



VMware を使用した ASA の導入

VMware を使用して ASA を導入できます。

- [ASA の VMware 機能のサポート \(1 ページ\)](#)
- [ASA と VMware の前提条件 \(3 ページ\)](#)
- [ASA と VMware のガイドラインと制限事項 \(4 ページ\)](#)
- [ASA ソフトウェアの開梱と第 0 日用コンフィギュレーション ファイルの作成 \(7 ページ\)](#)
- [VMware vSphere Web Client を使用した ASA の導入 \(10 ページ\)](#)
- [VMware vSphere スタンドアロン クライアントおよび第 0 日用構成を使用した ASA の導入 \(15 ページ\)](#)
- [OVF ツールおよび第 0 日用構成を使用した ASA の導入 \(16 ページ\)](#)
- [ASA 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 \(20 ページ\)](#)
- [ESXi 構成でのパフォーマンスの向上 \(21 ページ\)](#)

ASA の VMware 機能のサポート

次の表に、ASA の VMware 機能のサポートを示します。

表 1: ASA の VMware 機能のサポート

機能	説明	サポート (あり/なし)	注釈
コールド クローン	クローニング中に VM の電源がオフになります。	あり	—
DRS	動的リソースのスケジューリングおよび分散電源管理に使用されます。	Yes	VMware の ガイドライン を参照してください。

機能	説明	サポート（あり/なし）	注釈
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。	Yes	共有ストレージを使用します。 vMotion に関するガイドライン（5 ページ） を参照してください。
VMware FT	VM の HA に使用されます。	なし	ASA の VM 障害の場合は、ASA フェールオーバーを使用します。
VMware HA	ESXi およびサーバの障害に使用されます。	あり	ASA の VM 障害の場合は、ASA フェールオーバーを使用します。
VM ハートビートの VMware HA	VM 障害に使用されます。	なし	ASA の VM 障害の場合は、ASA 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
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	—

ASA 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 ASA 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、ASA インターフェイスによって使用されるポート グループに対してセキュリティ 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 ASA 設定については、これらの設定の変更が必要な場合があります。詳細については、[vSphere のマニュアル](#)を参照してください。

表 2: ポート グループのセキュリティ ポリシーの例外

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

ASA と VMware のガイドラインと制限事項

ASA 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。

OVF ファイルのガイドライン

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

- asav-vi : vCenter に導入する場合
- asav-esxi : ESXi に導入する場合 (vCenter なし)
- ASA OVF の導入では、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) はサポートされません。ご自身の環境の VMware vCenter と LDAP サーバが ASCII 互換モードでインストールされていることを確認してください。
- ASA をインストールして VM コンソールを使用する前に、キーボードを [United States English] に設定する必要があります。
- ASA 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います。
 - マウントされた 2 番目のドライブは day0.iso です。



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

ハイ アベイラビリティ ガイドラインのためのフェールオーバー

フェールオーバー配置の場合は、スタンバイ装置が同じライセンス権限付与を備えていることを確認してください (たとえば、両方の装置が 2Gbps の権限付与であることなど)。



重要 ASA を使用してハイ アベイラビリティ ペアを作成する場合は、データ インターフェイスを各 ASA に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASA に追加されると、ASA コンソールにエラーが表示される可能性があります。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。

IPv6 のガイドライン

VMware vSphere Web Client を使用して ASA OVF ファイルを最初に導入する場合は、管理インターフェイスに IPv6 アドレスを指定できません。ASDM または CLI を使用して、IPv6 アドレスを後で追加できます。

vMotion に関するガイドライン

- VMware では、vMotion を使用する場合、共有ストレージのみを使用する必要があります。ASA の導入時に、ホストクラスタがある場合は、ストレージをローカルに（特定のホスト上）、または共有ホスト上でプロビジョニングできます。ただし、ASA を vMotion を使用して別のホストに移行する場合、ローカルストレージを使用するとエラーが発生します。

スループット用のメモリと vCPU の割り当てとライセンス

- ASA に割り当てられたメモリのサイズは、スループットレベルに合わせたものです。異なるスループットレベルのライセンスを要求する場合を除いて、[Edit Settings] ダイアログボックスのメモリ設定または vCPU ハードウェア設定は変更しないでください。アンダープロビジョニングの場合、パフォーマンスに影響する場合があります。オーバープロビジョニングの場合、ASA によりリロードが行われることが警告されます。待機期間（100 ～ 125% のオーバープロビジョニングの場合は 24 時間、125% 以上の場合は 1 時間）の後、ASA はリロードします。



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

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

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

- リソース割り当ておよび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ているリソースを表示するには、ASA の **show vm** 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] ペインを使用します。

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 ASA 設定で発生することがあります。MAC アドレスがさまざまな場所で出現した場合、パケットはドロップされます。

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

- **VMware NIC チーミング** : UCS B シリーズにトランスペアレント モードで ASA 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、そのアップリンクは同じである必要があります。vCenter で VMware NIC チーミングを設定します。

NIC チーミング の設定方法の詳細については、VMware ドキュメントを参照してください。

- **ARP インスペクション** : ASA 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 Series General Operations Configuration Guide』を参照してください。

CD/DVD ドライブの接続を解除した後、ASA が到達不能になる

[Edit Settings] ダイアログボックスを使用して、CD/DVD ドライブを ASA 仮想マシンに接続したり、接続を解除したりできます。[VM Hardware] パネルからデバイスを接続したり、接続を解除したりできます。



重要

ASA に到達できなくなる可能性があるため、ASA の CD/DVD ドライブの接続を解除しないことをお勧めします。

回避策

接続を解除された CD/DVD ドライブが原因で ASA が到達不能状態になっている場合は、次の手順を実行します。

1. [Monitor] タブをクリックし、[Notifications] をクリックします。
2. 次のようなアラートを探します。「*The guest operating system has locked the CD-ROM door and is probably using the CD-ROM, which can prevent the guest from recognizing media changes. If possible, eject the CD-ROM from inside the guest before disconnecting. Disconnect anyway and override the lock?*」
3. アラートを確認します。プロンプトが表示されたら、ポップアップで [Yes] を選択し、[OK] をクリックします。
4. ASA 仮想マシンに再度到達可能になっている必要があります。

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 Client は ASA 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。

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

ASA 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、ASA の起動時に適用される ASA 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 サーバを設定するコマンドを含める必要がありますが、すべての ASA 設定を含めることもできます。空の day0-config を含むデフォルトの day0.iso がリリースとともに提供されています。day0.iso ファイル (カスタム day0 またはデフォルトの day0.iso) は、最初の起動中に使用できなければなりません。

始める前に

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

- 初期導入時に自動的に ASA 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。
- トランスペアレントモードで ASA 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、[ASA と VMware のガイドラインと制限事項（4 ページ）](#) の OVF ファイルのガイドラインを参照してください。

手順

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

<https://www.cisco.com/go/asa-software>

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

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

- asav-vi.ovf : vCenter への導入用。
- asav-esxi.ovf : vCenter 以外への導入用。
- boot.vmdk : ブート ディスク イメージ。
- disk0.vmdk : ASA 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。

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

最初の行は ASA のバージョンで始める必要があります。day0-config は、有効な ASA 構成である必要があります。day0-config を生成する最適な方法は、既存の ASA または ASA 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 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 192.168.1.1 255.255.255.0
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

```

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

このセクションでは、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](#) (10 ページ)
- [VMware vSphere Web Client を使用した ASAv の導入](#) (10 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

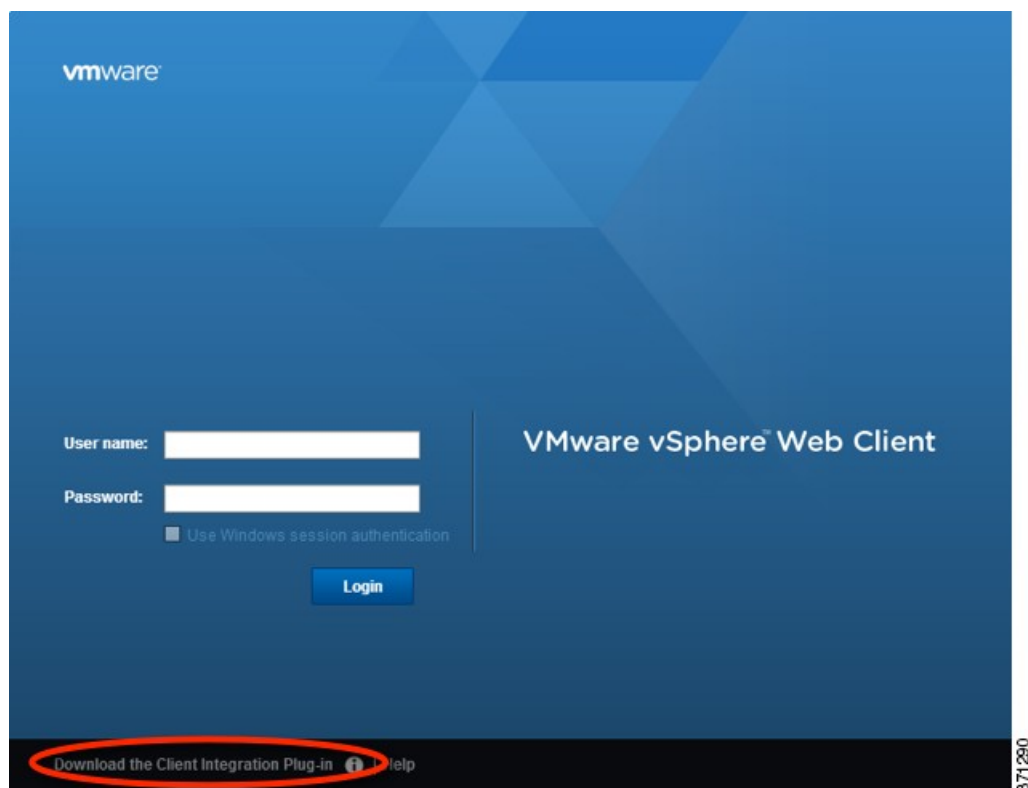
ステップ 1 ブラウザから VMware vSphere Web Client を起動します。

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

VMware vSphere Web Client を使用した ASA の導入

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

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

始める前に

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

手順

- ステップ 1** ASA ZIP ファイルを Cisco.com からダウンロードし、PC に保存します。
<http://www.cisco.com/go/asa-software>
 (注) Cisco.com のログインおよびシスコ サービス契約が必要です。
- ステップ 2** vSphere Web Client の [Navigator] ペインで、[vCenter] をクリックします。
- ステップ 3** [Hosts and Clusters] をクリックします。
- ステップ 4** ASA 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 ASA インターフェイスにネットワークをマッピングします。

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

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

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

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

ステップ 7 インターネット アクセスに HTTP プロキシを使用する場合は、[Smart Call Home Settings] 領域でスマート ライセンスのプロキシアドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

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

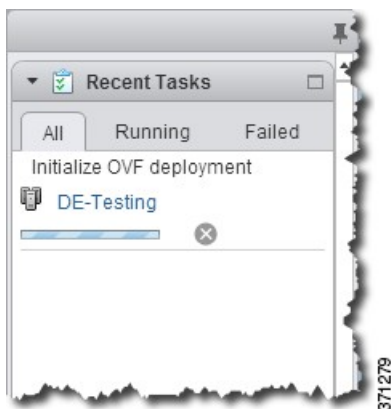
- スタンバイ管理 IP アドレスを指定します。

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

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

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

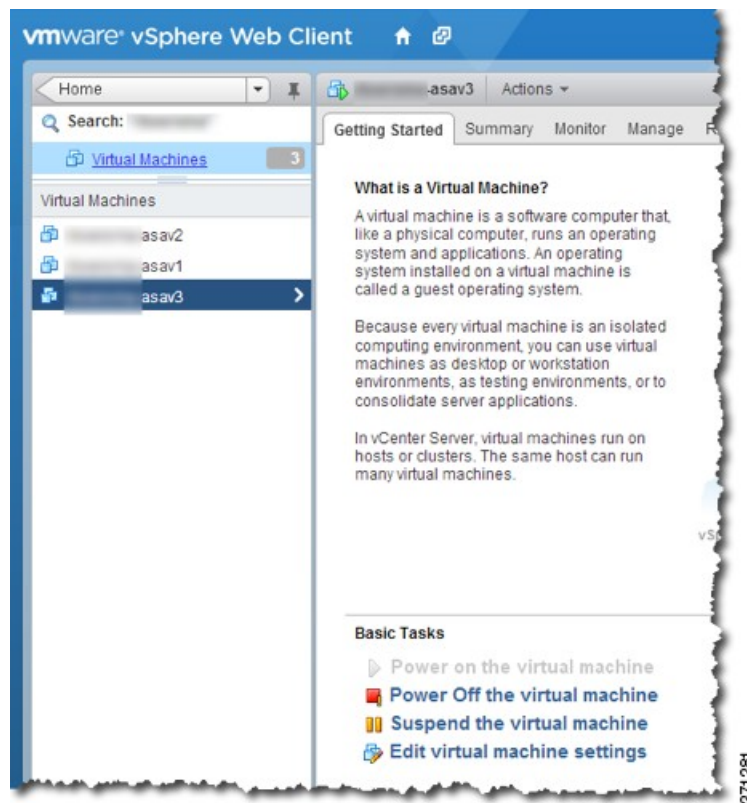
ステップ 9 ウィザードが完了すると、vSphere Web Client は VM を処理します。[Global Information] 領域の [Recent Tasks] ペインで [Initialize OVF deployment] ステータスを確認できます。



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



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

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

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 認証局に正常に登録するには、ASA をインターネット アクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

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

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

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

始める前に

- ASA を導入する前に、vSphere (管理用) に少なくとも 1 つのネットワークを設定しておく必要があります。
- [ASA ソフトウェアの開梱と第 0 日用コンフィギュレーションファイルの作成 \(7 ページ\)](#) の手順に従って、第 0 日用構成を作成します。

手順

- ステップ 1 VMware vSphere クライアントを起動し、**[File] > [Deploy OVF Template]** を選択します。
[Deploy OVF Template] ウィザードが表示されます。
 - ステップ 2 asav-vi.ovf ファイルを解凍した作業ディレクトリを参照し、それを選択します。
 - ステップ 3 [OVF Template Details] 画面が表示されます。次の画面に移動します。カスタムの第 0 日用コンフィギュレーションファイルを使用する場合は、構成を変更する必要はありません。
 - ステップ 4 最後の画面に導入設定の要約が表示されます。[Finish] をクリックして VM を導入します。
 - ステップ 5 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。
 - 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 日用コンフィギュレーション 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 ソフトウェアの開梱と第 0 日用コンフィギュレーションファイルの作成（7 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 サーバに接続できることを確認します。

手順

- ステップ 1 OVF ツールがインストールされていることを確認します。
例：

```
linuxprompt# which ovftool
```
- ステップ 2 必要な導入オプションを指定した .cmd ファイルを作成します。
例：


```
linuxprompt# cat launch.cmd
ovftool \
--name="asav-941-demo" \
--powerOn \
--deploymentOption=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@10.1.1.2.3/
```

ステップ 3 cmd ファイルを実行します。

例 :

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

ASA に電源を投入し、2 回目の起動を待機します。

ステップ 4 ASA 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、ASA 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、ASA は完全に動作可能な状態です。

ASA 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](#)

VMware vSphere コンソールの使用

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

始める前に

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

手順

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

ASA がまだ起動中の場合は、起動メッセージが表示されます。

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

- (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せん。ライセンスは、通常の操作に必要です。ライセンスをインストールするまで、次のメッセージがコンソールで繰り返し表示されます。

```
Warning: ASA platform license state is Unlicensed.
Install ASA 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。

- ステップ 3** 特権 EXEC モードにアクセスします。

例：

```
ciscoasa> enable
```

次のプロンプトが表示されます。

```
Password:
```

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

プロンプトが次のように変化します。

```
ciscoasa#
```

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

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

- ステップ 5** グローバル コンフィギュレーションモードにアクセスします。

```
ciscoasa# configure terminal
```

プロンプトが次のように変化します。

```
ciscoasa(config)#
```

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

ネットワーク シリアル コンソール ポートの設定

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

手順

ステップ 1 VMware vSphere でネットワーク シリアル ポートを設定します。VMware vSphere のマニュアルを参照してください。

ステップ 2 ASA 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できます。
- vSphere コンソールで、ファイル システム内の既存のファイル（任意のファイル）を新しい名前にコピーできます。次に例を示します。

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

ステップ 3 ASA をリロードします。

- ASDM から、**[Tools] > [System Reload]** を選択します。
- vSphere コンソールで **reload** を入力します。

ASA は vSphere コンソールへの送信を停止し、代わりにシリアル コンソールに送信します。

ステップ 4 シリアル ポートの追加時に指定した vSphere のホスト IP アドレスとポート番号に Telnet 接続するか、または vSPC の IP アドレスとポートに Telnet 接続します。

vCPU またはスループット ライセンスのアップグレード

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

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



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

手順

- ステップ 1 新しいライセンスを要求します。
- ステップ 2 新しいライセンスを適用します。フェールオーバーペアの場合、両方の装置に新しいライセンスを適用します。
- ステップ 3 フェールオーバーを使用するかどうかに応じて、次のいずれかを実行します。
 - フェールオーバーあり：vSphere Web Client で、スタンバイ ASA の電源を切断します。たとえば、ASA をクリックしてから [Power Off the virtual machine] をクリックするか、または ASA を右クリックして [Shut Down Guest OS] を選択します。
 - フェールオーバーなし：vSphere Web Client で、ASA の電源を切断します。たとえば、ASA をクリックしてから [Power Off the virtual machine] をクリックするか、または ASA を右クリックして [Shut Down Guest OS] を選択します。
- ステップ 4 ASA をクリックしてから [Edit Virtual machine settings] をクリックします（または ASA を右クリックして [Edit Settings] を選択します）。
[Edit Settings] ダイアログボックスが表示されます。
- ステップ 5 新しい vCPU ライセンスの正しい値を確認するには、[ASA のライセンス](#)にある CPU 要件とメモリ要件を参照してください。
- ステップ 6 [Virtual Hardware] タブの [CPU] で、ドロップダウン リストから新しい値を選択します。
- ステップ 7 [Memory] には、新しい RAM の値を入力します。
- ステップ 8 [OK] をクリックします。
- ステップ 9 ASA の電源をオンにします。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](#)」を参照してください。

ESXi 構成でのパフォーマンスの向上

ESXi ホストの CPU 構成時の設定を調整することによって、ESXi 環境内の ASA 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](#)。

