Cisco適応型セキュリティ仮想アプライアンス（ASAv）9.10スタートアップガイド

初版：2018年10月25日

最終更新：2020年7月20日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

目 次

第 1 章

ASAv の概要 1

ハイパーバイザのサポート 1

ASAv のライセンス 1

ASAv のライセンス 2

注意事項と制約事項 5

ASAv（すべてのモデル）のガイドラインと制限事項 5

ASAv5 のガイドラインと制限事項 6

ASAv10 のガイドラインと制限事項 7

ASAv50 のガイドラインと制限事項 8

ASAv インターフェイスおよび仮想 NIC 8

ASAv のインターフェイス 9

サポートされている vNIC 9

ASAv と SR-IOV インターフェイスのプロビジョニング 11

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 12

第 2 章

VMware を使用した ASAv の導入 17

VMware での ASAv のガイドラインと制限事項 17

ASAv の VMware 機能のサポート 21

ASAv と VMware の前提条件 23

ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 24

VMware vSphere Web Client を使用した ASAv の導入 27

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 28

VMware vSphere Web Client を使用した ASAv の導入 28

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 33
OVF ツールおよび第 0 日用構成を使用した ASAv の導入 34
ASAv コンソールへのアクセス 35
VMware vSphere コンソールの使用 35
ネットワーク シリアル コンソール ポートの設定 36
vCPU またはスループット ライセンスのアップグレード 37
VMware での ASAv のパフォーマンス調整 38
ESXi 構成でのパフォーマンスの向上 38
NUMA のガイドライン 39
Receive Side Scaling（RSS）用の複数の RX キュー 40
SR-IOV インターフェイスのプロビジョニング 42
注意事項と制約事項 43
ESXi ホスト BIOS の確認 43
ホスト物理アダプタ上での SR-IOV の有効化 44
vSphere スイッチの作成 45
仮想マシンの互換性レベルのアップグレード 46
ASAv への SR-IOV NIC の割り当て 47

第 3 章 **KVM を使用した ASAv の導入** 49
KVM での ASAv のガイドラインで制限事項 49
KVM を使用した ASAv の導入について 50
ASAv と KVM の前提条件 50
第 0 日のコンフィギュレーション ファイルの準備 52
仮想ブリッジ XML ファイルの準備 54
ASAv の起動 55
ホットプラグ インターフェイス プロビジョニング 56
注意事項と制約事項 56
ネットワーク インターフェイスのホットプラグ 57
KVM での ASAv のパフォーマンス調整 58
KVM 構成でのパフォーマンスの向上 58

CPU ピンニングの有効化 58
NUMA のガイドライン 60
Receive Side Scaling（RSS）用の複数の RX キュー 61
VPN の最適化 63
SR-IOV インターフェイスのプロビジョニング 64
SR-IOV インターフェイスのプロビジョニングに関する要件 64
KVM ホスト BIOS とホスト OS の変更 64
ASAv への PCI デバイスの割り当て 66
CPU 使用率とレポート 69
ASA Virtual の vCPU 使用率 70
CPU 使用率の例 70
KVM CPU 使用率レポート 70
ASA Virtual と KVM のグラフ 71

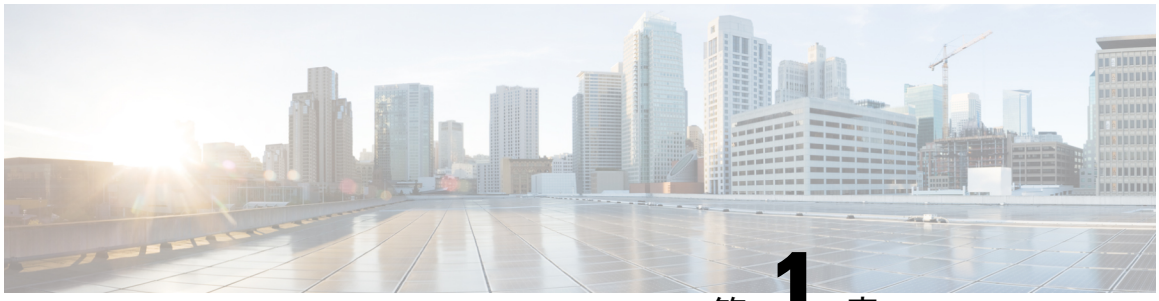
第 4 章 **AWS クラウドへの ASAv の導入 73**
AWS クラウドへの ASAv の導入について 73
ASAv と AWS の前提条件 74
ASAv および AWS のガイドラインと制限事項 75
設定の移行と SSH 認証 76
AWS 上の ASAv のネットワークトポロジの例 77
AWS での ASAv の展開 77

第 5 章 **Microsoft Azure クラウドへの ASAv の導入 81**
Microsoft Azure クラウドへの ASAv 導入について 81
ASAv および Azure の前提条件およびシステム要件 82
注意事項と制約事項 83
導入時に作成されるリソース 85
Azure ルーティング 87
仮想ネットワーク内の VM のルーティング設定 88
IP Addresses 88
DNS 89

Microsoft Azure への ASAv の導入 89
Azure Resource Manager からの ASAv の導入 89
Azure Security Center からの ASAv の導入 91
Azure Resource Manager からの ASAv for High Availability の導入 93

第 6 章 **Hyper-V を使用した ASAv の導入 97**
Hyper-V を使用した ASAv の導入について 97
ASAv および Hyper-V のガイドラインと制限事項 98
ASAv と Hyper-V の前提条件 99
第 0 日のコンフィギュレーション ファイルの準備 100
Hyper-V マネージャを使用した ASAv と第 0 日用構成ファイルの導入 102
コマンドラインを使用した Hyper-V への ASAv のインストール 103
Hyper-V マネージャを使用した Hyper-V への ASAv のインストール 104
Hyper-V マネージャからのネットワーク アダプタの追加 111
ネットワーク アダプタの名前の変更 113
MAC アドレス スプーフィング 114
Hyper-V マネージャを使用した MAC アドレス スプーフィングの設定 114
コマンド ラインを使用した MAC アドレス スプーフィングの設定 114
SSH の設定 115
CPU 使用率とレポート 115
ASA Virtual の vCPU 使用率 115
CPU 使用率の例 116

第 7 章 **ASAv の設定 117**
ASDM の起動 117
ASDM を使用した初期設定の実行 118
Startup Wizard の実行 118
（任意）ASAv の内側にあるパブリックサーバーへのアクセス許可 119
（オプション）VPN ウィザードの実行 119
（オプション）ASDM の他のウィザードの実行 120
詳細設定 120



第 1 章

ASAv の概要

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、データセント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。

- ハイパーバイザのサポート （1 ページ）
- ASAv のライセンス （1 ページ）
- ASAv のライセンス （2 ページ）
- 注意事項と制約事項 （5 ページ）
- ASAv インターフェイスおよび仮想 NIC （8 ページ）
- ASAv と SR-IOV インターフェイスのプロビジョニング （11 ページ）

ハイパーバイザのサポート

ハイパーバイザのサポートについては、Cisco ASA の互換性 [英語] を参照してください。

ASAv のライセンス

ASAv はシスコ スマート ソフトウェア ライセンシングを使用しています。詳細については、「Smart Software Licensing」を参照してください。

（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 ライセンスの権限付与と、サポートされているプライベートおよびパブリック導入ターゲットのリソース仕様については、以降の各セクションを参照してください。

ASAv のライセンス

ASAv ライセンス資格、ライセンスの状態、必要なリソース、およびモデル仕様に関する情報については、次の表を参照してください。

- 表 1 : ASAv スマートライセンス資格：ASAv プラットフォームのライセンスの権限付与の条件を満たすリソースシナリオ準拠を示しています。

（注） ASAv は Cisco Smart Software Licensing を使用します。スマート 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、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。

- 表 2 : ASAv ライセンスの状態：ASAv のリソースと資格に関連した状態とメッセージを示しています。
- 表 3 : ASAv モデルの説明と仕様：ASAv モデルと関連仕様、リソース要件、および制限事項を示しています。

スマート ライセンス資格

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 and ASA』を参照してください。

（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。

表 *1 : ASAv* スマートライセンス資格

ライセンスの権限付与	vCPU/RAM	スループット	適用されるレート リミッタ
ラボ エディション モード（ライセンスは不要）	すべてのプラットフォーム	100 Kbps	あり
ASAv5（100M）	1 vCPU/1 GB ～ 1.5 GB（2 GB 推奨）	100Mbps	あり
ASAv10（1 GB）	1 vCPU/2 GB	1Gbps	あり

ライセンスの権限付与	vCPU/RAM	スループット	適用されるレート リミッタ
ASAv30（2 GB）	4 vCPU/8 GB	2 Gbps	あり
ASAv50（10 GB）	8 vCPU/16 GB	10 Gbps	あり

ライセンスの状態

表 *2 : ASAv* ライセンスの状態

状態	リソース対権限付与	アクションおよびメッセージ
Compliant	リソース = 権限付与の上限 （vCPU、GB の RAM）	アプライアンスに最適にリソースが割り当てられます ASAv5（1vCPU、1G）、ASAv10（1vCPU、2G）、ASAv30（4vCPU、8G）、ASAv50（8vCPU、16G） アクションなし、メッセージなし
	リソース < 権限付与の上限 アンダープロビジョニングされます	ASAv がライセンスのスループットで実行できないとの警告メッセージが記録されている間はアクションなし
Non-compliant	リソース > 権限付与の上限 オーバープロビジョニングされます	ASAv レート リミッタによってパフォーマンスが制限され、コンソールに警告が出力されます。
		ASAv10、ASAv30、および ASAv50 は、エラー メッセージがコンソールに出力された後、リブートします。

モデルの説明と仕様

表 *3 : ASAv* モデルの説明と仕様

モデル	ライセンス要件
ASAv5	スマート 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 • 1 GB RAM（1.5 GB に調節可能） （注） 最適なパフォーマンスを実現するには、ASAv5 に 2 GB のメモリを推奨します。 • 50,000 の同時ファイアウォール接続 • AWS はサポート対象外 • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート
ASAv10	スマート 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 • c3.large、c4.large、および m4.large インスタンスで AWS をサポート • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート

モデル	ライセンス要件
ASAv30	スマート 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 • c3.xlarge、c4.xlarge、および m4.xlarge インスタンスで AWS をサポート • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート
ASAv50	スマート ライセンス 次の仕様を参照してください。 • 10 Gbps スループット • 8 vCPU（CPU ソケットあたり 8 個以上の物理コアが必要。複数の CPU ソケットにはプロビジョニングできない） • 16 GB メモリ • 2,000,000 の同時ファイアウォール接続 • AWS、Microsoft Azure、または Hyper-V をサポートしません。

注意事項と制約事項

ASAv ファイアウォール機能は ASA ハードウェア ファイアウォールとよく似ていますが、次のガイドラインと制限事項があります。

ASAv（すべてのモデル）のガイドラインと制限事項

ディスク ストレージ

ASAv は、デフォルトで最大 8 GB の仮想ディスクをサポートします。ディスクサイズを 8 GB を超えて増やすことはできません。VM リソースをプロビジョニングする場合は、この点に注意してください。

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。

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）。

重要 ASAv 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 ASAv 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 ASAv に追加されると、ASAv 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。

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。

- クラスタリング（KVM と VMware を除くすべての権限付与）
- 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

制限事項

- ASAv 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。（VMware のみ）

ASAv5 のガイドラインと制限事項

パフォーマンスのガイドライン

- 1 秒あたり 8000 接続、最大 25 の VLAN、50,000 の同時セッション、および 50 の VPN セッションをサポートします。
- ASAv5 は小さいメモリ フットプリントと低スループットを必要とするユーザー向けであるため、不要なメモリを使用することなく多数の ASAv5 を導入できます。
- 9.5(1.200) 以降、AVAv5 のメモリ要件は 1 GB に減りました。ASAv5 で使用可能なメモリを 2 GB から 1 GB にダウングレードすることはサポートされていません。1 GB のメモリで実行するには、ASAv5 VM を 9.5(1.200) 以降のバージョンで再導入する必要がありま

す。同様に、9.5(1.200) より前のバージョンにダウングレードする場合、メモリを 2 GB に増やす必要があります。

（注） 最適なパフォーマンスを実現するには、ASAv5 に 2 GB のメモリを推奨します。

- 場合によっては、ASAv5 のメモリが枯渇状態になります。これは、AnyConnect の有効化やファイルのダウンロードなど、特定リソースの利用が多い場合に発生することがあります。
  - 自動的な再起動に関するコンソールメッセージやメモリ使用量に関する重大な syslog が、メモリ枯渇の状態を示します。
  - このような場合、1.5 GB メモリの VM に ASAv5 を導入できます。1 GB から 1.5 GB に変更するには、VM の電源をオフにして、メモリを変更し、VM の電源を再度オンにします。
  - CLI から `show memory` コマンドを使用して、システムで使用可能な最大メモリと現在の空きメモリ量の概要を表示できます。
- ASAv5 は、100 Mbps のしきい値に達するとすぐに、パケットのドロップを開始します（100 Mbps をすべて使用できるように、多少のヘッドルームがあります）。

制限事項

- ASAv5 は AnyConnect HostScan 4.8 と互換性がありません。これには 2 GB の RAM が必要です。
- ASAv5 は Amazon Web Services（AWS）ではサポートされていません。
- ジャンボ フレームはサポートされていません。

ASAv10 のガイドラインと制限事項

パフォーマンスのガイドライン

- 9 つ以上の設定済み e1000 インターフェイスを使用した ASAv10 のジャンボフレーム予約によって、デバイスがリロードされる場合があります。**ジャンボ フレーム予約**が有効になっている場合は、インターフェイスの数を 8 つ以下に減らしてください。インターフェイスの正確な数は、その他の構成済み機能の操作で必要となるメモリの量によって異なりますが、8 つより少なくすることはできます。

ASAv50 のガイドラインと制限事項

パフォーマンスのガイドライン

- 集約トラフィックで 10 Gbps がサポートされます。
- ESXi と KVM でのみサポートされます。
- ASAv のパフォーマンスを向上させるために、次のプラクティスがサポートされています。
  - NUMA ノード
  - 複数の RX キュー
  - SR-IOV プロビジョニング
  - 詳細については、VMware での ASAv のパフォーマンス調整（38 ページ）および KVM での ASAv のパフォーマンス調整（58 ページ）を参照してください。
- フルスループットレートを実現するため、CPU ピンニングを推奨します。ESXi 構成でのパフォーマンスの向上（38 ページ）および KVM 構成でのパフォーマンスの向上（58 ページ）を参照してください。
- ジャンボフレーム予約で e1000 インターフェイスと i40e-vf インターフェイスが混在していると、i40e-vf インターフェイスがダウン状態のままになる場合があります。**ジャンボフレーム予約**が有効になっている場合は、e1000 ドライバと i40e-vf ドライバを使用するインターフェイスのタイプが混在しないようにしてください。

制限事項

- トランスペアレント モードはサポートされていません。
- ASAv 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。（VMware のみ）
- Amazon Web Services（AWS）、Microsoft Azure、および Hyper-V ではサポートされません。
- Ixgbe vNIC はこのリリースではサポートされていません。

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 のインターフェイス
- サポートされている vNIC

ASAv のインターフェイス

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

  AWS と Azure の場合は、Management 0/0 をトラフィック伝送用の「外部」インターフェイスにすることができます。

- 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。

（注） 構成を簡単に移行できるように、Ten GigabitEthernet（VMXNET3 ドライバで使用可能なインターフェイスなど）には GigabitEthernet というラベルが付いています。これは表面的なものであり、実際のインターフェイス速度には影響しません。

ASAv では、E1000 ドライバを 1 Gbps リンクとして使用してギガビット イーサネット インターフェイスが定義されます。VMware では E1000 ドライバの使用が推奨されなくなっていることに注意してください。

- Hyper-V は最大 8 つのインターフェイスをサポートします。Management 0/0 および GigabitEthernet 0/0 ～ 0/6。フェールオーバー リンクとして GigabitEthernet 0/6 を使用できます。

サポートされている vNIC

ASAv では次の vNIC がサポートされています。同じ ASAv での vNIC の混在（e1000 と vmxnet3 など）はサポートされていません。

表 *4*：サポートされている *vNIC*

表 *5*：サポートされている *vNIC*

vNIC のタイプ	ハイパーバイザのサポート		ASAv バージョン	注意
	VMware	KVM		
e1000	対応	対応	9.2(1) 以降	VMware のデフォルト
virtio	非対応	対応	9.3(2.200) 以降	KVM のデフォルト
ixgbe-vf	対応	対応	9.8(1) 以降	AWS のデフォルト。SR-IOV サポート用の ESXi と KVM

vNIC のタイプ	ハイパーバイザのサポート		ASAv バージョン	注意
	VMware	KVM		
VMXNET3	対応	非対応	9.9(2) 以降	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。VMware および VMXNET3 の LRO を無効にします （10 ページ）を参照してください。
i40e-vf	非対応	対応	9.10(1) 以降	SR-IOV サポート用の KVM

VMware および VMXNET3 の LRO を無効にします

Large Receive Offload（LRO）は、CPU オーバーヘッドを削減することによって、高帯域幅ネットワーク接続のインバウンドスループットを向上させる手法です。これは、1 つのストリームからの複数の着信パケットを大きなバッファに集約してから、ネットワークスタックの上位に渡されるようにすることによって、処理する必要があるパケットの数を減らすことによって機能します。ただし、LRO は、ネットワークパケット配信のフローが一貫せず、輻輳しているネットワークで「バースト」する可能性がある場合に、TCP パフォーマンスの問題を引き起こす可能性があります。

重要 VMware は、デフォルトで LRO を有効にして、全体的なスループットを向上させます。したがって、このプラットフォームで ASAv 導入の LRO を無効にする必要があります。

ASAv マシンで LRO を直接無効化できます。設定変更を行う前に、仮想マシンの電源をオフにします。

1. vSphere Web Client インベントリで ASAv マシンを検索します。
    1. 仮想マシンを検索するには、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ます。
    2. [Related Objects] タブをクリックし、[Virtual Machines] タブをクリックします。
2. 仮想マシンを右クリックして、[Edit Settings] をクリックします。
3. [VM Options] をクリックします。
4. [Advanced] を展開します。
5. [Configuration Parameters] の下で、[Edit Configuration] ボタンをクリックします。
6. [Add Parameter] をクリックし、LRO パラメータの名前と値を入力します。
    - Net.VmxnetSwLROSL | 0

- Net.Vmxnet3SwLRO | 0
- Net.Vmxnet3HwLRO | 0
- Net.Vmxnet2SwLRO | 0
- Net.Vmxnet2HwLRO | 0

（注） オプションで、LROパラメータが存在する場合は、値を調べて必要に応じて変更できます。パラメータが 1 に等しい場合、LRO は有効です。0 に等しい場合、LRO は無効です。

7. [OK] をクリックして変更を保存し、[Configuration Parameters] ダイアログボックスを終了します。
8. [保存（Save）] をクリックします。

詳細については、次の VMware サポート記事を参照してください。

- VMware KB 1027511
- VMware KB 2055140

ASAv と SR-IOV インターフェイスのプロビジョニング

Single Root I/O Virtualization（SR-IOV）により、さまざまなゲスト オペレーティング システムを実行している複数の VM が、ホスト サーバー内の単一の PCIe ネットワーク アダプタを共有できるようになります。SR-IOV では、VM がネットワーク アダプタとの間で直接データを移動でき、ハイパーバイザをバイパスすることで、ネットワークのスループットが増加しサーバーの CPU 負荷が低下します。最近の x86 サーバー プロセッサには、SR-IOV に必要なダイレクト メモリの転送やその他の操作を容易にする Intel VT-d テクノロジーなど、チップセットの拡張機能が搭載されています。

SR-IOV 仕様では、次の 2 つのデバイス タイプが定義されています。

- 物理機能（PF）：基本的にスタティック NIC です。PF は、SR-IOV 機能を含む完全な PCIe デバイスです。PF は、通常の PCIe デバイスとして検出、管理、設定されます。単一 PF は、一連の仮想関数（VF）の管理および設定を提供できます。
- Virtual Function（VF）：ダイナミック vNIC に似ています。VF は、データ移動に必要な最低限のリソースを提供する、完全または軽量の仮想 PCIe デバイスです。VF は直接的には管理されず、PF を介して配信および管理されます。1 つ以上の VF を 1 つの VM に割り当てることができます。

SR-IOV は、PCI 標準の開発および管理が公認されている業界組織である Peripheral Component Interconnect Special Interest Group（PCI SIG）によって定義および管理されています。SR-IOV の詳細については、『PCI-SIG SR-IOV Primer: An Introduction to SR-IOV Technology』を参照してください。

ASAv 上で SR-IOV インターフェイスをプロビジョニングするには、適切なオペレーティング システム レベル、ハードウェアと CPU、アダプタタイプ、およびアダプタの設定から始める計画が必要です。

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

ASAv の導入に使用する具体的なハードウェアは、サイズや使用要件によって異なります。ASAv のライセンス （1 ページ） には、さまざまな ASAv プラットフォームに関するライセンスの権限付与条件に準拠するリソースシナリオが説明されています。加えて、SR-IOV 仮想機能には特定のシステム リソースが必要です。

ホスト オペレーティング システムとハイパーバイザ サポート

SR-IOV サポートと VF ドライバは、以下で使用できます。

- Linux 2.6.30 カーネル以降

SR-IOV インターフェイスを備えた ASAv は、現在、次のハイパーバイザでサポートされています。

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

ハードウェア プラットフォーム サポート

（注） サポートされている仮想化プラットフォームを実行できる任意のサーバークラスの x86 CPU デバイスに ASAv を導入する必要があります。

このセクションでは、SR-IOV インターフェイスに関するハードウェア ガイドラインについて説明します。以下はガイドラインであって要件ではありませんが、このガイドラインに従っていないハードウェアを使用すると、機能の問題や性能の低下につながる可能性があります。

SR-IOV をサポートしており、SR-IOV 対応 PCIe アダプタを搭載したサーバーが必要です。以下のハードウェア検討事項に留意する必要があります。

- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。
- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。

（注） メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。

- VT-d 対応のチップセット、マザーボード、および CPU については、『virtualization-capable IOMMU supporting hardware』を参照してください。VT-d は、SR-IOV システムに必須の BIOS 設定です。
- VMware の場合は、オンラインの『Compatibility Guide』で SR-IOV サポートを検索できます。
- KVM の場合は、『CPU compatibility』を確認できます。KVM 上の ASAv では、x86 ハードウェアしかサポートされないことに注意してください。

（注） シスコでは、ASAv を Cisco UCS C シリーズ ラックサーバーでテストしました。Cisco UCS-B サーバーは ixgbe-vf vNIC をサポートしていないことに注意してください。

SR-IOV でサポートされている NIC

- Intel イーサネット ネットワーク アダプタ X710

注目 ASAv 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。（VMware のみ）

- Intel Ethernet Server Adapter X520 - DA2
- Intel Ethernet Server Adapter X540

CPU

- x86_64 マルチコア CPU

  Intel Sandy Bridge 以降（推奨）

（注） シスコでは、ASAv を 2.3GHz の Intel Broadwell CPU（E5-2699-v4）でテストしました。

- コア
  - CPU ソケットあたり 8 個以上の物理コア

- 単一のソケット上で 8 コアにする必要があります。

（注） CPU ピンニングは、ASAv50 および ASAv100 上でフルスループットレートを実現するために推奨されています。ESXi 構成でのパフォーマンスの向上 （38 ページ）とKVM 構成でのパフォーマンスの向上 （58 ページ）を参照してください。

BIOS 設定

SR-IOV は、BIOS だけでなく、ハードウェアで実行しているオペレーティング システム インスタンスまたはハイパーバイザのサポートも必要です。システム BIOS で次の設定をチェックします。

- SR-IOV が有効になっている。
- VT-x（仮想化テクノロジー）が有効になっている。
- VT-d が有効になっている。
- （オプション）ハイパースレッディングが無効になっている。

システムごとに BIOS 設定にアクセスして変更する方法が異なるため、ベンダーのマニュアルでプロセスを確認することをお勧めします。

制限事項

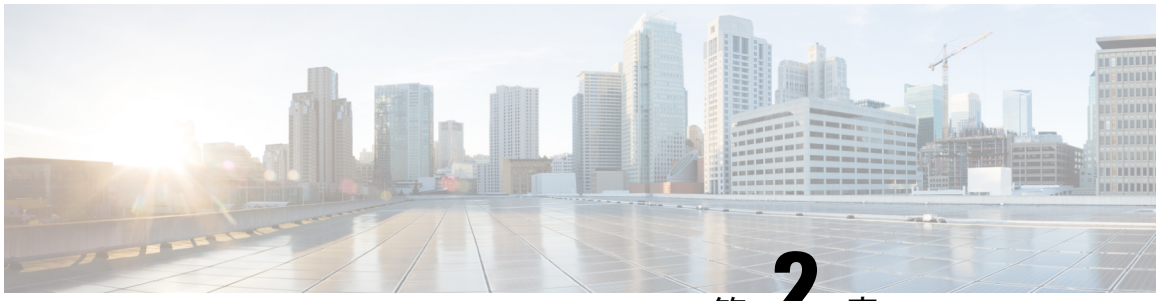
ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の ASA プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている ASAv（プライマリ装置）に障害が発生すると、スタンバイ ASAv 装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ ASAv 装置の新しい MAC アドレスで更新されます。その後、ASAv は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更を同じネットワーク上の他のデバイスに

通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。



第 2 章

VMware を使用した ASAv の導入

ASAv 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。

- VMware での ASAv のガイドラインと制限事項 （17 ページ）
- ASAv の VMware 機能のサポート （21 ページ）
- ASAv と VMware の前提条件 （23 ページ）
- ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 （24 ページ）
- VMware vSphere Web Client を使用した ASAv の導入 （27 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 ASAv の導入 （33 ページ）
- OVF ツールおよび第 0 日用構成を使用した ASAv の導入 （34 ページ）
- ASAv コンソールへのアクセス （35 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 （37 ページ）
- VMware での ASAv のパフォーマンス調整 （38 ページ）

VMware での ASAv のガイドラインと制限事項

ESXi サーバーに ASAv の複数のインスタンスを作成して導入できます。ASAv 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。

ASAv 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 ASAv 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。ASAvASAv 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、ASAv 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。

- ASAv 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、および 7.0 アップグレード 3 をサポートします。

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）
- 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。
- 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 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 ASAv 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、ASAv 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 ASAv 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 ASAv 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 ASAv 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。

ASAv 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、ASAv を導入します。VMware vSphere Web Client を使用した ASAv 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 ASAv 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 ASAv 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 ASAv に追加されると、ASAv 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。

ASAv 内部インターフェイスまたは ASAv 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、ASAv 高可用性リンクを稼働させたりするために必要です。

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。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。ただし、ASAv 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

- 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、ASAv のライセンス （1 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。

場合によっては、ASAv5 のメモリが枯渇状態になります。この状態は、AnyConnect クライアントの有効化やファイルのダウンロードなど、特定のリソースの利用が多い場合に発生することがあります。自動的な再起動に関するコンソールメッセージやメモリ使用量に関する重大な syslog が、メモリ枯渇の状態を示します。このような場合、1.5 GB メモリの VM に ASAv5 を導入できます。1 GB から 1.5 GB に変更するには、VM の電源をオフにして、メモリを変更し、VM の電源を再度オンにします。

CPU 予約

- デフォルトでは、ASAv 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、ASAv 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 ASAv 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。ASAv 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。ASAv 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、ASAv **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。

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 ASAv 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 ASAv 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 ASAv 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：ASAv 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 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 ASAv 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。

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 *6 : ASAv 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	–

機能	説明	サポート（あり/なし）	注釈
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	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	–
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	共有ストレージを使用します。vMotion に関するガイドライン（20 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	ASAv マシンの障害に対して ASAv のフェールオーバーを使用します。
VMware HA	ESXi およびサーバの障害に使用されます。	あり	ASAv マシンの障害に対して ASAv のフェールオーバーを使用します。

機能	説明	サポート（あり/なし）	注釈
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	ASAv マシンの障害に対して 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 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 ASAv を導入できます。システム要件については、Cisco 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、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 7: ポート グループのセキュリティ ポリシーの例外

	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	
セキュリティの例外	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

	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	
セキュリティの例外	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
不正送信	<任意>	承認	承認	承認

ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成

ASAv 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、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 ASAv 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 ASAv 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 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 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、VMware での ASAv のガイドラインと制限事項 （17 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。

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：ASAv 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 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 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。注意事項と制約事項 （43 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
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.10.20.10 255.255.255.0
!
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 ASAv 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 (bytes): 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 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」、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」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 （28 ページ）
- VMware vSphere Web Client を使用した ASAv の導入 （27 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。

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）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。

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 ASAv の導入

ASAv 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 ASAv 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、ASAv OVA ファイルを解析し、ASAv 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

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。

ステップ 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。

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 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。

ステップ 5 ウィザード画面の指示に従って進みます。

ステップ 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	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 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。

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。

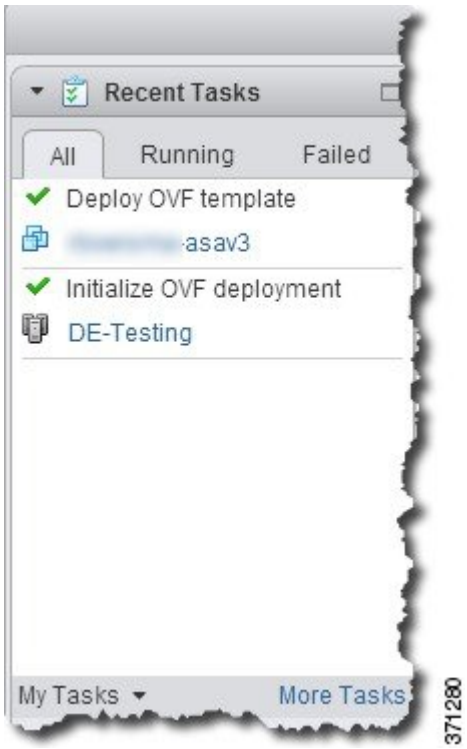
  インターフェイスを設定する場合、同じネットワーク上のアクティブ IP アドレスとスタンバイ IP アドレスを指定する必要があります。プライマリ装置が故障すると、セカンダリ装置はプライマリ装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。現在スタンバイになっている装置が、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

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

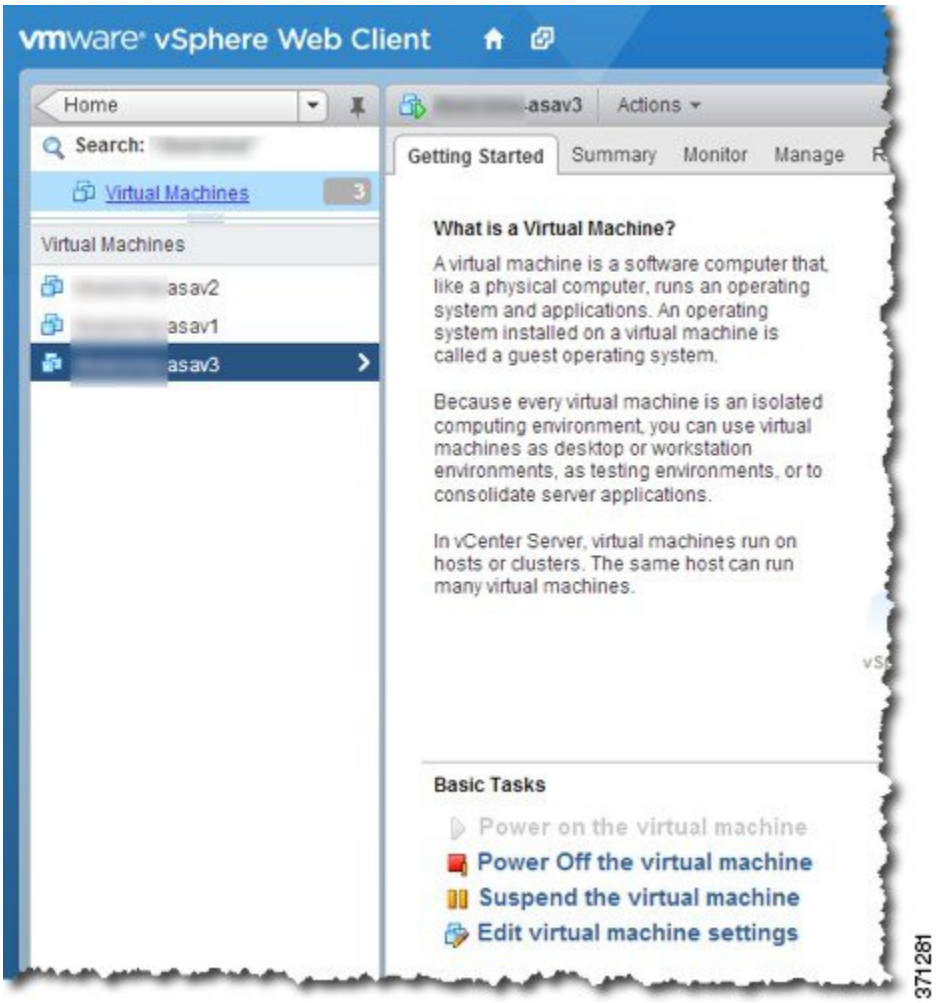
  フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。GigabitEthernet 0/8 がフェールオーバー リンクとして事前設定されています。同じネットワーク上のリンクに対するアクティブな IP アドレスとスタンバイの IP アドレスを入力します。

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、ASAv 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 ASAv 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、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。

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 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 ASAv の導入

ASAv 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 ASAv 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、ASAv OVA ファイルを解析し、ASAv 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

- 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。
- ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 （24 ページ）の手順に従って、第 0 日用構成を作成します。

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 ASAv 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 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、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

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 ASAv 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 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 ソフトウェアの解凍と第 0 日用構成ファイルの作成 （24 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。

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=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/
```

ステップ 3 cmd ファイルを実行します。

例：

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

ASAv の電源を投入し、2 回目の起動を待機します。

ステップ 4 ASAv 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、ASAv 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、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
- 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 ASAv 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。ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 （24 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、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。

ステップ 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。

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、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 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。

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 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 **[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 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。

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

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 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。

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 ASAv の電源を切断します。たとえば、ASAv 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 ASAv 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、ASAv の電源を切断します。たとえば、ASAv 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 ASAv 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 ASAv 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 ASAv 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、ASAv のライセンス （1 ページ）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 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。

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、「ASAv のライセンス （1 ページ）」を参照してください。

VMware での ASAv のパフォーマンス調整

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 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。

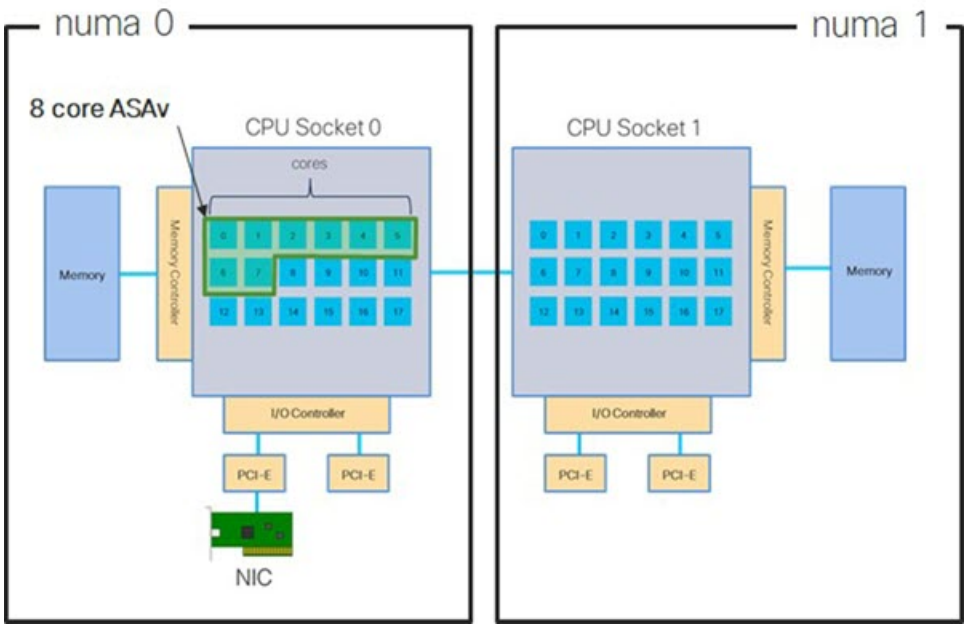
最適な ASAv パフォーマンスを実現するには：

- ASAv 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 ASAv 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 ASAv（図 1 : 8 コア NUMA アーキテクチャの例 （40 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。
- NIC は、ASAv マシンと同じ NUMA ノード上にある必要があります。

（注） ASAv 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 ASAv 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



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。

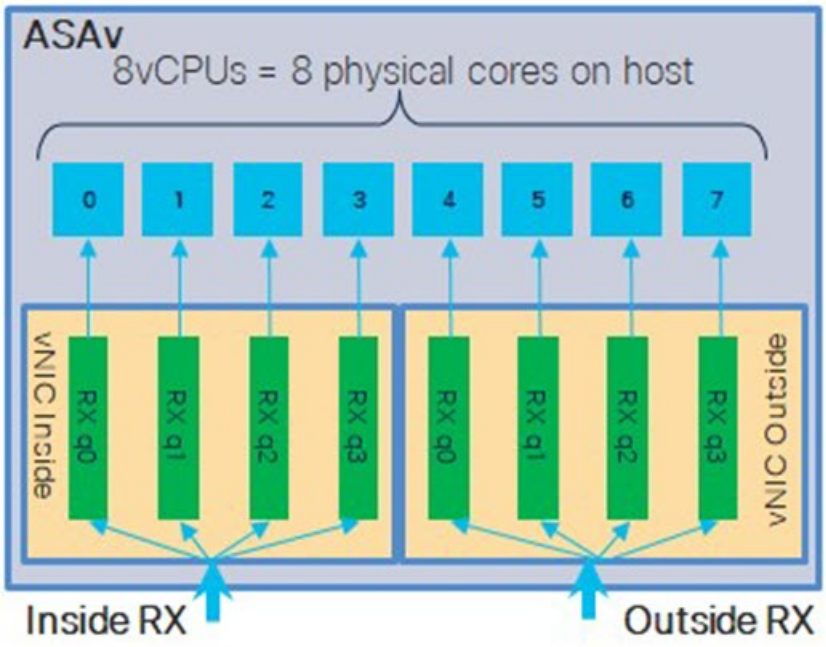
Receive Side Scaling（RSS）用の複数の RX キュー

ASAv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、ASAv 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 2 : 8 コア ASAv RSS RX キュー（41 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 *2 : 8* コア *ASAv RSS RX* キュー



次の表に、VMware 用の ASAv 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、#unique_21 unique_21_Connect_42_section_unm_s52_glbを参照してください。

表 *8 : 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 ASAv 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。

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
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。		
*ASAv 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 （42 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 ASAv 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。ASAv 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 （11 ページ）を参照してください。

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 （12 ページ） に記載されている ASAv 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。

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

ASAv 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 ASAv 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 ASAv 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。

ASAv 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 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。

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 （13 ページ）を参照してください。

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。

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。

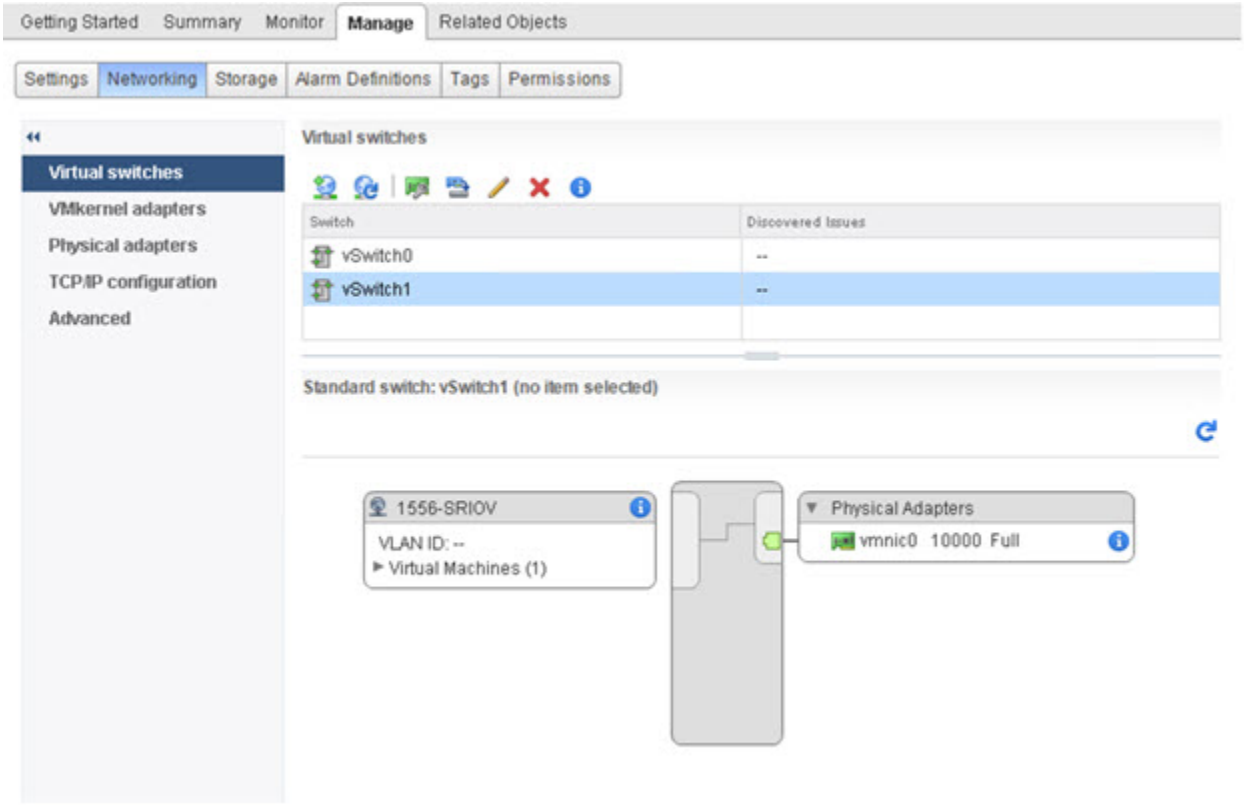
ステップ 6 物理ネットワーク アダプタを新しい標準スイッチに追加します。

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 *3 : 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。ASAv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。

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

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 ASAv 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 ASAv 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。

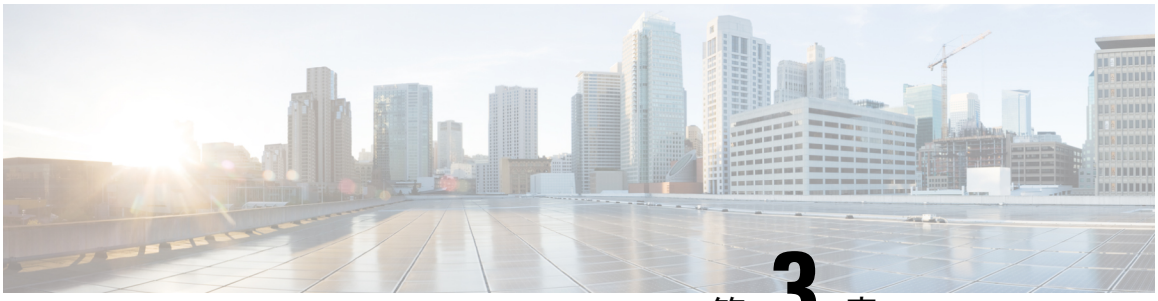
ステップ 6 [New Network] セクションを展開して、使用可能な SRIOV オプションを選択します。

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。



第 3 章

KVM を使用した ASAv の導入

カーネルベースの仮想マシン（KVM）を実行できる任意のサーバークラスの x86 CPU デバイスに ASAv を導入できます。

- KVM での ASAv のガイドラインで制限事項 （49 ページ）
- KVM を使用した ASAv の導入について （50 ページ）
- ASAv と KVM の前提条件 （50 ページ）
- 第 0 日のコンフィギュレーション ファイルの準備 （52 ページ）
- 仮想ブリッジ XML ファイルの準備 （54 ページ）
- ASAv の起動 （55 ページ）
- ホットプラグ インターフェイス プロビジョニング （56 ページ）
- KVM での ASAv のパフォーマンス調整 （58 ページ）
- CPU 使用率とレポート （69 ページ）

KVM での ASAv のガイドラインで制限事項

ASAv 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。

ASAv 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。

KVM での ASAv 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。ASAv 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、ASAv 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。

CPU ピニング

KVM 環境で ASAv を機能させるには、CPU ピニングが必要です。CPU ピンニングの有効化（58 ページ）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

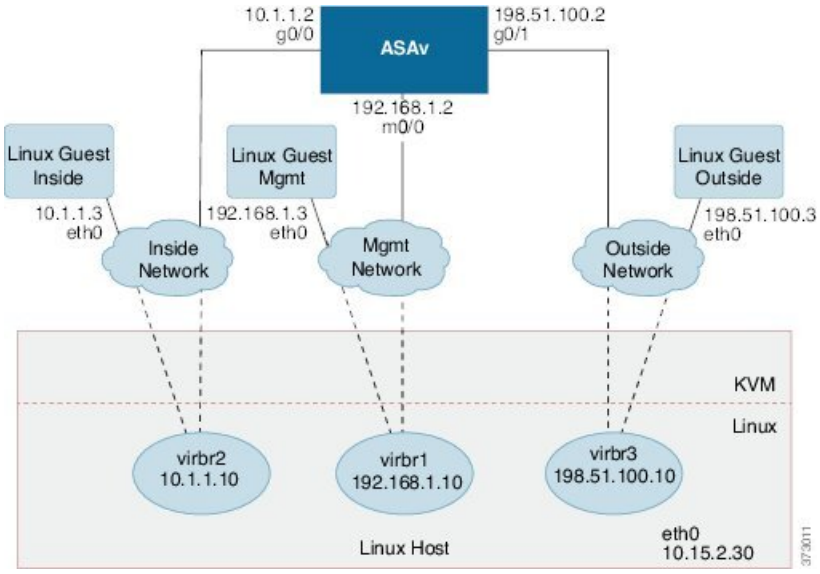
フェールオーバー配置の場合は、スタンバイ装置が同じモデルライセンスを備えていることを確認してください（たとえば、両方の装置が ASAv30s であることなど）。

重要 ASAv 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 ASAv 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 ASAv に追加されると、ASAv 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。

KVM を使用した ASAv の導入について

次の図は、ASAv と KVM のネットワークトポロジの例を示します。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。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 *4: 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。

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。

- このマニュアルの導入例では、ユーザーが 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、『NFV Delivers Packet Processing Performance with Intel』を参照してください。
- Ubuntu 14.04 の便利な最適化には、次のものが含まれます。
  - 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 Linux 7 Virtualization Tuning and Optimization Guide』を参照してください。
- ASA ソフトウェアおよび ASAv ハイパーバイザの互換性については、Cisco ASA の互換性 [英語] 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。

day0.iso ファイル（カスタム day0.iso またはデフォルト day0.iso）は、最初の起動中に使用できる必要があります。

- 初期導入時に自動的に ASAv 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 ASAv 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 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 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。

（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。

ステップ 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関連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。

例：

```
ASA Version 9.4.1
!
console serial
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
```

ステップ 2 （任意）ASAv の初期導入時に自動的にライセンスを許諾する場合は、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）SSmart 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 サーバー
- 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

ステップ 3 （任意）Cisco Smart Software Manager によって発行された 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、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。

ステップ 4 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$
```

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

ステップ 5 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構成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 ホスト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 （52 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。

ステップ 1 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。次の例では、virbr1.xml、virbr2.xml、および virbr3.xml です。

例：

```
<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>
```

例：

```
<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>
```

例：

```
<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>
```

ステップ 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
```

ステップ 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。このスクリプトは、仮想ネットワークを稼働状態にします。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。

ステップ 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$
```

ステップ 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

virt-install ベースの導入スクリプトを使用して ASAv を起動できます。

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

ASAv マシンの名前は、この KVM ホスト上の他の全 VM で一意である必要があります。

ASAv では最大 10 のネットワークがサポートされます。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（Management 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、GigabitEthernet 0/8 まで同様に続きます。仮想 NIC は Virtio でなければなりません。

例：

```
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 \
--virt-type=kvm \
--import \
--disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=virtio,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
```

ステップ 2 virt_install スクリプトを実行します。

例：

```
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。

ホットプラグ インターフェイス プロビジョニング

ASAv を停止して再起動することなく、インターフェイスを動的に追加および削除できます。ASAv マシンに新しいインターフェイスを追加する場合、ASAv はそのインターフェイスを通常のインターフェイスとして検出してプロビジョニングできる必要があります。同様に、ホットプラグ プロビジョニングによって既存のインターフェイスを削除する場合、ASAv はそのインターフェイスを削除して、関連付けられたすべてのリソースを解放する必要があります。

注意事項と制約事項

インターフェイスのマッピングと番号付け

- ホットプラグインターフェイスを追加する場合、そのインターフェイス番号は、現在の最後のインターフェイス番号に 1 を加えた数になります。
- ホットプラグインターフェイスを削除すると、それが最後の番号のインターフェイスである場合を除き、インターフェイス番号にギャップが生じます。
- インターフェイス番号にギャップがあると、次にホットプラグプロビジョニングされるインターフェイスはそのギャップを埋める番号を使用します。

フェールオーバー

- ホットプラグ インターフェイスをフェールオーバーリンクとして使用する場合、リンクは、ASAv のフェールオーバーペアとして指定されている両方のユニットでプロビジョニングする必要があります。
  - まずハイパーバイザのアクティブ ASAv にホットプラグ インターフェイスを追加してから、ハイパーバイザのスタンバイ ASAv にホットプラグ インターフェイスを追加します。
  - アクティブ ASAv に新たに追加したフェールオーバー インターフェイスを設定します。設定はスタンバイ装置に同期されます。
  - プライマリ ユニットのフェールオーバーを有効にします。
- フェールオーバーリンクを削除する場合、最初にアクティブな ASAv でフェールオーバー設定を削除します。
  - ハイパーバイザのアクティブな ASAv からフェールオーバー インターフェイスを削除します。
  - 次に、ハイパーバイザのスタンバイ ASAv から対応するインターフェイスをすぐに削除します。

制限事項と制約事項

- ホットプラグ インターフェイス プロビジョニングは Virtio 仮想 NIC に限定されます。
- サポートされるインターフェイスの最大数は 10 です。10 を超える数のインターフェイスを追加しようとすると、エラーメッセージが表示されます。
- インターフェイス カード（media_ethernet/port/id/10）を開くことはできません。
- ホットプラグ インターフェイス プロビジョニングでは ACPI が必要です。virt-install スクリプトには `--noacpi` フラグを含めないでください。

ネットワーク インターフェイスのホットプラグ

KVM ハイパーバイザのインターフェイスを追加および削除するには、virsh コマンド ラインを使用します。

ステップ 1 virsh コマンド ラインのセッションを開きます。

例：

```
[root@asav-kvmterm ~]# virsh
Welcome to virsh, the virtualization interactive terminal.
Type: 'help' for help with commands
'quit' to quit
```

ステップ 2 インターフェイスを追加するには、**attach-interface** コマンドを使用します。

attach-interface{ **--domain** *domain* **--type** *type* **--source** *source* **--model** *model* **--mac** *mac* **--live**}

--domain には、短整数、名前、または完全 UUID を指定できます。--type パラメータは、物理的なネットワーク デバイスを示す *network*、またはデバイスへのブリッジを示す *bridge* のどちらかを指定できます。--source パラメータは、接続のタイプを示します。--model パラメータは、仮想 NIC のタイプを示します。--mac パラメータは、ネットワーク インターフェイスの MAC アドレスを指定します。--live パラメータは、コマンドが実行しているドメインに影響を与えることを示します。

（注） 使用可能なオプションの詳細については、virsh の公式ドキュメントを参照してください。

例：

```
virsh # attach-interface --domain asav-network --type bridge --source br_hpi --model virtio --mac
52:55:04:4b:59:2f --live
```

（注） ASAv でインターフェイス コンフィギュレーション モードを使用して、トラフィックの送受信インターフェイスを設定して有効化します。詳細については、『Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』の「*Basic Interface Configuration*」の章を参照してください。

ステップ 3 インターフェイスを削除するには、**detach-interface** コマンドを使用します。

detach-interface{ **--domain** *domain* **--type** *type* **--mac** *mac* **--live**}

（注） 使用可能なオプションの詳細については、*virsh* の公式ドキュメントを参照してください。

例：

```
virsh # detach-interface --domain asav-network --type bridge --mac 52:55:04:4b:59:2f --live
```

KVM での ASAv のパフォーマンス調整

KVM 構成でのパフォーマンスの向上

KVM ホストの設定を変更することによって、KVM 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。これらの設定は、ホストサーバー上の構成時の設定とは無関係です。このオプションは、Red Hat Enterprise Linux 7.0 KVM で使用できます。

CPU ピニングを有効にすると、KVM 構成でのパフォーマンスを向上できます。

CPU ピンニングの有効化

ASAv では、KVM 環境での ASAv のパフォーマンスを向上させるために KVM CPU アフィニティオプションを使用する必要があります。プロセッサアフィニティ（CPU ピニング）により、プロセスまたはスレッドと中央処理装置（CPU）や幅広い CPU 間のバインドとバインド解除が可能になり、任意の CPU ではなく、指定された CPU でのみプロセスまたはスレッドが実行されるようになります。

ピン接続されていないインスタンスでピン接続されているインスタンスのリソース要件が使用されないようにするために、CPU ピニングを使用しないインスタンスとは別のホストに CPU ピニングを使用するインスタンスを展開するようにホスト集約を設定します。

注目 NUMA トポロジを持たないインスタンスと同じホストに NUMA トポロジを持つインスタンスを展開しないでください。

このオプションを使用する場合は、KVM ホストで CPU ピンニングを構成します。

ステップ 1 KVM ホスト環境で、ピンニングに使用できる vCPU の数を調べるために、ホストのトポロジを確認します。

例：

```
virsh nodeinfo
```

ステップ 2 使用可能な vCPU の数を確認します。

例：

```
virsh capabilities
```

ステップ 3 vCPU をプロセッサ コアのセットにピンニングします。

例：

```
virsh vcpupin <vm-name> <vcpu-number> <host-core-number>
```

virsh vcpupin コマンドは、ASAv 上の vCPU ごとに実行する必要があります。次の例は、vCPU が 4 個の ASAv 構成を使用し、ホストに 8 個のコアが搭載されている場合に必要になる KVM コマンドを示しています。

```
virsh vcpupin asav 0 2
virsh vcpupin asav 1 3
virsh vcpupin asav 2 4
virsh vcpupin asav 3 5
```

ホストのコア番号は、0 ～ 7 のどの番号でもかまいません。詳細については、KVM のドキュメンテーションを参照してください。

（注） CPU ピンニングを構成する場合は、ホスト サーバーの CPU トポロジを慎重に検討してください。複数のコアで構成されたサーバーを使用している場合は、複数のソケットにまたがる CPU ピンニングを設定しないでください。

KVM 構成でのパフォーマンスの向上には、専用のシステム リソースが必要になるという短所もあります。

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。

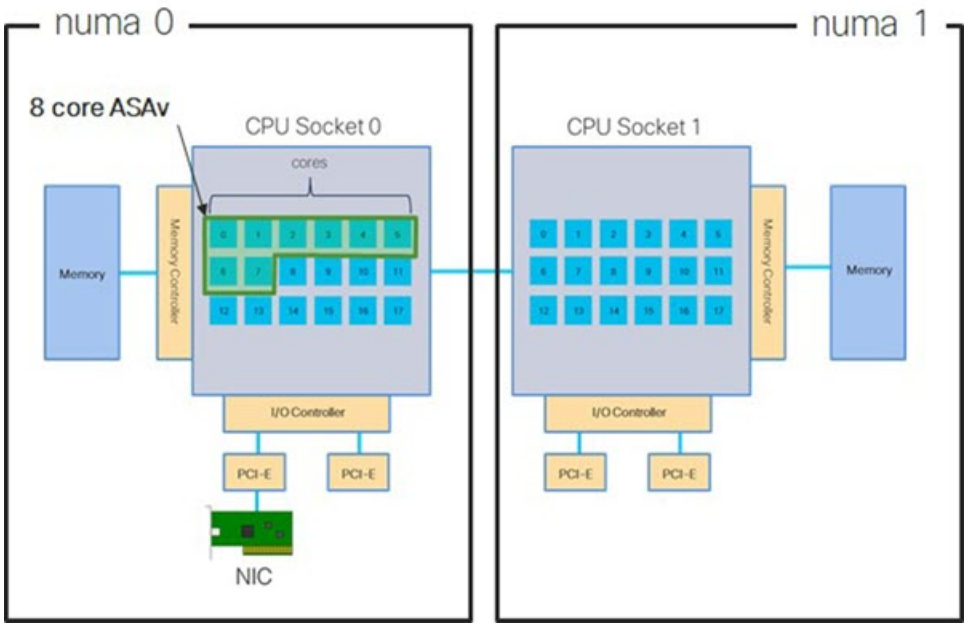
X86 サーバーアーキテクチャは、複数のソケットおよびソケット内の複数のコアで構成されています。各 CPU ソケットとそのメモリおよび I/O が、NUMA ノードと呼ばれます。メモリからパケットを効率的に読み取るには、ゲストアプリケーションおよび関連付けられている周辺機器（NIC など）が同じノード内に存在する必要があります。

最適な ASAv パフォーマンスを実現するには：

- ASAv 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 ASAv 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 ASAv（図 5 : 8 コア ASAv NUMA アーキテクチャの例 （60 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。
- NIC は、ASAv マシンと同じ NUMA ノード上にある必要があります。

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 ASAv 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 *5 : 8* コア *ASAv NUMA* アーキテクチャの例



NUMA の最適化

理想的には、ASAv マシンは、NIC が動作しているノードと同じ NUMA ノード上で実行する必要があります。手順は次のとおりです。

1. 「lstopo」を使用して NIC がオンになっているノードを判別し、ノードの図を表示します。NIC を見つけて、どのノードが接続されているかをメモします。
2. KVM ホストで、`virsh list` を使用して ASAv を検出します。
3. `virsh edit <VM Number>` を使用して VM を編集します。
4. 選択したノードに ASAv を配置します。次の例では、18 コアノードを想定しています。

   ノード 0 への配置：

   ```
   <vcpu placement='static' cpuset='0-17'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='0'/>
   </numatune>
   ```

   ノード 1 への配置：

   ```
   <vcpu placement='static' cpuset='18-35'>16</vcpu>
   <numatune>
       <memory mode='strict' nodeset='1'/>
   </numatune>
   ```

5. .xml の変更を保存し、ASAv マシンの電源を再投入します。
6. VM が目的のノードで実行されていることを確認するには、`ps aux | grep <name of your ASAv VM>` を実行して、プロセス ID を取得します。
7. `sudo numastat -c <ASAv VM Process ID>` を実行して、ASAv マシンが適切に配置されているか確認します。

KVM での NUMA 調整の使用に関する詳細については、RedHat のドキュメント『9.3. libvirt NUMA Tuning』を参照してください。

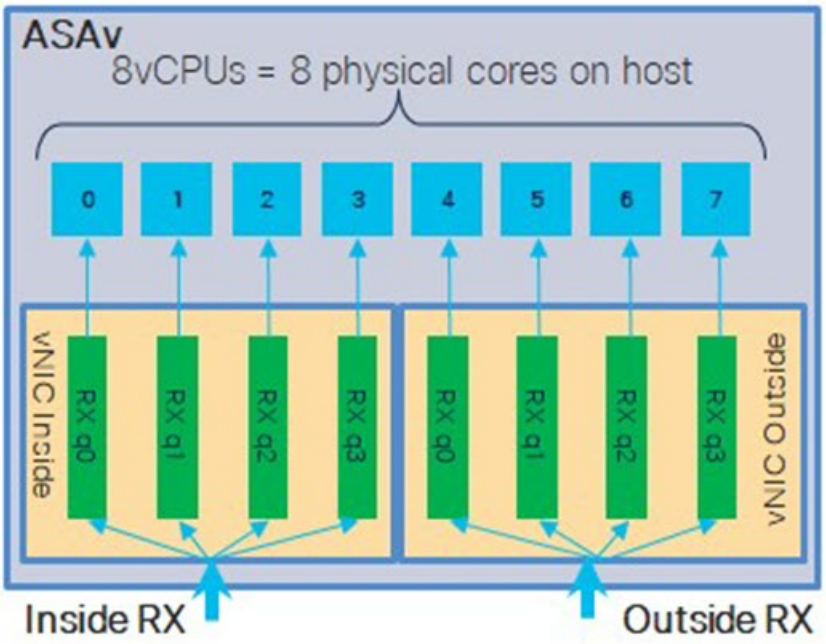
Receive Side Scaling（RSS）用の複数の RX キュー

ASAv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、ASAv バージョン 9.13(1) 以降が必要です。KVM の場合、*libvirt* のバージョンは 1.0.6 以降である必要があります。

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 6 : 8 コア ASAv RSS RX キュー（62 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 *6 : 8* コア *ASAv RSS RX* キュー



次の表に、KVM 用の ASAv 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、#unique_44 unique_44_Connect_42_section_pht_vfh_glbを参照してください。

表 *9 : KVM* 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	8（最大）	x710 の PCI パススルーおよび SR-IOV モードは、最適なパフォーマンスを提供します。通常、仮想展開では、複数の VM 間で NIC を共有できるため、SR-IOV が推奨されます。
	i40evf	SR-IOV	8	

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
x520	ixgbe	PCI パススルー	6	x520 NIC は、x710 よりも 10 ～ 30% パフォーマンスが低くなります。X520 の PCI パススルーおよび SR-IOV モードは、同様のパフォーマンスを提供します。通常、仮想展開では、複数の VM 間で NIC を共有できるため、SR-IOV が推奨されます。
	ixgbe-vf	SR-IOV	2	
該当なし	virtio	準仮想化	8（最大）	ASAv100 には推奨されません。 その他の展開については、KVM での Virtio のマルチキューサポートの有効化 （63 ページ） を参照してください。

KVM での Virtio のマルチキューサポートの有効化

次の例は、libvirt xml を編集するために、Virtio NIC RX キューの数を 4 に設定する方法を示しています。

```
<interface type='bridge'>
 <mac address='52:54:00:43:6e:3f'/>
 <source bridge='clients'/>
 <model type='virtio'/>
 <driver name='vhost' queues='4'/>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</interface>
```

重要 複数の RX キューをサポートするには、*libvirt* のバージョンが 1.0.6 以降である必要があります。

VPN の最適化

ASAv 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は、次のとおりです。

- IPSec のスループットは DTLS よりも高くなります。
- GCM 暗号には、CBC の約 2 倍のスループットがあります。

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 ASAv 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。ASAv 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 （11 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に関する要件

SR-IOV をサポートする物理 NIC がある場合、SR-IOV 対応 VF または仮想 NIC（vNIC）を ASAv インスタンスにアタッチできます。SR-IOV は、BIOS だけでなく、ハードウェア上で実行しているオペレーティング システム インスタンスまたはハイパーバイザでのサポートも必要です。KVM 環境で実行中の ASAv 用の SR-IOV インターフェイスのプロビジョニングに関する一般的なガイドラインのリストを以下に示します。

- ホスト サーバーには SR-IOV 対応物理 NIC が必要です。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 （12 ページ）を参照してください。
- ホスト サーバーの BIOS で仮想化が有効になっている必要があります。詳細については、ベンダーのマニュアルを参照してください。
- ホスト サーバーの BIOS で IOMMU グローバル サポートが SR-IOV に対して有効になっている必要があります。詳細については、ハードウェア ベンダーのマニュアルを参照してください。

KVM ホスト BIOS とホスト OS の変更

このセクションでは、KVM 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、Intel Ethernet Server Adapter X520 - DA2 を使用した Cisco UCS C シリーズ サーバー上の Ubuntu 14.04 を使用して、特定のラボ環境内のデバイスから作成されたものです。

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）が取り付けられていることを確認します。
- Intel 仮想化テクノロジー（VT-x）機能と VT-d 機能が有効になっていることを確認します。

（注） システム メーカーによっては、これらの拡張機能がデフォルトで無効になっている場合があります。システムごとに BIOS 設定にアクセスして変更する方法が異なるため、ベンダーのマニュアルでプロセスを確認することをお勧めします。

- オペレーティング システムのインストール中に、Linux KVM モジュール、ライブラリ、ユーザ ツール、およびユーティリティのすべてがインストールされていることを確認します。ASAv と KVM の前提条件 （50 ページ）を参照してください。
- 物理インターフェイスが稼働状態であることを確認します。ifconfig <*ethname*> を使用して確認します。

ステップ 1 "root" ユーザー アカウントとパスワードを使用してシステムにログインします。

ステップ 2 Intel VT-d が有効になっていることを確認します。

例：

```
kvmuser@kvm-host:/$ dmesg | grep -e DMAR -e IOMMU
[    0.000000] ACPI: DMAR 0x000000006F9A4C68 000140 (v01 Cisco0 CiscoUCS 00000001 INTL 20091013)
[    0.000000] DMAR: IOMMU enabled
```

最後の行は、VT-d が有効になっていることを示しています。

ステップ 3 */etc/default/grub* 設定ファイル内の GRUB_CMDLINE_LINUX エントリに *intel_iommu=on* パラメータを付加することによって、カーネル内の Intel VT-d をアクティブにします。

例：

```
# vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on"
...
```

（注） AMD プロセッサを使用している場合は、代わりに、*amd_iommu=on* をブート パラメータに付加します。

ステップ 4 iommu の変更を有効にするためにサーバーをリブートします。

例：

```
> shutdown -r now
```

ステップ 5 次の形式を使用して *sysfs* インターフェイス経由で *sriov_numvfs* パラメータに適切な値を書き込むことによって、VF を作成します。

```
#echo n > /sys/class/net/device name/device/sriov_numvfs
```

サーバーの電源を入れ直すたびに必要な数の VF が作成されるようにするには、*/etc/rc.d/* ディレクトリに配置されている *rc.local* ファイルに上記コマンドを付加します。Linux OS は、ブート プロセスの最後で *rc.local* スクリプトを実行します。

たとえば、ポートあたり 1 つの VF を作成するケースを以下に示します。お使いのセットアップではインターフェイスが異なる可能性があります。

例：

```
echo '1' > /sys/class/net/eth4/device/sriov_numvfs
echo '1' > /sys/class/net/eth5/device/sriov_numvfs
echo '1' > /sys/class/net/eth6/device/sriov_numvfs
echo '1' > /sys/class/net/eth7/device/sriov_numvfs
```

ステップ 6 サーバーをリブートします。

例：

```
> shutdown -r now
```

ステップ 7 *lspci* を使用して、VF が作成されたことを確認します。

例：

```
 > lspci | grep -i "Virtual Function"
kvmuser@kvm-racetrack:~$ lspci | grep -i "Virtual Function"
0a:10.0 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.1 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.2 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
0a:10.3 Ethernet controller: Intel Corporation 82599 Ethernet Controller Virtual Function (rev 01)
```

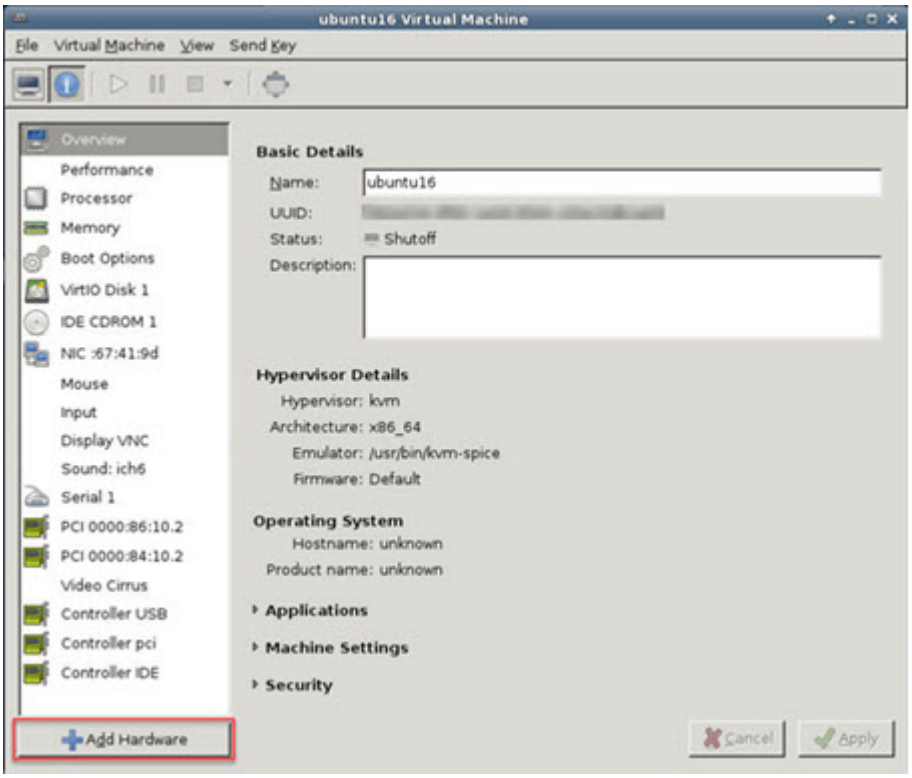
（注） **ifconfig** コマンドを使用して、新しいインターフェイスを表示します。

ASAv への PCI デバイスの割り当て

VF を作成したら、PCI デバイスを追加するのと同様に、VF を ASAv に追加できます。次の例では、グラフィカル **virt-manager** ツールを使用して、イーサネット VF コントローラを ASAv に追加する方法について説明します。

ステップ 1 ASAv を開いて、[Add Hardware] ボタンをクリックし、新しいデバイスを仮想マシンに追加します。

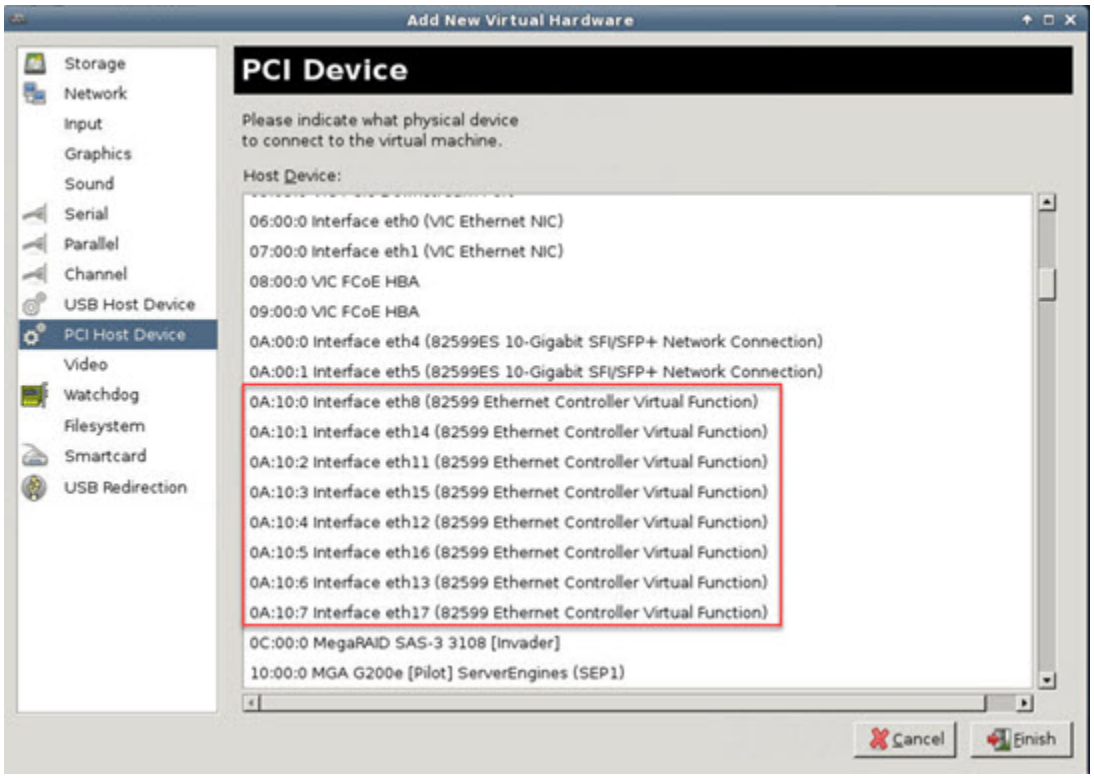
図 7: ハードウェアの追加



ステップ 2 左ペインの [Hardware] リストで [PCI Host Device] をクリックします。

VF を含む PCI デバイスのリストが中央ペインに表示されます。

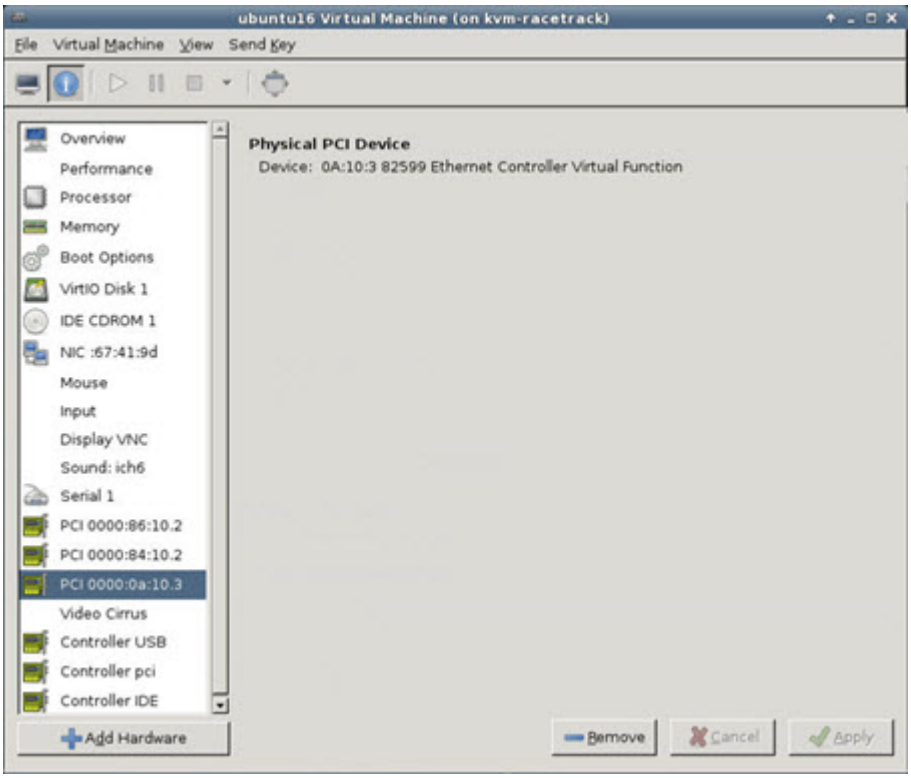
図 *8 :* 仮想機能のリスト



ステップ 3 使用可能な仮想機能のいずれかを選択して、[Finish] をクリックします。

PCI デバイスがハードウェア リストに表示されます。デバイスの記述が Ethernet Controller Virtual Function になっていることに注意してください。

図 *9* : 追加された仮想機能



次のタスク

- ASAv コマンドラインから、**show interface** コマンドを使用して、新しく設定したインターフェイスを確認します。
- ASAv でインターフェイス コンフィギュレーション モードを使用して、トラフィックの送受信インターフェイスを設定して有効化します。詳細については、『Cisco ASA シリーズ CLI コンフィギュレーション ガイド（一般的な操作）』の「*Basic Interface Configuration*」の章を参照してください。

CPU 使用率とレポート

CPU使用率レポートには、指定された時間内に使用されたCPUの割合の要約が表示されます。通常、コアはピーク時以外には合計 CPU 容量の約 30 ～ 40% で動作し、ピーク時は約 60 ～ 70% の容量で動作します。

ASA Virtual の vCPU 使用率

ASA Virtual の vCPU 使用率には、データパス、制御ポイント、および外部プロセスで使用されている vCPU の量が表示されます。

vSphere で報告される vCPU の使用率には、ASA Virtual の使用率に加えて、次のものが含まれます。

- ASA Virtual アイドル時間
- ASA Virtual マシンに使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

CPU 使用率の統計情報を表示するには、**show cpu usage** コマンドを使用します。

例

```
Ciscoasa#show cpu usage

CPU □□□□5□□□ 1%□1 □□□ 2%□5 □□□ 1%
```

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASA Virtual レポート：40%
- DP：35%
- 外部プロセス：5%
- ASA（ASA Virtual レポート）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

KVM CPU 使用率レポート

値は、

```
virsh cpu-stats domain --total start count
```

コマンドを実行すると、指定されたゲスト仮想マシンの CPU 統計情報が表示されます。デフォルトでは、すべての CPU の統計と合計が表示されます。`--total` オプションを指定すると、合

計統計のみ表示されます。`--count` オプションを指定すると、count 個の CPU の統計のみ表示されます。

OProfile、top などのツールを実行すると、ハイパーバイザと VM の両方の CPU 使用率を含む、特定の KVM VM の合計 CPU 使用率が表示されます。同様に、Xen VMM に固有の XenMon などのツールの場合、Xen ハイパーバイザ、つまり Dom 0 の合計 CPU 使用率が表示されますが、VM ごとのハイパーバイザ使用率には分割されません。

これらのツールとは別に、OpenNebula などのクラウド コンピューティング フレームワークには、VM によって使用される仮想 CPU の割合の大まかな情報のみを提供する特定のツールが存在します。

ASA Virtual と KVM のグラフ

ASA Virtual と KVM の間には CPU % の数値に違いがあります。

- KVM グラフの数値は ASA Virtual の数値よりも常に大きくなります。
- KVM ではこの値は「%CPU usage」と呼ばれ、ASA Virtual ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

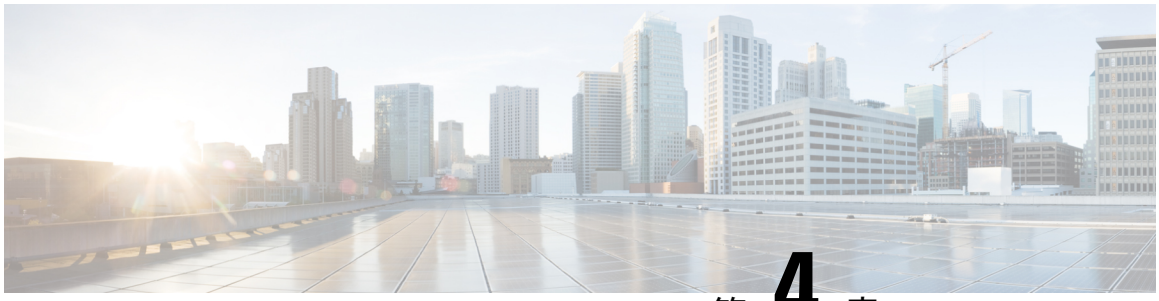
- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

KVM では「%CPU usage」は次のように計算されます。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。



第 4 章

AWS クラウドへの ASAv の導入

Amazon Web Services（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 （73 ページ）
- ASAv と AWS の前提条件 （74 ページ）
- ASAv および AWS のガイドラインと制限事項 （75 ページ）
- 設定の移行と SSH 認証 （76 ページ）
- AWS 上の ASAv のネットワークトポロジの例 （77 ページ）
- AWS での ASAv の展開 （77 ページ）

AWS クラウドへの ASAv の導入について

ASAvは、物理ASAと同じソフトウェアを実行して、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。ASAv は、パブリック AWS クラウドに導入できます。その後設定を行うことで、時間の経過とともにロケーションを展開、契約、またはシフトする仮想および物理データセンターのワークロードを保護できます。

ASAv は、次の AWS インスタンスタイプをサポートしています。

表 *10 : AWS* でサポートされているインスタンス タイプ

インスタンス	属性			ASAv モデルのサポート	注
	vCPU	メモリ（GB）	インターフェイスの最大数		
c3.large	2	3.75	3	• ASAv10 • ASAv30	リソースのアンダープロビジョニングのため、large インスタンスでの ASAv30 の使用は推奨されません。
c4.large	2	3.75	3		
m4.large	2	8	2		

インスタンス	属性			ASAv モデルのサポート	注
	vCPU	メモリ（GB）	インターフェイスの最大数		
c3.xlarge	4	7.5	4	ASAv30	xlarge インスタンスでサポートされるのは ASAv30 のみです。
c4.xlarge	4	7.5	4		
m4.xlarge	4	16	4		

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。

重要 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 へのライセンス付与。ASAv にライセンスを付与するまでは、100 回の接続と 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。「ASAv のライセンス（1 ページ）」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、DMZ ネットワークに ASAv を接続するために使用されます。

- ASAv システム要件については、Cisco ASA の互換性 [英語] 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

サポートされる機能

AWS 上の ASAv は、次の機能をサポートしています。

- 次世代の Amazon EC2 Compute Optimized インスタンスファミリである Amazon EC2 C5 インスタンスのサポート
- 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ー導入
- ルーテッド モード（デフォルト）
- Amazon CloudWatch

サポートされない機能

AWS 上の ASAv は、以下の機能をサポートしていません。

- 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）
- 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 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
- 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。

- IPv6

設定の移行と SSH 認証

SSH 公開キー認証使用時のアップグレードの影響：SSH 認証が更新されることにより、SSH 公開キー認証を有効にするための新たな設定が必要となります。そのため、アップグレード後は、公開キー認証を使用した既存の SSH 設定は機能しません。公開キー認証は、Amazon Web Services（AWS）の ASAv のデフォルトであるため、AWS ユーザーにはこの問題が表示されます。SSH 接続を失なう問題を避けるには、アップグレードの前に設定を更新します。または（ASDM アクセスが有効になっている場合）アップグレード後に ASDM を使用して設定を修正できます。

次は、ユーザー名「admin」の元の設定例です。

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

ssh authentication コマンドを使用するには、アップグレードの前に次のコマンドを入力します。

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

nopassword キーワードが存在している場合、これを維持するのではなく、代わりにユーザー名に対応したパスワードを設定することを推奨します。**nopassword** キーワードは、パスワードは入力不可を意味するのではなく、任意のパスワードを入力できます。9.6(2) より前のバージョンでは、**aaa** コマンドは SSH 公開キー認証に必須ではありませんでした。このため、**nopassword** キーワードはトリガーされませんでした。9.6(2) では **aaa** コマンドが必須となり、**password**（または **nopassword**）キーワードが存在する場合、自動的に **username** の通常のパスワード認証を許可するようになりました。

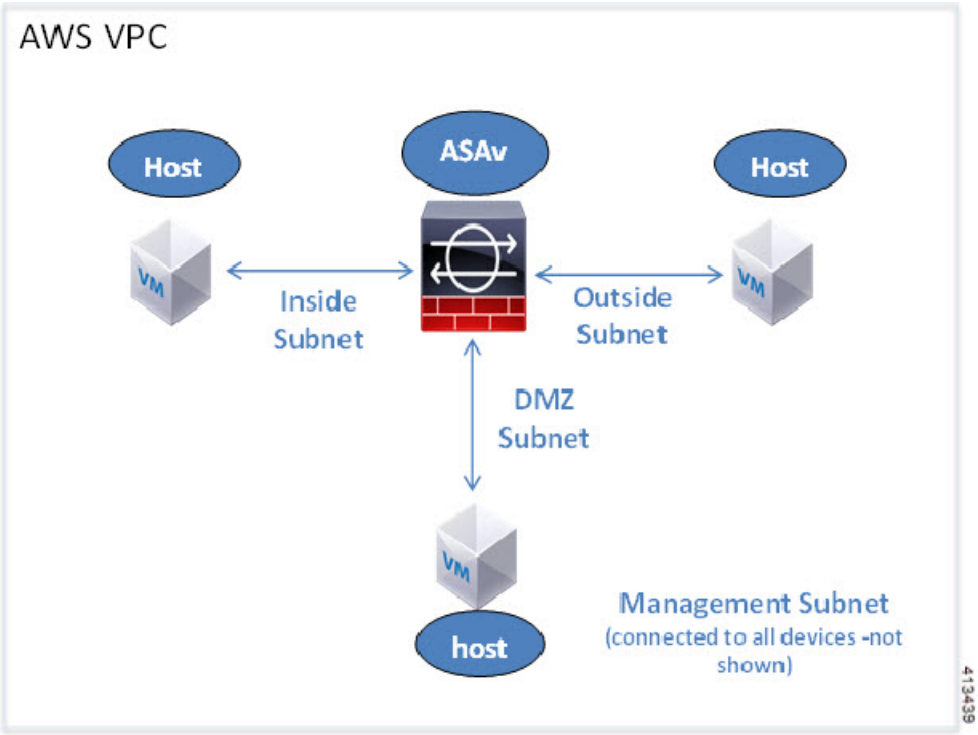
アップグレード後は、 **username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザーがパスワードを入力できなくするよう指定できるようになります。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

AWS 上の ASAv のネットワークトポロジの例

次の図は、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）を備えた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 *10 : AWS* への *ASAv* の導入例



AWS での ASAv の展開

次の手順は、ASAv で AWS をセットアップする手順の概略です。設定の詳細な手順については、『Getting Started with AWS』を参照してください。

ステップ 1 aws.amazon.com にログインし、地域を選択します。

（注） 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。

ステップ 2 **[My Account]** > **[AWS Management Console]** をクリックし、[Networking] で **[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、次を設定します（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）。

ステップ 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 でサポートされるインスタンスタイプ（c3.large など）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）。
- [高度な詳細（Advanced Details）] セクションを導入し、[ユーザーデータ（User data）] フィールドに、オプションで第 0 日用構成を入力できます。これは、ASAv の起動時に適用される ASAv 構成を含むテキスト入力です。第 0 日用構成にスマート 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」を参照してください。
  - **管理インターフェイス**：第 0 日用構成を選択する場合は、管理インターフェイスの詳細を指定する**必要**があります。これは DHCP を使用するように設定する必要があります。
  - **データインターフェイス**：データインターフェイスの IP アドレスは、その情報を第 0 日用構成の一部として指定した場合にのみ割り当てられ、設定されます。データインターフェイスは、DHCP を使用するように設定できます。または、接続するネットワーク インターフェイスがすでに作成されていて、IP アドレスがわかっている場合は、第 0 日用構成で IP の詳細を指定できます。
  - **第 0 日用構成なし**：第 0 日用構成を指定**せず**に ASAv を導入すると、ASAv はデフォルトの ASAv 構成を適用し、AWS メタデータサーバーから接続されたインターフェイスの IP を取得し、IP アドレスを割り当てます（データインターフェイスに IP は割り当てられますが、ENI はダウンします）。Management0/0 インターフェイスが起動し、DHCP アドレスで設定された IP を取得します。Amazon EC2 および Amazon VPC の IP アドレッシングについては、「VPC での IP アドレッシング」を参照してください。
- **第 0 日用構成の例**：

```
! ASA Version 9.x.1.200
!
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!
crypto key generate rsa modulus 2048
ssh 0 0 management
```

```
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Q1w2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

no shutdown
!
interface G0/1
nameif inside
ip address dhcp

no shutdown
!
```

- 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 のアクセス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。

ステップ 4 キー ペアを作成します。

注意 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。

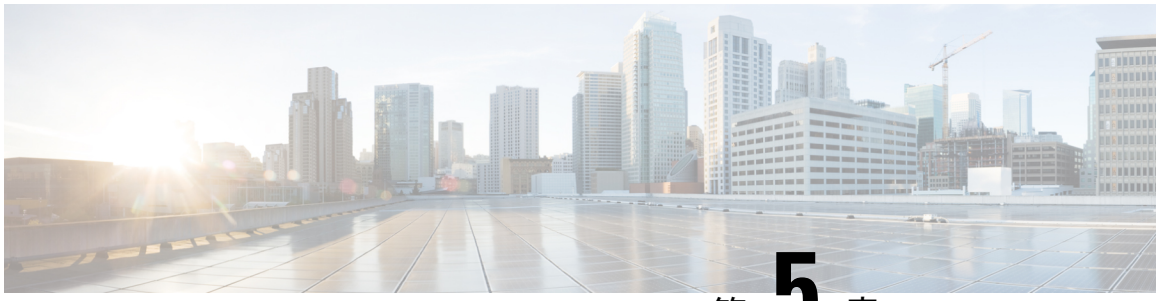
ステップ 5 [インスタンスの起動（Launch Instance）] をクリックして、ASAv を導入します。

ステップ 6 **[My Account]** > **[AWS Management Console]** > **[EC2]** > **[Launch an Instance]** > **[My AMIs]** をクリックします。

ステップ 7 ASAv のインターフェイスごとに [送信元または宛先の確認（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（IPv4）のトラフィックのみを受信でき、インスタンスは独自の IP アドレス（IPv4）からのみトラフィックを送信できます。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 [送信元または宛先の確認（Source/Destination Check）] を無効にする必要があります。



第 5 章

Microsoft Azure クラウドへの ASAv の導入

Microsoft Azure クラウドに ASAv を導入できます。

- Microsoft Azure クラウドへの ASAv 導入について （81 ページ）
- ASAv および Azure の前提条件およびシステム要件 （82 ページ）
- 注意事項と制約事項 （83 ページ）
- 導入時に作成されるリソース （85 ページ）
- Azure ルーティング （87 ページ）
- 仮想ネットワーク内の VM のルーティング設定 （88 ページ）
- IP Addresses （88 ページ）
- DNS （89 ページ）
- Microsoft Azure への ASAv の導入 （89 ページ）

Microsoft Azure クラウドへの ASAv 導入について

Microsoft Azure は、プライベート Microsoft Hyper V 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、Hyper V ハイパーバイザの Microsoft Azure 環境でゲストとして実行されます。Microsoft Azure の ASAv では、Standard D3 および Standard D3_v2 インスタンスがサポートされ、4 つの vCPU、14 GB、および 4 つのインターフェイスを使用できます。

表 *11 : ASAv* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	インスタンスタイプ（コア/RAM）	レート制限（Rate Limit）	RA VPN セッション制限
ASAv5	D3_v2 4 コア/14 GB	100 Mbps	50
ASAv10	D3_v2 4 コア/14 GB	1 Gbps	250
ASAv30	D3_v2 4 コア/14 GB	[2 Gbps]	750

パフォーマンス階層	インスタンスタイプ（コア/RAM）	レート制限（Rate Limit）	RA VPN セッション制限
ASAv50	D4_v2 8 コア/28 GB	5.5 Gbps	10,000
ASAv100	D5_v2 16 コア/56 GB	11 Gbps	20,000

次の方法で Microsoft Azure に ASAv を導入できます。

- 標準的な Azure パブリック クラウドおよび Azure Government 環境で、Azure Resource Manager を使用してスタンドアロン ファイアウォールとして導入
- Azure Security Center を使用して統合パートナー ソリューションとして導入
- 標準的な Azure パブリック クラウドおよび Azure Government 環境で、Azure Resource Manager を使用してハイ アベイラビリティ（HA）ペアとして導入

「Azure Resource Manager からの ASAv の導入 （89 ページ）」を参照してください。標準的な Azure パブリッククラウドおよび Azure Government 環境で ASAv HA 構成を導入できます。

ASAv および Azure の前提条件およびシステム要件

- Azure.com でアカウントを作成します。

  Microsoft Azure でアカウントを作成したら、ログインして、Microsoft Azure Marketplace 内で ASAv を選択し、ASAv を導入できます。

- ASAv へのライセンス付与。

  ASAv にライセンスを付与するまでは、100 回の接続と 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」を参照してください。

（注） Azure に導入する場合、ASAv にはデフォルトで ASAv30 の権限が付与されています。ASAv5、ASAv10、ASAv30、ASAv50、および ASAv100 の権限付与の使用が許可されています。ただし、ASAv5、ASAv10、ASAv30、ASAv50、および ASAv100 の権限付与を使用するためには、スループットレベルを明示的に設定する必要があります。

- インターフェイスの要件：

  4 つのネットワーク上の 4 つのインターフェイスとともに ASAv を導入する必要があります。任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パ

ブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、パブリック IP アドレス [英語] を参照してください。

- 管理インターフェイス：

  Azure では、最初に定義されたインターフェイスが常に管理インターフェイスです。

- 通信パス：
  - 管理インターフェイス：SSH アクセス、および ASAv を ASDM に接続するために使用されます。
  - 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）：Standard_D3 インターフェイスを使用する場合に、ASAv を DMZ ネットワークに接続するために使用されます。
- ASAv ハイパーバイザおよび仮想プラットフォームのサポート情報については、Cisco ASA の互換性 [英語] を参照してください。

注意事項と制約事項

サポートされる機能

- Microsoft Azure クラウドからの導入
- 選択したインスタンスタイプに基づく最大 16 個の vCPU

（注） Azure では L2 vSwitch 機能は設定できません。

- インターフェイスのパブリック IP アドレス

  任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、パブリック IP アドレス [英語] を参照してください。

- ルーテッド ファイアウォール モード（デフォルト）

（注） ルーテッドファイアウォールモードでは、ASAv はネットワーク内の従来のレイヤ 3 境界となります。このモードには、各インターフェイスの IP アドレスが必要です。Azure は VLAN タグ付きインターフェイスをサポートしていないため、IP アドレスはタグなしのトランク以外のインターフェイスで設定する必要があります。

既知の問題

アイドル タイムアウト

Azure 上の ASAv には、VM で設定可能なアイドルタイムアウトがあります。最小設定値は 4 分、最大設定値は 30 分です。ただし、SSH セッションでは最小設定値は 5 分、最大設定値は 60 分です。

（注） ASAv のアイドルタイムアウトにより、SSH タイムアウトは常に上書きされ、セッションが切断されることに注意してください。セッションがどちらの側からもタイムアウトしないように、VM のアイドルタイムアウトを SSH タイムアウトに合わせることができます。

プライマリ ASAv からスタンバイ ASAv へのフェールオーバー

Azure での ASAv HA 導入で Azure のアップグレードが発生すると、プライマリ ASAv からスタンバイ ASAv へのフェールオーバーが発生する場合があります。Azure のアップグレードにより、プライマリ ASAv が一時停止状態になります。プライマリ ASAv が一時停止している場合、スタンバイ ASAv は hello パケットを受信しません。スタンバイ ASAv がフェールオーバーホールド時間を経過しても hello パケットを受信しない場合、スタンバイ ASAv へのフェールオーバーが発生します。

また、フェールオーバーホールド時間を経過していなくてもフェールオーバーが発生する可能性があります。プライマリ ASAv が一時停止状態に入ってから 19 秒後に再開するシナリオを考えてみましょう。フェールオーバーホールド時間は 30 秒ですが、クロックは約 2 分ごとに同期されるため、スタンバイ ASAv は正しいタイムスタンプの hello パケットを受信しません。その結果、プライマリ ASAv からスタンバイ ASAv へのフェールオーバーが発生します。

（注） この機能は IPv4 のみをサポートし、ASA Virtual HA は IPv6 設定ではサポートされません。

サポートされない機能

- 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）
- ユーザー インスタンス インターフェイスの VLAN タギング

- ジャンボ フレーム
- Azure の観点からの、デバイスが所有していない IP アドレスのプロキシ ARP
- 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）

（注） Azure ポリシーでは、インターフェイスは無差別モードでは動作できないため、ASAv はトランスペアレント ファイアウォール モードでは動作しません。

- マルチ コンテキスト モード
- クラスタ
- ASAv ネイティブ HA
- VM のインポート/エクスポート
- デフォルトでは、Azureクラウド内で稼働する ASAv の FIPS モードは無効になっています。

（注） FIPS モードを有効にする場合は、**ssh key-exchange group dh-group14-sha1** コマンドを使用して、Diffie-Helman キー交換グループをより強力なキーに変更する必要があります。Diffie-Helman グループを変更しないと、ASAv に SSH 接続できなくなるため、グループの変更が、最初に ASAv を管理する唯一の方法です。

- IPv6

Azure DDoS Protection 機能

Microsoft Azure の Azure DDoS Protection は、ASAv の最前線に実装された追加機能です。仮想ネットワークでこの機能を有効にすると、ネットワークで予想されるトラフィックの 1 秒あたりのパケット数に応じて、一般的なネットワーク層攻撃からアプリケーションを保護するのに役立ちます。この機能は、ネットワーク トラフィック パターンに基づいてカスタマイズできます。

Azure DDoS Protection 機能の詳細については、『Azure DDoS Protection Standard overview』[英語] を参照してください。

導入時に作成されるリソース

Azure に ASAv を展開すると、次のリソースが作成されます。

- ASAv マシン
- リソース グループ（既存のリソース グループを選択していない場合）

  ASAv リソースグループは、仮想ネットワークとストレージアカウントで使用するリソースグループと同じである必要があります。
- vm name-Nic0、vm name-Nic1、vm name-Nic2、vm name-Nic3 という名前の 4 つの NIC

  これらの NIC は、それぞれ ASAv インターフェイスの Management 0/0、GigabitEthernet 0/0、GigabitEthernet 0/1、および GigabitEthernet 0/2 にマッピングされます。

（注） 要件に基づいて、IPv4 のみで VNet を作成できます。

- VM 名-SSH-SecurityGroup という名前のセキュリティ グループ

  セキュリティグループは、ASAv Management 0/0 にマッピングされる VM の Nic0 にアタッチされます。

  セキュリティ グループには、VPN 目的で SSH、UDP ポート 500、および UDP 4500 を許可するルールが含まれます。導入後に、これらの値を変更できます。
- パブリック IP アドレス（展開時に選択した値に従って命名）。

  パブリック IP アドレス（IPv4 のみ）。

  任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、「パブリック IP アドレス」を参照してください。
- 4 つのサブネットを備えた仮想ネットワーク（既存のネットワークを選択していない場合）
- サブネットごとのルーティング テーブル（既存の場合は最新のもの）

  このテーブルの名前は、サブネット名-ASAv-RouteTable です。

  各ルーティングテーブルには、ASAv IP アドレスを持つ他の 3 つのサブネットへのルートがネクストホップとして含まれています。トラフィックを他のサブネットまたはインターネットに到達させる必要がある場合は、デフォルト ルートを追加することもできます。
- 選択したストレージ アカウントの起動時診断ファイル

  起動時診断ファイルは、ブロブ（サイズの大きいバイナリ オブジェクト）内に配置されます。
- 選択したストレージ アカウントのブロブおよびコンテナ VHD にある 2 つのファイル（名前は、*vm name*-disk.vhd および *vm name*-<uuid>.status）
- ストレージ アカウント（既存のストレージ アカウントが選択されていない場合）

（注） VM を削除すると、保持を希望する任意のリソースを除き、これらの各リソースを個別に削除する必要があります。

Azure ルーティング

Azure 仮想ネットワークでのルーティングは、仮想ネットワークの有効なルーティング テーブルによって決まります。有効なルーティング テーブルは、既存のシステム ルーティング テーブルとユーザー定義のルーティング テーブルの組み合わせです。

（注） ASAv では、Azure クラウドルーティングの特性により、EIGRP や OSPF などのダイナミックな内部ルーティングプロトコルを使用できません。有効なルーティング テーブルは、仮想クライアントにスタティック/ダイナミック ルートが設定されているかどうかに関係なく、ネクスト ホップを決定します。

現在、有効なルーティング テーブルまたはシステム ルーティング テーブルはどちらも表示できません。

ユーザー定義のルーティング テーブルは表示および編集できます。システム テーブルとユーザー定義のテーブルを組み合わせて有効なルーティング テーブルを形成した場合、最も限定的なルート（同位のものを含め）がユーザー定義のルーティング テーブルに含められます。システム ルーティング テーブルには、Azure の仮想ネットワーク インターネット ゲートウェイを指すデフォルト ルート（0.0.0.0/0）が含まれます。また、システム ルーティング テーブルには、Azure の仮想ネットワーク インフラストラクチャ ゲートウェイを指すネクスト ホップとともに、他の定義済みのサブネットへの限定的なルートが含まれます。

ASAv を介してトラフィックをルーティングするために、ASAv 導入プロセスで、ASAv をネクストホップとして使用する他の 3 つのサブネットへのルートが各サブネットに追加されます。サブネット上の ASAv インターフェイスを指すデフォルトルート（0.0.0.0/0）を追加することもできます。これで、サブネットからのトラフィックはすべて ASAv を介して送信されますが、場合によっては、トラフィックを処理する前に、ASAv ポリシーを設定する必要があります（通常は NAT/PAT を使用）。

システム ルーティング テーブル内の既存の限定的なルートのために、ユーザー定義のルーティング テーブルに、ネクストホップとして ASAv を指す限定的なルートを追加する必要があります。追加しないと、ユーザー定義のテーブル内のデフォルトルートではなく、システム ルーティング テーブル内のより限定的なルートが選択され、トラフィックは ASAv をバイパスします。

仮想ネットワーク内の VM のルーティング設定

Azure 仮想ネットワーク内のルーティングは、クライアントの特定なゲートウェイ設定ではなく、有効なルーティングテーブルに依存します。仮想ネットワーク内で稼働するクライアントは、DHCPによって、それぞれのサブネット上の 1 アドレスとなるルートを指定されることがあります。これはプレースホルダで、仮想ネットワークのインフラストラクチャ仮想ゲートウェイにパケットを送信するためにだけ使用されます。パケットは、VM から送信されると、有効なルーティング テーブル（ユーザー定義のテーブルによって変更された）に従ってルーティングされます。有効なルーティング テーブルは、クライアントでゲートウェイが 1 として、または ASAv アドレスとして設定されているかどうかに関係なく、ネクストホップを決定します。

Azure VM ARP テーブルには、すべての既知のホストに対して同じ MAC アドレス（1234.5678.9abc）が表示されます。これによって、Azure VM からのすべてのパケットが、有効なルーティングテーブルを使用してパケットのパスを決定する Azure ゲートウェイに到達するように保証されます。

（注） ASAv では、Azure クラウドルーティングの特性により、EIGRP や OSPF などのダイナミックな内部ルーティングプロトコルを使用できません。有効なルーティングテーブルは、仮想クライアントにスタティック/ダイナミック ルートが設定されているかどうかに関係なく、ネクスト ホップを決定します。

IP Addresses

次の情報は Azure の IP アドレスに適用されます。

- ASAv インターフェイスの IP アドレスを設定するには、DHCP を使用する必要があります。

  Azure インフラストラクチャは、Azure に設定された IP アドレスが確実に ASAv インターフェイスに割り当てられるように動作します。

- Management 0/0 には、それが接続されているサブネット内のプライベート IP アドレスが割り当てられます。

  パブリック IP アドレスは、プライベート IP アドレスに関連付けられる場合があり、Azure インターネット ゲートウェイは NAT 変換を処理します。

- 任意のインターフェイスにパブリック IP アドレスを割り当てることができます。

- ダイナミック パブリック IP アドレスは Azure の停止/開始サイクル中に変更される場合があります。ただし、Azure の再起動時および ASAv のリロード時には、パブリック IP アドレスは保持されます。

- スタティック パブリック IP アドレスは Azure 内でそれらを変更するまで変わりません。

DNS

すべての Azure 仮想ネットワークが、次のように使用できる 168.63.129.16 で、組み込みの DNS サーバーにアクセスできます。

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

この構成は、Smart Licensing を設定し、専用の DNS サーバーをセットアップしていない場合に使用できます。

Microsoft Azure への ASAv の導入

Microsoft Azure に ASAv を導入できます。

- 標準的な Azure パブリッククラウドおよび Azure Government 環境で、Azure Resource Manager を使用してスタンドアロンファイアウォールとして ASAv を導入します。「Azure Resource Manager からの ASAv の導入」を参照してください。
- Azure Security Center を使用して、Azure 内の統合パートナーソリューションとして ASAv を導入します。セキュリティを重視するお客様には、Azure ワークロードを保護するためのファイアウォールオプションとして ASAv が提供されます。セキュリティイベントとヘルスイベントが単一の統合ダッシュボードからモニターされます。「Azure Security Center からの ASAv の導入」を参照してください。
- Azure Resource Manager を使用して ASAv 高可用性ペアを導入します。冗長性を確保するために、ASAv をアクティブ/バックアップ高可用性（HA）設定で導入できます。パブリッククラウドでの HA では、アクティブな ASAv の障害時に、バックアップ ASAv へのシステムの自動フェールオーバーをトリガーできるステートレスなアクティブ/バックアップソリューションが実装されます。「Azure Resource Manager からの ASAv for High Availability の導入 （93 ページ）」を参照してください。

Azure Resource Manager からの ASAv の導入

次の手順は、ASAv で Microsoft Azure をセットアップする手順の概略を示しています。Azure の設定の詳細な手順については、『Azure を使ってみる』を参照してください。

Azure に ASAv を導入すると、リソース、パブリック IP アドレス、ルートテーブルなどのさまざまな設定が自動的に生成されます。導入後に、これらの設定をさらに管理できます。たとえば、アイドル タイムアウト値を、デフォルトの短いタイムアウトから変更することができます。

ステップ 1 Azure Resource Manager（ARM）ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 Cisco ASAv のマーケットプレイスを検索し、導入する ASAv をクリックします。

ステップ 3 基本的な設定を行います。

a) 仮想マシンの名前を入力します。この名前は Azure サブスクリプション内で一意である必要があります。

重要 名前が一意でなく、既存の名前を再使用すると、導入に失敗します。

b) ユーザー名を入力します。

c) 認証タイプとして、[Password] または [SSH public key] を選択します。

[Password] を選択した場合は、パスワードを入力して確定します。

d) サブスクリプション タイプを選択します。

e) [Resource group] を選択します。

リソース グループは、仮想ネットワークのリソース グループと同じである必要があります。

f) 場所を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

g) [OK] をクリックします。

ステップ 4 ASAv の設定項目を設定します。

a) 仮想マシンのサイズを選択します。

ASAv では、Standard D3 および Standard D3_v2 がサポートされます。

b) ストレージ アカウントを選択します。

既存のストレージアカウントを使用するか、新しいストレージアカウントを作成できます。ストレージ アカウントの場所はネットワークおよび仮想マシンと同じである必要があります。

c) [Name] フィールドに IP アドレスのラベルを入力し、[OK] をクリックして、パブリック IP アドレスを要求します。

Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミック パブリック IP をデフォルトでは作成します。固定 IP アドレスを優先する場合は、ポータルのパブリック IP を開き、ダイナミック アドレスからスタティック アドレスに変更します。

d) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloupapp.azure.com* の形式になります。

e) 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。

f) ASAv を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要 各インターフェイスを一意のサブネットにアタッチする必要があります。

g) [OK] をクリックします。

ステップ 5 構成サマリを確認し、[OK] をクリックします。

ステップ 6 利用条件を確認し、[Create] をクリックします。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の起動」を参照してください。

Azure Security Center からの ASAv の導入

Microsoft Azure Security Center は、お客様がクラウド導入に対するセキュリティ リスクを防御、検出、および軽減できるようにする Azure 向けのセキュリティ ソリューションです。Security Center のダッシュボードから、セキュリティ ポリシーを設定したり、セキュリティ設定をモニターしたり、セキュリティ アラートを表示したりできます。

Security Center は、Azure リソースのセキュリティ状態を分析して、潜在的なセキュリティの脆弱性を特定します。推奨事項のリストに従い、必要なコントロールを設定するプロセスを実行します。対象には、Azure のお客様に対するファイアウォール ソリューションとしての ASAv の導入を含めることができます。

Security Center の統合ソリューションのように、数クリックで ASAv をすばやく導入し、単一のダッシュボードからセキュリティイベントと正常性イベントをモニターできます。次の手順は、Security Center から ASAv を導入する手順の概要です。詳細については、『Azure Security Center』を参照してください。

ステップ 1 Azure ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 Microsoft Azure メニューから、[Security Center] を選択します。

初めて Security Center にアクセスする場合は、[Welcome] ブレードが開きます。**[Yes! I want to Launch Azure Security Center]** を選択して、[Security Center] ブレードを開き、データ収集を有効にします。

ステップ 3 [Security Center] ブレードで、[Policy] タイルを選択します。

ステップ 4 [Security policy] ブレードで、[Prevention policy] を選択します。

ステップ 5 [Prevention policy] ブレードで、セキュリティ ポリシーの一部として表示する推奨事項をオンにします。

a) [Next generation firewall] を [On] に設定します。これで、ASAv が Security Center 内の推奨ソリューションとなります。

b) 必要に応じて、他の推奨事項を設定します。

ステップ 6 [Security Center] ブレードに戻って、[Recommendations] タイルを選択します。

Security Center は、Azure リソースのセキュリティ状態を定期的に分析します。Security Center が潜在的なセキュリティの脆弱性を特定すると、[Recommendations] ブレードに推奨事項が表示されます。

ステップ 7 [Recommendations] ブレードで [Add a Next Generation Firewall] 推奨事項を選択して、詳細を表示したり、問題を解決するためのアクションを実行したりします。

ステップ 8 [新規作成（Create New）] または [既存のソリューションを使用（Use existing solution）] を選択してから、導入する ASAv をクリックします。

ステップ 9 基本的な設定を行います。

a) 仮想マシンの名前を入力します。この名前は Azure サブスクリプション内で一意である必要があります。

重要 名前が一意でなく、既存の名前を再使用すると、導入に失敗します。

b) ユーザー名を入力します。

c) 認証のタイプとして、パスワードまたは SSH キーのいずれかを選択します。

パスワードを選択した場合は、パスワードを入力して確定します。

d) サブスクリプション タイプを選択します。

e) リソース グループを選択します。

リソース グループは、仮想ネットワークのリソース グループと同じである必要があります。

f) 場所を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

g) [OK] をクリックします。

ステップ 10 ASAv の設定項目を設定します。

a) 仮想マシンのサイズを選択します。

ASAv では、Standard D3 および Standard D3_v2 がサポートされます。

b) ストレージ アカウントを選択します。

既存のストレージ アカウントを使用するか、新しいストレージ アカウントを作成できます。ストレージ アカウントの場所はネットワークおよび仮想マシンと同じである必要があります。

c) [Name] フィールドに IP アドレスのラベルを入力し、[OK] をクリックして、パブリック IP アドレスを要求します。

Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミック パブリック IP をデフォルトでは作成します。固定 IP アドレスを優先する場合は、ポータルのパブリック IP を開き、ダイナミック アドレスからスタティック アドレスに変更します。

d) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloupapp.azure.com* の形式になります。

e) 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。

f) ASAv を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要 各インターフェイスを一意のサブネットにアタッチする必要があります。

g) [OK] をクリックします。

ステップ 11 構成サマリを確認し、[OK] をクリックします。

ステップ 12 利用条件を確認し、[Create] をクリックします。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の起動」を参照してください。
- Security Center 内の推奨事項がどのように Azure リソースの保護に役立つかの詳細については、Security Center から入手可能なマニュアルを参照してください。

Azure Resource Manager からの ASAv for High Availability の導入

次の手順は、Microsoft Azure で高可用性（HA）ASAv ペアを設定する手順の概略を示しています。Azure の設定の詳細な手順については、『Azure を使ってみる』を参照してください。

Azure の ASAv HA では、2 つの ASAv を可用性セットに導入し、リソース、パブリック IP アドレス、ルートテーブルなどの各種設定を自動的に生成します。導入後に、これらの設定をさらに管理できます。

ステップ 1 Azure ポータルにログインします。

Azure ポータルは、データセンターの場所に関係なく、現在のアカウントとサブスクリプションに関連付けられた仮想要素を表示します。

ステップ 2 マーケットプレイスで [Cisco ASAv] を検索し、[ASAv 4 NIC HA] をクリックして、フェールオーバー ASAv 構成を導入します。

ステップ 3 [Basics] 設定を構成します。

a) ASAv マシン名のプレフィックスを入力します。ASAv の名前は「プレフィックス」-A と「プレフィックス」-B になります。

重要 既存のプレフィックスを使用していないことを確認します。使用すると、導入は失敗します。

b) ユーザー名を入力します。

これは両方の仮想マシンの管理ユーザー名です。

重要 Azure では、admin というユーザー名は使用できません。

c) 両方の仮想マシンに認証タイプとして、[Password] または [SSH public key] のいずれかを選択します。

[Password] を選択した場合は、パスワードを入力して確定します。

d) サブスクリプション タイプを選択します。

e) [Resource group] を選択します。

[Create new] を選択して新しいリソース グループを作成するか、[Use existing] で既存のリソース グループを選択します。既存のリソース グループを使用する場合は、空である必要があります。そうでない場合は、新しいリソース グループを作成する必要があります。

f) [Location] を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

g) [OK] をクリックします。

ステップ 4 [Cisco ASAv settings] を設定します。

a) 仮想マシンのサイズを選択します。

ASAv では、Standard D3 および Standard D3_v2 がサポートされます。

b) [Managed] または [Unmanaged OS disk] ストレージを選択します。

重要 ASA HA モードでは常に [Managed] を使用します。

ステップ 5 [ASAv-A] 設定を構成します。

a) （オプション）[Create new] を選択して、[Name] フィールドに IP アドレスのラベルを入力し、[OK] をクリックしてパブリック IP アドレスを要求します。パブリック IP アドレスが必要ない場合は、[None] を選択します。

（注） Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミック パブリック IP をデフォルトでは作成します。固定 IP アドレスを優先する場合は、ポータルのパブリック IP を開き、ダイナミック アドレスからスタティック アドレスに変更します。

b) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、*<dnslabel>.<location>.cloupapp.azure.com* の形式になります。

c) ASAv-A 起動時診断のストレージ アカウントに必要な設定を構成します。

ステップ 6 [ASAv-B] 設定についても、この手順を繰り返します。

ステップ 7 既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。

a) ASAv を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要 各インターフェイスを一意のサブネットにアタッチする必要があります。

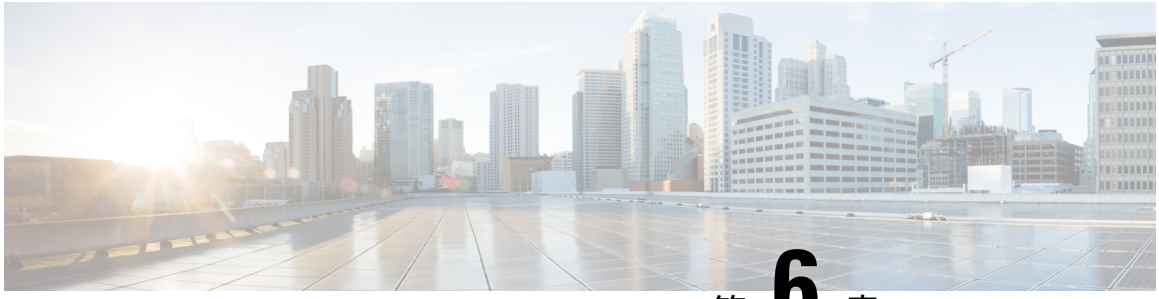
b) [OK] をクリックします。

ステップ 8 構成の [Summary] を確認し、[OK] をクリックします。

ステップ 9 利用条件を確認し、[Create] をクリックします。

次のタスク

- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の起動」を参照してください。
- Azure の ASAv HA 構成の詳細については、『ASA Series General Operations Configuration Guide』の「Failover for High Availability in the Public Cloud」の章を参照してください。



第 6 章

Hyper-V を使用した ASAv の導入

Microsoft Hyper-V を使用して ASAv を導入できます。

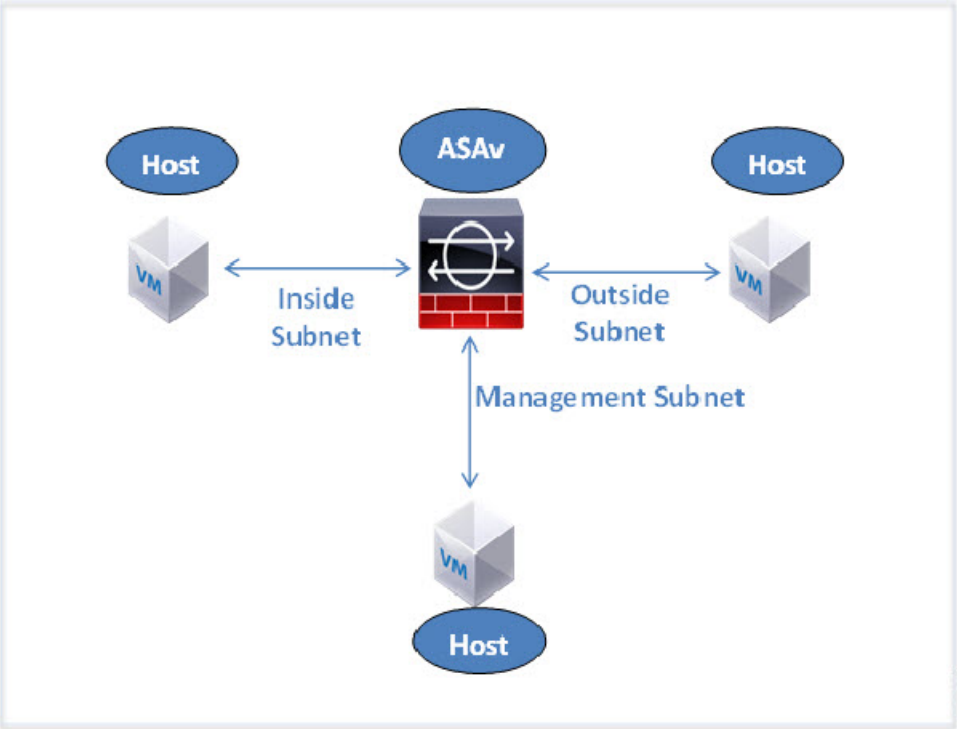
- Hyper-V を使用した ASAv の導入について （97 ページ）
- ASAv および Hyper-V のガイドラインと制限事項 （98 ページ）
- ASAv と Hyper-V の前提条件 （99 ページ）
- 第 0 日のコンフィギュレーション ファイルの準備 （100 ページ）
- Hyper-V マネージャを使用した ASAv と第 0 日用構成ファイルの導入 （102 ページ）
- コマンドラインを使用した Hyper-V への ASAv のインストール （103 ページ）
- Hyper-V マネージャを使用した Hyper-V への ASAv のインストール （104 ページ）
- Hyper-V マネージャからのネットワーク アダプタの追加 （111 ページ）
- ネットワーク アダプタの名前の変更 （113 ページ）
- MAC アドレス スプーフィング （114 ページ）
- SSH の設定 （115 ページ）
- CPU 使用率とレポート （115 ページ）

Hyper-V を使用した ASAv の導入について

スタンドアロンの Hyper-V サーバー上に、または Hyper-V マネージャを介して Hyper-V を導入できます。PowerShell CLI コマンドを使用したインストール手順については、「コマンドラインを使用した Hyper-V への ASAv のインストール」（46 ページ）を参照してください。Hyper-V マネージャを使用したインストール手順については、「Hyper-V マネージャを使用した Hyper-V への ASAv のインストール」（46 ページ）を参照してください。Hyper-V はシリアル コンソール オプションを提供していません。管理インターフェイスを介して SSH または ASDM を通じて Hyper-V を管理できます。SSH の設定については、「SSH の設定」の 54 ページを参照してください。

次の図は、ルーテッド ファイアウォール モードでの ASAv の推奨トポロジを示しています。ASAv 向けに Hyper-V でセットアップされた 3 つのサブネット（管理、内部、および外部）があります。

図 *11* : 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



ASAv および Hyper-V のガイドラインと制限事項

- プラットフォーム サポート
  - Cisco UCS B シリーズ サーバー
  - Cisco UCS C シリーズ サーバー
  - Hewlett Packard Proliant DL160 Gen8
- サポートされる OS
  - Windows Server 2012
  - ネイティブ Hyper-V

（注） ASAv は現在、仮想化に使用されている最新の 64 ビット高性能プラットフォームで稼働します。

- ファイル形式

  Hyper-V への ASAv の初期導入では、VHDX 形式がサポートされています。

- 第 0 日用（Day 0）構成

  必要な ASA CLI 設定コマンドを含むテキスト ファイルを作成します。手順については、「第 0 日のコンフィギュレーション ファイルの準備」を参照してください。

- 第 0 日用構成のファイアウォール トランスペアレント モード

  設定行「firewall transparent」は、第 0 日用コンフィギュレーション ファイルの先頭に配置する必要があります。ファイル内のそれ以外の場所にあると、異常な動作が起きる場合があります。手順については、「第 0 日のコンフィギュレーション ファイルの準備」を参照してください。

- フェールオーバー

  Hyper-V 上の ASAv はアクティブ/スタンバイ フェールオーバーをサポートしています。ルーテッド モードとトランスペアレント モードの両方でアクティブ/スタンバイ フェールオーバーを実行するには、すべての仮想ネットワーク アダプタで MAC アドレス スプーフィングを有効化する必要があります。「MAC アドレス スプーフィングの設定」の 53 ページを参照してください。スタンドアロン ASAv のトランスペアレントモードの場合、管理インターフェイスの MAC アドレススプーフィングは有効にしないでください。アクティブ/アクティブ フェールオーバーはサポートされていません。

- Hyper-V は最大 8 つのインターフェイスをサポートします。Management 0/0 および GigabitEthernet 0/0 ～ 0/6。フェールオーバー リンクとして GigabitEthernet を使用できます。

- VLANs

  トランク モードでインターフェイスに VLAN を設定するには、**Set-VMNetworkAdapterVLan** Hyper-V Powershell コマンドを使用します。管理インターフェイスの NativeVlanID は、特定の VLAN として、または VLAN がない場合は「0」として設定できます。トランク モードは、Hyper-V ホストをリブートした場合は保持されません。各リブート後に、トランク モードを再設定する必要があります。

- レガシー ネットワーク アダプタはサポートされていません。

- 第 2 世代仮想マシンはサポートされていません。

- Microsoft Azure はサポートされていません。

ASAv と Hyper-V の前提条件

- MS Windows 2012 に Hyper-V をインストールします。

- 第 0 日用コンフィギュレーション テキスト ファイルを使用する場合は、それを作成します。

  ASAv の初回導入前に、第 0 日用構成を追加する必要があります。追加しない場合は、第 0 日用構成を使用するために、ASAv から write erase を実行する必要があります。手順については、「第 0 日のコンフィギュレーション ファイルの準備」を参照してください。

- Cisco.com から ASAv VHDX ファイルをダウンロードします。

  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。

- Hyper-V スイッチには、3 つ以上のサブネット/VLAN が構成されます。
- Hyper-V システム要件については、Cisco ASA の互換性 [英語] 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 サーバー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。

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 ASAv 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。
- 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 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。
- ASAv の初回起動前に、第 0 日用構成ファイルを追加する必要があります。ASAv の初回起動後に第 0 日用構成ファイルを使用する場合は、**write erase** コマンドを実行し、第 0 日用構成 ファイルを適用してから、ASAv を起動する必要があります。

ステップ 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方法です。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 9.5.1
!
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
```

ステップ 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。

ステップ 3 （任意）ダウンロードしたファイルから ID トークンをコピーし、ID トークンのみを含むテキスト ファイルを作成します。

ステップ 4 （任意）ASAv の初期導入時に自動的にライセンスを許諾する場合は、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）SSmart 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 サーバー
- 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

ステップ 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 サーバーに ASAv が自動的に登録されます。

ステップ 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構成ファイルを作成します。

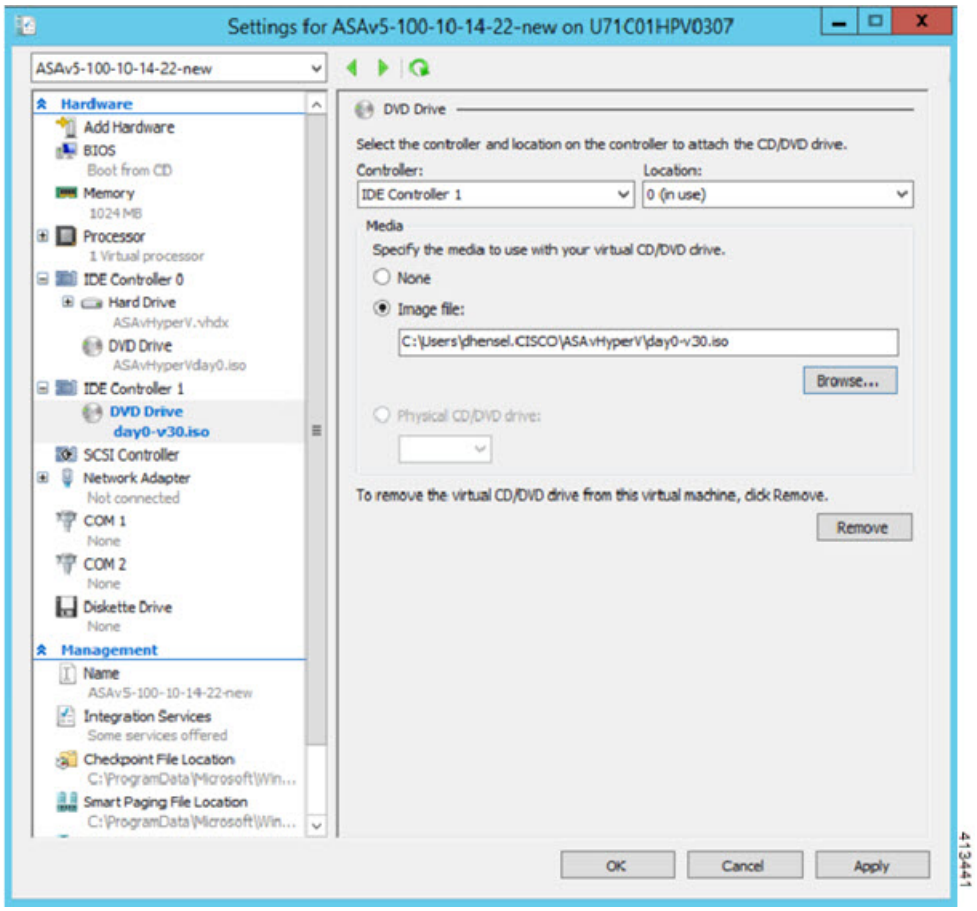
Hyper-V マネージャを使用した ASAv と第 0 日用構成ファイルの導入

第 0 日用コンフィギュレーションファイルを設定したら（「第 0 日のコンフィギュレーションファイルの準備」）、Hyper-V マネージャを使用して導入できます。

ステップ 1 **[Server Manager]** > **[Tools]** > **[Hyper-V Manager]** に移動します。

ステップ 2 Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] の下で、[IDE Controller 1] をクリックします。

図 *12 : Hyper-V* マネージャ



ステップ 3 右側のペインの [Media] の下で、[Image file] のラジオ ボタンを選択して、第 0 日用 ISO コンフィギュレーション ファイルを保存するディレクトリを参照し、[Apply] をクリックします。ASAv は、初回起動時に、第 0 日用構成ファイルの内容に基づいて構成されます。

コマンドラインを使用した Hyper-V への ASAv のインストール

Windows PowerShell コマンドラインを介して Hyper-V に ASAv をインストールできます。スタンドアロンの Hyper-V サーバー上にいる場合は、コマンド ラインを使用して Hyper-V をインストールする必要があります。

ステップ 1 Windows Powershell を開きます。

ステップ 2 ASAv を導入します。

例：

```
new-vm -name $fullVMName -MemoryStartupBytes $memorysize -Generation 1 -vhdpath
C:\Users\jsmith.CISCO\ASAvHyperV\$ImageName.vhdx -Verbose
```

ステップ 3 ASAv のモデルに応じて、CPU 数をデフォルトの 1 から変更します。

例：

```
set-vm -Name $fullVMName -ProcessorCount 4
```

ステップ 4 （任意）インターフェイス名をわかりやすい名前に変更します。

例：

```
Get-VMNetworkAdapter -VMName $fullVMName -Name "Network Adapter" | Rename-vmNetworkAdapter -NewName
mgmt
```

ステップ 5 （任意）ネットワークで必要な場合は、VLAN ID を変更します。

例：

```
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1151 -Access -VMNetworkAdapterName "mgmt"
```

ステップ 6 Hyper-V が変更を反映するように、インターフェイスを更新します。

例：

```
Connect-VMNetworkAdapter -VMName $fullVMName -Name "mgmt" -SwitchName 1151mgmtswitch
```

ステップ 7 内部インターフェイスを追加します。

例：

```
Add-VMNetworkAdapter -VMName $fullVMName -name "inside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1552 -Access -VMNetworkAdapterName "inside"
```

ステップ 8 外部インターフェイスを追加します。

例：

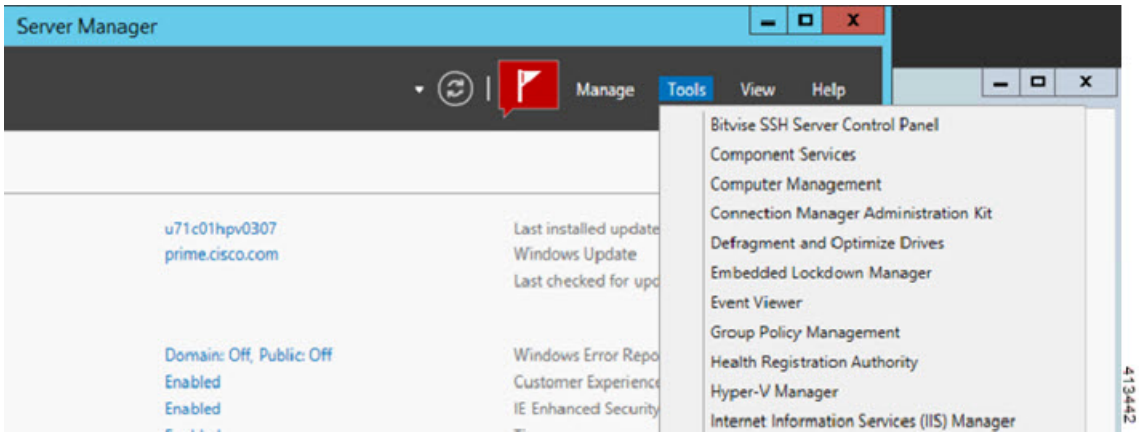
```
Add-VMNetworkAdapter -VMName $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName “outside"
```

Hyper-V マネージャを使用した Hyper-V への ASAv のインストール

Hyper-V マネージャを使用して、Hyper-V に ASAv をインストールできます。

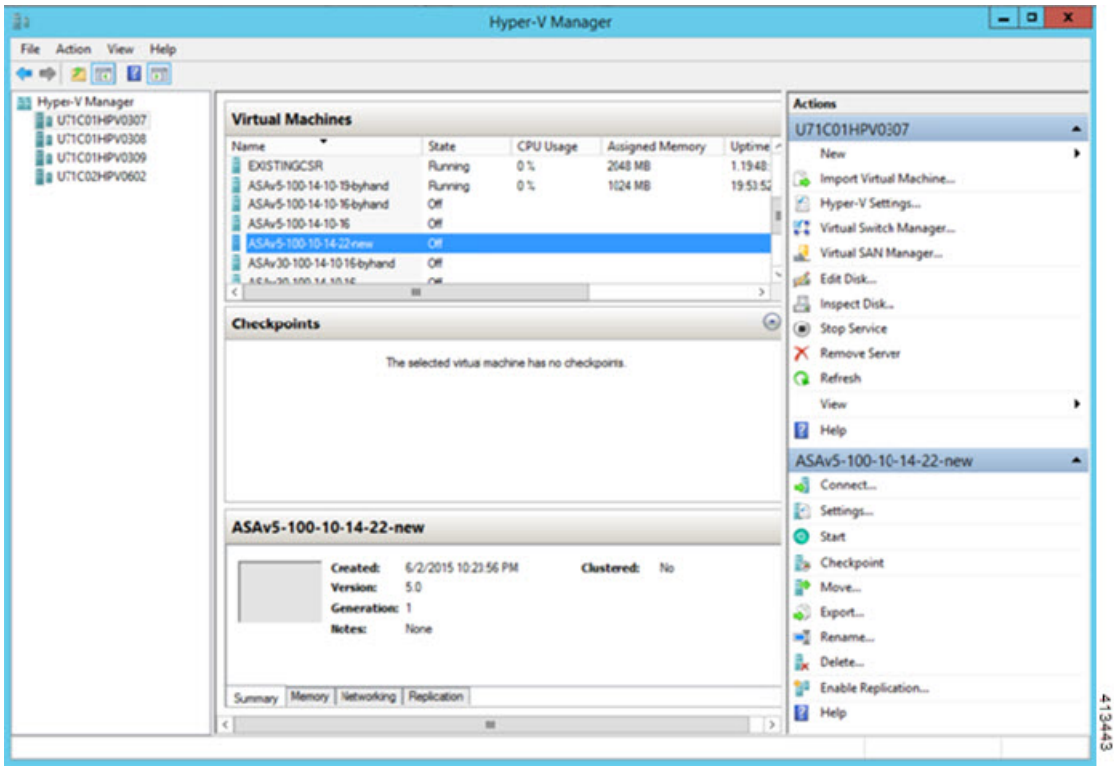
ステップ 1 **[Server Manager]** > **[Tools]** > **[Hyper-V Manager]** に移動します。

図 *13 : Server Manager*



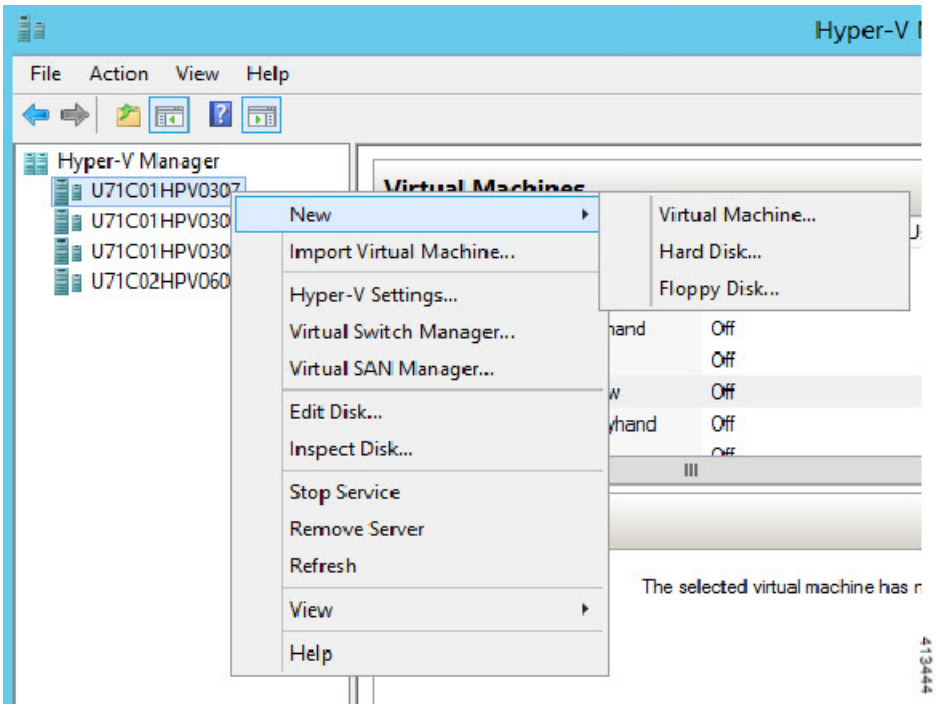
ステップ 2 Hyper-V マネージャが表示されます。

図 *14 : Hyper-V* マネージャ



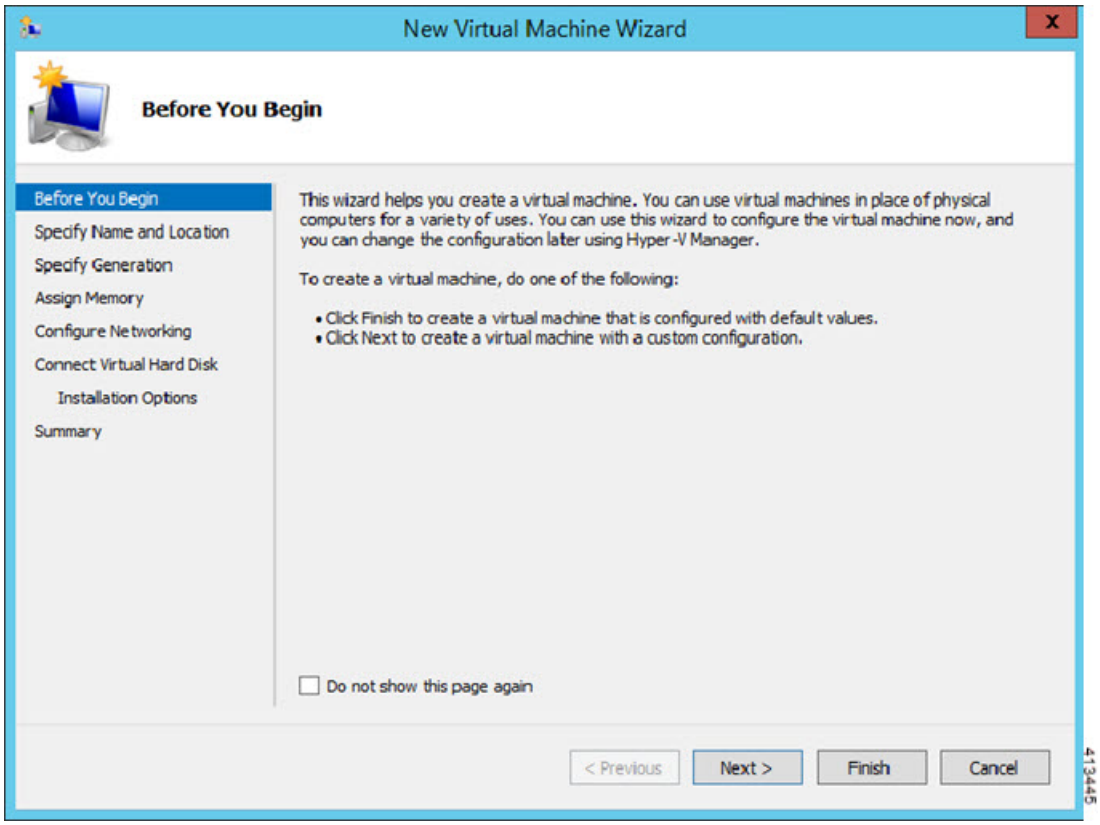
ステップ 3 右側のハイパーバイザのリストから、目的のハイパーバイザを右クリックし、**[New]** > **[Virtual Machine]** を選択します。

図 *15* : 新規仮想マシンの起動



ステップ 4 [New Virtual Machine] ウィザードが表示されます。

図 *16 : [New Virtual Machine]* ウィザード



ステップ 5 ウィザードを通じて作業し、次の情報を指定します。

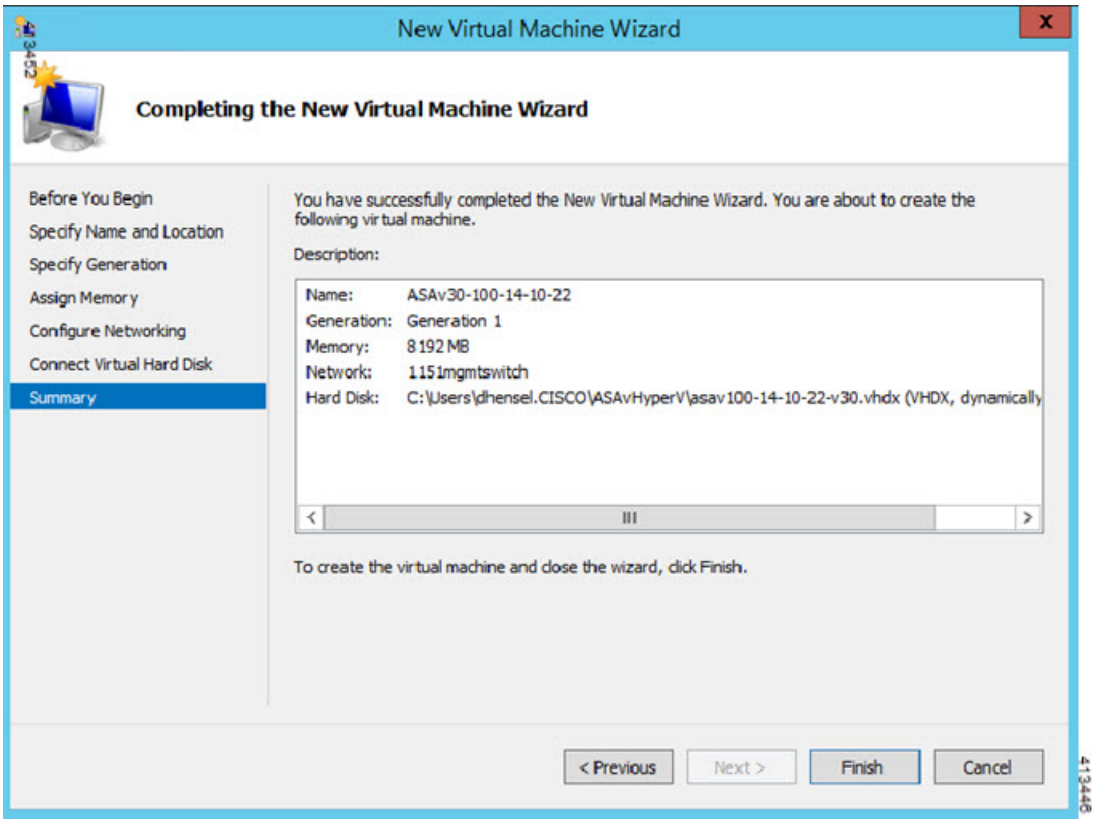
- ASAv の名前と場所
- ASAv の世代

  ASAv でサポートされている唯一の世代は [世代1（Generation 1）] です。
- ASAv のメモリ量（ASAv5 の場合は 1024 MB、ASAv10 の場合は 2048 MB、ASAv30 の場合は 8192 MB）
- ネットワーク アダプタ（セットアップ済みの仮想スイッチに接続）
- 仮想ハード ディスクと場所

  [Use an existing virtual hard disk] を選択し、VHDX ファイルの場所を参照します。

ステップ 6 [終了（Finish）] をクリックすると、ASAv 構成を示すダイアログボックスが表示されます。

図 *17* : 新規仮想マシンの概要

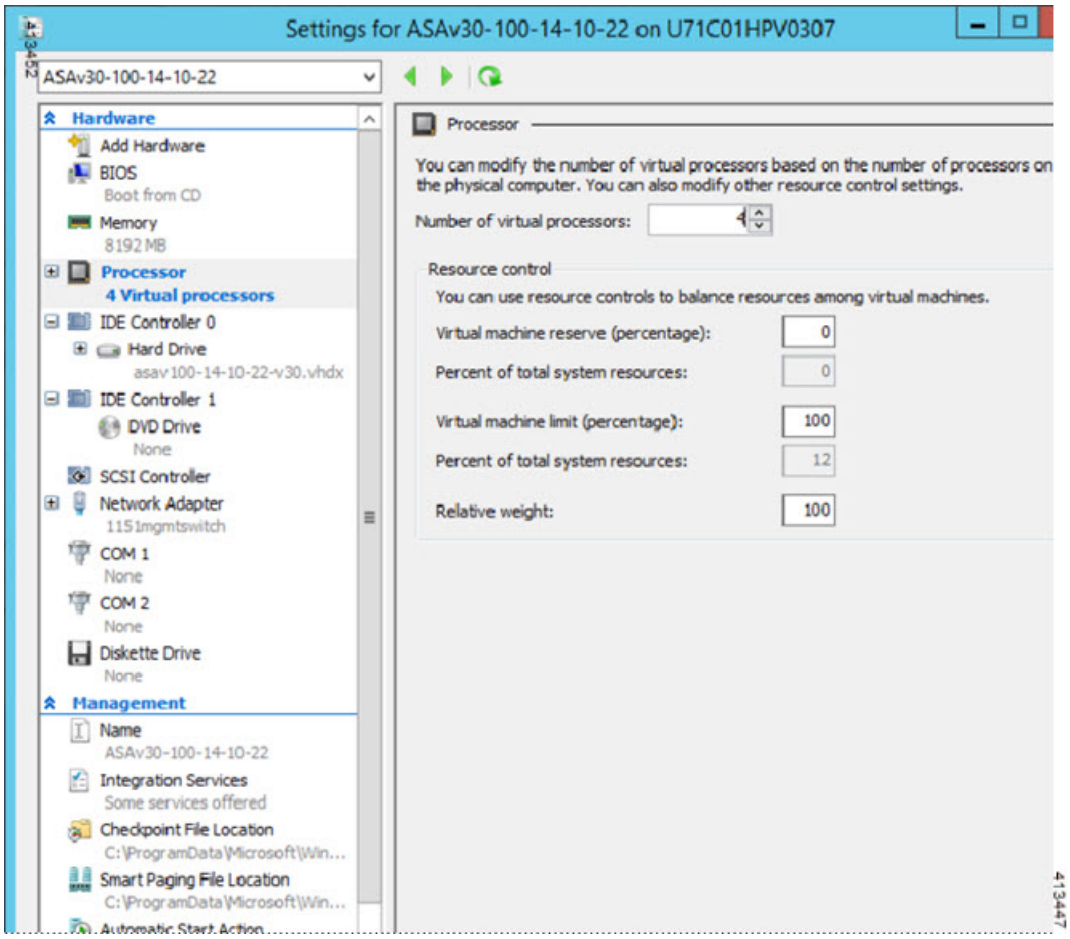


ステップ 7 ASAv に 4 つの vCPU がある場合は、ASAv を起動する前に、vCPU 値を変更する必要があります。Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Processor] をクリックし、[Processor] ペインを表示します。[Number of virtual processors] を 4 に変更します。

ASAv5 と ASAv10 には 1 つの vCPU があり、ASAv30 には 4 つの vCPU があります。デフォルトは 1 です。

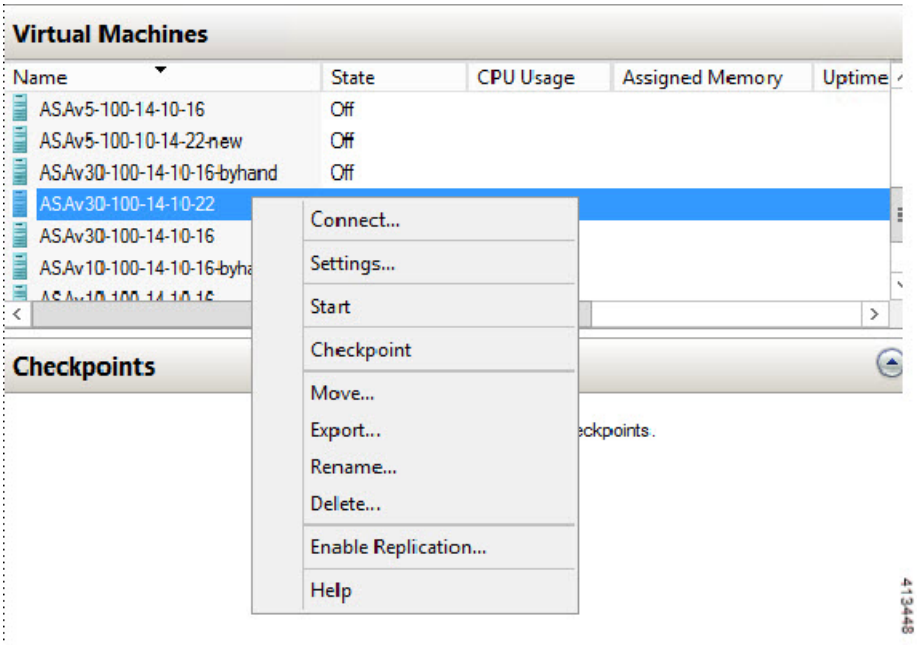
100Mbps および 1Gbps の権限付与では 1 個の vCPU、2Gbps の権限付与では 4 個の vCPU となります。デフォルトは 1 です。

図 *18* : 仮想マシンのプロセッサの設定



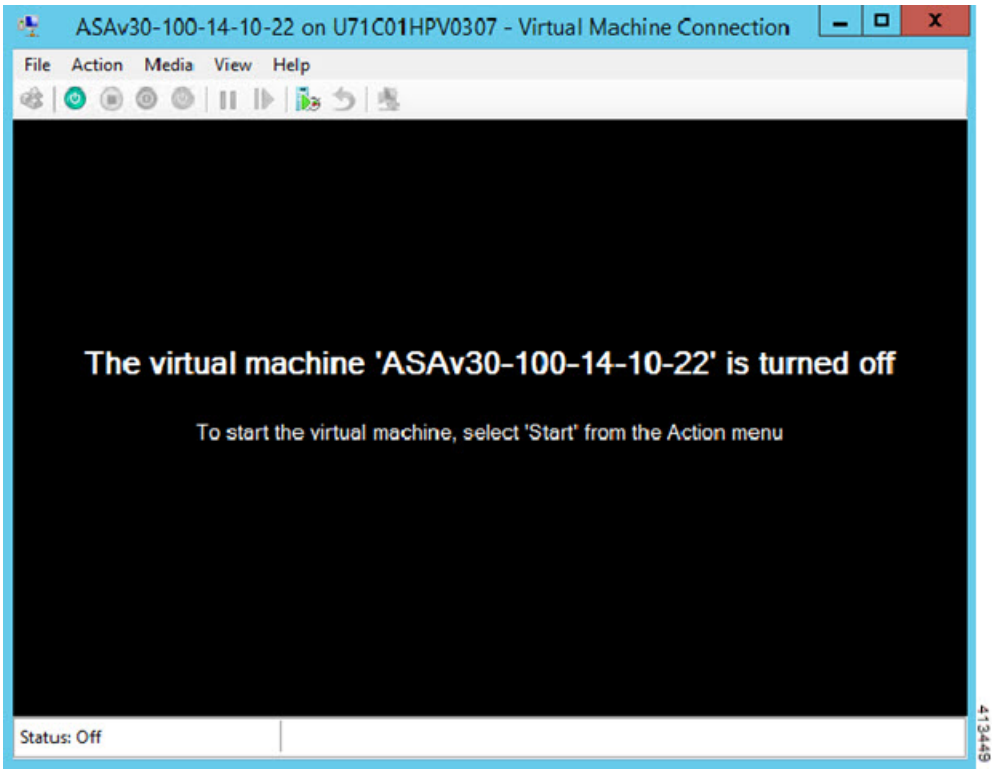
ステップ 8 [仮想マシン（Virtual Machines）] メニューで、リスト内の ASAv の名前を右クリックし、[接続（Connect）] をクリックして、ASAv に接続します。コンソールが開き、停止されている ASAv が表示されます。

図 *19* : 仮想マシンへの接続



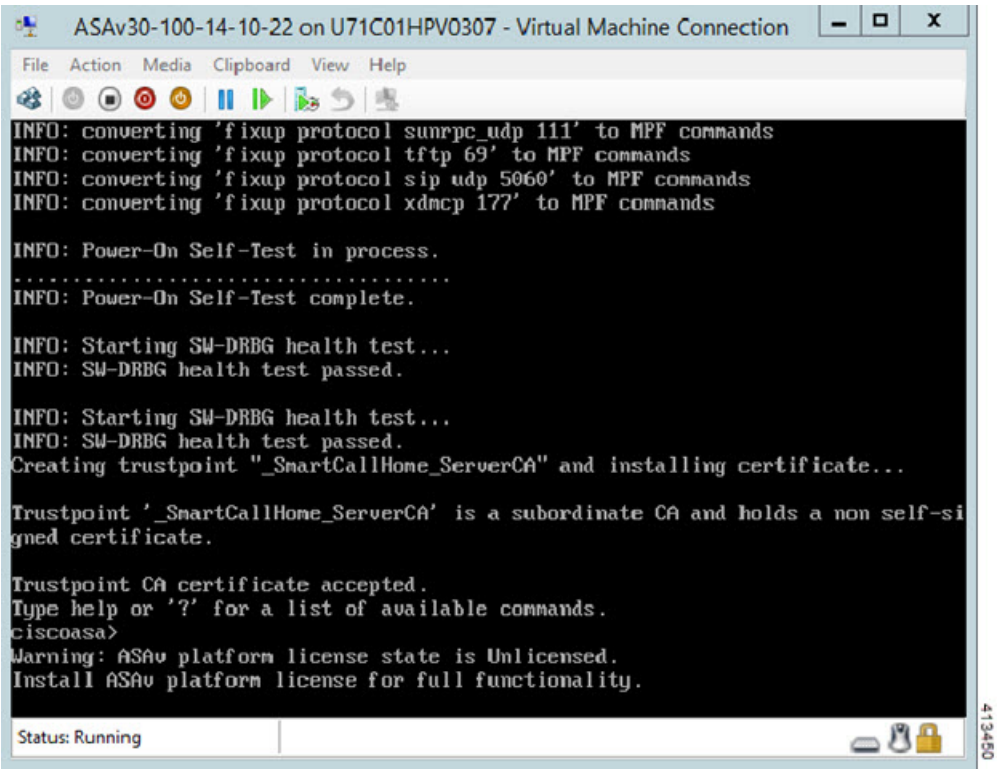
ステップ 9 [仮想マシンの接続（Virtual Machine Connection）] コンソールウィンドウで、青緑色の開始ボタンをクリックして、ASAv を起動します。

図 *20* : 仮想マシンの開始



ステップ 10 ASAv の起動の進行状況がコンソールに表示されます。

図 *21* : 仮想マシンの起動の進行状況



Hyper-V マネージャからのネットワーク アダプタの追加

新しく導入された ASAv のネットワークアダプタは 1 つだけです。さらに 2 つ以上のネットワーク アダプタを追加する必要があります。この例では、内部ネットワーク アダプタを追加します。

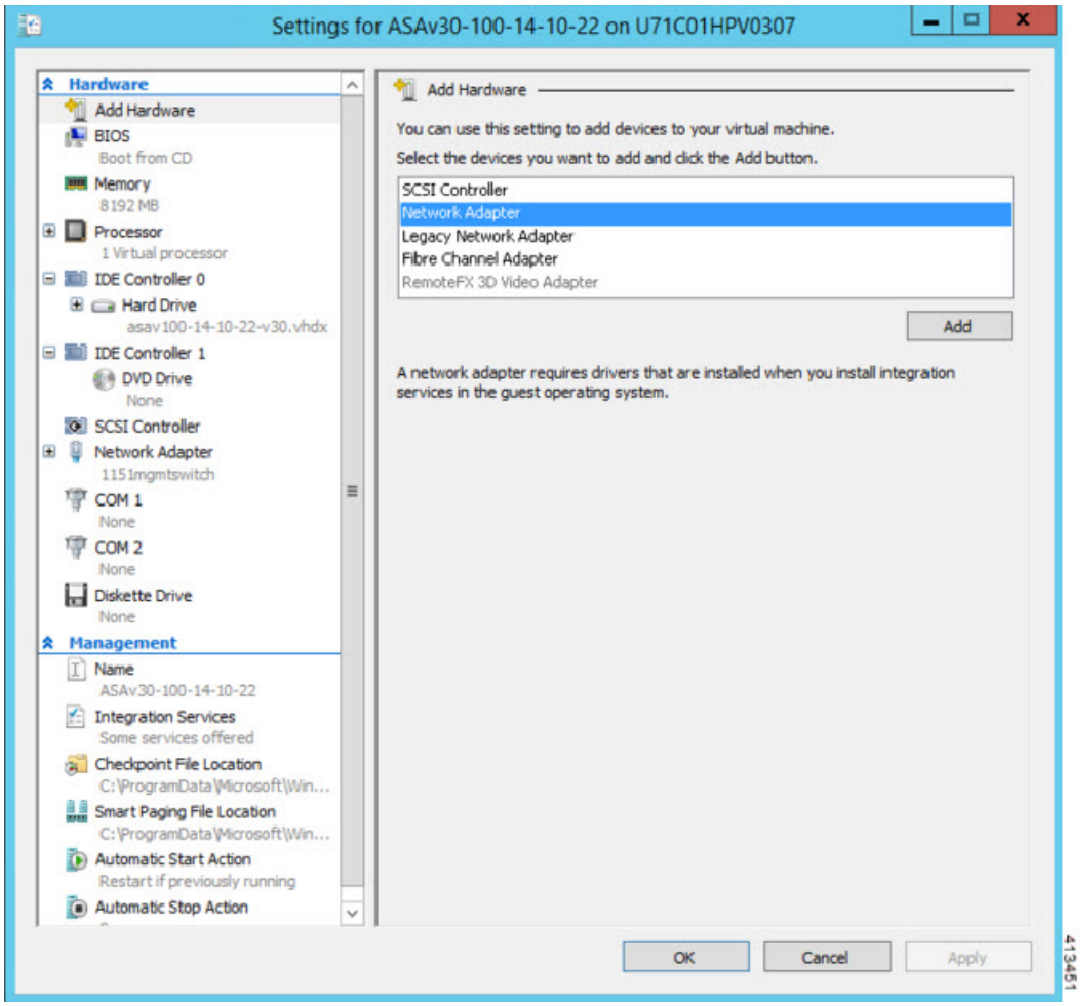
始める前に

- ASAv はオフ状態である必要があります。

ステップ 1 Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Add Hardware] をクリックし、次に [Network Adapter] をクリックします。

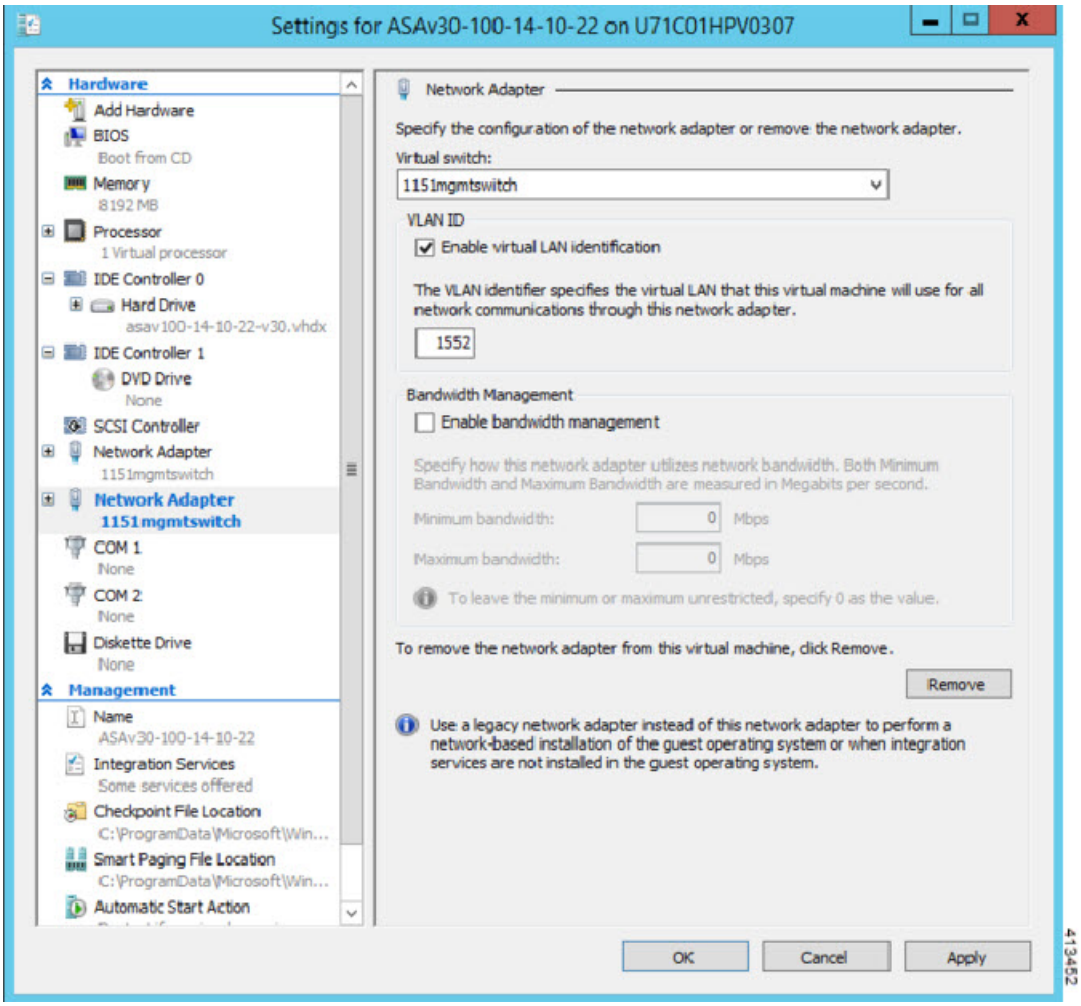
（注） レガシー ネットワーク アダプタを使用しないでください。

図 *22* : ネットワーク アダプタの追加



ステップ 2 ネットワーク アダプタの追加後、仮想スイッチとその他の機能を変更できます。また、必要に応じてVLAN ID を設定できます。

図 *23* : ネットワーク アダプタ設定の変更



ネットワーク アダプタの名前の変更

Hyper-V では、「Network Adapter」という汎用ネットワーク インターフェイス名が使用されます。このため、ネットワーク インターフェイスがすべて同じ名前であると、紛らわしい場合があります。Hyper-V マネージャを使用して名前を変更することはできません。Windows Powershell コマンドを使用して変更する必要があります。

ステップ 1 Windows Powershell を開きます。

ステップ 2 必要に応じてネットワーク アダプタを変更します。

例：

```
$NICRENAME= Get-VMNetworkAdapter -VMName 'ASAvVM' -Name "Network Adapter"
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[0] -newname inside
rename-VMNetworkAdapter -VMNetworkAdapter $NICRENAME[1] -newname outside
```

MAC アドレス スプーフィング

ASAvがトランスペアレントモードでパケットを渡し、HAアクティブ/スタンバイフェールオーバーに対応できるように、すべてのインターフェイスの MAC アドレススプーフィングを有効にする必要があります。Hyper-V マネージャ内で、または Powershell コマンドを使用して、これを実行できます。

Hyper-V マネージャを使用した MAC アドレス スプーフィングの設定

Hyper-V マネージャを使用して、MAC スプーフィングを Hyper-V に設定できます。

ステップ 1 **[Server Manager]** > **[Tools]** > **[Hyper-V Manager]** に移動します。

Hyper-V マネージャが表示されます。

ステップ 2 Hyper-V マネージャの右側の [Settings] をクリックして、設定ダイアログ ボックスを開きます。

ステップ 3 左側の [Hardware] メニューで次の操作をします。

1. [Inside] をクリックして、メニューを展開します。
2. [Advanced Features] をクリックして、MAC アドレス オプションを表示します。
3. [Enable MAC address spoofing] ラジオ ボタンをクリックします。

ステップ 4 外部インターフェイスでも、この手順を繰り返します。

コマンド ラインを使用した MAC アドレス スプーフィングの設定

Windows Powershell コマンド ラインを使用して、MAC スプーフィングを Hyper-V に設定できます。

ステップ 1 Windows Powershell を開きます。

ステップ 2 MAC アドレス スプーフィングを設定します。

例：

```
Set-VMNetworkAdapter -VMName $vm_name\
-ComputerName $computer_name -MacAddressSpoofing On\
-VMNetworkAdapterName $network_adapter\r"
```

SSH の設定

Hyper-V マネージャの [仮想マシンの接続（Virtual Machine Connection）] から管理インターフェイスを介して SSH アクセスできるように ASAv を設定できます。第 0 日用コンフィギュレーション ファイルを使用している場合は、ASAv への SSH アクセスを追加できます。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」を参照してください。

ステップ 1 RSAキー ペアが存在することを確認します。

例：

```
asav# show crypto key mypubkey rsa
```

ステップ 2 RSAキー ペアがない場合は、RSAキー ペアを生成します。

例：

```
asav(conf t)# crypto key generate rsa modulus 2048

username test password test123 privilege 15
aaa authentication ssh console LOCAL
ssh 10.7.24.0 255.255.255.0 management
ssh version 2
```

ステップ 3 別の PC から SSH を使用して ASAv にアクセスできることを確認します。

CPU 使用率とレポート

CPU使用率レポートには、指定された時間内に使用されたCPUの割合の要約が表示されます。通常、コアはピーク時以外には合計 CPU 容量の約 30 ～ 40% で動作し、ピーク時は約 60 ～ 70% の容量で動作します。

ASA Virtual の vCPU 使用率

ASA Virtual の vCPU 使用率には、データパス、制御ポイント、および外部プロセスで使用されている vCPU の量が表示されます。

Hyper-V で報告される vCPU 使用率には、ASA Virtual の使用率に加えて、次のものが含まれます。

- ASA Virtual アイドル時間

- ASA Virtual マシンに使用された %SYS オーバーヘッド

CPU 使用率の例

CPU 使用率の統計情報を表示するには、**show cpu usage** コマンドを使用します。

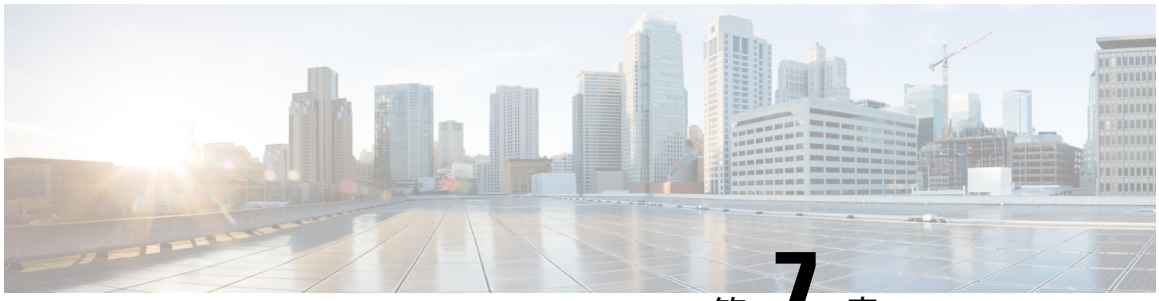
例

```
Ciscoasa#show cpu usage

CPU □□□□5□□□ 1%□1 □□□ 2%□5 □□□ 1%
```

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASA Virtual レポート：40%
- DP：35%
- 外部プロセス：5%
- ASA（ASA Virtual レポート）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%



第 7 章

ASAv の設定

ASAv の導入では、ASDM アクセスを事前設定します。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 の起動 （117 ページ）
- ASDM を使用した初期設定の実行 （118 ページ）
- 詳細設定 （120 ページ）

ASDM の起動

ステップ 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 起動ウィンドウが表示されます。

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

ステップ 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) ユーザー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、ユーザー名および**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。HTTPS 認証を有効にした場合、ユーザー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、ユーザー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。HTTPS 認証を有効にした場合、ユーザー名と関連付けられたパスワードを入力します。

ステップ 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、ショートカットをコンピュータに保存します。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) ユーザー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。HTTPS 認証を有効にした場合、ユーザー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。

- Startup Wizard の実行
- （任意）ASAv の内側にあるパブリックサーバーへのアクセス許可
- （オプション）VPN ウィザードの実行
- （オプション）ASDM の他のウィザードの実行

CLI の設定については、Cisco ASA シリーズ CLI コンフィギュレーション ガイド [英語] を参照してください。

Startup Wizard の実行

セキュリティ ポリシーをカスタマイズして導入方法に最適化するには、[Startup Wizard] を実行します。

ステップ 1 **[Wizards]** > **[Startup Wizard]** を選択します。

ステップ 2 セキュリティ ポリシーをカスタマイズして、導入方法に最適化します。次を設定できます。

- 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 サーバー
- ネットワーク アドレス変換規則
- その他の項目

（任意）ASAv の内側にあるパブリックサーバーへのアクセス許可

[設定（Configuration）] > [ファイアウォール（Firewall）] > [パブリックサーバー（Public Servers）] ペインで、セキュリティポリシーが自動的に設定され、インターネットから内部サーバーにアクセスできるようになります。ビジネス オーナーとして、内部ネットワーク サービス（Web サーバーや FTP サーバーなど）に外部ユーザー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 サーバーを配置すると、パブリック サーバー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。

- サイト間 VPN ウィザード：ASAv と別の VPN 対応デバイス間で IPsec サイト間トンネルを作成します。
- AnyConnect VPN ウィザード：Cisco AnyConnect VPN Client の SSL VPN リモートアクセスを設定します。AnyConnect クライアント では ASA へのセキュアな SSL 接続が提供されるため、リモートユーザーによる企業リソースへのフル VPN トンネリングが可能になります。ASA ポリシーを設定すると、リモートユーザーが最初にブラウザを使用して接続するときに、AnyConnect クライアントをダウンロードできます。AnyConnect クライアント 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、ユーザーは Web 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、ユーザー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ー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。

Azure への ASAv IPsec 仮想トンネルインターフェイス（VTI）接続の構成方法については、『Azure への ASA IPsec VTI 接続の構成』を参照してください。

（オプション）ASDM の他のウィザードの実行

高可用性を備えたフェールオーバー、VPN クラスタ ロード バランシング、およびパケット キャプチャを設定するには、ASDM でその他のウィザードを実行します。

- 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。

詳細設定

ASAv の設定を続行するには、Cisco ASA シリーズ ドキュント一覧 [英語] を参照してください。

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。