ハードウェアESA/SMAを仮想ESA/SMAに移行するためのベストプラクティスを理解する

内容

はじめに

このドキュメントでは、ハードウェアESA/SMAから仮想ESA/SMAへの導入、移行、および設定に関するベストプラクティスについて説明します。

重要なステップ

ステップ 1：仮想ESAイメージのダウンロードとVMの導入

設定を移行する前に、ハードウェアと同じAsyncOSバージョンで仮想Secure Email Gateway(ESA)/セキュリティ管理アプライアンス(SMA)を実行することをお勧めします。アプライアンスで実行しているバージョンに最も近いAsyncOSリリースを選択し、必要に応じてその後でアップグレードするか、またはAsyncOSの最新バージョンをダウンロードできます。

これらのプラットフォーム(Microsoft Hyper-V、キーボード/ビデオ/マウス(KVM)、およびVMWare ESXi)への導入がサポートされます。詳細については、インストレーションガイド(https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S照してください。

仮想イメージは、https://software.cisco.com/download/home/284900944/type/282975113/release/15.0.0からダウンロードできます。

ステップ 2：仮想ESA/SMAのライセンスの取得

仮想ESA/SMAをアップグレードできるようにするには、まずライセンスをインストールする必要があります。ハードウェアの既存のライセンスを新しい仮想ESAと共有できます（両方のESAを同時に実行できます）。

従来のライセンスの場合、vESA/vSMAの物理ライセンスが正常に共有され、ライセンスを受け取ったら、NotePad++またはWordPadで受け取った.XMLファイルを開きます。allを選択し、loadlicenseコマンドを使用してvESA/vSMA CLI経由でコピー/ペーストします。詳細については、https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.htmlを参照してください。

スマートライセンスの場合、スマートアカウントに新しいvESA/vSMAを追加し、トークンが生成されたら、記事https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214614-smart-licensing-overview-and-best-practi.htmlに記載されているプロセスに従ってデバイスを登録します。

ステップ 3：仮想ESA/SMAをハードウェアESA/SMAの正確なAsyncOSバージョンにアップグレードする（必要な場合）

ハードウェアと仮想アプライアンスは、移行前に同じバージョンである必要があります。ESAを適切なバージョンにアップグレードするために、記載されたリンクでSMAとESAの互換性マトリクスを確認できます
：https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html

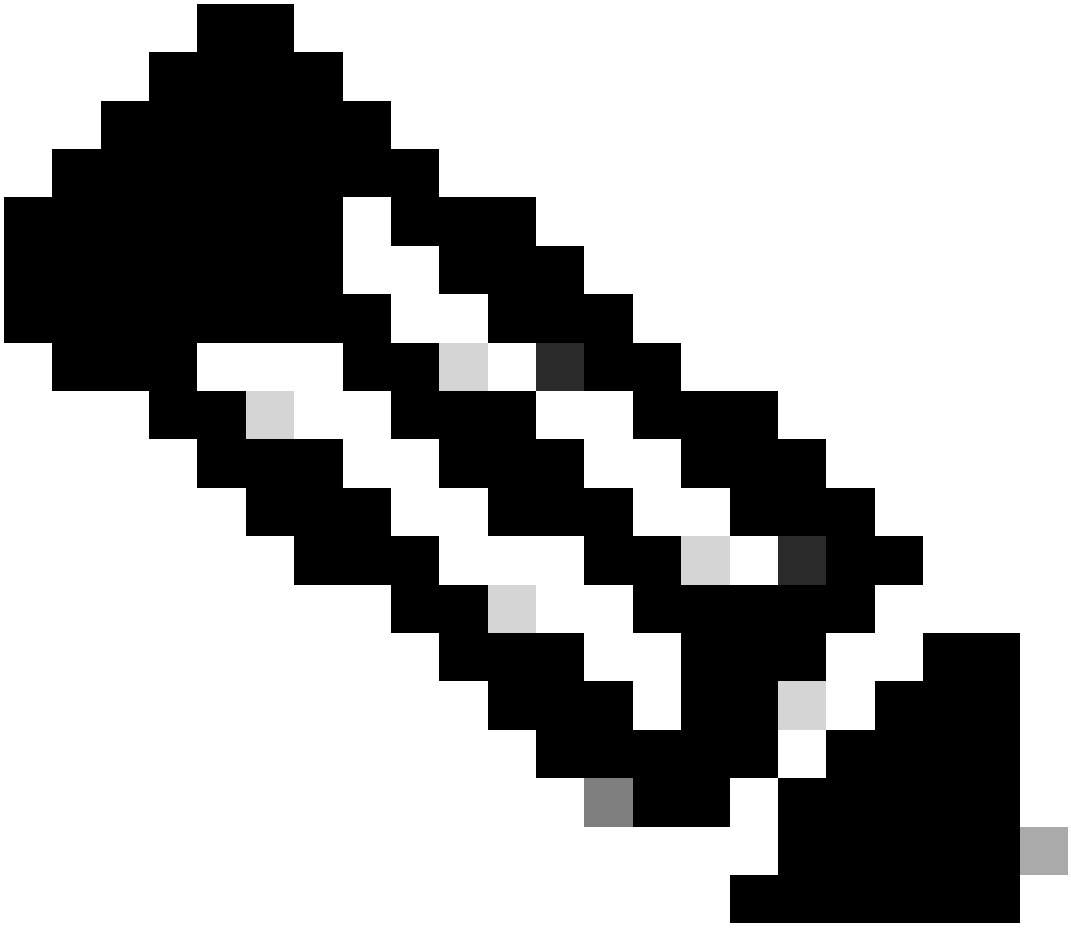
ステップ 4：ハードウェアESA/SMAから仮想ESA/SMAへの既存の設定の移行

仮想ESA/SMAは次のように設定できます。

- 既存のハードウェアがサポート終了(EOL)/サポート終了(EOS)またはアップグレードされたvESA/SMAイメージがインストールされている場合、または複数のデバイスを設定する必要がある場合は、デバイスを最初から設定します。

- ハードウェアデバイスがすでにクラスタ内にある場合は、新しいvESA/vSMAをクラスタに追加します。新しいデバイスは、クラスタから既存の設定のコピーを取得します。

- ハードウェアデバイスがスタンドアロンデバイスの場合、クラスタ設定を有効にし、新しい仮想ESA/SMAをクラスタに追加して、既存の設定のコピーを取得します。



注：仮想ESA/SMAが現在の設定を取得したら、要件に基づいてデバイスをクラスタから切断するか、そのまま維持するかを選択できます。ハードウェアデバイスをクラスタ構成から削除し、使用停止にすることができます。

ステップ 5：仮想ESA/SMAの更新されたサーバの修正

仮想ESA/SMAとハードウェアESA/SMAは異なるアップグレードサーバを使用し、設定の移行後にサーバが変更されます。vESA/vSMAをさらにアップグレードするには、vESA/vSMA CLIから次の手順でサーバを修正できます。

- updateconfigコマンドを実行し、次にサブコマンドdynamichostを実行します。
- サーバをupdate-manifests.sco.cisco.com:443に変更します。

- 変更を保存します。

移行に関するFAQについては、https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/215466-esa-sma-virtual-deployment-faq.pdfを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。