CHAPTER 5

サーバ アプリケーションのインストールとアップグレード

次のトピックでは、Security Manager サーバ ソフトウェアとその他のサーバ アプリケーション（Common Services、AUS など）のインストール方法について説明します。

必要なサーバ ユーザ アカウントについて

CiscoWorks Common Services と Security Manager は、必要な認可を受けているユーザにのみ特定の機能へのアクセスを許可する多層セキュリティ システムを採用しています。そのため、Common Services 上で動作するアプリケーションがインストールされたシステム上では、事前に定義された次の 3 つのユーザ アカウントが作成されます。

- **admin**：admin ユーザ アカウントは、Windows 管理者と等価で、Common Services、Security Manager、およびその他のアプリケーション タスクのすべてにアクセスできるようにします。インストール中にパスワードを入力する必要があります。このアカウントは、初めてサーバにログインするときに使用して、アプリケーションを日常的に使用するための他のユーザ アカウントを作成できます。
- **casuser**：casuser ユーザ アカウントは、Windows 管理者と等価で、Common Services タスクと Security Manager タスクのすべてにアクセスできるようにします。このアカウントを直接使用することはあまりありません。

  製品のインストール中に設定された casuser（デフォルト サービス アカウント）権限またはディレクトリ権限を変更しないでください。変更した場合は、次の操作ができなくなる可能性があります。

  - Web サーバへのログイン

  - クライアントへのログイン
  - データベースの正常なバックアップ

- *システム識別*: システム識別ユーザ アカウントは、Windows 管理者と等価で、Common Services タスクと Security Manager タスクのすべてにアクセスできるようにします。このアカウントには固定の名前がありません。ニーズに合った名前を使用してアカウントを作成できます。Common Services でアカウントを作成した場合は、そのアカウントにシステム管理者特権を付与する必要があります。ユーザ認証に Cisco Secure Access Control Server（ACS）を使用している場合は、ACS にすべての特権を付与する必要があります。

  Cisco Security Management Suite アプリケーションを別のサーバにインストールする場合（推奨アプローチ）は、マルチサーバ セットアップ内のすべてのサーバ上で同じシステム識別ユーザ アカウントを作成する必要があります。サーバ間の通信は、証明書と共有秘密キーを使用する信頼モデルに依存します。システム識別ユーザは、マルチサーバ セットアップ内の他のサーバから信頼できるアカウントと見なされるため、ドメイン内のサーバ間通信が容易になります。

必要な数のユーザ アカウントを追加できます。アカウントはユーザごとに一意にする必要があります。このような追加のアカウントを作成するには、システム管理者権限（admin アカウントの使用など）を持っている必要があります。ユーザ アカウントを作成したら、それにロールを割り当てる必要があります。このロールによって、表示も含めて、ユーザがアプリケーション内で可能な操作が定義されます。使用可能な権限の種類と ACS を使用してアプリケーションへのアクセスを制御する方法については、第 8 章「ユーザ アカウントの管理」を参照してください。

Remote Desktop Connection または VNC を使用したサーバ アプリケーションのインストール

サーバ アプリケーションは、サーバに直接ログインしてインストールすることを推奨します。

ただし、リモート インストール（別のワークステーション経由のログイン）を行わなければならない場合は、次のヒントを考慮してください。

- リモート ディスクからソフトウェアをインストールしようとしないでください。ソフトウェア インストーラは、サーバ内の DVD ドライブ上で動作している製品 DVD 上に存在するか、直接接続されたディスク ドライブ上に存在する必要があります。リモート ディスクからのインストールが成功したように見える場合がありますが、実際には成功していません。
- ソフトウェアのインストールに Virtual Network Computing（VNC）を使用できます。
- ソフトウェアのインストールに Remote Desktop Connection を使用できます。Remote Desktop Connection を使用する場合は、Remote Desktop Protocol 非コンソール セッションではなく、コンソール セッションを使用することを推奨します。

Security Manager サーバ、Common Services、および AUS のインストール

メインの Security Manager インストール プログラムで次のようなアプリケーションをインストールできます。

- CiscoWorks Common Services 4.0：サーバ アプリケーションに必要な基盤ソフトウェアです。Security Manager 4.4 から、[CiscoWorks Common Services 4.0] チェックボックスはコンポーネントの選択ページに表示されなくなりました。Common Services のインストールは、デフォルトで選択されます。

- Cisco Security Manager 4.4：Security Manager のメイン サーバ ソフトウェアです。
- Auto Update Server 4.4。
- Cisco Security Manager Client 4.4：Security Manager サーバとデータをやり取りするためのクライアント ソフトウェアです。サーバと同じコンピュータ上にインストールできますが、このセットアップを Security Manager を使用する通常の方法として使用しないでください。推奨されているクライアントのインストールとセットアップの詳細については、第 6 章「クライアントのインストールと設定」を参照してください。

ヒント Security Manager 4.4 から、インストール時間を短縮するために、AUS および Security Manager クライアントが同時にインストールされます。

次の手順を使用して、これらのアプリケーションをインストールまたは再インストールします。以前のバージョンのアプリケーションからアップグレードしている場合は、先に進む前に、「サーバ アプリケーションのアップグレード」（P.5-5）を参照してください。

はじめる前に

- このインストレーション ガイドの「ライセンス」の章を参照してください。
- すでにサーバ上にインストールされている既存のバージョンのアプリケーションに対するアップグレードとして製品をインストールしている場合は、「リモート アップグレード時のデータベースのバックアップ」（P.5-8）に記載されているようにバックアップを実行してください。アップグレードをインストールする前に、バックアップが正常に終了し、既存のアプリケーションが正しく機能していることを確認してください。
- Security Manager の永久ライセンスのインストール時は、Security Manager サーバにとってローカルなディスク上にライセンス ファイルを配置する必要があります。Security Manager を使用してサーバ上のディレクトリを参照する場合、マップされたドライブは表示されません。そのため、インストール時にライセンス ファイルを選択するには、そのライセンス ファイルがサーバ上に存在している必要があります。（Windows ではこの制限が課されますが、これにより Security Manager のパフォーマンスとセキュリティが向上します）。このファイルは製品をインストールするフォルダに配置しないでください。

（注） ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

- 「インストール準備状況チェックリスト」（P.4-3）を完了したことを確認してください。
- サーバが「サーバの要件および推奨事項」（P.3-3）に記載された要件を満たしていることを確認してください。
- Security Manager は制御環境下の専用サーバにインストールすることを推奨します。他のソフトウェア アプリケーションをインストールした場合は、Security Manager の通常動作と競合したり、サポートされていなかったりする可能性があります。
- Common Services のインストール後にシステム時間を変更しないでください。このような変更が一部の時間依存機能の動作に影響する可能性があります。
- Cisco Secure Access Control Server（ACS）を使用して、Security Manager または AUS へのユーザ アクセスに AAA サービスを提供する場合は、アプリケーションをインストールしてから、ACS を使用するように Common Services を設定します。ACS 制御の設定方法については、「Security Manager と Cisco Secure ACS の統合」（P.8-12）を参照してください。

ACS を使用するように Common Services を設定してから Security Manager または AUS をインストールした場合は、インストール中に、インストールしたアプリケーションを ACS に登録する必要があることが通知されます。まだアプリケーション（このサーバ上または別のサーバ上）を ACS に登録していない場合は、[Yes] を選択します。すでにアプリケーションを登録している場合は、[Yes] を選択すると、アプリケーションの ACS 内で設定されたユーザ ロールのカスタマイズが失われるため、[No] を選択する必要があります。同じ ACS サーバを使用するすべての Security Manager サーバと AUS サーバがユーザ ロールを共有します。

手順

Security Manager サーバ、Common Services、AUS、またはメインの Security Manager インストール プログラムを使用する複数のアプリケーションをインストールするには、次の手順を実行します。

ステップ 1　インストール プログラムを入手または検索します。次のいずれかの操作を実行できます。

- サーバの DVD ドライブに Security Manager インストール DVD を挿入します。インストール アプリケーションが自動的に起動しなかった場合は、**csm**<*version*>**_win_server** フォルダ内の **Setup.exe** ファイルを実行します。
- Cisco.com アカウントにログインして、http://www.cisco.com/go/csmanager にある Security Manager ホームページにアクセスします。[Download Software] をクリックして、圧縮された Security Manager のインストール ファイルをダウンロードします。
  - WinZip や圧縮フォルダの展開ウィザードなどの Windows Server 2008 に付属しているファイル圧縮ユーティリティのいずれかを使用して、圧縮されたソフトウェア インストール ファイル内のすべてのファイルを一時ディレクトリで解凍します。パス名があまり長くないディレクトリを使用してください。たとえば、C:\Documents and Settings\Administrator\Desktop よりは C: を選択してください。通常は、圧縮ファイルと同じディレクトリに解凍される、インストール プログラムの **Setup.exe** を開始します。
  - ファイルの内容を解凍できないというエラー メッセージが表示された場合は、Temp ディレクトリを空にして、ウイルスをスキャンし、C:\Program Files\Common Files\InstallShield ディレクトリを削除してから、リブートしてもう一度試してみてください。

ステップ 2　インストール ウィザードの指示に従います。インストール中に、次の情報の入力が要求されます。

- Backup location：特定のバージョンの Common Services、Security Manager、または AUS がすでにインストールされている場合は、インストール プログラムによってインストール中のデータベース バックアップが許可されます。バックアップを実施する場合は、バックアップに使用する場所を選択します。ただし、バックアップは、インストールを開始する前に実施することを推奨します。

（注）　バックアップに使用するために選択する場所は、*NMSROOT* の外にする必要があります。場所 *NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:\Program Files\CSCOpx** です。特に、*NMSROOT*\backup をバックアップに使用しないように注意してください。

- Destination folder：アプリケーションをインストールするフォルダ。他の場所にインストールする特別な理由がなければ、デフォルトを受け入れます。デフォルト フォルダ以外のフォルダを指定した場合は、その下にファイルが存在しないことと、パス名が 256 文字未満であることを確認してください。また、デフォルト フォルダ以外のフォルダを指定すると、パスに特殊文字を含めることはできません。
- Applications：インストールするアプリケーション：Security Manager、AUS、または両方。CiscoWorks Common Services 4.0 が Security Manager または AUS のインストール時に自動的にインストールされます。

- License information：次のいずれかを選択します。
  - [License File Location]：ライセンス ファイルのフル パス名を入力するか、[Browse] をクリックして検索します。永久ライセンス ファイルを事前にサーバ上に配置してあった場合は、そのファイルを指定できます。

（注）　ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

  - [Evaluation Only]：無料の 90 日の評価期間をイネーブルにします。
- Admin password：5 文字以上の **admin** ユーザ アカウント用パスワード。このアカウント、システム識別アカウント、および casuser アカウントの詳細については、「必要なサーバ ユーザ アカウントについて」（P.5-1）を参照してください。
- System Identity user：システム識別ユーザとして使用するアカウントのユーザ名とパスワード。Cisco Security Management Suite アプリケーションを複数のサーバ上にインストールする場合は、すべてのサーバ上で同じシステム識別ユーザ アカウントを使用してください。
- Create casuser：新しいインストールで casuser アカウントを作成するかどうか。このユーザ アカウントは作成する必要があります。

（注）　パスワードの複雑度の制限に対するセキュリティ ポリシーがある場合、このアカウント作成は失敗することがあります。そのような場合は、アカウントを手動で作成して、**resetcasuser.exe** コマンドを実行する必要があります。詳細については、表 A-3、「LiaisonServlet エラーの原因と対処法」の casuser パスワードを参照してください。

ステップ 3　インストールの完了後に、サーバが自動的に再起動しない場合は、サーバを再起動します。

サーバ アプリケーションのアップグレード

アプリケーションのアップグレードとは、古いバージョンからのデータを維持しながら、新しいバージョンのアプリケーションをインストールするプロセスです。3 種類のアップグレード パスがあります。

- ローカル：古いバージョンをアンインストールせずに、古いバージョンを実行中のサーバ上に新しいバージョンをインストールします。既存のデータが保存され、新しくインストールされたバージョンで使用できます。ローカル アップグレードを実施する場合は次の点に注意してください。
  - この方式を使用する前に、アップグレードするすべてのアプリケーションが正しく機能していることを確認してください。また、アップグレード対象のアプリケーションをインストールする前に、データベースのバックアップを実施して、正常に終了したことを確認してください。
  - サーバ上のオペレーティング システムもアップグレードしている場合、たとえば、Windows 2003 から Windows 2008 にアップグレードしている場合は、この方式が使用できません。オペレーティング システムのアップグレードも行いながら Security Manager をアップグレードしている場合は、代わりに、リモート バックアップ/復元アップグレード方式を使用します。同じ Security Manager リリースを維持しながらオペレーティング システムをアップグレードしている場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-12）に記載された手順を実行します。
  - データベースの移行エラーが発生した場合はエラー メッセージが表示されます。これが表示されるのは、停止しなくてもインストールを先に進めることが可能な時点です。

（注）　ローカル アップグレード時に、インストーラによって、Performance Monitor または Resource Manager Essentials がインストールされているかどうかがチェックされます。いずれか 1 つ、または両方が検出された場合、「Performance Monitor or Resource Manager Essentials (or both) needs to be uninstalled」というエラー メッセージを表示してインストーラが終了します。

- リモート（バックアップ/復元）：新しいバージョンをクリーン サーバ（古いアプリケーションがインストールされていないサーバ）にインストールしてから、古いバージョンから作成したバックアップからデータベースを復元します。新しいサーバ上にインストールする場合、または、インストールを実施する前にサーバをクリーンオフする（アプリケーションをアンインストールする前にバックアップを作成する）場合に、この手順を使用します。

  （注）　Security Manager サーバ アプリケーションを実行しているサーバのバックアップを作成する前に、すべての保留データがコミットされていることを確認する必要があります。「Security Manager の保留データが送信および承認されることの確認」（P.5-7）を参照してください。

- 間接：ローカルまたはリモート アップグレードでサポートされていない古いバージョンのアプリケーションを使用している場合は、2 段階プロセスを実行する必要があります。ローカルまたはリモート アップグレードでサポートされているバージョンにアップグレードしてから、ローカルまたはリモート アップグレードを実施します。中間のバージョンを Cisco.com からダウンロードします。

  使用中のバージョンが下の表に間接アップグレード用として掲載されておらず、古いデータを保存する必要がある場合は、3 つ以上の中間アップグレード手順を実施する必要があります。たとえば、Security Manager 3.0.x からアップグレードする場合は、3.2.2 にアップグレードしてから、4.1 にアップグレードし、その後で 4.4 にアップグレードする必要があります。

表 5-1 に、アップグレード パスごとにサポートされているソフトウェアのバージョンに関する説明を示します。

次のアップグレード パスがサポートされています。

- 4.1 > 4.4
- 4.2 > 4.4
- 4.3 > 4.4

表 5-1　アプリケーション アップグレード パス

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
ローカル	Security Manager 4.4 Auto Update Server 4.4	4.1、4.2、4.3	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-7）を参照してください。 2. その後で、ソフトウェアをインストールします。「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）を参照してください。 3. 最後に、アップグレード後の必要な変更を加えます。「アップグレード後の必要な変更の実施」（P.5-12）を参照してください。

表 5-1　アプリケーション アップグレード パス （続き）

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
リモート	Security Manager 4.4 Auto Update Server 4.4	4.1、4.2、4.3	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-7）を参照してください。 2. データベースをバックアップします。「リモート アップグレード時のデータベースのバックアップ」（P.5-8）を参照してください。 3. アプリケーションをインストールします。次の項を参照してください。 「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2） 4. 必要に応じて、データベースのバックアップをサーバに転送します。 5. データベースを回復します。「サーバ データベースの復元」（P.5-11）を参照してください。 6. 最後に、アップグレード後の必要な変更を加えます。「アップグレード後の必要な変更の実施」（P.5-12）を参照してください。
間接	Security Manager 4.4	3.x	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-7）を参照してください。 2. 次に、4.1 にアップグレードしてから、4.1 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 （注）　まず 4.1 にアップグレードしてから、リモート アップグレード パスを使用することもできます。

Security Manager の保留データが送信および承認されることの確認

Security Manager のアップグレードを成功させるためには、既存の Security Manager データベースに保留データが含まれていないことを確認する必要があります。保留データとは、データベースに対してコミットされていないデータのことです。保留データが残っている以前のバージョンの Security Manager からのデータベースは復元できません。復元できるのは、バックアップと同じバージョンを実行しているシステム上に保留データが残っているデータベースだけです。

ユーザごとに変更を送信または破棄する必要があります。Approver でワークフロー モードを使用している場合は、このような送信も承認する必要があります。すべてのデバイス設定と Security Manager データベースを同期させるためには、すべてのデータのコミット後に展開を実施する必要もあります。

- Workflow 以外のモードで、次の手順を実行します。
  - 変更をコミットするには、[File] > [Submit] を選択します。
  - コミットされていない変更を廃棄するには、[File] > [Discard] を選択します。

  - 別のユーザの変更をコミットまたは廃棄する必要がある場合は、そのユーザのセッションを引き継ぐことができます。セッションを引き継ぐには、[Tools] > [Security Manager Administration] > [Take Over User Session] を選択してから、[Take Over Session] をクリックします。
- Workflow モードで、次の手順を実行します。
  - 変更をコミットして承認するには、[Tools] > [Activity Manager] を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[Approve] をクリックします。Activity Approver を使用している場合は、[Submit] をクリックして、Approver にアクティビティを承認してもらいます。
  - コミットされていない変更を破棄するには、[Tools] > [Activity Manager] を選択します。[Activity Manager] ウィンドウで、アクティビティを選択してから、[Discard] を選択します。廃棄できるのは、Edit または Edit Open の状態にあるアクティビティだけです。

プロパティ ファイルに対する変更の復元

すべての Security Manager インストールにいくつかのプロパティ ファイルが含まれています。このファイルには、使用中に変更されたデータが保存されます。

- *$NMSROOT*\MDC\athena\config\csm.properties
- *$NMSROOT*\MDC\athena\config\DCS.properties
- *$NMSROOT*\MDC\athena\config\taskmgr.prop

ヒント　*$NMSROOT* は、Common Services インストール ディレクトリ（デフォルトは C:\Program Files\CSCOpx）のフル パス名です。

現在のインストールに対してサービス パックのアップグレードまたはインストールを実施した場合の Security Manager の動作は次のとおりです。

- アップグレードまたはサービス パックに関連する新しいファイルをインストールします。
- 新しいファイルと使用中に変更されたファイルを比較します。
- 新しいファイルと使用中に変更されたファイルが異なる場合は警告を発します。その場合は、Security Manager が次のように処理します。
  - 使用中に変更されたファイルを *<filename>.org* という名前で保存します。
  - 参考用として、差分ファイルを *<filename>.diff* という名前で保存します。

新しいファイルと使用中に変更されたファイルが異なるという内容の警告を受け取った場合は、*<filename>.org* と *<filename>.diff* 内の情報を使用して、アップグレードまたはサービス パックのインストール前に、加えた変更をプロパティ ファイルに復元します。

リモート アップグレード時のデータベースのバックアップ

CiscoWorks Common Services は、データベースのバックアップと復元に使用される Common Services バックアップ/復元ユーティリティで、すべてのサーバ アプリケーションのデータベースを管理します。そのため、バックアップを作成すると、サーバ上にインストールされたすべての CiscoWorks アプリケーションのバックアップが作成されます。

（注）　Security Manager 4.4 から、新しい属性の PURGE_DBBACKUP_LOG が backup.properties ファイルに追加されました。デフォルト値は 20 で、20 日経過した後にバックアップを削除するという意味です。この新しい属性が NIL に設定されている場合、バックアップは削除されません。dbbackup.log は dbbackup_[YYYY-MM-DD_HH-mm-ss].log のタイムスタンプ形式で作成されます。削除設定に関係なく、常時、dbbackup.log ファイルは少なくとも 5 個維持されます。

ヒント　このバックアップ手順はデータベースのみをバックアップします。イベント データ ストアをバックアップする必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-12）に記載されているデータ ストア コピー手順を使用します。

ステップ 1　Security Manager を実行しているサーバをバックアップしている場合は、Security Manager クライアントの [Tools] > [Backup] というショートカットを使用してバックアップ ページを表示できます。また、保留データがコミットされていることを確認します（「Security Manager の保留データが送信および承認されることの確認」（P.5-7）を参照）。

Security Manager を実行していないサーバの場合は、次の手順でバックアップ ページを表示します。

a.　サーバ上の Cisco Security Management Server デスクトップにログインします（「Web ブラウザを使用したサーバ アプリケーションへのログイン」（P.6-13）を参照）。

b.　[Server Administration] パネルをクリックします。次に、[Server] > [Admin] > [Backup] を選択します。

ステップ 2　[Immediate for Frequency] を選択して、必要に応じて他のフィールドを設定し、[Apply] をクリックしてデータをバックアップします。

CLI を使用したサーバ データベースのバックアップ

この項の手順では、サーバ上の Windows コマンドラインからスクリプトを実行することによって、サーバ データベースをバックアップする方法について説明します。

データベースのバックアップ中に、Common Services と Security Manager の両方のプロセスがシャットダウンされ、再起動されます。Security Manager の再起動が完了するまでには数分かかる可能性があるため、再起動の完了前にユーザがクライアントを起動してしまうことがあります。この場合、デバイス ポリシーのウィンドウに「error loading page」というメッセージが表示されることがあります。

CiscoWorks サーバ上にインストールされたすべてのアプリケーションをバックアップするのに 1 つのバックアップ スクリプトしか使用されません。個別のアプリケーションをバックアップできません。

ヒント　このバックアップ コマンドはデータベースのみをバックアップします。イベント データ ストアをバックアップする必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-12）に記載されているデータ ストア コピー手順を使用します。

ステップ 1　保留データがコミットされていることを確認します（「Security Manager の保留データが送信および承認されることの確認」（P.5-7）を参照）。

ステップ 2　コマンド プロンプトで、**net stop crmdmgtd** と入力してすべてのプロセスを停止します。

ステップ 3　次のコマンドを入力することによって、データベースをバックアップします。

*$NMSROOT***bin\perl** *$NMSROOT***bin\backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

引数の説明

- *$NMSROOT* : Common Services インストール ディレクトリのフル パス名（デフォルトは C:\Program Files\CSCOpx）。
- *backup_directory* : バックアップを作成するディレクトリ。C:\Backups などです。

（注） バックアップに使用するために選択する場所は、*NMSROOT* の外にする必要があります。場所 *NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:\Program Files\CSCOpx** です。特に、*NMSROOT*\backup をバックアップに使用しないように注意してください。

- *log_filename* :（任意）バックアップ中に生成されるメッセージ用のログ ファイル。現在のディレクトリ以外の場所にバックアップを作成する場合は、そのパスを追加します。C:\BackupLogs などです。名前を指定しなかった場合は、*$NMSROOT*\log\dbbackup.log になります。
- **email=***email_address* :（任意）通知を送信する電子メール アドレス。電子メール アドレスは指定しないが、後続のパラメータは指定する必要がある場合は、サイズまたはアドレスが一致しない **email** を入力します。CiscoWorks Common Services で SMTP を設定して、通知をイネーブルにする必要があります。
- *number_of_generations* :（任意）バックアップ ディレクトリに保存しておくバックアップの最大世代数。最大数に達すると、古いバックアップが削除されます。デフォルトは 0 で、保存される世代数に制限はありません。
- **compress** :（任意）バックアップ ファイルを圧縮するかどうか。このキーワードを入力しないと、backup.properties ファイル内に VMS_FILEBACKUP_COMPRESS=NO が指定されている場合、バックアップは圧縮されません。指定されていない場合は、このキーワードを入力しなくてもバックアップは圧縮されます。バックアップは圧縮することを推奨します。

たとえば、次に示されているコマンドは、perl コマンドと backup.pl コマンドが存在するディレクトリで発行することを想定しています。（ただし、該当ディレクトリの場合でも、DOS 8.1 形式（スペースなし）の完全修飾された、perl と backup.pl の完全なパスを指定する必要があります）。

次に示されているコマンドでは、バックアップ ディレクトリ内に圧縮されたバックアップおよびログ ファイルが作成され、admin@domain.com に通知が送信されます。

backup.pl コマンドを使用する場合、圧縮パラメータを含めるにはバックアップ世代を指定する必要があります。

ログ ファイル パラメータの後ろにパラメータを指定する場合は、先行するすべてのパラメータの値を含める必要があります。

次の例では、*$NMSROOT* は D:\CSM であり、デフォルト値の C:\Program Files\CSCOpx ではありません。

D:\CSM\bin\perl D:\CSM\bin\backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress

ステップ 4　ログ ファイルを調査して、データベースがバックアップされていることを確認します。

ステップ 5　コマンド プロンプトで、**net start crmdmgtd** と入力して、すべてのプロセスを再起動します。

サーバ データベースの復元

コマンドラインからスクリプトを実行することにより、データベースを復元できます。データの復元中に、CiscoWorks をシャットダウンしてから再起動する必要があります。ここでは、サーバ上のバックアップ データベースを復元する方法について説明します。バックアップおよび復元のための機能は 1 つだけであり、CiscoWorks サーバにインストールされているすべてのアプリケーションをバックアップおよび復元できます。個々のアプリケーションをバックアップまたは復元することはできません。

複数のサーバにアプリケーションをインストールした場合は、インストールされているアプリケーションに適したデータが含まれるデータベース バックアップを復元する必要があります。

ヒント

- 以前のリリースのアプリケーションから作成したバックアップは、このバージョンのアプリケーションへのダイレクト ローカル インライン アップグレードがサポートされているバージョンからのバックアップであれば、復元できます。アップグレードに対応したバージョンの詳細については、「サーバ アプリケーションのアップグレード」（P.5-5）を参照してください。
- restore コマンドは、データベースのみを復元します。イベント データ ストアを復元する必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-12）に記載されているデータ ストア コピー手順を使用します。

手順

ステップ 1　コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

ステップ 2　次のコマンドを入力することによって、データベースを復元します。

*$NMSROOT***bin\perl** *$NMSROOT***bin\restorebackup.pl** [**-t** *temporary_directory*] [**-gen** *generationNumber*] **-d** *backup_directory* [**-h**]

引数の説明

- *$NMSROOT* : Common Services インストール ディレクトリのフル パス名（デフォルトは C:\Program Files\CSCOpx）。
- **-t** *temporary_directory*：（任意）復元プログラムで一時ファイルを保存するために使用されるディレクトリまたはフォルダ。デフォルトでは、このディレクトリは *$NMSROOT*\tempBackupData です。
- **-gen** *generationNumber*：（任意）復元するバックアップ世代番号。デフォルトでは、最新の世代です。第 1 ～ 5 世代が存在する場合は、第 5 世代が最新です。
- **-d** *backup_directory*：復元するバックアップが保存されたバックアップ ディレクトリ。
- **-h**：（任意）ヘルプを表示します。**-d** *BackupDirectory* を使用した場合は、ヘルプに正しい構文と使用可能なスイートおよび世代が表示されます。

たとえば、c:\var\backup ディレクトリから最新のバージョンを復元する場合は、次のコマンドを入力します（これは 64 ビット OS の場合です）。

C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\restorebackup.pl -d C:\var\backup

ステップ 3　ログ ファイル *NMSROOT***log\restorebackup.log** を調べて、データベースが復元されたことを確認します。

ステップ 4　次のように入力して、システムを再起動します。

net start crmdmgtd

ステップ 5　Security Manager サービス パックのインストール前にバックアップされたデータベースを復元する場合は、データベースの復元後にサービス パックを再適用する必要があります。

アップグレード後の必要な変更の実施

アプリケーションをアップグレードすると、特定の情報の処理方法が変わって、手動で変更しなければならなくなる場合があります。このバージョンの製品にアップグレードしたら、下の必要な変更リストを参照して、状況に合わせて変更を適用する必要があります。

- 3.3.1 より以前のバージョンからアップグレードする場合は、4 ポート Gigabit Ethernet Fiber インターフェイス カード（ハードウェア タイプ：i82571EB 4F）が実装された ASA 5580 デバイス上でインベントリを再検出する必要があります。インベントリの再検出によって、デバイス上での速度非ネゴシエート設定を変更できない以前のリリースからのバグが解決されます。インベントリを再検出するには、Security Manager クライアントのデバイス ビューでデバイスを右クリックして、[Discover Policies on Device] を選択してから、[Policies to Discover] グループ内の [Live Device discovery and only the Inventory] チェックボックスをオンにします。再検出によって、デバイスに関するインターフェイス ポリシーが置き換えられます。
- 3.3.1 以前のバージョンからアップグレードしており、未サポートの共有ポート アダプタ（SPA）を使用する Cisco ASR 1000 シリーズ アグリゲーション サービス ルータを管理している場合は、Security Manager で、サポートされているバージョン 4.0 以降の SPA が検出できるように、デバイスに関するポリシーを再検出する必要があります。新しくサポートされる SPA には、すべてのイーサネット（すべての速度）、シリアル、ATM、および Packet over Sonet（POS）SPA が含まれますが、サービス SPA は含まれません。デバイス CLI で ATM、PVC、またはダイヤラ関連ポリシーを設定した場合は、再検出が必要です。

新しいコンピュータまたはオペレーティング システムへの Security Manager の移行

Security Manager を新しいサーバに移行しなければならない場合があります。この移行を新しい物理コンピュータに対して行う場合と、サーバ上のオペレーティング システムにメジャー アップグレードを施す場合（Windows 2003 から Windows 2008 に移行する場合など）があります。

Security Manager のバージョンは変更しないが、物理ハードウェアまたはオペレーティング システムを変更する場合は、移行プロセスを通過する必要があります。この移行プロセスは、基本的に、「サーバ アプリケーションのアップグレード」（P.5-5）に記載されているリモート バックアップ/復元アップグレード プロセスと同じものですが、Event Manager データ ストアに保存されたデータを移行する場合は追加のステップが必要です。Security Manager サーバの移行を実施する場合は、この手順を使用します。

（注）　オペレーティング システムに対するマイナー サービス パック アップデートは、それが Security Manager サーバ移行要件になるまで、アップグレードとは見なされません。サーバ移行は、オペレーティング システムの正式名称が変更される場合のように、異なるメジャー バージョンのオペレーティング システム同士を移行する場合に必要になります。

はじめる前に

この手順では、ターゲット サーバ（Security Manager を移行するサーバ）にソース コンピュータと同じデータベースとイベント データ ストアの内容を保存するものとします。ターゲット サーバ上で Security Manager の使用を開始している場合は、ソース システムとターゲット システムのデータベースまたはイベント データ ストアをマージできません。ターゲット データをソース データで置き換える必要があります。移行前にターゲット システム上に存在していたすべてのデータが、移行完了後に使用できなくなります。古いターゲット システム データを新しく移行するフォルダにコピーしないでください。

また、イベント データ ストアのコピーおよび復元ステップは、そのデータを保存する場合にのみ必要なことに注意してください。新しい空のイベント データ ストアから始める場合は、このステップを省略できます。

ステップ 1　ソース Security Manager サーバ（移行元のサーバ）上で次の手順を実行します。

a. イベント データ ストア フォルダの名前を特定します。Security Manager クライアントで、[Tools] > [Security Manager Administration] を選択し、コンテンツ テーブルから [Event Management] を選択します。フォルダは、[Event Data Store Location] フィールドに表示されています。デフォルトは *NMSROOT***MDC\eventing\database** で、NMSROOT はインストール ディレクトリ（通常は C:\Program Files\CSCOpx）です。

b. コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

c. *NMSROOT***MDC\eventing\config\collector.properties** ファイルのコピーとイベント データ ストア フォルダを作成します。そのコピーをターゲット コンピュータからアクセス可能なディスクに配置します。

d. 「CLI を使用したサーバ データベースのバックアップ」（P.5-9）に記載されているコマンドライン方式を使用して、Security Manager データベースをバックアップします。

ステップ 2　新しいターゲット コンピュータを準備します。例：

- オペレーティング システムをアップグレードするだけで、新しいハードウェアに移行しない場合は、オペレーティング システム アップグレードを実施して、オペレーティング システムが正しく機能していることを確認します。その後で、Security Manager をインストールします。
- 新しいコンピュータに移行する場合は、そのコンピュータが正しく機能していることを確認して、Security Manager をインストールします。

ステップ 3　ターゲット Security Manager サーバ上で次の手順を実行します。

a. コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

b. 「サーバ データベースの復元」（P.5-11）に記載されている手順を使用して、データベースを復元します。

c. データベース復元の完了後にプロセスを再起動しなかった場合は、ここで再起動します。

net start crmdmgtd

d. Security Manager クライアントを使用して新しいサーバにログインしてから、[Tools] > [Security Manager Administration] を選択して、目次から [Event Management] を選択します。

e. イベント データ ストア フォルダが存在し、それが空であることを確認します（必要に応じてファイルを削除します）。このフォルダには、ソース サーバ上のイベント データ ストアと同じ名前と場所を設定する必要があります。

f. 正しい [Event Data Store Location]（デフォルトが正しいフォルダでない場合）を選択して、[Enable Event Management] チェックボックスをオフにし、Event Manager サービスを停止します。[Save] をクリックして変更を保存します。サービスを停止するかどうかの確認が要求されます。[Yes] をクリックしてサービスの停止が通知されるまで待ちます。

g. バックアップされたイベント データ ストアをソース コンピュータからターゲット サーバ上の新しい場所にコピーします。

h. バックアップされた *NMSROOT***MDC\eventing\config\collector.properties** ファイルをソース コンピュータからターゲット コンピュータにコピーして、ターゲット サーバ上のファイルを上書きします。

i. Security Manager クライアントで、[Tools] > [Security Manager Administration] を選択し、コンテンツ テーブルから [Event Management] を選択します。[Enable Event Management] チェックボックスをオンにして、[Save] をクリックします。サービスを開始するかどうかの確認が要求されます。[Yes] をクリックしてサービスの開始が通知されるまで待ちます。

Security Manager の更新

インストール時に永久ライセンス ファイルを指定できますが、Security Manager のインストール後にもライセンスを追加できます。AUS にはライセンスは不要です。

はじめる前に

ライセンス ファイルをサーバ マシンまたはクライアント マシンにコピーしてから、ライセンスをアプリケーションに追加します。クライアント マシンを使用する場合は、クライアント側のブラウザをイネーブルにする必要があります。

（注） ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

ヒント Security Manager にログインする際にライセンスを適用することもできます。Security Manager から「Upgrade license」または「Continue Evaluation」というメッセージが表示されます。[Upgrade License] をクリックすることで、ライセンスを適用できます。

手順

Security Manager のライセンスをインストールするには、次の手順を実行します。

ステップ 1 Security Manager クライアント アプリケーションを使用してサーバにログインします（「Security Manager クライアントを使用した Security Manager へのログイン」（P.6-12）を参照）。

ステップ 2 [Tools] > [Security Manager Administration] を選択し、コンテンツ テーブルから [Licensing] を選択します。

ステップ 3 タブがアクティブになっていない場合は、[CSM] をクリックします。

ステップ 4 [Install a License] をクリックして、[Install a License] ダイアログボックスを開きます。このダイアログボックスを使用して、ライセンス ファイルを選択し、[OK] をクリックします。このプロセスを繰り返して他のライセンスを追加します。

（注）　パスとファイル名は、英語のアルファベット文字に制限されます。日本語文字はサポートされません。Windows 日本語 OS システムでファイルを選択する場合は、通常のファイル区切り文字 \ がサポートされますが、これは円記号（U+00A5）として表示されることがあることに注意する必要があります。

サービス パックとポイント パッチの入手

注意　Security Manager のサービス パックまたはポイント パッチは、シスコから入手してください。それ以外のファイルをダウンロードしたり、開いたりしないでください。サードパーティ製のサービス パックとポイント パッチはサポートされていません。

Security Manager またはその他のアプリケーションをインストールしたら、シスコから入手したサービス パックまたはポイント パッチをインストールして、バグを修復したり、新しいデバイス タイプをサポートしたり、アプリケーションを強化したりできます。

- 新しいサービス パックの入手可能な時期を知って、必要なサービス パックをダウンロードするには、Security Manager を開いて、[Help] > [Security Manager Online] を選択します。または、http://www.cisco.com/go/csmanager にアクセスします。
- 企業から Cisco TAC サービス リクエストが提出されると、TAC が、その問題の解決に役立つ未公開のポイント パッチがあるかどうかを通知します。これ以外の方法で Security Manager ポイント パッチが配布されることはありません。

サービス パックとポイント パッチは、クライアント ソフトウェア アップデートにサーバ サポートを提供し、クライアントとサーバ間のバージョン レベルのミスマッチを検出します。

サーバ アプリケーションのアンインストール

サーバ アプリケーションをアンインストールするには、この手順を使用します。アプリケーションをアンインストールする前に、アプリケーションの再インストールが必要な場合にデータを復元できるようにバックアップの実施を検討してください。バックアップの実施方法については、「リモート アップグレード時のデータベースのバックアップ」（P.5-8）を参照してください。

はじめる前に

任意のバージョンの Windows Defender がインストールされている場合は、それをディセーブルにしてからサーバ アプリケーションをアンインストールします。そうしなければ、アンインストール アプリケーションを起動できません。

手順

サーバ アプリケーションをアンインストールするには、次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Cisco Security Manager] > [Uninstall Cisco Security Manager] を選択します。

デフォルトでは、すべてのアプリケーションがアンインストールされます。

ステップ 2　アンインストーラによって、すべてのアプリケーションが削除されます。

（注） アンインストール中にエラーが発生した場合は、「アンインストール中のサーバ障害」（P.A-8）、および次の URL にある『*Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*』の「Troubleshooting and FAQs」の章を参照してください。
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html

ステップ 3　リブートは必須ではありませんが、アンインストール後はサーバをリブートして、サーバ上のレジストリ エントリと実行中のプロセスが将来の再インストールに適切な状態になるようにすることを推奨します。

ステップ 4　Common Services を含むすべての Cisco Security Management Suite アプリケーションをアンインストールする場合のみ：

a. *NMSROOT* が残っている場合は、それを削除、移動、または名前を変更します。*NMSROOT* は Security Manager インストール ディレクトリへのパスです。*NMSROOT* のデフォルト値は **C:\Program Files\CSCOpx** です。**E:\Program Files\CSCOpx** などのその他の値も使用できます。

b. C:\CMFLOCK.TXT ファイルが存在する場合は、それを削除します。

c. アプリケーションを再インストールする前に、レジストリ エディタを使用して、次のレジストリ エントリを削除します。

- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Resource Manager
- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\MDC

ステップ 5　アプリケーションをアンインストールする前に Windows Defender をディセーブルにした場合は、ここで、もう一度イネーブルにします。

サーバ アプリケーションのダウングレード

Security Manager アプリケーションを以前のリリースにダウングレードして、この製品リリースで作成した設定を保持することはできません。このリリースの Security Manager を使用しない場合は、これをアンインストールし、必要な古いバージョンの製品を再インストールします （これは、必要なライセンスと古いバージョンのインストール メディアがそろっていることが前提です）。その後で、「サーバ データベースの復元」（P.5-11）に記載されているように、ダウングレードされたバージョンの以前のインストールで保存した必要なデータベースのバックアップを復元できます。

Security Manager をダウングレードする場合は、Auto Update Server も、再インストールする Security Manager のバージョンでサポートされるバージョンにダウングレードする必要があります。

古いデータベースを復元した場合、管理対象デバイスの現在の状態と同期しなくなったデバイスのプロパティやポリシーが含まれる可能性があることに注意してください。たとえば、デバイス上のオペレーティング システムを、古いバージョンの Security Manager では直接サポートされないものにアップグレードしたり、古いバージョンには存在しないポリシーを設定し、展開したりした可能性があります。データベースとデバイスを正しく同期させるために、すべての管理対象デバイスのデバイス ポリシーを再検出することを検討してください。大幅な変更（オペレーティング システムのメジャー リリースのアップグレードなど）では、デバイスをインベントリから削除し、再度追加しなければならない場合があることに注意してください。一部の例では、オペレーティング システムのアップグレードを元に戻す必要がある場合もあります（たとえば、ASA ソフトウェア リリース 8.3 は特別な処理が必要で、下位互換モードではサポートできないため、使用する Security Manager のバージョンで直接サポートされている必要があります）。詳細については、『User Guide for Cisco Security Manager』の「Managing the Device Inventory」の章を参照してください。

ヒント　古いバージョンの Security Manager では管理できないデバイスとオペレーティング システム リリースの組み合わせを管理しようとした場合、展開エラーが発生します。