データ管理とシステム管理

この項では、次のトピックについて説明します。

Service Monitor データの管理

IP Communications Service Monitor（Service Monitor）は、登録されている Cisco 1040 からコール メトリック データを受信し処理します。オプションで、Service Monitor は、インストール時にアーカイブ用として指定されたディレクトリに、コール メトリック データをアーカイブします。アーカイブをイネーブルおよびディセーブルにするには、P.1-3 の「Service Monitor のセットアップ」を参照してください。

（注）　コール メトリックのアーカイブがイネーブルの場合、Service Monitor は、1 日あたり 1 つのデータ ファイルを作成します。各ファイルは午前 0 時に作成が開始されます。Service Monitor は、このファイルのバックアップや削除を行いません。

アーカイブがイネーブルの場合、次の操作を行う必要があります。

- ファイル システムをバックアップする方法と同じ方法で、Service Monitor データ ファイルをバックアップします（Common Services は Service Monitor データベースだけをバックアップします。Service Monitor データ ファイルは対象外です）。
- どの時点でサーバから古いデータ ファイルを削除するかを決定します。

Service Monitor データベースのバックアップおよび復元

Service Monitor データベースには、Cisco 1040 の設定に関する情報が保存されます。Service Monitor データベースの即時バックアップ、またはスケジュールされたバックアップを実行するには、Common Services ペインの CiscoWorks ホームページから、**Server > Admin > Backup** を選択し、Help をクリックして、その手順に従います。

Common Services には、データを復元するためのコマンドライン スクリプトがあります。手順を参照するには、Common Services ペインの CiscoWorks ホームページから **Server > Admin > Backup** を選択し、Help をクリックします。さらに、Restoring Data トピックへの Help リンクをクリックします。

Service Monitor データベースを復元するには、スイート名（*qovr*）を含むバックアップ ディレクトリ構造がわかっている必要があります。

- フォーマット：*/generation_number/suite*[*/directory*]*/filename*
- 例：/1/qovr/qovr.db

表 2-1 に、バックアップ ディレクトリ構造を示します。

表 2-1　Service Monitor バックアップ ディレクトリ構造

オプション	説明	使用方法
generationNumber	バックアップ番号	たとえば、1、2、および 3。3 が最新のデータベース バックアップです。
suite	アプリケーション、関数、またはモジュール	バックアップを実行する場合、すべてのスイートのデータがバックアップされます。CiscoWorks Common Services スイートは cmf です。Service Monitor アプリケーション スイートは qovr です。
directory	保存場所	スイート アプリケーション（適用可能な場合）

表 2-1　Service Monitor バックアップ ディレクトリ構造（続き）

オプション	説明	使用方法
filename	バックアップされる特定のファイル	ファイルにはデータベース（.db）が含まれます。 Service Monitor の場合、次のファイルが *generationNumber*/*suite* のすぐ下にリストされます。 qovr.db

Service Monitor データベースのパスワードの変更

Common Services には、qovr.db のパスワードを含むデータベース パスワードを変更するためのコマンドライン スクリプトがあります。手順を参照するには、CiscoWorks ホームページで Help をクリックし、*データベース パスワード*を検索します。

Syslog ファイルの管理

syslog ファイルが過剰に大きくなると、Service Monitor はメッセージの処理を停止します。したがって、ファイルのサイズをチェックし、過剰に大きくなった場合はそれを削除する必要があります。

ステップ 1　Service Monitor サーバのコマンド プロンプトで、次のコマンドを入力し、syslog サービスとデーモン マネージャを停止します。

```
net stop crmlog
net stop crmdmgtd
```

ステップ 2　syslog.log ファイルを削除します。通常、このファイルは次の場所にあります。

```
NMSROOT\log\syslog.log
```

（注）　NMSROOT は、システム上の CiscoWorks がインストールされているディレクトリです。インストール時にデフォルト ディレクトリを選択した場合は、C:\Program Files\CSCOpx です。

ステップ 3　次のコマンドを入力して、syslog サービスとデーモン マネージャを再開します。

```
net start crmlog
net start crmdmgdt
```

履歴ログ ファイルの管理

履歴ログ ファイルの ServiceMonitorHistory.log には、Cisco 1040 のリセット、設定のアップデート、エラーなどの Cisco 1040 イベントのレコードが含まれます。履歴ログ ファイルは、レコードが蓄積されるため、サイズが大きくなります。ファイルが過剰に大きくなった場合は、名前を変更して、Service Monitor が新しい履歴ログ ファイルの作成を開始できるようにします。

（注）　Common Services バックアップは、履歴ログ ファイルをバックアップしません。履歴ログ ファイルをバックアップする場合は、ファイル システムをバックアップする場合と同じ方法を使用します。

ログ ファイルの管理およびデバッグのイネーブル化とディセーブル化

次の情報はトラブルシューティング用に提供されます。Service Monitor ログ ファイルは、*NMSROOT*\log\qovr ディレクトリにあります。

- ProbeMgr.log：Cisco 1040 の通信が含まれます。
- QovrUI.log：Service Monitor ユーザ インターフェイスの処理が含まれます。
- Trapgen.log：アーカイブです。

（注） NMSROOT は、サーバ上の Service Monitor がインストールされているフォルダです。インストール時にデフォルト ディレクトリを選択した場合は、C:\Program Files\CSCOpx です。

次の手順で、ログ ファイルに書き込まれるメッセージのタイプ（および量）を増減できます。

ステップ 1　Service Monitor ホームページで、**Logging** を選択します。Logging: Level Configuration ページが表示されます。

（注） ロギングはディセーブルにできません。Service Monitor は常に、エラーおよび重大メッセージをアプリケーション ログ ファイルに書き込みます。

ステップ 2　Service Monitor 機能モジュールごとの Error チェックボックスは常にオンで、これをオフにすることはできません。

すべてのモジュールを、デフォルトのロギング レベルである Error に設定するには、次の手順に従います。

a. **Default** ボタンをクリックします。確認ページが表示されます。

b. **OK** をクリックします。

個々のモジュールのロギング レベルを変更するには、次の手順に従います。

a. 変更するモジュールごとに、次のロギング　レベルのいずれかを選択（または、すべて選択解除）します。

- Warning：エラー メッセージと警告メッセージをログに記録します。
- Informational：エラー、警告、および情報メッセージをログに記録します。
- Debug：エラー、警告、情報、およびデバッグ メッセージをログに記録します。

（注） モジュールのチェックボックスをすべて選択解除すると、デフォルトのロギング　レベルである Error に戻ります。

b. 変更内容を確認します。変更内容をキャンセルするには、**Cancel** ボタンをクリックします。変更内容を適用する場合は、**Apply** ボタンをクリックします。**Apply** ボタンをクリックすると、Service Monitor 機能モジュールが変更されたロギング レベルに即座にリセットされます。

システム アプリケーション MIB のロギング レベルの変更の詳細については、P.2-13 の「システム アプリケーション MIB ログ ファイルの表示」を参照してください。

ユーザの設定（ACS および非 ACS）

CiscoWorks サーバには、CiscoWorks アプリケーションのユーザを認証および認可するためのメカニズムがあります。ユーザが何を表示および実行できるかは、ユーザ ロールによって決まります。CiscoWorks サーバには、CiscoWorks アプリケーションのユーザを認証するための 2 種類のメカニズム（*モード*）があります。

- 非 ACS：認証および認可を提供する、サポートされるログイン モジュールを選択します。デフォルトでは、CiscoWorks サーバは CiscoWorks Local ログイン モジュールを使用します。Common Services の Permission Report に説明されているとおり、CiscoWorks は CiscoWorks Local ログイン モジュールを使用して、ロールとそれらのロールに関連付けられた特権を割り当てます（Common Services ホームページから Permission Report を生成するには、**Server > Reports > Permission Report** を選択して、**Help** をクリックします）。詳細については、P.2-6 の「非 ACS モードを使用したユーザの設定（CiscoWorks Local ログイン モジュール）」を参照してください。
- ACS：ACS モードでは、認証および認可は Cisco Secure Access Control Server（ACS）によって提供されます。Cisco Secure ACS は、ロールに関連付けられた特権を指定します。ただし、デバイスベースのフィルタリングも実行可能となるため、ユーザには認可されたデバイスだけが表示されます。ACS モードを使用するには、Cisco Secure ACS がネットワークにインストールされ、Service Monitor が Cisco Secure ACS に登録されている必要があります。詳細については、P.2-6 の「ACS モードを使用したユーザの設定」を参照してください。

Operations Manager が認証および認可に ACS モードを使用し、Service Monitor が同一システム上で稼働している場合は、Service Monitor も ACS モードを使用する必要があります。ACS モードを使用していない場合、Service Monitor ユーザにはアクセス権が一切付与されません。

非 ACS モードを使用したユーザの設定（CiscoWorks Local ログイン モジュール）

ユーザを追加し、CiscoWorks Local ログイン モジュールを使用してユーザ ロールを指定するには、**Administration > Add Users** を選択します。Common Services Local User Setup ウィンドウが開いたら、Help ボタンをクリックして設定手順に関する情報を表示します。

各ユーザ ロールと Service Monitor のタスクとの関係を理解するには、CiscoWorks Permission Report を使用します。CiscoWorks ホームページから、**Common Services > Server > Reports > Permission Report > Generate Report** を選択し、IP Communications Service Monitor までスクロール ダウンします。

ACS モードを使用したユーザの設定

認証および認可に ACS モードを使用するには、Cisco Secure ACS がネットワークにインストールされ、Service Monitor が Cisco Secure ACS に登録されている必要があります。

ステップ 1　CiscoWorks サーバの AAA モードを確認します。Common Services ホームページから、**Server > Security > AAA Mode Setup** を選択し、ACS または 非 ACS のどちらの Type オプション ボタンが選択されているかを確認します。

ステップ 2　Cisco Secure ACS サーバをチェックして、Service Monitor が Cisco Secure ACS に登録されているかどうかを確認します（ACS が選択されている場合）。

ステップ 3　ACS ロールを変更するには、次の手順に従います。

- ロールの変更の詳細については、Cisco Secure ACS のオンライン ヘルプ（Cisco Secure ACS サーバ上）を参照してください。
- DCR への Cisco Secure ACS の影響（特に、ロールの依存関係）の詳細については、Common Services のオンライン ヘルプを参照してください。

（注） Cisco Secure ACS を使用して Service Monitor ロールを変更すると、同じ Cisco Secure ACS サーバに登録された Common Services サーバを使用している Service Monitor のその他のすべてのインスタンスに変更内容が伝播されます。

ACS モードでの Service Monitor の使用方法

ここで説明するタスクを実行する前に、CiscoWorks サーバに Cisco Secure ACS が正常に設定されていることを確認しておく必要があります。CiscoWorks ログイン モジュールを ACS モードに設定した後に Service Monitor をインストールした場合、Service Monitor ユーザにはアクセス権が付与されません。ただし、Service Monitor アプリケーションは Cisco Secure ACS に登録されます。

（注） CiscoWorks サーバに定義されたシステム アイデンティティ セットアップ ユーザが Cisco Secure ACS に追加されており、ネットワーク管理者特権を持っている必要があります。

CiscoWorks ログイン モジュールを使用すると、CiscoWorks サーバのネイティブ メカニズム（CiscoWorks Local ログイン モジュール）以外の認証ソースによって新しいユーザを追加できます。この目的で、Cisco Secure ACS サービスを使用できます。

デフォルトでは、ACS モードの CiscoWorks サーバ認証方式には 5 つのロールがあります。ここでは、これらのロールを特権が小さなものから順に示します。

ヘルプ デスク	このロールのユーザには、固定的なデータからネットワーク ステータス情報にアクセスする特権があります。デバイスとやり取りしたり、ネットワークに到達するジョブをスケジュールしたりする特権はありません。 例：Cisco 1040、セットアップ、およびデフォルト設定の詳細表示（変更は実行できません）。
アプルーバ	このロールのユーザは、一切特権を持っていません。
ネットワーク オペレータ	このロールのユーザには、ネットワークからのデータ収集に関連したすべてのタスクを実行する特権があります。ネットワークへの書き込みアクセス権はありません。 例：Service Monitor のセットアップ、Cisco 1040 の追加、変更、削除。
ネットワーク管理者	このロールのユーザには、ネットワークを変更する特権があります。また、ネットワーク オペレータ タスクも実行できます。 例：ネットワーク オペレータと同じ。

システム管理者	このロールのユーザには、CiscoWorks システム管理タスクをすべて実行する特権があります。CiscoWorks ホームページで Permission Report を参照してください（**Common Services > Server > Reports > Permission Report**）。 例：デバッグのイネーブル化およびディセーブル化、ロギング レベルの設定。

Cisco Secure ACS を使用すると、特権をこれらのロールに変更できます。また、Common Services クライアント アプリケーションをビジネス ワークフローやニーズに最適化するために有効なカスタム ロールや特権を作成することもできます。デフォルトの CiscoWorks 特権の変更については、Cisco Secure ACS のオンライン ヘルプを参照してください（Cisco Secure ACS で、**Online Documentation > Shared Profile Components > Command Authorization Sets** をクリックします）。

Cisco Secure ACS での CiscoWorks ロールおよび特権の変更

Service Monitor の別のインスタンスが同じ Cisco Secure ACS に登録されている場合、Service Monitor のインスタンスはこれらのロール設定を継承します。さらに、Service Monitor ロールに加えた変更は、Cisco Secure ACS を通じて Service Monitor のその他のインスタンスに伝播されます。Service Monitor を再インストールすると、Cisco Secure ACS 設定が Service Monitor の再起動時に自動的に適用されます。

ステップ 1　**Shared Profile Components > IP Communication Service Monitor** を選択して、変更する Service Monitor ロールをクリックします。

ステップ 2　ビジネス ワークフローおよびニーズに適した Service Monitor タスクを選択または選択解除します。

ステップ 3　**Submit** をクリックします。

Service Monitor プロセスの起動および停止

Service Monitor プロセスを起動および停止するには、Common Services ペインの CiscoWorks ホームページで、**Server > Admin > Processes** を選択し、Help をクリックして操作手順を参照してください。表 2-2 に、Service Monitor 関連の CiscoWorks プロセスをすべて示します。

表 2-2　Service Monitor 関連の CiscoWorks プロセス

名前	説明	依存関係
QOVR	Service Monitor サーバ	QOVRDbMonitor
QOVRDbMonitor	Service Monitor データベース モニタ	QOVRDbEngine
QOVRDbEngine	Service Monitor データベース	—
QOVRMultiProcLogger	Service Monitor プロセス ロギング	—

CiscoWorks ホームページでの Service Monitor の追加登録

追加の Service Monitor を登録して、CiscoWorks ホームページに表示されるようにすることができます。登録可能な Service Monitor の数は無制限です。CiscoWorks ホームページは、各種アプリケーションのポータルにすぎません。ローカル Service Monitor 名が常に、CiscoWorks ホームページ上で最初に表示されます。

ホームページに複数の Service Monitor インスタンスがある場合は、常に、サーバ ホスト名（Service Monitor*@server*、CS*@server*）によって Service Monitor インスタンスを Common Services インスタンスにマップできます。

（注）　Service Monitor のリモート バージョンを起動すると、CiscoWorks はユーザ自体を再認証するためのプロンプトを表示します。

ステップ 1　Common Services ホームページから、**Home Page > Application Registration** を選択します。Application Registration Status ページが表示されます。

ステップ 2　**Registration** をクリックします。Registration Location ページが開きます。

ステップ 3　Import from Other Servers オプション ボタンを選択して、**Next** をクリックします。Import Server's Attributes ページが開きます。

ステップ 4　Import Server's Attributes ページに、次の情報を入力します。

- Server Name：ホスト名または IP アドレス。
- Server Display Name : CiscoWorks ホームページに表示されるユーザ指定の名前。Service Monitor インスタンスを選択した場合は、その Service Monitor ホームページのタイトルとしても表示されます。
- Port：1741

ステップ 5　**Next** をクリックします。CiscoWorks は、リモート サーバが到達可能であることを確認します。

CiscoWorks ホームページで新しい Service Monitor サーバ インスタンスを選択する場合は、リモート ホストのユーザ名とパスワードを入力して認証する必要があります。

SNMP を使用した Service Monitor の監視方法

Service Monitor は、システム アプリケーション MIB をサポートします。このサポートにより、サードパーティの SNMP 管理ツールを使用して Service Monitor を監視できます。したがって、次のことを実行できます。

- 複数のプラットフォームの一環した監視 : Service Monitor が常駐する 1 つのプラットフォーム、および CiscoWorks IP Communications Management Suite のアプリケーションが常駐する 1 つ以上のプラットフォーム
- システム アプリケーション MIB を使用したアプリケーション ヘルスの評価。次の情報が提供されます。
  - Service Monitor によってインストールされたアプリケーション
  - アプリケーションに関連付けられたプロセスと現在のプロセス ステータス
  - 以前に実行されたプロセスおよびアプリケーションの終了状態

MIB 実装の詳細と MIB ウォークのサンプルについては、付録 C「Service Monitor の SNMP MIB サポート」を参照してください。

（注）　MIB サポートはアンインストールできません。ただし、Windows SNMP サービスを停止して、起動タイプを Manual または Disabled に設定できます。P.2-12 の「Windows SNMP サービスのイネーブル化およびディセーブル化」を参照してください。

システムを SNMP クエリー対応に設定

SNMP クエリーをイネーブルにするには、SNMP サービスをインストールして、イネーブルにする必要があります。

ステップ 1　Service Monitor がインストールされているサーバに SNMP サービスがインストールされ、イネーブルになっていることを確認します。P.2-11 の「Windows SNMP サービスのステータスの判別」を参照してください。

ステップ 2　SNMP サービスがインストールされていないと判断された場合は、Windows SNMP サービスをインストールします。P.2-12 の「Windows SNMP サービスのインストールおよびアンインストール」を参照してください。

Windows SNMP サービスのステータスの判別

Windows SNMP サービスは、必要に応じて追加または削除できる Windows コンポーネントです。Service Monitor がサポートする MIB に対して SNMP クエリーをイネーブルにするには、SNMP サービスをインストールし、イネーブルにする必要があります。Windows SNMP サービスのステータスを確認するには、次の手順に従います。

ステップ 1　Windows 管理ツールの Services ウィンドウを開きます。

ステップ 2　次を確認します。

- SNMP サービスが Windows 管理ツールの Services ウィンドウに表示されているかどうか。表示されている場合は、Windows SNMP サービスがインストールされています。

（注）　Windows SNMP サービスをインストールするには、P.2-12 の「Windows SNMP サービスのインストールおよびアンインストール」を参照してください。

- SNMP サービスの起動タイプが Automatic か Manual であるかどうか。Automatic の場合、Windows SNMP サービスはイネーブルです。

（注）　Windows SNMP サービスをイネーブルにするには、P.2-12 の「Windows SNMP サービスのイネーブル化およびディセーブル化」を参照してください。

Windows SNMP サービスのインストールおよびアンインストール

Windows オンライン ヘルプに、Windows SNMP サービスなどの Windows コンポーネントを追加および削除する手順が記載されています。手順を検索するには、Windows オンライン ヘルプの Index タブを選択し、*SNMP サービスのインストール* などのキーワードまたは句を入力します。

Windows SNMP サービスをアンインストールするには、Windows コンポーネントの削除に関する Windows ヘルプの指示に従います。

Windows SNMP サービスのイネーブル化およびディセーブル化

Windows SNMP サービスをイネーブルまたはディセーブルにするには、Windows 管理ツールの Services を使用します。Services ウィンドウを開く手順については、Windows オンライン ヘルプを参照してください。

ステップ 1　Services ウィンドウで SNMP サービスを見つけます。ステータスと起動タイプが表示されます。

（注）　SNMP サービスが表示されていない場合、Windows SNMP サービスはインストールされていません。P.2-12 の「Windows SNMP サービスのインストールおよびアンインストール」を参照してください。

ステップ 2　SNMP サービスを右クリックして、Properties を選択します。SNMP Service Properties ウィンドウが開きます。

- SNMP サービスをディセーブルにするには、Startup Type を Disable に設定して、**OK** をクリックします。
- SNMP サービスをイネーブルにするには、Startup Type を Automatic または Manual に設定して、**OK** をクリックします。

（注）　SNMP サービスをイネーブルにした後で起動するには、SNMP サービスを右クリックして Start を選択します。

セキュリティを SNMP クエリー対応に設定

セキュリティを強化するには、SNMP set 操作をすべてのオブジェクト ID（OID）で拒否します。また、デフォルトまたは既知のコミュニティ ストリングを使用しないように SNMP サービスのクレデンシャルを変更する必要があります。

（注）　この目的でクレデンシャルを変更するために、SNMP サービスを再起動する必要はありません。

SNMP サービスのクレデンシャルは、Windows 管理ツールの Services を使用して変更できます。

ステップ 1　Services ウィンドウで SNMP サービスを見つけます。

ステップ 2　SNMP サービスを右クリックして、Properties を選択します。SNMP Service Properties ウィンドウが表示されます。

ステップ 3　Security タブを選択します。

ステップ 4　受け入れたコミュニティ名を編集して、**OK** をクリックします。

システム アプリケーション MIB ログ ファイルの表示

システム アプリケーション MIB ログ ファイルの SysAppl.log は、Service Monitor がインストールされているサーバの *NMSROOT*\log にあります。

（注）　NMSROOT は、システム上の CiscoWorks がインストールされているディレクトリです。インストール時にデフォルト ディレクトリを選択した場合は、C:\Program Files\CSCOpx です。

Service Monitor サーバのホスト名の変更

Service Monitor サーバのホスト名を変更するには、いくつかのファイルをアップデートし、サーバをリブートして、自己署名セキュリティ証明書を再生成する必要があります。その後、Service Monitor 上のコンフィギュレーションをアップデートする必要があります。

ホスト名の変更、サーバのリブート、および証明書の再生成

（注）　この手順の間にサーバを 2 回リブートします。また、一部の手順を実行するために、CiscoWorks デーモン マネージャと syslog マネージャを停止します。

ステップ 1　次のように、サーバ上のホスト名を変更します。

a. 次のコマンドを入力して、CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgtd
```

b. **My Computer > Properties > Computer Name > Change** を選択し、ホスト名を変更します。

c. リブート後、デーモン マネージャ サービスと syslog マネージャ サービスが再開しないように設定します。Control panel または Start から Services ウィンドウを開いて、次の両方のサービスの起動モードを Manual に変更します。

- CW2000 Daemon Manager
- CWCS syslog サービス

d. サーバをリブートします。

ステップ 2　md.properties ファイル（*NMSROOT*\lib\classpath\md.properties）内のホスト名を変更します。

（注）　NMSROOT は、Service Monitor をインストールしたディレクトリです。デフォルト ディレクトリを選択した場合は、C:\Program Files\CSCOpx です。

ステップ 3　次のレジストリ エントリのホスト名を変更します。

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
- HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager

（注）　これらのレジストリ エントリの下で旧ホスト名のインスタンスをすべて検索し、それらを新規ホスト名に置き換えます。

ステップ 4　次のファイル内のホスト名を変更します。

- regdaemon.xml (*NMSROOT*\MDC\etc\regdaemon.xml):
  - 旧ホスト名をメモします。ステップ 5 を完了するためにこのホスト名が必要です。
  - 新規ホスト名は大文字で入力します。
- web.xml（*NMSROOT*\MDC\tomcat\webapps\classic\WEB-INF\web.xml）

ステップ 5　ファイル *NMSROOT*\conf\cmic\changehostname.info を作成します。このファイルには、旧ホスト名と新規ホスト名が大文字で次の形式で含まれます。

```
OLDHOSTNAME:NEWHOSTNAME
```

（注）　このファイル内のホスト名は大文字小文字を区別します。大文字で入力する必要があります。新規ホスト名は、regdaemon.xml に入力したホスト名と正確に一致している必要があります。

ステップ 6　次のディレクトリから gatekeeper.ior ファイルを削除します。

NMSROOT\www\classpath

ステップ 7　サーバに Service Monitor だけがインストールされている場合は、ステップ 8 に進みます。Service Monitor が Operations Manager と同じサーバにインストールされている場合は、次のファイルに出現するすべての旧ホスト名を変更します。

- *NMSROOT*\objects\vhmsmarts\local\conf\runcmd_env.sh
- *NMSROOT*\conf\dfm\Broker.info

ステップ 8　cmf データベースのパスワードが不明の場合は、次のようにパスワードをリセットします。

a.　コマンド プロンプトを開いて、NMSROOT\bin に移動します。

b.　次のコマンドを入力します。

```
perl dbpasswd.pl dsn=cmf npwd=newpassword
```

ここで、newpassword は新規パスワードです。

（注）　このパスワードを覚えておいてください。ステップ 9 を完了するために必要です。

ステップ 9　ホスト名を変更する前に追加されたデバイスが Device Center で適切に分類されていることを確認するため、次のコマンドを入力します。

```
dbisqlc -c
"uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dsn=cmf;dbf=NMSROOT\databases\cmf\cmf.db" -q
update PIDM_app_device_map SET app_hostname=`NewhostName' where
app_hostname=`OldhostName'
```

それぞれの説明は次のとおりです。

- dbpassword は Common Services のデータベース パスワードです。
- NMSROOT は、Service Monitor をインストールしたディレクトリです。
- NewhostName は、新規ホスト名です。
- OldhostName は、旧ホスト名です。

ステップ 10 Control panel または Start から Services ウィンドウを開いて、次の両方のサービスの起動モードを Automatic に変更します。

- CW2000 Daemon Manager
- CWCS syslog サービス

ステップ 11 サーバをリブートします。

ステップ 12 自己署名セキュリティ証明書内の旧ホスト名を新規ホスト名に置き換え、証明書を再生成します。

a. **Common Services > Server > Security > Certificate Setup** を選択します。

b. 詳細については、Help をクリックしてください。

ステップ 13 Service Monitor を再設定します。P.2-16 の「ホスト名を変更後の Service Monitor の再設定」を参照してください。

ホスト名を変更後の Service Monitor の再設定

P.2-14 の「ホスト名の変更、サーバのリブート、および証明書の再生成」の手順を完了後、次の手順を完了する必要があります。

ステップ 1 次の各コンフィギュレーション ファイル内の IP アドレスまたはホスト名を変更します。

- デフォルトのコンフィギュレーションファイル：P.1-13 の「デフォルト設定の編集（自動登録）」を参照してください。
- Service Monitor によって管理される各 Cisco 1040 固有のコンフィギュレーション ファイル：P.1-11 の「特定の Cisco 1040 の設定の編集」を参照してください。

ステップ 2 Service Monitor サーバから TFTP サーバに、アップデートしたコンフィギュレーション ファイルをコピーします。P.1-5 の「TFTP サーバへのイメージ ファイルおよびコンフィギュレーション ファイルのコピー」を参照してください。

ステップ 3 Cisco 1040 をリセットします。P.1-14 の「Cisco 1040 のリセット」を参照してください。

ステップ 4 Operations Manager にトラップを送信するように Service Monitor が設定されている場合は、次を実行します。

- Operations Manager が Service Monitor と同じサーバにインストールされている場合は、新規ホスト名または IP アドレスにトラップを送信するように Service Monitor をセットアップします。P.1-3 の「Service Monitor のセットアップ」を参照してください。
- Operations Manager が別のサーバにインストールされている場合は、Operations Manager 上で Service Monitor を削除して再度追加します。詳細については、Operations Manager のオンラインヘルプを参照してください。