



Cisco 適応型セキュリティ仮想アプライアンス (ASA v) 9.6 ク イックスタートガイド

初版：2016年4月25日

最終更新：2019年1月22日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2016–2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

ASA の概要 1

- ハイパーバイザのサポート 1
- ASA のライセンス 1
- ASA のライセンス 2
- 注意事項と制約事項 5
 - ASA (すべてのモデル) のガイドラインと制限事項 5
 - ASA5 のガイドラインと制限事項 6
- ASA インターフェイスおよび仮想 NIC 7
 - ASA のインターフェイス 7
 - サポートされている vNIC 8

第 2 章

VMware を使用した ASA の導入 11

- ASA の VMware 機能のサポート 11
- ASA と VMware の前提条件 13
- VMware での ASA のガイドラインと制限事項 14
- ASA ソフトウェアの解凍と第 0 日用構成ファイルの作成 18
- VMware vSphere Web Client を使用した ASA の導入 20
 - 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 21
 - VMware vSphere Web Client を使用した ASA の導入 21
- 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 26
- OVF ツールおよび第 0 日用構成を使用した ASA の導入 27
- ASA コンソールへのアクセス 28
 - VMware vSphere コンソールの使用 28

ネットワーク シリアル コンソール ポートの設定	30
vCPU またはスループット ライセンスのアップグレード	30
トラフィックのモニタリングおよびシステム ダッシュボード	32

第 3 章**KVM を使用した ASA の導入 35**

KVM での ASA のガイドラインで制限事項	35
KVM を使用した ASA の導入について	36
ASA と KVM の前提条件	36
第 0 日のコンフィギュレーション ファイルの準備	38
仮想ブリッジ XML ファイルの準備	40
ASA の起動	41
KVM での ASA のパフォーマンス調整	42
KVM 構成でのパフォーマンスの向上	42
CPU ピンニングの有効化	42
NUMA のガイドライン	44
Receive Side Scaling (RSS) 用の複数の RX キュー	45
VPN の最適化	47
CPU 使用率とレポート	48
ASA Virtual の vCPU 使用率	48
CPU 使用率の例	48
KVM CPU 使用率レポート	49
ASA Virtual と KVM のグラフ	49

第 4 章**AWS クラウドへの ASA の導入 51**

AWS クラウドへの ASA の導入について	51
ASA と AWS の前提条件	52
ASA および AWS のガイドラインと制限事項	53
設定の移行と SSH 認証	54
AWS 上の ASA のネットワークトポロジの例	55
AWS での ASA の展開	55

第 5 章**Microsoft Azure クラウドへの ASA の導入 59**

- Microsoft Azure クラウドへの ASA の導入について 59
- ASA および Azure の前提条件およびシステム要件 60
- 注意事項と制約事項 61
- 導入時に作成されるリソース 63
- Azure ルーティング 65
- 仮想ネットワーク内の VM のルーティング設定 66
- IP アドレス 66
- DNS 67
- Microsoft Azure への ASA の導入 67
 - Azure Resource Manager からの ASA の導入 67

第 6 章**ASA の設定 71**

- ASDM の起動 71
- ASDM を使用した初期設定の実行 72
 - Startup Wizard の実行 72
 - (任意) ASA の内側にあるパブリックサーバーへのアクセス許可 73
 - (オプション) VPN ウィザードの実行 73
 - (オプション) ASDM の他のウィザードの実行 74
- 詳細設定 74



第 1 章

ASA の概要

適応型セキュリティ仮想アプライアンス (ASA) 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、ASA を管理およびモニタすることができます。その他の管理オプションを使用できる場合もあります。

- [ハイパーバイザのサポート \(1 ページ\)](#)
- [ASA のライセンス \(1 ページ\)](#)
- [ASA のライセンス \(2 ページ\)](#)
- [注意事項と制約事項 \(5 ページ\)](#)
- [ASA インターフェイスおよび仮想 NIC \(7 ページ\)](#)

ハイパーバイザのサポート

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

ASA のライセンス

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



- (注) ASA 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。

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

ASAのライセンス

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

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



(注) ASAはCisco Smart Software Licensingを使用します。スマートライセンスは、通常の操作に必要です。ライセンスをインストールするまで、スループットは100 Kbpsに制限されるため、予備接続テストを実行できます。

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

スマートライセンス資格

ASAはCisco Smart Software Licensingを使用します。詳細については、『[Smart Software Licensing for the ASA and ASA](#)』を参照してください。



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

表 1: ASA スマートライセンス資格

ライセンスの権限付与	vCPU/RAM	スループット	適用されるレートリミッタ
ラボエディションモード (ライセンスは不要)	すべてのプラットフォーム	100 Kbps	あり
ASA5 (100M)	1 vCPU/1 GB ~ 1.5 GB (2 GB 推奨)	100Mbps	あり
ASA10 (1 GB)	1 vCPU/2 GB	1Gbps	あり

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

ライセンスの状態

表 2: ASAv ライセンスの状態

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

モデルの説明と仕様

表 3: ASAv モデルの説明と仕様

モデル	ライセンス要件
ASAv5	<p>スマート ライセンス</p> <p>次の仕様を参照してください。</p> <ul style="list-style-type: none"> • 100 Mbps スループット • 1 vCPU • 1 GB RAM (1.5 GB に調節可能) <p>(注) 最適なパフォーマンスを実現するには、ASAv5 に 2 GB のメモリを推奨します。</p> <ul style="list-style-type: none"> • 50,000 の同時ファイアウォール接続 • AWS はサポート対象外 • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート
ASAv10	<p>スマート ライセンス</p> <p>次の仕様を参照してください。</p> <ul style="list-style-type: none"> • 1 Gbps スループット • 1 vCPU • 2 GB のメモリ • 100,000 の同時ファイアウォール接続 • c3.large、c4.large、および m4.large インスタンスで AWS をサポート • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート

モデル	ライセンス要件
ASAv30	<p>スマート ライセンス</p> <p>次の仕様を参照してください。</p> <ul style="list-style-type: none"> • 2 Gbps スループット • 4 vCPU • 8 GB RAM • 500,000 の同時ファイアウォール接続 • c3.xlarge、c4.xlarge、および m4.xlarge インスタンスで AWS をサポート • Standard D3 インスタンスと Standard D3_v2 インスタンスで Azure をサポート

注意事項と制約事項

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

ASAv（すべてのモデル）のガイドラインと制限事項

ディスクストレージ

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

コンテキストモードのガイドライン

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

ハイアベイラビリティガイドラインのためのフェールオーバー

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



重要 ASAv を使用して高可用性ペアを作成する場合は、データインターフェイスを各 ASAv に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASAv に追加されると、ASAv コンソールにエラーが表示されることがあります。また、フェールオーバー機能にも影響が出ることがあります。

サポートしない ASA 機能

ASAv は、次の ASA 機能をサポートしません。

- クラスタリング（KVM と VMware を除くすべての権限付与）
- マルチ コンテキスト モード
- アクティブ/アクティブ フェールオーバー
- EtherChannel
- AnyConnect Premium（共有）ライセンス

制限事項

- ASAv は、x710 NIC の 1.9.5 i40en ホストドライバと互換性がありません。これより古いバージョンまたは新しいバージョンのドライバは動作します。（VMware のみ）

ASAv5 のガイドラインと制限事項

パフォーマンスのガイドライン

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



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

- 場合によっては、ASA5 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 ASA5 を導入できます。1 GB から 1.5 GB に変更するには、VM の電源をオフにして、メモリを変更し、VM の電源を再度オンにします。
 - CLI から `show memory` コマンドを使用して、システムで使用可能な最大メモリと現在の空きメモリ量の概要を表示できます。
- ASA5 は、100 Mbps のしきい値に達するとすぐに、パケットのドロップを開始します（100 Mbps をすべて使用できるように、多少のヘッドルームがあります）。

制限事項

- ASA5 は AnyConnect HostScan 4.8 と互換性がありません。これには 2 GB の RAM が必要です。
- ASA5 は Amazon Web Services (AWS) ではサポートされていません。
- ジャンボ フレームはサポートされていません。

ASA インターフェイスおよび仮想 NIC

ASA 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。ASA 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。

- ASA のインターフェイス
- サポートされている vNIC

ASA のインターフェイス

ASA は、次のギガビットイーサネット インターフェイスがあります。

- Management 0/0

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

- GigabitEthernet 0/0 ~ 0/8。ASA 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 0/6 を使用できます。

サポートされている vNIC

ASAv では次の vNIC がサポートされています。

表 4: サポートされている vNIC

表 5: サポートされている vNIC

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

VMware および VMXNET3 の LRO を無効にします

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



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

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

1. vSphere Web Client インベントリで ASAv マシンを検索します。
 1. 仮想マシンを検索するには、データセンター、フォルダ、クラスタ、リソースプール、またはホストを選択します。
 2. [Related Objects] タブをクリックし、[Virtual Machines] タブをクリックします。
2. 仮想マシンを右クリックして、[Edit Settings] をクリックします。
3. [VM Options] をクリックします。

4. [Advanced] を展開します。
5. [Configuration Parameters] の下で、[Edit Configuration] ボタンをクリックします。
6. [Add Parameter] をクリックし、LRO パラメータの名前と値を入力します。
 - Net.VmxnetSwLROSL | 0
 - Net.Vmxnet3SwLRO | 0
 - Net.Vmxnet3HwLRO | 0
 - Net.Vmxnet2SwLRO | 0
 - Net.Vmxnet2HwLRO | 0



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

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

詳細については、次の VMware サポート記事を参照してください。

- VMware KB [1027511](#)
- VMware KB [2055140](#)



第 2 章

VMware を使用した ASA の導入

ASA は、VMware ESXi を実行できる任意のサーバークラスの x86 CPU デバイスに導入できません。

- [ASA の VMware 機能のサポート \(11 ページ\)](#)
- [ASA と VMware の前提条件 \(13 ページ\)](#)
- [VMware での ASA のガイドラインと制限事項 \(14 ページ\)](#)
- [ASA ソフトウェアの解凍と第 0 日用構成ファイルの作成 \(18 ページ\)](#)
- [VMware vSphere Web Client を使用した ASA の導入 \(20 ページ\)](#)
- [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 \(26 ページ\)](#)
- [OVF ツールおよび第 0 日用構成を使用した ASA の導入 \(27 ページ\)](#)
- [ASA コンソールへのアクセス \(28 ページ\)](#)
- [vCPU またはスループットライセンスのアップグレード \(30 ページ\)](#)
- [トラフィックのモニタリングおよびシステム ダッシュボード \(32 ページ\)](#)

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 6: 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。	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 (16 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 のマシンの障害に対して ASA のフェールオーバーを使用します。
VMware HA	ESXi およびサーバの障害に使用されます。	あり	ASA のマシンの障害に対して ASA 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 障害に使用されません。	なし	ASA のマシンの障害に対して ASA のフェールオーバーを使用します。

機能	説明	サポート（あり/なし）	注釈
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 Client、vSphere スタンドアロンクライアント、または OVF ツールを使用して ASA を導入できます。システム要件については、[Cisco ASA の互換性 \[英語\]](#) を参照してください。

vSphere 標準スイッチのセキュリティ ポリシー

vSphere スイッチについては、レイヤ2セキュリティポリシーを編集して、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 設定の場合、これらの設定の変更が必要な場合があります。詳細については、[vSphere のマニュアル](#)を参照してください。

表 7: ポートグループのセキュリティポリシーの例外

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

VMware での ASA のガイドラインと制限事項

ESXi サーバーに ASA の複数のインスタンスを作成して導入できます。ASA の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。作成する各仮想アプライアンスには、ホストマシン上での最小リソース割り当て（メモリ、CPU 数、およびディスク容量）が必要です。

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。

VMware ESXi での ASA のシステム要件

最適なパフォーマンスを確保するために、以下の仕様に準拠していることを確認してください。ASA には、次の要件があります。

- ホスト CPU は、仮想化拡張機能を備えたサーバークラスの x86 ベースの Intel または AMD CPU である必要があります。
たとえば、ASA パフォーマンステストラボでは、2.6GHz で動作する Intel® Xeon® CPU E5-2690v4 プロセッサを搭載した Cisco Unified Computing System™ (Cisco UCS®) C シリーズ M4 サーバーを最低限使用しています。
- ASA は、ESXi バージョン 6.0、6.5、6.7、7.0、7.0 アップグレード 1、7.0 アップグレード 2、および 7.0 アップグレード 3 をサポートします。

OVF ファイルのガイドライン

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

- asav-vi : vCenter に導入する場合
- asav-esxi : ESXi に導入する場合 (vCenter なし)
- ASA OVF の導入は、ローカリゼーション（非英語モードでのコンポーネントのインストール）をサポートしません。ご自身の環境の VMware vCenter と LDAP サーバーが ASCII 互換モードでインストールされていることを確認してください。
- 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 ASAv マシンが起動したら、両方のドライブのマウントを解除できます。ただし、[電源投入時に接続 (Connect at Power On)] がオフになっている場合でも、ドライブ 1 (OVF 環境変数を使用) は、ASAv の電源をオフ/オンにするたびに常にマウントされます。

OVF テンプレートのガイドラインのエクスポート

vSphere の OVF テンプレートのエクスポート機能は、既存の ASAv インスタンスパッケージを OVF テンプレートとしてエクスポートするのに役立ちます。エクスポートされた OVF テンプレートを使用して、同じ環境または異なる環境に ASAv インスタンスを導入できます。エクスポートされた OVF テンプレートを使用して vSphere に ASAv インスタンスを導入する前に、OVF ファイルの構成の詳細を変更して、導入の失敗を防ぐ必要があります。

ASAv のエクスポートされた OVF ファイルを変更するには、次の手順を実行します。

1. OVF テンプレートをエクスポートしたローカルマシンにログインします。
2. テキストエディタで OVF ファイルを参照して開きます。
3.

```
<vmw:ExtraConfig vmw:key="monitor_control.pseudo_perfctr"
vmw:value="TRUE"></vmw:ExtraConfig>
```

 タグが存在することを確認します。
4.

```
<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>
```

 タグを削除します。
または

```
<rasd:ResourceSubType>vmware.cdrom.iso</rasd:ResourceSubType>
```

 タグと

```
<rasd:ResourceSubType>vmware.cdrom.remotepassthrough</rasd:ResourceSubType>
```

 タグを交換します。
詳細については、VMware が公開した「[Deploying an OVF fails on vCenter Server 5.1/5.5 when VMware tools are installed \(2034422\)](#)」を参照してください。
5. UserPrivilege、OvfDeployment、および ControllerType のプロパティ値を入力します。
次に例を示します。

```
- <Property ovf:qualifiers="ValueMap{ "ovf", "ignore", "installer" }" ovf:type="string"
  ovf:key="OvfDeployment">
+ <Property ovf:qualifiers="ValueMap{ "ovf", "ignore", "installer" }" ovf:type="string"
  ovf:key="OvfDeployment" ovf:value="ovf">

- <Property ovf:type="string" ovf:key="ControllerType">
+ <Property ovf:type="string" ovf:key="ControllerType" ovf:value="ASAv">

- <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
  ovf:key="UserPrivilege">
+ <Property ovf:qualifiers="MinValue(0) MaxValue(255)" ovf:type="uint8"
  ovf:key="UserPrivilege" ovf:value="15">
```
6. OVF ファイルを保存します。

- OVF テンプレートを使用して、ASA を導入します。VMware vSphere Web Client を使用した ASA の導入 [英語] を参照してください。

ハイアベイラビリティガイドラインのためのフェールオーバー

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



重要 ASA を使用して高可用性ペアを作成する場合は、データインターフェイスを各 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ことがあります。また、フェールオーバー機能にも影響が出る可能性があります。

ASA 内部インターフェイスまたは ASA フェールオーバーの高可用性リンクに使用される ESX ポートグループについては、2 つの仮想 NIC を使用して ESX ポートグループのフェールオーバー順序を設定します（1 つはアクティブアップリンク、もう 1 つはスタンバイアップリンク）。この設定は、2 つの VM が相互に ping を実行したり、ASA 高可用性リンクを稼働させたりするために必要です。

vMotion に関するガイドライン

- VMware では、vMotion を使用する場合、共有ストレージのみを使用する必要があります。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は、パフォーマンスに影響を与える可能性があります。



- (注) メモリまたは vCPU ハードウェア設定を変更する必要がある場合は、ASA のライセンス (1 ページ) に記載されている値のみを使用してください。VMware が推奨するメモリ構成の最小値、デフォルト値、および最大値は使用しないでください。

場合によっては、ASA5 のメモリが枯渇状態になります。この状態は、AnyConnect クライアントの有効化やファイルのダウンロードなど、特定のリソースの利用が多い場合に発生することがあります。自動的な再起動に関するコンソールメッセージやメモリ使用量に関する重大な syslog が、メモリ枯渇の状態を示します。このような場合、1.5 GB メモリの

VM に ASAv5 を導入できます。1 GB から 1.5 GB に変更するには、VM の電源をオフにして、メモリを変更し、VM の電源を再度オンにします。

CPU 予約

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

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

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

- リソース割り当てとオーバープロビジョニングまたはアンダープロビジョニングされたリソースを表示するには、ASAv `show vm` および `show cpu` コマンド、あるいは ASDM [ホーム (Home)] > [デバイスダッシュボード (Device Dashboard)] > [デバイス情報 (Device Information)] > [仮想リソース (Virtual Resources)] タブまたは [モニタリング (Monitoring)] > [プロパティ (Properties)] > [システムリソースグラフ (System Resources Graphs)] > [CPU] ペインを使用できます。

UCS B シリーズ ハードウェアにおけるトランスペアレントモードに関するガイドライン

MAC フラップが、Cisco UCS B シリーズ ハードウェアのトランスペアレントモードで動作する一部の ASAv 設定で発生することがあります。MAC アドレスがさまざまな場所では出現した場合、パケットはドロップされます。

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

- VMware NIC チーミング：UCS B シリーズにトランスペアレントモードで ASAv を導入する場合、内部および外部インターフェイスに使用するポートグループにはアクティブアップリンクを1つだけ設定し、アップリンクは同じである必要があります。vCenter で VMware NIC チーミングを設定します。

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

- ARP インスペクション：ASAv で ARP インスペクションを有効にし、受信インターフェイスで MAC および ARP エントリを静的に設定します。[ARP インスペクション](#) と有効化の詳細については、Cisco ASA シリーズ コンフィギュレーションガイド (一般的な操作) [英語] を参照してください。

その他のガイドラインと制限事項

- ESXi 6.7、vCenter 6.7、ASA Virtual 9.12 以降を実行している場合、ASA Virtual は 2 つの CD/DVD IDE ドライブなしで起動します。
- vSphere Web Client は ASA OVA の導入ではサポートされないため、vSphere Client を使用してください。

ASA ソフトウェアの解凍と第 0 日用構成ファイルの作成

ASA を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、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 サーバーを設定するコマンドを含める必要がありますが、すべての ASA 設定を含めることもできます。空の day0-config を含むデフォルトの day0.iso がリリースとともに提供されています。day0.iso ファイル（カスタム day0 またはデフォルトの day0.iso）は、最初の起動中に使用できなければなりません。

始める前に

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

- 初期導入時に自動的に ASA にライセンスを付与するには、Cisco Smart Software Manager からダウンロードした Smart Licensing Identity (ID) トークンを「idtoken」というテキストファイルに格納し、第 0 日用構成ファイルと同じディレクトリに保存します。
- トランスペアレントモードで 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 構成ファイルを、第 0 日用構成ファイルとして使用する必要があります。これは、ルーテッドファイアウォールの第 0 日用コンフィギュレーションファイルには該当しません。
- ISO イメージが ESXi ハイパーバイザにどのようにマウントされるかの詳細については、[VMware での ASA のガイドラインと制限事項 \(14 ページ\)](#) 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 : ASAv ディスクイメージ。
- day0.iso : day0-config ファイルおよびオプションの idtoken ファイルを含む ISO。
- asav-vi.mf : vCenter への導入用のマニフェスト ファイル。
- asav-esxi.mf : vCenter 以外への導入用のマニフェスト ファイル。

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

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

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 サーバーに ASA 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 ASA の導入

この項では、VMware vSphere Web Client を使用して ASA 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 ASA の導入](#)」、または「[OVF ツールおよび第 0 日用構成を使用した ASA 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 \(21 ページ\)](#)
- [VMware vSphere Web Client を使用した ASA の導入 \(20 ページ\)](#)

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

1. ログイン画面で、[Download the Client Integration Plug-in] をクリックしてプラグインをダウンロードします。
2. ブラウザを閉じてから、インストーラを使用してプラグインをインストールします。
3. プラグインをインストールしたら、vSphere Web Client に再接続します。

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

VMware vSphere Web Client を使用した ASA の導入

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

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

始める前に

ASA 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

- 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、クラスター、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 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、ASA 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。

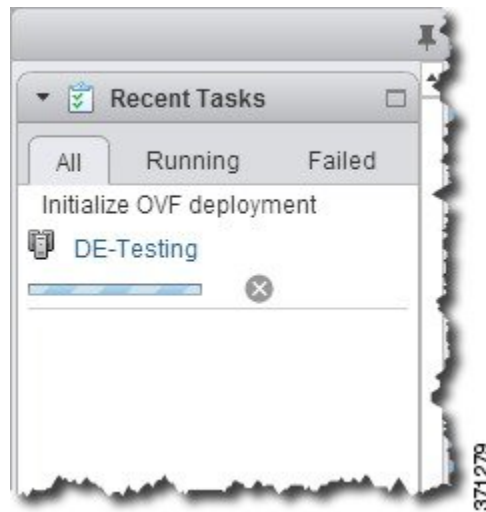
- スタンバイ管理 IP アドレスを指定します。

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。

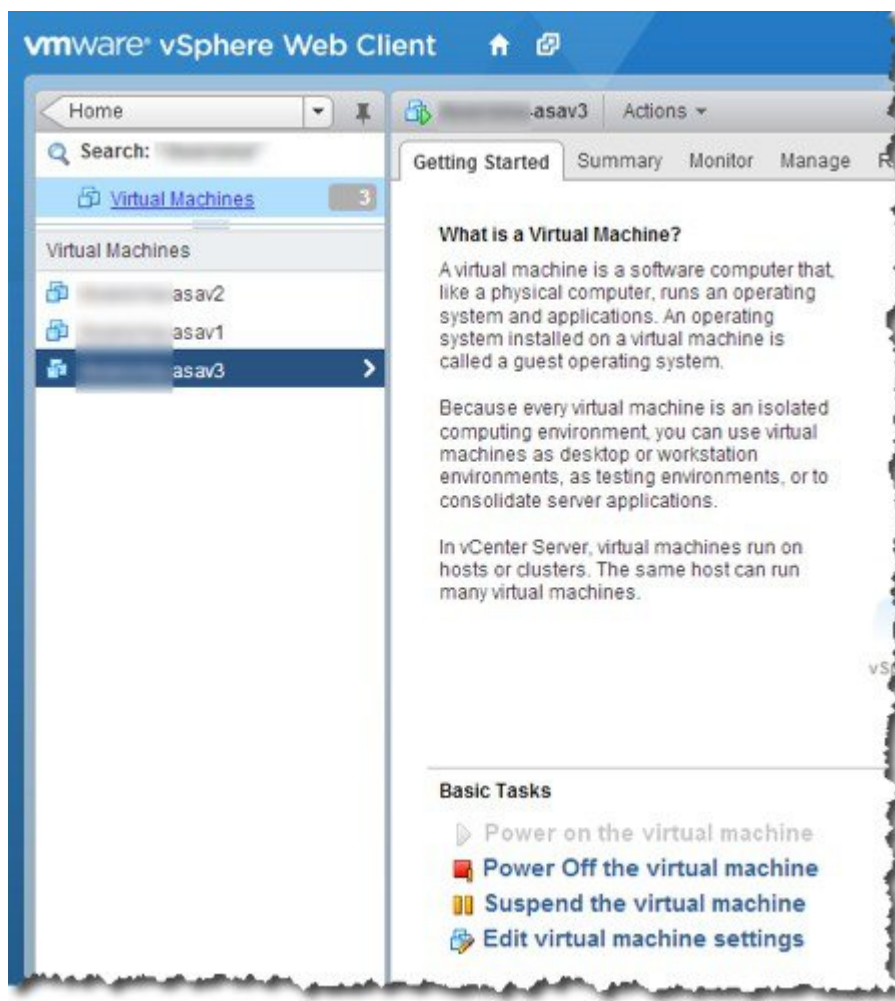
ステップ 9 ウィザードが完了すると、vSphere Web Client は VM を処理します。[Global Information] 領域の [Recent Tasks] ペインで [Initialize OVF deployment] ステータスを確認できます。



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



ステップ 10 ASA のマシンがまだ稼働していない場合は、[仮想マシンの電源をオン (Power on the virtual machine)] をクリックします。

ASDM で接続を試行したりコンソールに接続を試行する前に、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 Licensing Authority に ASAv を正常に登録するには、ASAv にインターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

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

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

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

始める前に

- ASAv を導入する前に、vSphere (管理用) で少なくとも 1 つのネットワークを設定しておく必要があります。
- [ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 \(18 ページ\)](#) 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 の電源を投入し、VMware コンソールを開いて、2 回目の起動を待機します。

ステップ 6 ASAv に SSH 接続し、必要な構成を完了します。第 0 日用コンフィギュレーションファイルに必要なすべての構成がされていない場合は、VMware コンソールを開いて、必要な構成を完了します。

これで、ASAv は完全に動作可能な状態です。

OVF ツールおよび第 0 日用構成を使用した ASAv の導入

このセクションでは、第 0 日用構成ファイルが必要とする OVF ツールを使用した ASAv の導入方法について説明します。

始める前に

- OVF ツールを使用して ASAv を導入する場合は、day0.iso ファイルが必要です。ZIP ファイルで提供されるデフォルトの空の day0.iso ファイルを使用するか、または、生成しカスタマイズした第 0 日用コンフィギュレーションファイルを使用できます。第 0 日用コンフィギュレーションファイルの作成方法については、[ASAv ソフトウェアの解凍と第 0 日用構成ファイルの作成 \(18 ページ\)](#) を参照してください。
- OVF ツールが Linux または Windows PC にインストールされ、ターゲット ESXi サーバーに接続できることを確認します。

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@10.1.2.3/
```

ステップ 3 cmd ファイルを実行します。

例 :

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

ASA の電源を投入し、2 回目の起動を待機します。

ステップ 4 ASA に SSH 接続し、必要に応じて設定を完了します。さらに設定が必要な場合は、ASA に対して VMware コンソールを開き、必要な設定を適用します。

これで、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 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。

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

(注) ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できません。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: ASAv platform license state is Unlicensed.  
Install ASAv platform license for full functionality.
```

次のプロンプトが表示されます。

```
ciscoasa>
```

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

ステップ 3 特権 EXEC モードにアクセスします。

例：

```
ciscoasa> enable
```

次のプロンプトが表示されます。

```
Password:
```

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

プロンプトが次のように変化します。

```
ciscoasa#
```

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

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

ステップ 5 グローバル コンフィギュレーションモードにアクセスします。

```
ciscoasa# configure terminal
```

プロンプトが次のように変化します。

```
ciscoasa(config)#
```

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

ネットワーク シリアル コンソール ポートの設定

コンソール エクスペリエンスの向上のために、コンソール アクセスについて、ネットワーク シリアルポートを単独で設定するか、または仮想シリアルポート コンセントレータ (vSPC) に接続するように設定できます。各方法の詳細については、VMware vSphere のマニュアルを参照してください。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 [ツール (Tools)] > [ファイル管理 (File Management)] ダイアログボックスを使用して、この名前で空のテキストファイルをアップロードできます。
- vSphere コンソールで、ファイル システム内の既存のファイル (任意のファイル) を新しい名前にコピーできます。次に例を示します。

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

ステップ 3 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 またはスルーブット 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ブット 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 の 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 [仮想マシンの電源をオフ (Power Off the virtual machine)] をクリックするか、または ASA を右クリックして [ゲスト OS をシャットダウン (Shut Down Guest OS)] を選択します。
 - フェールオーバーなし : vSphere Web クライアントで、ASA の電源を切断します。たとえば、ASA をクリックしてから [仮想マシンの電源をオフ (Power Off the virtual machine)] をクリックするか、または ASA を右クリックして [ゲスト OS をシャットダウン (Shut Down Guest OS)] を選択します。
- ステップ 4** ASA をクリックしてから [仮想マシンの設定の編集 (Edit Virtual machine settings)] をクリックします (または ASA を右クリックして [設定の編集 (Edit Settings)] を選択します)。
[Edit Settings] ダイアログボックスが表示されます。
- ステップ 5** 新しい vCPU ライセンスの正しい値を確認するには、[ASA のライセンス \(1 ページ\)](#) にある CPU 要件とメモリ要件を参照してください。
- ステップ 6** [Virtual Hardware] タブの [CPU] で、ドロップダウン リストから新しい値を選択します。
- ステップ 7** [Memory] には、新しい RAM の値を入力します。
- ステップ 8** [OK] をクリックします。
- ステップ 9** ASA の電源を入れます。たとえば、[Power On the Virtual Machine] をクリックします。
- ステップ 10** フェールオーバー ペアの場合 :
1. アクティブ装置へのコンソールを開くか、またはアクティブ装置で ASDM を起動します。
 2. スタンバイ装置の起動が終了した後、スタンバイ装置にフェールオーバーします。
 - ASDM : [Monitoring] > [Properties] > [Failover] > [Status] を選択し、[Make Standby] をクリックします。
 - CLI : **failover active**

3. アクティブ装置に対して、ステップ 3～9 を繰り返します。

次のタスク

詳細については、「[ASA のライセンス \(1 ページ\)](#)」を参照してください。

トラフィックのモニタリングおよびシステム ダッシュボード

システムには、デバイスを通過するトラフィックおよびセキュリティポリシーの結果を分析するために使用できる複数のダッシュボードがあります。ダッシュボード情報は、構成全体の有効性を評価し、ネットワークの問題を特定して解決するために使用します。



- (注) トラフィック関連のダッシュボードに使用されるデータは、接続またはファイルロギングを有効にするアクセス コントロール ルールから収集されます。ダッシュボードには、ロギングが有効になっていないルールと一致するトラフィックは反映されません。自分にとって重要な情報をログに記録するルールを設定してください。また、ユーザー情報はユーザー ID を収集するアイデンティティルールを設定している場合にのみ利用できます。さらに、侵入、ファイル、マルウェア、および Web カテゴリの情報は、それらの機能のライセンスがあり、機能を使用するルールを設定している場合のみ使用できます。

手順

- ステップ 1** メイン メニューの [モニタリング (Monitoring)] をクリックして、[ダッシュボード (Dashboards)] ページを開きます。

ダッシュボードのグラフと表に表示されるデータを制御するために、定義済みの時間範囲（最後の時間や週など）を選択できます。また、特定の開始時刻と終了時刻を指定してカスタムの時間範囲を定義することもできます。

トラフィック関連のダッシュボードには、次のタイプの表示が含まれます。

- 上位 5 つの棒グラフ：これらのグラフは [ネットワークの概要 (Network Overview)] ダッシュボードに表示されます。また、ダッシュボードテーブルで項目をクリックした場合、項目ごとのサマリーのダッシュボードにも表示されます。[トランザクション (Transactions)] または [データの usage (Data Usage)] (送受信バイトの合計) のカウント間で情報を切り替えることができます。すべてのトランザクション、許可トランザクション、または拒否トランザクションを表示するために表示を切り替えることもできます。グラフと関連付けられている表を確認する場合は、[追加表示 (View More)] をクリックします。

- 表：表には特定のタイプ（アプリケーションや Web カテゴリなど）の項目が、その項目の合計トランザクション、許可トランザクション、ブロックされたトランザクション、データの使用状況、送受信バイト数とともに表示されます。raw [値 (Values)] と [パーセンテージ (Percentages)] 間の数字は切り替えることができ、上位 10、100、または 1000 エントリが表示されます。項目がリンクの場合、そのリンクをクリックして、より詳細な情報が含まれているサマリー ダッシュボードを表示します。

ステップ 2 目次にある [ダッシュボード (Dashboard)] リンクをクリックして、次のデータのダッシュボードを表示します。

- [ネットワークの概要 (Network Overview)]：ネットワークのトラフィックに関する概要情報が表示されます。情報には、一致したアクセスルール（ポリシー）、ユーザーが送信側のトラフィック、接続で使用されているアプリケーション、一致した侵入シグネチャ、アクセスされた URL の Web カテゴリ、最も頻繁に接続されている宛先が含まれます。
- [ユーザー (Users)]：ネットワークの上位ユーザーが表示されます。ユーザー情報を表示するには、アイデンティティ ポリシーを設定する必要があります。
- [アプリケーション (Applications)]：ネットワークで使用されている上位アプリケーション（Facebook など）が表示されます。この情報は、インスペクションを実行済みの接続にのみ提供されます。接続は、「許可」ルールと一致するか、またはゾーン、アドレス、およびポート以外の基準を使用するブロックルールと一致するかどうかのインスペクションが実行されます。そのため、インスペクションが必要なルールにヒットする前に接続が信頼またはブロックされている場合、アプリケーション情報は使用できません。
- [Web カテゴリ (Web Categories)]：訪問した Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトの上位カテゴリ（ギャンブルや教育機関など）が表示されます。この情報を取得するためには、トラフィックの一致基準として Web カテゴリを使用するアクセスコントロールルールが少なくとも 1 つ必要です。情報は、ルールに一致するトラフィック、またはルールに一致するかどうかを判断するためにインスペクションを実行する必要があるトラフィックに関してのみ提供されます。最初の Web カテゴリのアクセスコントロールルールよりも前にあるルールと一致する接続に関するカテゴリ（またはレピュテーション）情報は表示されません。
- [ポリシー (Policies)]：一致する上位のアクセスルールがネットワークトラフィック別に表示されます。
- [入力ゾーン (Ingress Zones)]：デバイスに入るトラフィックが通過する上位のセキュリティゾーンが表示されます。
- [出力ゾーン (Egress Zones)]：デバイスから出るトラフィックが通過する上位のセキュリティゾーンが表示されます。
- [宛先 (Destinations)]：ネットワークトラフィックの上位の宛先が表示されます。
- [攻撃者 (Attackers)]：侵入イベントをトリガーする接続の送信元である上位の攻撃者が表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [ターゲット (Targets)]：攻撃の被害者である、侵入イベントの上位のターゲットが表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。

- [脅威 (Threats)] トリガーされた上位の侵入ルールが表示されます。この情報を表示するには、アクセスルールに侵入ポリシーを設定する必要があります。
- [ファイルログ (File Logs)] : ネットワークトラフィックで確認された上位のファイルタイプが表示されます。この情報を表示するには、アクセスルールにファイルポリシーを設定する必要があります。
- [システム (System)] : インターフェイスとインターフェイスのステータス (IP アドレスを確認するには、そのインターフェイスにマウスオーバーします)、システムの全体的なスループット、およびシステム イベント、CPU 使用率、メモリ使用率、ディスク使用率に関する概要情報など、システムの全体的情報が表示されます。すべてのインターフェイスではなく特定のインターフェイスを表示するように、スループットグラフを制限できます。

(注) [システム (System)] ダッシュボードに表示される情報は、全体的なシステムレベルの情報です。デバイスの CLI にログインすると、さまざまなコマンドを使用して詳細情報を確認できます。たとえば、**show cpu** および **show memory** コマンドには、他の詳細を示すパラメータが含まれますが、これらのダッシュボードには **show cpu system** および **show memory system** コマンドからのデータが表示されます。

ステップ 3 目次でこれらのリンクをクリックすることもできます。

- [イベント (Events)] : イベント発生時にイベントが表示する場合に選択します。個々のアクセスルールに関連する接続イベントを表示するには、それぞれのアクセスルールで接続のロギングを有効にする必要があります。これらのイベントは、ユーザーの接続の問題を解決するのに役立ちます。



第 3 章

KVM を使用した ASA の導入

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

- [KVM での ASA のガイドラインで制限事項 \(35 ページ\)](#)
- [KVM を使用した ASA の導入について \(36 ページ\)](#)
- [ASA と KVM の前提条件 \(36 ページ\)](#)
- [第 0 日のコンフィギュレーションファイルの準備 \(38 ページ\)](#)
- [仮想ブリッジ XML ファイルの準備 \(40 ページ\)](#)
- [ASA の起動 \(41 ページ\)](#)
- [KVM での ASA のパフォーマンス調整 \(42 ページ\)](#)
- [CPU 使用率とレポート \(48 ページ\)](#)

KVM での ASA のガイドラインで制限事項

ASA の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。作成する各仮想アプライアンスには、ホストマシン上での最小リソース割り当て (メモリ、CPU 数、およびディスク容量) が必要です。

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。

KVM での ASA のシステム要件

最適なパフォーマンスを確保するために、以下の仕様に準拠していることを確認してください。ASA には、次の要件があります。

- ホスト CPU は、仮想化拡張機能を備えたサーバークラスの x86 ベースの Intel または AMD CPU である必要があります。

たとえば、ASA パフォーマンステストラボでは、2.6GHz で動作する Intel® Xeon® CPU E5-2690v4 プロセッサを搭載した Cisco Unified Computing System™ (Cisco UCS®) C シリーズ M4 サーバーを最低限使用しています。

CPU ピニング

KVM 環境で ASA を機能させるには、CPU ピニングが必要です。[CPU ピニングの有効化 \(42 ページ\)](#) を参照してください。

ハイアベイラビリティガイドラインのためのフェールオーバー

フェールオーバー配置の場合は、スタンバイ装置が同じモデルライセンスを備えていることを確認してください（たとえば、両方の装置が ASA30s であることなど）。

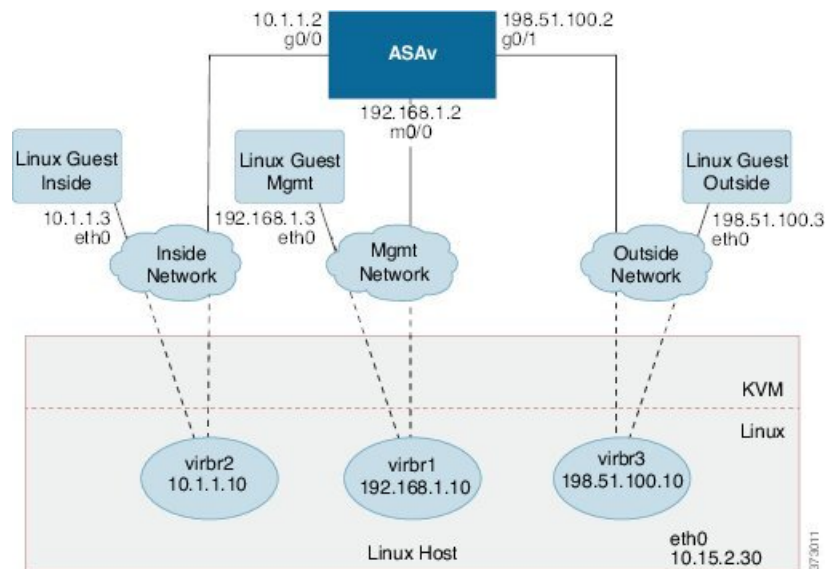


重要 ASA を使用して高可用性ペアを作成する場合は、データインターフェイスを各 ASA に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASA に追加されると、ASA コンソールにエラーが表示されることがあります。また、フェールオーバー機能にも影響が出る可能性があります。

KVM を使用した ASA の導入について

次の図は、ASA と KVM のネットワークトポロジの例を示します。この章で説明している手順は、このトポロジの例に基づいています。ASA 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 ASA の導入例



ASA と KVM の前提条件

- Cisco.com から ASA qcw2 ファイルをダウンロードし、Linux ホストに格納します。

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



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

- このマニュアルの導入例では、ユーザーが Ubuntu 14.04 LTS を使用していることを前提としています。Ubuntu 14.04 LTS ホストの最上部に次のパッケージをインストールします。
 - qemu-kvm
 - libvirt bin
 - bridge-utils
 - Virt-Manager
 - virtinst
 - virsh tools
 - genisoimage
- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での ASA のスループットを最大化できます。一般的なホスト調整の概念については、『[NFV Delivers Packet Processing Performance with Intel](#)』を参照してください。
- Ubuntu 14.04 の便利な最適化には、次のものが含まれます。
 - macvtap : 高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
 - Transparent Huge Pages : メモリページサイズを増加させます。Ubuntu 14.04 では、デフォルトでオンになっています。
Hyperthread disabled : 2 つの vCPU を 1 つのシングルコアに削減します。
 - txqueuelength : デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップレートを低減します。
 - pinning : qemu および vhost プロセスを特定の CPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。
- RHEL ベースのディストリビューションの最適化については、『[Red Hat Enterprise Linux 7 Virtualization Tuning and Optimization Guide](#)』を参照してください。
- ASA ソフトウェアおよび ASA ハイパーバイザの互換性については、『[Cisco ASA の互換性 \[英語\]](#)』を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

ASAv を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、ASAv の起動時に適用される ASAv の設定を含むテキストファイルです。この初期設定は、「day0-config」というテキストファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。第 0 日コンフィギュレーションファイルには、少なくとも、管理インターフェイスをアクティブ化するコマンドと、公開キー認証用 SSH サーバーを設定するコマンドを含める必要がありますが、すべての ASA 設定を含めることもできます。

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

- 初期導入時に自動的に ASAv にライセンスを付与するには、Cisco Smart Software Manager からダウンロードした Smart Licensing Identity (ID) トークンを「idtoken」というテキストファイルに格納し、第 0 日構成ファイルと同じディレクトリに保存します。
- トランスペアレントモードで ASAv を導入する場合は、トランスペアレントモードで実行される既知の ASA 構成ファイルを、第 0 日構成ファイルとして使用する必要があります。これは、ルーテッドファイアウォールの第 0 日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

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

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

例：

```
ASA Version 9.4.1
!
console serial
interface management0/0
nameif management
security-level 100
ip address 192.168.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
```

```
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
```

ステップ 2 (任意) ASA の初期導入時に自動的にライセンスを許諾する場合は、`day0-config` ファイルに次の情報が含まれていることを確認してください。

- 管理インターフェイスの IP アドレス
- (任意) SSmart Licensing で使用する HTTP プロキシ
- HTTP プロキシ (指定した場合) または `tools.cisco.com` への接続を有効にする `route` コマンド
- `tools.cisco.com` を IP アドレスに解決する DNS サーバー
- 要求する ASA ライセンスを指定するための Smart Licensing の設定
- (任意) CSSM での ASA の検索を容易にするための一意のホスト名

ステップ 3 (任意) Cisco Smart Software Manager によって発行された Smart License ID トークンファイルをコンピュータにダウンロードし、ダウンロードファイルから ID トークンをコピーし、ID トークンのみを含む「`idtoken`」というテキストファイルを作成します。

ステップ 4 テキスト ファイルを ISO ファイルに変換して仮想 CD-ROM を生成します。

例 :

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

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

ステップ 5 ステップ 1 から 5 を繰り返し、導入する ASA ごとに、適切な IP アドレスを含むデフォルトの構成ファイルを作成します。

仮想ブリッジ XML ファイルの準備

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



(注) この手順では、KVM ホストから外部への接続は確立されません。

KVM ホスト上に仮想ブリッジ XML ファイルを準備します。[第 0 日のコンフィギュレーション ファイルの準備 \(38 ページ\)](#) 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

ステップ 1 3 つの仮想ネットワーク ブリッジ XML ファイルを作成します。次の例では、virbr1.xml、virbr2.xml、および virbr3.xml です。

例 :

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

例 :

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

例 :

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

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

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

ステップ 3 このスクリプトを実行して、仮想ネットワークを設定します。このスクリプトは、仮想ネットワークを稼働状態にします。ネットワークは、KVM ホストが動作している限り稼働します。

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

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

ステップ 4 仮想ネットワークが作成されたことを確認します。

```
stack@user-ubuntu:~/KvmAsa$ brctl show
bridge name bridge id STP enabled Interfaces
virbr0 8000.00000000000000 yes
virbr1 8000.5254000056eed yes virb1-nic
virbr2 8000.5254000056eee yes virb2-nic
virbr3 8000.5254000056eec yes virb3-nic
stack@user-ubuntu:~/KvmAsa$
```

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

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

ASA の起動

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

手順

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

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

ASA では最大 10 のネットワークがサポートされます。この例では 3 つのネットワークが使用されています。ネットワークブリッジの句の順序は重要です。リストの最初の句は常に ASA の管理インターフェイス (Management 0/0)、2 番目の句は ASA の GigabitEthernet 0/0、3 番目の句は ASA の GigabitEthernet 0/1 に該当し、GigabitEthernet 0/8 まで同様に続きます。仮想 NIC は Virtio でなければなりません。

例 :

```

virt-install \
--connect=qemu:///system \
--network network=default,model=virtio \
--network network=default,model=virtio \
--network network=default,model=virtio \
--name=asav \
--cpu host \
--arch=x86_64 \
--machine=pc-1.0 \
--vcpus=1 \
--ram=2048 \
--os-type=linux \
--virt-type=kvm \
--import \
--disk path=/home/kvmparf/Images/desmo.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
\
--disk path=/home/kvmparf/asav_day0.iso,format=iso,device=cdrom \
--console pty,target_type=virtio \
--serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet

```

ステップ 2 virt_install スクリプトを実行します。

例 :

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

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

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

KVM での ASA のパフォーマンス調整

KVM 構成でのパフォーマンスの向上

KVM ホストの設定を変更することによって、KVM 環境内の ASA のパフォーマンスを向上させることができます。これらの設定は、ホストサーバー上の構成時の設定とは無関係です。このオプションは、Red Hat Enterprise Linux 7.0 KVM で使用できます。

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

CPU ピニングの有効化

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

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



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

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

手順

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

例：

```
virsh nodeinfo
```

ステップ 2 使用可能な vCPU の数を確認します。

例：

```
virsh capabilities
```

ステップ 3 vCPU をプロセッサ コアのセットにピンニングします。

例：

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

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

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

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

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

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

NUMA のガイドライン

Non-uniform Memory Access (NUMA) は、マルチプロセッサシステムのプロセッサに対するメインメモリモジュールの配置について記述する共有メモリアーキテクチャです。プロセッサが自身のノード（リモートメモリ）内に存在しないメモリにアクセスする場合は、ローカルメモリにアクセスする場合よりも低速の速度で、NUMA 接続を介してデータを転送する必要があります。

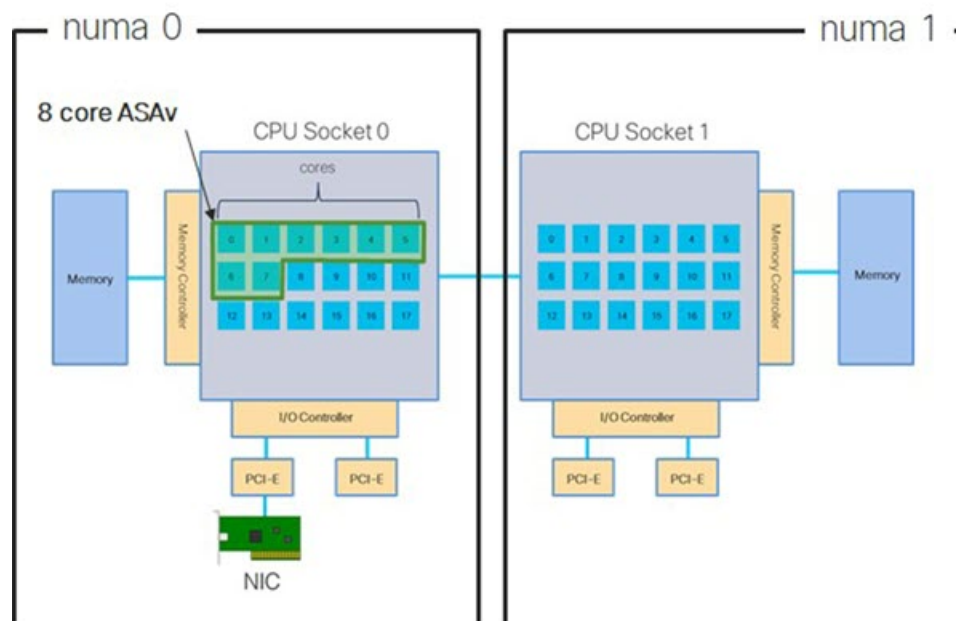
X86 サーバーアーキテクチャは、複数のソケットおよびソケット内の複数のコアで構成されています。各 CPU ソケットとそのメモリおよび I/O が、NUMA ノードと呼ばれます。メモリからパケットを効率的に読み取るには、ゲストアプリケーションおよび関連付けられている周辺機器（NIC など）が同じノード内に存在する必要があります。

最適な ASA のパフォーマンスを実現するには：

- ASA マシンは、1つの NUMA ノード上で実行する必要があります。1つの ASA が 2つのソケットで実行されるように導入されている場合、パフォーマンスは大幅に低下します。
- 8 コア ASA（[図 2: 8 コア ASA NUMA アーキテクチャの例 \(44 ページ\)](#)）では、ホスト CPU の各ソケットが、それぞれ 8 個以上のコアを備えている必要があります。サーバー上で実行されている他の VM についても考慮する必要があります。
- NIC は、ASA マシンと同じ NUMA ノード上にある必要があります。

次の図は、2つの CPU ソケットがあり、各 CPU に 18 個のコアが搭載されているサーバーを示しています。8 コア ASA では、ホスト CPU の各ソケットに最低 8 個のコアが必要です。

図 2: 8 コア ASA NUMA アーキテクチャの例



NUMA の最適化

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

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

ノード 0 への配置：

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

ノード 1 への配置：

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

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

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

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

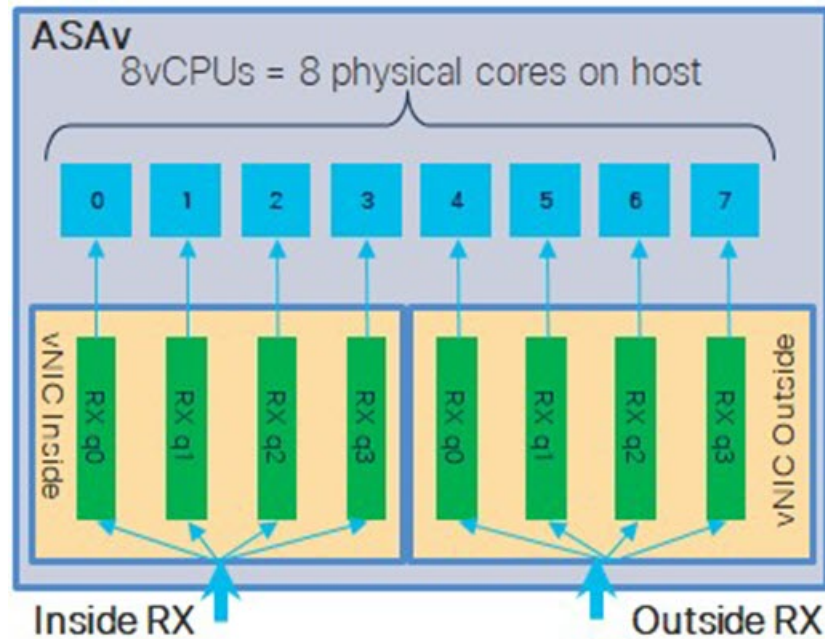
ASAv は、複数のプロセッサコアにネットワーク受信トラフィックを分散するためにネットワークアダプタによって使用されるテクノロジーである Receive Side Scaling (RSS) をサポートしています。最大スループットを実現するには、各 vCPU (コア) に独自の NIC RX キューが設定されている必要があります。一般的な RA VPN 展開では、1つの内部/外部ペアのインターフェイスを使用する場合があることに注意してください。



重要 複数の RX キューを使用するには、ASAv バージョン 9.13(1) 以降が必要です。KVM の場合、*libvirt* のバージョンは 1.0.6 以降である必要があります。

内部/外部ペアのインターフェイスを持つ 8 コア VM の場合、[図 3: 8 コア ASA RSS RX キュー \(46 ページ\)](#) に示すように、各インターフェイスには 4 つの RX キューがあります。

図 3: 8 コア ASA RSS RX キュー



次の表に、KVM 用の ASA の vNIC およびサポートされている RX キューの数を示します。サポートされている vNIC の説明については、[#unique_28 unique_28_Connect_42_section_pht_vfh_glb](#) を参照してください。

表 8: KVM で推奨される NIC/vNIC

NIC カード	vNIC ドライバ	ドライバテクノロジー	RX キューの数	パフォーマンス
x710	i40e	PCI パススルー	8 (最大)	x710 の PCI パススルーおよび SR-IOV モードは、最適なパフォーマンスを提供します。通常、仮想展開では、複数の VM 間で NIC を共有できるため、SR-IOV が推奨されます。
	i40evf	SR-IOV	8	

NIC カード	vNIC ドライバ	ドライバテクノロジー	RX キューの数	パフォーマンス
x520	ixgbe	PCI パススルー	6	x520 NIC は、x710 よりも 10 ～ 30% パフォーマンスが低くなります。X520 の PCI パススルーおよび SR-IOV モードは、同様のパフォーマンスを提供します。通常、仮想展開では、複数の VM 間で NIC を共有できるため、SR-IOV が推奨されます。
	ixgbe-vf	SR-IOV	2	
該当なし	virtio	準仮想化	8 (最大)	ASAv100 には推奨されません。その他の展開については、 KVM での Virtio のマルチキューサポートの有効化 (47 ページ) を参照してください。

KVM での Virtio のマルチキューサポートの有効化

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

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



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

VPN の最適化

ASAv で VPN パフォーマンスを最適化するための追加の考慮事項は、次のとおりです。

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

CPU 使用率とレポート

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

ASA Virtual の vCPU 使用率

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

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

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

CPU 使用率の例

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

例

```
Ciscoasa#show cpu usage
CPU 500005000 1% 1000 2% 5000 1%
```

報告された vCPU の使用率が大幅に異なる例を次に示します。

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

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

KVM CPU 使用率レポート

値は、

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

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

OProfile、top などのツールを実行すると、ハイパーバイザと VM の両方の CPU 使用率を含む、特定の KVM VM の合計 CPU 使用率が表示されます。同様に、Xen VMM に固有の XenMon などのツールの場合、Xen ハイパーバイザ、つまり Dom0 の合計 CPU 使用率が表示されますが、VM ごとのハイパーバイザ使用率には分割されません。

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

ASA Virtual と KVM のグラフ

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

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

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

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

KVM では「%CPU usage」は次のように計算されます。

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

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

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



第 4 章

AWS クラウドへの ASA v の導入

Amazon Web Services (AWS) クラウドに ASA v を導入できます。

- [AWS クラウドへの ASA v の導入について \(51 ページ\)](#)
- [ASA v と AWS の前提条件 \(52 ページ\)](#)
- [ASA v および AWS のガイドラインと制限事項 \(53 ページ\)](#)
- [設定の移行と SSH 認証 \(54 ページ\)](#)
- [AWS 上の ASA v のネットワークトポロジの例 \(55 ページ\)](#)
- [AWS での ASA v の展開 \(55 ページ\)](#)

AWS クラウドへの ASA v の導入について

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

ASA v は、次の AWS インスタンスタイプをサポートしています。

表 9: AWS でサポートされているインスタンスタイプ

インスタンス	属性			ASA v モデルのサポート	注
	vCPU	メモリ (GB)	インターフェイスの最大数		
c3.large	2	3.75	3	• ASA v10 • ASA v30	リソースのアンダープロビジョニングのため、large インスタンスでの ASA v30 の使用は推奨されません。
c4.large	2	3.75	3		
m4.large	2	8	2		

インスタンス	属性			ASA モデルのサポート	注
	vCPU	メモリ (GB)	インターフェイスの最大数		
c3.xlarge	4	7.5	4	ASA30	xlarge インスタンスでサポートされるのは ASA30 のみです。
c4.xlarge	4	7.5	4		
m4.xlarge	4	16	4		

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



重要 AMI イメージは AWS 環境の外部ではダウンロードできません。

ASA と AWS の前提条件

- aws.amazon.com でアカウントを作成します。
- ASA へのライセンス付与。ASA にライセンスを付与するまでは、100 回の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「[ASA のライセンス \(1 ページ\)](#)」を参照してください。
- インターフェイスの要件：
 - 管理インターフェイス
 - 内部および外部インターフェイス
 - (任意) 追加のサブネット (DMZ)
- 通信パス：
 - 管理インターフェイス：ASDM に ASA 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 ASA 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)：ASA をパブリック ネットワークに接続するために使用されます。
 - DMZ インターフェイス (任意)：c3.xlarge インターフェイスを使用する場合、DMZ ネットワークに ASA を接続するために使用されます。

- ASA システム要件については、[Cisco ASA の互換性 \[英語\]](#) を参照してください。

ASA および AWS のガイドラインと制限事項

サポートされる機能

AWS 上の ASA は、次の機能をサポートしています。

- 次世代の Amazon EC2 Compute Optimized インスタンスファミリーである Amazon EC2 C5 インスタンスのサポート
- 仮想プライベートクラウド (VPC) への導入
- 拡張ネットワーク (SR-IOV) (使用可能な場合)
- Amazon マーケットプレイスからの導入
- インスタンスあたり最大 4 つの vCPU
- L3 ネットワークのユーザー導入
- ルーテッドモード (デフォルト)
- Amazon CloudWatch

サポートされない機能

AWS 上の ASA は、以下の機能をサポートしていません。

- コンソールアクセス (管理は、ネットワークインターフェイスを介して SSH または ASDM を使用して実行される)
- VLAN
- 無差別モード (スニファなし、またはトランスペアレントモードのファイアウォールのサポート)
- マルチ コンテキスト モード
- クラスタ
- ASA ネイティブ HA
- EtherChannel は、ダイレクト物理インターフェイスのみでサポートされる
- VM のインポート/エクスポート
- ハイパーバイザに非依存のパッケージ
- VMware ESXi
- ブロードキャスト/マルチキャスト メッセージ

これらのメッセージは AWS 内で伝播されないため、ブロードキャスト/マルチキャストを必要とするルーティングプロトコルは AWS で予期どおりに機能しません。VXLAN はスタティックピアでのみ動作できます。

- Gratuitous/非要請 ARP

これらの ARPS は AWS 内では受け入れられないため、Gratuitous ARP または非要請 ARP を必要とする NAT 設定は期待どおりに機能しません。

- IPv6

設定の移行と SSH 認証

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

次は、ユーザー名「admin」の元の設定例です。

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

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

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

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

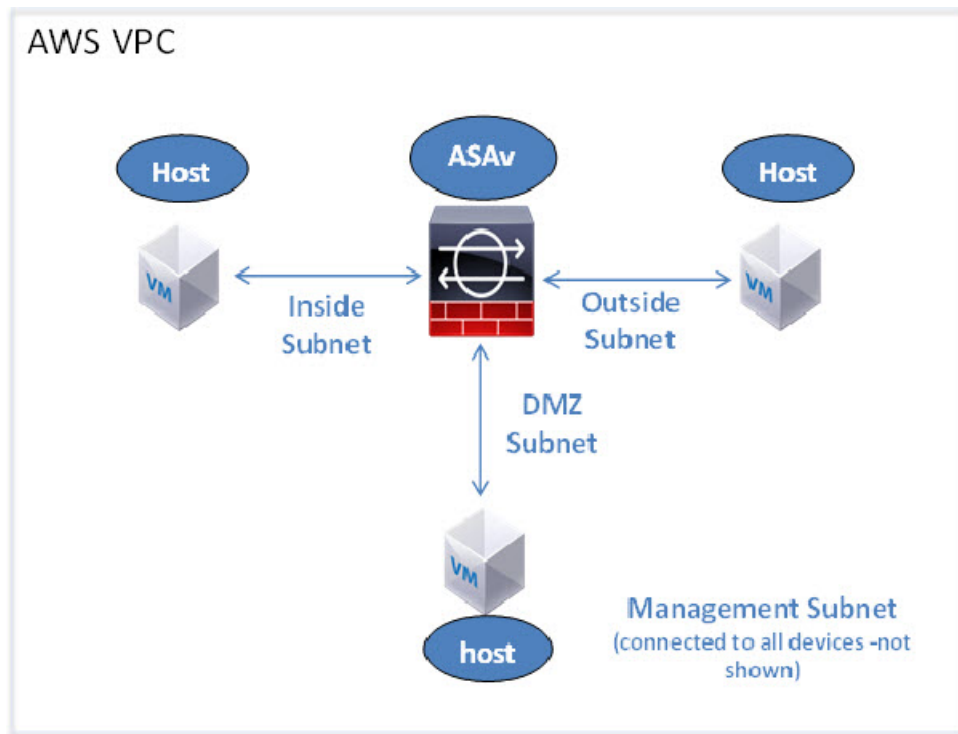
アップグレード後は、**username** コマンドに対する **password** または **nopassword** キーワードの指定は任意となり、ユーザーがパスワードを入力できなくするよう指定できるようになります。よって、公開キー認証のみを強制的に使用する場合は、**username** コマンドを入力しなおします。

```
username admin privilege 15
```

AWS 上の ASA のネットワークトポロジの例

次の図は、ASA 用に AWS 内で設定された 4 つのサブネット（管理、内部、外部、および DMZ）を備えたルーテッドファイアウォールモードの ASA の推奨トポロジを示しています。

図 4: AWS への ASA の導入例



AWS での ASA の展開

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

手順

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

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

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

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

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

- AMI（たとえば、Ubuntu Server 14.04 LTS）を選択します。
イメージ配信通知で識別された AMI を使用します。
- ASAv でサポートされるインスタンスタイプ（c3.large など）を選択します。
- インスタンスを設定します（CPU とメモリは固定です）。
- [高度な詳細（Advanced Details）] セクションを導入し、[ユーザーデータ（User data）] フィールドに、オプションで第 0 日用構成を入力できます。これは、ASAv の起動時に適用される ASAv 構成を含むテキスト入力です。第 0 日用構成にスマートライセンスなどの詳細情報を設定する方法の詳細については、「[第 0 日のコンフィギュレーションファイルの準備](#)」を参照してください。
 - **管理インターフェイス**：第 0 日用構成を選択する場合は、管理インターフェイスの詳細を指定する**必要**があります。これは DHCP を使用するよう設定する必要があります。
 - **データインターフェイス**：データインターフェイスの IP アドレスは、その情報を第 0 日用構成の一部として指定した場合にのみ割り当てられ、設定されます。データインターフェイスは、DHCP を使用するよう設定できます。または、接続するネットワークインターフェイスがすでに作成されていて、IP アドレスがわかっている場合は、第 0 日用構成で IP の詳細を指定できます。
 - **第 0 日用構成なし**：第 0 日用構成を指定せずに ASAv を導入すると、ASAv はデフォルトの ASAv 構成を適用し、AWS メタデータサーバーから接続されたインターフェイスの IP を取得し、IP アドレスを割り当てます（データインターフェイスに IP は割り当てられますが、ENI はダウンします）。Management0/0 インターフェイスが起動し、DHCP アドレスで設定された IP を取得します。Amazon EC2 および Amazon VPC の IP アドレッシングについては、「[VPC での IP アドレッシング](#)」を参照してください。

• **第 0 日用構成の例**：

```
! ASA Version 9.x.1.200
!
```

```

interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shutdown
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh ::/0 management
ssh timeout 60
ssh version 2
username admin password Qlw2e3r4 privilege 15
username admin attributes
service-type admin
aaa authentication ssh console LOCAL
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list allow-all extended permit ip any any
access-list allow-all extended permit ip any6 any6
access-group allow-all global
!
interface G0/0
nameif outside
ip address dhcp setroute

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

no shutdown
!

```

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

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

- 設定を確認し、[Launch] をクリックします。

ステップ 4 キー ペアを作成します。

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

- ステップ 5** [インスタンスの起動 (Launch Instance)] をクリックして、ASA を導入します。
- ステップ 6** [My Account] > [AWS Management Console] > [EC2] > [Launch an Instance] > [My AMIs] をクリックします。
- ステップ 7** ASA のインターフェイスごとに [送信元または宛先の確認 (Source/Destination Check)] が無効になっていることを確認します。

AWS のデフォルト設定では、インスタンスはその IP アドレス (IPv4) のトラフィックのみを受信でき、インスタンスは独自の IP アドレス (IPv4) からのみトラフィックを送信できます。ASA のルーテッドホップとしての動作を有効にするには、ASA の各トラフィック インターフェイス (内部、外部、および DMZ) の [送信元または宛先の確認 (Source/Destination Check)] を無効にする必要があります。



第 5 章

Microsoft Azure クラウドへの ASA の導入

Microsoft Azure クラウドに ASA を導入できます。

- [Microsoft Azure クラウドへの ASA 導入について \(59 ページ\)](#)
- [ASA および Azure の前提条件およびシステム要件 \(60 ページ\)](#)
- [注意事項と制約事項 \(61 ページ\)](#)
- [導入時に作成されるリソース \(63 ページ\)](#)
- [Azure ルーティング \(65 ページ\)](#)
- [仮想ネットワーク内の VM のルーティング設定 \(66 ページ\)](#)
- [IP アドレス \(66 ページ\)](#)
- [DNS \(67 ページ\)](#)
- [Microsoft Azure への ASA の導入 \(67 ページ\)](#)

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

表 10: ASA 権限付与に基づくライセンス機能の制限

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

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

次の方法で Microsoft Azure に ASA を導入できます。

- 標準的な Azure パブリック クラウドおよび Azure Government 環境で、Azure Resource Manager を使用してスタンドアロンファイアウォールとして導入

ASA および Azure の前提条件およびシステム要件

- [Azure.com](https://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 ASA を選択し、ASA を導入できます。

- ASA へのライセンス付与。

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



(注) Azure に導入する場合、ASA にはデフォルトで ASA30 の権限が付与されています。ASA5、ASA10、ASA30、ASA50、および ASA100 の権限付与の使用が許可されています。ただし、ASA5、ASA10、ASA30、ASA50、および ASA100 の権限付与を使用するためには、スループットレベルを明示的に設定する必要があります。

- インターフェイスの要件：

4 つのネットワーク上の 4 つのインターフェイスとともに ASA を導入する必要があります。任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、[パブリック IP アドレス \[英語\]](#) を参照してください。

- 管理インターフェイス：

Azure では、最初に定義されたインターフェイスが常に管理インターフェイスです。そして、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 ASA 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、[management-only] の設定は含まれていません。

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

注意事項と制約事項

サポートされる機能

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



(注) Azure では L2 vSwitch 機能は設定できません。

- インターフェイスのパブリック IP アドレス

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

- ルーテッドファイアウォール モード（デフォルト）



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

既知の問題

アイドル タイムアウト

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



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

プライマリ ASA からスタンバイ ASA へのフェールオーバー

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

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



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

サポートされない機能

- コンソールアクセス（管理は、ネットワーク インターフェイスを介して SSH または ASDM を使用して実行される）
- ユーザー インスタンス インターフェイスの VLAN タギング
- ジャンボ フレーム
- Azure の観点からの、デバイスが所有していない IP アドレスのプロキシ ARP
- 無差別モード（スニファなし、またはトランスペアレントモードのファイアウォールのサポート）



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

- マルチ コンテキスト モード
- クラスタ
- ASA ネイティブ HA。



(注) ステートレスのアクティブ/バックアップ高可用性 (HA) 設定で ASA を Azure に展開できます。

- 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 ASA の FIPS モードは無効になっています。



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

- IPv6

Azure DDoS Protection 機能

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

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

導入時に作成されるリソース

Azure に ASA を展開すると、次のリソースが作成されます。

- ASA マシン
- リソース グループ (既存のリソース グループを選択していない場合)
ASA リソースグループは、仮想ネットワークとストレージアカウントで使用するリソースグループと同じである必要があります。
- vm name-Nic0、vm name-Nic1、vm name-Nic2、vm name-Nic3 という名前の 4 つの NIC
これらの NIC は、それぞれ ASA インターフェイスの Management 0/0、GigabitEthernet 0/0、GigabitEthernet 0/1、および GigabitEthernet 0/2 にマッピングされます。



(注) 要件に基づいて、IPv4 のみで VNet を作成できます。

- VM 名-SSH-SecurityGroup という名前のセキュリティ グループ
セキュリティグループは、ASA Management 0/0 にマッピングされる VM の Nic0 にアタッチされます。
セキュリティグループには、VPN 目的で SSH、UDP ポート 500、および UDP 4500 を許可するルールが含まれます。導入後に、これらの値を変更できます。
- パブリック IP アドレス (展開時に選択した値に従って命名)。
パブリック IP アドレス (IPv4 のみ)。
任意のインターフェイスにパブリック IP アドレスを割り当てることができます。パブリック IP アドレスの作成、変更、削除など、パブリック IP に関する Azure のガイドラインについては、「[パブリック IP アドレス](#)」を参照してください。
- 4 つのサブネットを備えた仮想ネットワーク (既存のネットワークを選択していない場合)
- サブネットごとのルーティング テーブル (既存の場合は最新のもの)
このテーブルの名前は、サブネット名-ASA-RouteTable です。
各ルーティングテーブルには、ASA 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、ブローブ (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ーブおよびコンテナ VHD にある 2 つのファイル (名前は、vm name-disk.vhd および vm name-<uuid>.status)
- ストレージアカウント (既存のストレージアカウントが選択されていない場合)



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

Azure ルーティング

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



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

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

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

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

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

仮想ネットワーク内の VM のルーティング設定

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

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



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

IP アドレス

次の情報は Azure の IP アドレスに適用されます。

- ASA インターフェイスの IP アドレスを設定するには、DHCP を使用する必要があります。
- Azure インフラストラクチャは、Azure に設定された IP アドレスが確実に ASA インターフェイスに割り当てられるように動作します。
- Management 0/0 には、それが接続されているサブネット内のプライベート IP アドレスが割り当てられます。
- パブリック IP アドレスは、プライベート IP アドレスに関連付けられる場合があり、Azure インターネットゲートウェイは NAT 変換を処理します。
- 任意のインターフェイスにパブリック IP アドレスを割り当てることができます。
- ダイナミックパブリック IP アドレスは Azure の停止/開始サイクル中に変更される場合があります。ただし、Azure の再起動時および ASA のリロード時には、パブリック IP アドレスは保持されます。
- スタティックパブリック IP アドレスは Azure 内でそれらを変更するまで変わりません。

DNS

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

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

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

Microsoft Azure への ASA の導入

Microsoft Azure に ASA を導入できます。

- 標準的な Azure パブリッククラウドおよび Azure Government 環境で、Azure Resource Manager を使用してスタンドアロンファイアウォールとして ASA を導入します。「[Azure Resource Manager からの ASA の導入](#)」を参照してください。

Azure Resource Manager からの ASA の導入

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

Azure に ASA 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

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

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

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

ステップ 3 基本的な設定を行います。

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

重要 名前が一意でなく、既存の名前を再使用すると、導入に失敗します。

- b) ユーザー名を入力します。
- c) 認証タイプとして、[パスワード (Password)] または [SSH 公開キー (SSH public key)] を選択します。

[パスワード (Password)] を選択した場合は、パスワードを入力して確定します。

- d) サブスクリプションタイプを選択します。
- e) [Resource group] を選択します。

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

- f) 場所を選択します。

場所は、ネットワークおよびリソースグループと同じである必要があります。

- g) [OK] をクリックします。

ステップ 4 ASA の設定項目を設定します。

- a) 仮想マシンのサイズを選択します。

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

- b) ストレージアカウントを選択します。

既存のストレージアカウントを使用するほか、新規に作成することもできます。ストレージアカウントの場所はネットワークおよび仮想マシンと同じである必要があります。

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

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

- d) 必要に応じて、DNS のラベルを追加します。

完全修飾ドメイン名は、DNS ラベルと Azure URL の組み合わせで、`<dnslabel>.<location>.clouppapp.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) ASA を導入する 4 つのサブネットを設定し、[OK] をクリックします。

重要 各インターフェイスを一意的サブネットにアタッチする必要があります。

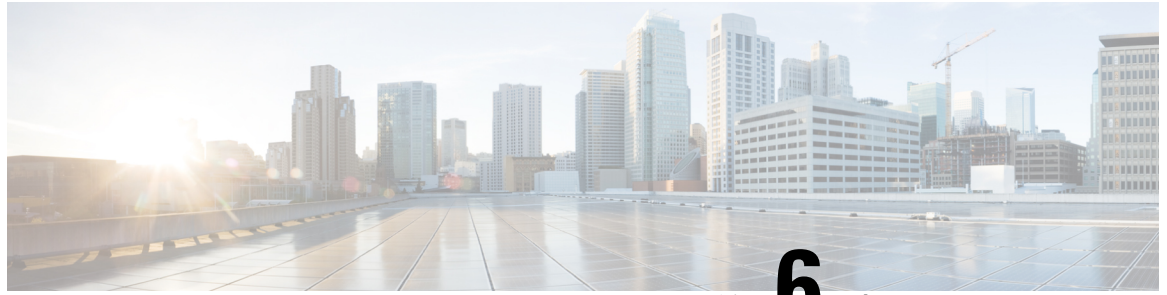
- g) [OK] をクリックします。

ステップ 5 構成サマリを確認し、[OK] をクリックします。

ステップ 6 利用条件を確認し、[作成 (Create)] をクリックします。

次のタスク

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



第 6 章

ASAv の設定

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

- [ASDM の起動 \(71 ページ\)](#)
- [ASDM を使用した初期設定の実行 \(72 ページ\)](#)
- [詳細設定 \(74 ページ\)](#)

ASDM の起動

手順

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

`https://asa_ip_address/admin`

次のボタンを持つ ASDM 起動ウィンドウが表示されます。

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

ステップ 2 ランチャをダウンロードするには、次の手順を実行します。

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

- c) インストーラをPCに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
- d) 管理IPアドレスを入力し、ユーザー名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証を有効にした場合、ユーザー名と関連付けられたパスワードを入力します。

ステップ 3 Java Web Start を使用するには：

- a) [Run ASDM] または [Run Startup Wizard] をクリックします。
- b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。
- c) ショートカットから Java Web Start を起動します。
- d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
- e) ユーザー名とパスワードを空白のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証を有効にした場合、ユーザー名と関連付けられたパスワードを入力します。

ASDM を使用した初期設定の実行

次の ASDM ウィザードおよび手順を使用して初期設定を行うことができます。

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

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

Startup Wizard の実行

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

手順

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

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

- ホスト名

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

(任意) ASA の内側にあるパブリックサーバーへのアクセス許可

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

(オプション) VPN ウィザードの実行

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

- サイト間 VPN ウィザード : ASA と別の VPN 対応デバイス間で IPsec サイト間トンネルを作成します。
- AnyConnect VPN ウィザード : Cisco AnyConnect VPN Client の SSL VPN リモートアクセスを設定します。AnyConnect クライアントでは ASA へのセキュアな SSL 接続が提供されるため、リモートユーザーによる企業リソースへのフル VPN トンネリングが可能になります。ASA ポリシーを設定すると、リモートユーザーが最初にブラウザを使用して接続するときに、AnyConnect クライアントをダウンロードできます。AnyConnect クライアント 3.0 以降を使用する場合、クライアントは、SSL または IPsec IKEv2 VPN プロトコルを実行できます。
- Clientless SSL VPN Wizard : ブラウザにクライアントレス SSL VPN リモートアクセスを設定します。クライアントレス ブラウザベース SSL VPN によって、ユーザーは Web ブラウザを使用して ASA へのセキュアなリモートアクセス VPN トンネルを確立できます。認証されると、ユーザーにはポータルページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザーにリ

ソースへのアクセス権限を付与します。ACLは、特定の企業リソースへのアクセスを制限したり、許可するために適用できます。

- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard : Cisco IPsec クライアント用の IPsec VPN リモートアクセスを設定します。

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

(オプション) ASDM の他のウィザードの実行

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

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

詳細設定

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

翻訳について

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