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 9.3

発行日：14/07/24
更新日：14/11/11

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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.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 IP 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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S.and other countries.To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2014 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」（P.3）
- 「ASAv のガイドライン」（P.3）
- 「ASAv のライセンス」（P.4）

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*』[英語] を参照してください。

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html

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）。

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

ASAv のライセンス

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 に仮想 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。

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」（P.5）
- 「ASAv と VMware の前提条件」（P.6）
- 「ASAv および VMware のガイドライン」（P.6）
- 「VMware を使用した ASAv の導入」（P.7）
- 「ASAv コンソールへのアクセス」（P.11）
- 「vCPU ライセンスのアップグレード」（P.13）

ASAv の VMware 機能のサポート

次の表に、ASAv の VMware 機能のサポートを示します。

表 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	–
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	–
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。

表 1　　ASAv （続き）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
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 システム要件

ASA 互換性マトリクスを参照してください。

http://www.cisco.com/c/en/us/td/docs/security/asa/compatibility/asamatrx.html

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 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	フェールオーバーあり	フェールオーバーなし	フェールオーバーあり
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。

ASAv および VMware のガイドライン

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）。

VMware を使用した ASAv の導入

IPv6 のガイドライン

VMware vSphere Web Client 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。

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 に割り当てられるメモリは、特に、導入時に選択した vCPU の数に合わせてサイズ調整されます。異なる数の vCPU 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」（P.4）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。

  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。

- 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 Client は ASAv OVA の導入ではサポートされません。代わりに vSphere Client 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入力して、重複したフィールドは無視してください。

VMware 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。

1. 「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」（P.7）
2. 「VMware vSphere Web Client を使用した ASAv の導入」（P.8）

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

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

スタンドアロン vSphere Client 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 Client についてのみ説明します。

VMware を使用した ASAv の導入

手順

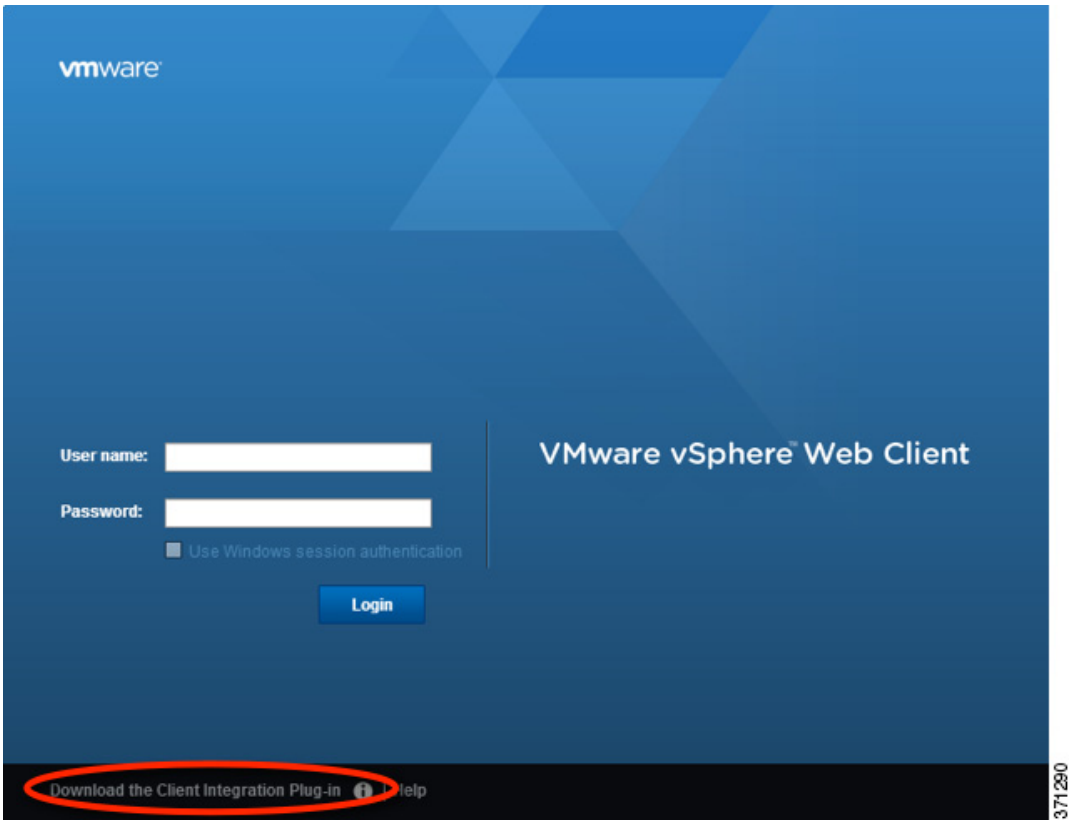
1. ブラウザから VMware vSphere Web Client を起動します。

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

   デフォルトでは、ポートは 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 Client（または vSphere Client）、およびオープン仮想化フォーマット（OVF）のテンプレート ファイルを使用します。ASAv については、OVF パッケージが単一のオープン仮想アプライアンス（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 Client で 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 の標準的なものです。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。

VMware を使用した ASAv の導入

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 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。

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。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 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。

VMware を使用した ASAv の導入

7. 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。

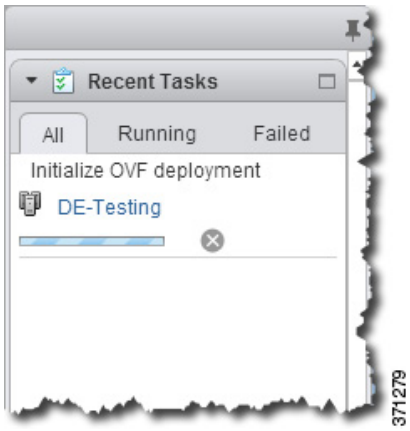
   – スタンバイ管理 IP アドレスを指定します。

     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。

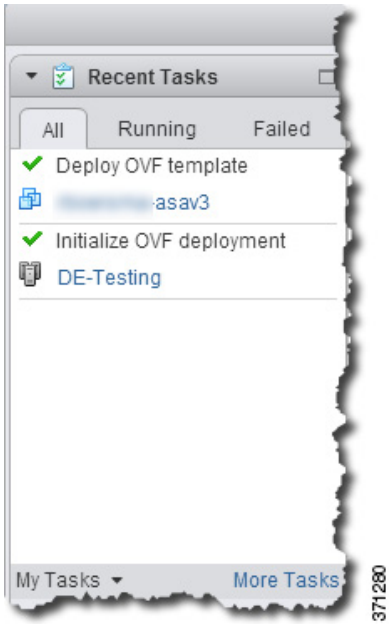
   – [HA Connection Settings] 領域で、フェールオーバー リンクを設定します。

     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。

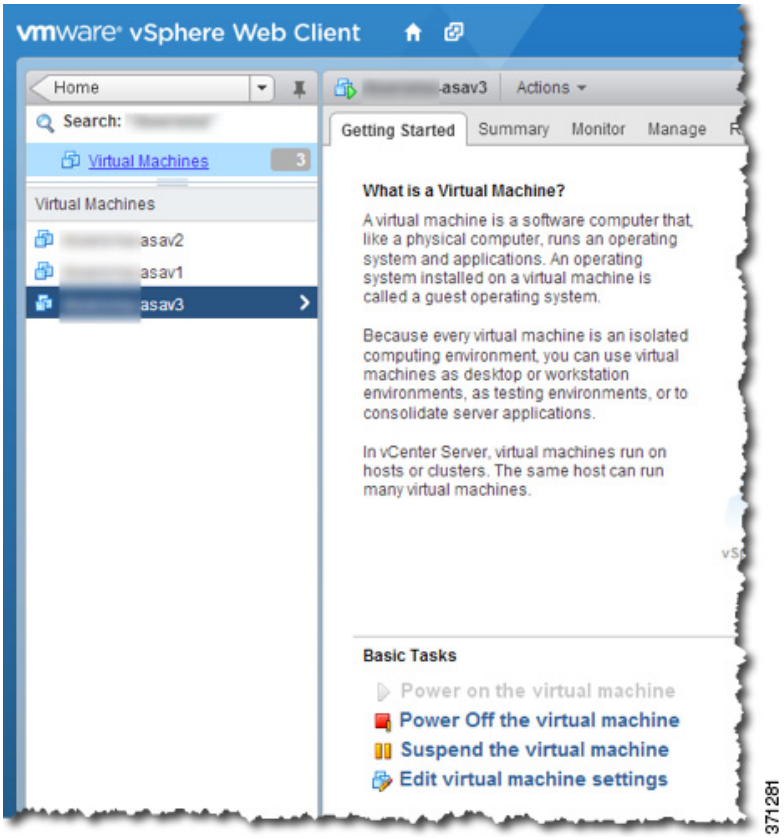
8. ウィザードが完了すると、vSphere Web Client は VM を処理します。[Recent Tasks] ペインの [Global Information] 領域で [Initialize OVF deployment] ステータスを確認できます。



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。



9. 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。

10. 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 vCPU 数を設定します。
   – 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。

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」（P.12）
■ 「ネットワーク シリアル コンソール ポートの設定」（P.13）

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、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。

   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 ライセンスのアップグレード

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 ライセンスと一致している必要があります。vCPU 周波数限界と RAM も、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

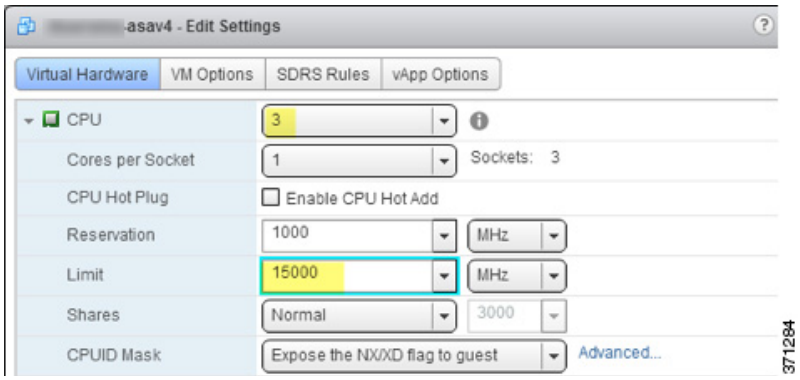
1. 新しいライセンスを要求します。
2. 新しいライセンスを適用します。フェールオーバー ペアの場合、両方の装置に新しいライセンスを適用します。
3. フェールオーバーを使用するかどうかに応じて、次のいずれかを実行します。
   - フェールオーバーあり：vSphere Web Client で、*スタンバイ* ASAv の電源を切断します。たとえば、ASAv をクリックしてから [Power Off the virtual machine] をクリックするか、または ASAv を右クリックして [Shut Down Guest OS] を選択します。
   - フェールオーバーなし：vSphere 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」（P.4）にある CPU/周波数/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。また、vCPU 周波数の [Limit] の値を変更するには、展開の矢印をクリックする必要があります。



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# no failover active
       ```

    c. アクティブ装置に対して、順 3～9 を繰り返します。

関連項目

- 「ASAv ライセンスの適用」（P.16）
- 「ASAv のライセンス」（P.4）

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」（P.15）
- 「ASAv ライセンスの適用」（P.16）
- 「ASDM を使用した初期設定の実行」（P.17）
- 「高度な設定」（P.18）

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。

ASAv ライセンスの適用

ASAv を導入した後、vCPU 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、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.
```

CLI ライセンスの手順

手順

1. ASAv コンソールで、次のコマンドを入力してシリアル番号を表示しメモします。

   ```
   ciscoasa# show version | grep Serial
   ```

   次に例を示します。

   ```
   ciscoasa# show version | grep Serial
   Serial Number: VBXQEFMXX44
   ciscoasa#
   ```

2. シスコ代理店から購入できる製品認証キーを入手します。機能ライセンスごとに個別の製品認証キーを購入する必要があります。ASAv の場合は、唯一の必須の機能ライセンスは CPU（1 ～ 4）に対してのものですが、他の機能キーも購入できます。

3. ASA ライセンス ガイドに従って、シリアル番号に対するアクティベーション キーを Cisco.com から依頼します。必ず、ASAv の導入時に指定した CPU 数に一致する CPU ライセンスを依頼してください。

4. シスコからアクティベーション キーを受け取った後、ASAv コンソールでそのキーを適用します。

   ```
   ciscoasa# activation-key key
   ```

   次に例を示します。

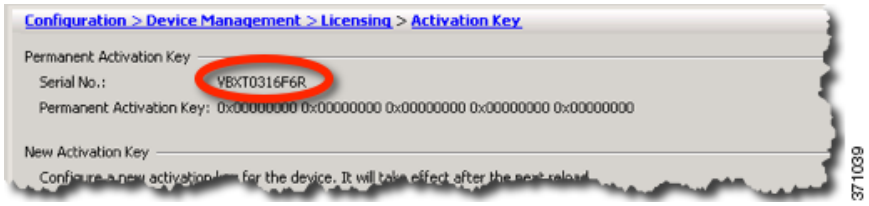
   ```
   ciscoasa# activation-key 592811f1 19ed804b 613befa3 d85bb703 c61b7da2
   Validating activation key.This may take a few minutes...
   The requested key is a timebases key and is activated, it has 364 days remaining.

   ASAv platform license state is Compliant
   ```

ASDM ライセンスの手順

手順

1. メインの ASDM ページで [License] タブをクリックし、次に [More Licenses] をクリックして、シリアル番号を確認します。

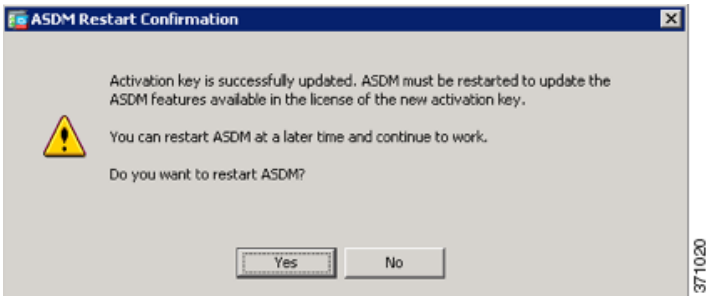
2. [Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインから、シリアル番号を書き留めます。



3. シスコ代理店から購入できる製品認証キーを入手します。機能ライセンスごとに個別の製品認証キーを購入する必要があります。ASAv の場合は、唯一の必須の機能ライセンスは vCPU（1 ～ 4）に対してのものですが、他の機能キーも購入できます。
4. ASA ライセンス ガイドに従って、シリアル番号に対するアクティベーション キーを Cisco.com から依頼します。必ず、ASAv の導入時に指定した CPU 数に一致する CPU ライセンスを依頼してください。
5. シスコからアクティベーション キーを受け取った後、[Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインで、キーを [New Activation Key] フィールドに貼り付けます。
6. [Update Activation Key] をクリックします。

   ASDM には、キーを検証中にステータス ダイアログボックスが表示されます。

   キーの更新が完了すると、次のダイアログボックスが表示されます。



7. [Yes] をクリックして ASDM を再起動します。

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」（P.17）
- 「（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」（P.18）
- 「（オプション）VPN ウィザードの実行」（P.18）
- 「（オプション）ASDM の他のウィザードの実行」（P.18）

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、非武装地帯（DMZ）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、お使いのソフトウェア バージョンのマニュアルを参照してください。
http://www.cisco.com/go/asadocs