CHAPTER 4

メンテナンス作業

この章では、HA/DR コンフィギュレーションで使用される場合の Security Manager に関するメンテナンス作業について説明します。この章の内容は以下のとおりです。

VCS の動作のカスタマイズ

VCS では、リソースの障害への対応などの VCS の動作を制御するための多数の変数がサポートされます。このマニュアルで説明しているデフォルトのインストールに従った場合、次に説明するようなフェールオーバー動作が行われます。『*Veritas Cluster Server User's Guide*』に説明されているように、これらやその他の動作の制御を確認する必要があります。

- Security Manager に障害が発生した場合、VCS は同じサーバでアプリケーションの再起動を試行しません。代わりに、VCS はクラスタ内のスタンバイ サーバにフェールオーバーします。ただし、リソースレベルの属性 RestartLimit を使用して、エージェントがリソースの障害を宣言する前に、リソースの再起動を試行する回数を制御できます。
- 特定のサーバ上で最初に Security Manager アプリケーションをオンラインにしようとすると、VCS は一度だけリソースをオンラインにしようとします。OnlineRetryLimit リソースレベルの属性は、最初の試行が失敗した場合に、オンライン エントリ ポイントが試行される回数を指定します。
- デフォルトでは、VCS は Security Manager アプリケーションの監視スクリプトを 60 秒ごとに実行します。そのため、アプリケーションの障害を検出するために、最大 60 秒かかる可能性があります。MonitorInterval は調整可能なリソースレベルの属性です。
- デュアル クラスタを使用している場合、デフォルトでは、クラスタ間のフェールオーバーは手動の操作です。これによって、両方のクラスタでアプリケーションを同時に実行することが防止されます。クラスタ間の通信が失われた場合（地理的に離れているデータ センター間に冗長パスが存

在していない場合に発生しやすい)、VCS はリモート クラスタに障害が発生したか、通信に問題があるかを判断できません。クラスタ間の自動フェールオーバーが望ましい場合は、APP サービス グループで ClusterFailOverPolicy 属性で設定できます。

SSL 用のセキュリティ証明書

Security Manager では、サーバとクライアントのブラウザまたはアプリケーションの間の Secure Socket Layer（SSL）暗号化の使用を設定できます。SSL の暗号化では、サーバ上でデジタル証明書を作成して配置する必要があります。デジタル証明書に含まれる識別情報の一部は共通サービスの Web GUI に表示される Common Name（CN; 共通名）または「ホスト名」です。複数のサーバと対応するホスト名が存在する HA/DR コンフィギュレーションの場合、アプリケーションにアクセスするために使用されるホスト名または IP アドレスと一致する証明書を維持できるように、特別な手順が必要になる場合があります。

単一のクラスタでは、単一の仮想 IP アドレスまたは仮想ホスト名を使用してアプリケーションにアクセスします。この場合、仮想 IP アドレスまたは仮想ホスト名と等しい CN で証明書を作成する必要があります。アプリケーションを実行しているクラスタ内のサーバに関係なく、仮想 IP または仮想ホスト名アドレスが有効であるため、フェールオーバーの発生時にデジタル証明書ファイルを更新する必要はありません。

ただし、デュアル地域クラスタ コンフィギュレーションの場合、各クラスタにアプリケーションに関連付けられた独自の IP アドレスまたはホスト名があります。その結果、デジタル証明書ファイルが 1 つのクラスタと一致するように作成されている場合、アプリケーションが他のクラスタにフェールオーバーされると、一致しなくなります。この場合、クラスタ間のフェールオーバーが発生したときに、デジタル証明書ファイルを他のクラスタと一致するように更新する必要があります。

（注）　アプリケーションにアクセスするために仮想ホスト名を使用する場合、代わりに DNS の更新を使用して、クラスタ間のフェールオーバーのために証明書を更新することを防止できます。クラスタ間のフェールオーバーの発生時に、DNS は仮想ホスト名に関連付けられた新しい IP アドレスで更新されます。クライアントがアプリケーションにアクセスする場合に、必ず同じ仮想ホスト名を使用するため、証明書ファイルを更新する必要がありません。

VCS 用の Security Manager Agent では、アプリケーションを起動する前に、共有されず、レプリケーションされていないローカル ディレクトリに保存されているデジタル証明書ファイルが自動的にコピーされます。ただし、クラスタ内の各サーバでこのディレクトリに適切なファイルを配置する必要があります。このディレクトリは、CertificateDir パラメータを使用して、エージェントに対して指定されます。

各サイトに 1 台のサーバが存在している地理的冗長性（DR）コンフィギュレーションの場合、よりシンプルなオプションを使用できます。サーバのホスト名に基づいて証明書ファイルを再生成するようにエージェントを設定できます。このようなことが可能なのは、仮想 IP アドレスまたは仮想ホスト名が関係しないからです。エージェントのこの動作を設定するには、CertificateDir パラメータの値にキーワード **regen** を指定します。

Security Manager がインストールされている場合、デフォルトでは、サーバのローカル ホスト名と一致する自己署名証明書が作成されます。コンフィギュレーションに応じて、この手順に従って、仮想 IP アドレスまたは仮想ホスト名と一致する自己署名証明書を生成します。

ステップ 1　サーバの Web ブラウザ インターフェイス（http://<*ホスト名または IP アドレス*>:1741）にログインします。

ステップ 2　自己署名証明書のセットアップ画面にアクセスするには、Cisco Security Management Suite のホームページの [CiscoWorks] リンクをクリックし、[Common Services] > [Server] > [Security] を選択し、[Certificate Setup] をクリックします。

ステップ 3　証明書のフィールドに入力し、[CN] フィールドで仮想 IP アドレスまたは仮想ホスト名のいずれかを指定して、[Apply] をクリックします。

次の証明書に関するファイルが NMSROOT¥MDC¥Apache¥conf¥ssl ディレクトリに生成されます。

- server.key
- server.crt
- server.pk8
- server.csr
- openssl.conf
- chain.cer

使用しているクラスタが 1 つの場合、以降の操作は不要です。ただし、各クラスタの複数サーバでデュアル地域クラスタ コンフィギュレーションを使用している場合、上記の証明書に関するファイルをクラスタ内の各サーバ上の共有されず、レプリケーションされていないローカル ディレクトリにコピーする必要があります。セカンダリ クラスタに対して同じ手順を実行する必要があります。ただし、このときはセカンダリ クラスタの仮想 IP アドレスまたは仮想ホスト名を指定します。CSManager リソースを定義する場合、**CertificateDir** 属性の選択された共有されず、レプリケーションされていないローカル ディレクトリを指定します。フェールオーバー後、アプリケーションを起動する前に、適切な作業ディレクトリに証明書ファイルが自動的にコピーされます。

Security Manager の手動での起動、終了、またはフェールオーバー

HA/DR 以外のコンフィギュレーションでは、通常、Windows Services アプリケーションまたはコマンドラインでそれに相当する **net start** および **net stop** を使用して、Security Manager を起動および終了します。ただし、HA/DR コンフィギュレーションでは、この方法を使用しないでください。HA/DR コンフィギュレーションでは、Security Manager の起動および終了のための専用スクリプトが提供されます。別のサーバで Security Manager を起動する場合、これらのスクリプトで、必要な追加手順を実行します。これらのスクリプトやその他のスクリプトによって、VCS 用の Security Manager エージェントが作成されます。このエージェントによって、VCS で Security Manager を制御および監視できます。VCS を使用しない場合、これらのスクリプトを使用して、手動で Security Manager を起動および終了できます。

この項は、次の内容で構成されています。

VCS の場合

VCS を使用する場合、VCS のコントロールを使用して Security Manager サービス グループ（APP）を手動で起動、終了、またはフェールオーバーする必要があります。VCS の用語では、起動と終了がそれぞれ、オンラインとオフラインと呼ばれます。VCS の GUI または VCS のコマンドライン インターフェイスを使用して、Security Manager サービス グループをオンラインにしたり、オフラインにしたり、フェールオーバーしたりできます。付録 B の 「ハイ アベイラビリティおよび障害回復保証テスト プラン」（P.B-1）に、このような操作の実行例を説明します。

注意　VCS 以外（net stop の使用など）から手動で Security Manager を終了する場合、VCS ではこれをアプリケーションの障害と認識し、回復を開始しようとします。

VCS 以外の場合

VCS を使用しない場合は、Security Manager で提供される **online** および **offline** スクリプトを使用して、Security Manager を起動および終了できます。これらのスクリプトは、次の場所にあります。

$NMSROOT¥MDC¥athena¥ha¥agent（32 ビット オペレーティング システムの場合）

$NMSROOT¥MDC¥athena¥ha¥agent¥64agent（64 ビット オペレーティング システムの場合）

online スクリプトの構文は、Windows Server 2003 と Windows Server 2008 で異なっています。

Windows Server 2003 の構文：

perl online.pl CSManager *<PathName>* *<EventIPAddress>* [*<CertificateDir>*|**regen**]

次の例を参考にしてください。

```
perl online.pl CSManager F:¥Progra~1¥CSCOpx 10.76.10.238
```

Windows Server 2008 の構文：

perl online.pl CSManager PathName 1 *<PathName>* EventIPAddress 1 *<EventIPAddress>*
[CertificateDir 1 *<CertificateDir>*|**regen**]

次の例を参考にしてください。

```
perl online.pl CSManager PathName 1 F:¥Progra~1¥CSCOpx EventIPAddress 1 10.76.10.238
```

（注）　Windows Server 2008 では、[Command Prompt] を開いたときに、[Run as administrator] を選択する必要があります。

構文	説明
<PathName>	Security Manager のインストール パス（たとえば、「F:¥Program Files¥CSCOpx」）。インストール パスにスペースが含まれる場合、引数を引用符で囲みます。

<EventIPAddress>	Security Manager アプリケーションでクライアント / サーバおよびサーバ / デバイスの通信に使用する IP アドレス。
<CertificateDir>	オプション。SSL 証明書ファイルの保存先となる、非共有のレプリケーションされていないローカル ディレクトリを指定できます。指定される場合、スクリプトによって、これらのファイルがアプリケーションによって使用されるインストール ディレクトリの下の適切なディレクトリにコピーされます。キーワード **regen** が使用される場合、このスクリプトでサーバのローカル ホスト名に基づいて SSL 証明書が再生成されます。このパラメータに使用される値に関係なく、サーバのホスト名が Security Manager アプリケーション ファイルと一致する場合、証明書に対して行う処理はありません。「SSL 用のセキュリティ証明書」（P.4-2）も参照してください。

offline スクリプトには Windows Server 2003 用および Windows Server 2008 用の複数の構文があります。

Windows Server 2003 の構文：

perl offline.pl CSManager *<PathName>*

次の例を参考にしてください。

```
perl offline.pl CSManager F:¥Progra~1¥CSCOpx
```

Windows Server 2008 の構文：

perl offline.pl CSManager PathName 1 *<PathName>*

次の例を参考にしてください。

```
perl offline.pl CSManager PathName 1 F:¥Progra~1¥CSCOpx
```

（注） Windows Server 2008 では、[Command Prompt] を開いたときに、[Run as administrator] を選択する必要があります。

構文	説明
PathName	Security Manager のインストール パス（たとえば、「F:¥Program Files¥CSCOpx」）。インストール パスにスペースが含まれる場合、引数を引用符で囲みます。

簡単に使用するために、コンフィギュレーションに適した属性が含まれる online および offline のバッチ ファイル（たとえば、online.bat や offline.bat）を作成することもできます。

手動フェールオーバーを実行するには、VEA またはコマンド ラインを使用して、レプリケートされたボリューム グループ内でプライマリ ロールを転送できます。プライマリ サーバとセカンダリ サーバの両方が機能している場合、プライマリ ロールをセカンダリに移行（レプリケーションの方向を効率的に逆に）することができます。または、プライマリ サーバに障害が発生して使用できない場合、（高速フェールバックの有無に関係なく）セカンダリ サーバにプライマリ ロールを引き継がせることができます。詳細は、『Veritas Volume Replicator administrator's guide』を参照してください。

次に、2 台のサーバ間のレプリケーションを使用する障害回復コンフィギュレーションのための手動フェールオーバー手順の概要を説明します。

ステップ 1　offline.pl スクリプトを使用して、プライマリ サーバで Security Manager を終了します。

ステップ 2　プライマリ サーバの Security Manager に使用されるボリュームからドライブ文字の割り当てを解除します。

ステップ 3　VEA の GUI を使用してプライマリ サーバからセカンダリ サーバに所有権を移行します。

ステップ 4　セカンダリ サーバの Security Manager に使用されるボリュームにドライブ文字を割り当てます。

ステップ 5　online.pl スクリプトを使用して、セカンダリ サーバで Security Manager を起動します。

（注）　最初にセカンダリ サーバに移行/フェールオーバーする場合、casusers グループのファイルの権限をアップグレードする必要があります。この操作は 1 回だけ行います。詳細については、「動作しているボリュームに対する権限の更新」（P.3-14）を参照してください。

Cisco Secure ACS と Security Manager の統合

『*Installation Guide for Cisco Security Manager*』で説明しているように、Cisco Secure ACS を Security Manager を統合して、Security Manager のユーザに高度な権限を付与できます。HA/DR コンフィギュレーションで、ACS の AAA クライアントとして、コンフィギュレーションに含まれる各 Security Manager サーバを追加する必要があります。ACS でサーバを指定するときは、サーバの物理ホスト名に関連付けられた固定 IP アドレスを指定します。

Security Manager と ACS の統合のために HA/DR コンフィギュレーションを使用する場合、複数の ACS サーバを展開して、ACS がシングル ポイント障害となるのを防止する必要があります。ACS サーバが 1 台のみで、障害が発生している場合、ACS を復元するか、または Security Manager サーバをリセットしてローカル認証を使用するための対策を行うことなく、Security Manager にログインすることはできません。ACS では、プライマリ ACS を複数のセカンダリ ACS とともに展開することがサポートされます。この場合、セカンダリ ACS のプライマリ ACS との同期を維持するためにデータベース レプリケーションが使用されます。Security Manager では、最大 3 つの ACS を指定することがサポートされるため、最初の ACS が使用できない場合、2 番目の ACS を試行し、必要に応じて最後に 3 番目の ACS を試行します。

Security Manager のアップグレード

Security Manager のアップグレードは、さまざまな方法で行われます。

- メジャー リリース（リリースの最初の数字が変更される。たとえば、3.x から 4.x へ）
- マイナー リリース（リリースの 2 桁目の数字が変更される。たとえば、3.1 から 3.2 へ）
- メンテナンス リリース（リリースの 3 桁目の数字が変更される。たとえば、3.1 から 3.1.1 へ）
- サービス パック（サービス パックの識別子によって識別される。たとえば、Security Manager 3.1 の SP2）

HA/DR コンフィギュレーションで Security Manager をアップグレードする場合、主な違いは Security Manager のアクティブ インスタンスでプライマリ サーバをアップグレードすることだけが必要か、または Security Manager をサーバ上で実行するために必要な正しいレジストリ設定を確立するために、Security Manager のスペア コピーのみが存在しているセカンダリ サーバもアップグレードする必要があるかということです。アップグレードでレジストリが変更される場合、HA/DR コンフィギュレーションのすべてのサーバでアップグレードを実行する必要があります。通常、サービス パックはレジ

ストリには影響しないため、プライマリ サーバにサービス パックをインストールするだけで十分です。メジャー、マイナー、またはメンテナンス リリースの場合、通常、すべてのサーバをアップグレードする必要があります。ただし、ガイドラインの例外を readme ファイルまたはリリース ノートで確認してください。

セカンダリ サーバをアップグレードする場合、Security Manager のスペア コピーを、コンフィギュレーション内のすべてのサーバで使用される標準の $NMSROOT（たとえば、F:¥Program Files¥CSCOpx）のパスにマウントし、標準アップグレードをインストールする必要があります。これによって、セカンダリ サーバで、アップグレードされたバージョンの Security Manager を実行するために、レジストリ設定が適切であることが保証されます。

アップグレードする前に、すべてのサーバで VCS を終了します（クラスタ内の任意のサーバで **hastop -all -force** を使用して、クラスタ内のすべてのサーバで VCS を終了し、アプリケーションとそのリソースの動作を停止する）。すべてのサーバでアップグレードを実行し、コンフィギュレーションでレプリケーションを使用する場合、アップグレード中にレプリケーションを一時停止するか、終了し、アップグレードの完了後にセカンダリ サーバを同期します。

Security Manager のバックアップ

Security Manager の HA/DR 導入コンフィギュレーションによって、Security Manager を定期的にバックアップする必要性が変わることはありません。HA/DR コンフィギュレーションによって、ハードウェアの障害が原因のデータ損失またはアプリケーションのダウンタイムから保護されますが、Security Manager で維持されている重要な情報が誤って、または悪意に基づいて変更または削除されることからは保護されません。したがって、Security Manager のデータベースおよび情報ファイルのバックアップを継続する必要があり、Security Manager のバックアップ機能を使用できます。

バックアップする必要があるのは Security Manager のプライマリ アクティブ インスタンスのみで、セカンダリ サーバに関連付けられたスペア インスタンスのバックアップは不要です。Security Manager は、HA/DR コンフィギュレーション内のサーバまたは互換性のある Security Manager アプリケーションがインストールされているサーバに復元できます。

Security Manager のアンインストール

HA/DR コンフィギュレーション内のすべてのサーバから Security Manager をアンインストールするには、次の手順に従います。

ステップ 1　プライマリ クラスタのプライマリ サーバ上で Security Manager が動作していることを確認します。

ステップ 2　Cluster Explorer を使用して、[APP_CSManager] リソースを右クリックし、[critical] チェックボックスをオフにします。read/write モードに切り替えるプロンプトが表示される場合、このダイアログ ボックスが表示されたら、[Yes] をクリックします。

ステップ 3　[APP_CSManager] リソースを右クリックし、プライマリ サーバで [Offline] を選択します。Security Manager がオフラインになるのを待ちます。

ステップ 4　[APP_CSManager] リソースを削除し、VCS 設定を保存します。

ステップ 5　レプリケーションを使用している場合、VEA の GUI を使用してレプリケーションを終了します。

ステップ 6　プライマリ サーバで Security Manager をアンインストールするには、[Start] > [All Programs] > [Cisco Security Manager] > [Uninstall Security Manager] を選択します。

ステップ 7　セカンダリ サーバで、cscopx_spare ボリュームが含まれるディスク グループのインポートが完了していない場合は、VEA の GUI またはコマンド ラインを使用してインポートします。

ステップ 8　VEA の GUI を使用して、cscopx_spare ボリュームに選択したドライブ文字を割り当てます。

ステップ 9　プライマリ サーバで Security Manager をアンインストールするには、[Start] > [All Programs] > [Cisco Security Manager] > [Uninstall Security Manager] を選択します。

ステップ 10　その他のセカンダリ サーバまたはセカンダリ クラスタ内のプライマリ サーバで、ステップ 7 ～ 9 を繰り返します。

（注）　Security Manager を再インストールする予定がなく、レプリケーションを使用している場合は、Security Manager および Replicated Volume Group に関連付けられた VCS 内のサービス グループも削除する必要があります。また、不要なボリュームやディスク グループも削除する必要があります。

非 HA Security Manager の HA への移行

通常の HA 以外のコンフィギュレーションで既存の Security Manager をインストールした場合について、ここで HA コンフィギュレーションにインスタンスを移行する方法について説明します。移行を実行するには、次の手順を使用します。

ステップ 1　『*User Guide for CiscoWorks Common Services 3.2*』で説明しているように、既存の Security Manager インスタンスのバックアップを実行します。次の URL にある「*Configuring the Server*」の章の「*Backing Up Data*」の項を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/admin.html

ステップ 2　このマニュアルで説明しているように、必要な Security Manager の HA または DR の導入環境を作成します。

ステップ 3　『*User Guide for CiscoWorks Common Services 3.2*』で説明しているように、元の Security Manager インスタンスから作成したバックアップを、HA または DR の導入環境のプライマリ サーバに復元します。上記のリンク先の「Restoring Data」を参照してください。

ステップ 4　セカンダリ サーバのレジストリ内のデータベースのパスワードを、プライマリ サーバのパスワードと手動で同期します。プライマリ サーバで、レジストリ エディタを使用して（[Start] > [Run] > [regedit] ）、HKEY_LOCAL_MACHINE¥SOFTWARE¥OBDC¥OBDC.INI の下のフォルダ cmf、vms、rmeng、および aus の下で CWEPWD レジストリ エントリの値を検索し、メモしてください。セカンダリ マシンの CWEPWD レジストリ値をプライマリ マシンの値に合わせて編集します。