選択ツリーから、[Site-to-Site VPN] を選択します。

ステップ 3　[Email Recipients]、[Trap Recipients]、および [Syslog Recipients] の通知が設定されていることを確認してください。設定されていない場合は、設定してください。「通知の設定」（P.12-3）を参照してください。

通知をディセーブルにするにはどうすればよいですか。

ステップ 1　[Admin] > [Notifications] を選択します。

ステップ 2　選択ツリーで、関連するサービスのフォルダをクリックします。

[Service Notifications] ページに [Email Recipients]、[Trap Recipients]、および [Syslog Recipients] の通知が表示されます。通知はすぐにディセーブルになります。元に戻す機能はありません。

ステップ 3　ディセーブルにする通知を選択し、その通知のタイプの [Delete] をクリックします。

ポーリング情報がディスクに保存されないようにするにはどうすればよいですか。

高い頻度のポーリングで情報を収集し、ディスクがフルになることを防止するには、ポーリング データの保存日数を設定します。[Admin] > [System Parameters] を選択し、値を小さくして [Apply] をクリックします。「システム パラメータの操作」（P.12-9）を参照してください。

SNMP トラップでイベントが生成されないのはなぜですか。

SNMP トラップでイベントが生成されない場合、原因は次のいずれかまたは両方です。

- Performance Monitor だけではなく、別のアプリケーションでサーバの UDP ポート 162 を使用している。
- SNMP トラップを送信するようにデバイスが設定されていない。

ステップ 1　サーバ上の別のアプリケーションで UDP ポート 162 を使用して SNMP トラップを受信している場合、Performance Monitor で別のポートでトラップを受信するように再設定する必要があります。Windows のコマンドラインから、次のように入力します。

NMSROOT¥**bin¥perl.exe** *NMSROOT*¥**mcp¥bin¥modifyTrapReceiverPort.pl** *port*

NMSROOT は Common Services をインストールしたサブディレクトリのフル パス名で、*port* は、使用するポートの数値です（このコマンドでは Performance Monitor の Fault.properties ファイルを編集します）。

ステップ 2　Performance Monitor を再起動します。

再起動すると、Performance Monitor は新しいポート番号でトラップを待ち受けます。

ステップ 3　SNMP トラップを送信するようにデバイスが設定されていることを確認してください。必要な手順の詳細については、「デバイスのブートストラップ」（P.2-2）を参照してください。次のいずれかの方法で実行できます。

- Real Server Status ロード バランシング イベントを生成するように、SNMP トラップをセットアップします。
- 次のサイト間 VPN イベントを生成するように SNMP トラップをセットアップします。
  - Crypto Map Binding
  - Crypto Map Change
  - ISAKMP Policy Change
  - Tunnel Status
  - Interface Status

Performance Monitor データベースのバックアップと復元を行うにはどうすればよいですか。

Performance Monitor では、Common Services を使用してデータベースのバックアップと復元を行います。データベースのバックアップと復元を行う場合、Common Services を使用するすべてのアプリケーションのデータベースがバックアップまたは復元されます（たとえば、Performance Monitor と Security Manager が同じサーバにインストールされている場合、バックアップと復元が両方のアプリケーションに対して実行されます）。

バックアップまたは定期的なバックアップのスケジュールを作成するには、Common Services を開き、[Server] > [Admin] > [Backup] を選択します。バックアップと復元の詳細については、[Help] ボタンをクリックしてください。

レポート

- 「デバイスを削除してから、再び追加しました。レポートを実行すると、デバイスを追加する前のデータが表示されていることに気付きました。なぜでしょうか。」
- 「VPN 3000 コンセントレータのユーザ セッション レポートで SSL VPN（WEBVPN）ユーザ ログインの詳細が省略されるのはなぜですか。」
- 「VPN 3000 コンセントレータのユーザ セッション レポートが空白になるのはなぜですか。」

- 「Cisco 800 シリーズのルータの [CPU Usage%] カラムと [Memory Usage%] カラムが空白なのはなぜですか。」

デバイスを削除してから、再び追加しました。レポートを実行すると、デバイスを追加する前のデータが表示されていることに気付きました。なぜでしょうか。

デバイスを削除すると、データベースで Deleted とマークされますが、そのデバイスに関連するデータは 2 時間経過するまで削除されません。2 時間ごとに、バックグランド プロセスでデータベースが更新され、削除されたデバイスのデータが削除されます。2 時間以内に（データベースで関連データを削除される前に）デバイスを再び追加し、翌日にレポートを実行した場合、その日の情報とその週のそれ以前の日の情報が表示されます（2 時間以内にデバイスが削除された情報を除きます）。

VPN 3000 コンセントレータのユーザ セッション レポートで SSL VPN（WEBVPN）ユーザ ログインの詳細が省略されるのはなぜですか。

コンセントレータで WEBVPN Syslog クラス名をイネーブルにする必要があります。

ステップ 1　VPN 3000 Concentrator Series Manager にログインします。

ステップ 2　[Configuration] > [System] > [Events] > [Classes] を選択します。

ステップ 3　[Add] をクリックします。

ステップ 4　[Class Name] リストから [WEBVPN] を選択し、[Enable] チェックボックスをオンにします。

ステップ 5　[Events to Syslog] リストから [1-5] を選択し、[Add] をクリックします。

ステップ 6　右上にある [Save Needed] をクリックします。

ステップ 7　[OK] をクリックします。

ステップ 8　Syslog をイネーブルにします。手順については、「VPN 3000 コンセントレータのユーザ セッション レポートが空白になるのはなぜですか。」を参照してください。

VPN 3000 コンセントレータのユーザ セッション レポートが空白になるのはなぜですか。

VPN 3000 コンセントレータで Syslog がイネーブルになっていないために発生している可能性があります。Syslog をイネーブルにするには、次の手順を実行します。

ステップ 1　VPN 3000 Concentrator Series Manager にログインします。

ステップ 2　[Configuration] > [System] > [Events] > [Classes] を選択し、[Add] をクリックします。

ステップ 3　[Class Name] リストから [AUTH] を選択し、[Enable] チェックボックスをオンにします。

ステップ 4　[Severity to Syslog] リストから [1-5] を選択し、[Add] を 2 回クリックします。

ステップ 5　[Class Name] リストから [IKE] を選択し、[Enable] チェックボックスをオンにします。

ステップ 6　[Severity to Syslog] リストから [1-5] を選択し、[Add] をクリックします。

ステップ 7　右上にある [Save Needed] をクリックし、[OK] をクリックます。

ステップ 8　[Configuration] > [System] > [Events] > [Syslog Servers] を選択し、[Add] をクリックします。

ステップ 9　[Syslog Server] フィールドに Performance Monitor サーバの IP アドレスを入力し、[Add] をクリックします。

ステップ 10　（任意）Performance Monitor がコンセントレータで Syslog メッセージを送信する唯一のアプリケーションである場合、このアプリケーション自体のパフォーマンスを向上するには、次の手順を実行します。

a.　[Configuration] > [System] > [Events] > [General] を選択します。

b.　[Severity to Syslog] リストから、[None] を選択します。

c.　[Apply] をクリックします。

Cisco 800 シリーズのルータの [CPU Usage%] カラムと [Memory Usage%] カラムが空白なのはなぜですか。

これは既知の問題です。Cisco 800 シリーズのルータの Management Information Base（MIB; 管理情報ベース）では CPU 使用率の情報が提供されず、場合によっては（特定の IOS イメージがインストールされている場合）、メモリ使用率の情報が提供されません。

デバッグ

デバッグをオンにするにはどうすればよいですか。

ステップ 1　Performance Monitor を起動します。

ステップ 2　URL を **https://***server_name*/**mcp/debuglog.do** に変更します。*server_name* は Performance Monitor サーバの DNS 名または IP アドレスです。

[Enable Debug Log] ウィンドウが表示されます。

ステップ 3　必要なログ ファイルごとに、[debug] カラムでリストから [on] を選択します。

ステップ 4　[Submit] をクリックし、ウィンドウを閉じます。

ステップ 5　完了後にデバッグをオフにするには、次の手順を実行します。

a.　**https://***server_name*/**mcp/debuglog.do** に戻ります。

b.　[debug] カラムでリストから [off] を選択します。

c.　[Submit] をクリックし、ウィンドウを閉じます。

デバイスのインポートに関連する問題をデバッグするにはどうすればよいですか。

ステップ 1　次のログ ファイルのデバッグをオンにします。

- validation.log
- mcpui.log

手順については、「デバッグをオンにするにはどうすればよいですか。」を参照してください。

ステップ 2　Performance Monitor を再起動し、デバイスのポーリングを再試行してください。

ステップ 3　[Admin] > [Logs] > [Debugging Log Files] を選択します。

ステップ 4　validation.log および mcpui.log ファイルを選択し、[Download] をクリックします。

ステップ 5　ダウンロードしたファイルを、問題を処理している TAC サポート エンジニアに送信してください。

ステップ 6　完了後にデバッグをオフにします。

a. **https://***server_name*/**mcp/debuglog.do** に移動します。*server_name* は Performance Monitor サーバの DNS 名または IP アドレスです。

b. [debug] カラムでリストから [off] を選択します。

INDEX

P

R

S

T

V

い

か

く

け

こ

さ

し

す

せ

そ

た

つ

て

と

に

は

ひ

ふ

へ

ほ

め

も

ゆ

よ

り

る

れ

ろ