Amazon Web Services（AWS）EC2/VPC の導入

Amazon Web Services（AWS）の Amazon Elastic Compute Cloud（EC2）への Cisco Web セキュリティ仮想アプライアンスおよびセキュリティ管理仮想アプライアンスの導入ガイドを参照してください。

仮想アプライアンスのライセンスファイルのインストール

（注） 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとに次の手順を実行します。

始める前に

（任意）ライセンスファイルをアップロードする仮想アプライアンスへの FTP 接続を実行します。端末にライセンスを貼り付ける場合は、この作業を行う必要はありません。

ステップ 1 端末アプリケーションの SSH または Telnet を使用して、admin/ironport ユーザとしてアプライアンスの CLI にログインします。

（注） vSphere クライアントコンソールを使用して CLI にライセンスファイルの内容を貼り付けることはできません。

ステップ 2 **loadlicense** コマンドを実行します。

ステップ 3 次のいずれかのオプションを使用してライセンスファイルをインストールします。

- オプション 1 を選択して、端末にライセンスファイルの内容を貼り付けます。
- すでに FTP を使用してライセンスファイルをアプライアンスの **configuration** ディレクトリにアップロードした場合は、オプション 2 を選択して、ライセンスファイルを **configuration** ディレクトリにロードします。

ステップ 4 ライセンス契約を読み、同意します。

ステップ 5 （任意）**showlicense** を実行して、ライセンスの詳細を見直します。

次のタスク

Microsoft Hyper-V の導入の場合

- 「Microsoft Hyper-V への導入」に戻ります。

KVM の導入の場合

- 「KVM での導入」に戻ります。

ESXi の導入の場合

- 管理インターフェイスの IP アドレスの詳細については、「VMWare ESXi での導入」を参照してください。
- 仮想セキュリティ アプライアンス イメージのクローンを作成した場合は、イメージごとにこのトピックの手順を繰り返します。
- 「VMWare ESXi での導入」の残りのセットアップ手順を参照してください。

別の物理ホストへの仮想アプライアンスの移行

VMware® VMotion™ を使用して、実行中の仮想アプライアンスを別の物理ホストに移行できます。

要件：

- 両方の物理ホストのネットワーク構成が同じである必要があります。
- 両方の物理ホストに、仮想アプライアンスのインターフェイスがマップされているものと同じ定義済みのネットワークへのアクセス権がなければなりません。
- 両方の物理ホストに、仮想アプライアンスで使用するデータストアへのアクセス権がなければなりません。このデータストアには、ストレージ エリア ネットワーク（SAN）またはネットワーク接続ストレージ（NAS）が有効です。
- Cisco Secure Email Virtual Gateway のキューにはメールが含まれていない必要があります。

（注） VMotion のマニュアルを参考にして、仮想マシンを移行します。現在、自動 VMotion は Secure Web Appliance ではサポートされていません。

すでに使用中の仮想アプライアンスのクローン作成

始める前に

- 仮想マシンのクローンを作成する手順の詳細については、http://www.vmware.com/support/ws55/doc/ws_clone.html [英語] にある VMware の技術文書を参照してください。
- ご使用のアプライアンスのネットワーク設定およびセキュリティ機能の管理方法については、Cisco Secure 製品およびリリースのユーザーガイドを参照してください。

ステップ 1 Cisco Secure Email Virtual Gateway のクローンを作成する場合：

CLI で **suspend** コマンドを使用してアプライアンスを一時停止し、アプライアンスがキュー内のすべてのメッセージを配信するのに十分な遅延期間を入力します。

ステップ 2 セキュリティ管理仮想アプライアンスのクローンを作成する場合：

管理対象となる E メールおよび Web セキュリティアプライアンスの集約管理サービスを無効にします。

ステップ 3 CLI で **shutdown** コマンドを実行して、仮想アプライアンスをシャット ダウンします。

ステップ 4 仮想アプライアンスイメージのクローンを作成します。

ステップ 5 VMware vSphere Client を使用してクローンを作成したアプライアンスを起動し、次を実行します。

1. Cisco.com からダウンロードした未変更の .OVF イメージファイルではなく、構成済みのイメージのクローンを作成した場合：

   — クローン作成された仮想アプライアンスにライセンスファイルをインストールします。

   — クローン作成された仮想アプライアンスのネットワーク設定を変更します。

   電源投入時に、ネットワーク アダプタは自動的に接続しません。IP アドレス、ホスト名、および IP アドレスを再設定します。次に、ネットワークアダプタの電源を入れます。

   設定は、機能キーをインストールするまで完了しません。

2. クローン作成された Cisco Secure Email Virtual Gateway アプライアンスの場合：

   — 隔離されたすべてのメッセージを削除します。

   — メッセージトラッキングおよびレポーティングのデータを削除します。

3. クローン作成された Web セキュリティ仮想アプライアンスの場合：

— プロキシキャッシュを消去します。

— CLI で **authcache > flushall** コマンドを使用してプロキシ認証キャッシュを消去します。

— CLI で **diagnostic > reporting > flushall > deletedb** コマンドを使用して、レポーティングおよびトラッキングのデータを削除します。

—システムセットアップウィザード（SSW）を実行します。ライセンスが使用可能になっている必要があります。

— 認証レルムの場合は、ドメインに再参加します。

— 認証の設定の場合は、リダイレクトホスト名を変更します。

— 元の仮想アプライアンスがセキュリティ管理アプライアンスで管理されている場合は、クローン作成されたアプライアンスをセキュリティ管理アプライアンスに追加します。

ステップ 6 VMware vSphere クライアントを使用して元の仮想アプライアンスを起動して、動作を再開します。正常に動作していることを確認します。

ステップ 7 クローン作成されたアプライアンスで動作を再開します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。