Cisco 適応型セキュリティ仮想アプライアンス(ASAv)クイック スタート ガイド

バージョン 9.4

発行日:2015 年 5 月 12 日
改訂日:2015 年 8 月 31 日

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco ASAv の概要

Cisco 適応型セキュリティ仮想アプライアンス（ASAv）は、仮想化環境に包括的なファイアウォール機能を提供し、データセンター トラフィックとマルチテナント環境のセキュリティを強化します。

ASDM または CLI を使用して、ASAv を管理およびモニタすることができます。その他の管理オプションを使用できる場合もあります。

ASAv の前提条件

ハイパーバイザのサポートについては、『Cisco ASA Compatibility』を参照してください。

ASAv のガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

フェールオーバーのガイドライン

フェールオーバー配置の場合は、スタンバイ装置が同じモデル ライセンスを備えていることを確認してください（たとえば、両方の装置が ASAv30s であることなど）。

サポートしない ASA 機能

ASAv は、次の ASA 機能をサポートしません。

- クラスタ
- マルチ コンテキスト モード
- アクティブ/アクティブ フェールオーバー
- EtherChannel
- AnyConnect Premium（共有）ライセンス

ASAv のライセンス

ASAv は Cisco Smart Software Licensing を使用します。詳細については、「Smart Software Licensing for the ASAv（ASAv の Smart Software Licensing）」を参照してください。

モデル	ライセンス要件
ASAv5	標準ライセンス 次の仕様を参照してください。 ■ 100 Mbps スループット ■ 1 vCPU ■ 2 GB のメモリ ■ 100,000 の同時ファイアウォール接続 ■ AWS はサポート対象外
ASAv10	標準ライセンス 次の仕様を参照してください。 ■ 1 Gbps スループット ■ 1 vCPU ■ 2 GB のメモリ ■ 100,000 の同時ファイアウォール接続 ■ AWS をサポート
ASAv30	標準ライセンス 次の仕様を参照してください。 ■ 2 Gbps スループット ■ 4 vCPU ■ 8 GB RAM ■ 500,000 の同時ファイアウォール接続 ■ AWS をサポート

注：ASAv にスマート ライセンスをインストールする必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。スマート ライセンスは、通常の操作に必要です。

ASAv インターフェイスおよび仮想 NIC

ASAv は、仮想プラットフォーム上のゲストとして、基盤となる物理プラットフォームのネットワーク インターフェイスを利用します。ASAv の各インターフェイスは仮想 NIC（vNIC）にマッピングされます。

■ ASAv インターフェイス、5 ページ
■ サポートされる vNIC、5 ページ

ASAv インターフェイス

ASAv は、次のギガビット イーサネット インターフェイスがあります。

- Management 0/0
- GigabitEthernet 0/0 ～ 0/8。ASAv をフェールオーバー ペアの一部として展開する場合は GigabitEthernet 0/8 がフェールオーバー リンクに使用されることに注意してください。

サポートされる vNIC

ASAv は次の vNIC をサポートします。

vNIC のタイプ	ハイパーバイザのサポート		ASAv のバージョン	注意
	VMware	KVM		
e1000	あり	あり	9.2(1) 以降	VMware のデフォルト。
Virtio	なし	あり	9.3(2.200) 以降	KVM のデフォルト。

ASAv インターフェイスおよび仮想 NIC

VMware を使用した ASAv の導入

VMware を使用して ASAv を導入できます。

ASAv の VMware 機能のサポート

次の表に、ASAv の VMware 機能のサポートを示します。

表 1　ASAv の VMware 機能のサポート

機能	説明	サポート（あり / なし）	注記
コールド クローン	クローニング中に VM の電源がオフになります。	あり	–
DRS	動的リソースのスケジューリングおよび分散電源管理に使用されます。	あり	VMware のガイドラインを参照してください。
ホット追加	追加時に VM が動作しています。	なし	–
ホット クローン	クローニング中に VM が動作しています。	なし	–
ホット リムーブ	取り外し中に VM が動作しています。	なし	–
スナップショット	VM が数秒間フリーズします。	あり	使用には注意が必要です。トラフィックが失われる可能性があります。フェールオーバーが発生することがあります。
一時停止と再開	VM が一時停止され、その後再開します。	あり	–
vCloud Director	VM の自動配置が可能になります。	なし	–
VM の移行	移行中に VM の電源がオフになります。	あり	–
VMotion	VM のライブ マイグレーションに使用されます。	あり	–
VMware FT	VM の HA に使用されます。	なし	ASAv VM の障害に対して ASAv のフェールオーバーを使用します。

表 1　ASAv の VMware 機能のサポート（続き）

機能	説明	サポート（あり / なし）	注記
VMware HA	ESX およびサーバの障害に使用されます。	あり	ASAv VM の障害に対して ASAv のフェールオーバーを使用します。
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	ASAv VM の障害に対して ASAv のフェールオーバーを使用します。
VMware vSphere スタンドアロン Windows クライアント	VM を導入するために使用されます。	あり	–
VMware vSphere Web Client	VM を導入するために使用されます。	あり	–

ASAv と VMware の前提条件

VMware vSphere Web クライアント、vSphere スタンドアロン クライアント、または OVF ツールを使用して ASAv を導入できます。システム要件については、『Cisco ASA Compatibility』を参照してください。

vSphere 標準スイッチのセキュリティ ポリシー

vSphere スイッチについては、レイヤ 2 セキュリティ ポリシーを編集して、ASAv インターフェイスによって使用されるポート グループに対しセキュリティ ポリシーの例外を適用できます。次のデフォルト設定を参照してください。

- 無差別モード：**拒否**
- MAC アドレスの変更：**許可**
- 不正送信：**許可**

次の ASAv 設定については、これらの設定の変更が必要な場合があります。詳細については、vSphere のマニュアルを参照してください。

表 2　ポート グループのセキュリティ ポリシーの例外

セキュリティの例外	ルーテッド ファイアウォール モード		トランスペアレント ファイアウォール モード	
	フェールオーバーなし	フェールオーバー	フェールオーバーなし	フェールオーバー
無差別モード	<任意>	<任意>	承認	承認
MAC アドレスの変更	<任意>	承認	<任意>	承認
不正送信	<任意>	承認	承認	承認

ASAv および VMware のガイドライン

OVF ファイルのガイドライン

導入対象に基づいて、asav-vi.ovf ファイルまたは asav-esxi.ovf ファイルを選択します。

- asav-vi：vCenter に導入する場合
- asav-esxi：ESXi に導入する場合（vCenter なし）

フェールオーバーのガイドライン

フェールオーバー配置の場合は、スタンバイ装置が同じモデル ライセンスを備えていることを確認してください（たとえば、両方の装置が ASAv30s であることなど）。

IPv6 のガイドライン

VMware vSphere Web クライアントを使用して ASAv OVF ファイルを最初に導入する場合は、管理インターフェイスに IPv6 アドレスを指定できません。ASDM または CLI を使用して、IPv6 アドレッシングを後で追加できます。

その他のガイドラインと制限事項

- ASAv OVF の導入は、ローカリゼーション（非英語モードでのコンポーネントのインストール）をサポートしません。ご自身の環境の VMware vCenter と LDAP サーバが ASCII 互換モードでインストールされていることを確認してください。
- ASAv をインストールして VM コンソールを使用する前に、キーボードを [United States English] に設定する必要があります。
- ASAv に割り当てられたメモリのサイズは、スループット レベルに合わせたものです。異なるスループット レベルのライセンスを要求する場合を除いて、[Edit Settings] ダイアログボックスのメモリ設定または vCPU ハードウェア設定は変更しないでください。アンダープロビジョニングの場合、パフォーマンスに影響する場合があり、オーバープロビジョニングの場合、ASAv によりリロードが行われることが警告されます。待機期間（100 ～ 125% のオーバープロビジョニングの場合は 24 時間、125% 以上の場合は 1 時間）の後、ASAv はリロードします。

  注：メモリまたは vCPU ハードウェア設定を変更する必要がある場合は、ASAv のライセンス、4 ページに記載されている値のみを使用してください。VMware が推奨するメモリ構成の最小値、デフォルト値、および最大値は使用しないでください。

  リソース割り当てとオーバープロビジョニングまたはアンダープロビジョニングされたリソースを表示するには、ASAv の **show vm** コマンドおよび **show cpu** コマンドか、ASDM の [Home] > [Device Dashboard] > [Device Information] > [Virtual Resources] タブまたは [Monitoring] > [Properties] > [System Resources Graphs] > [CPU] ペインを使用します。

- ASAv の導入時に、ホスト クラスタがある場合は、ストレージをローカルに（特定のホスト上）または共有ホスト上でプロビジョニングできます。しかし、ASAv を vMotion で別のホストに移行する場合は、いかなるタイプのストレージ（SAN またはローカル）を使用しても接続の中断が発生します。
- ESXi 5.0 を実行している場合、vSphere Web クライアントは ASAv OVF の導入ではサポートされません。代わりに、vSphere クライアントを使用してください。

ASAv ソフトウェアの開梱と VMware 対応第 0 日用コンフィギュレーション ファイルの作成

ASAv を起動する前に、第 0 日（Day 0）用のコンフィギュレーション ファイルを準備できます。このファイルは、ASAv の起動時に適用される ASAv の設定を含むテキスト ファイルです。この初期設定は、「day0-config」というテキスト ファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。第 0 日用コンフィギュレーション ファイルには、少なくとも、管理インターフェイスをアクティブ化するコマンドと、公開キー認証用 SSH サーバをセットアップするコマンドを含める必要がありますが、すべての ASA 設定を含めることもできます。空の day0-config を含むデフォルトの day0.iso がリリースとともに提供されています。day0.iso ファイル（カスタム day0 またはデフォルトの day0.iso）は、最初の起動中に使用できなければなりません。

注：初期導入時に自動的に ASAv をライセンス許諾するには、Cisco Smart Software Manager からダウンロードした Smart Licensing Identity（ID）トークンを「idtoken」というテキスト ファイルに格納し、第 0 日用コンフィギュレーション ファイルと同じディレクトリに保存します。

注：トランスペアレント モードで ASAv を導入する場合は、トランスペアレント モードで実行される既知の ASA コンフィギュレーション ファイルを第 0 日用コンフィギュレーション ファイルとして使用します。これは、ルーテッド ファイアウォールの第 0 日用コンフィギュレーション ファイルには該当しません。

注：この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

手順

1. ZIP ファイルを Cisco.com からダウンロードし、ローカル ディスクに保存します。

   http://www.cisco.com/go/asa-software

   注：Cisco.com のログインおよびシスコ サービス契約が必要です。

2. ファイルを作業ディレクトリに解凍します。ディレクトリからファイルを削除しないでください。次のファイルが含まれています。

   - asav-vi.ovf：vCenter への導入用。
   - asav-esxi.ovf：vCenter 以外への導入用。
   - boot.vmdk：ブート ディスク イメージ。
   - disk0.vmdk：ASAv のディスク イメージ。
   - day0.iso：day0-config ファイルおよびオプションの idtoken ファイルを含む ISO。
   - asav-vi.mf：vCenter への導入用のマニフェスト ファイル。
   - asav-esxi.mf：vCenter 以外への導入用のマニフェスト ファイル。

3. 「day0-config」というテキスト ファイルに ASAv の CLI 設定を記入します。3 つのインターフェイスの設定とその他の必要な設定を追加します。

   最初の行は ASA のバージョンで始める必要があります。day0-config は、有効な ASA 構成である必要があります。day0-config を生成する最適な方法は、既存の ASA または ASAv から実行コンフィギュレーションの必要な部分をコピーすることです。day0-config 内の行の順序は重要で、既存の show run コマンド出力の順序と一致している必要があります。

   例：

```
ASA Version 9.4.1
!
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

4. (任意)Cisco Smart Software Manager により発行された Smart License ID トークン ファイルをコンピュータにダウンロードします。
5. (任意)ダウンロード ファイルから ID トークンをコピーし、ID トークンのみを含む「idtoken」というテキスト ファイルに保存します。

   この ID トークンによって、Smart Licensing サーバに ASAv が自動的に登録されます。
6. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

7. day0.iso 用に Linux で新しい SHA1 値を計算します。

```
openssl dgst -sha1 day0.iso
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
```

8. 新しいチェックサムを作業ディレクトリの asav-vi.mf ファイルに含め、day0.iso SHA1 値を新しく生成された値で置き換えます。

   Example.mf ファイル

```
SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

9. ZIP ファイルを解凍したディレクトリに day0.iso ファイルをコピーします。デフォルト(空)の day0.iso ファイルが上書きされます。

   このディレクトリから VM が導入される場合は、新しく生成された day0.iso 内の構成が適用されます。

VMware vSphere Web Client を使用した ASAv の導入

この項では、VMware vSphere Web Client を使用して ASAv を導入する方法について説明します。Web クライアントには、vCenter が必要です。vCenter がない場合は、VMware vSphere スタンドアロン クライアントおよび第 0 日用構成を使用した ASAv の導入、16 ページまたは OVF ツールおよび第 0 日用構成を使用した ASAv の導入、17 ページを参照してください。

vSphere Web Client へのアクセスとクライアント統合プラグインのインストール

この項では、vSphere Web Client にアクセスする方法について説明します。また、ASAv コンソール アクセスに必要なクライアント統合プラグインをインストールする方法についても説明します。一部の Web クライアント機能（プラグインなど）は、Macintosh ではサポートされていません。完全なクライアントのサポート情報については、VMware の Web サイトを参照してください。

手順

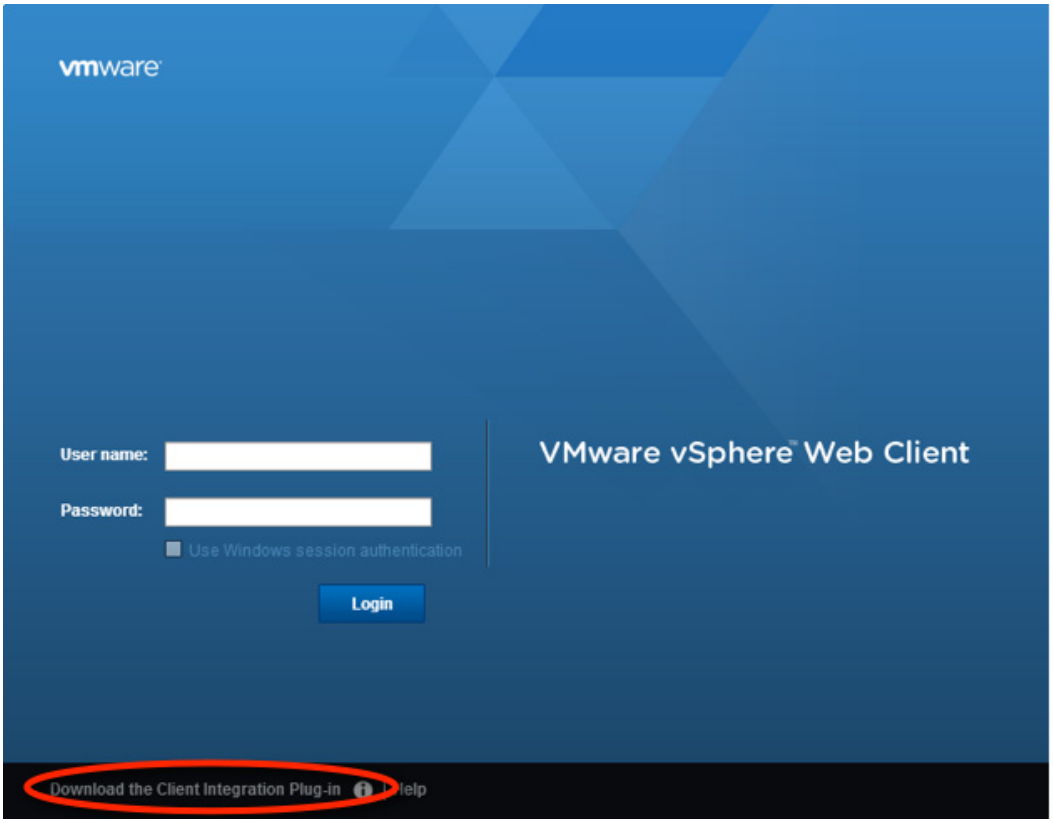
1. ブラウザから VMware vSphere Web Client を起動します。

   https://*vCenter_server*:*port*/**vsphere-client/**

   デフォルトでは、port は 9443 です。

2. （1 回のみ）ASAv コンソールへのアクセスを可能にするため、クライアント統合プラグインをインストールします。

   a. ログイン画面で、[Download the Client Integration Plug-in] をクリックしてプラグインをダウンロードします。



   b. ブラウザを閉じてから、インストーラを使用してプラグインをインストールします。

   c. プラグインをインストールしたら、vSphere Web Client に再接続します。

3. ユーザ名とパスワードを入力し、[Login] をクリックするか、[Use Windows session authentication] チェックボックスをオンにします（Windows のみ）。

VMware vSphere Web Client を使用した ASAv の導入

ASAv を導入するには、VMware vSphere Web クライアント（または vSphere クライアント）、およびオープン仮想化フォーマット（OVF）のテンプレート ファイルを使用します。シスコの ASAv パッケージを展開するには、vSphere Web クライアントで [Deploy OVF Template] ウィザードを使用します。このウィザードは、ASAv OVF ファイルを解析し、ASAv を実行する仮想マシンを作成して、パッケージをインストールします。

ウィザードの手順のほとんどは、VMware に対し標準のものです。Deploy OVF Template の詳細については、VMware vSphere Web Client のオンライン ヘルプを参照してください。

はじめる前に

ASAv を導入する前に、vSphere（管理用）で少なくとも 1 つのネットワークを設定しておく必要があります。

手順

1. ASAv ZIP ファイルを Cisco.com からダウンロードし、PC に保存します。

   http://www.cisco.com/go/asa-software

   注：Cisco.com のログインおよびシスコ サービス契約が必要です。

2. vSphere Web Client の [Navigator] ペインで、[vCenter] をクリックします。
3. [Hosts and Clusters] をクリックします。
4. ASAv を導入するデータセンター、クラスタ、またはホストを右クリックして、[Deploy OVF Template] を選択します。

   [Deploy OVF Template] ウィザードが表示されます。

5. ウィザード画面の指示に従って進みます。
6. [Setup networks] 画面で、使用する各 ASAv インターフェイスにネットワークをマッピングします。

   ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、[Edit Settings] ダイアログボックスからネットワークを後で変更できます。導入後、ASAv インスタンスを右クリックし、[Edit Settings] を選択して [Edit Settings] ダイアログボックスにアクセスします。ただし、この画面には ASAv インターフェイス ID は表示されません（ネットワーク アダプタ ID のみ）。次のネットワーク アダプタ ID と ASAv インターフェイス ID の対応一覧を参照してください。

ネットワーク アダプタ ID	ASAv インターフェイス ID
ネットワーク アダプタ 1	Management0/0
ネットワーク アダプタ 2	GigabitEthernet0/0
ネットワーク アダプタ 3	GigabitEthernet0/1
ネットワーク アダプタ 4	GigabitEthernet0/2
ネットワーク アダプタ 5	GigabitEthernet0/3
ネットワーク アダプタ 6	GigabitEthernet0/4
ネットワーク アダプタ 7	GigabitEthernet0/5
ネットワーク アダプタ 8	GigabitEthernet0/6
ネットワーク アダプタ 9	GigabitEthernet0/7
ネットワーク アダプタ 10	GigabitEthernet0/8

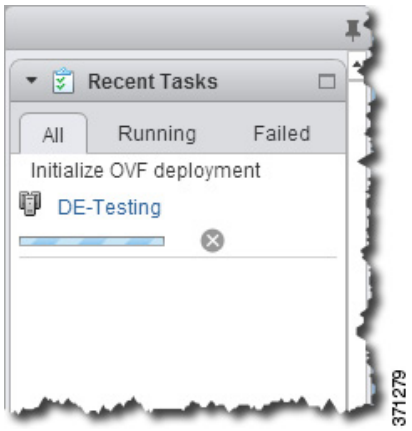
すべての ASAv インターフェイスを使用する必要はありません。ただし、vSphere Web Client ではすべてのインターフェイスにネットワークを割り当てる必要があります。使用しないインターフェイスについては、ASAv 設定内でインターフェイスを無効のままにしておくことができます。ASAv を導入した後、任意で vSphere Web Client に戻り、[Edit Settings] ダイアログボックスから余分なインターフェイスを削除することができます。詳細については、vSphere Web Client のオンライン ヘルプを参照してください。

注: フェールオーバー/HA 配置では、GigabitEthernet 0/8 がフェールオーバー インターフェイスとして事前設定されます。

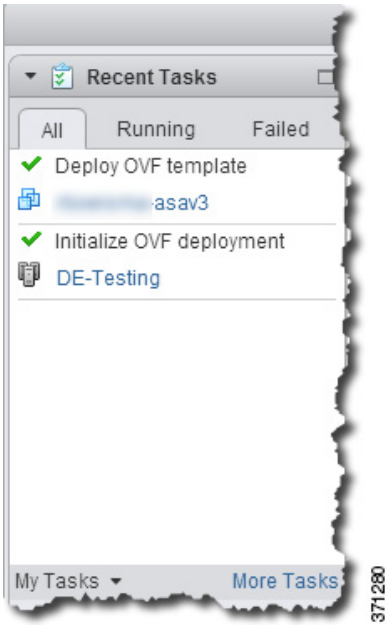
7. インターネット アクセスに HTTP プロキシを使用する場合は、[Smart Call Home Settings] 領域でスマート ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。
8. フェールオーバー/HA 配置の場合、[Customize template] 画面で次の処理を行います。
   - スタンバイ管理 IP アドレスを指定します。

     インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定する必要があります。プライマリ装置が故障すると、セカンダリ装置はプライマリ装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。
   - [HA Connection Settings] 領域で、フェールオーバー リンクを設定します。

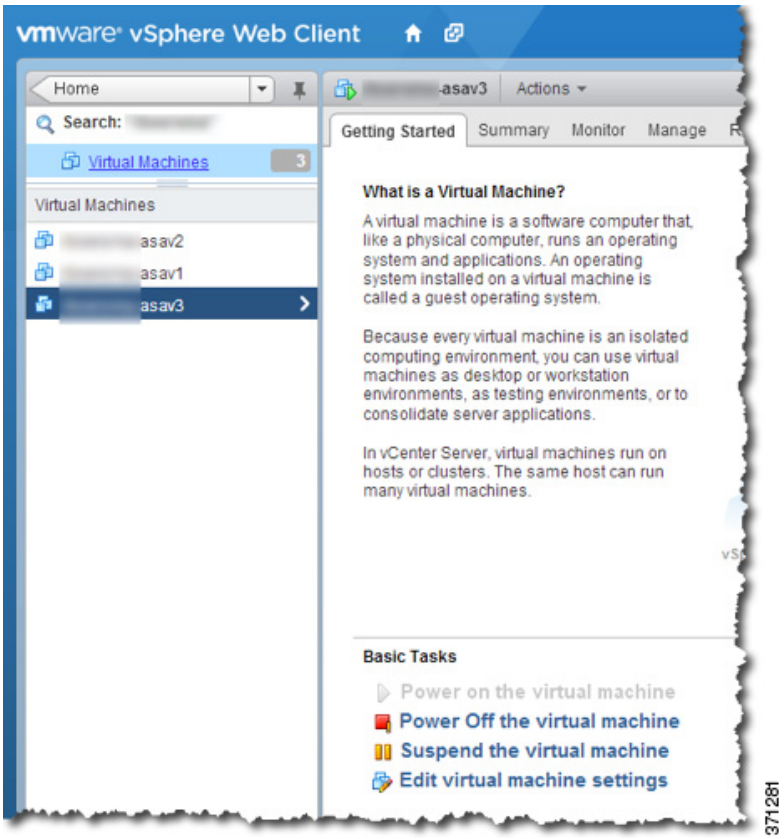
     フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。GigabitEthernet 0/8 がフェールオーバー リンクとして事前設定されています。同じネットワーク上のリンクに対するアクティブな IP アドレスとスタンバイの IP アドレスを入力します。
9. ウィザードが完了すると、vSphere Web Client は VM を処理します。[Recent Tasks] ペインの [Global Information] 領域で [Initialize OVF deployment] ステータスを確認できます。



この手順が終了すると、[Deploy OVF Template] 完了ステータスが表示されます。



その後 ASAv VM インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。



10. ASAv VM がまだ稼働していない場合は、[Power on the virtual machine] をクリックします。

    ASDM で接続を試行したりコンソールに接続を試行する前に、ASAv が起動するのを待ちます。ASAv が初めて起動すると、OVF ファイルから提供されたパラメータを読み込み、それらを ASAv システム構成に追加します。その後、起動プロセスが自動的に再開され、稼働を開始します。この二重起動プロセスは、初めて ASAv を導入した場合にのみ発生します。起動メッセージを確認するには、[Console] タブをクリックして、ASAv コンソールにアクセスします。

11. フェールオーバー/HA 配置の場合は、この手順を繰り返してセカンダリ装置を追加します。次のガイドラインを参照してください。

    - プライマリ装置と同じスループット レベルを設定します。
    - プライマリ装置と*正確に同じ IP アドレス設定*を入力します。両方の装置のブートストラップ設定は、プライマリまたはセカンダリとして装置を識別するパラメータを除いて同一にします。

注: Cisco Licensing Authority に ASAv を正常に登録するには、ASAv にインターネット アクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

VMware vSphere スタンドアロン クライアントおよび第 0 日用構成を使用した ASAv の導入

ASAv を導入するには、VMware vSphere クライアントおよびオープン仮想化フォーマット（OVF）のテンプレート ファイル（vCenter へ導入する場合は asav-vi.ovf または vCenter 以外へ導入する場合は asav-esxi.ovf）を使用します。シスコの ASAv パッケージを展開するには、vSphere クライアントで [Deploy OVF Template] ウィザードを使用します。このウィザードは、ASAv OVF ファイルを解析し、ASAv を実行する仮想マシンを作成して、パッケージをインストールします。

ウィザードの手順のほとんどは、VMware に対し標準のものです。[Deploy OVF Template] ウィザードの詳細については、VMware vSphere クライアントのオンライン ヘルプを参照してください。

はじめる前に

- ASAv を導入する前に、vSphere（管理用）に少なくとも 1 つのネットワークを設定しておく必要があります。
- ASAv ソフトウェアの開梱と VMware 対応第 0 日用コンフィギュレーション ファイルの作成、9 ページの手順に従って、第 0 日用構成を作成します。

手順

1. VMware vSphere クライアントを起動し、[File] > [Deploy OVF Template] を選択します。

   [Deploy OVF Template] ウィザードが表示されます。

2. asav-vi.ovf ファイルを解凍した作業ディレクトリを参照し、それを選択します。

3. [OVF Template Details] 画面が表示されます。次の画面に移動します。カスタムの第 0 日用コンフィギュレーション ファイルを使用する場合は、構成を変更する必要はありません。

4. 最後の画面に導入設定の要約が表示されます。[Finish] をクリックしてVM を導入します。

5. ASAv に電源を投入し、VMware コンソールを開いて、2 回目の起動を待機します。

6. ASAv に SSH 接続し、必要な構成を完了します。第 0 日用コンフィギュレーション ファイルに希望するすべての構成がない場合は、VMware コンソールを開いて、必要な構成を完了します。

   これで、ASAv は完全に動作可能な状態です。

OVF ツールおよび第 0 日用構成を使用した ASAv の導入

はじめる前に

- OVF ツールを使用して ASAv を導入する場合は、day0.iso ファイルが必要です。ZIP ファイルで提供されるデフォルトの空の day0.iso ファイルを使用するか、または、生成しカスタマイズした第 0 日用コンフィギュレーション ファイルを使用できます。第 0 日用コンフィギュレーション ファイルの作成方法については、ASAv ソフトウェアの開梱と VMware 対応第 0 日用コンフィギュレーション ファイルの作成、9 ページを参照してください。
- OVF ツールが Linux または Windows PC にインストールされ、ターゲット ESXi サーバに接続できることを確認します。

手順

1. OVF ツールがインストールされていることを確認します。

   ```
   linuxprompt# which ovftool
   ```

2. 必要な導入オプションを指定した .cmd ファイルを作成します。

   例:

   ```
   linuxprompt# cat launch.cmd
   ovftool \
   --name="asav-941-demo" \
   --powerOn \
   --deploymentOption=ASAv30 \
   --diskMode=thin \
   --datastore=datastore1 \
   --acceptAllEulas \
   --net:Management0-0="Portgroup_Mgmt" \
   --net:GigabitEthernet0-1="Portgroup_Inside" \
   --net:GigabitEthernet0-0="Portgroup_Outside" \
   --prop:HARole=Standalone \
   asav-esxi.ovf \
   vi://root@10.1.2.3/
   ```

3. cmd ファイルを実行します。

   ```
   linuxprompt# ./launch.cmd
   ```

   ASAv に電源を投入し、2 回目の起動を待機します。

4. ASAv に SSH 接続し、必要に応じて構成を完了します。さらに構成が必要な場合は、ASAv に対して VMware コンソールを開き、必要な構成を適用します。

   これで、ASAv は完全に動作可能な状態です。

ASAv コンソールへのアクセス

ASDM を使用する場合、トラブルシューティングに CLI を使用する必要がある場合があります。デフォルトでは、組み込みの VMware vSphere コンソールにアクセスできます。または、コピー アンド ペーストなどのより優れた機能を持つネットワーク シリアル コンソールを設定できます。

- VMware vSphere コンソールの使用、18 ページ
- ネットワーク シリアル コンソール ポートの設定、19 ページ

VMware vSphere コンソールの使用

初期設定またはトラブルシューティングを行うには、VMware vSphere Web Client により提供される仮想コンソールから CLI にアクセスします。後で Telnet または SSH の CLI リモート アクセスを設定できます。

はじめる前に

vSphere Web Client では、ASAv コンソール アクセスに必要なクライアント統合プラグインをインストールします。

手順

1. VMware vSphere Web Client で、インベントリの ASAv インスタンスを右クリックし、[Open Console] を選択します。または、[Summary] タブの [Launch Console] をクリックできます。
2. コンソールでクリックして Enter を押します。注：Ctrl + Alt を押すと、カーソルが解放されます。

   ASAv がまだ起動中の場合は、起動メッセージが表示されます。

   ASAv が初めて起動すると、OVF ファイルから提供されたパラメータを読み込み、それらを ASAv システム構成に追加します。その後、起動プロセスが自動的に再開され、稼働を開始します。この二重起動プロセスは、初めて ASAv を導入した場合にのみ発生します。

   注：ライセンスをインストールするまで、予備接続テストを実行できるように、スループットは 100 Kbps に制限されます。ライセンスは、通常の操作に必要です。ライセンスをインストールするまで、次のメッセージがコンソールで繰り返し表示されます。

   ```
   Warning: ASAv platform license state is Unlicensed.
   Install ASAv platform license for full functionality.
   ```

   次のプロンプトが表示されます。

   ```
   ciscoasa>
   ```

   このプロンプトは、ユーザ EXEC モードで作業していることを示します。ユーザ EXEC モードでは、基本コマンドのみを使用できます。
3. 特権 EXEC モードにアクセスします。

   ```
   ciscoasa> enable
   ```

   次のプロンプトが表示されます。

   ```
   Password:
   ```
4. Enter キーを押して、次に進みます。デフォルトでは、パスワードは空白です。以前にイネーブル パスワードを設定した場合は、Enter を押す代わりにこれを入力します。

   プロンプトが次のように変化します。

   ```
   ciscoasa#
   ```

   設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

   特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。
5. グローバル コンフィギュレーション モードにアクセスします。

   ```
   ciscoasa# configure terminal
   ```

   プロンプトが次のように変化します。

   ```
   ciscoasa(config)#
   ```

   グローバル コンフィギュレーション モードから ASAv の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

ネットワーク シリアル コンソール ポートの設定

コンソール エクスペリエンスの向上のために、コンソール アクセスについて、ネットワーク シリアル ポートを単独で設定するか、または仮想シリアル ポート コンセントレータ（vSPC）に接続するように設定できます。各方法の詳細については、VMware vSphere のマニュアルを参照してください。ASAv では、仮想コンソールの代わりにシリアル ポートにコンソール出力を送信する必要があります。この項では、シリアル ポート コンソールを有効にする方法について説明します。

手順

1. VMware vSphere でネットワーク シリアル ポートを設定します。VMware vSphere のマニュアルを参照してください。
2. ASAv で、「use_ttyS0」という名前のファイルを disk0 のルート ディレクトリに作成します。このファイルには内容が含まれている必要はありません。この場所に存在することのみが必要です。

   disk0:/use_ttyS0

   - ASDM から [Tools] > [File Management] ダイアログボックスを使用して、この名前で空のテキスト ファイルをアップロードすることができます。
   - vSphere コンソールで、ファイル システム内の既存のファイル（任意のファイル）を新しい名前にコピーできます。次に例を示します。

     ```
     ciscoasa(config)# cd coredumpinfo
     ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
     ```

3. ASAvをリロードします。
   - ASDM から、[Tools] > [System Reload] を選択します。
   - vSphere コンソールで **reload** を入力します。

   ASAv は vSphere コンソールへの送信を停止し、代わりにシリアル コンソールに送信します。
4. シリアル ポートの追加時に指定した vSphere のホスト IP アドレスとポート番号に Telnet 接続するか、または vSPC の IP アドレスとポートに Telnet 接続します。

vCPU またはスループット ライセンスのアップグレード

ASAv は、使用できる vCPU の数に影響するスループット ライセンスを使用します。

ASAv の vCPU の数を増やす（または減らす）場合は、新しいライセンスを要求してその新しいライセンスを適用し、新しい値と一致するように VMware の VM プロパティを変更します。

注：割り当てられた vCPU は、ASAv 仮想 CPU ライセンスまたはスループット ライセンスと一致している必要があります。RAM は、vCPU 用に正しくサイズ調整されている必要があります。アップグレードまたはダウングレード時には、この手順に従って、ライセンスと vCPU を迅速に調整するようにします。永続的な不一致がある場合、ASAv は適切に動作しません。

手順

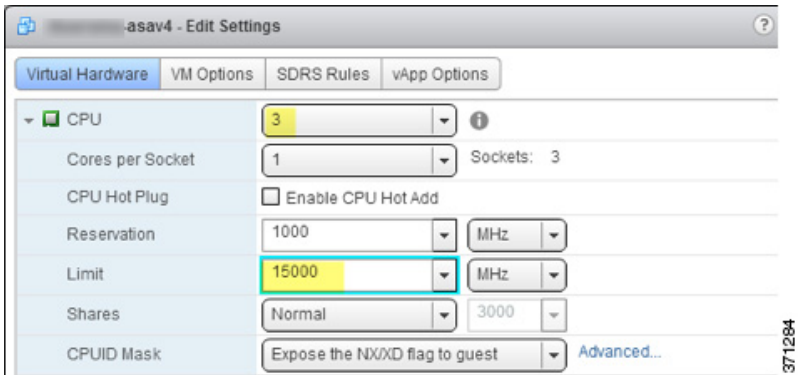
1. 新しいライセンスを要求します。
2. 新しいライセンスを適用します。フェールオーバー ペアの場合、両方の装置に新しいライセンスを適用します。
3. フェールオーバーを使用するかどうかに応じて、次のいずれかを実行します。
   - フェールオーバーあり：vSphere Web Client で、*スタンバイ* ASAv の電源を切断します。たとえば、ASAv をクリックしてから [Power Off the virtual machine] をクリックするか、または ASAv を右クリックして [Shut Down Guest OS] を選択します。
   - フェールオーバーなし：vSphere Web クライアントで、ASAv の電源を切断します。たとえば、ASAv をクリックしてから [Power Off the virtual machine] をクリックするか、または ASAv を右クリックして [Shut Down Guest OS] を選択します。

4. ASAv をクリックしてから [Edit Virtual machine settings] をクリックします(または ASAv を右クリックして [Edit Settings] を選択します)。

   [Edit Settings] ダイアログボックスが表示されます。

5. 新しい vCPU ライセンスの正しい値を確認するには、ASAv のライセンス、4 ページにある CPU メモリの各要件を参照してください。

6. [Virtual Hardware] タブの [CPU] で、ドロップダウン リストから新しい値を選択します。



7. [Memory] には、新しい RAM の値を入力します。

8. [OK] をクリックします。

9. ASAv の電源を入れます。たとえば、[Power On the Virtual Machine] をクリックします。

10. フェールオーバー ペアの場合:

    a. アクティブ装置へのコンソールを開くか、またはアクティブ装置で ASDM を起動します。

    b. スタンバイ装置の起動が終了した後、スタンバイ装置にフェールオーバーします。

       - ASDM:[Monitoring] > [Properties] > [Failover] > [Status] を選択して [Make Standby] をクリックします。

       - CLI:ciscoasa# **failover active**

    c. アクティブ装置に対して、ステップ 3 ～ 9 を繰り返します。

関連項目

- ASAv のライセンス、4 ページ

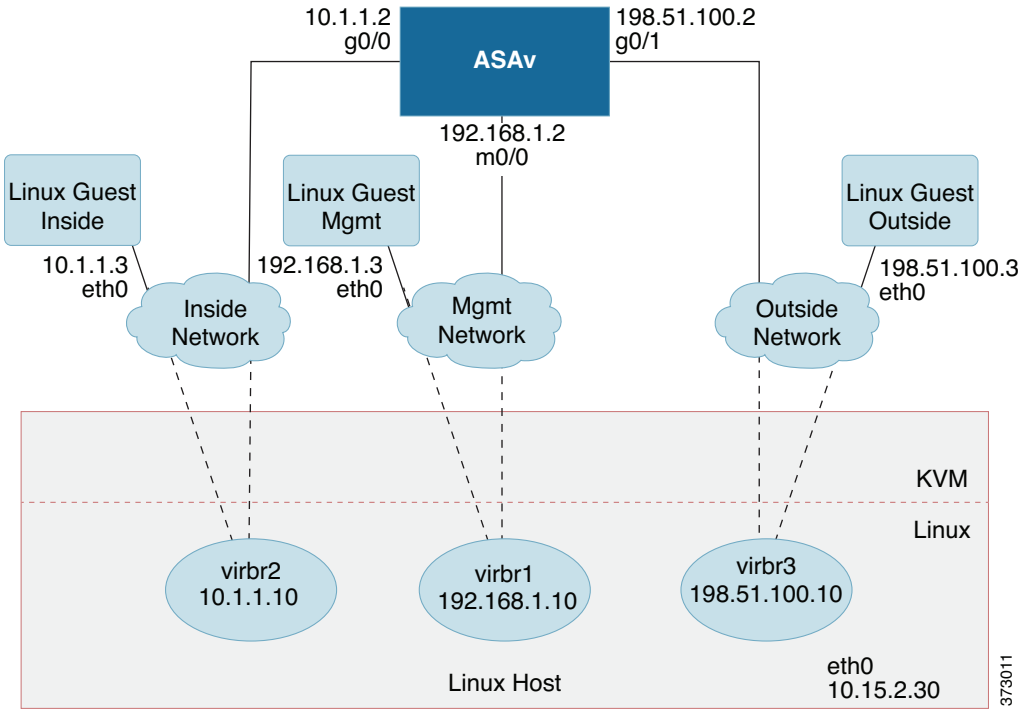
KVM を使用した ASAv の導入

カーネルベースの仮想マシン（KVM）を使用して ASAv を導入することができます。

KVM を使用した ASAv の導入について

図 1（21 ページ）は、ASAv と KVM によるネットワーク トポロジの例を示しています。この章で説明している手順は、このトポロジの例に基づいています。実際に必要な手順は、各自の要件に応じて異なります。ASAv は、内部ネットワークと外部ネットワークの間のファイアウォールとして動作します。また、別個の管理ネットワークが設定されます。

図 1　KVM を使用した ASAv の導入例



ASAv と KVM の前提条件

- Cisco.com から ASAv qcow2 ファイルをダウンロードし、Linux ホストに格納します。

  注：Cisco.com のログインおよびシスコ サービス契約が必要です。

- このマニュアルの導入例では、ユーザが Ubuntu 14.04 LTS を使用していることを前提としています。Ubuntu 14.04 LTS ホストの最上部に次のパッケージをインストールします。
  - qemu-kvm
  - libvirt bin
  - bridge-utils
  - Virt-Manager
  - virtinst
  - virsh tools
  - genisoimage
- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での ASAv のスループットを最大化できます。一般的なホスト調整の概念については、『Network Function Virtualization Packet Processing Performance of Virtualized Platforms with Linux and Intel Architecture』を参照してください。
- 以下の機能は Ubuntu 14.04 の最適化に役立ちます。
  - macvtap：高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
  - Transparent Huge Pages：メモリ ページ サイズを増加させます。Ubuntu 14.04 では、デフォルトでオンになっています。
  - Hyperthread disabled：2 つの vCPUを 1 つのシングル コアに削減します。
  - txqueuelength：デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップ レートを低減します。
  - pinning：qemu および vhost プロセスを特定のCPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。
- RHEL ベースのディストリビューションの最適化については、『Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide』を参照してください。
- KVM のシステム要件については、『Cisco ASA Compatibility』を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

ASAv を起動する前に、第 0 日（Day 0）用のコンフィギュレーション ファイルを準備できます。このファイルは、ASAv の起動時に適用される ASAv の設定を含むテキスト ファイルです。この初期設定は、「day0-config」というテキスト ファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。第 0 日用コンフィギュレーション ファイルには、少なくとも、管理インターフェイスをアクティブ化するコマンドと、公開キー認証用 SSH サーバをセットアップするコマンドを含める必要がありますが、すべての ASA 設定を含めることもできます。day0.iso ファイル（カスタム day0 またはデフォルトの day0.iso）は、最初の起動中に使用できなければなりません。

注：初期導入時に自動的に ASAv をライセンス許諾するには、Cisco Smart Software Manager からダウンロードした Smart Licensing Identity（ID）トークンを「idtoken」というテキスト ファイルに格納し、第 0 日用コンフィギュレーション ファイルと同じディレクトリに保存します。

注：トランスペアレント モードで ASAv を導入する場合は、トランスペアレント モードで実行される既知の ASA コンフィギュレーション ファイルを第 0 日用コンフィギュレーション ファイルとして使用します。これは、ルーテッド ファイアウォールの第 0 日用コンフィギュレーション ファイルには該当しません。

注：この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

手順

1. 「day0-config」というテキスト ファイルに ASAv の CLI 設定を記入します。3 つのインターフェイスの設定とその他の必要な設定を追加します。

   最初の行は ASA のバージョンで始める必要があります。day0-config は、有効な ASA 構成である必要があります。day0-config を生成する最適な方法は、既存の ASA または ASAv から実行コンフィギュレーションの必要な部分をコピーすることです。day0-config 内の行の順序は重要で、既存の show run コマンド出力の順序と一致している必要があります。

   例:

   ```
   ASA Version 9.4.1
   !
   interface management0/0
      nameif management
      security-level 100
      ip address 192.168.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/0
      nameif inside
      security-level 100
      ip address 10.1.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/1
      nameif outside
      security-level 0
      ip address 198.51.100.2 255.255.255.0
      no shutdown
   http server enable
   http 192.168.1.0 255.255.255.0 management
   crypto key generate rsa modulus 1024
   username AdminUser password paSSw0rd
   ssh 192.168.1.0 255.255.255.0 management
   aaa authentication ssh console LOCAL
   ```

2. （任意）Cisco Smart Software Manager により発行された Smart License ID トークン ファイルをコンピュータにダウンロードします。

3. （任意）ダウンロード ファイルから ID トークンをコピーし、ID トークンのみを含む「idtoken」というテキスト ファイルを作成します。

4. （任意）ASAv の初期導入時に自動的にライセンス許諾を行う場合は、day0-config ファイルに次の情報が含まれていることを確認してください。

   - 管理インターフェイスの IP アドレス
   - （任意）Smart Licensing で使用する HTTP プロキシ
   - HTTP プロキシ（指定した場合）または tools.cisco.com への接続を有効にする **route** コマンド
   - tools.cisco.com を IP アドレスに解決する DNS サーバ
   - 要求する ASAv ライセンスを指定するための Smart Licensing の設定
   - （任意）CSSM での ASAv の検索を容易にするための一意のホスト名

5. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

   ```
   stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
   I: input-charset not specified, using utf-8 (detected in locale settings)
   Total translation table size: 0
   Total rockridge attributes bytes: 252
   Total directory bytes: 0
   ```

```
Path table size (byptes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

この ID トークンによって、Smart Licensing サーバに ASAv が自動的に登録されます。

6. ステップ 1から 5 を繰り返し、導入する ASAv ごとに、適切な IP アドレスを含むデフォルトのコンフィギュレーション ファイルを作成します。

仮想ブリッジ XML ファイルの準備

ASAv ゲストを KVM ホストに接続し、ゲストを相互接続する仮想ネットワークを設定する必要があります。

注: この手順では、KVM から外部への接続は確立されません。

KVM ホスト上に仮想ブリッジ XMLファイルを準備します。第 0 日のコンフィギュレーション ファイルの準備、22 ページに記載されている仮想ネットワーク トポロジの例では、3 つの仮想ブリッジ ファイル（virbr1.xml、virbr2.xml、virbr3.xml）が必要です（これらの 3 つのファイル名を使用する必要があります。たとえば、virbr0 はすでに存在しているため使用できません）。各ファイルには、仮想ブリッジの設定に必要な情報が含まれています。仮想ブリッジに対して名前と一意の MAC アドレスを指定する必要があります。IP アドレスの指定は任意です。

手順

1. 次の 3 つの仮想ネットワーク ブリッジ XML ファイルを作成します。

   virbr1.xml：

```
<network>
  <name>virbr1</name>
  <bridge name='virbr1' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:00' />
  <ip address='192.168.1.10' netmask='255.255.255.0' />
</network>
```

   virbr2.xml：

```
<network>
  <name>virbr2</name>
  <bridge name='virbr2' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:01' />
  <ip address='10.1.1.10' netmask='255.255.255.0' />
</network>
```

   virbr3.xml：

```
<network>
  <name>virbr3</name>
  <bridge name='virbr3' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:02' />
  <ip address='198.51.100.10' netmask='255.255.255.0' />
</network>
```

2. 以下を含むスクリプトを作成します（この例では、スクリプトに virt_network_setup.sh という名前を付けます）。

```
virsh net-create virbr1.xml
virsh net-create virbr2.xml
virsh net-create virbr3.xml
```

3. このスクリプトを実行して仮想ネットワークを設定します。スクリプトによって仮想ネットワークが確立されます。ネットワークは、KVM ホストが動作している限り稼動します。

```
stack@user-ubuntu:-/KvmAsa$ virt_network_setup.sh
```

注:Linux ホストをリロードする場合は、virt_network_setup.sh スクリプトを再実行する必要があります。スクリプトはリブート後に継続されません。

4. 仮想ネットワークが作成されたことを確認します。

```
stack@user-ubuntu:-/KvmAsa$ brctl show
bridge name     bridge id               STP enabled     Interfaces
virbr0          8000.0000000000000      yes
virbr1          8000.5254000056eed      yes             virb1-nic
virbr2          8000.5254000056eee      yes             virb2-nic
virbr3          8000.5254000056eec      yes             virb3-nic
stack@user-ubuntu:-/KvmAsa$
```

5. virbr1 ブリッジに割り当てられている IP アドレスを表示します。これは、XML ファイルで割り当てた IP アドレスです。

```
stack@user-ubuntu:-/KvmAsa$ ip address show virbr1
S: virbr1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:05:6e:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global virbr1
      valid_lft forever preferred_lft forever
```

ASAv の起動

ASAv を起動するには、virt-install ベースの導入スクリプトを使用します。

手順

1. 「virt_install_asav.sh」という virt-install スクリプトを作成します。

ASAv VM の名前は、KVM ホスト上の他の仮想マシン（VM）全体において一意である必要があります。ASAv は最大 10 のネットワークをサポートできます。この例では 3 つのネットワークが使用されています。ネットワーク ブリッジの句の順序は重要です。リストの最初の句は常に ASAv の管理インターフェイス（管理 0/0）、2 番目の句は ASAv の GigabitEthernet 0/0、3 番目の句は ASAv の GigabitEthernet 0/1 に該当し、GigabitEthernet0/8 まで同様に続きます。仮想 NIC は Virtio でなければなりません。

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=asav \
   --cpu host \
   --arch=x86_64 \
   --machine=pc-1.0 \
   --vcpus=1 \
   --ram=2048 \
   --os-type=linux \
   --os-variant=generic26 \
   --noacpi \
   --virt-type=kvm \
   --import \
   --disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=ide,cache=none \
   --disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
   --console pty,target_type=virtio \
   --serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

2. virt_install スクリプトを実行します。

```
stack@user-ubuntu:-/KvmAsa$ ./virt_install_asav.sh

Starting install...
Creating domain...
```

ウィンドウが開き、VM のコンソールが表示されます。VM が起動中であることを確認できます。VM が起動するまでに数分かかります。VM が起動したら、コンソール画面から CLI コマンドを実行できます。

AWS クラウドへの ASAv の導入

Amazon Web Sources（AWS）クラウドに ASAv を導入できます。

AWS クラウドへの ASAv の導入について

AWS は、プライベート Xen ハイパーバイザを使用するパブリック クラウド環境です。ASAv は Xen ハイパーバイザの AWS 環境内でゲストとして実行されます。AWS 上の ASAv は、次のインスタンス タイプをサポートします。

- c3.large：2 つの vCPU、3.75 GB、2 つのインターフェイス、1 つの管理インターフェイス

  注：ASAv10 と ASAv30 はどちらも c3.large でサポートされていますが、リソースがアンダープロビジョニングされるため、c3.large での ASAv30 の使用は推奨しません。

- c3.xlarge：4 つの vCPU、7.5 GB、3 つのインターフェイス、1 つの管理インターフェイス

  注：ASAv30 のみが c3.xlarge でサポートされます。

注：ASAv は AWS 環境外部の Xen ハイパーバイザをサポートしていません。

AWS にアカウントを作成し、AWS ウィザードを使用して ASAv をセットアップして、Amazon Machine Image（AMI）を選択します。AMI はインスタンスを起動するために必要なソフトウェア構成を含むテンプレートです。

注：AMI イメージは AWS 環境の外部ではダウンロードできません。

ASAv と AWS の前提条件

- aws.amazon.com でアカウントを作成します。
- ASAv にライセンスを付与します。ASAv にライセンスを付与するまでは、100 の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「Smart Software Licensing for the ASAv（ASAv の Smart Software Licensing）」を参照してください。
- インターフェイスの要件：
  - 管理インターフェイス
  - 内部および外部インターフェイス
  - （任意）追加のサブネット（DMZ）

- 通信パス：
  - 管理インターフェイス：ASDM に ASAv を接続するために使用され、トラフィックの通過には使用できません。
  - 内部インターフェイス（必須）：内部ホストに ASAv を接続するために使用されます。
  - 外部インターフェイス（必須）：ASAv をパブリック ネットワークに接続するために使用されます。
  - DMZ インターフェイス（任意）：c3.xlarge インターフェイスを使用する場合に、DMZ ネットワークに ASAv を接続するために使用されます。
- ASAv のシステム要件については、『Cisco ASA Compatibility』を参照してください。

ASAv および AWS のガイドラインと制限事項

AWS 上の ASAv は次の機能をサポートします。

- 仮想プライベート クラウド（VPC）への導入
- 拡張ネットワーク（SR-IOV）（使用可能な場合）
- Amazon マーケットプレイスからの導入
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザ導入
- ルーテッド モード（デフォルト）

AWS 上の ASAv は以下をサポートしません。

- コンソール アクセス（管理は、ネットワーク インターフェイスを介して SSH または ASDM を使用して実行される）
- IPv6
- VLAN
- 無差別モード（スニファなし、またはトランスペアレント モードのファイアウォールのサポート）
- マルチ コンテキスト モード
- クラスタ
- ASAv のネイティブ HA
- EtherChannel は、ダイレクト物理インターフェイスのみでサポートされる
- VM のインポート/エクスポート
- Amazon Cloudwatch
- ハイパーバイザに非依存のパッケージ
- VMware ESXi
- ブロードキャスト/マルチキャスト メッセージ

  これらのメッセージは AWS 内で伝播されないため、ブロードキャスト/マルチキャストを必要とするルーティング プロトコルは AWS で予期どおりに機能しません。VXLAN はスタティック ピアでのみ動作できます。

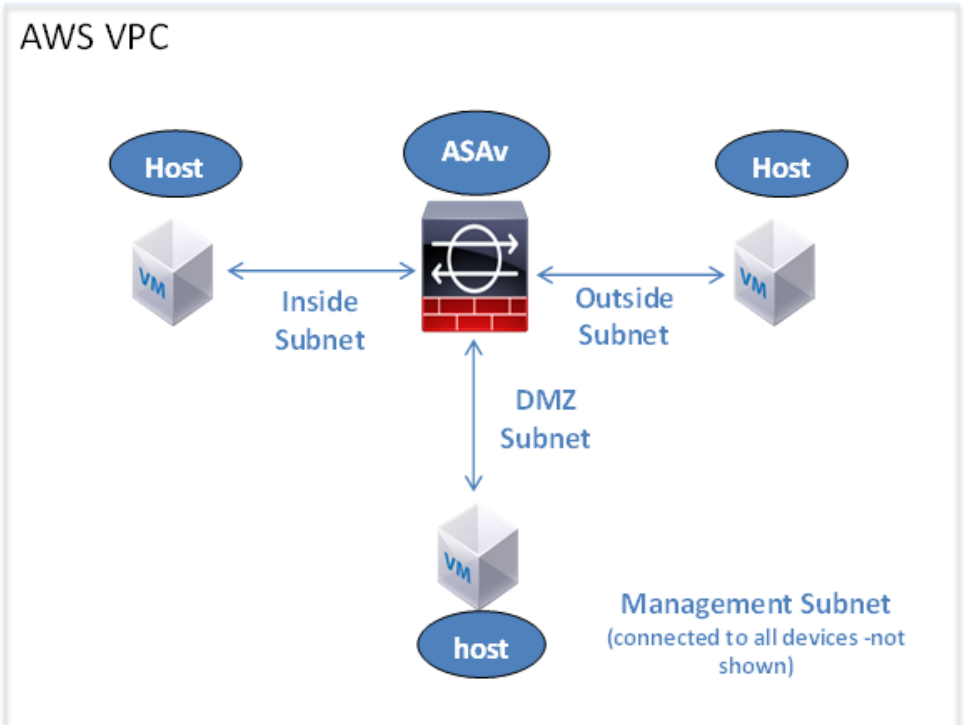
- Gratuitous/非要請 ARP

  これらの ARPS は AWS 内では受け入れられないため、Gratuitous ARP または非要請 ARP を必要とする NAT 設定は期待どおりに機能しません。

AWS 上の ASAv のネットワーク トポロジの例

図 1（29 ページ）は、ASAv 用に AWS 内で設定された 4 つのサブネット（管理、内部、外部、および DMZ）を備えるルーテッド ファイアウォール モードの ASAv の推奨トポロジを示しています。

図 1　AWS への ASAv の導入の例



AWS への ASAv の導入

次の手順は、ASAv で AWS をセットアップする手順の概略を示しています。セットアップの詳細な手順については、「AWS の使用開始ドキュメント」を参照してください。

手順

1. aws.amazon.com にログインし、地域を選択します。

   AWS は互いに分離された複数の地域に分割されます。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。定期的に、目的の地域内に存在していることを確認してください。

2. [Networking] の下で [My Account] > [AWS Management Console] をクリックし、[VPC] > [Start VPC Wizard] をクリックして、単一のパブリック サブネットを選択して VPC を作成し、次をセットアップします（特記のないかぎり、デフォルト設定を使用できます）。

   - 内部および外部のサブネット：VPC およびサブネットの名前を入力します。
   - インターネット ゲートウェイ：インターネット経由の直接接続を有効にします（インターネット ゲートウェイの名前を入力します）。
   - 外部テーブル：インターネットへの発信トラフィックを有効にするためのエントリを追加します（インターネット ゲートウェイに 0.0.0.0/0 を追加します）。

3. [My Account] > [AWS Management Console] > [EC2] をクリックし、さらに、[Create an Instance] をクリックします。
   - AMI（たとえば、Ubuntu Server 14.04 LTS）を選択します。

     イメージ配信通知で識別された AMI を使用します。
   - ASAv（たとえば、c3.large）によってサポートされるインスタンス タイプを選択します。
   - インスタンスを設定します（CPU とメモリは固定です）。
   - [Advanced Details] で、必要に応じて第 0 日用構成を追加します。第 0 日構成にスマート ライセンスなどの詳細情報を設定する方法の詳細については、第 0 日のコンフィギュレーション ファイルの準備、22 ページを参照してください。

     第 0 日用構成の例

     ```
     ! ASA Version 9.4.1.200
     interface management0/0
     management-only
     nameif management
     security-level 100
     ip address dhcp setroute
     no shut
     !
     same-security-traffic permit inter-interface
     same-security-traffic permit intra-interface
     !
     crypto key generate rsa modulus 2048
     ssh 0 0 management
     ssh timeout 30
     username admin nopassword privilege 15
     username admin attributes
     service-type admin
     ! required config end
     ! example dns configuration
     dns domain-lookup management
     DNS server-group DefaultDNS
     ! where this address is the .2 on your public subnet
     name-server 172.19.0.2
     ! example ntp configuration
     name 129.6.15.28 time-a.nist.gov
     name 129.6.15.29 time-b.nist.gov
     name 129.6.15.30 time-c.nist.gov
     ntp server time-c.nist.gov
     ntp server time-b.nist.gov
     ntp server time-a.nist.gov
     ```
   - ストレージ（デフォルトを受け入れます）。
   - タグ インスタンス：デバイスを分類するため、多数のタグを作成できます。タグを容易に見つけるために使用できる名前を付けます。
   - セキュリティ グループ：セキュリティ グループを作成して名前を付けます。セキュリティ グループは、着信および発信トラフィックを制御するためのインスタンスの仮想ファイアウォールです。

     デフォルトでは、セキュリティ グループはすべてのアドレスに対して開かれています。ASAv にアクセスするために使用するアドレスからの SSH 接続だけを許可するように、ルールを変更します。
   - 設定を確認し、[Launch] をクリックします。
4. キー ペアを作成します。

   キー ペアにわかりやすい名前を付け、キーを安全な場所にダウンロードします。再度、ダウンロードすることはできません。キー ペアを失った場合は、インスタンスを破棄し、それらを再度導入する必要があります。

5. [Launch Instance] をクリックして、ASAv を導入します。
6. [My Account] > [AWS Management Console] > [EC2] > [Launch an Instance] > [My AMIs] をクリックします。
7. ASAv のインターフェイスごとに [Source/Destination Check] が無効になっていることを確認します。

   AWS のデフォルト設定では、インスタンスは、その IP アドレス宛てのトラフィックの受信のみが許可され、さらに、自身の IP アドレスからのトラフィックの送信のみが許可されます。ASAv のルーテッド ホップとしての動作を有効にするには、ASAv の各トラフィック インターフェイス（内部、外部、および DMZ）の [Source/Destination Check] を無効にする必要があります。

AWS への ASAv の導入

ASAv の設定

ASAv の導入により、ASDM アクセスが事前設定されます。導入時に指定したクライアント IP アドレスから、Web ブラウザで ASAv 管理 IP アドレスに接続できます。この章では、他のクライアントが ASDM にアクセスできるようにする方法と CLI アクセスを許可する方法（SSH または Telnet）についても説明します。この章で取り上げるその他の必須の設定作業には、ASDM でウィザードが提供するライセンスのインストールおよび一般的な設定作業が含まれます。

ASDM の開始

手順

1. ASDM クライアントとして指定した PC で次の URL を入力します。

   https://*asa_ip_address***/admin**

   次のボタンを持つ ASDM 起動ページが表示されます。

   - **Install ASDM Launcher and Run ASDM**
   - **Run ASDM**
   - **Run Startup Wizard**

2. ランチャをダウンロードするには、次の手順を実行します。

   a. [Install ASDM Launcher and Run ASDM] をクリックします。

   b. ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名および**イネーブル** パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。注：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

   c. インストーラを PC に保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。

   d. 管理 IP アドレスを入力し、ユーザ名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。注：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

3. Java Web Start を使用するには：

   a. [Run ASDM] または [Run Startup Wizard] をクリックします。

   b. プロンプトが表示されたら、ショートカットを PC に保存します。オプションで、アプリケーションを保存せずに開くこともできます。

   c. ショートカットから Java Web Start を起動します。

d. 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。

e. ユーザ名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。注：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

ASDM を使用した初期設定の実行

次の ASDM ウィザードおよび手順を使用して初期設定を行うことができます。CLI の設定については、CLI コンフィギュレーション ガイドを参照してください。

Startup Wizard の実行

導入環境に応じてセキュリティ ポリシーをカスタマイズできるように、**Startup Wizard**（[Wizards] > [Startup Wizard] を選択）を実行します。Startup Wizard を使用して、次の項目を設定できます。

- ホスト名
- ドメイン名
- 管理パスワード
- インターフェイス
- IP アドレス
- スタティック ルート
- DHCP サーバ
- ネットワーク アドレス変換規則
- その他

（オプション）ASAv の背後のパブリック サーバへのアクセス許可

[Configuration] > [Firewall] > [Public Servers] ペインでは、インターネットから内部サーバにアクセスできるようにするためのセキュリティ ポリシーが自動的に設定されます。ビジネス オーナーとして、内部ネットワーク サービス（Web サーバや FTP サーバなど）に外部ユーザがアクセスできるようにする必要がある場合があります。これらのサービスは、ASAvの背後にある、Demilitarized Zone（DMZ; 非武装地帯）と呼ばれる別のネットワーク上に配置できます。DMZ にパブリック サーバを配置すると、パブリック サーバに対する攻撃は内部ネットワークには影響しません。

（オプション）VPN ウィザードの実行

次のウィザード（[Wizards] > [VPN Wizards]）を使用して、VPN を設定できます。

- Site-to-Site VPN Wizard：2 台の ASAv 間で、IPsec サイト間トンネルを作成します。
- AnyConnect VPN Wizard：Cisco AnyConnect VPN クライアントに対する SSL VPN リモート アクセスを設定します。AnyConnect は ASA へのセキュアな SSL 接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能となります。ASA ポリシーは、リモート ユーザがブラウザを使用して最初に接続するときに、AnyConnect クライアントをダウンロードするように設定できます。AnyConnect 3.0 以降を使用する場合、クライアントは、SSL または IPSec IKEv2 VPN プロトコルを実行できます。

- Clientless SSL VPN Wizard：ブラウザにクライアントレス SSL VPN リモート アクセスを設定します。クライアントレス ブラウザベース SSL VPN によって、ユーザはブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。認証されると、ユーザにはポータル ページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザにリソースへのアクセス権限を付与します。ACL は、特定の企業リソースへのアクセスを制限したり、許可するために適用できます。
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard：Cisco IPsec クライアント用の IPsec VPN リモート アクセスを設定します。

（オプション）ASDM の他のウィザードの実行

- High Availability and Scalability Wizard：フェールオーバーまたは VPN ロード バランシングを設定します。
- Packet Capture Wizard：パケット キャプチャを設定し、実行します。このウィザードは、入出力インターフェイスのそれぞれでパケット キャプチャを 1 回実行します。パケットをキャプチャすると、PC にパケット キャプチャを保存し、パケット アナライザでチェックおよびリプレイできます。

高度な設定

ASAv の設定を続行するには、『Navigating the Cisco ASA Series Documentation』を参照してください。

高度な設定