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

バージョン 9.7

発行日:2017 年 1 月 18 日
更新日:2018 年 4 月 3 日

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

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご覧いただくことができます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

Cisco ASAv の概要

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

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

- ASAv の前提条件（3 ページ）
- ASAv のガイドライン（3 ページ）
- ASAv のレート リミッタ（4 ページ）
- ASAv のライセンス（5 ページ）
- ASAv インターフェイスおよび仮想 NIC（6 ページ）

ASAv の前提条件

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

ASAv のガイドライン

コンテキスト モードのガイドライン

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

フェールオーバーのガイドライン

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

サポートしない ASA 機能

ASAv は、次の ASA 機能をサポートしません。

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

ASAv5 のガイドライン、機能、および制約事項

- ジャンボ フレームはサポートされていません。
- 1 GB のメモリ搭載の VMware、KVM、および Hyper-V に導入できます。

  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プロビジョニングする必要があります。9.5.1.200 以降のバージョンを実行する ASAv のみが 1 GB のメモリで動作可能です。以前のバージョンにダウングレードする場合は、メモリを 2 GB に増やす必要があります。
- スループットは 100 Mbps です。

  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）。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。
- 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。

ASAv のレート リミッタ

注: ASAv レート リミッタは、いくらかの余剰なヘッドルームを使用して ASAv5 のスループット パフォーマンスを、権限付与と組み込みのラボ エディション モードの ASAv プラットフォームに適合させます。

表 1（4 ページ）は、ASAv のライセンスの権限付与に一致する準拠したリソース シナリオを示しています。

表 1　ライセンスの権限付与

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	100Mbps	あり
ASAv10（1 G）	1 vCPU/2 GB	vCPU/RAM 制限付き	なし
ASAv30（2 G）	4 vCPU/8 GB	vCPU/RAM 制限付き	なし

表 2（4 ページ）は、ASAv のリソースおよび権限付与に関連する ASAv の状態とメッセージを示しています。

表 2　ASAv の状態とメッセージ

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、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（1 vCPU、1 G）、ASAv10（1 vCPU、2 G）、ASAv30（4 vCPU、8 G） 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	ASAv5 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 および ASAv30 は、エラー メッセージがコンソールに出力された後、リブートされます。

ASAv のライセンス

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

モデル	ライセンス要件
ASAv5	標準ライセンス 次の仕様を参照してください。 ■ 100 Mbps スループット ■ 1 vCPU ■ 1GB RAM ■ 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 インスタンスで Azure をサポート
ASAv10	標準ライセンス 次の仕様を参照してください。 ■ 1 Gbps スループット ■ 1 vCPU ■ 2 GB のメモリ ■ 100,000 の同時ファイアウォール接続 ■ c3.large インスタンスで AWS をサポート ■ Standard D3 インスタンスで Azure をサポート
ASAv30	標準ライセンス 次の仕様を参照してください。 ■ 2 Gbps スループット ■ 4 vCPU ■ 8 GB RAM ■ 500,000 の同時ファイアウォール接続 ■ c3.xlarge インスタンスで AWS をサポート ■ Standard D3 インスタンスで Azure をサポート

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

ASAv インターフェイスおよび仮想 NIC

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

- ASAv インターフェイス（6 ページ）
- サポートされる vNIC（6 ページ）

ASAv インターフェイス

ASAv は、次のギガビット イーサネット インターフェイスがあります。

- Management 0/0

  Azure の場合、Management 0/0 はトラフィック伝送用の「外部」インターフェイスの場合があります。

- 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。
- 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。

サポートされる vNIC

ASAv は次の vNIC をサポートします。

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

VMware を使用した ASAv の導入

VMware を使用して ASAv を導入できます。

- ASAv の VMware 機能のサポート（7 ページ）
- ASAv と VMware の前提条件（8 ページ）
- ASAv および VMware のガイドライン（8 ページ）
- ASAv ソフトウェアの開梱と VMware 対応第 0 日用コンフィギュレーション ファイルの作成（10 ページ）
- VMware vSphere Web Client を使用した ASAv の導入（12 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（16 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（17 ページ）
- ASAv コンソールへのアクセス（17 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（19 ページ）

ASAv の VMware 機能のサポート

表 1（7 ページ）に、ASAv の VMware 機能のサポートを示します。

表 1　の VMware 機能のサポート ASAv

機能	説明	サポート（あり/なし）	コメント
コールド クローン	クローニング中に VM の電源がオフになります。	あり	–
DRS	動的リソースのスケジューリングおよび分散電源管理に使用されます。	あり	VMware のガイドラインを参照してください。
ホット追加	追加時に VM が動作しています。	なし	–
ホット クローン	クローニング中に VM が動作しています。	なし	–
ホット リムーブ	取り外し中に VM が動作しています。	なし	–
スナップショット	VM が数秒間フリーズします。	あり	使用には注意が必要です。トラフィックが失われる可能性があります。フェールオーバーが発生することがあります。
一時停止と再開	VM が一時停止され、その後再開します。	あり	–
vCloud Director	VM の自動配置が可能になります。	なし	–
VM の移行	移行中に VM の電源がオフになります。	あり	–
VMotion	VM のライブ マイグレーションに使用されます。	あり	共有ストレージを使用します。vMotion に関するガイドライン（9 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 VM の障害に対して ASAv のフェールオーバーを使用します。

表 1　の VMware 機能のサポート ASAv（続き）

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

ASAv と VMware の前提条件

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

vSphere 標準スイッチのセキュリティ ポリシー

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

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

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

表 2　ポート グループのセキュリティ ポリシーの例外

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

ASAv および VMware のガイドライン

OVF ファイルのガイドライン

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

- asav-vi：vCenter に導入する場合
- asav-esxi：ESXi に導入する場合（vCenter なし）
- ASAv OVF の導入は、ローカリゼーション（非英語モードでのコンポーネントのインストール）をサポートしません。ご自身の環境の VMware vCenter と LDAP サーバが ASCII 互換モードでインストールされていることを確認してください。
- ASAv をインストールして VM コンソールを使用する前に、キーボードを [United States English] に設定する必要があります。

フェールオーバーのガイドライン

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

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の場合、パフォーマンスに影響する場合があり、オーバープロビジョニングの場合、ASAv によりリロードが行われることが警告されます。待機期間(100 ～ 125 % のオーバープロビジョニングの場合は 24 時間、125 % 以上の場合は 1 時間)の後、ASAv はリロードします。

  注:メモリまたは vCPU ハードウェア設定を変更する必要がある場合は、ASAv のライセンス(5 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。

CPU 予約

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

  仮想マシンの [Performance] タブの [Home] ビューに配置された [CPU Usage (MHz)] チャートからすべての仮想マシンに関する CPU 使用率をホストの視点から確認できます。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れば、その情報を CPU 予約の調整時の入力として使用できます。

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

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

IPv6 のガイドライン

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

vMotion に関するガイドライン

- vMotion を使用する場合、共有ストレージのみを使用することをお勧めします。ASAv の導入時に、ホスト クラスタがある場合は、ストレージをローカルに(特定のホスト上)、または共有ホスト上でプロビジョニングできます。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。

その他のガイドラインと制限事項

- ESXi 5.0 を実行している場合、vSphere Web クライアントは ASAv OVF の導入ではサポートされません。代わりに、vSphere クライアントを使用してください。

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

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

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

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

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

手順

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

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

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

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

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

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

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

   例：

```
ASA Version 9.5.1
!
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
```

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

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

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

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

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

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

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

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

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

   Example.mf ファイル

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

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

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

VMware vSphere Web Client を使用した ASAv の導入

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

- vSphere Web Client へのアクセスとクライアント統合プラグインのインストール（12 ページ）
- VMware vSphere Web Client を使用した ASAv の導入（13 ページ）

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

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

手順

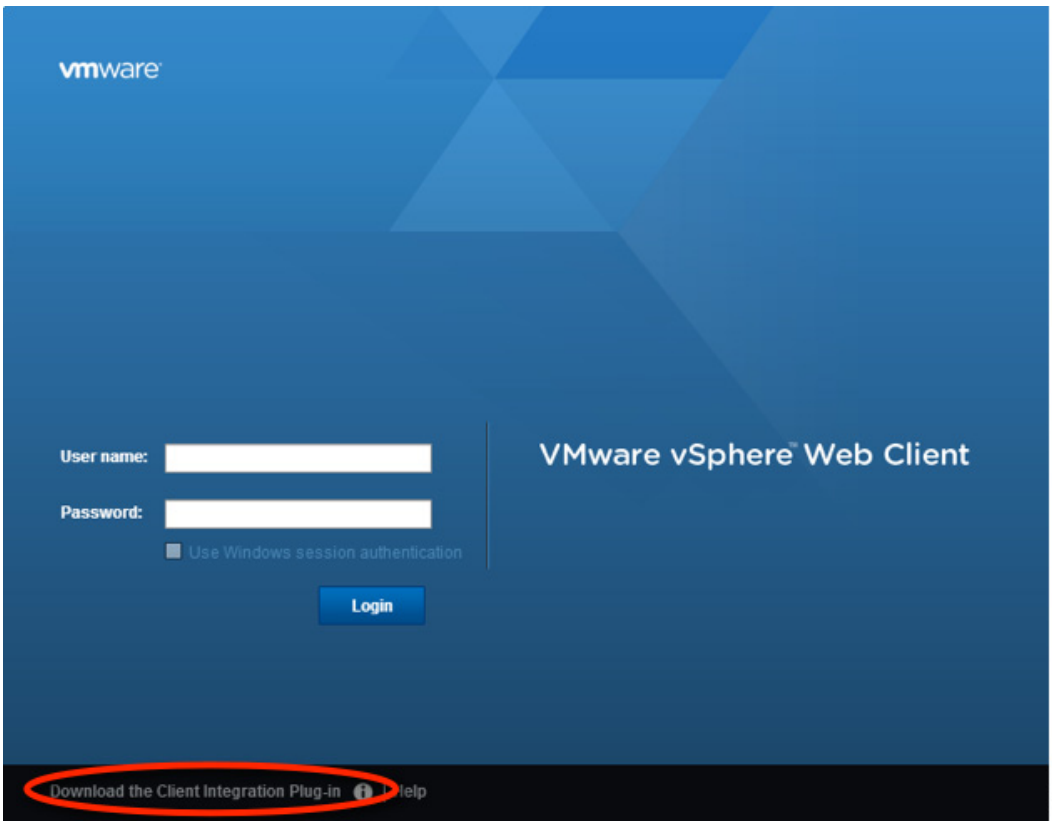
1. ブラウザから VMware vSphere Web Client を起動します。

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

   デフォルトでは、port は 9443 です。

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

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



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

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

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

VMware vSphere Web Client を使用した ASAv の導入

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

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

はじめる前に

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

手順

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

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

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

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

3. [Hosts and Clusters] をクリックします。

4. ASAv を導入するデータセンター、クラスタ、またはホストを右クリックして、[Deploy OVF Template] を選択します。

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

5. ウィザード画面の指示に従って進みます。

6. [Setup networks] 画面で、使用する各 ASAv インターフェイスにネットワークをマッピングします。

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

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

ネットワーク アダプタ ID	ASAv インターフェイス ID
ネットワーク アダプタ 8	GigabitEthernet0/6
ネットワーク アダプタ 9	GigabitEthernet0/7
ネットワーク アダプタ 10	GigabitEthernet0/8

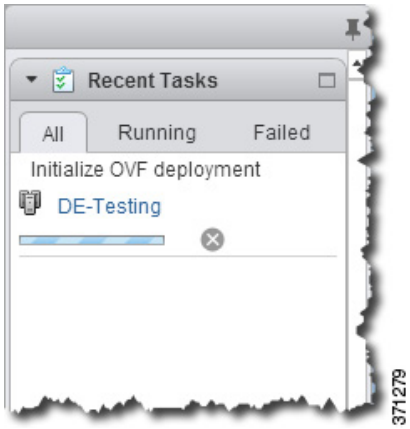
すべての ASAv インターフェイスを使用する必要はありません。ただし、vSphere Web Client ではすべてのインターフェイスにネットワークを割り当てる必要があります。使用しないインターフェイスについては、ASAv 設定内でインターフェイスを無効のままにしておくことができます。ASAv を導入した後、任意で vSphere Web Client に戻り、[Edit Settings] ダイアログボックスから余分なインターフェイスを削除することができます。詳細については、vSphere Web Client のオンライン ヘルプを参照してください。

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

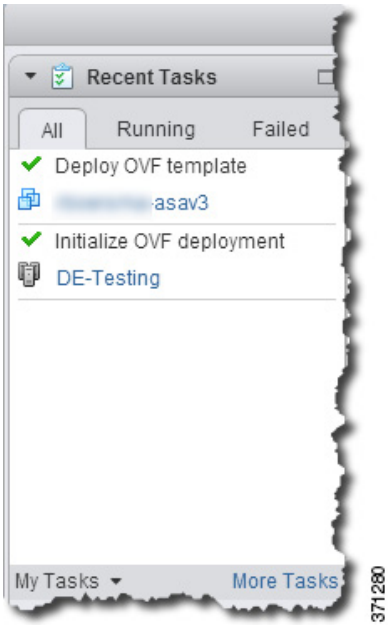
7. インターネット アクセスに HTTP プロキシを使用する場合は、[Smart Call Home Settings] 領域でスマート ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。
8. フェールオーバー/HA 配置の場合、[Customize template] 画面で次の処理を行います。
   - スタンバイ管理 IP アドレスを指定します。

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

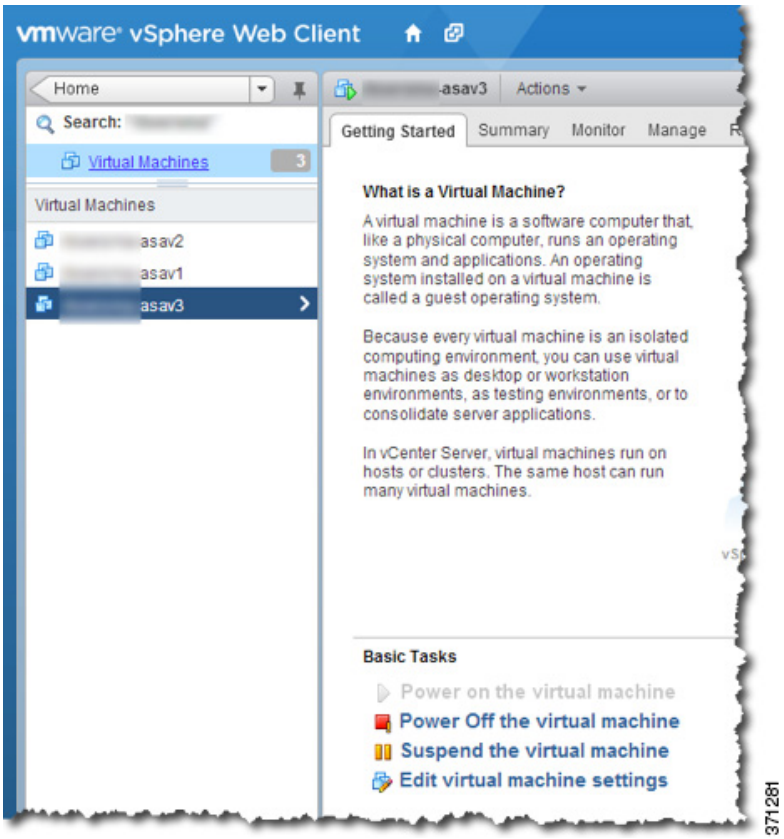
     フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。GigabitEthernet 0/8 がフェールオーバー リンクとして事前設定されています。同じネットワーク上のリンクに対するアクティブな IP アドレスとスタンバイの IP アドレスを入力します。
9. ウィザードが完了すると、vSphere Web Client は VM を処理します。[Recent Tasks] ペインの [Global Information] 領域で [Initialize OVF deployment] ステータスを確認できます。



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



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



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

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

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

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

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

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

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

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

はじめる前に

- ASAv を導入する前に、vSphere（管理用）に少なくとも 1 つのネットワークを設定しておく必要があります。
- ASAv ソフトウェアの開梱と VMware 対応第 0 日用コンフィギュレーション ファイルの作成（10 ページ）の手順に従って、第 0 日用構成を作成します。

手順

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

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

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

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

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

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

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

   これで、ASAv は完全に動作可能な状態です。

OVF ツールおよび第 0 日用構成を使用した ASAv の導入

はじめる前に

- OVF ツールを使用して ASAv を導入する場合は、day0.iso ファイルが必要です。ZIP ファイルで提供されるデフォルトの空の day0.iso ファイルを使用するか、または、生成しカスタマイズした第 0 日用コンフィギュレーション ファイルを使用できます。第 0 日用コンフィギュレーション ファイルの作成方法については、ASAv ソフトウェアの開梱と VMware 対応第 0 日用コンフィギュレーション ファイルの作成（10 ページ）を参照してください。
- OVF ツールが Linux または Windows PC にインストールされ、ターゲット ESXi または vCenter サーバに接続できることを確認します。

手順

1. OVF ツールがインストールされていることを確認します。

   ```
   linuxprompt# which ovftool
   ```

2. 必要な導入オプションを指定した .cmd ファイルを作成します。

   例：

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

3. cmd ファイルを実行します。

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

   ASAv に電源を投入し、2 回目の起動を待機します。

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

   これで、ASAv は完全に動作可能な状態です。

ASAv コンソールへのアクセス

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

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

VMware vSphere コンソールの使用

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

はじめる前に

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

手順

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

   ASAv がまだ起動中の場合は、起動メッセージが表示されます。

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

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

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

   次のプロンプトが表示されます。

   ```
   ciscoasa>
   ```

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

   ```
   ciscoasa> enable
   ```

   次のプロンプトが表示されます。

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

   プロンプトが次のように変化します。

   ```
   ciscoasa#
   ```

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

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

   ```
   ciscoasa# configure terminal
   ```

   プロンプトが次のように変化します。

   ```
   ciscoasa(config)#
   ```

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

ネットワーク シリアル コンソール ポートの設定

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

手順

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

   disk0:/use_ttyS0

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

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

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

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

vCPU またはスループット ライセンスのアップグレード

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

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

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

手順

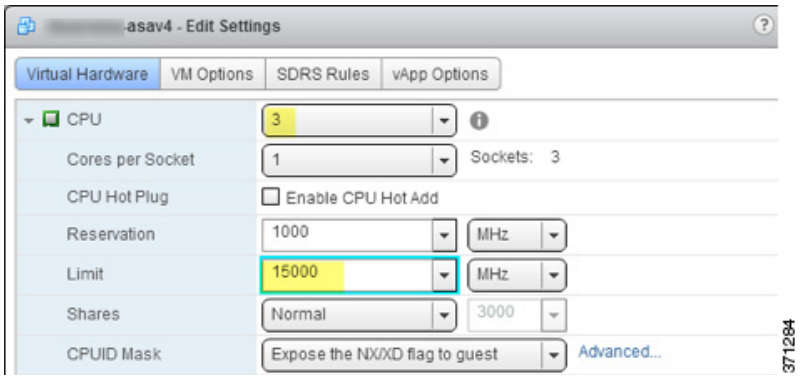
1. 新しいライセンスを要求します。
2. 新しいライセンスを適用します。フェールオーバー ペアの場合、両方の装置に新しいライセンスを適用します。
3. フェールオーバーを使用するかどうかに応じて、次のいずれかを実行します。
   - フェールオーバーあり：vSphere Web Client で、*スタンバイ* ASAv の電源を切断します。たとえば、ASAv をクリックしてから [Power Off the virtual machine] をクリックするか、または ASAv を右クリックして [Shut Down Guest OS] を選択します。
   - フェールオーバーなし：vSphere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

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

   [Edit Settings] ダイアログボックスが表示されます。

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

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



7. [Memory] には、新しい RAM の値を入力します。

8. [OK] をクリックします。

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

10. フェールオーバー ペアの場合:

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

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

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

       - CLI:ciscoasa# **failover active**

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

関連項目

- ASAv のライセンス(5 ページ)

KVM を使用した ASAv の導入

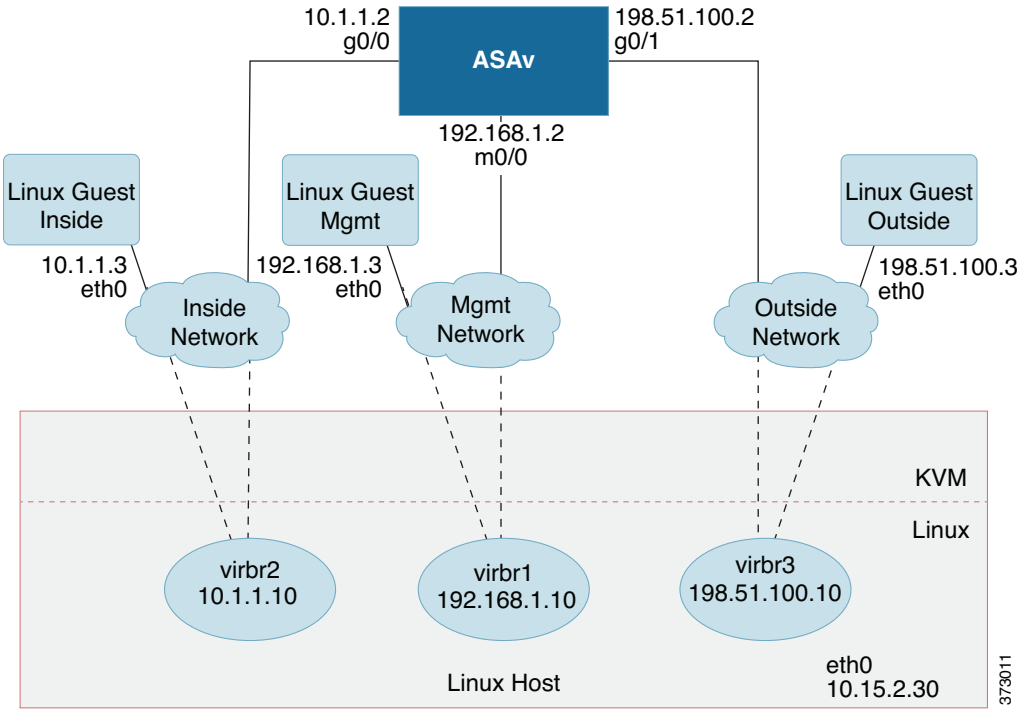
カーネルベースの仮想マシン（KVM）を使用して ASAv を導入することができます。

- KVM を使用した ASAv の導入について（21 ページ）
- ASAv と KVM の前提条件（22 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（22 ページ）
- 仮想ブリッジ XML ファイルの準備（24 ページ）
- ASAv の起動（25 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（26 ページ）

KVM を使用した ASAv の導入について

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

図 1　KVM を使用した ASAv の導入例



ASAv と KVM の前提条件

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

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

第 0 日のコンフィギュレーション ファイルの準備

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

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

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

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

手順

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

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

   例:

   ```
   ASA Version 9.5.1
   !
   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
   ```

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

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

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

   - 管理インターフェイスの IP アドレス
   - （任意）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
   - 要求する ASAv ライセンスを指定するための Smart Licensing の設定
   - （任意）CSSM での ASAv の検索を容易にするための一意のホスト名

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

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

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

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

仮想ブリッジ XML ファイルの準備

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

注: この手順では、KVM から外部への接続は確立されません。

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

手順

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

virbr1.xml：

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

virbr2.xml：

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

virbr3.xml：

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

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

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

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

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

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

4. 仮想ネットワークが作成されたことを確認します。

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

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

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

ASAv の起動

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

手順

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

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

   注: *watchdog* 要素は、KVM ゲストの仮想ハードウェア ウォッチドッグ デバイスです。ASAv が何らかの理由で応答しなくなると、ウォッチドッグは KVM ゲストの再起動を開始できます。

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=asav \
   --cpu host \
   --arch=x86_64 \
   --machine=pc-1.0 \
   --vcpus=1 \
   --ram=2048 \
   --os-type=linux \
   --os-variant=generic26 \
```

```
--virt-type=kvm \
--import \
 --watchdog i6300esb,action=reset
--disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=ide,cache=none \
--disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
--console pty,target_type=virtio \
--serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

2. virt_install スクリプトを実行します。

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

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

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

ホットプラグ インターフェイス プロビジョニング

ASAv を停止して再起動しなくても、インターフェイスを動的に追加および削除できます。ASAv 仮想マシンに新しいインターフェイスを追加したときに、ASAv はそれ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と、ASAv は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。

ホットプラグ インターフェイス プロビジョニングのためのガイドライン

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、それ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 に新しく追加され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 ユニットに同期されます。
  - 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 リンクを解除するには、次の手順に従います。
  - 最初にアクティブ ASAv の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 ASAv からフェールオーバー インターフェイスを削除し、その後すぐ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。

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。

手順

1. virsh コマンド ラインのセッションを開きます。

```
[root@asav-kvmterm ~]# virsh
Welcome to virsh, the virtualization interactive terminal.

Type:    'help' for help with commands
         'quit' to quit
```

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。

```
virsh # attach-interface domain type source model mac live
```

例：

```
virsh # attach-interface --domain asav-network --type bridge --source br_hpi --model virtio --mac
52:55:04:4b:59:2f --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：トラフィックを送受信するためのインターフェイスを設定して有効にするには、ASAv のインターフェイス コンフィギュレーション モードを使用します。詳細については、「Navigating the Cisco ASA Series Documentation」を参照してください。

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。

```
virsh # detach-interface domain type mac live
```

例：

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

ホットプラグ インターフェイス プロビジョニング

AWS クラウドへの ASAv の導入

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

- AWS クラウドへの ASAv の導入について（29 ページ）
- ASAv と AWS の前提条件（29 ページ）
- ASAv および AWS のガイドラインと制限事項（30 ページ）
- 設定の移行と SSH 認証（30 ページ）
- AWS 上の ASAv のネットワーク トポロジの例（31 ページ）
- AWS への ASAv の導入（32 ページ）

AWS クラウドへの ASAv の導入について

注：ASAv5 は AWS ではサポートされていません。

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

- c3.large と c4.large：2 つの vCPU、3.75 GB、3 つのインターフェイス、1 つの管理インターフェイス

  注：ASAv10 と ASAv30 はどちらも c3.large インスタンス上でサポートされます。ただし、リソースがプロビジョニング中のため、c3.large 上の ASAv30 の導入はお勧めできません。

- c3.xlarge と c4.xlarge：4 つの vCPU、7.5 GB、3 つのインターフェイス、1 つの管理インターフェイス

  注：ASAv30 のみが c3.xlarge でサポートされます。

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

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

注：AMI イメージは AWS 環境の外部ではダウンロードできません。

ASAv と AWS の前提条件

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

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

ASAv および AWS のガイドラインと制限事項

サポートされる機能

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

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）
- IPv6
- VLAN
- 100Mbps スループットの ASAv5
- 無差別モード（スニファなし、またはトランスペアレント モードのファイアウォールのサポート）
- マルチ コンテキスト モード
- クラスタ
- ASAv のネイティブ HA
- EtherChannel は、ダイレクト物理インターフェイスのみでサポートされる
- VM のインポート/エクスポート
- Amazon Cloudwatch
- ハイパーバイザに非依存のパッケージ
- VMware ESXi

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 サービス（AWS）の ASAv のデフォルトであるため、AWS のユーザはこの問題を確認する必要があります。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。

ユーザ名が「admin」の場合の設定例を示します。

```
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、パスワードが入力できないのではなく、どのようなパスワードでも入力できることを意味します。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。

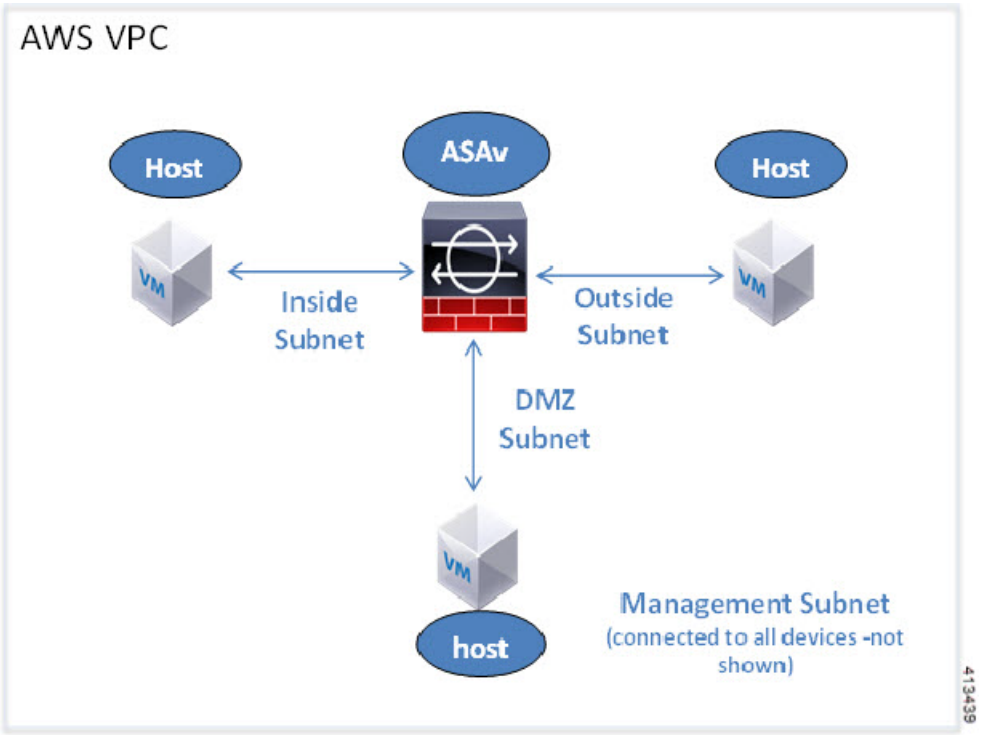
アップグレード後は、**username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザがパスワードを入力できなくするよう指定できるようになります。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

AWS 上の ASAv のネットワーク トポロジの例

図 1（31 ページ）は、ASAv 用に AWS 内で設定された 4 つのサブネット（管理、内部、外部、および DMZ）を備えるルーテッド ファイアウォール モードの ASAv の推奨トポロジを示しています。

図 1　AWS への ASAv の導入の例



AWS への ASAv の導入

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

手順

1. aws.amazon.com にログインし、地域を選択します。

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

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

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

3. [My Account] > [AWS Management Console] > [EC2] をクリックし、さらに、[Create an Instance] をクリックします。

   - AMI（たとえば、Ubuntu Server 14.04 LTS）を選択します。

     イメージ配信通知で識別された AMI を使用します。

   - ASAv（たとえば、c3.large）によってサポートされるインスタンス タイプを選択します。
   - インスタンスを設定します（CPU とメモリは固定です）。
   - [Advanced Details] で、必要に応じて第 0 日用構成を追加します。第 0 日構成に詳細情報を設定する方法の手順については、第 0 日のコンフィギュレーション ファイルの準備（22 ページ）を参照してください。

     第 0 日用構成の例

```
! ASA 9.5.1.200
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 30
username admin nopassword privilege 15
username admin attributes
service-type admin
! required config end
! example dns configuration
dns domain-lookup management
DNS server-group DefaultDNS
! where this address is the .2 on your public subnet
name-server 172.19.0.2
! example ntp configuration
name 129.6.15.28 time-a.nist.gov
name 129.6.15.29 time-b.nist.gov
```

```
name 129.6.15.30 time-c.nist.gov
ntp server time-c.nist.gov
ntp server time-b.nist.gov
ntp server time-a.nist.gov
```

- ストレージ(デフォルトを受け入れます)。
- タグ インスタンス:デバイスを分類するため、多数のタグを作成できます。タグを容易に見つけるために使用できる名前を付けます。
- セキュリティ グループ:セキュリティ グループを作成して名前を付けます。セキュリティ グループは、着信および発信トラフィックを制御するためのインスタンスの仮想ファイアウォールです。

  デフォルトでは、セキュリティ グループはすべてのアドレスに対して開かれています。ASAv にアクセスするために使用するアドレスからの SSH 接続だけを許可するように、ルールを変更します。

- 設定を確認し、[Launch] をクリックします。

4. キー ペアを作成します。

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

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

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

AWS への ASAv の導入

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 の導入について（35 ページ）
- ASAv および Azure の前提条件およびシステム要件（35 ページ）
- ASAv および Azure のガイドラインと制限事項（36 ページ）
- Azure 上の ASAv のネットワーク トポロジの例（37 ページ）
- 導入時に作成されるリソース（38 ページ）
- Azure ルーティング（38 ページ）
- 仮想ネットワーク内の VM のルーティング設定（39 ページ）
- IP アドレス（39 ページ）
- DNS（39 ページ）
- Microsoft Azure への ASAv の導入（40 ページ）

Microsoft Azure クラウドへの ASAv の導入について

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 上の ASAv は、4 つの vCPU、14 GB、4 つのインターフェイスをサポートする Standard D3 の 1 つのインスタンス タイプをサポートします。

Microsoft Azure に ASAv を導入するには、2 つの方法（Azure Resource Manager を使用したスタンドアロン ファイア ウォールとして、または、Azure Security Center を使用した統合パートナー ソリューションとして）があります。Microsoft Azure への ASAv の導入（40 ページ）を参照してください。

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 にライセンスを付与します。

  ASAv にライセンスを付与するまでは、100 の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「Smart Software Licensing for the ASAv（ASAv の Smart Software Licensing）」を参照してください。

  注：Azure に展開する場合、ASAv にはデフォルトで ASAv30 の権限が付与されています。ASAv5 および ASAv10 の権限付与の使用が許可されています。ただし、ASAv5 または ASAv10 の権限付与を使用できるように、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。

  - 管理インターフェイス

    注:エッジ ファイアウォール構成の場合、管理インターフェイスは、「外部」インターフェイスとしても使用されます。

    注:Azure では、最初に定義されたインターフェイス(常に、管理インターフェイス)が、それに Azure パブリック IP アドレスを関連付けることができる唯一のインターフェイスです。このため、Azure 内の ASAv は管理インターフェイス上でのデータ トラフィックの通過を許可します。そのため、管理インターフェイスの初期設定には、**管理専用**の設定は含まれていません。

  - 内部および外部インターフェイス
  - 追加のサブネット(DMZ または選択したネットワーク)
- 通信パス:
  - 管理インターフェイス:SSH アクセスと、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 のシステム要件については、「Cisco ASA Compatibility」を参照してください。

ASAv および Azure のガイドラインと制限事項

サポートされる機能

- Microsoft Azure クラウドからの導入
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザ導入

  注:Azure は設定可能な L2 vSwitch 機能は提供していません。
- 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。

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)
- IPv6
- ユーザ 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
- インターフェイスのパブリック IP アドレス

  Management 0/0 インターフェイスのみが、それに関連付けられたパブリック IP アドレスを保持できます。
- 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 ポリシーによって、インターフェイスの無差別モードでの動作は許可されていないため、ASAv のトランスペアレント ファイアウォール モードでの動作は阻止されます。

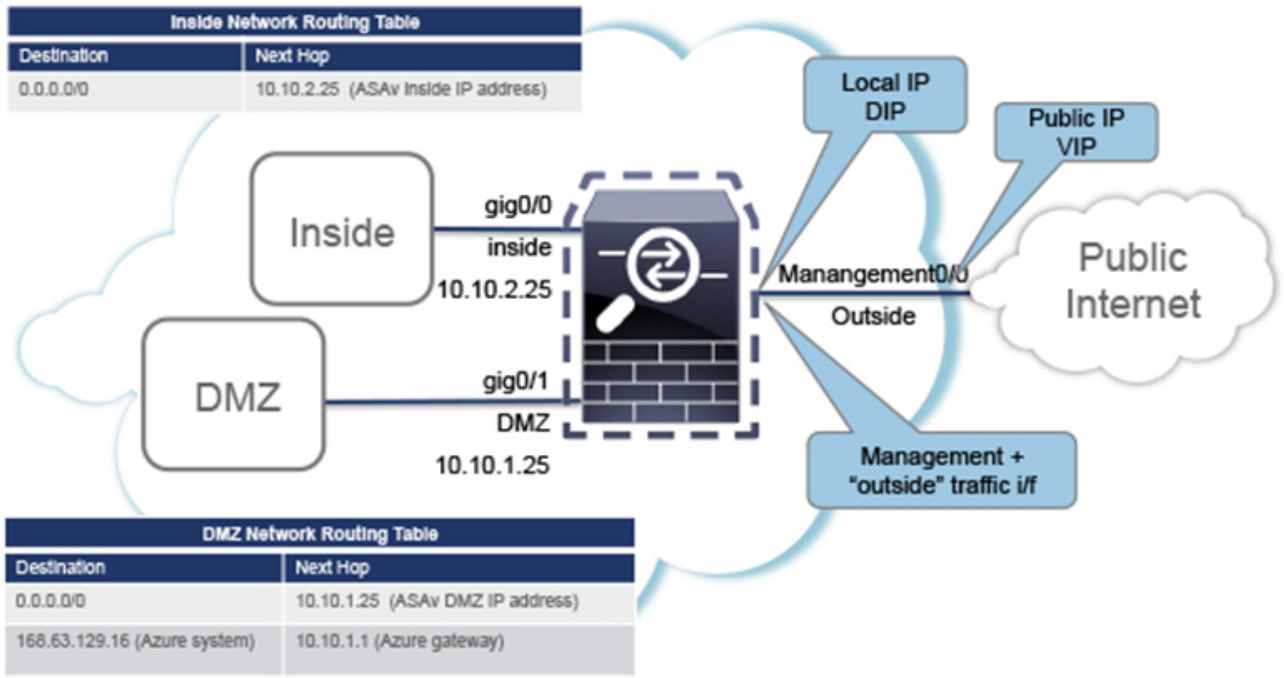
- マルチ コンテキスト モード
- クラスタ
- ASAv のネイティブ HA
- VM のインポート/エクスポート
- デフォルトでは、Azureクラウド内で稼働する ASAv の FIPS モードは無効になっています。

  注意：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、それ以降 ASAv に SSH 接続できなくなります。そのため、グループの変更が、最初に ASAv を管理する唯一の方法となります。

Azure 上の ASAv のネットワーク トポロジの例

図 1（37 ページ）は、Azure 内に設定された 3 つのサブネット（管理、内部、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。4 番目の必須インターフェイス（外部）は示されていません。

図 1　Azure への ASAv の導入の例



導入時に作成されるリソース

Azure に ASAv を導入すると、次のリソースが作成されます。

- ASAv 仮想マシン（VM）
- 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 アカウントが使用するリソース グループと同じである必要があります。

- 4 枚の NIC（名前は、*vm name*-Nic0、*vm name*-Nic1、*vm name*-Nic2、*vm name*-Nic3）

  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。

- セキュリティ グループ（名前は、*vm name*-SSH-SecurityGroup）

  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（導入時に選択した値に従って命名）

  パブリック IP アドレスは、Management 0/0 にマッピングされる VM の Nic0 に関連付けられます。Azure では、パブリック IP アドレスを最初の NIC のみに関連付けることができます。

  注: パブリック IP アドレスを選択する必要があります（新規または既存）。[None] オプションはサポートされていません。

- 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）

  テーブル（名前は、*subnet name*-ASAv-RouteTable）

  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 テーブルとユーザ定義のルーティング テーブルの組み合わせです。

注: 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。これは、サブネットからのすべてのトラフィックを ASAv を介して送信します。その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生じる場合があります（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、トラフィックが ASAv をバイパスしてしまいます。

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。

IP アドレス

次の情報は Azure の IP アドレスに適用されます。

- ASAv 上の最初の NIC（Management 0/0 にマッピングされる）には、アタッチ先のサブネット内のプライベート IP アドレスが付与されます。

  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。

- VM の最初の NIC のみにパブリック IP アドレスをアタッチできます。
- 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、それらは保持されます。
- 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。
- ASAv インターフェイスは、DHCP を使用して、自身の IP アドレスを設定します。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 ASAv インターフェイスに割り当てられるように確保します。

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

次の 2 つの方法のどちらかで ASAv を Microsoft Azure に導入できます。

- ASAv を Azure Resource Manager を使用したスタンドアロン ファイアウォールとして導入します。Azure Resource Manager からの ASAv の導入（40 ページ）を参照してください。
- ASAv を Azure Security Center を使用した Azure 内の統合パートナー ソリューションとして導入します。セキュリティを重視するお客様には、ASAv を Azure ワークロードを保護するためのファイアウォール オプションとして提案します。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されます。Azure Security Center からの ASAv の導入（41 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 のセットアップ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。

手順

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。

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。
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。

      注：既存の名前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。
4. ASAv 設定を構成します。
   a. 仮想マシンのサイズを選択します。

      注：ASAv で使用できる唯一のサイズが Standard D3 です。

b. ストレージ アカウントを選択します。

注: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 アカウントを作成することができます。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。

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。

注: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。

注: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。

5. 構成サマリを確認し、[OK] をクリックします。

6. 利用条件を確認し、[Create] をクリックします。

次の作業

- 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 の開始(61 ページ)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。推奨事項のリストが、必要なコントロールを設定するためのプロセスを誘導します。これには、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として、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 イベントとヘルス イベントをモニタできます。次のリストは、Security Center から ASAv を導入するための手順概要です。詳細については、『Azure Security Center』を参照してください。

手順

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。

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。

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

4. [Security policy] ブレードで、[Prevention policy] を選択します。
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。これにより、ASAv が Security Center 内の推奨ソリューションであることが確認されます。
   b. 必要に応じて、他の推奨事項を設定します。
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。
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。
8. [Create New] または [Use existing solution] を選択してから、導入する ASAv をクリックします。
9. 基本的な設定を行います。
   c. 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。

      注:既存の名前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。
   d. ユーザ名を入力します。
   e. 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。
   f. サブスクリプション タイプを選択します。
   g. 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。
   h. 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。
   i. [OK] をクリックします。
10. ASAv 設定を構成します。
   a. 仮想マシンのサイズを選択します。

      注:ASAv で使用できる唯一のサイズが Standard D3 です。
   b. ストレージ アカウントを選択します。

      注: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 アカウントを作成することができます。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。

      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。

      注: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。

注：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。

11. 構成サマリを確認し、[OK] をクリックします。

12. 利用条件を確認し、[Create] をクリックします。

次の作業

- 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 の開始（61 ページ）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。

Microsoft Azure への ASAv の導入

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。

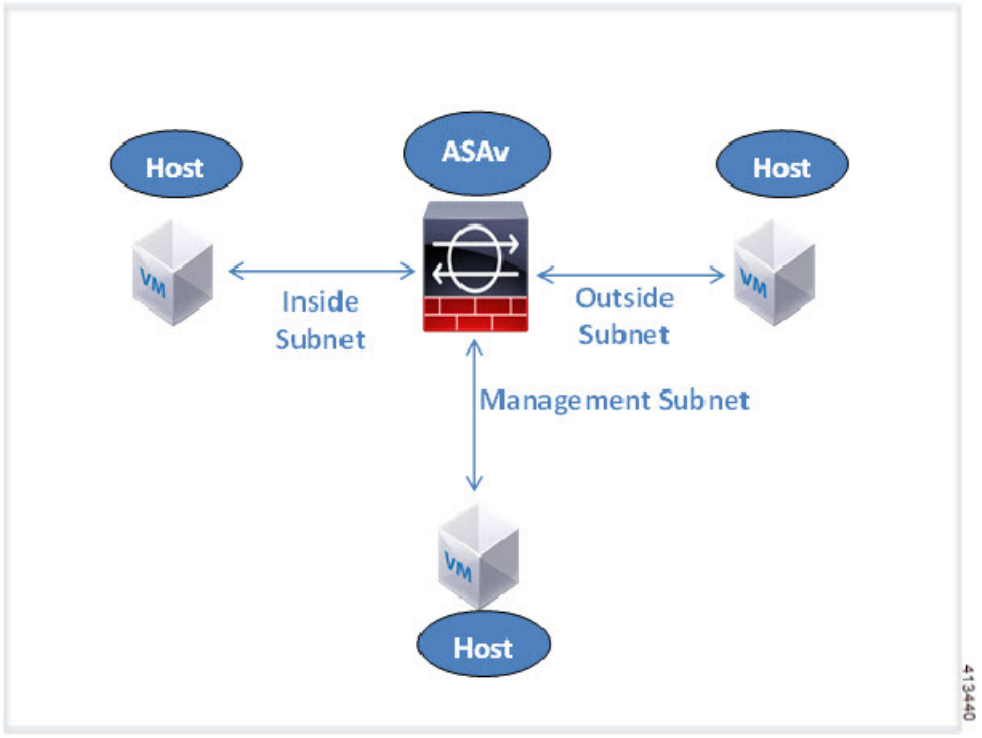
- Hyper-V を使用した ASAv の導入について（45 ページ）
- ASAv および Hyper-V のガイドラインと制限事項（46 ページ）
- ASAv と Hyper-V の前提条件（47 ページ）
- 第 0 日のコンフィギュレーション ファイルの準備（47 ページ）
- コマンドラインを使用した Hyper-V への ASAv のインストール（50 ページ）
- Hyper-V マネージャを使用した Hyper-V への ASAv のインストール（51 ページ）
- Hyper-V マネージャからのネットワーク アダプタの追加（57 ページ）
- ネットワーク アダプタの名前の変更（59 ページ）
- MAC アドレス スプーフィングの設定（60 ページ）
- SSH の設定（60 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 の CLI コマンドを使用してインストールする手順については、コマンドラインを使用した Hyper-V への ASAv のインストール（50 ページ）を参照してください。Hyper-V マネージャを使用してインストールする手順については、Hyper-V マネージャを使用した Hyper-V への ASAv のインストール（51 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 をセットアップするための情報については、SSH の設定（60 ページ）を参照してください。

図 1（46 ページ）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、管理、内部、および外部の 3 つのサブネットがあります。

図 1　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
  - Cisco UCS C シリーズ サーバ
  - 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の大多数で稼働します。
- ファイル形式

  Hyper-V への ASAv の初期導入の場合は、VHDX 形式をサポートしています。
- 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（47 ページ）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（47 ページ）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（60 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（47 ページ）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 Compatibility」を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

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

注：ASAv の初回起動前に、第 0 日用コンフィギュレーション 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 日用コンフィギュレーション ファイルを使用することにした場合は、**write erase** コマンドを実行し、第 0 日用コンフィギュレーション ファイルを適用してから、ASAv を起動する必要があります。

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

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

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

手順

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

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

   例

   ```
   ASA Version 9.5.1
   !
   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
   ```

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

3. （任意）ダウンロードしたファイルから 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。

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

   - 管理インターフェイスの IP アドレス
   - （任意）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
   - 要求する ASAv ライセンスを指定するための Smart Licensing の設定
   - （任意）CSSM での ASAv の検索を容易にするための一意のホスト名

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

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

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

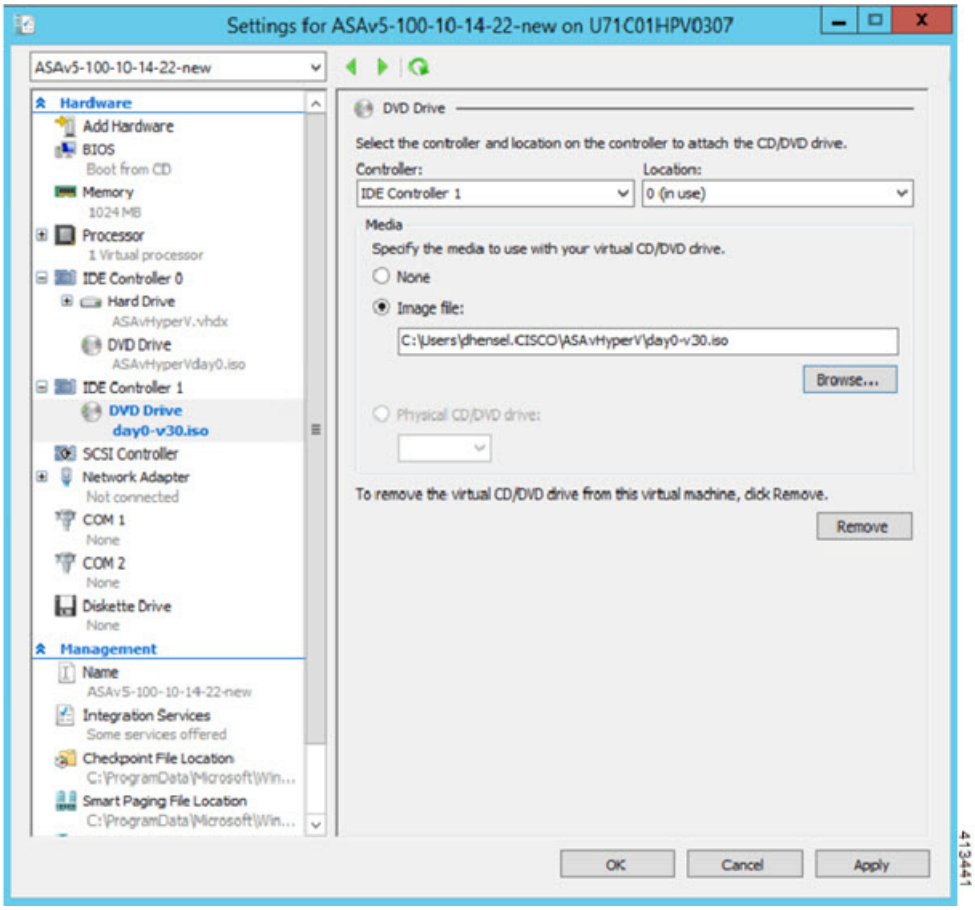
6. ステップ 1から 5 を繰り返し、導入する ASAv ごとに、適切な IP アドレスを含むデフォルトのコンフィギュレーション ファイルを作成します。

Hyper-V マネージャを使用した ASAv と第 0 日用コンフィギュレーション ファイルの導入

第 0 日用コンフィギュレーション ファイルをセットアップした後（第 0 日のコンフィギュレーション ファイルの準備（47 ページ））、Hyper-V マネージャを使用してそれを導入できます。

手順

1. [Server Manager] > [Tools] > [Hyper-V Manager] に移動します。
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。



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 日用コンフィギュレーション 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。

手順

1. Windows Powershell を開きます。
2. ASAv を導入します。

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

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。

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

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。

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

5. （任意）ネットワークで必要な場合は、VLAN ID を変更します。

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

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。

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

7. 内部インターフェイスを追加します。

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

8. 外部インターフェイスを追加します。

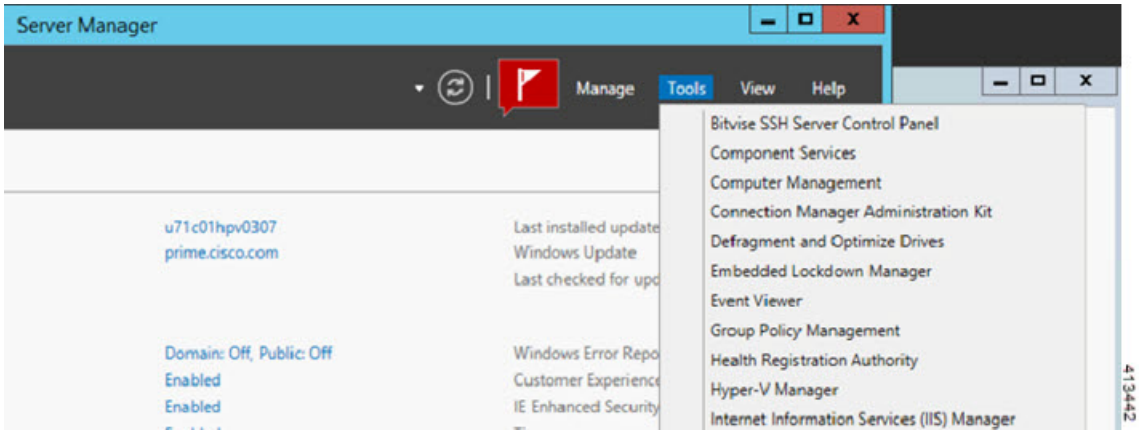
```
Add-VMNetworkAdapter -VMName $fullVMName -name "outside" -SwitchName 1151mgmtswitch
Set-VMNetworkAdapterVlan -VMName $fullVMName -VlanId 1553 -Access -VMNetworkAdapterName "outside"
```

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

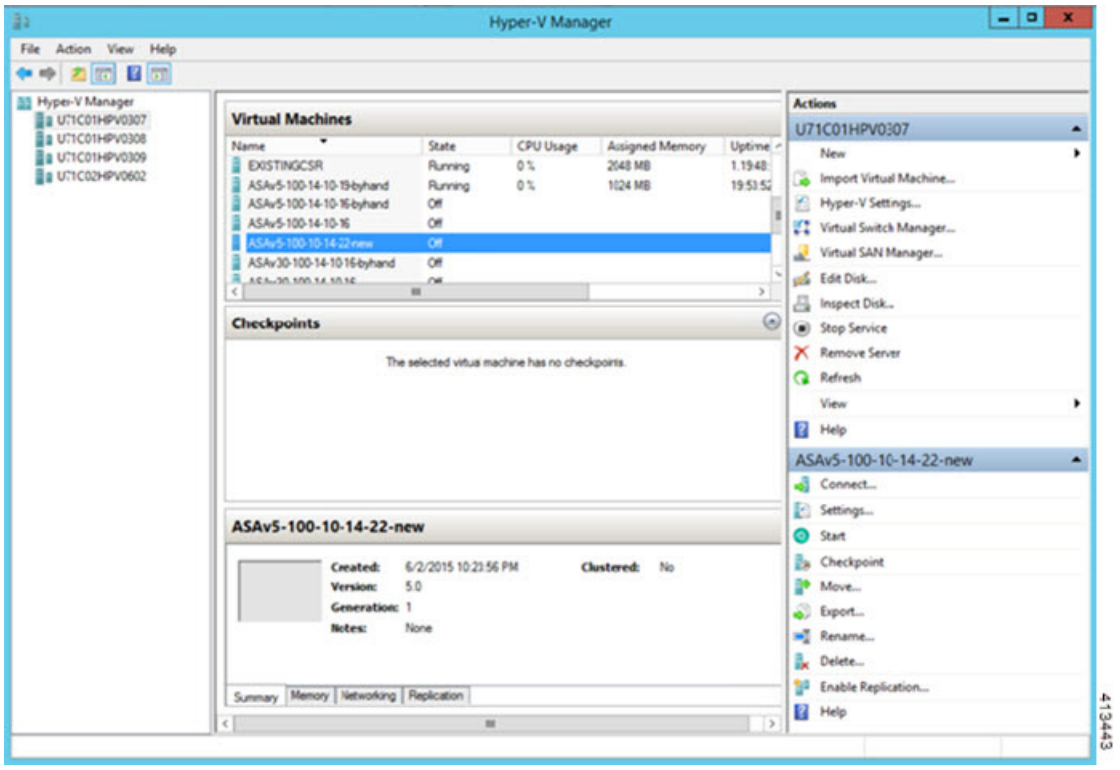
Hyper-V マネージャを使用して、Hyper-V に ASAv をインストールできます。

手順

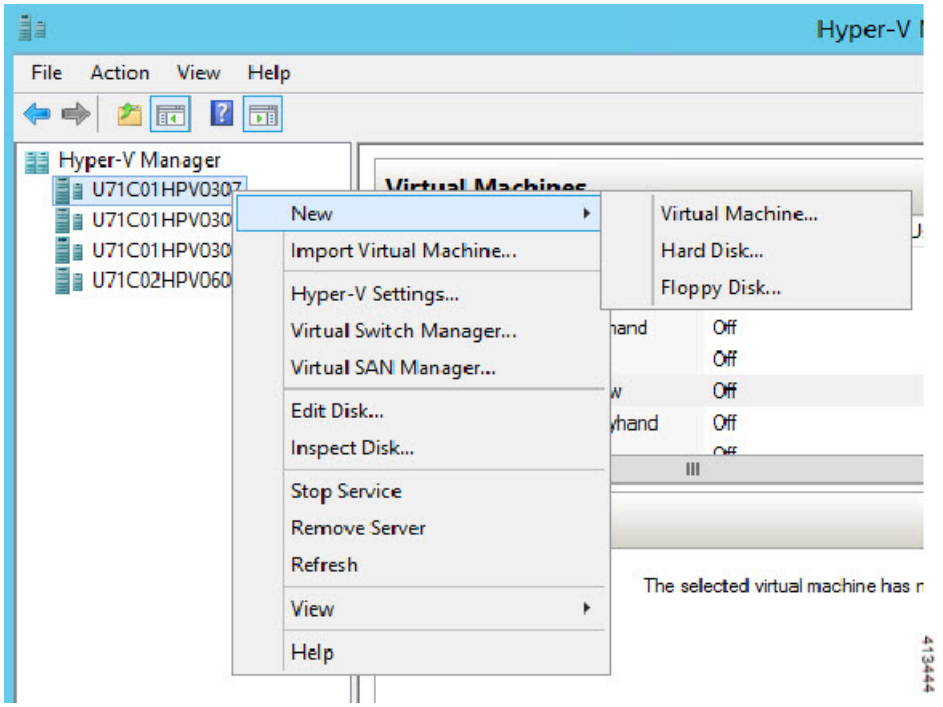
1. [Server Manager] > [Tools] > [Hyper-V Manager] に移動します。



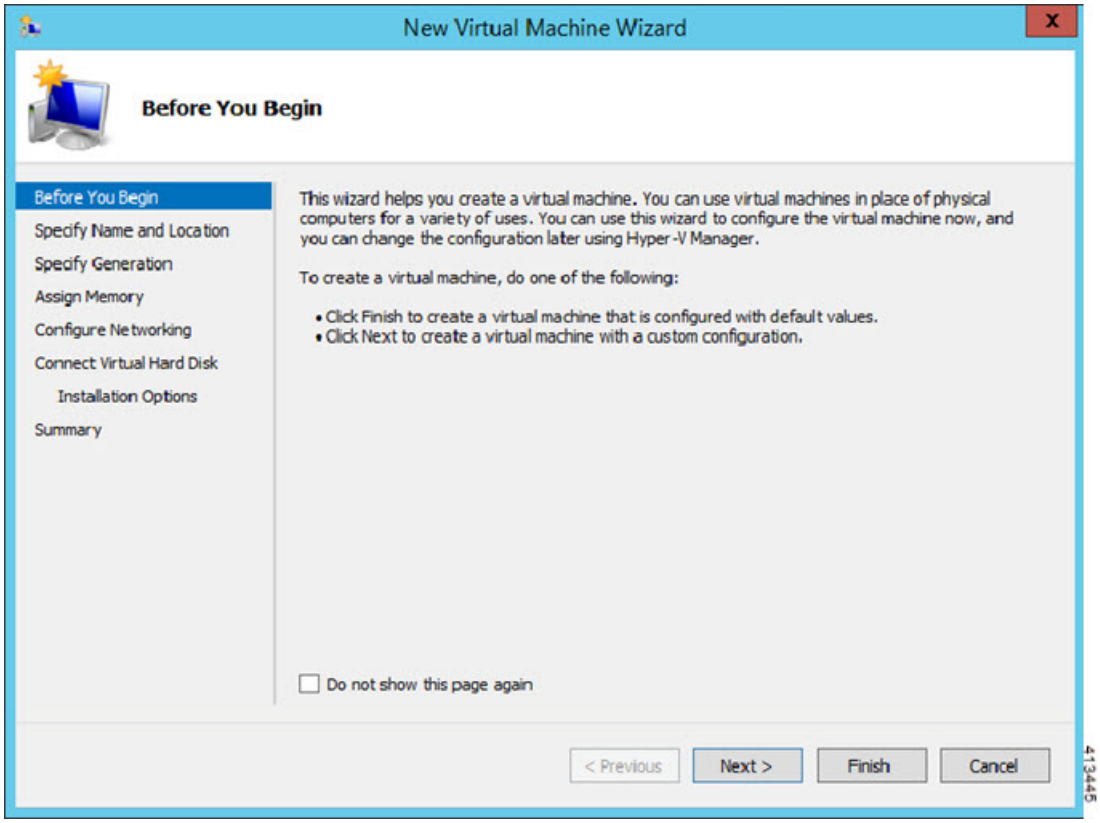
2. Hyper-V マネージャが表示されます。



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。



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



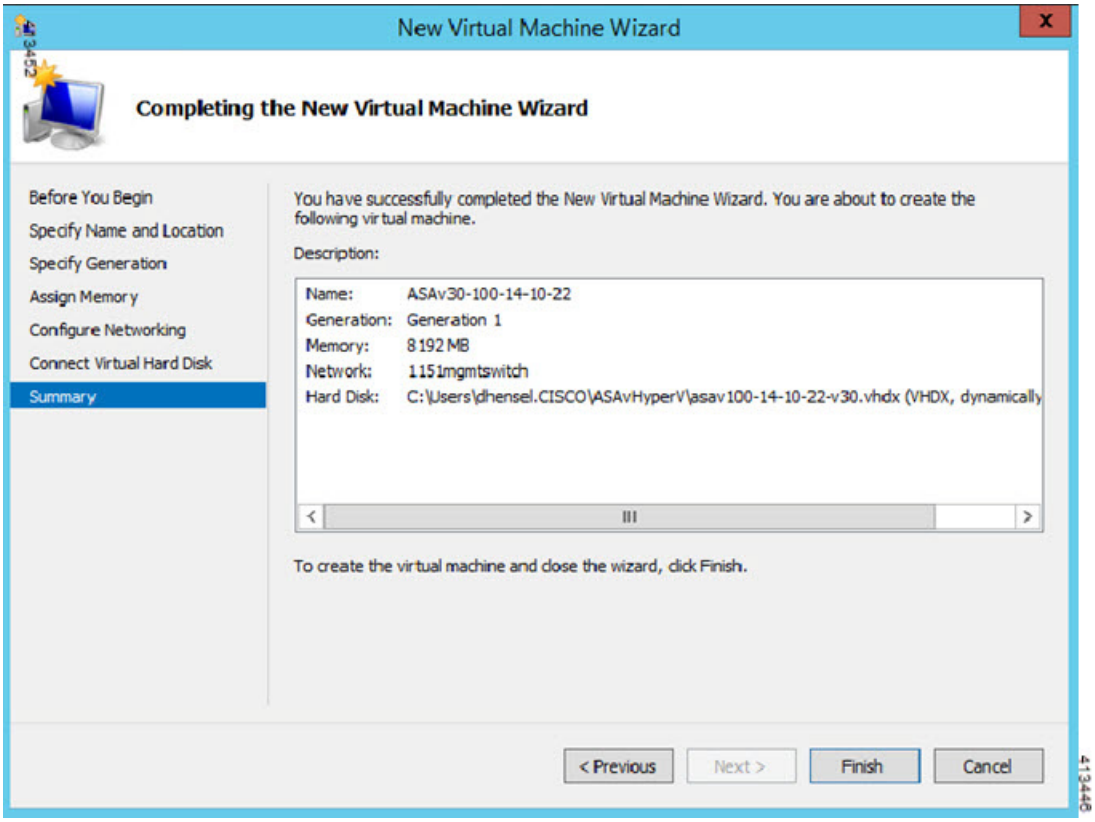
5. ウィザードを通じて作業し、次の情報を指定します。

   - 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 [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

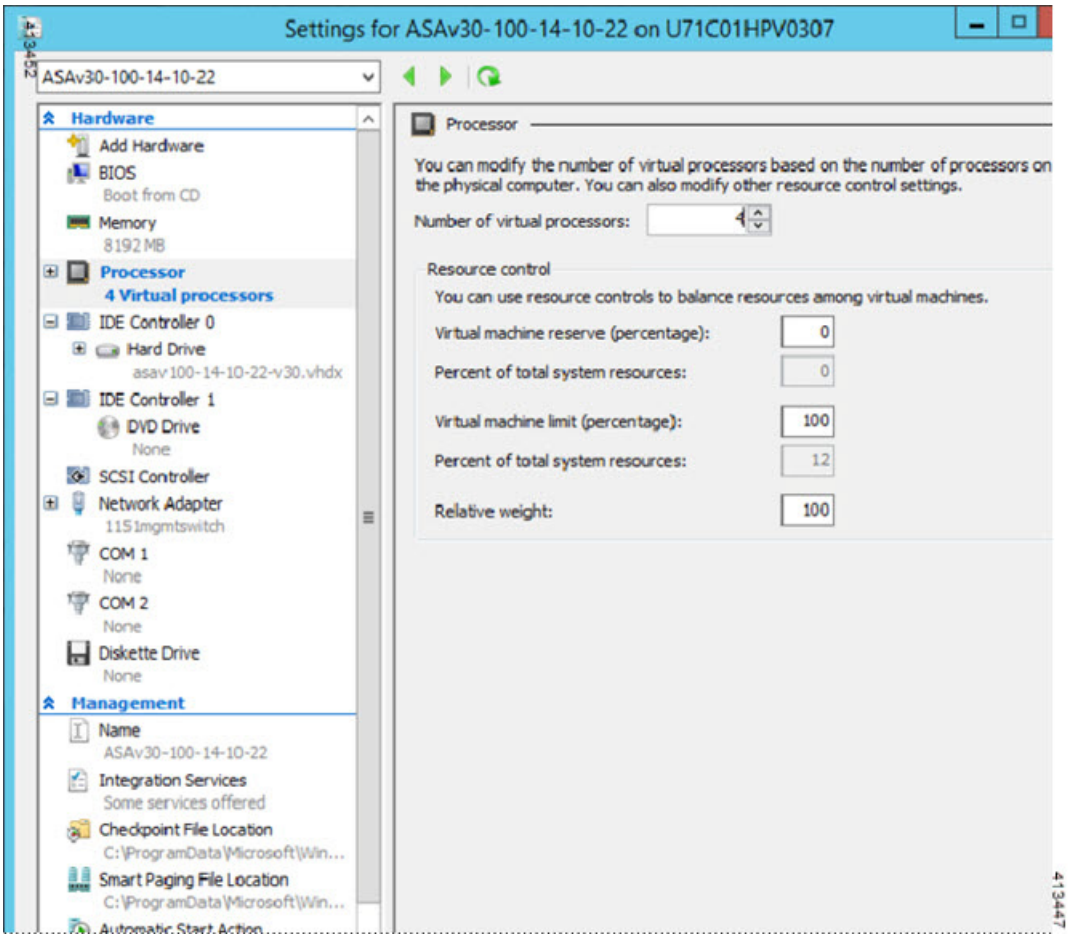
     [Use an existing virtual hard disk] を選択し、VHDX ファイルの場所を参照します。

6. [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。

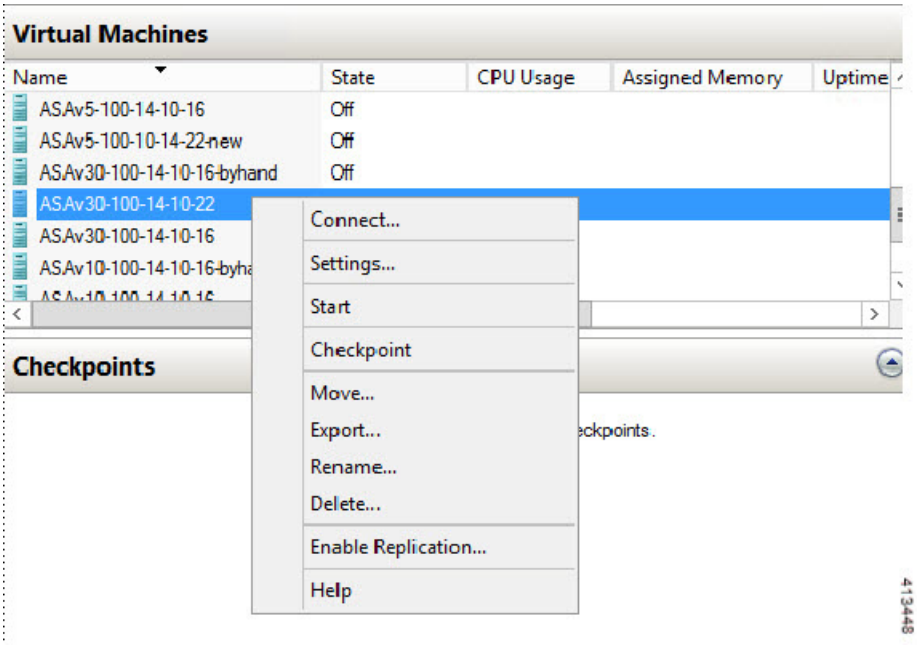


7. ASAv に 4 つの vCPU がある場合は、ASAv を起動する前に、vCPU 値を変更する必要があります。Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Processor] をクリックし、[Processor] ペインを表示します。[Number of virtual processors] を 4 に変更します。

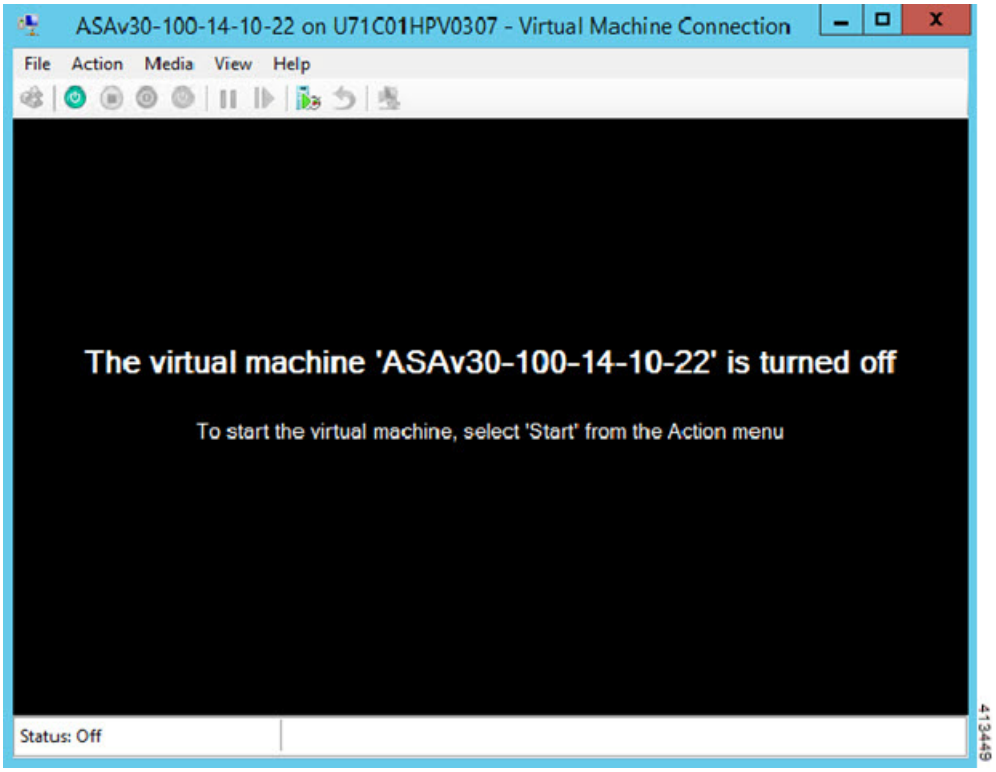
   ASAv5 と ASAv10 には 1 つの vCPU があり、ASAv30 には 4 つの vCPU があります。デフォルトは 1 です。



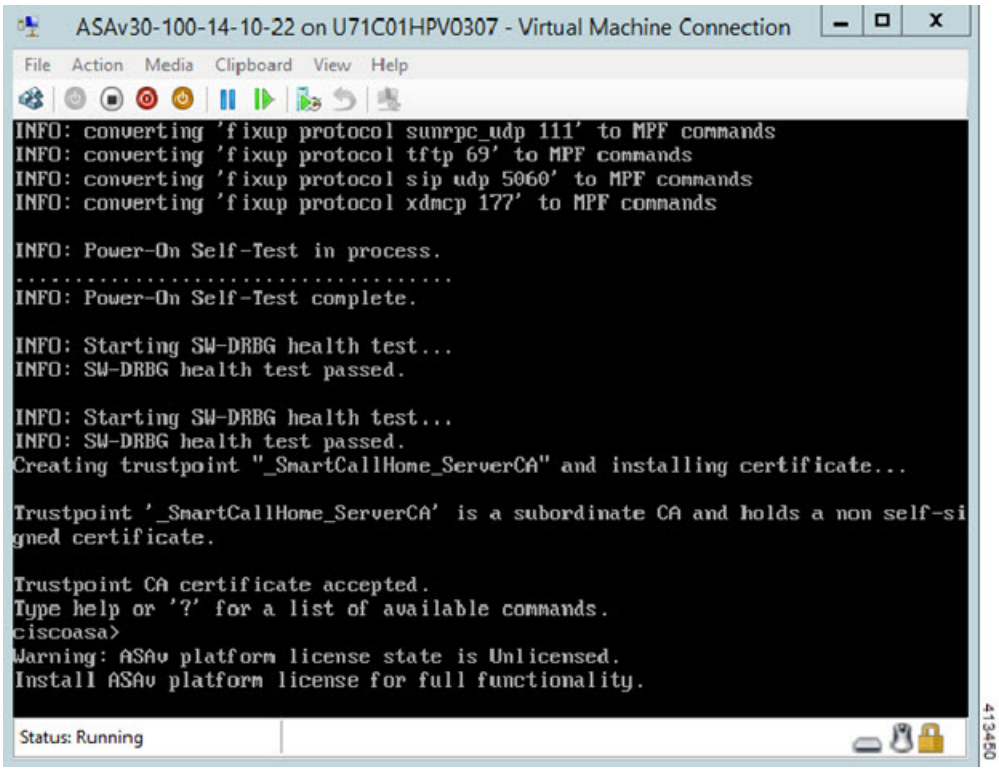
8. [Virtual Machines] メニューで、リスト内の ASAv の名前を右クリックし、[Connect] をクリックして、ASAv に接続します。コンソールが開き、停止されている ASAv が示されます。



9. [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。



10. ASAv の起動の進行状況がコンソールに表示されます。



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。

はじめる前に

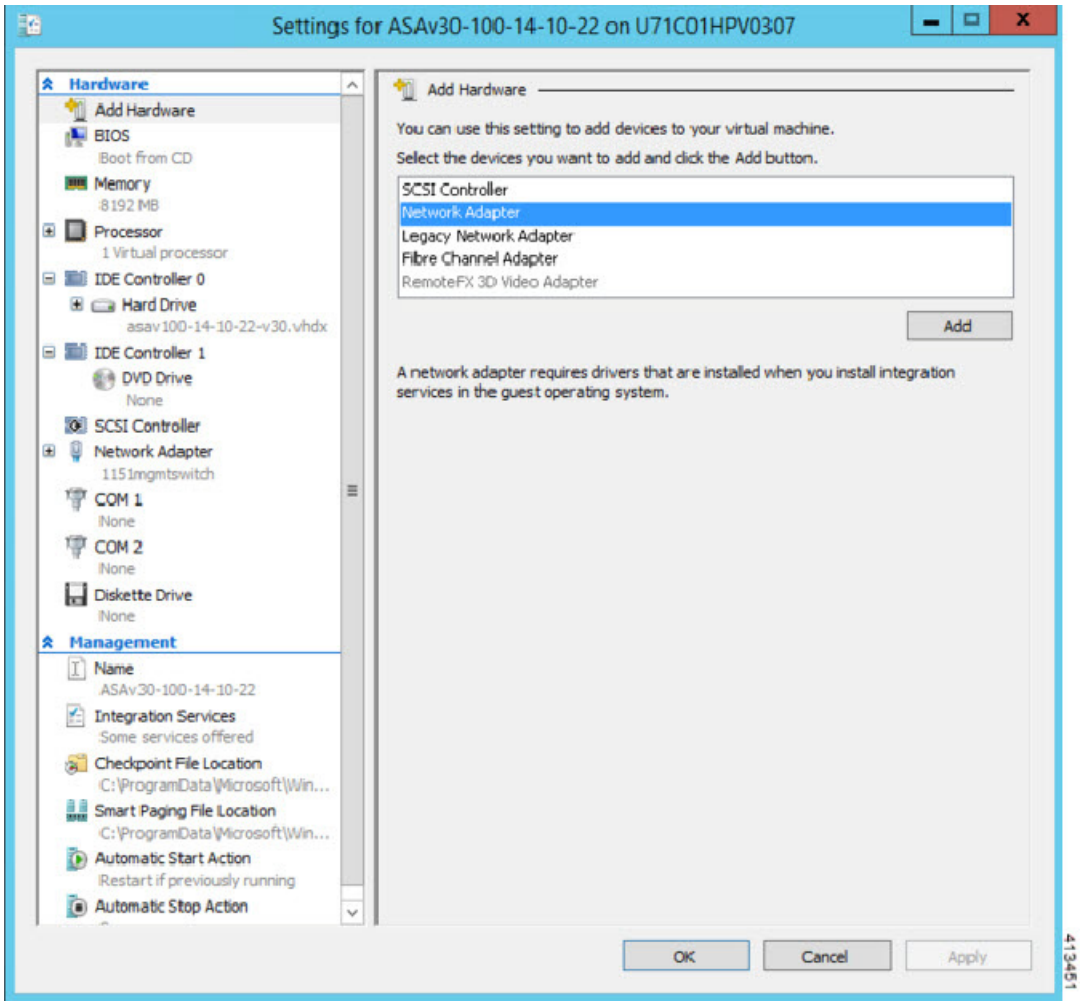
- ASAv はオフ状態になっている必要があります。

手順

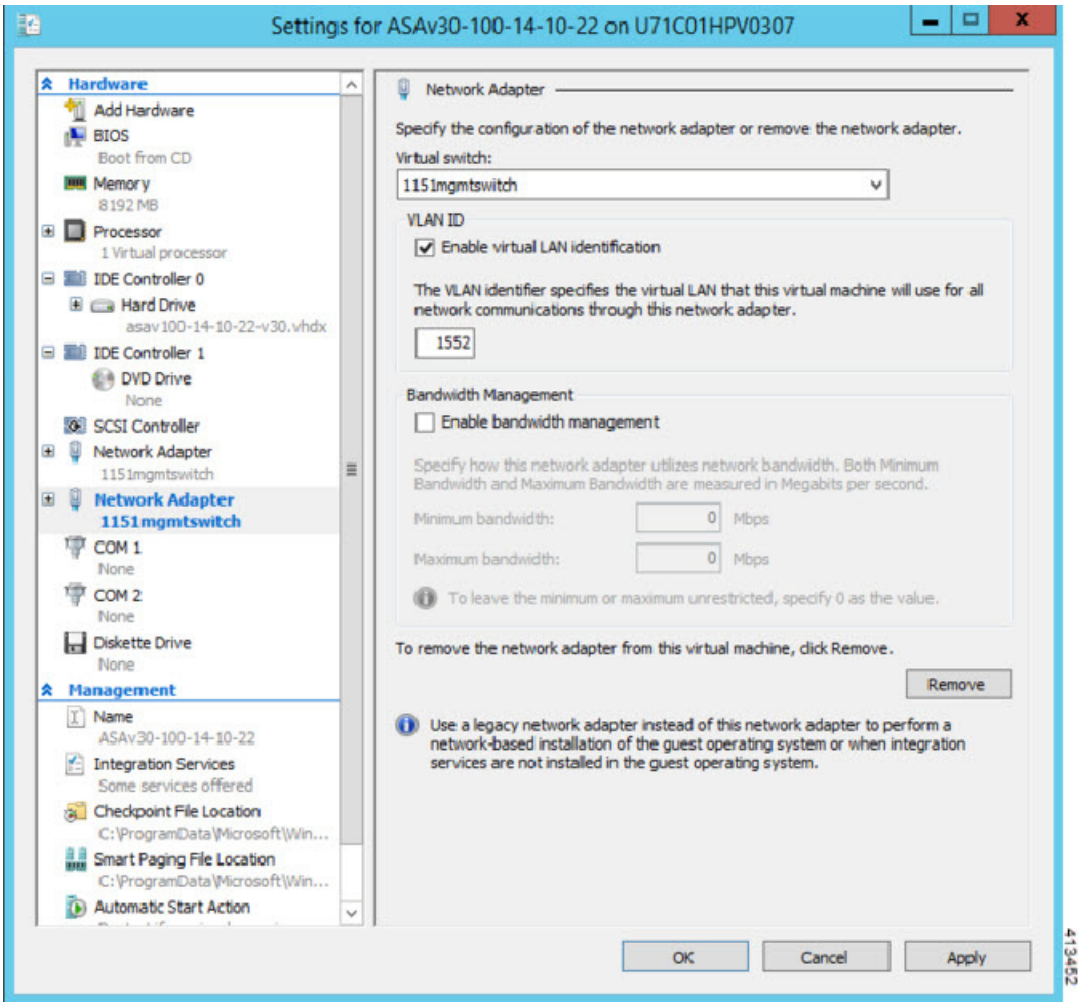
1. Hyper-V マネージャの右側にある [Settings] をクリックします。[Settings] ダイアログボックスが開きます。左側の [Hardware] メニューで、[Add Hardware] をクリックし、次に [Network Adapter] をクリックします。

   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。

Hyper-V マネージャからのネットワーク アダプタの追加



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。



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。

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 スプーフィングの設定

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 スプーフィングをオン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 マネージャでの手順

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、[Inside] をクリックし、メニューを展開して [Advanced Features] をクリックし、MAC アドレス オプションを表示します。[Enable MAC address spoofing] ラジオ ボタンをクリックします。
2. 外部インターフェイスでステップ 1 を繰り返します。

Powershell コマンド

```
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 [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（47 ページ）」を参照してください。

手順

1. RSAキー ペアが存在することを確認します。

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

2. RSAキー ペアがない場合は、RSA キー ペアを生成します。

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

   例

   ```
   asav((conf t)#
   username test password test123 privilege 15
   aaa authentication ssh console LOCAL
   ssh 10.7.24.0 255.255.255.0 management
   ssh version 2
   ```

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。

ASAv の設定

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

- ASDM の開始（61 ページ）
- ASDM を使用した初期設定の実行（62 ページ）
- 高度な設定（63 ページ）

ASDM の開始

手順

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

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

   次のボタンを持つ ASDM 起動ページが表示されます。

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

2. ランチャをダウンロードするには、次の手順を実行します。

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

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

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

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

3. Java Web Start を使用するには：

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

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

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

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

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

ASDM を使用した初期設定の実行

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

- Startup Wizard の実行（62 ページ）
- （オプション）ASAv の背後のパブリック サーバへのアクセス許可（62 ページ）
- （オプション）VPN ウィザードの実行（62 ページ）
- （オプション）ASDM の他のウィザードの実行（63 ページ）

Startup Wizard の実行

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

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

（オプション）ASAv の背後のパブリック サーバへのアクセス許可

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

（オプション）VPN ウィザードの実行

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

- Site-to-Site VPN Wizard：2 台の ASAv 間で、IPsec サイト間トンネルを作成します。
- AnyConnect VPN Wizard：Cisco AnyConnect VPN クライアントに対する SSL VPN リモート アクセスを設定します。AnyConnect は ASA へのセキュアな SSL 接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能となります。ASA ポリシーは、リモート ユーザがブラウザを使用して最初に接続するときに、AnyConnect クライアントをダウンロードするように設定できます。AnyConnect 3.0 以降を使用する場合、クライアントは、SSL または IPSec IKEv2 VPN プロトコルを実行できます。
- Clientless SSL VPN Wizard：ブラウザにクライアントレス SSL VPN リモート アクセスを設定します。クライアントレス ブラウザベース SSL VPN によって、ユーザはブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。認証されると、ユーザにはポータル ページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザにリソースへのアクセス権限を付与します。ACL は、特定の企業リソースへのアクセスを制限したり、許可するために適用できます。
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard：Cisco IPsec クライアント用の IPsec VPN リモート アクセスを設定します。

（オプション）ASDM の他のウィザードの実行

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

高度な設定

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

高度な設定