



システム管理およびデータ管理

ここでは、次の内容について説明します。

- 「Service Monitor データベースの管理」 (P.6-1)
- 「センサー アrchive ファイルの消去について」 (P.6-5)
- 「ログ ファイルの管理」 (P.6-5)
- 「E メール通知のイネーブル化」 (P.6-7)
- 「E メールがブロックされていないことの確認」 (P.6-8)
- 「CWCS TFTP サービスのディセーブル化」 (P.6-9)
- 「Service Monitor プロセスの起動および停止」 (P.6-9)
- 「SNMP を使用した Service Monitor のモニタ方法」 (P.6-10)
- 「Service Monitor サーバの設定」 (P.6-12)



(注)

セキュリティおよびユーザの設定については、『*Installation Guide for Cisco Unified Service Monitor 8.5*』を参照してください。

Service Monitor データベースの管理

Cisco Unified Service Monitor (Service Monitor) は、次のソースからコール メトリックを受信して処理し、データベースに格納します。

- Service Monitor に登録されている Cisco 1040。
- Service Monitor データベースへのアクセス、または Service Monitor へのデータ送信ができるように設定されている、Unified Communications Manager クラスター。詳細については、「[Unified Communications Manager の設定](#)」 (P.B-1) を参照してください。

Service Monitor はデータを設定可能な日数の間保存し、古いデータをデータベースから消去するジョブを毎日実行します。Service Monitor データベースに保持される日数を確認するには、「[その他の設定項目の設定と表示](#)」 (P.3-34) を参照してください。データの消去スケジュールを更新するには、「[低ボリューム スケジュールおよびデータ消去の設定](#)」 (P.6-2) を参照してください。

詳細については、次の項を参照してください。

- 「[データベースのバックアップおよび復元](#)」 (P.6-3)
- 「[Service Monitor データベースのパスワードの変更](#)」 (P.6-5)

低ボリューム スケジュールおよびデータ消去の設定

低ボリューム スケジュール時、Service Monitor はピーク時の処理量のおよそ 20% のレコード数を処理し、データベースのメンテナンスを実行します。表 6-1 に、低ボリューム処理およびデータベース消去のデフォルト スケジュール、およびスケジュールの更新に必要な情報を示します

表 6-1 Service Monitor システムのスケジュールリング

アクティビティ	日次スケジュール	注意事項と設定可能なプロパティ
データベースのメンテナンス（低ボリューム スケジュール）	午後 10 時～午前 6 時 (デフォルト)	<p>Service Monitor は、1 日のうち 8 時間の低ボリューム期間が必要であり、午前 0 時～午前 1 時は低ボリューム期間としてスケジュールされている必要があります。スケジュールを変更するには、Service Monitor サーバで <code>NMSROOT\qovr\qovrconfig.properties</code> ファイルの次のプロパティの値を変更します。</p> <pre>lowcallvolume-Mon=0-6,22-24 lowcallvolume-Tue=0-6,22-24 lowcallvolume-Wed=0-6,22-24 lowcallvolume-Thu=0-6,22-24 lowcallvolume-Fri=0-6,22-24 lowcallvolume-Sat=0-20,22-24 lowcallvolume-Sun=0-20,22-24</pre> <p>(注) NMSROOT は、Service Monitor がインストールされている場所です。フォルトの場所を使用した場合は、<code>C:\Program Files\CSCOPx</code> です。</p> <p>次の条件を満たす場合、複数の低ボリューム期間を設定することができます。</p> <ul style="list-style-type: none"> 午前 0 時～午前 1 時を低ボリューム期間にする。 低ボリューム期間を、1 日あたりの合計で 8 時間以上に設定する。 <p>次に例を示します。</p> <pre>lowcallvolume-Mon=0-1,4-6,7-8,17-18,19-23 lowcallvolume-Tue=0-6,21-22,23-24</pre> <p><code>qovrconfig.properties</code> を編集した後で変更を有効にするには、QOVR プロセスを停止してから開始する必要があります。Service Monitor がインストールされているサーバにログインしている状態で、コマンドラインから次のコマンドを入力します。</p> <pre>pdterm QOVR pdexec QOVR</pre>

表 6-1 Service Monitor システムのスケジューリング (続き)

アクティビティ	日次スケジュール	注意事項と設定可能なプロパティ
データ消去	午前 2 時～午前 6 時 (デフォルト)	<p>Service Monitor は、4 時間のデータ消去期間が必要です。データ消去は、低ボリューム スケジュール時に行う必要があります。かつ午前 0 時～午前 1 時は実行してはいけません。スケジュールを変更するには、Service Monitor サーバで <code>NMSROOT\qovr\qovrconfig.properties</code> ファイルの次のプロパティ値を変更します。</p> <pre>datapurge-Mon=2-6; datapurge-Tue=2-6; datapurge-Wed=2-6; datapurge-Thu=2-6; datapurge-Fri=2-6; datapurge-Sat=2-6; datapurge-Sun=2-6;</pre> <p>データ消去は、4 時間連続して実行する必要はありません。次の条件を満たす限り、複数のデータ消去期間を設定できます。</p> <ul style="list-style-type: none"> 合計時間が 4 時間である。 データ消去は低ボリューム スケジュールに発生する。 午前 0 時～午前 1 時はデータ消去が発生しない。 <p>次に例を示します。</p> <pre>datapurge-Mon=2-5;22-23; datapurge-Tue=2-3;4-6;23-24</pre> <p><code>qovrconfig.properties</code> を編集した後で変更を有効にするには、QOVR プロセスを停止してから開始する必要があります。Service Monitor がインストールされているサーバにログインしている状態で、コマンドラインから次のコマンドを入力します。</p> <pre>pdterm QOVR pdexec QOVR</pre>
重要なシステム操作	午前 0 時～午前 1 時 (変更できません)	この時間帯は、データ消去を実行しないでください。



(注)

`qovrconfig.properties` ファイルには、この他にも設定可能なプロパティがあります。デフォルト値を表示するには、「その他の設定項目の設定と表示」(P.3-34) を参照してください。その他の設定については、「診断レポート検索と CSV エクスポート制限の設定」(P.3-36) を参照してください。

データベースのバックアップおよび復元

Service Monitor が Operations Manager とともにサーバにインストールされている場合、Operations Manager のマニュアルに記述されたバックアップおよび復元の手順を使用します。

Service Monitor をスタンドアロンでインストールする場合、データベースに 25 GB があらかじめ割り当てられます。Common Services によるバックアップ手順を使用した場合、バックアップが完了する前にタイムアウトが発生します。代わりに、次の手順を使用します。

- 「データベースのバックアップ」(P.6-4)
- 「データベースの復元」(P.6-4)

データベースのバックアップ



(注) この手順の実行中は、すべての Service Monitor プロセスを停止します。

ステップ 1 Service Monitor がインストールされているシステムにログインします。

ステップ 2 次のコマンドを使用して、CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgttd
```

ステップ 3 *NMSROOT*\databases\qovr から、ファイル *qovr.db* および *qovrx.log* をテープ、外付けドライブ、ネットワーク ディレクトリ（ローカル ディレクトリでなく）にコピーします。そうすることで、ハードウェア障害時のデータ整合性が確保され、バックアップ データによってローカル ディスク領域が消費されないようになります。

ステップ 4 次のコマンドを使用して、CiscoWorks デーモン マネージャを再起動します。

```
net start crmdmgttd
```



(注) センサー アーカイブ ファイルのコピーを保存するには、「[センサー アーカイブ ファイルの消去について](#)」(P.6-5) を参照してください。

データベースの復元

この手順の実行中は、すべての Service Monitor プロセスを停止します。

ステップ 1 Service Monitor がインストールされているシステムにログインします。

ステップ 2 次のコマンドを使用して、CiscoWorks デーモン マネージャを停止します。

```
net stop crmdmgttd
```

ステップ 3 *NMSROOT*\databases\qovr ディレクトリから、次のいずれかを実行します。

- 現在のデータベースのコピーを保持するには、ファイル *qovr.db* および *qovrx.log* を *NMSROOT* の外部に移動します（ハードウェア障害時のデータ整合性を確保したり、ローカル ドライブの領域不足を防止したりするために、テープ、外付けドライブ、またはネットワーク ドライブを推奨します）。
- qovr.db* および *qovr.log* を削除します。

ステップ 4 データベース ファイル *qovr.db* および *qovrx.log* を保存したテープ、外付けドライブ、またはネットワーク ドライブから *NMSROOT*\databases\qovr にコピーします。

ステップ 5 次のコマンドを使用して、CiscoWorks デーモン マネージャを再起動します。

```
net start crmdmgttd
```



(注) データベースを復元すると、ロギング設定がデフォルト値に戻ります。そのため、ログ ファイルに書き込まれるのはエラー メッセージだけになります。問題のデバッグのために、その他の情報もログ ファイルに書き込む必要がある場合は、ロギング設定を再設定します。「[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](#)」(P.6-6) を参照してください。

Service Monitor データベースのパスワードの変更

コマンドライン スクリプトを使用すると、データベースのパスワード (Service Monitor データベースのパスワード `qovr.db` を含む) を変更できます。手順は Common Services のオンライン ヘルプで参照できます。



(注) Common Services のオンラインヘルプは、[Administration] タブにある、[Common Services] ページを使用することでのみ利用できます。

Common Services のオンライン ヘルプにアクセスするには、次の手順を使用します。

1. [Administration] > [Server Administration (Common Services)] > [Security] を選択します。
[Setting up Security] ページが表示されます。
2. [Help] をクリックします。オンライン ヘルプが表示されます。

-
- ステップ 1** Common Services オンライン ヘルプを表示します。
- ステップ 2** [Index] を選択します。
- ステップ 3** 表示された [search] フィールドに、*database password* と入力します。
-

センサー アーカイブ ファイルの消去について

オプションで、Service Monitor はセンサー コール メトリック データをサーバ上のディレクトリ内のファイルにアーカイブします。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、「[Cisco 1040 センサーのデフォルト設定の設定](#)」(P.4-3) を参照してください。

アーカイブがイネーブルの場合 (デフォルト)、Service Monitor は次を実行します。

- 毎日午前 0 時に新しいデータ ファイルを作成する。
- 現在のデータ ファイルのサイズが 3 MB を超えると、新しいデータ ファイルを作成する。データ ファイルがこのサイズに達すると、Service Monitor は次を実行します。
 - データ ファイルをバックアップする。ファイル形式の末尾に *.n* が追加されます。たとえば、*.csv.1*、*.csv.2* のように、1 日最大 50 まで追加されます。
 - 新しいデータ ファイルを作成する。元のファイル形式 (*.csv*) が保持されます。
- データ ファイルを 30 日間保存した後、削除する。データ ファイルを 30 日より長く保存する場合は、ファイル システムのバックアップと同じ方法で Service Monitor データ ファイルをバックアップできます

ログ ファイルの管理

ここで説明する内容は、次のとおりです。

- 「[Cisco 1040 センサーの Syslog の処理について](#)」(P.6-6)
- 「[Cisco 1040 センサーの履歴ログ ファイルの管理](#)」(P.6-6)
- 「[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](#)」(P.6-6)

Cisco 1040 センサーの Syslog の処理について

Service Monitor は、Cisco 1040 から syslog メッセージを受信して処理します。Service Monitor は、syslog メッセージを処理したら、これらを syslog ファイル `syslog.log` (`NMSROOT\log\qovr` にある) に書き込みます。

Cisco 1040 センサーの履歴ログ 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 イベントの記録が含まれます。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) Service Monitor 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



(注) シスコからの指示がない限り、[Debug All] ボタンはクリックしないでください。

この情報は、トラブルシューティング目的で提供されます。Service Monitor ログ ファイルは、`NMSROOT\log\qovr` ディレクトリにあります。



(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 [Administration] > [System Settings] > [Logging] を選択します。[Logging: Level Configuration] ページが表示されます。

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す。オフにはできません。



(注) ログギングはディセーブルできません。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。

次の表で説明するように、適切なログレベルを設定します。

ロギング レベルの処置	手順
個々のモジュールのログレベルを変更する	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p> (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。</p> <p>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。</p>
すべてのモジュールを、デフォルトである Error に設定する	<p>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。</p> <p>b. [OK] をクリックします。Service Monitor は、ただちにログレベルを Error に設定し始めます。</p>
すべてのモジュールを Debug に設定する	<p>[Debug All] ボタンをクリックします。Service Monitor は、ただちにログレベルを Debug に設定し始めます。</p> <p>(注) デバッグが完了したら、ロギングをデフォルト レベルに戻すことを忘れないでください。</p>

E メール通知のイネーブル化

Service Monitor で E メール通知を送信できるようにするには、SMTP サーバと E メールを受信するユーザを設定する必要があります。

- 「E メール通知の SMTP サーバの設定」 (P.6-8)
- 「E メール通知の受信者の設定」 (P.6-8)

Service Monitor は、次の状況で E メール通知を送信します。

- Service Monitor が問題に反応してサーバプロセスの再起動を開始した。Service Monitor は、E メールを送信して、再起動が発生したことを通知し、考えられる原因を示します
(Service Monitor は、ユーザが開始したサーバプロセスの再起動について E メールを送信しません。Service Monitor は、ユーザが次のいずれかを実行したときに通知しません。
 - デーモン マネージャを停止および開始する。
 - qovr プロセスを停止および開始する。
 - コンピュータをリブートする)。

E メールがブロックされていないことの確認

- Service Monitor サーバプロセスの開始時に、データ クレデンシャルの確認に失敗した。
ユーザが開始した再起動か Service Monitor が開始した再起動かにかかわらず、Service Monitor サーバ プロセスが起動するたびに、Service Monitor はクレデンシャルの確認を実行します。起動時にクレデンシャルの確認に失敗した場合、Service Monitor は、失敗したこと、および Service Monitor との接続を失ったデータ ソースの IP アドレスを通知する E メールを送信します。



(注) Service Monitor は、サーバ プロセスの起動時のみこの通知を送信します。

E メール通知の SMTP サーバの設定



(注) SMTP サーバがまだ設定されていない場合、Service Monitor は [データ ソース クレデンシャル ページ](#) のメッセージを表示します。

Service Monitor が使用する SMTP サーバを設定するには、次の手順を実行します。

- [Administration] > [Configuration] > [Export Settings] を選択します。
- [SMTP Server] フィールドに SMTP サーバを入力します (通知の受信者を設定するには、[E-mail to] フィールドに E メール アドレスを入力します)。

E メール通知の受信者の設定

この手順を使用して受信者を設定しない場合、Service Monitor は [Export Settings] ページの [E-Mail to] フィールドに設定されたアドレスに E メール通知を送信します。[Export Settings] ページの [E-Mail to] フィールドが空白で、この手順を使用して受信者を設定しない場合、Service Monitor は通知を送信しません。

ステップ 1 Service Monitor サーバに Windows 管理者としてログインします。

ステップ 2 NMSROOT\qovr ディレクトリに移動します。次に例を示します。

```
C:\Program Files\CSCOpX\qovr
```



(注) NMSROOT は Service Monitor をインストールしたディレクトリ。デフォルトの場所は C:\Program Files\CSCOpX です。

ステップ 3 qovrconfig.properties ファイルを編集します。

ステップ 4 SMDBMonitor_Email の値を入力します。次に例を示します。

```
SMDBMonitor_Email=johnsmith@xyz.com
```

E メールがブロックされていないことの確認

デフォルトの SMTP サーバでウイルス対策アプリケーションを使用している場合は、ポートブロッキングルールで通知 Eメールの送信を停止していないことを確認します。一部のウイルス対策アプリケーションでは、大量にメールを送信するワームをブロックするためにポートブロッキングを使用しています。必要に応じてポートブロッキングルールを削除します。Service Monitor では、SMTP にポート 25 を使用します。

CWCS TFTP サービスのディセーブル化

CWCS TFTP サービスは、Service Monitor サーバ上で実行され、リモート ホストから利用して Service Monitor サーバ上のファイルを読み取ることができます。Service Monitor では CWCS TFTP サービスを使用しないため、ディセーブルにすることを推奨します。

-
- ステップ 1** 管理者として、Service Monitor がインストールされている Windows サーバにログインします。
- ステップ 2** [Services] ウィンドウを開きます。
- ステップ 3** エントリ [CWCS tftp service] を探して右クリックし、[Properties] を選択します。
- ステップ 4** [Properties] ウィンドウで、次の手順を実行します。
- a. [Startup type] を [Disabled] に設定します。
 - b. [Stop] ボタンをクリックします。
 - c. サービスが停止したら、[OK] をクリックします。
-

Service Monitor プロセスの起動および停止

-
- ステップ 1** [Administration] > [Server Administration (Common Services)] > [Administration] > [Process Management] を選択します。[Process Management] ページが表示されます。
- ステップ 2** 開始または停止するサービスの隣にあるチェックボックスを選択します。
- ステップ 3** [Start] または [Stop] をチェックします。

表 6-2 に、Service Monitor 関連のプロセスの一覧を示します。

表 6-2 Service Monitor 関連のプロセス

名前	説明	依存関係
QOVR	Service Monitor サーバ	—
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	—
SSHD	Service Monitor SFTP サーバ	—

表 6-3 に、Service Monitor サーバ上で実行される Common Services プロセスの一部を Windows の [Services] での表記で示します。

表 6-3 Common Services 関連のプロセス

Service Monitor および Operations Manager が同時にインストールされている場合のプロセス名	Service Monitor が単独でインストールされている場合の同等のプロセス名
CW2000 Daemon Manager	Service Monitor Daemon Manager
CW2000 Tomcat Servlet Engine	Service Monitor Tomcat Servlet Engine
CW2000 VisiBroker Smart Agent	Service Monitor VisiBroker Smart Agent
CW2000 Web Server	Service Monitor Web Server

SNMP を使用した Service Monitor のモニタ方法

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 をモニタできます。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貫したモニタ：Service Monitor が常駐する 1 つのプラットフォーム、および Cisco Unified 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 E 「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。[「Windows SNMP サービスのイネーブル化およびディセーブル化」\(P.6-11\)](#) 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。[「Windows SNMP サービスのステータスの判別」\(P.6-11\)](#) 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。[「Windows SNMP サービスのインストールおよびアンインストール」\(P.6-11\)](#) 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、「[Windows SNMP サービスのインストールおよびアンインストール](#)」(P.6-11) 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、「[Windows SNMP サービスのイネーブル化およびディセーブル化](#)」(P.6-11) 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、「*installing SNMP service*」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。「[Windows SNMP サービスのインストールおよびアンインストール](#)」(P.6-11) を参照してください。

ステップ 2 [SNMP Service] 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 Service] 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 Service] を見つけます。
- ステップ 2** [SNMP Service] 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 Service Monitor 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 サーバの設定

このトピックで説明する内容は、次のとおりです。

- 「Service Monitor サーバのホスト名の変更」(P.6-13)
- 「Service Monitor サーバの IP アドレスの変更」(P.6-15)
- 「Service Monitor サーバの時刻の変更」(P.6-15)

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。いくつかの手順を実行するため、デーモン マネージャも停止します。

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 crmdmgt
```

- 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、CW2000 デーモン マネージャ サービスの起動モードを [Manual] に変更します。
 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。デフォルトの場所は 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 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 7](#)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 7 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。

- コマンドプロンプトを開いて、`NMSROOT\bin` に移動します。
- 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 8](#)を完了するために必要です。

ステップ 8 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`
```

このコマンドで

- 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 9 [Control Panel] または [Start] から [Services] ウィンドウを開いて、CW2000 デーモン マネージャ サービスの起動モードを [Automatic] に変更します。

ステップ 10 サーバをリブートします。

ステップ 11 [Administration] > [Server Administration (Common Services)] > [Security] > [Certificate Setup] を選択し、自己署名セキュリティ証明書内の古いホスト名を新しいホスト名に置き換え、自己署名セキュリティ証明書を再生成します。

ステップ 12 Service Monitor を再設定します。「[ホスト名を変更後の Service Monitor の再設定](#)」(P.6-14) を参照してください。

ホスト名を変更後の Service Monitor の再設定

「[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](#)」(P.6-13) 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** 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。
「Cisco 1040 センサーのデフォルト設定の設定」(P.4-3) 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。
- ステップ 2** システムで Cisco 1040 センサーを使用している場合は、次の手順を実行します。
- a. 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: 「Cisco 1040 センサーのデフォルト設定の設定」(P.4-3) 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: 「Cisco 1040 のコンフィギュレーション ファイルの編集」(P.4-9) を参照してください。
 - b. Cisco 1040 をリセットします。「Cisco 1040 のリセット」(P.4-11) を参照してください。
- ステップ 3** Service Monitor で Unified Communications Manager バージョン 5.x 以降をモニタしている場合、アプリケーション ビリング サーバとして設定されている Service Monitor の IP アドレスをアップデートします。詳細については、「ビリング サーバとしての Service Monitor の Unified Communications Manager 5.x 以降への追加」(P.B-4) を参照してください (Service Monitor でサポートする Unified Communications Manager ソフトウェアのバージョンについては、「サポートされているデータ ソース ソフトウェア バージョン」(P.3-7) を参照してください)。

Service Monitor サーバの IP アドレスの変更

- ステップ 1** 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 crmdmgt
```
- ステップ 2** Service Monitor サーバの IP アドレスを変更します。
- ステップ 3** ステップ 1 を実行してから 15 分経過したら、次のコマンドを入力して、デーモン マネージャを再開します。
- ```
net start crmdmgt
```
- ステップ 4** Service Monitor を再設定します。「ホスト名を変更後の Service Monitor の再設定」(P.6-14) を参照してください。

Service Monitor サーバの時刻の変更

Service Monitor がインストールされているサーバの時刻を変更したら、デーモン マネージャを停止および起動します。コマンドラインから次のコマンドを実行します。

```
net stop crmdmgt
net start crmdmgt
```



(注) Service Monitor は Cisco 1040 に 1 時間に 1 回時刻を送信します。それを受けて、Cisco 1040 は必要に応じて時計をアップデートします。Service Monitor サーバで時刻が変更されたらただちに Cisco 1040 を同期するには、Cisco 1040 をリセットします。「Cisco 1040 のリセット」(P.4-11) を参照してください。

インストールされている Service Monitor のビルド ID の確認

時々トラブルシューティングのために、インストールされている Service Monitor のビルドを確認する必要があります。ビルド ID は、次の方法で確認できます。

1. [Administration] > [Software Center (Common Services)] > [Software Update] を選択します。新しいウィンドウが開きます。
2. [Products Installed] で該当するリンク ([Cisco Unified Service Monitor *n.n*]、*n.n* はソフトウェアリリースバージョン) をクリックします。新しいウィンドウが開きます。
3. ページの上部にある「Build Id」と表記された値を確認します (例: Build Id: NT_SM2_2_20090925_1028)。



(注) NT_SM2_2_20090925_1028 は、ビルド ID の形式を例示したものです。