CHAPTER 11

その他の管理作業

この章では、システムのメンテナンスおよびセットアップに必要となる可能性のあるさまざまな作業について説明します。内容は次のとおりです。

バージョン情報の取得

すべてのアプライアンスには、特定リリースのアプライアンス ソフトウェアを識別するバージョン番号があります。シスコのサポート担当者への問い合わせ時や、クラスタ内のすべてのアプライアンスで同じソフトウェア バージョンが稼動していることを確認する際には、この情報が必要となる場合があります。

アプライアンスからバージョン情報を取得するには、次の手順を実行します。

ステップ 1 `root` ユーザとしてアプライアンス シェルにログインします。

ステップ 2 [Main Menu] から、[Advanced Options] メニュー項目を選択します。

[Advanced Options] メニューが表示されます。

ステップ 3 [Version Information] メニュー項目を選択します。

このリリース識別ストリングは、画面上部にバナーとして表示されます。この画面の中央には、現在インストールされている Gateway ソフトウェア、OS カーネル、Tarari XML コプロセッサ カードのファームウェア（このオプション情報はすでに使用されなくなったハードウェア アドオン オプションに関するもの）、および nForce ハードウェア キーストア カードのファームウェアのバージョン番号が表示されます。

アプライアンス ユーザ アカウントの作成

システムには数種類のユーザ アカウントがあります。Manager ユーザ アカウントは Manager の Web コンソール インターフェイスへのアクセスを提供します。

アプライアンスのコマンドライン環境へのアクセスには、別の種類のユーザ アカウントが使用されます。このアカウントは、OS アカウントと呼ばれ、アプライアンスにローカル接続されているコンソールを使用するのか、リモートで Secure Shell（SSH; セキュア シェル）を使用するのかに関係なく、アプライアンス上の端末セッションにアクセスできます。

各アプライアンスには、`root` アカウントが組み込まれています。`root` ユーザには、アプライアンスを操作するための広範な特権が与えられています。セキュリティ上、`root` アカウントへのアクセスは厳密に管理する必要があります。追加のログイン アカウントを作成すれば、アプライアンスに対する限定的な管理特権を割り当てることができます。ユーザ アカウントを利用すると、設定変更も簡単に管理できます。

アプライアンス用のユーザ アカウントは 2 種類あります。

- developer ユーザ - SDK 拡張機能を導入するためにアプライアンスにアクセスします。
- operator ユーザ - ログ ファイルの循環や取得のためにアプライアンスにアクセスします。

いずれの場合も特権は非常に限定されています。たとえば、どちらのユーザ タイプも、メニュー方式の シェル インターフェイスは使用できません。また、どちらの場合もリストされるタスクに制限があります。

アプライアンスに新しいログイン アカウントを作成するには、次の手順を実行します。

ステップ 1　`root` ユーザとしてアプライアンス シェルにログインします。

ステップ 2　[Main Menu] から、[Advanced Options] の項目を選択します。

ステップ 3　[Advanced Options] ページで、[Run Bash] オプションを選択します。

ステップ 4　`bash` プロンプトで、2 タイプのユーザのいずれかを作成します。

- operator ユーザを作成する場合は、次のコマンドを入力します。

  ```
  reactivity-operator-add [username]
                  "[description]"
  ```

  上記のコマンドで、

  - *[username]* は新しい operator ユーザのログイン名です。
  - *[description]* は、そのアカウントの目的を示す簡単な記述です。

- developer ユーザを作成する場合は、次のコマンドを入力します。

  ```
  reactivity-developer-add [username]
                  "[description]"
  ```

  上記のコマンドで、

  - *[username]* は新しいユーザのログイン名です。
  - *[description]* は、そのアカウントを説明する簡単な記述です。

シェルが記述内容を正しく解釈できるようにするため、記述は必ず二重引用符（"）で囲む必要があります。

ステップ 5　新しいアカウントのパスワードを入力します。プロンプトが表示されたら、再度パスワードを入力してこれを確認します。

これで新しいユーザはシェル インターフェイスにログインできるようになります。

ステップ 6　exit を入力して、管理メニューに戻ります。

システムのバックアップと復元

作業ポリシーは、多くの場合、何時間もの計画と設定の結果であり、非常に重要な文書です。これらには、ネットワークについての重要な機密情報も含まれています。これらは、業務上不可欠な他の機密データと同様、バックアップや障害回復計画も含めて、慎重に取り扱う必要があります。

システムのバックアップには 2 つの方法があります。

- 各ポリシーのアーカイブとオフラインでの保存 - この方法では、Manager インターフェイスからのポリシーの変更は取り込まれますが、アプライアンスに直接行われた設定は除外されます。
- backup コマンドによるアプライアンスの状態のバックアップ - この方法では、設定値、ポリシー、ログ ファイルなど、アプライアンスのシステム状態を含むアーカイブ ファイルが作成されます。

ほとんどのユーザはこれらを両方とも利用します。つまり、必要に応じて個々のポリシーを保存し、定期的にシステムのバックアップも実行します。個々のポリシーのアーカイブは、Manager の Web コンソールから実行できます （この操作の手順については、『*Cisco ACE XML Gateway User Guide*』の「Exporting a Policy to a File」の章を参照してください）。ここではシステム全体のバックアップ方法を説明します。

システムをバックアップするか、または以前に保存したバックアップに基づいてアプライアンスを復元するには、そのアプライアンスに対して backup コマンドを使用します。backup コマンドは、Gateway システムと Manager の両方で使用できます。

このコマンドを実行すると、そのアプライアンス上のファイルに元の状態との違いがないかどうか検査されます（ランタイム処理型の変更は除外されます）。相違点の情報はアーカイブ ファイルに書き込まれます。このファイルは、バックアップまたは回復に適したストレージ メディアに移動できます。

システムのバックアップ

バックアップ ユーティリティは、取り込まれた時の状態にシステムを復元できるようにします。バックアップ ユーティリティは、初期状態のシステムから加えられた変更を認識し、それらの変更をアーカイブに保存することによって、アプライアンスの状態を保存します。バックアップがアプライアンス上で復元されると、システムは保存済みの状態に戻ります。

（注）　バックアップ ファイルからの復元は、アプライアンスの設定が空の場合にだけ機能するようになっています。設定が空でないアプライアンスでは復元が機能しない場合もあります。

バックアップ ユーティリティが保存するシステム機能には、ポリシー状態、システムのネットワーク設定、ログ情報のほか、システム導入以降に作成されたり変更されたりしたファイル（スクリプトまたはデータ ファイルなど）が含まれます。

バックアップ/復元ユーティリティではバックアップされないようなタイプのシステム変更またはシステム機能もいくつかあります。たとえば、アクティブ プロセス情報のようにランタイム型の情報は統合されません。また、ソフトウェアのアップデート、ホットフィックス、RPM にインストールされた正規の拡張機能のようなシステム変更も除外されます（ユーザ自身が作成およびインストールした SDK 拡張機能は、バックアップ*される*ことに注意してください）。バックアップおよび復元プロセスを開始する前に、これらを個別に復元する必要があります。

backup コマンドを実行する前に、バックアップ プロセスが機能するのに十分な空き容量がアプライアンスにあることを確認してください。正確な必要スペースは、システムで使用されているスペースおよび実行するバックアップのタイプによって異なります。システムにアップデータまたは以前のバックアップ アーカイブ ファイルなどがある場合、後継アーカイブを -filestore または -all オプションで作成すると、このアーカイブにこれらのファイルが含められますが、作成されるアーカイブのサイズは非常に大きくなります。後継アーカイブに不要なファイルまたはアーカイブが含まれないようにするには、不要なアーカイブをシステムから削除するか、または tmp ディレクトリに保存する必要があります。tmp ファイルにあるアーカイブは 10 日が経過すると自動的に消去されます。イベント ログ、監査ログ、またはトラフィック ログをバックアップする場合は、ログのサイズと同量のディスク空き容量が必要です。

（注） バックアップ動作自体としては、開始前に十分なディスク容量があるかどうかの確認は行われません。使用可能な容量が足りないと、バックアップ動作は正常に終了しません。

バックアップを完了するために、バックアップ ユーティリティは実行中の ACE XML Gateway サービスを停止しません。このため、この手順によりメッセージ トラフィックが妨げられることはありません。

システムをバックアップするには、次の手順を実行します。

ステップ 1　バックアップするアプライアンスのアプライアンス シェルにアクセスします。

ステップ 2　[Advanced Options] > [Run Bash] の順に選択します。

ステップ 3　次のように `backup` コマンドを使用して、バックアップ ファイルを作成します。

```
backup -all <filename>
```

上記のコマンドでは、filename はバックアップ アーカイブの保存先となる `tgz` ファイルの名前です。次に例を示します。

```
backup -all applianceBackup.tgz
```

`-all` スイッチを指定すると、ネットワークおよび Gateway の設定値、ポリシー ファイルストア、ログ ファイルを含め、すべてのデータがバックアップされます。代わりに、次に示すコマンド スイッチを使用すると、指定したデータ部分だけをバックアップすることができます。

```
backup -filestore applianceBackup.tgz
```

filestore スイッチを指定すると、ログ情報を除くすべてのデータがバックアップされます。ログ データだけをバックアップする場合は、`-userlog`（イベント ログ）、`-auditlog`、または `-traffic` スイッチを使用します。

コマンド オプションを指定しなかった場合には、ネットワークおよび Gateway の設定だけがバックアップされます。

（注） `backup -h` を入力すると、このコマンドに使用できるオプションがすべて表示されます。`-e` と `-l` のスイッチには注意してください。これらを指定すると、コマンド動作のエラーが標準エラー出力に出力されます。通常、シスコのサポート担当者に指示されない限り、これらのオプションを使う必要はありません。

プロセスが完了してバックアップ アーティファクトが作成されれば、scp（セキュア コピー）ユーティリティを使用して、アーカイブを外部にコピーできます。特別な必要性がなければ、アーカイブを外部にコピーしたのち、アプライアンスからバックアップ アーカイブを削除してください。削除しない場合、次回に作成するバックアップ アーカイブにこのアーカイブが含まれます。

システムの復元

バックアップ ファイルからの復元は、アプライアンスが初期状態の場合、つまり設定が空の場合にだけ機能するようになっています。ポリシーが設定されていたり、初期状態からその他の変更が加えられているアプライアンスでは復元が機能しない場合もあります。ただし、アプライアンスのソフトウェア バージョン、ホットフィックス、SDK 拡張機能は、バックアップの作成にシステムが使用したものと同じでなければなりません。これらは、バックアップ復元コマンドを実行する前に、個別にインストールする必要があります。

さらに、アプライアンスは、バックアップ ファイルの作成にシステムが使用した動作モードと同じ動作モードでなければなりません。つまり、ソース システムが独立型モードで設定された場合、ターゲット システムも独立型モードに設定される必要があります。

これらの前提条件の確認後、次の手順でシステムを復元します。

ステップ 1　システムを復元するアプライアンスのアプライアンス シェルにアクセスします。

ステップ 2　[Advanced Options] > [Run Bash] の順に選択します。

ステップ 3　`backup` スクリプトを使用して、バックアップ ファイルからシステムを復元します。ファイルは、システム上、またはアプライアンスの OS からアクセス可能なディスク ロケーションに存在していなければなりません。

次に例を示します。

```
backup -restore <filename>
```

上記の filename は `backup` スクリプトで以前に保存された `tgz` ファイルの名前です。次に例を示します。

```
backup -restore -verbose applianceBackup.tgz
```

`-verbose` スイッチを指定すると、バックアップまたは復元のプロセス中に発生するエラー メッセージが画面に出力されます。

（注）　`backup -h` を入力すると、すべてのオプションのリストが表示されます。動作時のエラーを画面に出力するには、`-e` または `-l` のスイッチを使用します。

コマンドを入力すると、システムはファイルを読み取り、現在のシステムを上書きして、ファイル内に示されているアプライアンス状態にします。変更の適用後、アプライアンスはリブートします。再起動後のシステムは、バックアップ アーカイブから復元された状態になります。

ステップ 4　ターゲット アプライアンスのハードウェア システムが、ソース アプライアンスと異なる場合には、新しいアプライアンスにライセンスを設定して正常に動作できるようにする必要があります。ACE XML Gateway のライセンスは特定のマシンに関連付けられるため、個別に取得して各物理アプライアンスにインストールする必要があります。ライセンスの取得およびインストールに関する詳細については、「製品ライセンスの設定」（P.5-11）を参照してください。

アップデートの適用

シスコから ACE XML Gateway と Manager のソフトウェアのアップデートが発行される場合があります。これらのアップデートには、通常、セキュリティ強化、新機能または強化機能、バグ フィックスが含まれています。ソフトウェア アップデートについての情報は、シスコのサポート担当者にお問い合わせください。また、シスコのサポート用 Web サイトでもソフトウェア アップデート情報を調べることができます。

各ソフトウェアのアップデート パッケージには、そのリリース固有のインストレーションに関する説明が含まれています。アップグレード方法の詳細は、リリースによって異なる可能性があるので、アップデートを実行する際には、シスコのサポート担当者に問い合わせてください。

一般的に、アップデートを行うには次の手順を実行します。

1. アップデート ファイルを取得します。

   ソフトウェア用のアップデートを使用できる場合は、シスコのサポート担当者から必要なファイルを入手できます。ほとんどの場合、アップデート パッケージは、自動インストール パッケージとインストレーションに関する説明で構成されています。

2. アップデートに関する説明をすべて読みます。

   アップデート パッケージに添付されている説明書は、必ずすべてに目を通してください。アップグレード方法の細部は、そのアップデートによって影響を受ける機能により、リリースごとに異なる可能性があります。

3. アップデートのターゲット アプライアンスを準備します。

   アップデートを適用する前に、重要なファイルをバックアップし、作業ポリシー、必要なリソース、またはユーザ アカウントが失われないようにすることを推奨します。

   このようなバックアップは、Manager に対してだけでなく、各 ACE XML Gateway に対しても実行してください。重要なファイルのバックアップに関する詳細は、「システムのバックアップと復元」（P.11-3）を参照してください。

4. すべての ACE XML Gateway および Manager アプライアンスにアップデートを適用します。具体的な方法は、アップデート パッケージの付属資料を参照してください。

なんらかの理由で ACE XML Gateway のインスタンスを以前のバージョンのシステム ソフトウェアに復元する必要がある場合には、アップデート パッケージを入手し、ロールバックの実行に関する説明を参照します。

シリアル コンソールによるブート制御の設定

デフォルトでは、ほとんどのアプライアンスはシリアル コンソール アクセスをサポートし、接続の設定は 9600 bps、8 データ ビット、パリティなし、1 ストップ ビットです。

ただし、デフォルトでは、ブート メッセージはシリアル コンソールではなくビデオ コンソールに出力されます。ブート メッセージがシリアル コンソールに表示されるように設定を変更するには、次の手順を実行します。

ステップ 1　`root` ユーザとしてアプライアンス シェルにログインします。

ステップ 2　[Main Menu] から、[Advanced Options] の項目を選択します。

ステップ 3　[Advanced Options] から [Boot Settings] の項目を選択します。

ステップ 4　[Serial Port] の項目を選択して、起動時にブート出力がシリアル コンソールに表示されるようにします。

（注）　アプライアンスに直接接続されているか、または KVM スイッチを通じて接続されているキーボード、モニタ、マウスを使用する場合、[Console] の項目を選択します。

[Advanced Options] 画面が表示されます。新しい設定を有効にするためには、アプライアンスをリブートする必要があります。

ステップ 5　[Advanced Options] から、[Return to Main Menu] を選択します。

ステップ 6　[Main Menu] から、[Shutdown/Reboot] の項目を選択します。

ステップ 7　[Shutdown/Reboot] 画面で、[Reboot] を選択します。

ステップ 8　選択を確認するように求めるプロンプトが表示されます。[Yes] を選択して、アプライアンスを新しい設定で再起動します。

アプライアンスににシリアル ケーブルが接続されている場合は、そのケーブルがアプライアンスに搭載されているカードではなく、アプライアンスのシリアル インターフェイスに接続されていることを確認してください。とくに、アプラインスとともに出荷される nCipher カードには、nCipher カード リーダ専用のシリアル ポートがあります。端末セッションはサポートしていません。

ディスク容量が不足している場合の復元

アプライアンスに不測のシャットダウンが発生した場合は、ディスク容量が足りない可能性があります。デフォルトでは、ディスク使用量が設定したしきい値を超えるとログ ファイルが削除されます。ただし場合によっては、とくに大量のメッセージ トラフィックを処理している場合には、ディスク容量が上限に達してしまう可能性があります。

ACE XML Gateway および Manager は使用可能なディスク容量がディスク容量全体の 10 パーセント未満になると、シャットダウンするように設計されています。ディスク容量不足でアプライアンスがシャットダウンした場合、そのアプライアンスを再起動するには、ディスクの空き容量が必要です。

ディスク容量の上限に達したことが原因で Manager がシャットダウンした場合は、これ以降スペースが確保されるまで正常には起動しません （この動作はハード ドライブのスペース不足によるポリシーの破損エラーを防止します）。この状態で Manager を起動しようとすると、「Starting ACE XML Manager: ACE XML Gateway console: detected full disk, cannot start」というメッセージが表示されます。

（注）　メモリの使用量が指定したしきい値を超えた場合にも ACE XML Gateway はシャットダウンします。ただし、その場合には、アプライアンスは自動的に復元されます。

ディスク容量不足でシャットダウンしたアプライアンスを復元するには、次の手順を実行します。

ステップ 1　SSH を使用してアプライアンスに接続し、root ユーザとしてログインします。

（注）　ディスク容量不足により他のプロセスがシャットダウンしてしまった場合でも、アプライアンスは SSH 接続を引き続き許可します。

ステップ 2　[Main Menu] から、[Advanced Options] > [Run Bash] の順に選択します。

ステップ 3　`df` コマンドを使用すると、ディスク容量が不足しているかどうか確認できます。このコマンドを実行すると、使用済みのディスク容量と空きディスク容量が表示されます。

ステップ 4　ディスクから不要なファイルを削除します。削除するファイルの詳細については、シスコのサポート担当者に問い合わせてください。必要な場合には、最初に `scp`、`cp`、または別のコピー ツールを使用してファイルを削除する前に別の場所にコピーします。

ステップ 5　Bash シェルで `exit` を入力してメニューに戻ってから、該当するメニュー オプションを選択して、[Main Menu] に戻ります。

ステップ 6　[Manage Gateway Processes] メニューで、次のいずれかを選択し、アプライアンスを再起動します。

- [Start Gateway]
- [Start Manager]
- [Restart All Configured Services]（Gateway がユーザ環境で動作している状態でこのオプションを選択すると、Gateway が再起動し、これがネットワーク トラフィックの停止につながる場合があります）

ディスク容量の上限に達してしまった場合には、自動ログ ファイル消去を制御する設定を確認する必要があります。これを実行するには、Manager の Web コンソールで [Gateway Settings] ページを開きます。このページは [System Management] ページからアクセスできます。適切な場合には、[Delete old log files when total message log disk usage exceeds] と表記されたオプションのサイズしきい値を下げます。このしきい値を超えると、削除されたログ ファイルの情報は失われてしまうことに注意してください。ユーザ環境でログ情報の保持が必要な場合には、定期的に自動でログをディスクから移動するスクリプトを使用する必要があります。

詳細については、Manager から使用できるオンライン ヘルプを参照してください。

システム パスワードの復元

ACE XML Gateway システムで管理インターフェイスにアクセスするためのパスワードは、必要に応じて再設定が可能です。次の手順では、アプライアンスのコンソールおよび Manager の Web コンソールにアクセスするためのパスワードを再設定する方法を説明しています。

コンソール アクセス用パスワード

アプライアンスのコンソール インターフェイスは、アプライアンスの初期動作およびネットワークの設定に使用します。コンソール インターフェイス アクセス用のユーザ アカウントには、組み込みユーザ アカウントの `root` と、`reactivity-operator-add` の手順で作成したカスタム アカウントが含まれます。

これらの 2 タイプの場合のパスワード再設定手順は、次の点で異なります。

カスタム ユーザ アカウントのパスワード再設定

カスタム ユーザ アカウントのパスワード（reactivity-operator-add の操作で作成したアカウント）は、`root` ユーザが `sudo passwd` コマンドを使用することで再設定できます。つまり、次の手順でアプライアンスの bash シェルから、`root` ユーザはユーザ アカウントのパスワードを変更できます。

sudo psswd <username>

コマンド入力後、ユーザのパスワード入力を要求するプロンプトが表示されます。

このコマンドは、ユーザがアクセスする各アプライアンスの bash シェルから実行する必要があります。

root ユーザ アカウントのパスワード再設定

root ユーザ アカウントのパスワードを再設定するには、アプライアンスへの物理的アクセスが必要です。さらに、アプライアンスをシャットダウンし、サービスを一時停止する必要があります。

手順を開始する前に、シリアルまたはビデオ接続により、コンソールをアプライアンスに接続します。

ステップ 1　可能な場合には、コンソールからシステムのリブートを開始します（CTRL+ALT+DEL キーを同時に押します）。この方法でリブートができない場合には、アプライアンスの電源を直接再度入れ直します。

（注）　アクティブなアプライアンスの電源を再度入れ直すと、まれにデータが壊れてしまう場合があることに十分注意してください。この操作を実行する前に、アプライアンスをバックアップしておくことを推奨します。

ステップ 2　アプライアンスがリブートする際、「GRUB Loading Stage 2」という GRUB メッセージに注意してください。これが表示されたら、すぐに Esc キーを押します。

底部に手順が表示されたボックスが画面に現れたら、次に進みます。これ以外の場合には、リブートのプロセスを繰り返します。

ステップ 3　次のキー操作を実行してコマンドを入力します。

a. レコードを編集するには、「e」を入力します。

b. カーソルを「kernel」の行に移動するには矢印キーを使用します。

c. kernel の行を編集するには、「e」を入力します。

d. 1 番を行の最後に追加するには、スペースに続いて 1 番（つまり「1」）を入力します。

e. 変更を確定するには、Enter キーを押します。

f. 「b」を入力して、変更した設定で起動し、シェル プロンプトが表示されるまで待ちます。

g. 「Y」を押してディスクの確認を実行するかどうかを尋ねられた場合には、ディスクの確認を実行することを推奨します。このプロセスにはさらに時間が必要です。

h. シェル プロンプトで、`passwd` コマンドを使用して root パスワードを変更します。

i. 新パスワードの入力後、「`reboot`」コマンドでリブートし、通常の動作を実行します。

システムの再起動後、新パスワードを使用して、root ユーザとしてログインできます。

Manager の Web コンソールのパスワード再設定

ACE Manager の Web コンソールで、管理者ユーザはカスタム ユーザ アカウントのパスワードをいつでも変更できます。管理者は [User Administration] ページでユーザ アカウントを編集することで変更を実行できます。ただし、組み込み管理者アカウントのパスワードを変更するには、次に説明する手順を実行する必要があります。

（注）　次の手順は、外部の LDAP または RADIUS システムにより検証される Manager ユーザ アカウントの場合には該当しません。LDAP または RADIUS の許可モードを使用している場合には、外部システムを使用してパスワードを再設定する必要があります。

Manager が管理する各クラスタには、明確な管理者アカウントが存在していることに注意してください。複数のクラスタを管理する Manager インスタンスの管理者パスワードを再設定する際には、パスワードの再設定が必要なクラスタを把握する必要があります。

ステップ 1　この手順を開始する前に、アプライアンスのコンソール メニューから Manager をシャットダウンします（[Main Menu] から [Manage Gateway Processes]、[Stop Manager] の順に選択します）。

ステップ 2　Manager アプライアンスの bash シェルにアクセスし、再設定が必要なクラスタのファイルストアを探します。ファイルストアは次の場所にあります。

- バージョン 5.0.x 以前では、/usr/local/reactivity/console_documents/filestore にあります。
- バージョン 5.1 以降では、/var/lib/reactivity/console_documents/cluster<cluster_id>/filestore にあります。

  ここで、<cluster_id> はクラスタを内部で識別する一意のストリングです。

（注）　クラスタ ID の決定に関する詳細については、「設定データの概要」（P.13-3）を参照してください。

ファイル `00/00/000000000003.00000000` の内容を下記のテキストに置き換えてください。

```
<object type="user">
 <AccessControlRole>true</AccessControlRole>
 <ActiveGroupID>
  <ID>0000000000000004</ID>
 </ActiveGroupID>
 <ConsoleAdminRole>true</ConsoleAdminRole>
 <ExternalDeveloperRole>true</ExternalDeveloperRole>
 <FailedLoginCount>0</FailedLoginCount>
 <HashedPassword>mcVyzSCfpKjxx4W9KugFFPYPSB8=</HashedPassword>
 <IsDisabled>false</IsDisabled>
 <IsOperator>true</IsOperator>
 <MessageTrafficLogRole>true</MessageTrafficLogRole>
 <OperationsRole>true</OperationsRole>
 <PolicyViewRole>true</PolicyViewRole>
 <RoutingRole>true</RoutingRole>
 <Username>administrator</Username>
</object>
```

これで管理者パスワードを出荷時のデフォルトに再設定できました。

ステップ 3　Manager プロセスを起動します。

ステップ 4　パスワード `swordfish` を使用して、`administrator` ユーザとして Web コンソールにログインします。ログイン後、必ず管理者パスワードを出荷時のデフォルトから変更してください。

MTA ポストマスタ アドレスの変更

ACE XML Gateway は、一定のサービス タイプの SMTP トラフィックを受信します。たとえば、電子メール添付として渡された ebXML コンテンツの処理と検証を実行できます。Gateway で ebXML サービスの処理を使用するには、Manager の Web コンソールで ebXML ベースのサービス定義を設定します。

（注）　ebXML 機能は Cisco ACE XML Gateway のライセンスを付与された製品以外では使用できないため、Cisco ACE Web Application Firewall ではこの機能を使用できません。

Gateway の SMTP サーバはリレーとしては機能しません。受け入れるのはローカル アドレスへの着信メッセージと Gateway からの発信メッセージだけです。SMTP サーバは一時的な障害の影響を受けたメッセージの再送信を定期的に試行します。MTA は SSL による SMTP や SMTP 内の TLS はサポートしていません。

ebXML サービスがポリシーに追加されると、アプライアンスはポート 25 を開いて SMTP トラフィックを処理します。それ以降、ACE XML Gateway MTA はそのポストマスタ メールボックスに電子メールを受信できます。

ポストマスタ アドレスは、MTA の標準管理アドレスです（SMTP プロトコルに必要）。このアドレスは、Gateway の着信トラフィックと発信トラフィックのいずれにも影響を与えません。

必要な場合、ポストマスタへのメールが別の場所に送信されるようにアドレスを変更することも可能です。デフォルトのままにしておく場合、ポストマスタ メールボックスは ACE XML Gateway の root ユーザのメールボックスになります。

既存のアドレスを変更するには、次の手順を実行します。

ステップ 1　`root` ユーザとして、Gateway アプライアンスのシェル インターフェイスにログインします。

ステップ 2　[Main Menu] から、[Advanced Options] の項目を選択します。

ステップ 3　[Advanced Options] で、[MTA Configuration] を選択します。

ステップ 4　[Configure postmaster address] の項目を選択します。

ステップ 5　管理情報の宛先とする電子メール アドレスを入力します。

ステップ 6　完了したら、[MTA Menu] から、[Advanced Options] メニューに戻ります。

クラスタ内の各 Gateway に対して、この手順を実行します。