



# VMware を使用した ASA の導入

VMware を使用して ASA を導入できます。

- ASA の VMware 機能のサポート、11 ページ
- ASA と VMware の前提条件、12 ページ
- ASA および VMware のガイドライン、12 ページ
- ASA 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、14 ページ
- VMware vSphere Web Client を使用した ASA の導入、17 ページ
- 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 ASA の導入、22 ページ
- OVF ツールおよび第 0 日用構成を使用した ASA の導入、22 ページ
- ASA コンソールへのアクセス、23 ページ
- vCPU またはスループット ライセンスのアップグレード、25 ページ
- SR-IOV インターフェイスのプロビジョニング、26 ページ
- ESXi 構成でのパフォーマンスの向上、30 ページ

## ASA の VMware 機能のサポート

表 1 頁 11 に、ASA の VMware 機能のサポートを示します。

表 1 ASA の VMware 機能のサポート

機能	説明	サポート(あり/なし)	コメント
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	-
ホット追加	追加時に VM が動作しています。	あり	-
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。	あり	-
Snapshot	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	-

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)	コメント
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。
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		トランスパレント 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 ASA30s であることなど)。

## スループット用のメモリと vCPU の割り当てとライセンス

- ASA 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ます。オーバープロビジョニングの場合、ASA 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、ASA 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、[ASA のライセンス](#)、6 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。

## CPU 予約

- デフォルトで、ASA の CPU 予約は 1000 MHz です。共有、予約、および制限の設定([Edit Settings] > [Resources] > [CPU])を使用することによって、ASA に割り当てられた CPU リソースの量を変更できます。ASA がより低い設定で必要なトラフィック負荷が課されている状況でその目的を果たすことができる場合は、CPU 予約の設定を 1000 Mhz 未満にすることができます。ASA によって使用される CPU の量は、それが動作しているハードウェア プラットフォームだけでなく、それが行っている作業のタイプと量によっても異なります。

仮想マシンの [Performance] タブの [Home] ビューに配置された [CPU Usage (MHz)] チャートからすべての仮想マシンに関する CPU 使用率をホストの視点から確認できます。ASA が標準的なトラフィック量を処理しているときの CPU 使用率のベンチマークを設定すれば、その情報を CPU 予約の調整時の入力として使用できます。

詳細については、VMware から発行されている『[CPU Performance Enhancement Advice](#)』を参照してください。

- 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、ASA 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] ペインを使用できます。

## IPv6 のガイドライン

VMware vSphere Web クライアントを使用して ASA 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

- ASA 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。
- ASA 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。
- ASA 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、ASA 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。

## 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。

day0-config ファイルの 2 つの例を示します。1 つ目の例では、ギガビット イーサネット インターフェイスを備えた ASAv を導入する場合の day0-config を示します。2 つ目の例では、10 ギガビット イーサネット インターフェイスを備えた ASAv を導入する場合の day0-config を示します。この day0-config を使用して、SR-IOV インターフェイスを備えた ASAv50 を導入します。[SR-IOV インターフェイスのプロビジョニング](#)、[26 ページ](#)を参照してください。

**例 1: ギガビット イーサネット インターフェイスを備えた ASA day0-config**

```
ASA Version 9.8.1
!
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
```

**例 2: 10 ギガビット イーサネット インターフェイスを備えた ASA day0-config**

```
ASA Version 9.8.1
!
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface TenGigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
ipv6 address 2001:10::1/64
!
interface TenGigabitEthernet0/1
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
ipv6 address 2001:20::1/64
!
route management 0.0.0.0 0.0.0.0 192.168.0.254
!
username cisco password cisco123 privilege 15
!
aaa authentication ssh console LOCAL
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 60
```

```

ssh version 2
!
http 0.0.0.0 0.0.0.0 management
!
logging enable
logging timestamp
logging buffer-size 99999
logging buffered debugging
logging trap debugging
!
dns domain-lookup management
DNS server-group DefaultDNS
    name-server 64.102.6.247
!
license smart
feature tier standard
throughput level 10G
!
crypto key generate rsa modulus 2048

```

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。

ID トークンは、自動的に ASA をスマート ライセンス サーバに登録し、day0.iso ファイルと同じ作業ディレクトリに配置する必要があります。ステップ 2. 頁 14 を参照してください。

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 (bytes): 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、22 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、22 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、17 ページ](#)
- [VMware vSphere Web Client を使用した ASAv の導入、18 ページ](#)

### 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。

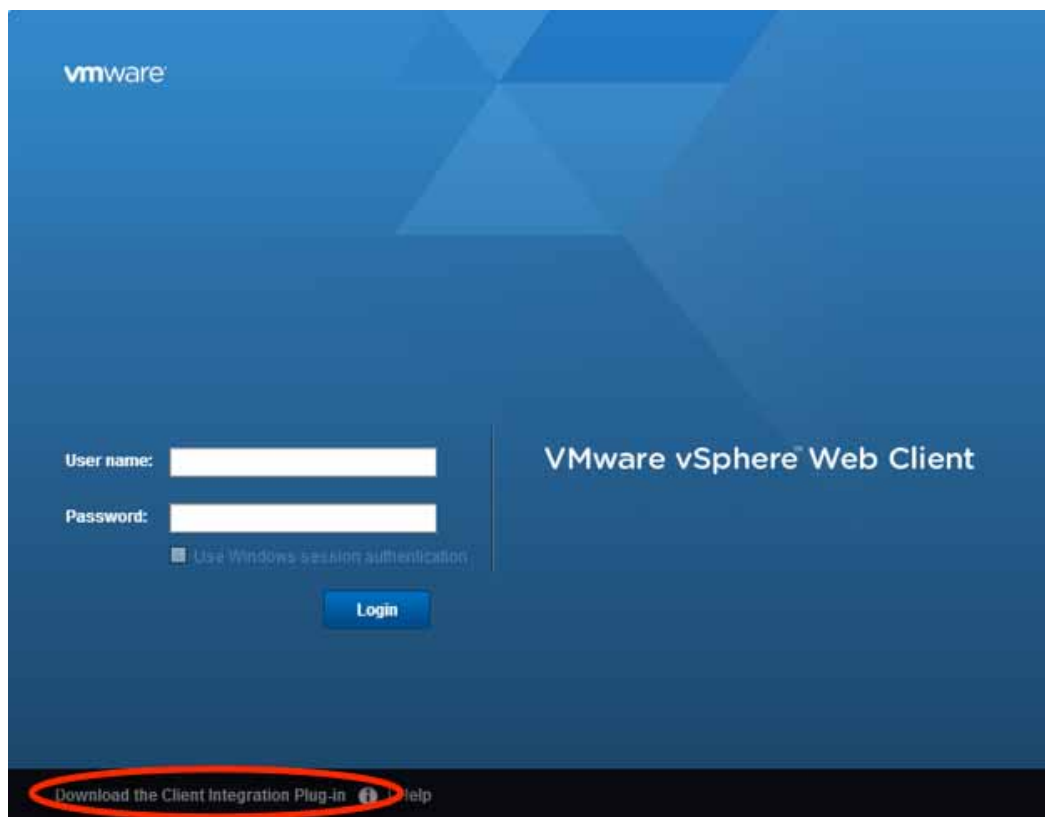
#### 手順

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. ユーザー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 ASA の導入

ASA 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 ASA 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、ASA OVF ファイルを解析し、ASA 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

ASA 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. ASA 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. ASA 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 ASA 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、ASA 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 ASA 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 ASA 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	ASA 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 ID	ASA インターフェイス ID
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

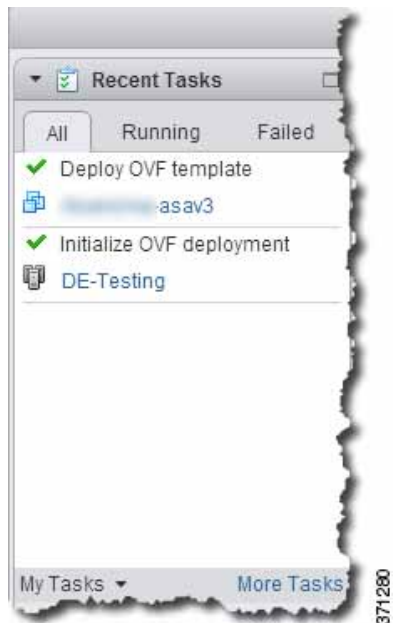
すべての ASA インターフェイスを使用する必要はありません。ただし、vSphere Web Client ではすべてのインターフェイスにネットワークを割り当てる必要があります。使用しないインターフェイスについては、ASA 設定内でインターフェイスを無効のままにしておくことができます。ASA を導入した後、任意で vSphere Web Client に戻り、[Edit Settings] ダイアログボックスから余分なインターフェイスを削除することができます。詳細については、vSphere Web Client のオンライン ヘルプを参照してください。

**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. ASA の 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、ASA が起動するのを待ちます。ASA 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 ASA 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 ASA 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、ASA 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 ASA を正常に登録するには、ASA 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 ASA の導入

ASA 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 ASA 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、ASA OVF ファイルを解析し、ASA 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、[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

- ASA 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。
- [ASA 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、14 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。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. ASA 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. ASA 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、ASA 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 ASA の導入

### はじめる前に

- OVF ツールを使用して ASA 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、[ASA 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、14 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 または vCenter サーバに接続できることを確認します。
- ハードウェア バージョンの互換性の問題により、SR-IOV 10 Gbps インターフェイスを利用する ASA50 を導入する場合は OVF ツールを使用できません。[仮想マシンの互換性レベルのアップグレード、29 ページ](#)を参照してください。

### 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、23 ページ](#)
- [ネットワーク シリアル コンソール ポートの設定、24 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。

## ASAv コンソールへのアクセス

**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 に制限されません。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. ASA 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。

ASA 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

ASA 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。

ASA 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。

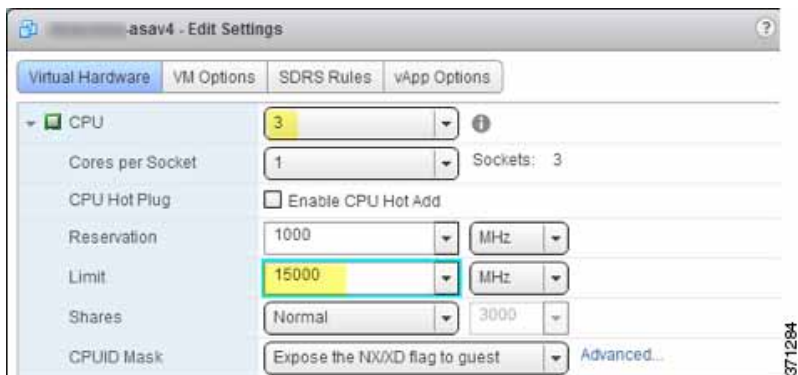
**注:** 割り当てられた vCPU は、ASA 仮想 CPU ライセンスまたはスループット ライセンスと一致している必要があります。RAM は、vCPU 用に正しくサイズ調整されている必要があります。アップグレードまたはダウングレード時には、この手順に従って、ライセンスと vCPU を迅速に調整するようにします。永続的な不一致がある場合、ASA は適切に動作しません。

### 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 ASA の電源を切断します。たとえば、ASA 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 ASA 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、ASA の電源を切断します。たとえば、ASA 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 ASA を右クリックして [Shut Down Guest OS] を選択します。
4. ASA をクリックしてから [Edit Virtual machine settings] をクリックします(または ASA 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、[ASA のライセンス、6 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。

## SR-IOV インターフェイスのプロビジョニング



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. ASA 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、手順 3 ~ 9 を繰り返します。

## 関連項目

- [ASAv のライセンス、6 ページ](#)

## SR-IOV インターフェイスのプロビジョニング

SR-IOV を使用すれば、複数の VM でホスト内部の 1 台の PCIe ネットワーク アダプタを共有することができます。SR-IOV は次の機能を定義しています。

- 物理機能 (PF): PF は、SR-IOV 機能を含むフル PCIe 機能です。これらは、ホスト サーバ上の通常のスタティック NIC として表示されます。
- 仮想機能 (VF): VF は、データ転送を支援する軽量 PCIe 機能です。VF は、PF から抽出され、PF を介して管理されます。

VF は、仮想化されたオペレーティング システム フレームワーク内の ASA 仮想マシンに最大 10 Gbps の接続を提供できません。このセクションでは、VMware 環境で VF を設定する方法について説明します。ASA 上の SR-IOV サポートについては、[ASAv と SR-IOV インターフェイスのプロビジョニング、8 ページ](#)で説明します。

## SR-IOV インターフェイスのプロビジョニングに関するガイドライン

VMware vSphere 5.1 以降のリリースは、特定の設定の環境でしか SR-IOV をサポートしません。vSphere の一部の機能は、SR-IOV が有効になっていると機能しません。

ASAv と SR-IOV に関する [システム要件、4 ページ](#)に加えて、VMware と SR-IOV に関する要件、サポートされている NIC、機能の可用性、およびアップグレード要件の詳細については、VMware マニュアル内の「[Supported Configurations for Using SR-IOV](#)」で確認する必要があります。



このセクションでは、VMware システム上の SR-IOV インターフェイスのプロビジョニングに関するさまざまなセットアップ手順と設定手順を示します。このセクション内の情報は、VMware ESXi 6.0 と vSphere Web Client、Cisco UCS C シリーズ サーバ、および Intel Ethernet Server Adapter X520 - DA2 を使用した特定のラボ環境内のデバイスから作成されたものです。

## ESXi ホスト BIOS の確認

VMware に SR-IOV インターフェイスを備えた ASAv を導入するには、仮想化をサポートして有効にする必要があります。VMware では、SR-IOV サポートに関するオンライン [Compatibility Guide](#) だけでなく、仮想化が有効か無効かを検出するダウンロード可能な [CPU Identification Utility](#) も含めて、仮想化サポートの確認手段をいくつか提供しています。

また、ESXi ホストにログインすることによって、BIOS 内で仮想化が有効になっているかどうかを判断することもできます。

### 手順

1. 次のいずれかの方法を使用して、ESXi シェルにログインします。
  - ホストへの直接アクセスがある場合は、Alt+F2 を押して、マシンの物理コンソールのログイン ページを開きます。
  - ホストにリモートで接続している場合は、SSH または別のリモート コンソール接続を使用して、ホスト上のセッションを開始します。
2. ホストによって認識されるユーザ名とパスワードを入力します。
3. 次のコマンドを実行します。

```
esxcfg-info|grep "\----\HV Support"
```

HV Support コマンドの出力は、使用可能なハイパーバイザ サポートのタイプを示します。可能性のある値の説明を以下に示します。

0:VT/AMD-V は、サポートがこのハードウェアでは使用できないことを示します。

1:VT/AMD-V は、VT または AMD-V を使用できますが、このハードウェアではサポートされないことを示します。

2:VT/AMD-V は、VT または AMD-V を使用できますが、現在、BIOS 内で有効になっていないことを示します。

3:VT/AMD-V は、VT または AMD-V が BIOS 内で有効になっており、使用できることを示します。

次に例を示します。

```
~ # esxcfg-info|grep "\----\HV Support"
|----HV Support.....3
```

値の 3 は、仮想化がサポートされており、有効になっていることを示します。

### 次の作業

ホスト物理アダプタ上で SR-IOV を有効にします。

## ホスト物理アダプタ上での SR-IOV の有効化

仮想マシンを仮想機能に接続する前に、vSphere Web Client を使用して、SR-IOV を有効にし、ホスト上の仮想機能の数を設定します。

### はじめる前に

- SR-IOV 互換ネットワーク インターフェイス カード (NIC) がインストールされていることを確認します。[SR-IOV に対してサポートされている NIC、5 ページ](#)を参照してください。

## SR-IOV インターフェイスのプロビジョニング

## 手順

1. vSphere Web Client で、SR-IOV を有効にする ESXi ホストに移動します。
2. [Manage] タブで、[Networking] をクリックし、[Physical adapters] を選択します。  
SR-IOV プロパティを調査することにより、物理アダプタが SR-IOV をサポートしているかどうかを確認できます。
3. 物理アダプタを選択し、[Edit adapter settings] をクリックします。
4. SR-IOV の下で、[Status] ドロップダウン メニューから [Enabled] を選択します。
5. [Number of virtual functions] テキスト ボックスに、アダプタに設定する仮想機能の数を入力します。

注:ASAv50 では、インターフェイスあたり 2 つ以上の VF を使用しないことをお勧めします。物理インターフェイスを複数の仮想機能で共有すると、パフォーマンスが低下する可能性があります。

6. [OK] をクリックします。
7. ESXi ホストを再起動します。

物理アダプタ エントリで表現された NIC ポートで仮想機能がアクティブになります。これらは、ホストの [Settings] タブの [PCI Devices] リストに表示されます。

## 次の作業

SR-IOV 機能と設定を管理するための標準 vSwitch を作成します。

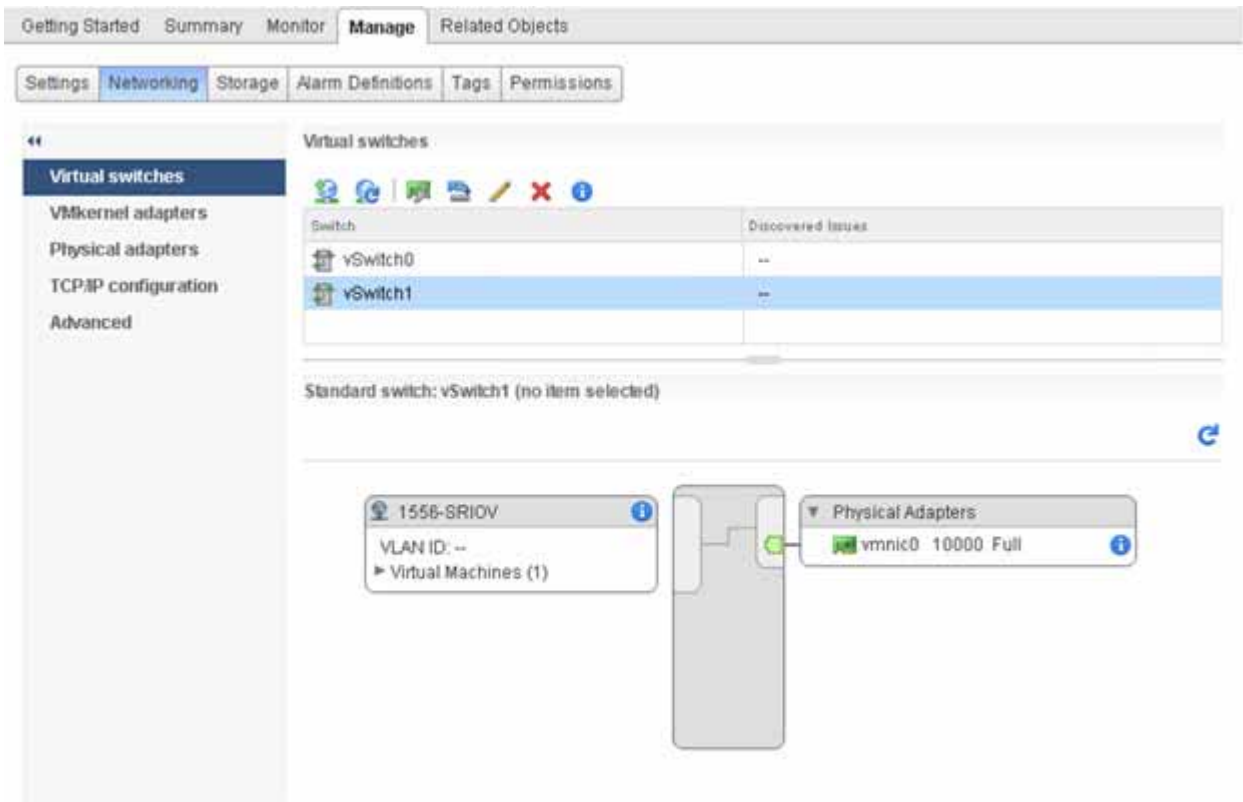
## vSphere スイッチの作成

SR-IOV インターフェイスを管理するための vSphere スイッチを作成します。

## 手順

1. vSphere Web Client で、ESXi ホストに移動します。
2. [Manage] で、[Networking] を選択してから、[Virtual switches] を選択します。
3. プラス (+) 記号付きの緑色の地球アイコンである [Add host networking] アイコンをクリックします。
4. [Virtual Machine Port Group for a Standard Switch] 接続タイプを選択して、[Next] をクリックします。
5. [New standard switch] を選択して、[Next] をクリックします。
6. 物理ネットワーク アダプタを新しい標準スイッチに追加します。
  - a. 割り当てられたアダプタの下で、緑色のプラス (+) 記号をクリックしてアダプタを追加します。
  - b. リストから SR-IOV に対応するネットワーク インターフェイスを選択します。たとえば、Intel(R) 82599 10 Gigabit Dual Port Network Connection を選択します。
  - c. [Failover order group] ドロップダウン メニューで、[Active adapters] から選択します。
  - d. [OK] をクリックします。
7. SR-IOV vSwitch の [Network label] を入力して、[Next] をクリックします。
8. [Ready to complete] ページで選択を確認してから、[Finish] をクリックします。

図 1 SR-IOV インターフェイスがアタッチされた新しい vSwitch



#### 次の作業

- 仮想マシンの互換性レベルを確認します。

## 仮想マシンの互換性レベルのアップグレード

互換性レベルは、ホストマシンで使用可能な物理ハードウェアに対応する仮想マシンで使用可能な仮想ハードウェアを決定します。ASAv 仮想マシンは、ハードウェア レベルを 10 以上にする必要があります。これにより、SR-IOV のパススルー機能が ASAv に公開されます。この手順では、ASAv を短時間で最新のサポートされている仮想ハードウェアバージョンにアップグレードします。

仮想マシンのハードウェアバージョンと互換性については、vSphere 仮想マシン管理マニュアルを参照してください。

#### 手順

1. vSphere Web Client から vCenter Server にログインします。
2. 変更する ASAv 仮想マシンを特定します。
  - a. データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択して、[Related Objects] タブをクリックします。
  - b. [Virtual Machines] をクリックして、リストから ASAv マシンを選択します。
3. 選択した仮想マシンの電源をオフにします。
4. ASAv を右クリックして、[Actions] > [All vCenter Actions] > [Compatibility] > [Upgrade VM Compatibility] を選択します。

## ESXi 構成でのパフォーマンスの向上

5. [Yes] をクリックして、アップグレードを確認します。
6. 互換性を持たせる仮想マシンの [ESXi 5.5 and later] オプションを選択します。
7. (オプション) [Only upgrade after normal guest OS shutdown] を選択します。

選択された仮想マシンが、選択された [Compatibility] 設定の対応するハードウェアバージョンにアップグレードされ、仮想マシンの [Summary] タブで新しいハードウェアバージョンが更新されます。

## 次の作業

SR-IOV パススルー ネットワーク アダプタを介して ASAv と仮想機能を関連付けます。

## ASAv への SR-IOV NIC の割り当て

ASAv 仮想マシンと物理 NIC がデータを交換可能なことを保証するには、ASAv を SR-IOV パススルー ネットワーク アダプタとして 1 つ以上の仮想機能に関連付ける必要があります。次の手順では、vSphere Web Client を使用して、SR-IOV NIC を ASAv 仮想マシンに割り当てる方法について説明します。

## 手順

1. vSphere Web Client から vCenter Server にログインします。
2. 変更する ASAv 仮想マシンを特定します。
  - a. データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択して、[Related Objects] タブをクリックします。
  - b. [Virtual Machines] をクリックして、リストから ASAv マシンを選択します。
3. 仮想マシンの [Manage] タブで、[Settings] > [VM Hardware] を選択します。
4. [Edit] をクリックして、[Virtual Hardware] タブを選択します。
5. [New device] ドロップダウン メニューで、[Network] を選択して、[Add] をクリックします。

[New Network] インターフェイスが表示されます。
6. [New Network] セクションを展開して、使用可能な SRIOV オプションを選択します。
7. [Adapter Type] ドロップダウン メニューで、[SR-IOV passthrough] を選択します。
8. [Physical function] ドロップダウン メニューで、パススルー仮想マシン アダプタに対応する物理アダプタを選択します。
9. 仮想マシンの電源をオンにします。

仮想マシンの電源をオンにすると、ESXi ホストが物理アダプタから空いている仮想機能を選択して、それを SR-IOV パススルー アダプタにマップします。ホストが仮想マシン アダプタと基礎となる仮想機能のすべてのプロパティを確認します。

## ESXi 構成でのパフォーマンスの向上

ESXi ホストの CPU 構成時の設定を調整することによって、ESXi 環境内の ASAv のパフォーマンスを向上させることができます。[Scheduling Affinity] オプションは、仮想マシンの CPU をホストの物理コア(およびハイパースレッディングが有効になっている場合のハイパースレッド)にどのように分散させるかを制御できるようにします。この機能を使用すれば、各仮想マシンを、指定したアフィニティ セット内のプロセッサに割り当てることができます。

詳細については、以下の VMware ドキュメントを参照してください。

- 『[vSphere Resource Management](#)』の「*Administering CPU Resources*」の章。
- 「[Performance Best Practices for VMware vSphere](#)」。
- vSphere Client [オンラインヘルプ](#)。

