インストール後のサーバ タスク

次のトピックは、Security Manager またはその関連アプリケーションをサーバ上にインストールしてから実行すべきタスクです。

すぐに実行すべきサーバ タスク

インストール直後に次のタスクを実行してください。

✓	タスク
❑	**1. アンチウイルス スキャナと同等の製品を再イネーブルまたは再インストールします。**アンチウイルス ツールなどのサーバ セキュリティ ソフトウェアをアンインストールまたは一時的にディセーブルにした場合は、今すぐ、そのソフトウェアを再インストールまたは再起動して、必要に応じてサーバを再起動します。 **（注）** アンチウイルス ソフトウェアが原因で Security Manager サーバの効率性や応答性が損なわれていることが判明した場合は、アンチウイルス ソフトウェアのマニュアルで推奨設定を確認してください。
❑	**2. インストール中にディセーブルにしたサービスとサーバ プロセスを再イネーブルします。**IIS は再イネーブルしないでください。
❑	**3. Sybase テクノロジーやソフトウェア コードを使用しているアプリケーションも含めて、インストール中にディセーブルにした基幹業務アプリケーションを再イネーブルします。**
❑	**4. サーバ上で、自己署名証明書を信頼できる証明書のリストに追加します。**手順については、ブラウザのマニュアルを参照してください。
❑	**5. Cisco.com 上で Security Manager とその関連アプリケーションのアップデートをチェックします。**アップデートが入手可能なことがわかった場合は、組織やネットワークに関連するアップデートをインストールします。

必要なプロセスが動作しているかどうかの確認

Windows のコマンド プロンプト ウィンドウから **pdshow** コマンドを実行して、インストールする Cisco サーバ アプリケーションに必要なプロセスのすべてが正しく動作していることを確認できます。プロセス要件はアプリケーションによって異なります。

ヒント　**pdshow** の詳細については、Common Services のマニュアルを参照してください。

表 7-1 を使用して、どのアプリケーションにどのプロセスが必要かを確認してください。

表 7-1　アプリケーション プロセス要件

アプリケーション	必要な Daemon Manager プロセス
Common Services	Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSRegistryServer DCRServer diskWatcher EDS EDS-GCF ESS EssMonitor jrm LicenseServer Proxy Tomcat TomcatMonitor NameServer NameServiceMonitor EventFramework
Cisco Security Manager	AthenaOGSServer ccrWrapper CsmReportServer rptDbEngine rptDbMonitor VmsBackendServer vmsDbEngine vmsDbMonitor VmsEventServer CsmHPMServer
Auto Update Server	AusDbEngine AusDbMonitor

MRF を使用した Security Manager プロセスのヒープ サイズの設定

Security Manager 4.1 で導入された機能である Memory Reservation Framework（MRF）は、Cisco Security Manager 管理者に、主要プロセスのヒープ サイズを変更する機能を提供します。それにより、サーバのパフォーマンスを向上させることができます。MRF を使用すると、プロセスは、サーバに搭載された RAM の容量に基づいてヒープ サイズを調整できるようになります。

MRF を使用して設定可能な Security Manager プロセスを表 7-2 に示します。

表 7-2　MRF を使用して設定可能な Security Manager プロセス [1]

プロセス	pdshow で表示される名前[2]	説明
バックエンド プロセス	VmsBackendServer	デバイス検出操作と展開操作を実行します。
Tomcat	Tomcat	ポリシーなどの編集および検証を行うためのアプリケーションをホストします。
レポート サーバ	CsmReportServer	レポート データを生成します。
イベント サーバ	VmsEventServer	デバイスから送信されているイベントを収集します。

1. HPM（Health and Performance Monitor）サーバの MRF 設定はありません。
2. pdshow コマンドの詳細については、前述の必要なプロセスが動作しているかどうかの確認および Common Services のマニュアルを参照してください。

デフォルト コンフィギュレーション

表 7-3 に示されているプロセス（MRF を使用して設定可能な Security Manager プロセス）は、ヒープ サイズに対してデフォルト値が事前に設定されています。表 7-3 には、MRF を使用して設定可能な Security Manager プロセスごとに、サーバで使用可能なさまざまな RAM 容量に応じたデフォルトの最小および最大ヒープ サイズが MB 単位で示されています。

表 7-3　Security Manager プロセスに対して事前に設定されるデフォルトのヒープ サイズ

サーバ上の物理 RAM（GB）	VmsBackendServer	Tomcat	CsmReportServer	VmsEventServer	CsmHPMServer
< 8	1024、2048	512、1024	512、1024	1024、2048	512、1024
8	1024、3072	1024、2048	1024、1024	1024、3072	512、1024
12	2048、4096	2048、3072	1024、1024	2048、4096	512、1024
16	2048、4096	2048、4096	1024、1024	4096、4096	512、1024
24	4096、8192	4096、4096	1024、1024	4096、8192	512、1024
>= 28	8192、8192	4096、4096	1024、1024	4096、8192	512、1024

レポート サーバ（CsmReportServer）に対する最大ヒープ サイズは、必要に応じて 1408 MB まで増やすことができます。

一定量の RAM がオペレーティング システム用とその他のプロセス用に予約されていますが、この表には示されていません。たとえば、表 7-3 の RAM が 16 GB の場合について考えてみます。4 つすべてのプロセスに対する最大ヒープ サイズの合計は、(4096 + 4096 + 1024 + 4096) = 13312 MB、つまり 13 GB です。残りの 3 GB の RAM がオペレーティング システム用とその他のプロセス用に使用できます。

コンフィギュレーション コマンド

MRF では、1 つのコマンドと一連のサブコマンドが提供され、Security Manager サーバ プロセスのヒープ サイズの読み取りや変更に使用されます。各プロセスの最小および最大ヒープ サイズは、mrf コマンドを使用して設定できます。次のようにこのコマンドを実行すると、このコマンドの使用方法に関する情報が表示されます。

```
> mrf
mrf help
           Prints this message.
mrf backup
           Backup existing configuration
mrf revert
           Restores backed up configuration
mrf set_heap_params process X-Y [min],[max]
           Sets minimum and maximum heap sizes
           process -> process name
           X-Y -> Memory Range in MB to which heap sizes apply
           [min],[max] -> minimum and maximum heap sizes in MB. These are optional but
atleast one should be specified.
mrf get_heap_params process [memory]
           Prints minimum and maximum heap sizes in MB
           process -> process name
           [memory] -> memory size in MB for which heap sizes are to be printed. If not
specified heap sizes are to be printed for current system memory.
```

mrf コマンドを実行する際は、有効なプロセス名のみを使用してください。無効なプロセス名を指定しても、エラーは発生しません。有効なプロセス名は、表 7-2 に示されています。プロセス名は大文字と小文字が区別されます。

プロセスに対するヒープ サイズの設定

Security Manager プロセスに対するヒープ サイズの設定は、次の主要な 3 つの手順で構成されます。

1. 既存の設定の保存
2. 既存の設定の読み取り
3. 設定の変更

1. 既存の設定の保存

プロセスのヒープ サイズの設定は、Security Manager のパフォーマンスに影響する可能性のある重要な手順であるため、アプリケーションの専門家の指示の下でのみ実施することを推奨します。

また、予防措置として、プロセスの既存のメモリ設定を変更する前に、それらを保存しておくことも推奨します。MRF では、2 種類の保存方法が用意されています。

1. 1 つ目の方法は、設定変更をテストする場合に使用できます。この場合、次に示す 2 つのコマンドを使用して、それぞれ、古い設定を保存すること、および新しい変更を古い設定に戻すことができます。

```
mrf backup
mrf revert
```

2. 2 つ目の方法は、新しい設定をしばらく使用した後に、古い値に戻す場合に役立ちます。これには 2 つの方法があり、次のうちのいずれか一方を使用できます。

a. 設定変更を行った後に mrf backup を実行していなければ、mrf revert を実行できます。

b. Cisco Security Manager サーバのバックアップを取ってから、設定変更を行います。変更を元に戻すときは、バックアップを復元します。この場合、バックアップ後に行われたデータの変更は失われます。

2. 既存の設定の読み取り

データの保存が完了しましたので、次のコマンドを使用して、プロセスの既存の値を問い合わせることができます。

mrf get_heap_params *[process name] [memory]*

このコマンドで memory 値を指定しなければ、現在の RAM サイズが使用されます。一般に関心があるのは、現在の RAM サイズに対する情報です。パラメータ *[process name]* は、表 7-2 に示されている値のいずれかになります。プロセス名は大文字と小文字が区別されます。

このコマンドの出力は、次のように表示されます。値の単位は MB です。

```
Minimum Heap Size = 1024
Maximum Heap Size = 2048
```

3. 設定の変更

現在の設定を確認した後、この項に記載された説明に従って設定を変更することができます。

ヒープ サイズを設定するには、次のコマンドを使用します。

mrf set_heap_params *[process name] [X-Y] [min],[max]*

パラメータ *[process name]* は、表 7-2 に示されているプロセスのいずれかにすることができます。プロセス名は大文字と小文字が区別されます。

このコマンドを実行した後、Security Manager サーバを再起動して変更を反映させる必要があります。

（注）　**mrf set_heap_params** を使用して行われた変更は、ヒープ パラメータの変更前に取られたバックアップが復元されると、失われる可能性があります。この場合、新しい値を保持する必要があるときは、次の手順を実行できます。

1. mrf backup を実行します。
2. アプリケーションの復元を行います。
3. mrf revert を実行します。

このコマンドでは、次の構文が使用されます。

mrf set_heap_params *[process name] [X-Y] [min],[max]*

最小および最大ヒープ サイズを設定します。

[X-Y]：ヒープ サイズを適用するメモリ範囲（単位は MB）

[min],[max]：最小および最大ヒープ サイズ（単位は MB）。これらはオプションですが、少なくとも 1 つは指定する必要があります。

パラメータ *[process name]* は、表 7-2 に示されている値のいずれかになります。プロセス名は大文字と小文字が区別されます。

設定変更の例

次に、ヒープ サイズの設定変更の例を示します。

- mrf set_heap_params Tomcat 7372-8192 2048,4096

  RAM サイズが 7372 ～ 8192 MB の範囲内のときの Tomcat プロセスに対して最小および最大ヒープ サイズをそれぞれ 2048 MB と 4096 MB に設定します。

- mrf set_heap_params Tomcat 7372-8192 2048

  RAM サイズが 7372 ～ 8192 MB の範囲内のときの Tomcat プロセスに対して最小ヒープ サイズを 2048 MB に設定します。

- mrf set_heap_params Tomcat 7372-8192,4096

  RAM サイズが 7372 ～ 8192 MB の範囲内のときの Tomcat プロセスに対して最大ヒープ サイズを 4096 MB に設定します。

- mrf set_heap_params Tomcat 8080-8080 2048,4096

  RAM サイズが 8080 MB ときの Tomcat プロセスに対して最小および最大ヒープ サイズをそれぞれ 2048 MB と 4096 MB に設定します。**getramsize** コマンドを実行すると、既存の RAM サイズを MB 単位で取得できます。

設定変更の確認

ヒープ パラメータを設定した後、**mrf get_heap_params** コマンドを実行して変更を確認できます。

プロセスに対するヒープ サイズの設定の要約

ここで説明した、Security Manager プロセスに対するヒープ サイズの設定のための 3 つの主要手順は、次のように要約されます。これらのコマンドは、実行順で示されています。

```
mrf backup
mrf get_heap_params process
mrf set_heap_params Tomcat 7372-8192 2048,4096
mrf revert #if required to revert changes
```

ユーザがヒープ サイズの再設定を必要とする一般的なシナリオ

シナリオ 1

ある Security Manager 4.0 ユーザが、バックエンド プロセス（VmsBackendServer）に対して 4 GB の最大ヒープ サイズを使用しています。これは、8 GB RAM に対して Security Manager 4.1 で割り当てられるデフォルトの最大ヒープ サイズである 3 GB を超えています。このシナリオのユーザは、バックエンド プロセスのヒープ サイズを 4 GB に再設定する必要があります。イベント管理（Event Server プロセス（VmsEventServer）を使用）がイネーブルになっていなければ、そうすることができます。

シナリオ 2

Security Manager が設定専用モードで使用されています（イベント管理とレポートがディセーブルになっている）。このシナリオでは、バックエンド プロセスと Tomcat のヒープ サイズを増やすことができます。

シナリオ 3

Security Manager が設定専用モードで使用されており（イベント管理とレポートがディセーブルになっている）、イベント管理をイネーブルにする必要があります。このシナリオでは、すべての Security Manager プロセスのヒープ サイズの合計がサーバで使用可能な RAM サイズを超えないように、バックエンド プロセスと Tomcat のヒープ サイズを減らしてから、イベント管理をイネーブルにする必要があります。

シナリオ 4

イベント管理とバックエンド プロセスは、メモリを大量に消費するため、より多くの RAM 割り当てを必要とします。（イベント管理が使用されない場合は、その分の RAM がバックエンド プロセスに割り当てられるように、バックエンド プロセスの最大ヒープ サイズを増やすことができます）。

現行のサーバ セキュリティに関するベスト プラクティス

システムの最小限のセキュア コンポーネントによってシステムの安全性が定義されます。下のチェックリスト内のステップは、Security Manager のインストール後のサーバとその OS のセキュリティ保護に役立ちます。

✓	タスク
❑	**1. サーバ セキュリティを定期的にモニタします。**システム アクティビティを記録して確認します。Microsoft Security Configuration Tool Set（MSCTS）や Fport などのセキュリティ ツールを使用して、サーバのセキュリティ設定を定期的に確認します。Security Manager サーバ上にインストールされたスタンドアロン バージョンの Cisco Security Agent に関するログ ファイルを確認します。 **ヒント** MSCTS は Microsoft の Web サイトから、Fport は Foundstone/McAfee の Web サイトから入手できます。
❑	**2. サーバへの物理アクセスを制限します。**サーバに取り外し可能なメディア ドライブが接続されている場合は、ハード ドライブから起動するようにサーバを設定します。誰かが取り外し可能なメディア ドライブからサーバを起動した場合に、データが侵害されるおそれがあります。通常は、システム BIOS 内で起動順序を設定できます。BIOS が強力なパスワードで保護されていることを確認します。
❑	**3. リモート アクセス ツールやリモート管理ツールをサーバ上にインストールしないでください。**このようなツールは、サーバへのエントリ ポイントを提供するセキュリティ リスクになります。
❑	**4. サーバ上で自動的かつ継続的に動作するようにウイルス スキャン アプリケーションを設定します。**ウイルス スキャン アプリケーションは、トロイの木馬アプリケーションのサーバへの侵入を阻止できます。ウイルス署名を定期的に更新します。
❑	**5. サーバ データベースを頻繁にバックアップします。**すべてのバックアップをアクセスが制限されたセキュアな場所に保管します。

インストールまたはアップグレードの確認

Common Services を使用して、Security Manager のインストールまたはアップグレードが成功したかどうかを確認できます。Security Manager インターフェイスが表示されない、または、正しく表示されないことが原因でインストールを確認する場合は、「インストール後のサーバ障害」（P.A-5）を参照してください。

ステップ 1　クライアント システム上のブラウザを使用して、次のいずれかを使用している Security Manager サーバにログインします。

- HTTP サービスの場合：**http://**<*server_name*>**:1741**
- SSL サービスの場合：**https://**<*server_name*>**:443**

サポートされているブラウザとブラウザのバージョンを確認するには、「クライアントの要件」（P.3-8）を参照してください。

ステップ 2　[Cisco Security Management Suite] ページで、[Server Administration] パネルをクリックして、Common Services の [Server] > [Admin] ページを開きます。

ステップ 3　[Process Management] ページを表示するには、[Processes] をクリックします。

結果のリストには、すべてのサーバ プロセスの名前とプロセスごとの動作ステータスの説明が表示されます。次のプロセスが正常に動作している必要があります。

- vmsDbEngine
- vmsDbMonitor
- EDS

関連情報

項目	対応
基本の理解	Security Manager を起動すると表示される対話形式の *JumpStart* ガイドを参照してください。
製品の迅速な稼働	オンライン ヘルプの「Getting Started with Security Manager」トピックを参照するか、『*User Guide for Cisco Security Manager*』の第 1 章を参照してください。
製品設定の実施	オンライン ヘルプの「Completing the Initial Security Manager Configuration」トピックを参照するか、『*User Guide for Cisco Security Manager*』の第 1 章を参照してください。
ユーザの認証と認可の管理	次の項を参照してください。 • 「ユーザの権限」（P.8-3） • 「Security Manager と Cisco Secure ACS の統合」（P.8-12）
デバイスのブート	オンライン ヘルプの「Preparing Devices for Management」トピックを参照するか、http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html から入手可能な『*User Guide for Cisco Security Manager 4.4*』の第 2 章を参照してください。