CHAPTER 4

メンテナンス作業

この章では、HA/DR 構成で使用される Security Manager に関連するメンテナンス作業について説明します。この章は、次の内容で構成されています。

VCS 動作のカスタマイズ

VCS では、リソース障害への対応など、VCS 動作を制御するための大量の変数をサポートします。ここでは、このマニュアルの説明に従ってデフォルト インストールを行った場合のフェールオーバー動作の一部を示します。『*Veritas Cluster Server のガイド*』の説明に従って、このような動作の制御を確認する必要があります。

- Security Manager が失敗すると、VCS は同じサーバ上でアプリケーションを再起動しようとしません。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、リソースレベル属性 RestartLimit を使用して、エージェントがリソースの障害状態として宣言する前にリソースを再起動しようとする回数を制御できます。
- 特定のサーバで最初に 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 はリソースを一度だけオンラインにしようとします。OnlineRetryLimit リソースレベル属性では、最初の試行が失敗した場合にオンライン エントリ ポイントを再試行する回数を指定します。
- デフォルトでは、VCS は 60 秒ごとに Security Manager アプリケーション モニタ スクリプトを実行します。これは、アプリケーションの障害を検出するのに最大 60 秒かかる可能性があることを意味します。MonitorInterval は調整できるリソースレベル属性です。
- デュアル クラスタを使用する場合、クラスタ間のフェールオーバーは、デフォルトでは手動操作です。これは、両方のクラスタで同時にアプリケーションを実行するのを回避します。クラスタ間の通信が失われた場合（冗長パスが地理的に離れたデータセンター間にない場合に発生しやすくなります）、VCS はリモート クラスタに障害が発生したかどうか、または通信に問題があるかどう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必要な場合は、APP サービス グループの 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、サーバおよびクライアント ブラウザまたはアプリケーション間における Secure Socket Layer（SSL）の暗号化の使用を設定できます。SSL 暗号化には、サーバにおけるデジタル証明書の作成と配置が必要です。デジタル証明書に含まれている ID 情報の一部は、Common Services Web GUI に表示される Common Name（CN）または「Host Name」です。複数のサーバおよび対応するホスト名が存在する HA/DR 構成では、アプリケーションへのアクセスに使用されるホスト名または IP アドレスに一致する証明書を保持するために、特別な手順が必要になることがあります。

シングル クラスタの場合、単一の仮想 IP アドレスまたは仮想ホスト名でアプリケーションにアクセスします。この場合は、仮想 IP アドレスまたは仮想ホスト名と同じ CN で証明書を作成する必要があります。仮想 IP または仮想ホスト名のアドレスはアプリケーションを実行するクラスタ内のサーバに関係なく有効であるため、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、デュアル地理的クラスタ構成の場合、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。そのため、デジタル証明書ファイルがある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すると一致しなくなります。この場合は、クラスタ間のフェールオーバーの発生時に、他のクラスタに一致するようにデジタル証明書ファイルを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は、代わりに DNS 更新を使用すると、クラスタ間フェールオーバーのために証明書を更新する必要がなくなります。クラスタ間フェールオーバーが発生すると、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。クライアントは常に同じ仮想ホスト名を使用してアプリケーションにアクセスするため、証明書ファイルを更新する必要はありません。

VCS 用の Security Manager エージェントは、アプリケーションを開始する前に非共有の複製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を自動的にコピーできます。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。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指定されます。

各サイトにサーバが 1 台ある地理的冗長性（DR）構成の場合は、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。これは、仮想 IP アドレスまたは仮想ホスト名がないため動作します。エージェントをこのように動作するように設定するには、CertificateDir パラメータの値にキーワード **regen** を指定します。

Security Manager をインストールすると、サーバのローカル ホスト名に一致する自己署名証明書がデフォルトで作成されます。構成に応じて、仮想 IP アドレスまたは仮想ホスト名に一致する自己署名証明書を生成するには、次の手順に従います。

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

ステップ 2　次のように自己署名証明書セットアップ画面にアクセスします。

a. Cisco Security Management Suite のホームページで、[Server Administration] をクリックします。

b. [Server Admin] ページのメニューから、[Server] > [Single Server Management] > [Certificate Setup] を選択します。

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を指定し、[Apply] をクリックします。

次の証明書関連ファイルは、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

シングル クラスタを使用する場合は、これ以上の処理は必要ありません。ただし、各クラスタ内に複数のサーバが配置されたデュアル地理的クラスタ構成を使用する場合は、クラスタ内の各サーバでこれらの証明書関連ファイルを非共有の複製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。次に、セカンダリ クラスタに対して同じ手順を実行します。ただし、今度はセカンダリ 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、選択された非共有の複製されていないローカル ディレクトリを **CertificateDir** 属性に指定します。エージェントは、フェールオーバー後、アプリケーションを開始する前に適切な作業ディレクトリに自動的に証明書ファイルをコピーします。

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

非 HA/DR 構成では、通常、Windows Services アプリケーションまたはコマンドラインのそれに相当する **net start** および **net stop** を使用して Security Manager を起動および停止します。ただし、HA/DR 構成では、この方法を使用しないでください。HA/DR 構成では、Security Manager を起動および停止するための特定のスクリプトが提供されています。これらのスクリプトでは、異なるサーバで Security Manager を起動する場合に必要な追加手順を実行します。これらのスクリプトおよびその他のスクリプトは VCS 用の Security Manager エージェントを構成します。エージェントを使用すると、VCS で Security Manager を制御およびモニタできます。VCS を使用しない場合は、これらのスクリプトを使用して、Security Manager を手動で起動および停止できます。

ここでは、次の内容について説明します。

VCS の場合

VCS を使用する場合、VCS 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、停止、およびフェールオーバーする必要があります。VCS 用語では、起動および停止はそれぞれオンラインおよびオフラインと呼ばれます。VCS GUI または VCS 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「ハイ アベイラビリティおよびディザスタ リカバリ証明テスト計画」（P.B-1）に、このような操作の実行例があります。

注意　VCS の外部で Security Manager を手動で（net stop を使用するなどして）を停止すると、VCS はこれをアプリケーション障害として認識し、リカバリの開始を試行します。

VCS 以外の場合

VCS を使用しない場合は、Security Manager に付属の **online** および **offline** スクリプトを使用して Security Manager を起動および停止できます。これらのスクリプトは次の場所にあります。

$NMSROOT\MDC\athena\ha\agent（Veritas 5.1 SP1 用）

$NMSROOT\MDC\athena\ha\agent\Veritas60（Veritas 6.0 用）

Veritas 5.1 SP1 用の Windows Server 2008 の構文：

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

例：

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

（注） コマンド プロンプトを開くときに [Run as administrator] オプションを選択する必要があります。

Veritas 6.0 用の Windows Server 2008 の構文：

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

例：

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

（注） コマンド プロンプトを開くときに [Run as administrator] オプション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、引用符で引数を囲みます。
<EventIPAddress>	Security Manager アプリケーションがクライアント/サーバとサーバ/デバイスの通信に使用する IP アドレス。
<CertificateDir>	任意。SSL 証明書ファイルが保管される、非共有の複製されていないローカル ディレクトリを指定できます。指定した場合、スクリプトは、アプリケーションが使用するインストール ディレクトリの下の適切なディレクトリにこれらのファイルをコピーします。**regen** キーワードが使用されている場合、スクリプトは、サーバのローカル ホスト名に基づいて SSL 証明書を再生成します。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 ファイルのホスト名と一致する場合は、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。

Windows Server 2008 用の **offline** スクリプトの構文は次のとおりです。

Veritas 5.1 用の Windows Server 2008 の構文：

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

例：

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

（注） コマンド プロンプトを開くときに [Run as administrator] オプションを選択する必要があります。

Veritas 6.0 用の Windows Server 2008 の構文：

```
perl offline.pl CSManager <PathName>
```

例：

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

（注） コマンド プロンプトを開くときに [Run as administrator] オプション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、引用符で引数を囲みます。

使いやすさのために、構成に適した属性を含むオンラインおよびオフライン バッチ ファイル（online.bat、offline.bat など）を作成する必要がある場合があります。

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、複製されたボリューム 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 サーバの両方が動作している場合、プライマリ ロールをセカンダリに移行（複製の方向を効果的に逆に）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は、（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。詳細については、『Veritas Volume Replicator administrator's guide』を参照してください。

次は、2 台のサーバ間で複製を使用するディザスタ リカバリ構成の手動フェールオーバー手順の概要です。

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 を停止します。

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

ステップ 3　VEA 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 サーバの Security Manager を起動します。

（注）　セカンダリ サーバへの移行またはフェールオーバーが初めての場合、casusers グループのファイル権限をアップグレードする必要があります。これは、ワンタイム アクティビティです。詳細については、「作業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*』で説明されているように、Cisco Secure ACS を Security Manager に統合して、Security Manager ユーザに高度な許可を付与できます。HA/DR 構成では、ACS の AAA クライアントとして設定に関連する各 Security Manager サーバを追加する必要があります。ACS でサーバを指定した場合、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。

ACS 統合で Security Manager に HA/DR 構成を使用する場合は、複数の ACS サーバを展開して、ACS がシングル ポイント障害になるのを回避する必要もあります。ACS サーバが 1 台だけあり、そのサーバで障害が発生した場合は、修正措置を行って ACS を復元するかローカル認証を使用するように Security Manager サーバをリセットしなければ、Security Manager にログインできません。ACS は、プライマリ ACS とのセカンダリ ACS の同期を維持するためにデータベース複製が使用される、プライマリ ACS と複数のセカンダリ ACS の展開をサポートします。Security Manager では、最大 3 つの ACS の指定をサポートするため、最初の ACS が使用できない場合は、必要に応じて 2 台目を試行し、最後に 3 台目を試行します。

Security Manager のアップグレード

Security Manager のアップグレードには、さまざまな形態があります。

- メジャー リリース（リリースの最初の数字の変更。たとえば、3.x から 4.x に変更）
- マイナー リリース（リリースの 2 桁目の数字の変更。たとえば、3.1 から 3.2 に変更）
- メンテナンス リリース（リリースの 3 桁目の数字の変更。たとえば、3.1 から 3.1.1 に変更）
- サービス パック（Security Manager 3.1 用の SP2 など、サービス パック ID で識別される）

HA/DR 構成の 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 サーバのみをアップグレードする必要があるのか、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行うために、Security Manager のスペア コピーのみが存在するセカンダリ 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。アップグレードによってレジストリが変更される場合、HA/DR 構成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影響しないため、プライマリ サーバだけにサービス 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 リリースでは、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、readme ファイルまたはリリース ノートでこれらのガイドラインの例外を確認してください。

セカンダリ サーバをアップグレードする場合は、Security Manager サーバのスペア コピーを構成内のすべてのサーバで使用される標準の $NMSROOT（F:\Program Files\CSCOpx など）パスにマウントして、定期的なアップグレードをインストールする必要があります。これにより、セカンダリ サーバで Security Manager のアップグレード バージョンを実行するために正しいレジストリ設定が行われます。

アップグレードする前に、すべてのサーバで VCS を停止します（クラスタ内の任意のサーバで **hastop -all -force** を使用すると、クラスタ内のすべてのサーバで VCS が停止し、アプリケーションとリソースは動作可能なままになります）。すべてのサーバでアップグレードし、構成で複製が使用されている場合は、アップグレード時に複製を一時停止するか停止し、アップグレードの完了後にセカンダリ サーバを同期する必要があります。

Security Manager のバックアップ

Security Manager の HA/DR 展開構成によって、Security Manager の定期的なバックアップが不要になるわけではありません。HA/DR 構成により、ハードウェア障害によるデータ損失やアプリケーションのダウンタイムから保護されます。ただし、Security Manager に保持されている重要な情報を誤って、または悪意を持って変更または削除されるなどのユーザ アクションからは保護されません。したがって、Security Manager データベースおよび情報ファイルを引き続きバック アップする必要があります。Security Manager のバック アップ機能を使用できます。

セカンダリ サーバに関連付けられているスペア インスタンスではなく、Security Manager のプライマリ アクティブ インスタンスのみをバックアップする必要があります。Security Manager は、HA/DR 構成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で復元できます。

Security Manager のアンインストール

HA/DR 構成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 クラスタ内のプライマリ サーバで Security Manager が実行され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。読み取り / 書き込みモードに切り替えるよう求められるため、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まで待ちます。

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　複製を利用する場合は、VEA GUI を使用して複製を停止します。

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 Cisco Security Manager] を選択します。

ステップ 7　セカンダリ サーバで、VEA GUI またはコマンドラインを使用して、cscopx_spare ボリュームを含むディスク グループをインポートします（まだインポートしていない場合）。

ステップ 8　VEA GUI またはコマンドラインを使用して、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 Cisco Security Manager] を選択します。

ステップ 10　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い場合は、Security Manager に関連付けられた VCS 内のサービス グループおよび複製を使用している場合は複製されたボリューム グループを削除する必要があります。不要なボリュームおよびディスク グループも削除する必要があります。

HA への非 HA Security Manager の移行

通常の非 HA 構成に既存の Security Manager がインストールされている場合は、この項で HA 構成にその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* 』の説明に従って、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*」という章の「*Backing* Up Data」という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　このマニュアルの説明に従って、目的の Security Manager HA または DR 導入環境を作成します。

ステップ 3　『*User Guide for CiscoWorks Common Services 3.2* 』の説明に従って、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 導入環境のプライマリ サーバに復元します。上記のリンクにある「Restoring Data」という項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 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（[Start] > [Run] > [regedit]）を使用して、HKEY_LOCAL_MACHINE\SOFTWARE\OBDC\OBDC.INI の cmf、vms、rmeng フォルダにある CWEPWD エントリの値を探して書き留めます。セカンダリ マシンの CWEPWD レジストリ値をプライマリの値と一致するように編集します。