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。

2 通りの可能性が考えられます。

- 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.2-10）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; 汎用命名規則）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一部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.2-10）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。

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。次の作業を実行できます。

- 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

- 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。どうしてですか。

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。