



# Microsoft Azure クラウドへの ASAv の導入

Microsoft Azure クラウドに ASAv を導入できます。



**重要** 9.13(1) 以降では、サポートされているすべての ASAv vCPU/メモリ構成ですべての ASAv ライセンスを使用できるようになりました。これにより、ASAv を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。また、サポート対象の Azure インスタンスタイプの数も増えます。

- [Microsoft Azure クラウドへの ASAv 導入について \(1 ページ\)](#)
- [ASAv および Azure の前提条件およびシステム要件 \(3 ページ\)](#)
- [注意事項と制約事項 \(4 ページ\)](#)
- [導入時に作成されるリソース \(6 ページ\)](#)
- [Azure ルーティング \(7 ページ\)](#)
- [仮想ネットワーク内の VM のルーティング設定 \(8 ページ\)](#)
- [IP アドレス \(9 ページ\)](#)
- [DNS \(9 ページ\)](#)
- [Microsoft Azure への ASAv の導入 \(9 ページ\)](#)

## Microsoft Azure クラウドへの ASAv 導入について

ASAv のニーズに合わせて Azure 仮想マシンの階層とサイズを選択します。すべての ASAv ライセンスを、サポートされているすべての ASAv vCPU/メモリ構成で使用できます。そのため、さまざまな Azure インスタンスタイプで ASAv を実行できます。

表 1: Azure 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		インターフェイス
	vCPU	メモリ (GB)	
D3、D3_v2、DS3、DS3_v2	4	14	4

インスタンス	属性		インターフェイス
	vCPU	メモリ (GB)	
D4、D4_v2、DS4、DS4_v2	8	28	8
D8_v3	8	32	4
F4、F4s	4	8	4
F8、F8s	8	16	8

表 2: ASA の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
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
- Azure Security Center を使用して統合パートナー ソリューションとして導入
- 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 を使用してハイ アベイラビリティ (HA) ペアとして導入

「[Azure Resource Manager からの ASA の導入 \(10 ページ\)](#)」を参照してください。標準的な Azure パブリッククラウドおよび Azure Government 環境で ASA HA 構成を導入できます。

# 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 2Gbps の権限が付与されています。100Mbps および 1Gbps の権限付与を使用できます。ただし、100Mbps または 1Gbps の権限付与を使用できるように、スループットレベルを明示的に設定する必要があります。

- インターフェイスの要件：

4 つのネットワーク上の 4 つのインターフェイスとともに 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。

- 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 には、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
- 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）内に配置されません。

- 選択したストレージアカウントのブロブおよびコンテナ VHD にある 2 つのファイル（名前は、*vm name-disk.vhd* および *vm name-<uuid>.status*）
- ストレージアカウント（既存のストレージアカウントが選択されていない場合）



---

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

---

## Azure ルーティング

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



---

(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。

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固有ルートが含まれます。

ASA を介してトラフィックをルーティングするために、ASA 導入プロセスで、ASA 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 ASA 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 ASA 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、ASA 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 ASA 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 ASA 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が指定されることがあります。これはプレースホルダーで、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 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ます。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 Security Center を使用して、Azure 内の統合パートナーソリューションとして ASA を導入します。セキュリティを重視するお客様には、Azure ワークロードを保護するため

のファイアウォールオプションとして ASA が提供されます。セキュリティイベントとヘルスイベントが単一の統合ダッシュボードからモニターされます。「[Azure Security Center からの ASA の導入](#)」を参照してください。

- Azure Resource Manager を使用して ASA 高可用性ペアを導入します。冗長性を確保するために、ASA をアクティブ/バックアップ高可用性 (HA) 設定で導入できます。パブリッククラウドでの HA では、アクティブな ASA の障害時に、バックアップ ASA へのシステムの自動フェールオーバーをトリガーできるステートレスなアクティブ/バックアップソリューションが実装されます。「[Azure Resource Manager からの ASA for High Availability の導入 \(13 ページ\)](#)」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 を使ってみる](#)』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。

**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。

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

**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。
- 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>.cloudapp.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 の開始](#)」を参照してください。

## Azure Security Center からの ASA の導入

Microsoft Azure Security Center は、お客様がクラウド導入に対するセキュリティリスクを防御、検出、および軽減できるようにする Azure 向けのセキュリティソリューションです。Security Center のダッシュボードから、セキュリティポリシーを設定したり、セキュリティ設定をモニターしたり、セキュリティアラートを表示したりできます。

Security Center は、Azure リソースのセキュリティ状態を分析して、潜在的なセキュリティの脆弱性を特定します。推奨事項のリストに従い、必要なコントロールを設定するプロセスを実行します。対象には、Azure のお客様に対するファイアウォールソリューションとしての ASA の導入を含めることができます。

Security Center の統合ソリューションのように、数クリックで ASAv をすばやく導入し、単一のダッシュボードからセキュリティイベントと正常性イベントをモニターできます。次の手順は、Security Center から ASAv を導入する手順の概要です。詳細については、『[Azure Security Center](#)』を参照してください。

**ステップ 1** Azure ポータルにログインします。

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

**ステップ 2** Microsoft Azure メニューから、[Security Center] を選択します。

初めて Security Center にアクセスする場合は、[Welcome] ブレードが開きます。[**Yes! I want to Launch Azure Security Center**] を選択して、[Security Center] ブレードを開き、データ収集を有効にします。

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

**ステップ 4** [Security policy] ブレードで、[Prevention policy] を選択します。

**ステップ 5** [Prevention policy] ブレードで、セキュリティ ポリシーの一部として表示する推奨事項をオンにします。

- a) [Next generation firewall] を [On] に設定します。これで、ASAv が Security Center 内の推奨ソリューションとなります。
- b) 必要に応じて、他の推奨事項を設定します。

**ステップ 6** [Security Center] ブレードに戻って、[Recommendations] タイルを選択します。

Security Center は、Azure リソースのセキュリティ状態を定期的に分析します。Security Center が潜在的なセキュリティの脆弱性を特定すると、[Recommendations] ブレードに推奨事項が表示されます。

**ステップ 7** [Recommendations] ブレードで [Add a Next Generation Firewall] 推奨事項を選択して、詳細を表示したり、問題を解決するためのアクションを実行したりします。

**ステップ 8** [新規作成 (Create New) ] または [既存のソリューションを使用 (Use existing solution) ] を選択してから、導入する ASAv をクリックします。

**ステップ 9** 基本的な設定を行います。

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

**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) 認証のタイプとして、パスワードまたは SSH キーのいずれかを選択します。

パスワードを選択した場合は、パスワードを入力して確定します。

- d) サブスクリプションタイプを選択します。
- e) リソース グループを選択します。

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

- f) 場所を選択します。

場所は、ネットワークおよびリソース グループと同じである必要があります。

g) [OK] をクリックします。

**ステップ 10** 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>.cloudapp.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 11** 構成サマリを確認し、[OK] をクリックします。

**ステップ 12** 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 の開始](#)」を参照してください。
- Security Center 内の推奨事項がどのように Azure リソースの保護に役立つかの詳細については、Security Center から入手可能な[マニュアル](#)を参照してください。

## Azure Resource Manager からの ASA for High Availability の導入

次の手順は、Microsoft Azure で高可用性 (HA) ASA ペアを設定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 を使ってみる](#)』を参照してください。

Azure の ASA HA では、2 つの ASA を可用性セットに導入し、リソース、パブリック IP アドレス、ルートテーブルなどの各種設定を自動的に生成します。導入後に、これらの設定をさらに管理できます。

**ステップ 1** Azure ポータルにログインします。

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

**ステップ 2** マーケットプレイスで [Cisco ASA] を検索し、[ASA 4 NIC HA] をクリックして、フェールオーバー ASA 構成を導入します。

**ステップ 3** [Basics] 設定を構成します。

a) ASA マシン名のプレフィックスを入力します。ASA の名前は「プレフィックス」-A と「プレフィックス」-B になります。

**重要** 既存のプレフィックスを使用していないことを確認します。使用すると、導入は失敗します。

b) ユーザー名を入力します。

これは両方の仮想マシンの管理ユーザー名です。

**重要** Azure では、admin というユーザー名は使用できません。

c) 両方の仮想マシンに認証タイプとして、[Password] または [SSH public key] のいずれかを選択します。  
[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。

[Create new] を選択して新しいリソースグループを作成するか、[Use existing] で既存のリソースグループを選択します。既存のリソースグループを使用する場合は、空である必要があります。そうでない場合は、新しいリソースグループを作成する必要があります。

f) [Location] 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** [Cisco ASA settings] を設定します。

a) 仮想マシンのサイズを選択します。

b) [Managed] または [Unmanaged OS disk] ストレージを選択します。

**重要** ASA HA モードでは常に [Managed] を使用します。

**ステップ 5** [ASA-A] 設定を構成します。

a) (オプション) [Create new] を選択して、[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。パブリック IP アドレスが必要な場合は、[None] を選択します。

(注) Azure は、VM を停止して再起動すると変更される可能性のある、ダイナミックパブリック IP をデフォルトでは作成しません。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。

b) 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>.cloudapp.azure.com` の形式になります。

c) ASA-A 起動時診断のストレージアカウントに必要な設定を構成します。

**ステップ 6** [ASAv-B] 設定についても、この手順を繰り返します。

**ステップ 7** 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。

a) 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。

b) [OK] をクリックします。

**ステップ 8** 構成の [Summary] を確認し、[OK] をクリックします。

**ステップ 9** 利用条件を確認し、[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 の開始](#)」を参照してください。
- Azure の ASA HA 構成の詳細については、『[ASA Series General Operations Configuration Guide](#)』の「Failover for High Availability in the Public Cloud」の章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。