CHAPTER 1

Cisco ASAv 仮想アプライアンスの導入

ASAv に関する情報

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。ASAv は、VMware vSphere 上で稼働します。

Adaptive Security Device Manager（ASDM）または CLI を使用して ASAv を管理および監視できます。

VMware システム要件

ASAv を導入する前に、VMware vSphere 5.x から次のコンポーネントをインストールする必要があります。

- ESXi サーバ
- vCenter Server
- Windows または Linux 向け vSphere Web クライアントまたは vSphere クライアント

vSphere およびハードウェアの要件に関する詳細については、VMware のマニュアルを参照してください。

http://www.vmware.com/support/pubs/

（注） vCenter を使用せずに ESXi ホスト上に ASAv を直接インストールすることはできません。

vCloud Director を使用して ASAv を配置することはできません。

ASAv の VMware 機能のサポート

表 1 に、ASAv の VMware 機能のサポートを示します。

表 1　　ASAv の VMware 機能のサポート

機能	説明	サポート（あり/なし）	コメント
コールド クローン	クローニング中に VM の電源がオフになります。	あり	—
DRS	動的リソースのスケジューリングおよび分散電源管理に使用されます。	あり	—
ホット追加	追加時に VM が動作しています。	あり	—
ホット クローン	クローニング中に VM が動作しています。	なし	—
ホット リムーブ	取り外し中に VM が動作しています。	あり	—
Snapshot	VM が数秒間フリーズします。	あり	使用には注意が必要です。トラフィックが失われる可能性があります。フェールオーバーが発生することがあります。
一時停止と再開	VM が一時停止され、その後再開します。	あり	—
vCloud Director	VM の自動配置が可能になります。	なし	—
VM の移行	移行中に VM の電源がオフになります。	あり	—
VMotion	VM のライブ マイグレーションに使用されます。	あり	—
VMware FT	VM の HA に使用されます。	なし	ASAv VM の障害に対して ASAv のフェールオーバーを使用します。
VMware HA	ESX およびサーバの障害に使用されます。	あり	ASAv VM の障害に対して ASAv のフェールオーバーを使用します。
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	ASAv VM の障害に対して ASAv のフェールオーバーを使用します。
VMware vSphere スタンドアロン Windows クライアント	VM を配置するために使用されます。	あり	—
VMware vSphere Web クライアント	VM を配置するために使用されます。	あり	—

ASAv の前提条件

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。

表 1-2　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 >	許可	許可
MAC アドレスの変更	< 任意 >	許可	< 任意 >	許可
不正送信	< 任意 >	許可	許可	許可

詳細については、vSphere のマニュアルを参照してください。

注意事項と制約事項

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。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

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では、スタンバイ装置に割り当てられる vCPU の数がプライマリ装置に割り当てられる数と同じであることを確認してください（vCPU のライセンス数とも一致すること）。

IPv6 のガイドライン

- IPv6 をサポートします。
- VMware vSphere Web クライアントを使用して ASAv OVA ファイルを最初に配置する際は、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。

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

その他のガイドラインと制限事項

- ASAv OVA の導入は、ローカリゼーション（非英語モードでのコンポーネントのインストール）をサポートしません。ご自身の環境の VMware vCenter と LDAP サーバが ASCII 互換モードでインストールされていることを確認してください。
- ASAv をインストールして VM コンソールを使用する前に、キーボードを [United States English] に設定する必要があります。
- ASAv に割り当てられたメモリのサイズは、導入時に選択した vCPU 数に合わせたものです。異なる vCPU 数のライセンスを要求する場合を除き、[Edit Settings] ダイアログボックスでメモリ設定を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：**メモリを変更する必要がある場合は、ASAv ライセンスのセクションで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。
- 異なる vCPU 数のライセンスを要求している場合は、vCPU の制限値を変更する必要がありますが、それ以外では、vSphere の vCPU ハードウェア設定を変更しないでください。変更しなければ、ASAv を導入したときに正しい設定が適用されます。[Edit Settings] ダイアログボックスでこれらの設定を変更すると、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。リソース割り当てとオーバー プロビジョニングまたはアンダー プロビジョニングされたリソースを表示するには、ASAv の **show vm** コマンドと **show cpu** コマンド [ASDM Home] > [Device Dashboard] > [Device Information] > [Virtual Resources] タブまたは [Monitoring] > [Properties] > [System Resources Graphs] > [CPU] ペインを使用します。
- ASAv の導入時に、ホスト クラスタがある場合は、ストレージをローカルに（特定のホスト上）または共有ホスト上でプロビジョニングできます。しかし、ASAv を vMotion で別のホストに移行する場合は、いかなるタイプのストレージ（SAN またはローカル）を使用しても接続の中断が発生します。
- ESXi 5.0 を実行している場合
  - vSphere Web クライアントは ASAv OVA 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。
  - 導入用のフィールドが重複している場合があります。最初に表示されるフィールドに記入して、重複したフィールドは無視してください。

ASAv のライセンス要件

モデル	ライセンス要件
ASAv	• 1 つの仮想 CPU：1 つの vCPU に対する次の仕様を参照してください。 – 2 GB のメモリ – 5000 MHz の vCPU 周波数限界 – 100,000 の同時ファイアウォール接続 – 標準ライセンス：2 つの SSL VPN セッション。プレミアム ライセンス：250 の SSL VPN セッション、Advanced Endpoint Assessment、AnyConnect for Cisco VPN Phone、AnyConnect for Mobile。 • 4 つの仮想 CPU：4 つの vCPU に対する次の仕様を参照してください。 – 8 GB RAM – 20000 MHz の vCPU 周波数限界 – 500,000 の同時ファイアウォール接続 – 標準ライセンス：2 つの SSL VPN セッション。プレミアム ライセンス：750 の SSL VPN セッション、Advanced Endpoint Assessment、AnyConnect for Cisco VPN Phone、AnyConnect for Mobile。 （注） 4 つの vCPU ライセンスを適用するが 2 つまたは 3 つの vCPU を導入する場合は、次の値を参照してください。 2 つの仮想 CPU：4 GB の RAM、10000 MHz の vCPU 周波数限界、250,000 の同時ファイアウォール接続。 3 つの仮想 CPU：4 GB の RAM、15000 MHz の vCPU 周波数限界、350,000 の同時ファイアウォール接続。

（注） ASAv で仮想 CPU 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。通常の操作には、仮想 CPU ライセンスが必要です。

ASAv の導入

- 「vSphere Web クライアント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」（P.1-6）
- 「VMware vSphere Web クライアントを使用した ASAv の導入」（P.1-7）

vSphere Web クライアント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 クライアント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。

スタンドアロン vSphere クライアントを使用することを選択することもできますが、このガイドでは Web クライアントについてのみ説明します。

手順の詳細

ステップ 1　ブラウザから VMware vSphere Web クライアントを起動します。

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

デフォルトでは、ポートは 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。

a.　サインオン画面で、[**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 クライアントに再接続します。

ステップ 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クリックします（Windows のみ）。

VMware vSphere Web クライアントを使用した 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 Open Virtualization Format（OVF）形式のテンプレート ファイルを使用します。ASAv については、OVF パッケージが単一の Open Virtual Appliance（OVA）ファイルとして提供されることに留意してください。シスコの ASAv パッケージを展開するには、vSphere Web クライアントの [Deploy OVF Template] ウィザードを使用します。このウィザードは、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 クライアントのオンライン ヘルプを参照してください。

前提条件

ASAv を導入する前に、vSphere （管理用）に設定されているネットワークが少なくとも 1 つなければなりません。

手順の詳細

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

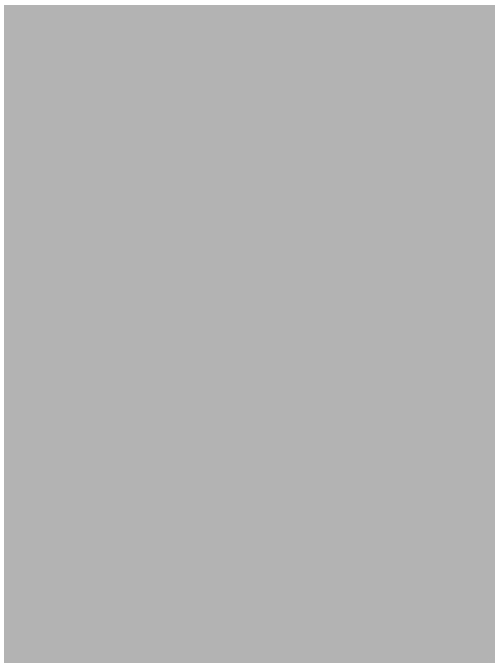
http://www.cisco.com/go/asa-software

（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 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　[Select Source] 画面で、URL を入力するか、ダウンロードした ASAv OVA パッケージを参照し、[**Next**] をクリックします。

ステップ 6　[Review Details] 画面で、ASAv パッケージの情報を確認し、[**Next**] をクリックします。

ステップ 7　[Accept EULAs] 画面で、エンド ユーザ ライセンス契約を確認および受諾し、[**Next**] をクリックします。

ステップ 8　[Select name and folder] 画面で、ASAv 仮想マシン（VM）インスタンスの名前を入力し、VM のインベントリ ロケーションを選択して、[**Next**] をクリックします。

ステップ 9　[Select Configuration] 画面で、次のオプションの 1 つを選択します。

- スタンドアロン：ASAv 配置構成に [**1**（または **2**、**3**、**4**）**vCPU Standalone**] を選択し、[**Next**] をクリックします。
- フェールオーバー：ASAv 配置構成に [**1**（または **2**、**3**、**4**）**vCPU HA Primary**] を選択し、[**Next**] をクリックします。

ステップ 10　[Select Storage] 画面で：

a. 仮想ディスク フォーマットを選択します。プロビジョニングに使用できる形式は、[Thick Provision]、[Thick Provision Lazy Zeroed]、および [Thin Provision] です。シック プロビジョニングおよびシン プロビジョニングの詳細については、VMware vSphere Web クライアントのオンライン ヘルプを参照してください。ディスク領域を節約するには、[**Thin Provision**] オプションを選択します。

b. ASAv を実行するデータストアを選択します。

c. [Next] をクリックします。

ステップ 11　[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、[**Next**] をクリックします。

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

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

すべての ASAv インターフェイスを使用する必要はありません。ただし、vSphere Web クライアントではネットワークをすべてのインターフェイスに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 クライアントに戻り、[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 クライアントのオンライン 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 12　[Customize template] 画面で：

a. 管理インターフェイスの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを設定します。また、ASDM アクセスが許可されるクライアント IP アドレスも設定する必要があり、別のゲートウェイがクライアントに到達する必要がある場合は、そのゲートウェイ IP アドレスを入力します。フェールオーバー配置では、スタティック アドレスとして IP アドレスを指定してください。DHCP は使用できません。

b. フェールオーバー配置では、管理 IP スタンバイ 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。

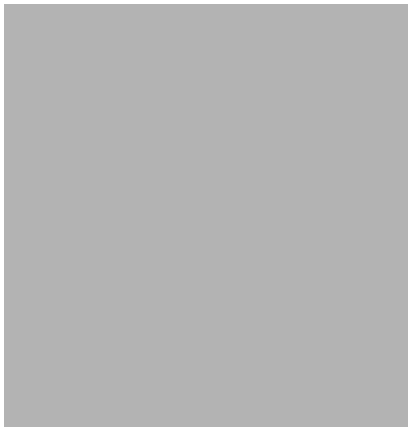
   ネットワーク デバイスは、MAC と IP アドレスの組み合わせについて変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

   また、[HA Settings] 領域でフェールオーバー リンク設定を行う必要があります。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。

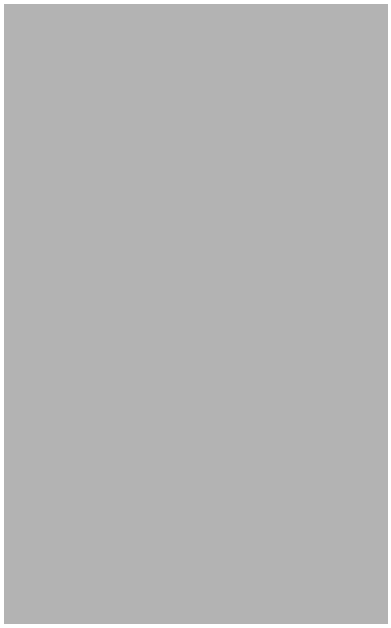
c. [Next] をクリックします。

ステップ 13 [Ready to complete] 画面で、ASAv 設定の概要を確認し、任意で [**Power on after deployment**] チェックボックスを確認したら、[**Finish**] をクリックして導入を開始します。

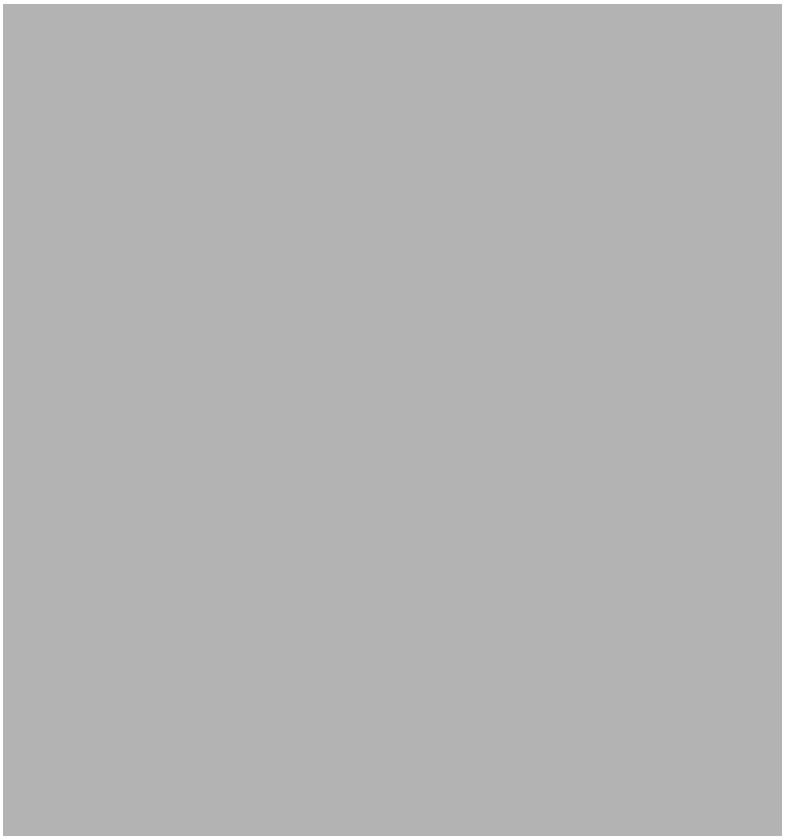
vSphere Web クライアントは VM を処理します。[Recent Tasks] ペインの [Global Information] 領域で「Initialize OVF deployment」ステータスを確認できます。



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。



ステップ 14　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、OVA 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 15　フェールオーバー配置の場合は、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。

a.　[Select Configuration] 画面で、ASAv 配置構成に [**1**（または **2**、**3**、**4**）**vCPU HA Secondary**] を選択します。

b.　[Customize template] 画面で、プライマリ装置と**全く同じ IP アドレス設定**を入力します（ステップ 12b. を参照）。装置をプライマリまたはセカンダリと認定するパラメータを除き、両方の装置のブートストラップ設定は同一です。