VMware を使用した ASA 仮想 の導入

ASA 仮想 は、VMware ESXi を実行できる任意のサーバークラスの x86 CPU デバイスに導入できます。

重要 ASA 仮想 の最小メモリ要件は 2GB です。現在の ASA 仮想 が 2GB 未満のメモリで動作している場合、ASA 仮想 マシンのメモリを増やさないと、以前のバージョンから 9.13(1) 以降にアップグレードできません。また、最新バージョンを使用して新しい ASA 仮想 マシンを再導入できます。

注意事項と制約事項

ESXi サーバーに ASA 仮想 の複数のインスタンスを作成して導入できます。ASA 仮想 の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。作成する各仮想アプライアンスには、ホストマシン上での最小リソース割り当て（メモリ、CPU 数、およびディスク容量）が必要です。

重要 ASA 仮想 は、8GB のディスクストレージサイズで導入されます。ディスク容量のリソース割り当てを変更することはできません。

ASA 仮想 を導入する前に、次のガイドラインと制限事項を確認します。

VMWare ESXi での ASA 仮想 のシステム要件

最適なパフォーマンスを確保するために、以下の仕様に準拠していることを確認してください。ASA 仮想ASA 仮想 には、次の要件があります。

- ホスト CPU は、仮想化拡張機能を備えたサーバークラスの x86 ベースの Intel または AMD CPU である必要があります。

  たとえば、ASA 仮想 パフォーマンステストラボでは、2.6GHz で動作する Intel® Xeon® CPU E5-2690v4 プロセッサを搭載した Cisco Unified Computing System™（Cisco UCS®）C シリーズ M4 サーバーを最低限使用しています。

- ASA 仮想 は、ESXi バージョン 6.0、6.5、6.7、7.0、7.0 アップグレード 1、7.0 アップグレード 2、7.0 アップグレード 3、および 8.0 をサポートします。ASA virtual の各リリースバージョンでサポートされている ESXi バージョンについては、「Cisco Secure Firewall ASA の互換性」を参照してください。

推奨される vNIC

最適なパフォーマンスを得るためには、次の vNIC を推奨します。

- PCI パススルーでの i40e：サーバーの物理 NIC を VM に関連付け、DMA（ダイレクトメモリアクセス）を介して NIC と VM の間でパケットデータを転送します。パケットの移動に CPU サイクルは必要ありません。

- i40evf/ixgbe-vf：実質的に上記と同じですが（NIC と VM 間の DMA パケット）、NIC を複数の VM 間で共有できます。SR-IOV は、導入の柔軟性が高いため、一般的に推奨されます。注意事項と制約事項 （30 ページ）を参照してください。

- vmxnet3：10Gbps の動作をサポートしますが、CPU サイクルも必要な準仮想化ネットワークドライバです。これが VMware のデフォルトです。

  vmxnet3 を使用する場合は、TCP パフォーマンスの低下を避けるために大量受信オフロード（LRO）を無効にする必要があります。

パフォーマンスの最適化

ASA 仮想 の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、パフォーマンスの調整 （25 ページ）を参照してください。

- **NUMA**：ゲスト VM の CPU リソースを単一の Non-Uniform Memory Access（NUMA）ノードに分離することで、ASA 仮想 のパフォーマンスを向上できます。詳細については、NUMA のガイドライン （25 ページ）を参照してください。

- **Receive Side Scaling**：ASA 仮想 は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 9.13(1) 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー （27 ページ）」を参照してください。
- **VPN の最適化**：ASA 仮想 で VPN パフォーマンスを最適化するための追加の考慮事項については、VPN の最適化を参照してください。

クラスタリング

バージョン 9.17 以降、クラスタリングは VMware で展開された ASA 仮想インスタンスでサポートされます。詳細については、「ASA Cluster for the ASAv」を参照してください。

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）
- ASA 仮想 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 サーバーが 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 仮想 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 仮想 を導入すると、2 つの異なる ISO イメージが ESXi ハイパーバイザにマウントされます。
  - マウントされた最初のドライブには、vSphere によって生成された OVF 環境変数が備わってます。
  - マウントされた 2 番目のドライブは day0.iso です。

注目 ASA 仮想 マシンが起動したら、両方のドライブのマウントを解除できます。ただし、[電源投入時に接続（Connect at Power On）] がオフになっている場合でも、ドライブ 1（OVF 環境変数を使用）は、ASA 仮想 の電源をオフ/オンにするたびに常にマウントされます。

OVF テンプレートのガイドラインのエクスポート

vSphere の OVF テンプレートのエクスポート機能は、既存の ASA 仮想 インスタンスパッケージを OVF テンプレートとしてエクスポートするのに役立ちます。エクスポートされた OVF テンプレートを使用して、同じ環境または異なる環境に ASA 仮想インスタンスを導入できます。

エクスポートされた OVF テンプレートを使用して vSphere に ASA 仮想 インスタンスを導入する前に、OVF ファイルの構成の詳細を変更して、導入の失敗を防ぐ必要があります。

ASA 仮想 のエクスポートされた OVF ファイルを変更するには、次の手順を実行します。

1. OVF テンプレートをエクスポートしたローカルマシンにログインします。
2. テキストエディタで OVF ファイルを参照して開きます。
3. `<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr" vmw:value="TRUE"></vmw:ExtraConfig>` タグが存在することを確認します。
4. `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` タグを削除します。

   または

   `<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>` タグと `<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>` タグを交換します。

   詳細については、VMware が公開した「Deploying an OVF fails on vCenter Server 5.1/5.5 when VMware tools are installed (2034422)」を参照してください。
5. `UserPrivilege`、`OvfDeployment`、および `ControllerType` のプロパティ値を入力します。

   次に例を示します。

```
- <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
 ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{"ovf", "ignore", "installer"}" ovf:type="string"
 ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege">
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
ovf:key="UserPrivilege" ovf:value="15">
```

6. OVF ファイルを保存します。
7. OVF テンプレートを使用して、ASA 仮想 を導入します。VMware vSphere Web Client を使用した ASA 仮想 の導入 [英語] を参照してください。

ハイ アベイラビリティ ガイドラインのためのフェールオーバー

フェールオーバー配置の場合は、スタンバイ装置が同じライセンス権限付与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 2Gbps の権限付与であることなど）。

重要 ASA 仮想 を使用して高可用性ペアを作成する場合は、データインターフェイスを各 ASA 仮想 に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASA 仮想 に追加されると、ASA 仮想 コンソールにエラーが表示されることがあります。また、フェールオーバー機能にも影響が出ることがあります。

ASA 仮想 内部インターフェイスまたは ASA 仮想 フェールオーバーの高可用性リンクに使用される ESX ポートグループについては、2 つの仮想 NIC を使用して ESX ポートグループのフェールオーバー順序を設定します（1 つはアクティブアップリンク、もう 1 つはスタンバイアップリンク）。この設定は、2 つの VM が相互に ping を実行したり、ASA 仮想 高可用性リンクを稼働させたりするために必要です。

IPv6 のガイドライン

VMware vSphere Web クライアントを使用して ASA 仮想 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。

vMotion に関するガイドライン

- VMware では、vMotion を使用する場合、共有ストレージのみを使用する必要があります。ASA 仮想 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。ただし、ASA 仮想 を vMotion を使用して別のホストに移行する場合、ローカル ストレージを使用するとエラーが発生します。

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 仮想 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は、パフォーマンスに影響を与える可能性があります。

（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 仮想 のライセンス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

- デフォルトでは、ASA 仮想 の CPU 予約は 1000 MHz です。共有、予約、および制限の設定（[設定の編集（Edit Settings）]>[リソース（Resources）]>[CPU]）を使用することで、ASA 仮想 に割り当てられる CPU リソースの量を変更できます。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 ASA 仮想 が目的を達成できる場合は、CPU 予約の設定を 1000 Mhz 未満にできます。ASA 仮想 によって使用される CPU の量は、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、実行し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で確認できます。ASA

仮想 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ると、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 仮想 **show vm** および **show cpu** コマンド、あるいは ASDM **[ホーム（Home）]** > **[デバイスダッシュボード（Device Dashboard）]** > **[デバイス情報（Device Information）]** > **[仮想リソース（Virtual Resources）]** タブまたは **[モニタリング（Monitoring）]** > **[プロパティ（Properties）]** > **[システムリソースグラフ（System Resources Graphs）]** > **[CPU]** ペインを使用できます。
- ASA 仮想 バージョン 9.16.x 以降で、デバイス構成が 16 vCPU および 32GB RAM の ASAv100 から ASAv10 にダウングレードする場合は、デバイス構成を 1 vCPU および 4GB RAM にする必要があります。

UCS B シリーズ ハードウェアにおけるトランスペアレント モードに関するガイドライン

MAC フラップが、Cisco UCS B シリーズ ハードウェアのトランスペアレントモードで動作する一部の ASA 仮想 設定で発生することがあります。MAC アドレスがさまざまな場所で出現した場合、パケットはドロップされます。

VMware 環境にトランスペアレントモードで ASA 仮想 を導入する場合に MAC フラップを回避するには、次のガイドラインを参考にしてください。

- VMware NIC チーミング：UCS B シリーズにトランスペアレントモードで ASA 仮想 を導入する場合、内部および外部インターフェイスに使用するポートグループにはアクティブアップリンクを 1 つだけ設定し、アップリンクは同じである必要があります。vCenter で VMware NIC チーミングを設定します。

  NIC チーミングの設定方法の詳細については、VMware ドキュメントを参照してください。
- ARP インスペクション：ASA 仮想 で ARP インスペクションを有効にし、受信インターフェイスで MAC および ARP エントリを静的に設定します。ARP インスペクションと有効化の詳細については、Cisco Secure Firewall ASA シリーズ コンフィギュレーション ガイド（一般的な操作）[英語] を参照してください。

その他のガイドラインと制限事項

- ESXi 6.7、vCenter 6.7、ASA Virtual 9.12 以降を実行している場合、ASA Virtual は 2 つの CD/DVD IDE ドライブなしで起動します。
- vSphere Web Client は ASA 仮想 OVA の導入ではサポートされないため、vSphere Client を使用してください。

Vector Packet Processing を使用した IPsec フローオフロード

フローがNIC自体で切り替えられる超高速パスにオフロードされるトラフィックを識別して選択できます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション（SA）の初期設定後、IPsec 接続を ASA 仮想 デバイスの Vector Packet Processing（VPP）にオフロードできます。

（注） IPsec フローのオフロードはデフォルトで有効になっており、ASAv100 デバイスに適用されます。

シスコが開発したオープンソース アプリケーションである VPP は、IPsec 暗号化操作を実行するための IPsec オフロードに使用されます。

ASA 仮想 で IPsec オフロード機能を有効にすると、次の点で役立ちます。

- デバイスのパフォーマンスを向上させ、CPU リソースを解放して他の重要なタスクを処理する。
- IPsec 接続の総スループットパフォーマンスを向上させる。
- エレファントフローとも呼ばれる IPsec への単一接続のパフォーマンスを向上させる。

この機能をサポートするプラットフォームでは、この機能がデフォルトで無効になっています。

制限事項

次の IPsec フローはオフロードされません。

- IKEv1 トンネル。ASAv100 で有効にすると、IKEv2、ESP、および NAT-T のみが自動的にオフロードされます。IKEv2 は、より強力な暗号をサポートしています。
- 圧縮が設定されているフロー。
- 圧縮が設定されているフロー。
- トランスポートモードのフロー。トンネルモードのフローのみがオフロードされます。
- ポストフラグメンテーションが設定されているフロー。
- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。
- 64 ビット以外のアンチリプレイ ウィンドウ サイズを持ち、アンチリプレイが無効になっていないフロー。
- ファイアウォールフィルタが有効になっているフロー。
- マルチコンテキスト

VMware vSphere Web クライアントでの展開中に IPsec オフロードを有効にする方法については、VMware vSphere Web Client を使用した ASA 仮想 の導入 （15 ページ）を参照してください。

ASA 仮想 の VMware 機能のサポート

次の表に、ASA 仮想 の VMware 機能のサポートを示します。

表 *1: ASA* 仮想 の *VMware* 機能のサポート

機能	説明	サポート（あり/なし）	注釈
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。	Yes	対象外です。
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	–
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	–

機能	説明	サポート（あり/なし）	注釈
VMotion	VM のライブ マイグレーションに使用されます。	あり	共有ストレージを使用します。vMotion に関するガイドライン（5 ページ）を参照してください。
VMware FT	VM の HA に使用されます。	なし	ASA 仮想 マシンの障害に対して ASA 仮想 のフェールオーバーを使用します。
VMware HA	ESXi およびサーバの障害に使用されます。	あり	ASA 仮想 マシンの障害に対して ASA 仮想 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	ASA 仮想 マシンの障害に対して ASA 仮想 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	–

前提条件

VMware vSphere Web Client、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 ASA 仮想 を導入できます。システム要件については、Cisco Secure Firewall ASA の互換性 [英語] 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、ASA 仮想 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 Address Changes]：[Accept]
- [Forged Transmits]：[Accept]

次の ASA 仮想 設定の場合、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

ASA 仮想 ソフトウェアの解凍と第 0 日用構成ファイルの作成

ASA 仮想 を起動する前に、第 0 日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、ASA 仮想 の起動時に適用される ASA 仮想 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 サーバーを設定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。

始める前に

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。

- 初期導入時に自動的に ASA 仮想 にライセンスを付与するには、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 日用構成ファイルと同じディレクトリに保存します。
- 仮想 VGA コンソールではなく、ハイパーバイザのシリアルポートから ASA 仮想 にアクセスし、設定する場合は、第 0 日用構成ファイルに**コンソール シリアル**の設定を追加して初回ブート時にシリアルポートを使用する必要があります。

- トランスペアレントモードで ASA 仮想 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 構成ファイルを、第 0 日用構成ファイルとして使用する必要があります。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。
- ISO イメージが ESXi ハイパーバイザにどのようにマウントされるかの詳細については、注意事項と制約事項 （1 ページ）の OVF ファイルのガイドラインを参照してください。

手順

ステップ 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。

https://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。

ステップ 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：ASA 仮想 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。

ステップ 3 「day0-config」というテキストファイルに ASA 仮想 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 ASA 仮想 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方法です。day0-config 内の行の順序は重要で、既存の **show running-config** 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 ASA 仮想 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 ASA 仮想 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 ASA 仮想 を導入します。注意事項と制約事項 （30 ページ）を参照してください。

例：

```
ASA Version 9.4.1
!
console serial
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：

```
ASA Version 9.8.1
!
console serial
interface management 0/0
management-only
nameif management
security-level 0
ip address 192.168.0.230 255.255.255.0
!
interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0
ipv6 address 2001:10::1/64
!
interface GigabitEthernet0/1
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
```

ステップ 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。

ステップ 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 サーバーに ASA 仮想 が自動的に登録されます。

ステップ 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。

例：

```
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$
```

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

例：

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

ステップ 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。

例：

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

ステップ 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 ASA 仮想 の導入

この項では、VMware vSphere Web Client を使用して ASA 仮想 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ASA仮想の導入」、または「OVF ツールおよび第 0 日用構成を使用した ASA 仮想 の導入」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、ASA 仮想 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

ステップ 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。

ステップ 2 （1 回のみ）ASA 仮想 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。

1. 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。
2. 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。
3. 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。

ステップ 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 仮想 の導入

ASA 仮想 を導入するには、VMware vSphere Web Client（または vSphere Client）、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 仮想 パッケージを展開するには、vSphere Web Client で Deploy OVF Template ウィザードを使用します。このウィザードでは、ASA 仮想 OVA ファイルを解析し、ASA 仮想 を実行する仮想マシンを作成し、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。

始める前に

ASA 仮想 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

ステップ 1 ASA 仮想 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。

ステップ 2 vSphere Web Client の [Navigator] ペインで、[vCenter] をクリックします。

ステップ 3 [Hosts and Clusters] をクリックします。

ステップ 4 ASA 仮想 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。

ステップ 5 ウィザード画面の指示に従って進みます。

Cisco Secure Firewall ASA バージョン 9.22 以降では、[設定（Configuration）] ウィンドウで、[ASAvU - 32 コア/64 GB（ASAvU - 32 Core / 64 GB）] または [ASAvU - 64コア/128 GB（ASAvU - 64 Core / 128 GB）] の導入設定を選択してレート制限を削除することができます。ASAvU ライセンスの詳細については、『Licensing for the ASA Virtual』を参照してください。

ステップ 6 [Setup networks] 画面で、使用する各 ASA 仮想 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 仮想 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 仮想 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 仮想 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 仮想 インターフェイス ID
ネットワーク アダプタ 1	Management 0/0
ネットワーク アダプタ 2	GigabitEthernet 0/0
ネットワーク アダプタ 3	GigabitEthernet 0/1
ネットワーク アダプタ 4	GigabitEthernet 0/2
ネットワーク アダプタ 5	GigabitEthernet 0/3
ネットワーク アダプタ 6	GigabitEthernet 0/4
ネットワーク アダプタ 7	GigabitEthernet 0/5
ネットワーク アダプタ 8	GigabitEthernet 0/6
ネットワーク アダプタ 9	GigabitEthernet 0/7
ネットワーク アダプタ 10	GigabitEthernet 0/8

すべての ASA 仮想 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 仮想 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 仮想 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。

ステップ 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。

ステップ 8 フェールオーバー/HA 配置では、[Customize] テンプレート画面で次を設定します。

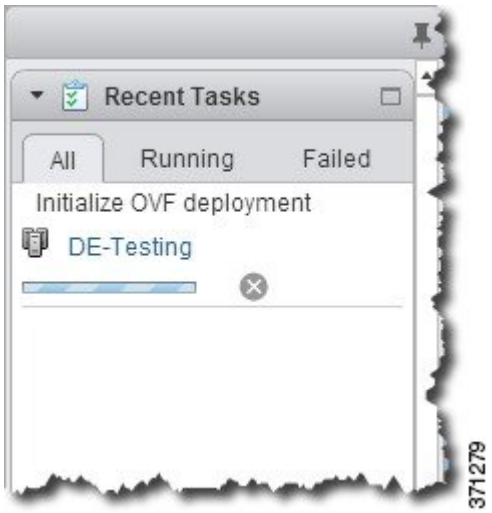
- スタンバイ管理 IP アドレスを指定します。

  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。

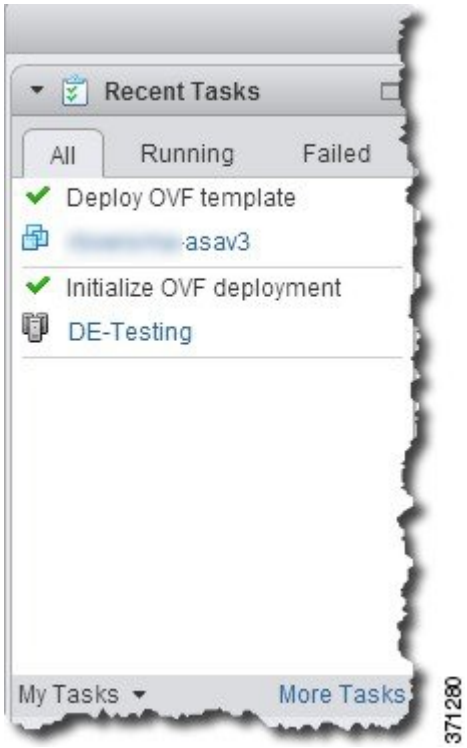
- [HA Connection Settings] 領域で、フェールオーバー リンクを設定します。

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。

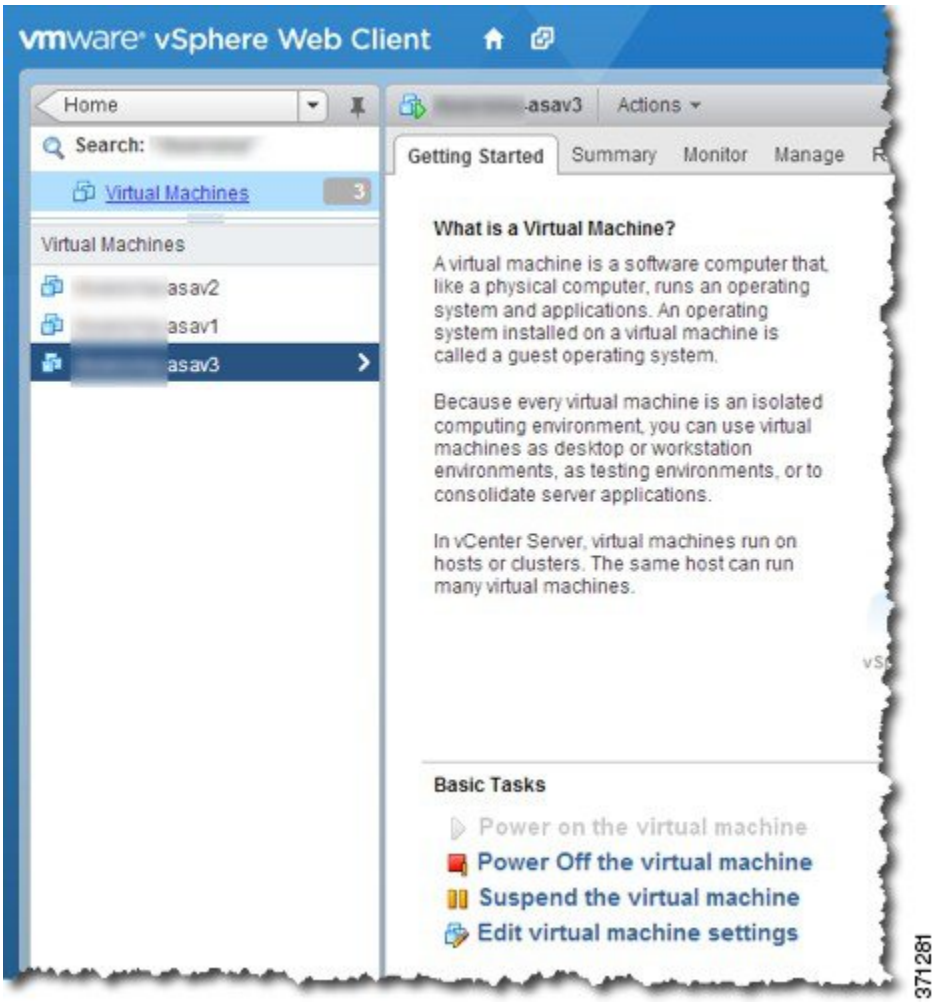
ステップ 9 ウィザードが完了すると、vSphere Web Client は VM を処理します。[Global Information] 領域の [Recent Tasks] ペインで [Initialize OVF deployment] ステータスを確認できます。



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、ASA 仮想 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。



ステップ 10 ASA 仮想マシンがまだ稼働していない場合は、[仮想マシンの電源をオン（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 仮想 が起動するのを待ちます。ASA 仮想 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 仮想 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 仮想 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 仮想 コンソールにアクセスします。

ステップ 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。

- プライマリ装置とまったく同じ 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。

次のタスク

Cisco Licensing Authority に ASA 仮想 を正常に登録するには、ASA 仮想 にインターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、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 仮想 の導入

ASA 仮想 を導入するには、VMware vSphere Client 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、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 仮想 パッケージを導入するには、vSphere Client で [OVFテンプレートの導入（Deploy OVF Template）] ウィザードを使用します。このウィザードでは、ASA 仮想 OVA ファイルを解析し、ASA 仮想 を実行する仮想マシンを作成し、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。

始める前に

- ASA 仮想 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。
- ASA 仮想 ソフトウェアの解凍と第 0 日用構成ファイルの作成 （10 ページ）の手順に従って、第 0 日用構成を作成します。

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5 ASA 仮想 の電源を投入し、VMware コンソールを開いて、2 回目の起動を待機します。

ステップ 6 ASA 仮想 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 ファイルに必要なすべての構成がされていない場合は、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 仮想 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 仮想 の導入

このセクションでは、第 0 日用構成ファイルを必要とする OVF ツールを使用した ASA 仮想 の導入方法について説明します。

始める前に

- OVF ツールを使用して ASA 仮想 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 仮想 ソフトウェアの解凍と第 0 日用構成ファイルの作成 （10 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 サーバーに接続できることを確認します。

手順

ステップ 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。

例：

```
linuxprompt# which ovftool
```

ステップ 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=4Core8GB \
--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/
```

ステップ 3 cmd ファイルを実行します。

例：

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

ASA 仮想 の電源を投入し、2 回目の起動を待機します。

ステップ 4 ASA 仮想 に SSH 接続し、必要に応じて設定を完了します。さらに設定が必要な場合は、ASA 仮想 に対して VMware コンソールを開き、必要な設定を適用します。

これで、ASA 仮想 は完全に動作可能な状態です。

ASA 仮想 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
- ネットワーク シリアル コンソール ポートの設定

（注） 第 0 日用構成ファイルを使用して ASA 仮想 を導入する場合、構成ファイルに**コンソールシリアル**の設定を追加して、初回ブート時に仮想 VGA コンソールではなくシリアルポートを使用できます。ASA 仮想 ソフトウェアの解凍と第 0 日用構成ファイルの作成 （10 ページ）を参照してください。

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。

始める前に

vSphere Web Client では、ASA 仮想 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

ステップ 1 VMware vSphere Web Client で、インベントリの ASA 仮想 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] をクリックします。

ステップ 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。

ASA 仮想 がまだ起動中の場合は、起動メッセージが表示されます。

ASA 仮想 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 仮想 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 仮想 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、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。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、ユーザー EXEC モードで作業していることを示します。ユーザー EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

例：

```
ciscoasa> enable
```

次のプロンプトが表示されます。

```
Password:
```

ステップ 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。

ステップ 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 ASA 仮想 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。ASA 仮想 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。この手順では、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

ステップ 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。

ステップ 2 ASA 仮想 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 **[ツール（Tools）]** > **[ファイル管理（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
```

ステップ 3 ASA 仮想をリロードします。

- 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 仮想 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。

ステップ 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 仮想 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 仮想 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 仮想 は適切に動作しません。

手順

ステップ 1 新しいライセンスを要求します。

ステップ 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。

ステップ 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 仮想 の電源を切断します。たとえば、ASA 仮想 をクリックしてから [仮想マシンの電源をオフ（Power Off the virtual machine）] をクリックするか、または ASA 仮想 を右クリックして [ゲストOSをシャットダウン（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 仮想 の電源を切断します。たとえば、ASA 仮想 をクリックしてから [仮想マシンの電源をオフ（Power Off the virtual machine）] をクリックするか、または ASA 仮想 を右クリックして [ゲストOSをシャットダウン（Shut Down Guest OS）] を選択します。

ステップ 4 ASA 仮想 をクリックしてから [仮想マシンの設定の編集（Edit Virtual machine settings）] をクリックします（または ASA 仮想 を右クリックして [設定の編集（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。

ステップ 5 新しい vCPU ライセンスの正しい値を確認するには、ASA 仮想 のライセンスにある CPU 要件とメモリ要件を参照してください。

ステップ 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。

ステップ 7 [Memory] には、新しい RAM の値を入力します。

ステップ 8 [OK] をクリックします。

ステップ 9 ASA 仮想の電源を入れます。たとえば、[Power On the Virtual Machine] をクリックします。

ステップ 10 フェールオーバー ペアの場合：

1. 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。
2. 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、[Make Standby] をクリックします。
   - CLI： **failover active**
3. アクティブ装置に対して、ステップ 3 ～ 9 を繰り返します。

次のタスク

詳細については、「ASA 仮想 のライセンス」を参照してください。

パフォーマンスの調整

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 ASA 仮想 のパフォーマンスを向上させることができます。[Scheduling Affinity] オプションによって、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。

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

NUMA のガイドライン

Non-uniform Memory Access（NUMA）は、マルチプロセッサシステムのプロセッサに対するメインメモリモジュールの配置について記述する共有メモリアーキテクチャです。プロセッサが自身のノード（リモートメモリ）内に存在しないメモリにアクセスする場合は、ローカルメモリにアクセスする場合よりも低速の速度で、NUMA 接続を介してデータを転送する必要があります。

X86 サーバーアーキテクチャは、複数のソケットおよびソケット内の複数のコアで構成されています。各 CPU ソケットとそのメモリおよび I/O が、NUMA ノードと呼ばれます。メモリか

らパケットを効率的に読み取るには、ゲストアプリケーションおよび関連付けられている周辺機器（NIC など）が同じノード内に存在する必要があります。

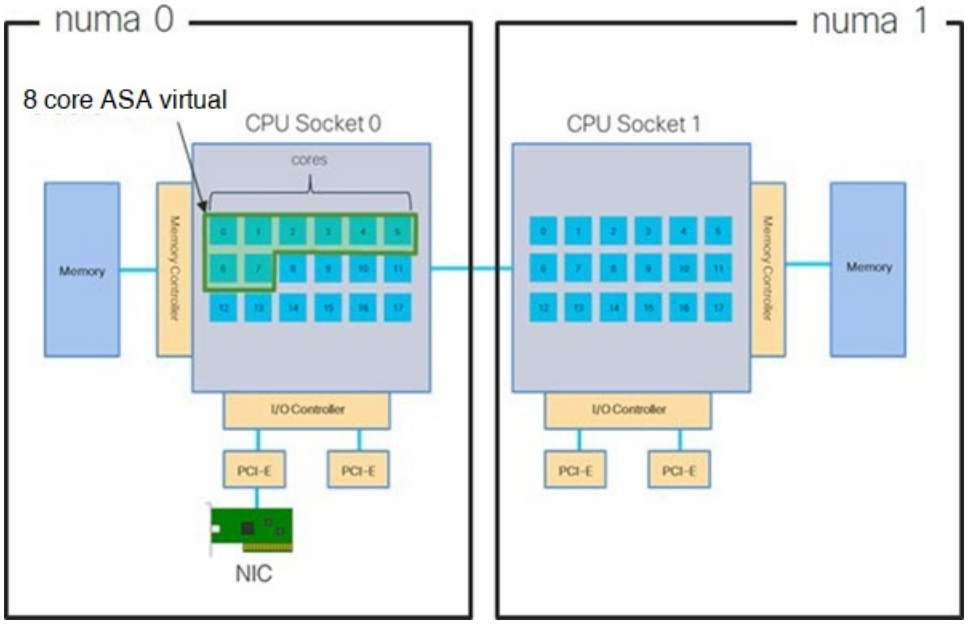
最適な ASA 仮想 パフォーマンスを実現するには：

- ASA 仮想 マシンは、1つの NUMA ノード上で実行する必要があります。1つの ASA 仮想 が2つのソケットで実行されるように導入されている場合、パフォーマンスは大幅に低下します。
- 8 コア ASA 仮想（図 1 : 8 コア NUMA アーキテクチャの例 （26 ページ））では、ホスト CPU の各ソケットが、それぞれ8個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- 16 コア ASA 仮想（図 2 : 16 コア ASA 仮想 NUMA アーキテクチャの例 （27 ページ））では、ホスト CPU 上の各ソケットが、それぞれ 16 個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- NIC は、ASA 仮想 マシンと同じ NUMA ノード上にある必要があります。

（注） ASA 仮想 は、複数の Non-uniform Memory Access（NUMA）ノードおよび物理コア用の複数の CPU ソケットをサポートしません。

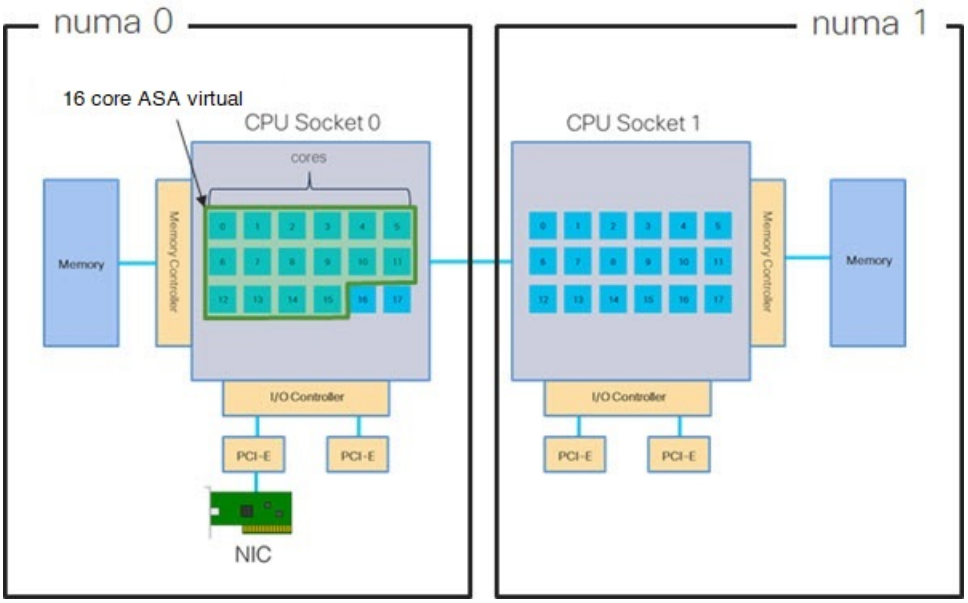
次の図は、2 つの CPU ソケットがあり、各 CPU に 18 個のコアが搭載されているサーバーを示しています。8 コア ASA 仮想 では、ホスト CPU の各ソケットに最低 8 個のコアが必要です。

図 *1 : 8* コア *NUMA* アーキテクチャの例



次の図は、2 つの CPU ソケットがあり、各 CPU に 18 個のコアが搭載されているサーバーを示しています。16 コア ASA 仮想 では、ホスト CPU の各ソケットに最低 16 個のコアが必要です。

図 *2 : 16* コア *ASA* 仮想 *NUMA* アーキテクチャの例



NUMA システムと ESXi の使用に関する詳細については、VMware ドキュメント『*vSphere Resource Management*』で、お使いの VMware ESXi バージョンを参照してください。このドキュメントおよびその他の関連ドキュメントの最新のエディションを確認するには、http://www.vmware.com/support/pubs を参照してください。

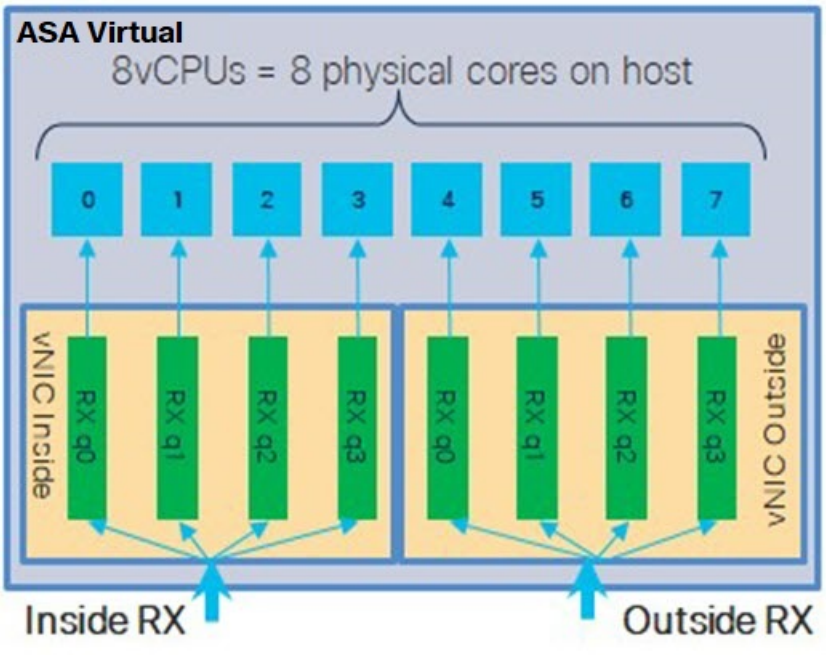
Receive Side Scaling（RSS）用の複数の RX キュー

ASA 仮想 は、複数のプロセッサコアにネットワーク受信トラフィックを分散するためにネットワークアダプタによって使用されるテクノロジーである Receive Side Scaling（RSS）をサポートしています。最大スループットを実現するには、各 vCPU（コア）に独自の NIC RX キューが設定されている必要があります。一般的な RA VPN 展開では、1つの内部/外部ペアのインターフェイスを使用する場合があることに注意してください。

重要 複数の RX キューを使用するには、ASA 仮想 バージョン 9.13(1) 以降が必要です。

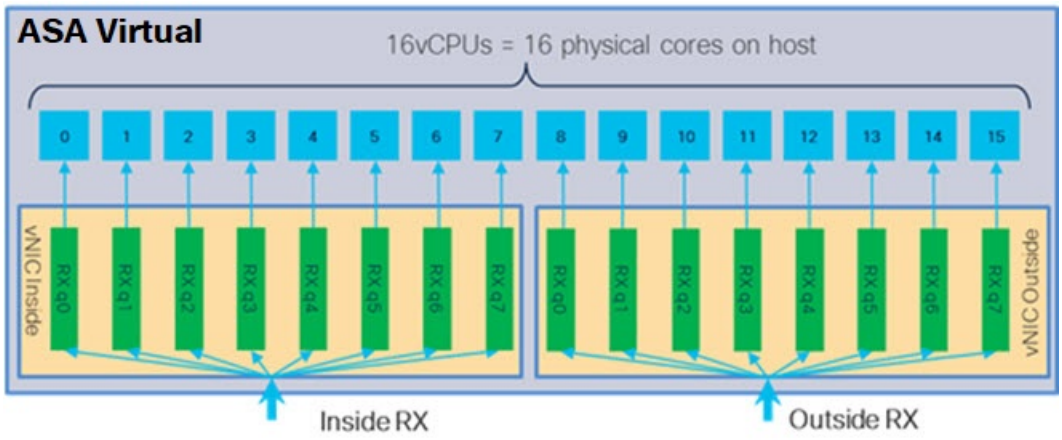
内部/外部ペアのインターフェイスを持つ 8 コア VM の場合、図 3 : 8 コア ASA 仮想 RSS RX キュー （28 ページ）に示すように、各インターフェイスには 4 つの RX キューがあります。

図 *3 : 8* コア *ASA* 仮想 *RSS RX* キュー



内部/外部ペアのインターフェイスを持つ 16 コア VM の場合、図 4 : 16 コア ASA 仮想 RSS RX キュー （28 ページ）に示すように、各インターフェイスには 8 つの RX キューがあり ます。

図 *4 : 16* コア *ASA* 仮想 *RSS RX* キュー



次の表に、VMware 用の ASA 仮想 の vNIC およびサポートされている RX キューの数を示します。サポートされている vNIC の説明については、推奨される vNIC （2 ページ）を参照してください。

表 *3 : VMware* で推奨される *NIC/vNIC*

NIC カード	vNIC ドライバ	ドライバテクノロジー	RX キューの数	パフォーマンス
x710*	i40e	PCI パススルー	最大 8	PCIパススルーは、テストされたNIC の中で最高のパフォーマンスを提供します。パススルーモードでは、NIC は ASA 仮想 専用であり、仮想環境に最適な選択肢ではありません。
	i40evf	SR-IOV	4	X710 NIC を使用した SR-IOV のスループットは PCI パススルーよりも（最大 30%）低下します。VMware の i40evf には、i40evf ごとに最大 4 つの RX キューがあります。16 コア VM で最大スループットを実現するには、8 つの RX キューが必要です。
x520	ixgbe-vf	SR-IOV	2	—
	ixgbe	PCI パススルー	6	ixgbe ドライバ（PCI パススルーモード）には、6 つの RX キューがあります。パフォーマンスは i40evf（SR-IOV）と同等です。
該当なし	VMXNET3	準仮想化	最大 8	ASAv100 には推奨されません。
該当なし	e1000	VMware では推奨されません。		
*ASA 仮想 は、x710 NIC の 1.9.5 i40en ホストドライバと互換性がありません。これより古いバージョンまたは新しいバージョンのドライバは動作します。NIC ドライバとファームウェアのバージョンを識別または確認するための ESXCLI コマンドの詳細については、NIC ドライバとファームウェアバージョンの識別 （29 ページ）を参照してください。				

NIC ドライバとファームウェアバージョンの識別

特定のファームウェアおよびドライバのバージョン情報を識別または確認する必要がある場合は、ESXCLI コマンドを使用してそのデータを見つけることができます。

- インストールされている NIC のリストを取得するには、関連するホストに SSH 接続し、`esxcli network nic list` コマンドを実行します。このコマンドから、デバイスおよび一般情報の記録が得られるはずです。

- インストールされているNICのリストを取得すれば、詳細な設定情報を得ることができます。必要なNICの名前を指定して、`esxcli network nic get` コマンドを実行します：`esxcli network nic get -n <nic name>`。

（注） 一般的なネットワークアダプタ情報は、VMware vSphere クライアントから確認することもできます。アダプタとドライバは、[Configure] タブ内の [Physical Adapters] の下にあります。

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 サーバー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す。このセクションでは、KVM 環境で VF を設定する方法について説明します。ASA 仮想 上の SR-IOV サポートについては、ASA 仮想 と SR-IOV インターフェイスのプロビジョニングを参照してください。

ASAv5 および ASAv10 で最適なパフォーマンスを得るため、VMXNET3 ドライバを強く推奨します。さらに、SR-IOV インターフェイスを組み合わせて（インターフェイスが混在した状態で）使用すると、特により多くの CPU コアとリソースを割り当てることで、ASA 仮想 とのネットワークパフォーマンスが向上します。

注意事項と制約事項

SR-IOV インターフェイス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。

SR-IOV インターフェイスに関するガイドラインと制限事項 に記載されている ASA 仮想 と SR-IOV に関するシステム要件に加えて、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。

SR-IOV インターフェイスを使用する VMware 上の ASA 仮想 では、インターフェイスタイプの混在がサポートされています。管理インターフェイスにはSR-IOV またはVMXNET3 を使用し、データインターフェイスには SR-IOV を使用することができます。

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 サーバー、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。

SR-IOV インターフェイスに関する制限事項

ASA 仮想 を起動すると、ESXi で表示される順序とは逆の順序で、SR-IOV インターフェイスが表示される場合があります。これにより、インターフェイス設定エラーが発生し、特定の ASA 仮想 マシンへのネットワーク接続が切断する場合があります。

⚠

注意 ASA 仮想 で SR-IOV ネットワーク インターフェイスの設定を開始する前に、インターフェイスのマッピングを確認することが重要です。これにより、ネットワーク インターフェイスの設定が、VM ホストの正しい物理 MAC アドレスインターフェイスに適用されます。

ASA 仮想 が起動したら、MAC アドレスとインターフェイスのマッピングを確認できます。**show interface** コマンドを使用して、インターフェイスの MAC アドレスなど、インターフェイスの詳細情報を確認します。インターフェイス割り当てが正しいことを確認するには、**show kernel ifconfig** コマンドの結果と MAC アドレスを比較します。

ESXi ホスト BIOS の確認

VMware に SR-IOV インターフェイスを備えた ASA 仮想 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、仮想化サポートの各種確認手段を提供しています。

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

ステップ 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。

ステップ 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。

ステップ 3 次のコマンドを実行します。

例：

```
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。

例：

```
~ # 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。

次のタスク

- 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

vSphere Web Client を使用して、ホストで SR-IOV を有効にし、仮想機能の数を設定します。設定しないと、仮想マシンを仮想機能に接続できません。

始める前に

- 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 でサポートされている NICを参照してください。

手順

ステップ 1 vSphere Web Client で、SR-IOV を有効にする ESXi ホストに移動します。

ステップ 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。

ステップ 3 物理アダプタを選択し、[Edit adapter settings] をクリックします。

ステップ 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。

ステップ 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。

ステップ 6 [OK] をクリックします。

ステップ 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。

次のタスク

- 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

ステップ 1 vSphere Web Client で、ESXi ホストに移動します。

ステップ 2 [Manage] で、[Networking] を選択してから、[Virtual switches] を選択します。

ステップ 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。

ステップ 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。

ステップ 5 [New standard switch] を選択して、[Next] をクリックします。

ステップ 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。

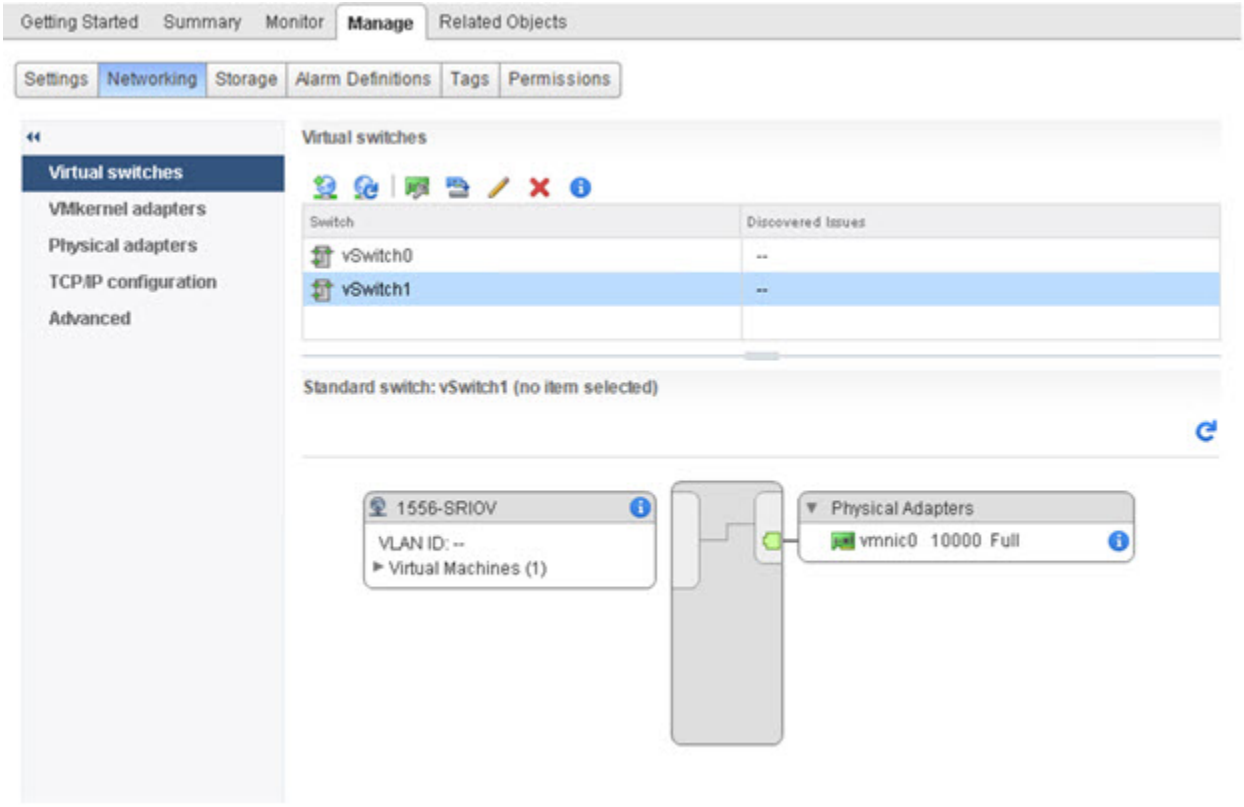
c) [Failover order group] ドロップダウン メニューで、[Active adapters] から選択します。

d) [OK] をクリックします。

ステップ 7 SR-IOV vSwitch の [Network label] を入力して、[Next] をクリックします。

ステップ 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 *5 : SR-IOV* インターフェイスがアタッチされた新しい *vSwitch*



次のタスク

- 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。ASA 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 ASA 仮想 に公開されます。この手順では、ASA 仮想 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

ステップ 1 vSphere Web Client から vCenter Server にログインします。

ステップ 2 変更する ASA 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) [仮想マシン（Virtual Machines）] をクリックして、リストから ASA 仮想 マシンを選択します。

ステップ 3 選択した仮想マシンの電源をオフにします。

ステップ 4 ASA 仮想 を右クリックして、**[アクション（Actions）]** > **[すべてのvCenterアクション（All vCenter Actions）]** > **[互換性（Compatibility）]** > **[VMアップグレードの互換性（Upgrade VM Compatibility）]** を選択します。

ステップ 5 [Yes] をクリックして、アップグレードを確認します。

ステップ 6 仮想マシンの互換性で [ESXi 5.5 and later] オプションを選択します。

ステップ 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。

次のタスク

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

ASA 仮想 への SR-IOV NIC の割り当て

ASA 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、ASA 仮想 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 ASA 仮想 マシンに割り当てる方法について説明します。

手順

ステップ 1 vSphere Web Client から vCenter Server にログインします。

ステップ 2 変更する ASA 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) [仮想マシン（Virtual Machines）] をクリックして、リストから ASA 仮想 マシンを選択します。

ステップ 3 仮想マシンの [Manage] タブで、**[Settings]** > **[VM Hardware]** を選択します。

ステップ 4 [Edit] をクリックして、[Virtual Hardware] タブを選択します。

ステップ 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。

ステップ 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。

ステップ 7 [Adapter Type] ドロップダウン メニューで、[SR-IOV passthrough] を選択します。

ステップ 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。

ステップ 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。

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。