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

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
D4、D4_v2、DS4、DS4_v2	8	36	8
D5、D5_v2、DS5、DS5_v2	16	72	8
D8_v3	8	32	4
D16_v3	16	64	4
F4、F4s	4	8	4
F8、F8s	8	16	8
F16、F16s	16	32	8

表 *2: ASAv* 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	**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 ASAv 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 ASAv の導入 （11 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 ASAv HA 構成を導入できます。

ASAv および Azure の前提条件およびシステム要件

- 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 ASAv を選択し、ASAv を導入できます。

- ASAv へのライセンス付与。

  ASAv 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 ASAv」を参照してください。

（注） Azure に導入する場合、ASAv 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 ASAv 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 ASAv を ASDM に接続するために使用されます。

（注） Azure Accelerated Networking は、管理インターフェイスではサポートされていません。

- 内部インターフェイス（必須）：内部ホストに ASAv 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）：ASAv 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、ASAv を DMZ ネットワークに接続するために使用されます。

- ASAv 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
- Azure Accelerated Networking（AN）
- 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、ASAv 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 ASAv 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） ASAv 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ことができます。

プライマリ ASAv からスタンバイ ASAv へのフェールオーバー

Azure での ASAv HA 導入で Azure のアップグレードが発生すると、プライマリ ASAv からスタンバイ ASAv 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 ASAv が一時停止状態になります。プライマリ ASAv が一時停止している場合、スタンバイ ASAv は hello パケットを受信しません。スタンバイ ASAv 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 ASAv 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 ASAv 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 ASAv 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 ASAv からスタンバイ ASAv 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、ASAv 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
- ASAv 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 ASAv 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 ASAv 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、ASAv に SSH 接続できなくなるため、グループの変更が、最初に ASAv 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、ASAv 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 ASAv を展開すると、次のリソースが作成されます。

- ASAv 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）

  ASAv 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 ASAv 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、ASAv 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-ASAv-RouteTable です。

  各ルーティングテーブルには、ASAv 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）内に配置されます。

- 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） 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て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 テーブルに含められます。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。

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ASAv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） 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。

IP アドレス

次の情報は Azure の IP アドレスに適用されます。

- ASAv 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 ASAv 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 ASAv 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。

Accelerated Networking（AN）

Azure の Accelerated Networking（AN）機能により、VM に対するシングルルート I/O 仮想化（SR-IOV）が可能になります。これにより、VM NIC がハイパーバイザをバイパスしてその下の PCIe カードに直接アクセスできるようになり、ネットワークが高速化します。AN は VM のスループットパフォーマンスを大幅に向上させ、コアの追加（つまり VM の拡大）にも対応します。

AN はデフォルトではディセーブルになっています。Azure は、事前プロビジョニングされた仮想マシンでの AN の有効化をサポートしています。Azure で VM を停止し、ネットワークカードのプロパティを更新して *enableAcceleratedNetworking* パラメータを true に設定するだけです。Microsoft ドキュメントの「既存の VM で高速ネットワークを有効にする」を参照してください。その後、VM を再起動します。

Mellanox ハードウェアのサポート

Microsoft Azure クラウドには、AN 機能をサポートする Mellanox 4（MLX4）と Mellanox 5（MLX5）の 2 種類のハードウェアがあります。ASAv は、リリース 9.15 以降の次のインスタンスに対する Mellanox ハードウェアの AN をサポートしています。

- D3、D3_v2、DS3、DS3_v2
- D4、D4_v2、DS4、DS4_v2
- D5、D5_v2、DS5、DS5_v2
- D8_v3、D8s_v3
- D16_v3、D16s_v3
- F4、F4s
- F8、F8s、F8s_v2
- F16、F16s、F16s_v2

（注） MLX4（Mellanox 4）は connectx3 = cx3 とも呼ばれ、MLX5（Mellanox 5）は connectx4 = cx4 とも呼ばれます。

VM の導入に Azure が使用する NIC（MLX4 または MLX5）は指定できません。シスコでは、高速ネットワーキング機能を使用するために、ASAv 9.15 バージョン以降にアップグレードすることを推奨しています。

Microsoft Azure への ASAv の導入

Microsoft Azure に ASAv 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 ASAv を導入します。「Azure Resource Manager からの ASAv 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 ASAv 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 ASAv 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 ASAv の導入」を参照してください。
- Azure Resource Manager を使用して ASAv 高可用性ペアを導入します。冗長性を確保するために、ASAv 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 ASAv の障害時に、バックアップ ASAv 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 ASAv for High Availability の導入 （15 ページ）」を参照してください。
- VHD（cisco.com から入手可能）から管理対象イメージを使用し、カスタムテンプレートで ASAv または ASAv 高可用性ペアを導入します。シスコでは、圧縮仮想ハードディスク（VHD）を提供しています。この VHD を Azure にアップロードすることで、ASAv の導入プロセスを簡素化できます。管理対象イメージと 2 つの JSON ファイル（テンプレートファイルおよびパラメータファイル）を使用して、単一の協調操作で ASAv のすべてのリソースを導入およびプロビジョニングできます。カスタムテンプレートを使用するには、「VHD およびリソーステンプレートを使用した Azure からの ASAv の導入 （17 ページ）」を参照してください。

Azure Resource Manager からの ASAv の導入

次の手順は、ASAv 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 ASAv 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想要素を表示します。

ステップ 2 Cisco ASAv のマーケットプレイスを検索し、導入する ASAv 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 ASAv 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>.cloupapp.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) ASAv 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の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 ASAv 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 ASAv 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 ASAv 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。

ASAv 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>.cloupapp.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) ASAv 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の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 ASAv for High Availability の導入

次の手順は、Microsoft Azure で高可用性（HA）ASAv 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 ASAv HA では、2 つの ASAv 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 ASAv] を検索し、[ASAv 4 NIC HA] をクリックして、フェールオーバー ASAv 構成を導入します。

ステップ 3 [Basics] 設定を構成します。

a) ASAv マシン名のプレフィックスを入力します。ASAv 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。

[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。

[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 ASAv 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 [ASAv-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 アドレスが必要ない場合は、[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。

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>.cloupapp.azure.com* の形式になります。

c) ASAv-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) ASAv 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の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、[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 の ASAv 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。

VHD およびリソーステンプレートを使用した Azure からの ASAv の導入

シスコが提供する圧縮 VHD イメージを使用して、独自のカスタム ASAv イメージを作成できます。VHD イメージを使用して展開するには、Azure ストレージアカウントに VHD イメージをアップロードする必要があります。次に、アップロードしたディスクイメージおよび Azure Resource Manager テンプレートを使用して、管理対象イメージを作成できます。Azure テンプレートは、リソースの説明とパラメータの定義が含まれている JSON ファイルです。

始める前に

- ASAv テンプレートの展開には、JSON テンプレートおよび対応する JSON パラメータファイルが必要です。テンプレートファイルは、次の GitHub リポジトリからダウンロードできます。

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- テンプレートとパラメータファイルを構築する手順については、付録：Azure リソーステンプレートの例 （20 ページ）を参照してください。
- この手順では、Azure に Linux VM が存在している必要があります。一時的な Linux VM（Ubuntu 16.04 など）を使用して、Azure に圧縮 VHD イメージをアップロードすることをお勧めします。このイメージを解凍するには、約 50 GB のストレージが必要です。また、Azure の Linux VM から Azure ストレージへのアップロード時間が短くなります。

  VM を作成する必要がある場合は、次のいずれかの方法を使用します。

  - Azure CLI による Linux 仮想マシンの作成
  - Azure ポータルでの Linux 仮想マシンの作成

- Azure サブスクリプションには、ASAv を展開する場所で使用可能なストレージアカウントが必要です。

ステップ 1 https://software.cisco.com/download/home ページから、ASAv 圧縮 VHD イメージをダウンロードします。

a) [Products] > [Security] > [Firewalls] > [Adaptive Security Appliances (ASA)] > [Adaptive Security Appliance (ASA) Software] に移動します。

b) [Adaptive Security Virtual Appliance (ASAv)] をクリックします。

手順に従ってイメージをダウンロードしてください。

たとえば、asav9-14-1.vhd.bz2

ステップ 2 Azure の Linux VM に圧縮 VHD イメージをコピーします。

Azure との間でファイルをやり取りするために使用できるオプションが数多くあります。この例では、SCP（セキュアコピー）を示します。

```
# scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```

ステップ 3 Azure の Linux VM にログインし、圧縮 VHD イメージをコピーしたディレクトリに移動します。

ステップ 4 ASAv VHD イメージを解凍します。

ファイルを解凍または圧縮解除するために使用できるオプションが数多くあります。この例では Bzip2 ユーティリティを示しますが、Windows ベースのユーティリティも正常に機能します。

```
# bunzip2 asav9-14-1.vhd.bz2
```

ステップ 5 Azure ストレージアカウントのコンテナに VHD をアップロードします。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名には、小文字と数字のみを使用できます。

ストレージアカウントに VHD をアップロードするために使用できるオプションが数多くあります。AzCopy、Azure Storage Copy Blob API、Azure Storage Explorer、Azure CLI、Azure ポータルなどです。ASAv と同等の大きさのファイルには、Azure ポータルを使用しないことを推奨します。

次の例は、Azure CLI を使用した構文を示しています。

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

ステップ 6 VHD から管理対象イメージを作成します。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) [追加（Add）] をクリックして、新しいイメージを作成します。
c) 次の情報を入力します。

- [名前（Name）]：管理対象イメージのユーザー定義の名前を入力します。
- [サブスクリプション（Subscription）]：ドロップダウンリストからサブスクリプションを選択します。
- [リソースグループ（Resource group）]：既存のリソースグループを選択するか、新しいリソースグループを作成します。
- [OSディスク（OS disk）]：OS タイプとして Linux を選択します。
- [ストレージブロブ（Storage blob）]：ストレージアカウントを参照して、アップロードした VHD を選択します。
- [アカウントタイプ（Account type）]：ドロップダウンリストから [標準（HDD）（Standard (HDD)）] を選択します。
- [ホストキャッシング（Host caching）]：ドロップダウンリストから [読み取り/書き込み（Read/write）] を選択します。

- [データディスク（Data disks）]：デフォルトのままにしておきます。データディスクを追加しないでください。

d) [作成（Create）] をクリックします。

「イメージが正常に作成されました（Successfully created image）」というメッセージが [通知（Notifications）] タブの下に表示されるまで待ちます。

（注） 管理対象イメージが作成されたら、アップロードした VHD とアップロード ストレージ アカウントを削除できます。

ステップ 7 新規に作成した管理対象イメージのリソース ID を取得します。

Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。リソース ID は、この管理対象イメージから新しい ASAv ファイアウォールを展開するときに必要になります。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) 前のステップで作成した管理対象イメージを選択します。
c) [概要（Overview）] をクリックして、イメージのプロパティを表示します。
d) クリップボードに**リソース ID** をコピーします。

リソース ID は、次の形式を取ります。

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>
/providers/Microsoft.Compute/<container>/ <vhdname>

ステップ 8 管理対象イメージおよびリソーステンプレートを使用して、ASAv ファイアウォールを構築します。

a) [新規（New）] を選択し、オプションから選択できるようになるまで [テンプレート展開（Template Deployment）] を検索します。
b) [作成（Create）] を選択します。
c) [エディタで独自のテンプレートを構築する（Build your own template in the editor）] を選択します。

カスタマイズできる空白のテンプレートが作成されます。テンプレートを作成する方法の例については、リソース テンプレートの作成 （21 ページ）を参照してください。

d) カスタマイズした JSON テンプレートコードをウィンドウに貼り付け、[保存（Save）] をクリックします。
e) ドロップダウンリストから [サブスクリプション（Subscription）] を選択します。
f) 既存の [リソースグループ（Resource group）] を選択するか、新しいリソースグループを作成します。
g) ドロップダウンリストから [ロケーション（Location）] を選択します。
h) 前ステップからの管理対象イメージの [リソースID（Resource ID）] を [VM管理対象イメージID（Vm Managed Image Id）] フィールドに貼り付けます。

ステップ 9 [カスタム展開（Custom deployment）] ページの最上部にある [パラメータの編集（Edit parameters）] をクリックします。カスタマイズできるパラメータテンプレートが作成されます。

a) [ファイルのロード（Load file）] をクリックし、カスタマイズした ASAv パラメータファイルを参照します。パラメータテンプレートを作成する例については、「パラメータ ファイルの作成 （30 ページ）」を参照してください。

b) カスタマイズした JSON パラメータコードをウィンドウに貼り付け、[保存（Save）] をクリックします。

ステップ 10 カスタム展開の詳細を確認します。[基本（Basics）] と [設定（Settings）] の情報（[リソースID（Resource ID）] など）が、想定した展開設定に一致することを確認します。

ステップ 11 利用規約を確認し、[上記の利用規約に同意します（I agree to the terms and conditions stated above）] チェックボックスをオンにします。

ステップ 12 [購入（Purchase）] をクリックし、管理対象イメージおよびカスタムテンプレートを使用して ASAv ファイアウォールを導入します。

テンプレートファイルとパラメータファイルに競合がなければ、展開が正常に完了しているはずです。

管理対象イメージは、同じサブスクリプションおよび地域内の複数の展開に使用できます。

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。

付録：Azure リソース テンプレートの例

この項では、ASAv を展開するために使用できる Azure Resource Manager テンプレートの構造について説明します。Azure リソーステンプレートは JSON ファイルです。必須の全リソースの展開を簡素化するため、この例には 2 つの JSON ファイルが含まれています。

- **テンプレートファイル**：これは、リソースグループ内のすべてのコンポーネントを展開するメインリソースファイルです。
- **パラメータ ファイル**：このファイルには、ASAv を正常に展開するために必要なパラメータが含まれています。このファイルには、サブネット情報、仮想マシンの階層とサイズ、ASAv のユーザー名とパスワード、ストレージコンテナの名前など、詳細な情報が含まれています。このファイルは Azure Stack Hub 展開環境用にカスタマイズできます。

テンプレート ファイルの形式

この項では、Azure Resource Manager テンプレートの構造について説明します。次の例は、テンプレートファイルを縮小表示したもので、テンプレートのさまざまな部分を示しています。

Azure Resource Manager JSON テンプレート ファイル

```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "",
```

```
    "parameters": { },
    "variables": { },
    "resources": [ ],
    "outputs": { }
}
```

テンプレートは、ASAv 展開の値を作成するために使用できる JSON および式で構成されています。その最も単純な構造では、テンプレートに次の要素が含まれています。

表 *3*：定義済みの *Azure Resource Manager JSON* テンプレートファイル要素

要素	必須	説明
$schema	はい	テンプレート言語のバージョンを説明する JSON スキーマファイルの場所。前の図に示した URL を使用します。
contentVersion	はい	テンプレートのバージョン（1.0.0.0 など）。この要素には任意の値を指定できます。テンプレートを使用してリソースを展開するときは、この値を使用して、適切なテンプレートが使用されていることを確認できます。
パラメータ	いいえ	展開を実行してリソース展開をカスタマイズするときに指定する値。パラメータにより、展開時に値を入力できます。絶対に必要というわけではありませんが、指定しないと、JSON テンプレートは毎回同じパラメータでリソースを展開します。
変数	いいえ	テンプレート言語式を簡素化するためにテンプレートで JSON フラグメントとして使用される値。
リソース	はい	リソースグループで展開または更新されるリソースタイプ。
outputs	いいえ	展開後に返される値。

JSON テンプレートは、展開するリソース タイプを宣言するためだけでなく、その関連する設定パラメータを宣言するためにも利用できます。次の例は、新しい ASAv を展開するテンプレートを示しています。

リソース テンプレートの作成

以下の例を使用して、テキストエディタを使用した独自の導入テンプレートを作成できます。

ステップ 1 次の例に示したテキストをコピーします。

例：

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "defaultValue": "ngfw",
            "metadata": {
                "description": "Name of the NGFW VM"
            }
        },
        "vmManagedImageId": {
            "type": "string",
            "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",

            "metadata": {
                "description": "The ID of the managed image used for deployment.
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"

            }
        },
        "adminUsername": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Username for the Virtual Machine. admin, Administrator among other
 values are disallowed - see Azure docs"
            }
        },
        "adminPassword": {
            "type": "securestring",
            "defaultValue" : "",
            "metadata": {
                "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars
 and have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
            }
        },
        "vmStorageAccount": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "A storage account name (boot diags require a storage account).
Between 3 and 24 characters. Lowercase letters and numbers only"
            }
        },
        "virtualNetworkResourceGroup": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network's Resource Group"
            }
        },
        "virtualNetworkName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Name of the virtual network"
            }
        },
        "mgmtSubnetName": {
            "type": "string",
            "defaultValue": "",
```

```
            "metadata": {
                "description": "The FTDv management interface will attach to this subnet"
            }
        },
        "mgmtSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
            }
        },
        "diagSubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
            }
        },
        "diagSubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
            }
        },
        "gig00SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
            }
        },
        "gig00SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
            }
        },
        "gig01SubnetName": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
            }
        },
        "gig01SubnetIP": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
            }
        },
        "VmSize": {
            "type": "string",
            "defaultValue": "Standard_D3_v2",
            "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
            "metadata": {
                "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
            }
        }
    },
    "variables": {
```

```
        "virtualNetworkID":
"[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",

        "vmNic0Name":"[concat(parameters('vmName'),'-nic0')]",
        "vmNic1Name":"[concat(parameters('vmName'),'-nic1')]",
        "vmNic2Name":"[concat(parameters('vmName'),'-nic2')]",
        "vmNic3Name":"[concat(parameters('vmName'),'-nic3')]",

        "vmNic0NsgName":"[concat(variables('vmNic0Name'),'-NSG')]",

        "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
        "vmMgmtPublicIPAddressType": "Static",
        "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
    },
    "resources": [
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/publicIPAddresses",
            "name": "[variables('vmMgmtPublicIPAddressName')]",
            "location": "[resourceGroup().location]",
            "properties": {
              "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
              "dnsSettings": {
                "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
              }
            }
        },
        {
            "apiVersion": "2015-06-15",
            "type": "Microsoft.Network/networkSecurityGroups",
            "name": "[variables('vmNic0NsgName')]",
            "location": "[resourceGroup().location]",
            "properties": {
                "securityRules": [
                    {
                        "name": "SSH-Rule",
                        "properties": {
                            "description": "Allow SSH",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "22",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 100,
                            "direction": "Inbound"
                        }
                    },
                    {
                        "name": "SFtunnel-Rule",
                        "properties": {
                            "description": "Allow tcp 8305",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "8305",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 101,
                            "direction": "Inbound"
                        }
                    }
                ]
```

```
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic0Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Network/networkSecurityGroups/',variables('vmNic0NsgName'))]",
                "[concat('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('mgmtSubnetName'))]"
                            },
                            "publicIPAddress":{
                                "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
                            }
                        }
                    }
                ],
                "networkSecurityGroup": {
                    "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
                },
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic1Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('diagSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('diagSubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic2Name')]",
```

```
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig00SubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic3Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig01SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig01SubnetName'))]"

                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[concat(parameters('vmStorageAccount'))]",
            "apiVersion": "2015-06-15",
            "location": "[resourceGroup().location]",
            "properties": {
              "accountType": "Standard_LRS"
            }
        },
        {
            "apiVersion": "2017-12-01",
            "type": "Microsoft.Compute/virtualMachines",
            "name": "[parameters('vmName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic0Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic1Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic2Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic3Name'))]"
            ],
```

```
            "properties": {
                "hardwareProfile": {
                    "vmSize": "[parameters('vmSize')]"
                },
                "osProfile": {
                    "computername": "[parameters('vmName')]",
                    "adminUsername": "[parameters('AdminUsername')]",
                    "adminPassword": "[parameters('AdminPassword')]"
                },
                "storageProfile": {
                    "imageReference": {
                        "id": "[parameters('vmManagedImageId')]"
                    },
                    "osDisk": {
                        "osType": "Linux",
                        "caching": "ReadWrite",
                        "createOption": "FromImage"
                    }
                },
                "networkProfile": {
                    "networkInterfaces": [
                        {
                            "properties": {
                                "primary": true
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
                        }
                    ]
                },
                "diagnosticsProfile": {
                    "bootDiagnostics": {
                        "enabled": true,
                        "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
                    }
                }
            }
        }
    ],
    "outputs": {  }
}
```

ステップ 2 このファイルを、たとえば **azureDeploy.json** というように、JSON ファイルとしてローカルに保存します。

ステップ 3 ファイルを編集し、導入パラメータに合うテンプレートを作成します。

ステップ 4 VHD およびリソーステンプレートを使用した Azure からの ASAv の導入 （17 ページ）で説明しているように、このテンプレートを使用して ASAv を展開します。

パラメータファイルの形式

新しい展開を開始するときには、リソーステンプレートにパラメータが定義されています。展開を開始するには、これらを入力しておく必要があります。リソーステンプレートに定義したパラメータを手動で入力することも、パラメータをテンプレートパラメータ JSON ファイルに配置しておくこともできます。

パラメータ ファイルには、パラメータ ファイルの作成 （30 ページ）のパラメータの例に表示される各パラメータの値が含まれています。これらの値は、展開時にテンプレートに自動的に渡されます。さまざまな展開シナリオに合わせて複数のパラメータ ファイルを作成できます。

この例の ASAv テンプレートの場合、パラメータ ファイルに次のパラメータを定義する必要があります。

表 *4: ASAv* パラメータの定義

フィールド	説明	例
vmName	Azure における ASAv マシンの名前。	cisco-asav
vmManagedImageId	展開に使用される管理対象イメージの ID。Azure の内部では、あらゆるリソースがリソース ID に関連付けられています。	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv910-Managed-Image
adminUsername	ASAv にログインするためのユーザー名。予約名の「admin」にすることはできません。	jdoe
adminPassword	管理者アカウントのパスワード。これは、12 ～ 72 文字の長さで、1 つの小文字、1 つの大文字、1 つの数字、1 つの特殊文字のうち 3 つを含める必要があります。	Pw0987654321

フィールド	説明	例
vmStorageAccount	Azure ストレージアカウント。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名は、3 ～ 24 文字で、小文字と数字のみ含めることができます。	ciscoasavstorage
virtualNetworkResourceGroup	仮想ネットワークのリソースグループの名前。ASAv は常に新しいリソースグループに配置されます。	ew-west8-rg
virtualNetworkName	仮想ネットワークの名前。	ew-west8-vnet
mgmtSubnetName	管理インターフェイスは、このサブネットに接続されます。これは、Nic0（最初のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	mgmt
mgmtSubnetIP	管理インターフェイス IP アドレス。	10.8.0.55
gig00SubnetName	GigabitEthernet 0/0 インターフェイスは、このサブネットに接続されます。これは、Nic1（2番目のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	inside
gig00SubnetIP	GigabitEthernet 0/0 インターフェイス IP アドレス。これは、ASAv の最初のデータインターフェイス用です。	10.8.2.55

フィールド	説明	例
gig01SubnetName	GigabitEthernet 0/1 インターフェイスは、このサブネットに接続されます。これは、Nic2（3番目のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	outside
gig01SubnetIP	GigabitEthernet 0/1 インターフェイス IP アドレス。これは、ASAv の 2 番目のデータインターフェイス用です。	10.8.3.55
gig02SubnetName	GigabitEthernet 0/2 インターフェイスは、このサブネットに接続されます。これは、Nic3（4番目のサブネット）にマップされます。既存のネットワークに参加する場合、これは既存のサブネット名に一致する必要があります。	dmz
gig02SubnetIP	GigabitEthernet 0/2 インターフェイスの IP アドレス。これは、ASAv の 3 番目のデータインターフェイス用です。	10.8.4.55
vmSize	ASAv VM に使用する VM のサイズ。Standard_D3_V2 と Standard_D3 がサポートされています。Standard_D3_V2 がデフォルトです。	Standard_D3_V2 または Standard_D3

パラメータ ファイルの作成

以下の例を使用して、テキスト エディタを使用した独自のパラメータ ファイルを作成できます。

（注） 次の例は、IPV4 専用です。

ステップ 1 次の例に示したテキストをコピーします。

例：

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ff1db61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"

    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

ステップ 2 このファイルを、たとえば **azureParameters.json** というように、JSON ファイルとしてローカルに保存します。

ステップ 3 ファイルを編集し、導入パラメータに合うテンプレートを作成します。

ステップ 4 VHD およびリソーステンプレートを使用した Azure からの ASAv の導入 （17 ページ）で説明しているように、このパラメータ テンプレートを使用して ASAv を展開します。

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。