



CHAPTER 2

はじめる前に

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。重要なデバイス属性のローカル 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.2-8) 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.2-11) 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.2-15) 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.2-15) 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.2-16) 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」 (P.2-2)
- 「ルータのセットアップ」 (P.2-3)
- 「Catalyst 6500 スイッチのセットアップ」 (P.2-4)
- 「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)
- 「VPN 3000 コンセントレータのセットアップ」 (P.2-6)
- 「IPSec VPN 共有ポート アダプタ (VPN SPA) のセットアップ」 (P.2-8)

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	<p>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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> – <code>ssl-proxy(config) # ip ssh rsa keypair-name ssh-key</code> – <code>ssl-proxy(config) # crypto key generate rsa general-keys ssh-key</code> • 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。 <pre>ssl-proxy# show ip ssh</pre> <p>次のメッセージが表示されます。</p> <pre>SSH Enabled - version 1.5</pre>

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
<p>ステップ 1 SNMP をイネーブルにして、コミュニティ スtring 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。</p> <p>コンフィギュレーション モードに切り替えて、<code>snmp community community_string ro</code> と入力します。<code>community_string</code> は割り当てるコミュニティ スtring (読み取り専用) です。</p>
<p> 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。</p>
<p>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。</p> <ul style="list-style-type: none"> システム名を設定するには、<code>hostname name</code> と入力します。 システムの連絡先を設定するには、<code>snmp contact contact</code> と入力します。 場所を設定するには、<code>snmp location location</code> と入力します。
<p>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。</p> <pre>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</pre>
<p>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、<code>ip http secure-server</code> と入力します。</p> <p>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。</p>

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
<p>ステップ 1 SNMP をイネーブルにして、コミュニティ スtring 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。</p> <p>コンフィギュレーション モードに切り替えて、<code>snmp community community_string ro</code> と入力します。<code>community_string</code> は割り当てるコミュニティ スtring (読み取り専用) です。</p>
<p> 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。</p>
<p>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。</p> <ul style="list-style-type: none"> システム名を設定するには、<code>hostname name</code> と入力します。 システムの連絡先を設定するには、<code>snmp contact contact</code> と入力します。 場所を設定するには、<code>snmp location location</code> と入力します。
<p>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。</p> <pre>snmp-server enable traps slb real. snmp-server enable traps snmp. snmp-server host ip_address traps version 2 public casa slb snmp,</pre> <p><code>ip_address</code> 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。</p>
<p>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。</p> <pre>snmp-server host ip_address version 2c community_string ipsec isakmp snmp</pre> <p><code>ip_address</code> 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、<code>community_string</code> は割り当て済みのコミュニティ スtring (読み取り専用) です。</p> <pre>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</pre>

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	<p>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 <code>snmp-server host inside ip_address</code> コマンドを入力します。<code>ip_address</code> 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。</p> <p> 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。</p>
ステップ 2	<p>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 <code>http ip_address netmask if_name</code> と入力します。</p> <ul style="list-style-type: none"> <code>ip_address</code> は Performance Monitor をインストールしたサーバの IP アドレスです。 <code>netmask</code> 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。 <code>if_name</code> はインターフェイスの名前です (<code>inside</code> など)。 <p><code>netmask</code> 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 <code>171.69.74.0</code> を指定するには、<code>http: 171.69.74.0 255.255.255.0 inside</code> と入力します。</p>
ステップ 3	<p>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 <code>http server enable</code> と入力します。</p> <p>(注) <code>http server enable</code> 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せん。</p>
ステップ 4	<p>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、<code>no logging on</code> と入力します。</p> <ul style="list-style-type: none"> 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、<code>logging on</code> 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、<code>clock set hh:mm:ss {day month month day} year</code> 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、<code>logging timestamp</code> と入力します。 ログレベルを設定するには、<code>logging trap level</code> と入力します。<code>level</code> は、該当する最も低い重大度レベルです。たとえば、<code>logging trap error</code> と入力すると、重大度レベルが <code>error</code> (レベル 3) から <code>emergency</code> (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)。 <p> (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。<code>error</code> 重大度レベルを使用することを推奨します。</p> <ul style="list-style-type: none"> 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、<code>logging host if_name ip_address</code> と入力します。<code>if_name</code> はインターフェイス名で (たとえば、<code>dmz</code>)、<code>ip_address</code> 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、<code>logging host dmz 10.1.20.111</code>) 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
<p>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。</p> <p>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。</p> <ol style="list-style-type: none"> 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。 ブラウザの [Address] または [Location] フィールドで、https://address と入力します。<i>address</i> 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。 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。
<p>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。</p> <ul style="list-style-type: none"> 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。
<p>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。</p> <ol style="list-style-type: none"> 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。 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。<i>address</i> 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。 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。 [Configuration] > [Interfaces] を選択し、インターフェイス名をクリックします。 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.2-8)」を参照してください。 [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。 [Apply] 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 4	<p>SNMP をイネーブルにします。</p> <ol style="list-style-type: none"> この表の説明のとおり、VPN 3000 Concentrator Series Manager にログインします。 (任意) コミュニティ スtring 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。 コミュニティ スtring を入力し、[Add] をクリックして、[Save Needed] をクリックします。 [Configuration] > [System] > [Management Protocols] > [SNMP] 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。 <p> 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。</p>
ステップ 5	<p>XML インターフェイスをイネーブルにします。</p> <p>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。</p> <ol style="list-style-type: none"> 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。 [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	<p>linkup トラップと linkdown トラップを設定します。</p> <ol style="list-style-type: none"> 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。 [Class Name] リストから [IP] を選択します。 [Severity to Trap] リストから [1-3] を選択し、[Add] をクリックします。 [Configuration] > [System] > [Events] > [Trap Destinations] を選択し、[Add] をクリックします。 [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。 [SNMP Version] リストから [SNMPv2] を選択し、[Add] をクリックします。
ステップ 7	<p>Syslog を設定します。</p> <p>[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。</p> <ol style="list-style-type: none"> 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。 [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。 [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。 [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。 [Severity to Syslog] リストから [1-5] を選択し、[Add] をクリックします。 [Save Needed] をクリックし、[OK] をクリックします。 [Configuration] > [System] > [Events] > [Syslog Servers] を選択し、[Add] をクリックします。 [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。 (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。 [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手動で入力します。インポートは、デバイス属性の説明リスト（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 Comma-Separated Value (CSV; カンマ区切り値) ファイルまたは Device Credentials Repository (DCR) からデバイス属性をインポートできます。また、手動でデバイス属性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.3-17) 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。

はじめる前に

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。

デバイス属性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 モジュール属性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、デバイス属性情報の 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属性をマークします。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. 属性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tring を指定します。
read コミュニティ スtring 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tring 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tring がデフォルトとは異なる場合、検証を開始したり、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tring 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、属性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ーを確認できます。

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属性をマークします。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、属性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ーを確認できます。

- 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.2-11) を参照してください。



ヒント CSV ファイルからデバイス属性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 クレデンシア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、適切なクレデンシアルがあり、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 クレデンシアルを使用していて、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.3-17) 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 のクレデンシアルが指定され、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.2-11)
- 「[検証タスクの履歴の表示](#)」(P.2-12)

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。

は始める前に

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。

はじめる前に

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 <i>t</i> sec.	変数は次の内容を表します。
Failed: <i>x</i> of <i>y</i> devices were not imported. The task was completed in <i>t</i> sec.	<ul style="list-style-type: none"> <i>t</i>: 指定された検証にかかった秒数。 <i>x</i>: 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。 <i>y</i>: Performance Monitor で検証を試行したデバイスの数。
Partial Success: Some of the VPN 3000 Series Concentrator clusters failed to be validated. The task was completed in <i>t</i> 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 <i>DNS name</i> <i>IP address</i> could not be imported because the SNMP request timed out.
	The device <i>DNS name</i> <i>IP address</i> could not be imported because the object identifier is not supported.
	The device <i>DNS name</i> <i>IP address</i> could not be imported. Either HTTPS was not enabled or the credentials are not correct.
	The device <i>DNS name</i> <i>IP address</i> 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 <i>DNS name</i> <i>IP address</i> could not be imported. The chassis does not contain any supported services modules.
SSL	(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。
	The device <i>DNS name</i> <i>IP address</i> could not be imported. Either the version of SSL is not supported or the IP address is not for an SSL module.
	The device <i>DNS name</i> <i>IP address</i> could not be imported because the SSL module credentials are unknown.
	The device <i>DNS name</i> <i>IP address</i> could not be imported because Performance Monitor could not communicate with the SSL module.
	The device <i>DNS name</i> <i>IP address</i> could not be imported because the SSL login credentials are not correct.

サービス タイプ	メッセージ
ファイアウォール	The device <i>DNS name</i> <i>IP address</i> could not be imported. Either the firewall HTTPS interface was not enabled or the credentials are not correct.
	The device <i>DNS name</i> <i>IP address</i> could not be imported. The device must be imported using the Admin context IP address or DNS name.
ルータ	The device <i>DNS name</i> <i>IP address</i> could not be imported because this router does not support the IPSec MIB.
RAS VPN	The device <i>DNS name</i> <i>IP address</i> import was partially successful. To monitor the cluster <i>clustername</i> , you must import the device <i>IP address</i> .
	The device <i>DNS name</i> <i>IP address</i> 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 <i>DNS name</i> <i>IP address</i> 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 <i>DNS name</i> <i>IP address</i> 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 <i>DNS name</i> <i>IP address</i> could not be imported. Performance Monitor cannot establish an HTTPS connection with the VPN 3000 Concentrator Series Manager: HTTP < <i>HTTPCode</i> > - < <i>HTTPResponse</i> >. 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。

は始める前に

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。
- [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。
 - [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、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）。