Azure での Threat Defense Virtual の展開

この章では、 Azure ポータルから Secure Firewall Threat Defense Virtual を展開する方法について説明します。

概要

Secure Firewall Threat Defense Virtual は、Microsoft Azure マーケットプレイスに統合され、次のインスタンスタイプをサポートします。

- Standard D3（4 つの vCPU、14 GB、4 つの vNIC）
- Standard D3_v2（4 つの vCPU、14 GB、4 つの vNIC）
- Standard D4_v2（8 つの vCPU、28 GB、8 つの vNIC）（**バージョン 6.5 の新機能**）
- Standard D5_v2（16 の vCPU、56 GB、8 つの vNIC）（**バージョン 6.5 の新機能**）
- Standard_D8s_v3—8 vCPU、32 GB、4vNIC（**バージョン 7.1 の新機能**）
- Standard_D16s_v3—16 vCPU、64 GB、8vNIC（**バージョン 7.1 の新機能**）
- Standard_F8s_v2—8 vCPU、16 GB、4vNIC（**バージョン 7.1 の新機能**）
- Standard_F16s_v2—16 vCPU、32 GB、4vNIC（**バージョン 7.1 の新機能**）

前提条件

- Microsoft Azure アカウント。https://azure.microsoft.com/en-us/ で 1 つ作成できます。

  Azure でアカウントを作成した後は、ログインしてマーケットプレイスから Cisco Firepower Threat Defense を検索し、「Cisco Firepower NGFW Virtual (NGFWv)」を選択します。

- Cisco スマートアカウント。Cisco Software Central で作成できます。

  Threat Defense Virtual のライセンス。ヘルプリンクをはじめとしたファイアウォールシステムで使用できる機能ライセンスの概要については、『Cisco Secure Firewall Management Center 機能ライセンス』を参照してください。

- Threat Defense Virtual とシステムの互換性については、『Threat Defense Virtual Compatibility Guide 』を参照してください。

通信パス

- 管理インターフェイス：Threat Defense Virtual を Secure Firewall Management Center に接続するために使用されます。

（注） 6.7 以降では、必要に応じて、管理インターフェイスの代わりにデータインターフェイスを Management Center の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。Management Center にアクセスするためのデータインターフェイスの設定に関する詳細については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』の **configure network management-data-interface** コマンドを参照してください。

- 診断インターフェイス — 診断およびレポートに使用されます。通過トラフィック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 Threat Defense Virtual 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）：Threat Defense Virtual 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。

注意事項と制約事項

サポートされる機能

- ルーテッド ファイアウォール モードのみ
- Azure Accelerated Networking（AN）
- 管理モード：次の 2 つのいずれかを選択できます。
  - Secure Firewall Management Center を使用して Threat Defense Virtual を管理することができます。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。
  - 統合 Secure Firewall デバイスマネージャ を使用して Threat Defense Virtual を管理することができます。「Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください
- クラスタリング（バージョン 7.3 以降）。詳細については、『パブリッククラウドにおける Threat Defense Virtual のクラスタリング』を参照してください。
- パブリック IP アドレス：Management 0/0 および GigabitEthernet 0/0 にパブリック IP アドレスが割り当てられます。

  必要に応じて、その他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。

- IPv6

  IPv6 をサポートする Threat Defense Virtual を展開する際に考慮する必要があるガイドラインと制限事項を、以下に示します。

  - IPv6 サポートのために Azure CLI メソッドを使用してプログラムによる展開オプションを有効にする場合、Threat Defense Virtual インスタンスの事前導入は必要ありません。
  - IPV4 から IPV6 アドレッシングに手動でアップグレードしたものと同じ Vnet に、Azure Marketplace から Threat Defense Virtual を追加することはできません。

- インターフェイス:
  - Threat Defense Virtual デフォルトでは 4 つの vNIC を使用して展開されます。
  - より大規模なインスタンスのサポートにより、最大 8 つの vNIC を使用して Threat Defense Virtual を展開できます。
  - Threat Defense Virtual の展開に vNIC を追加するには、Microsoft の「仮想マシンのネットワーク インターフェイスの追加と削除」に示されるガイドラインに従います。
  - Threat Defense Virtual インターフェイスは、マネージャを使用して設定します。インターフェイスのサポートと設定の詳細については、管理プラットフォーム（Management Center または Device Manager ）のコンフィギュレーション ガイドを参照してください。

ライセンシング

- シスコ スマート ライセンス アカウントを使用する BYOL（Bring Your Own License）。
- PAYG（Pay As You Go）ライセンス。顧客がシスコ スマート ライセンシングを購入せずに Threat Defense Virtual を実行できる従量制課金モデル。登録された PAYG Threat Defense Virtual デバイスでは、ライセンス供与されたすべての機能（マルウェア、脅威、URL フィルタリング、VPN など）が有効になっています。ライセンス供与された機能は、Management Center から編集または変更することはできません（バージョン 6.5 以上）。

（注） PAYG ライセンスは、Device Manager モードで展開されている Threat Defense Virtual デバイスではサポートされていません。

Threat Defense Virtual デバイスのライセンス取得のガイドラインについては、『Secure Firewall Management Center Administration Guide』の「Licensing」の章を参照してください。

Threat Defense Virtual スマートライセンスのパフォーマンス階層

Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。

表 *1 : Threat Defense Virtual* 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	デバイス仕様（コア/RAM）	レート制限	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/34 GB	16 Gbps	10,000

パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「Azure での仮想化の調整と最適化」を参照してください。

Receive Side Scaling：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって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使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

サポートされない機能

- ライセンス：
  - PLR（パーマネントライセンス予約）
  - PAYG（Pay As You Go）（バージョン 6.4 以前）
- ネットワーキング（これらの制限事項の多くは Microsoft Azure の制約）：
  - ジャンボフレーム
  - 802.1Q VLAN
  - トランスペアレントモードおよびその他のレイヤ 2 機能。ブロードキャストなし、マルチキャストなし。
  - Azure の観点からデバイスが所有していない IP アドレスのプロキシ ARP（一部の NAT 機能に影響）
  - 無差別モード（サブネットトラフィックのキャプチャなし）
  - インラインセットモード、パッシブモード

（注） Azure ポリシーにより Threat Defense Virtual のトランスペアレントファイアウォールモードやインラインモードでの動作は阻止されます。これは、Azure ポリシーがインターフェイスの無差別モードでの動作を許可していないためです。

- ERSPAN（GRE を使用。これは Azure では転送されません）

- 管理：
  - コンソールアクセス。管理は Management Center を使用してネットワーク上で実行されます（SSH はセットアップおよびメンテナンスの一部の作業に使用可能）
  - Azure ポータルの「パスワードのリセット」機能
  - コンソールベースのパスワード回復。ユーザーはコンソールにリアルタイムアクセスができないため、パスワードの回復もできません。パスワード回復イメージの起動ができません。唯一の方法は、新しい Threat Defense Virtual VM を展開することです。
- 高可用性（アクティブ/スタンバイ）
- VM のインポート/エクスポート
- Azure での Gen 2 VM の生成
- 展開後の VM のサイズ変更
- VM の OS ディスクの Azure ストレージ SKU を Premium から Standard SKU に移行または更新、およびその逆
- Device Manager ユーザーインターフェイス（バージョン 6.4 以前）

Azure DDoS 防御機能

Microsoft Azure の Azure DDoS Protection は、Threat Defense Virtual 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。

Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、お

よび読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。

- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual デバイスの管理には次の 2 つのオプションを選択できます。

Secure Firewall Management Center

多数のデバイスを管理している場合、または Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Device Manager の代わりに Management Center を使用してデバイスを設定します。

重要 Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager のオンボード管理サービスは無効になります。

注意 現在、シスコには Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

Secure Firewall Device Manager

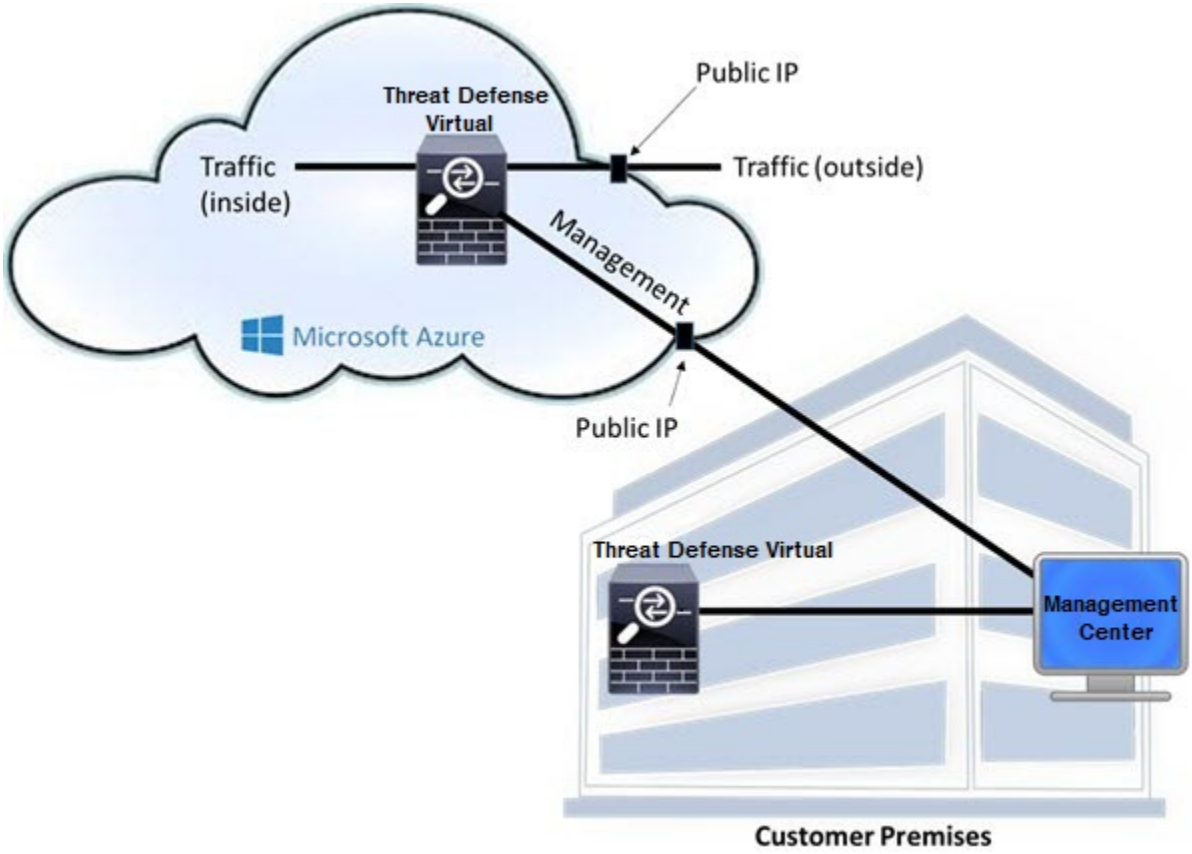
Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

（注） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

Azure 上の Threat Defense Virtual のネットワークトポロジの例

次の図は、Azure 内でルーテッド ファイアウォール モードに設定された Threat Defense Virtual の代表的なトポロジを示しています。最初に定義されるインターフェイスが常に管理インターフェイスであり、Management 0/0 および GigabitEthernet 0/0 のみにパブリック IP アドレスが割り当てられます。



導入時に作成されるリソース

Azure に Secure Firewall Threat Defense Virtual を展開すると、次のリソースが作成されます。

- Threat Defense Virtual マシン（VM）
- リソースグループ
  - Threat Defense Virtual は常に新しいリソースグループに配置されます。ただし、Firepower Threat Defense Virtual を別のリソースグループ内の既存仮想ネットワークにアタッチすることはできます。
- 4 枚の NIC（名前は、*vm name*-Nic0、*vm name*-Nic1、*vm name*-Nic2、*vm name*-Nic3）

（注） 要件に基づいて、IPv4 のみまたはデュアルスタック（IPv4 および IPv6 が有効）で VNet を作成できます。

これらの NIC は、Threat Defense Virtual インターフェイスの Management、Diagnostic 0/0、GigabitEthernet 0/0、GigabitEthernet 0/1 にそれぞれマッピングされます。

- セキュリティグループ（名前は、*vm name*-mgmt-SecurityGroup）

  セキュリティ グループは、Threat Defense Virtual 管理インターフェイスにマッピングされる VM の Nic0 にアタッチされます。

  このセキュリティグループには、Management Center インターフェイス（TCP ポート 8305）用の SSH（TCP ポート 22）および管理トラフィック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（導入時に選択した値に従って命名）。

  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。

- [新規ネットワーク（New Network）] オプションを選択すると、4 つのサブネットを備えた仮想ネットワークが作成されます。
- 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）

  テーブルには、*subnet name*-FTDv-RouteTable という名前が付けられます。

  各ルーティングテーブルには、Threat Defense Virtual 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。

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。

ixgbe-vf インターフェイスの使用の制限事項

ixgbe-vf インターフェイスを使用する場合、次の制限事項があります。

- ゲスト VM では、VF を無差別モードに設定できません。そのため、ixgbe-vf の使用時はトランスペアレント モードがサポートされません。
- ゲスト VM では、VF 上で MAC アドレスを設定できません。そのため、HA 中は MAC アドレスが転送されません。他の Threat Defense Virtual プラットフォームや他のインターフェイス タイプを使用した場合は転送されます。HA フェールオーバーは、IP アドレスをアクティブからスタンバイに移行することによって機能します。

（注） この制限は、i40e-vf インターフェイスにも適用されます。

- Cisco UCSB サーバーは ixgbe-vf の vNIC をサポートしません。
- フェールオーバー セットアップでは、ペアになっている Threat Defense Virtual（プライマリ装置）に障害が発生すると、スタンバイ装置がプライマリ装置のロールを引き継ぎ、そのインターフェイス IP アドレスがスタンバイ Threat Defense Virtual 装置の新しい MAC アドレスで更新されます。その後、Threat Defense Virtual は Gratuitous Address Resolution Protocol（ARP）更新を送信して、インターフェイス IP アドレスの MAC アドレスの変更

を同じネットワーク上の他のデバイスに通知します。ただし、インターフェイスタイプの非互換性により、Gratuitous ARP 更新は、インターフェイス IP アドレスをグローバル IP アドレスに変換するための NAT または PAT ステートメントで定義されているグローバル IP アドレスに送信されません。

Azure ルーティング

Azure 仮想ネットワークサブネットでのルーティングは、サブネットの有効ルーティングテーブルによって決定されます。有効ルーティングテーブルは、組み込みのシステムルートとユーザー定義ルート（UDR）テーブルが組み合わされたものです。

（注） 有効ルーティングテーブルは VM NIC のプロパティの下に表示されます。

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。システムルートとユーザー定義ルートを組み合わせて有効ルーティングテーブルを構成する際に、最も固有なルート（同位のものを含め）がユーザー定義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（IPv4：0.0.0.0/0 または IPv6：[::/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。

Azure Routing Threat Defense Virtual 経由でトラフィックをルーティングするには、各データサブネットに関連付けられたユーザー定義ルーティングテーブルのルートを追加または更新する必要があります。対象トラフィックは、そのサブネット上の Threat Defense Virtual IPアドレスをネクストホップとして使用してルーティングする必要があります。また、必要に応じて、0.0.0.0/0（IPv4）または [::/0]（IPv6）のデフォルトルートを Threat Defense Virtual IP のネクストホップとともに追加できます。

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 Threat Defense Virtual 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 Threat Defense Virtual 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 Threat Defense Virtual 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。

IP アドレス

次の情報は Azure の IP アドレスに適用されます。

- Threat Defense Virtual 上の最初の NIC（Management にマッピングされる）には、アタッチ先のサブネット内のプライベート IP アドレスが付与されます。

  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。

  Threat Defense Virtual の導入後に、パブリック IP アドレスをデータインターフェイス（GigabitEthernet0/0 など）に関連付けることができます。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、『Public IP addresses』 [英語] を参照してください。

- 仮想マシンスケールセット（VMSS）の Threat Defense Virtual アプライアンスに接続されているネットワーク インターフェイスで [IP転送（IP Forwarding）] を有効にすることができます。ネットワークトラフィックの宛先がネットワーク インターフェイスで設定されている IP アドレスのいずれでもない場合、このオプションを有効にすると、そのようなネットワークトラフィックが仮想マシンで設定されている IP アドレス以外の他の IP アドレスに転送されます。ネットワーク インターフェイスで IP 転送を有効にする方法については、Azure のドキュメント「Enable or disable IP forwarding」を参照してください。

- パブリック IP アドレス（IPv4 および IPv6）はダイナミックアドレスであるため、Azure の停止/開始サイクル中に変化する可能性があります。ただし、Azure の再起動時および Threat Defense Virtual のリロード時には保持されます。IPv6 パブリック IP アドレスの標準規格 [英語] を参照してください。

- 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。

- Threat Defense Virtual インターフェイスは、DHCP を使用して自身の IP アドレスを設定できます。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 Threat Defense Virtual インターフェイスに割り当てられるようにします。

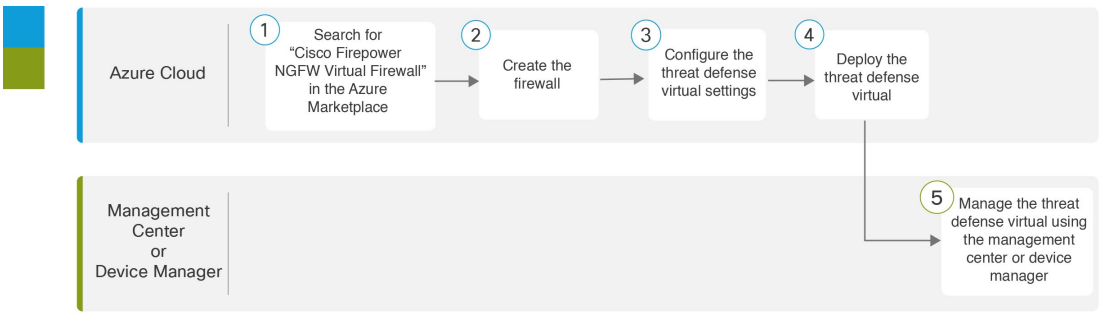
Threat Defense Virtual の導入

テンプレートを使用して、Azure に Threat Defense Virtual を展開できます。2 種類のテンプレートが用意されています。

- **Azure マーケットプレイスのソリューションテンプレート**：Azure マーケットプレイスで使用可能なソリューションテンプレートを使用すると、Azure ポータルを使用して Threat Defense Virtual を展開できます。既存のリソースグループおよびストレージアカウントを使用して（あるいは、それらを新規に作成して）、仮想アプライアンスを展開できます。ソリューションテンプレートを使用するには、「ソリューションテンプレートを使用した Azure マーケットプレイスからの展開 （15 ページ）」を参照してください。
- **VHD からの管理対象イメージを使用したカスタムテンプレート**（https://software.cisco.com/download/home から入手可能）：マーケットプレイスベースの展開の他に、圧縮仮想ディスク（VHD）が用意されています。これを Azure にアップロードして、Azure に Threat Defense Virtual を展開する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 Threat Defense Virtual 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 からの展開 （19 ページ）」を参照してください。

エンドツーエンドの手順

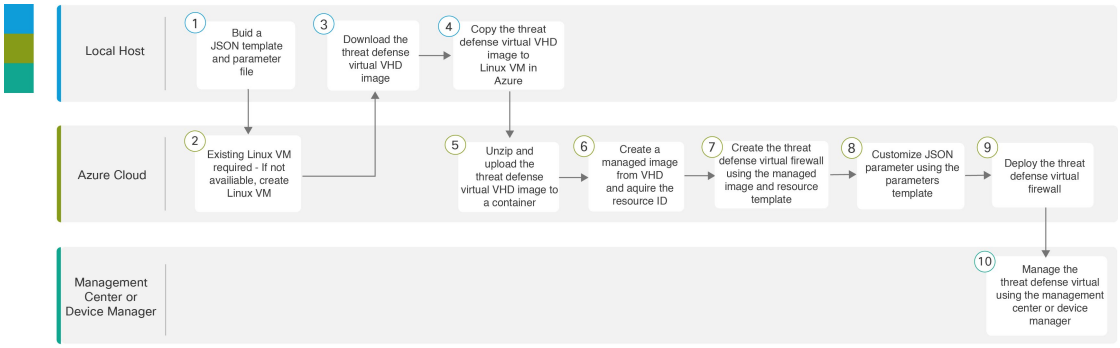
次のフローチャートは、ソリューションテンプレートを使用して Microsoft Azure に Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	Azure Cloud	ソリューションテンプレートを使用した Azure マーケットプレイスからの展開：Azure マーケットプレイスで「Cisco Firepower NGFW Virtual Firewall」を検索します。
2	Azure Cloud	ソリューションテンプレートを使用した Azure マーケットプレイスからの展開：ファイアウォールを作成します。

	ワークスペース	手順
3	Azure Cloud	ソリューションテンプレートを使用した Azure マーケットプレイスからの展開：Threat Defense Virtual を設定します。
4	Azure Cloud	ソリューションテンプレートを使用した Azure マーケットプレイスからの展開：Threat Defense Virtual を展開します。
5	Management Center またはDevice Manager	Threat Defense Virtual を管理します。 • Management Center を使用した Threat Defense Virtual の管理 • Device Manager を使用した Threat Defense Virtual の管理

次のフローチャートは、VHD とリソーステンプレートを使用して Microsoft Azure に Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	VHD およびリソーステンプレートを使用した Azure からの展開：JSON テンプレートとパラメータファイルを作成します。
2	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開：既存の Linux VM が必要です。利用できない場合は、Linux VM を作成します。 • Azure CLI による Linux 仮想マシンの作成 • Azure ポータルによる Linux 仮想マシンの作成
3	ローカルホスト	VHD およびリソーステンプレートを使用した Azure からの展開：シスコのソフトウェア ダウンロード ページから Threat Defense Virtual VHD イメージをダウンロードします。
4	ローカルホスト	VHD およびリソーステンプレートを使用した Azure からの展開：Azure の Linux VM に Threat Defense Virtual VHD イメージをコピーします

	ワークスペース	手順
5	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開：Threat Defense Virtual VHD イメージを解凍し、コンテナにアップロードします。
6	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開：VHD から管理対象イメージを作成し、イメージのリソース ID を取得します。
7	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開：管理対象イメージとリソーステンプレートを使用して Threat Defense Virtual ファイアウォールを作成します。
8	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開：パラメータテンプレートを使用して JSON パラメータをカスタマイズします。
9	Azure Cloud	VHD およびリソーステンプレートを使用した Azure からの展開：Threat Defense Virtual ファイアウォールを展開します。
10	Management Center または Device Manager	Threat Defense Virtual を管理します。 • Management Center を使用した Threat Defense Virtual の管理 • Device Manager を使用した Threat Defense Virtual の管理

ソリューションテンプレートを使用した Azure マーケットプレイスからの展開

次の手順は、Azure マーケットプレイスで使用できる Threat Defense Virtual のソリューションテンプレートを展開する方法を示しています。これは、Microsoft Azure 環境で Threat Defense Virtual をセットアップする手順の概略です。Azure のセットアップ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 Threat Defense Virtual を導入すると、リソース、パブリック IP アドレス（IPv4 および IPv6）、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。

（注） GitHub リポジトリで使用できるカスタマイズ可能な ARM テンプレートについては、「VHD およびリソーステンプレートを使用した Azure からの展開 （19 ページ）」を参照してください。

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 [Azureマーケットプレイス（Azure Marketplace）] > [仮想マシン（Virtual Machines）] を順に選択します。

ステップ 3 マーケットプレイスで「Cisco Firepower NGFW Virtual (Threat Defense Virtual)」を検索して選択し、[作成（Create）] をクリックします。

ステップ 4 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 既存の名前を使用している場合、導入は失敗します。

b) **Byol** または **PAYG** のいずれかのライセンス方式を選択します。

シスコ スマート ライセンス アカウントを使用する **Byol**（Bring Your Own License）を選択します。

シスコ スマート ライセンシングを購入せずに従量制課金モデルを使用するには、**PAYG**（Pay As You Go）ライセンスを選択します。

重要 **PAYG** は、Management Center を使用して Threat Defense Virtual を管理する場合にのみ使用できます。

c) Threat Defense Virtual 管理者のユーザー名を入力します。

（注） 「admin」という名前は Azure で予約されており、使用できません。

d) 認証タイプとして、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。

SSH キーを選択した場合は、リモート ピアの RSA 公開キーを指定します。

e) Threat Defense Virtual の設定時にログインする際に **Admin** ユーザーアカウントで使用するパスワードを作成します。

f) [FTDv管理（FTDv Management）] ドロップダウンリストから、Threat Defense Virtual を登録する Management Center を選択します。

[FMC: Firepower Management Center] をデバイスの Management Center として選択している場合は、次のオプションを使用してデバイスの Management Center を設定できます。

- [はい（Yes）] をクリックして、[FMC登録情報（FMC registration information）] を入力します。

  1. [FMC IP] アドレスを入力します。
  2. Threat Defense Virtual インスタンスを登録するための [FMC登録キー（FMC Registration Key）] を入力します。
  3. （任意）インスタンスの登録時に使用される Management Center NAT ID を入力します。

g) クラスタとして展開する仮想マシンを使用している場合は、[はい（Day-0クラスタ構成を提供します）（Yes (provide day0 cluster configuration)）] をクリックして、基本的な Day-0 構成を作成して詳細を入力します。

- [Day-0クラスタ構成（Day0 cluster configuration）] フィールドに Day-0 構成の詳細を入力します。

  Azure の Day-0 構成の作成の詳細については、『Azure への Threat Defense Virtual クラスタの展開』ガイドの「Azure 向け Day-0 構成の作成」を参照してください。

  （注） 部分的な Day-0 構成（クラスタ構成）："Cluster": {...} OR "run_config": [...] の詳細のみ設定できます。

h) サブスクリプションを選択します。

i) 新しいリソースグループを作成します。

Threat Defense Virtual は新しいリソースグループに導入する必要があります。既存のリソースグループに展開するオプションは、既存のリソースグループが空の場合にのみ機能します。

ただし、後の手順でネットワークオプションを設定する際に、Threat Defense Virtual を別のリソースグループ内に存在している仮想ネットワークへ接続できます。

j) 地理的なロケーションを選択します。このロケーションは、導入で使用される全リソース（Threat Defense Virtual、ネットワーク、ストレージアカウントなど）で統一する必要があります。

k) [OK] をクリックします。

ステップ 5 Threat Defense Virtual 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。

（注） 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。

c) パブリック IP アドレスを選択します。

選択したサブスクリプションとロケーションで使用可能なパブリック IP アドレスを選択するか、[新規作成（Create new）] をクリックします。

新しいパブリック IP アドレスを作成する場合は、Microsoft が所有する IP アドレスのブロックの中から 1 つ取得するため、特定のアドレスを選択することはできません。インターフェイスに割り当てることができるパブリック IP アドレスの最大数は、Azure サブスクリプションに基づいています。

重要 Azure は、デフォルトでダイナミックパブリック IP アドレスを作成します。VM を停止させて再起動すると、パブリック IP が変わることがあります。固定 IP アドレスを使用する場合は、スタティックアドレスを作成する必要があります。導入後にパブリック IP アドレスを変更して、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することもできます。

VM でパブリック IPv6 アドレスを割り当てる必要がある場合は、IPv6 パブリック IP アドレスの標準規格 [英語] を参照してください。

d) DNS ラベルを追加します。

（注） 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) 仮想ネットワークを選択します。

既存の Azure Virtual Network（VNet）を選択するか、新しいものを作成して、VNet の IP アドレス空間を入力できます。デフォルトでは、Classless Inter-Domain Routing（CIDR）の IP アドレスは 10.0.0.0/16 です。

IPv6 アドレッシングに仮想マシンが必要な場合は、仮想ネットワークでそれを有効にする必要があります。例：デフォルトでは、CIDR IPv6 アドレスは [ace:cab:deca::/48] です。

（注） IPv6 だけを使用して、仮想ネットワーク、サブネット、インターフェースなどを構築することはできません。デフォルトでは IPv4 が使用され、IPv6 も一緒に有効にできます。IPv6 の詳細については、Azure IPv6 の概要 [英語] を参照してください。

f) Threat Defense Virtual ネットワーク インターフェイスで 4 つのサブネットを構成します。

- **FTDv 管理**インターフェイス（第 1 サブネット（Azure の Nic0）に接続）
- **FTDv 診断**インターフェイス（第 2 サブネット（Azure の Nic1）に接続）
- **FTDv 外部**インターフェイス（第 3 サブネット（Azure の Nic2）に接続）
- **FTDv 内部**インターフェイス（第 4 サブネット（Azure の Nic3）に接続）

（注） 上記のサブネットについて、サブネットの作成中に IPv6 の設定が必要な場合は、IPv6 オプションを選択して、インターフェイスの IPv6 サブネットを構成します。

g) [パブリックインバウンドポート（mgmt.interface）（Public inbound ports (mgmt.interface)）] の入力を指定して、ポートをパブリック用に開くかどうかを示します。デフォルトでは、[なし（None）] が選択されています。

- Azure のデフォルトのセキュリティルールを使用してネットワーク セキュリティ グループを作成し、管理インターフェイスに接続するには、[なし（None）] をクリックします。このオプションを選択すると、同じ仮想ネットワーク内の送信元からのトラフィックと Azure ロードバランサからのトラフィックが許可されます。
- インターネットでアクセスするために開くインバウンドポートを表示および選択するには、[選択したポートを許可（Allow selected ports）] をクリックします。[インバウンドポートの選択（Select Inbound Ports）] ドロップダウンリストから、次のいずれかのポートを選択します。デフォルトでは、**SSH（22）**が選択されています。
  - SSH（22）
  - SFTunnel（8305）
  - HTTPS（443）

h) [OK] をクリックします。

ステップ 6 構成サマリを確認し、[OK] をクリックします。

ステップ 7 利用条件を確認し、[購入（Purchase）] をクリックします。

導入時間は Azure によって異なります。Threat Defense Virtual VM が実行されていることが Azure から報告されるまで待機します。

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Secure Firewall Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。
- [ローカルマネージャを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、統合されている Secure Firewall Device Manager を使用して Threat Defense Virtual を管理します。「Secure Firewall Device Manager を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

管理オプションの選択方法の概要については、「Secure Firewall Threat Defense Virtual デバイスの管理方法」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 からの展開

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 Threat Defense Virtual 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

- Threat Defense Virtual 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。これらのファイルは、Github リポジトリからダウンロードできます。
- 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推奨します。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縮されます。

  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 ポータルによる Linux 仮想マシンの作成

- Azure サブスクリプションには、Threat Defense Virtual 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 シスコ ダウンロード ソフトウェア ページから Threat Defense Virtual 圧縮 VHD イメージをダウンロードします。

a) [製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > **[次世代ファイアウォール（NGFW）（Next-Generation Firewalls (NGFW)）] > [Cisco Secure Firewall Threat Defense Virtual]** の順に選択します。

b) **[Firepower Threat Defenseソフトウェア（Firepower Threat Defense Software）]** 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、Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2 です。

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/Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.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 Threat Defense Virtual 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 Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.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。Threat Defense Virtual VHD ほどの容量があるファイルには、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。

- [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。
- [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。
- [リージョン（Region）]：VM が展開されるリージョンを選択します。
- [OSタイプ（OS type）]：OS タイプとして [Linux] を選択します。
- [VMの世代（VM generation）]：[世代1（Gen 1）] を選択します。

  （注） [世代2（Gen 2）] はサポートされていません。

- [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）]：要件に応じて、ドロップダウンリストから [Standard HDD]、[Standard SSD]、または [Premium SSD] を選択します。

  このイメージの展開用に予定している VM サイズを選択する場合は、選択したアカウントタイプがその VM サイズでサポートされていることを確認します。
- [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、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 Threat Defense Virtual 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、Threat Defense Virtual 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。テンプレートファイルについては、「Github」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 Threat Defense Virtual パラメータファイルを参照します。テンプレートパラメータについては、「Github」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 Threat Defense Virtual ファイアウォールを展開します。

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

- Azure で Threat Defense Virtual の IP 設定を更新します。

Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開について

Cisco Secure Firewall バージョン 7.3 以前では、Threat Defense Virtual は少なくとも 4 つのインターフェイス（1 つの管理インターフェイス、1 つの診断インターフェイス、2 つのデータインターフェイス）で展開されます。

Cisco Secure Firewall バージョン 7.4.1 以降では、診断インターフェイスを削除し、少なくとも 3 つのインターフェイス（1 つの管理インターフェイスと 2 つのデータインターフェイス）を備えた Threat Defense Virtual を展開できます。この機能により、同じインスタンスタイプに追加のデータインターフェイスを使用して Threat Defense Virtual を展開できます。たとえば、Standard D4_v2 VM インスタンスでは、1 つの管理インターフェイス、1 つの診断インターフェイス、および 6 つのデータインターフェイスを備えた Threat Defense Virtual を展開する代わりに、1 つの管理インターフェイスと 7 つのデータインターフェイスを備えた Threat Defense Virtual を展開できます。

この機能は、Azure 上の Threat Defense Virtual インスタンスの新しい展開でのみサポートされます。

（注） サポートされるインターフェイスの最大数は 8 であるため、Threat Defense Virtual を展開後に最大 5 つのインターフェイスを追加して、最大 8 つのインターフェイスを持つことができます。

Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開のガイドラインと制限事項

- 診断インターフェイスが削除されると、診断インターフェイスの代わりに Threat Defense Virtual 管理インターフェイスまたはデータインターフェイスを使用して syslog および SNMP がサポートされます。
- この展開では、クラスタリングと Auto Scale がサポートされています。
- 診断インターフェイスポートを持つ Threat Defense Virtual インスタンスと、診断インターフェイスポートを持たない Threat Defense Virtual インスタンスのグループ化はサポートされていません。

（注） ここでの Threat Defense Virtual インスタンスのグループ化は、Azure 上の仮想マシンスケールセット（VMSS）内のインスタンスのグループ化を指します。これは、Management Center Virtual での Threat Defense Virtual インスタンスのグループ化には関係しません。

- CMI はサポートされていません。

Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開におけるデータインターフェイスへの NIC マッピング

以下に、診断インターフェイスを使用せずに Azure に Threat Defense Virtual を展開するためのデータインターフェイスへの NIC マッピングを示します。

Net-Interface	Vnet/Subnet	Port
NIC0	mgmt-subnet	Management
NIC1	diag-subnet	M0/0*
NIC2	inside-subnet	Gig0/0
NIC3	outside-subnet	Gig0/1

Threat Defense Virtual-4-NICs

*Diagnostic interface

Net-Interface	Vnet/Subnet	Port
NIC0	mgmt-subnet	Management
NIC1	inside-subnet	Gig0/0
NIC2	outside-subnet	Gig0/1

Threat Defense Virtual-3-NICs

Azure での診断インターフェイスを使用しない Threat Defense Virtual の展開

診断インターフェイスを使用せずに Threat Defense Virtual を展開するには、次の手順を実行します。

ステップ 1 展開オプションに応じて、次のいずれかの方法を使用してこの機能を有効にできます。

- **Solution template in the Azure Marketplace**：Azure コンソールで **`Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYG`** を検索し、[作成（Create）] をクリックします。[基本（Basics）] ウィンドウで必要な情報を入力し、[ソフトウェアバージョン（Software version）] ドロップダウンリストから [7.4.x] を選択します。[診断インターフェイスの接続（Attach diagnostic interface）] の横にある [いいえ（No）] ボタンを選択します。デフォルトでは、[No] が選択されています。

  Azure マーケットプレイスのソリューションテンプレートを使用して、Azure に Threat Defense Virtual を展開する完全な手順については、「ソリューションテンプレートを使用した Azure マーケットプレイスからの展開」を参照してください。

- **Custom Template using a Managed Image from a VHD**：[仮想マシン（Virtual Machines）] > [+作成（+ Create）] > [Azure仮想マシン（Azure Virtual Machine）] > [詳細（Advanced）] ウィンドウに移動し、**Custom data** フィールドにキーと値のペア **`Diagnostic: OFF`** を含む Day-0 構成スクリプトを入力します。**Custom data** フィールドに入力できる Day-0 構成スクリプトの例を以下に示します。

  ```
  {
  "AdminPassword": "E28@2OiUrhx!",
  "Hostname": "ciscothreatdefensevirtual",
  "FirewallMode": "routed",
  "ManageLocally": "No",
  "Diagnostic": "OFF"
  }
  ```

  （注）　キーと値のペア "Diagnostic": "ON/OFF" では、大文字と小文字が区別されます。

  新規展開に使用される ARM テンプレートの **Customdata** フィールドのスクリプトも変更できます。デフォルトでは、キーと値のペアは **`Diagnostic: ON`** に設定されていて、診断インターフェイスが起動します。キーと値のペアが **`Diagnostic: OFF`** に設定されている場合、展開は診断インターフェイスを使用せずに起動します。

  VHD の管理対象イメージを使用し、カスタムテンプレートを使用して Azure に Threat Defense Virtual を展開する完全な手順については、「VHD およびリソーステンプレートを使用した Azure からの展開」を参照してください。

ステップ 2 必要な最小数の NIC（3 枚）を接続します。Azure でのインターフェイスの接続の詳細については、「仮想マシンのネットワーク インターフェイスの追加と削除」を参照してください。

図 *1 : Azure* でのネットワーク インターフェイスの接続

インターフェイスの詳細については、「Interface Overview」を参照してください。

ステップ 3 （任意） コンソールで **show interface ip brief** コマンドを使用して、インターフェイスの詳細を表示します。次に示されているように、Management Center Virtual でインターフェイスの詳細を表示することもできます。

Management Center Virtual では、インターフェイスは次のように表示されます。

With Diagnostic Interface

Interface	Logical Name	Type	Security Zones
Management0/0	management	Physical	
GigabitEthernet0/0		Physical	
GigabitEthernet0/1		Physical	

Without Diagnostic Interface

Interface	Logical Name	Type	Security Zones
GigabitEthernet0/0	outside	Physical	
GigabitEthernet0/1	inside	Physical	

アップグレードのシナリオ

Threat Defense Virtual インスタンスは、以下のシナリオに従ってアップグレードできます。

- すべての Cisco Secure Firewall バージョン：診断インターフェイスを使用して展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用して Threat Defense Virtual インスタンスにアップグレードできます。
- Cisco Secure Firewall バージョン 7.4 以降：診断インターフェイスを使用せずに展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用せずに Threat Defense Virtual インスタンスにアップグレードできます。

次に示すアップグレードシナリオはサポートされていません。

- すべての Cisco Secure Firewall バージョン：診断インターフェイスを使用して展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用せずに Threat Defense Virtual インスタンスにアップグレードできません。
- Cisco Secure Firewall バージョン 7.4.1 以降：診断インターフェイスを使用せずに展開された Threat Defense Virtual インスタンスは、診断インターフェイスを使用して Threat Defense Virtual インスタンスにアップグレードできません。

（注） NIC の数と順序は、アップグレード後も維持されます。

診断インターフェイスを使用しない Threat Defense Virtual クラスタまたは Auto Scale ソリューションの展開

Threat Defense Virtual クラスタ、または診断インターフェイスを使用しない Threat Defense Virtual インスタンスで構成される Auto Scale ソリューションの新しい展開を実行するには、キーと値のペア **Diagnostic: OFF/ON** が Day-0 構成スクリプトで **OFF** に設定されていることを確認します。

トラブルシューティング

Threat Defense Virtual の展開時に診断インターフェイスが削除されない場合は、キーと値のペア **Diagnostic: OFF/ON** が Day-0 構成スクリプトで **OFF** に設定されているか確認します。

Azure での Threat Defense Virtual の Auto Scale ソリューション

概要

Auto Scale ソリューションにより、パフォーマンス要件に合わせてリソースを割り当て、コストを削減できます。リソースの需要が増加した場合、システムは必要に応じてリソースが割り当てられるようにします。リソースの需要が減少すると、コストを削減するためにリソースの割り当てが解除されます。

Threat Defense Virtual Auto Scale for Azure は、Azure が提供するサーバーレス インフラストラクチャ（Logic App、Azure 関数、ロードバランサ、セキュリティグループ、仮想マシンスケールセットなど）を使用する完全なサーバーレス導入です。

Threat Defense Virtual Auto Scale for Azure 導入の主な特徴は次のとおりです。

- Azure Resource Manager（ARM）テンプレートベースの展開。
- CPU およびメモリ（RAM）に基づくスケーリングメトリックのサポート：

（注） 詳細については、「Auto Scale ロジック （70 ページ）」を参照してください。

- Threat Defense Virtual 展開とマルチ可用性ゾーンのサポート。
- Management Center による Threat Defense Virtual インスタンスの登録と登録解除の完全な自動化。
- スケールアウトされた Threat Defense Virtual インスタンスへの NAT ポリシー、アクセスポリシー、およびルートの自動適用。
- ロードバランサとマルチ可用性ゾーンのサポート。
- Auto Scale 機能の有効化と無効化をサポート。
- Management Center でのみ動作し、Device Manager はサポート対象外。
- PAYG または BYOL ライセンスモードでの Threat Defense Virtual 展開をサポート。PAYG は、Threat Defense Virtual ソフトウェアバージョン 6.5 以降にのみ適用可能。「サポートされるソフトウェア プラットフォーム （29 ページ）」を参照してください。
- シスコでは、導入を容易にするために、Auto Scale for Azure 導入パッケージを提供しています。

Azure の Threat Defense Virtual Auto Scale ソリューションは、異なるトポロジを使用して構成された 2 種類の導入例をサポートします。

- サンドイッチテクノロジーを使用した Auto Scale：Threat Defense Virtual スケールセットを Azure の内部ロードバランサ（ILB）と Azure の外部ロードバランサ（ELB）の間に配置します。
- Azure ゲートウェイロードバランサ（GWLB）を使用した Auto Scale：Azure GWLB は、セキュアファイアウォール、パブリックロードバランサ、および内部サーバーと統合されており、ファイアウォールの展開、管理、およびスケーリングを簡素化します。

サポートされるソフトウェア プラットフォーム

Threat Defense Virtual Auto Scale ソリューションは、Management Center によって管理される Threat Defense Virtual に適用可能です。ソフトウェアバージョンには依存しません。『Cisco Firepower Compatibility Guide』には、オペレーティングシステムとホスティング環境の要件を含む、ソフトウェアとハードウェアの互換性が記載されています。

- Management Center（仮想）の表に、Management Center Virtual の互換性と仮想ホスティング環境要件を示します。
- Threat Defense Virtual の互換性の表に、Azure 上の Threat Defense Virtual の互換性と仮想ホスティング環境要件を示します。

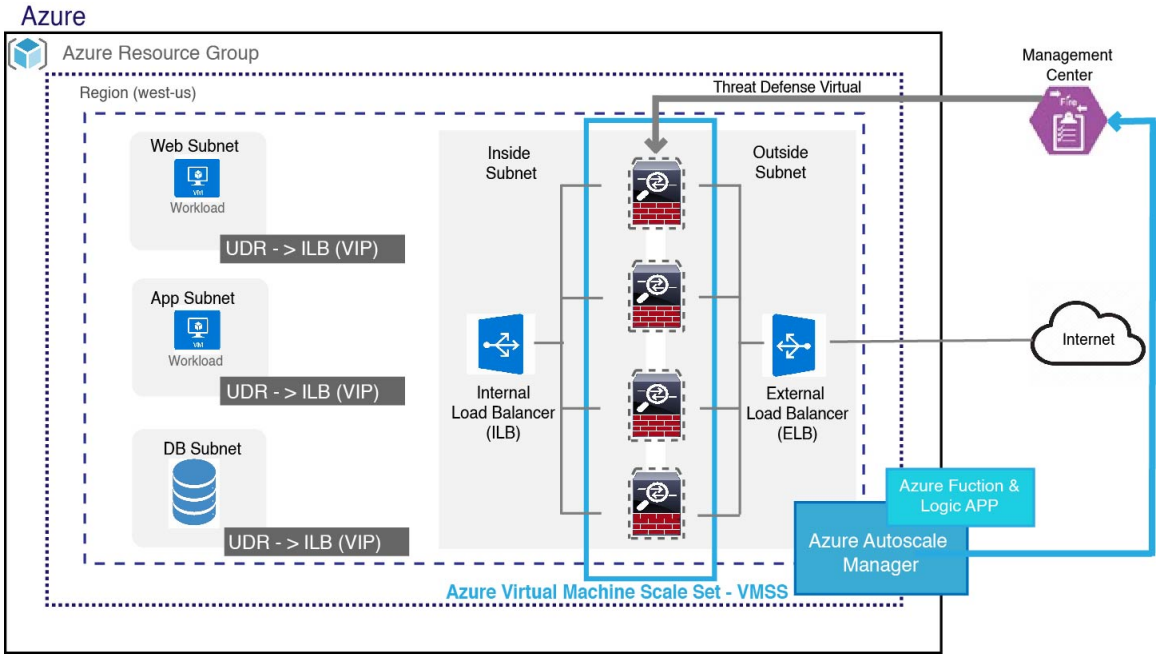
（注） Azure Auto Scale ソリューションを導入するためには、Azure 上で Threat Defense Virtual バージョン 6.4 以上を使用する必要があります。

サンドイッチトポロジを使用した Auto Scale の導入例

Threat Defense Virtual Auto Scale for Azure は、Threat Defense Virtual スケールセットを Azure の内部ロードバランサ（ILB）と Azure の外部ロードバランサ（ELB）の間に配置する自動水平スケーリングソリューションです。

- ELB は、インターネットからのトラフィックをスケールセット内の Threat Defense Virtual インスタンスに分散させます。その後、ファイアウォールがアプリケーションにトラフィックを転送します。
- ILB は、アプリケーションからのアウトバウンド インターネット トラフィックをスケールセット内の Threat Defense Virtual インスタンスに分散させます。その後、ファイアウォールがインターネットにトラフィックを転送します。
- ネットワークパケットが、単一の接続で両方（内部および外部）のロードバランサを通過することはありません。
- スケールセット内の Threat Defense Virtual インスタンスの数は、負荷条件に基づいて自動的にスケーリングおよび設定されます。

図 *2*：サンドイッチトポロジを使用した *Threat Defense Virtual Auto Scale* の導入例の図



Azure Gateway Load Balancer を使用した Auto Scale の導入例

Azure Gateway Load Balancer（GWLB）は、アプリケーションサーバーなどの Azure VM との間のインターネットトラフィックが、ルーティングの変更を必要とせずに Secure Firewall によって検査されるようにします。この Azure GWLB と Secure Firewall の統合により、ファイアウォールの展開、管理、およびスケーリングが簡素化されます。また、この統合により、運用の複雑さが軽減され、ファイアウォールでのトラフィックの単一のエントリポイントとエグジットポイントが提供されます。アプリケーションとインフラストラクチャは、送信元 IP アドレスの可視性を維持できます。一部の環境では、この可視性が非常に重要です。

Azure GWLB Auto Scale の導入例では、Threat Defense Virtual は、管理インターフェイスとデータインターフェイスの 2 つのインターフェイスのみを使用します。

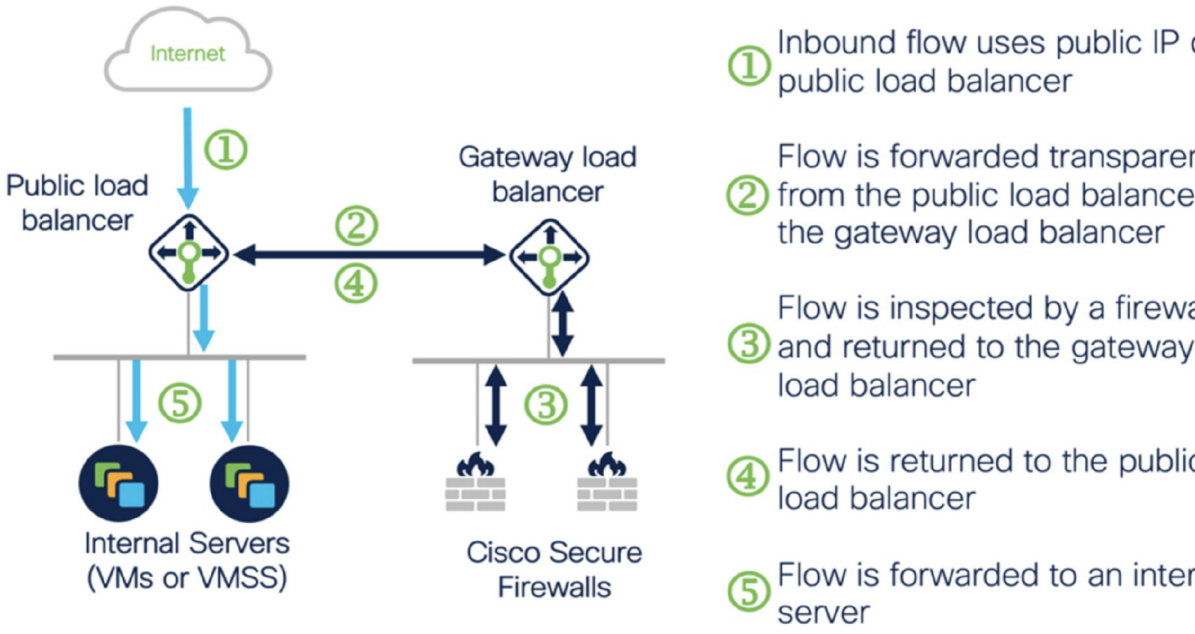
（注）
- Azure GWLB を展開する場合、ネットワークアドレス変換（NAT）は必要ありません。
- IPv4 だけがサポートされます。

ライセンシング

PAYG と BYOL の両方がサポートされています。

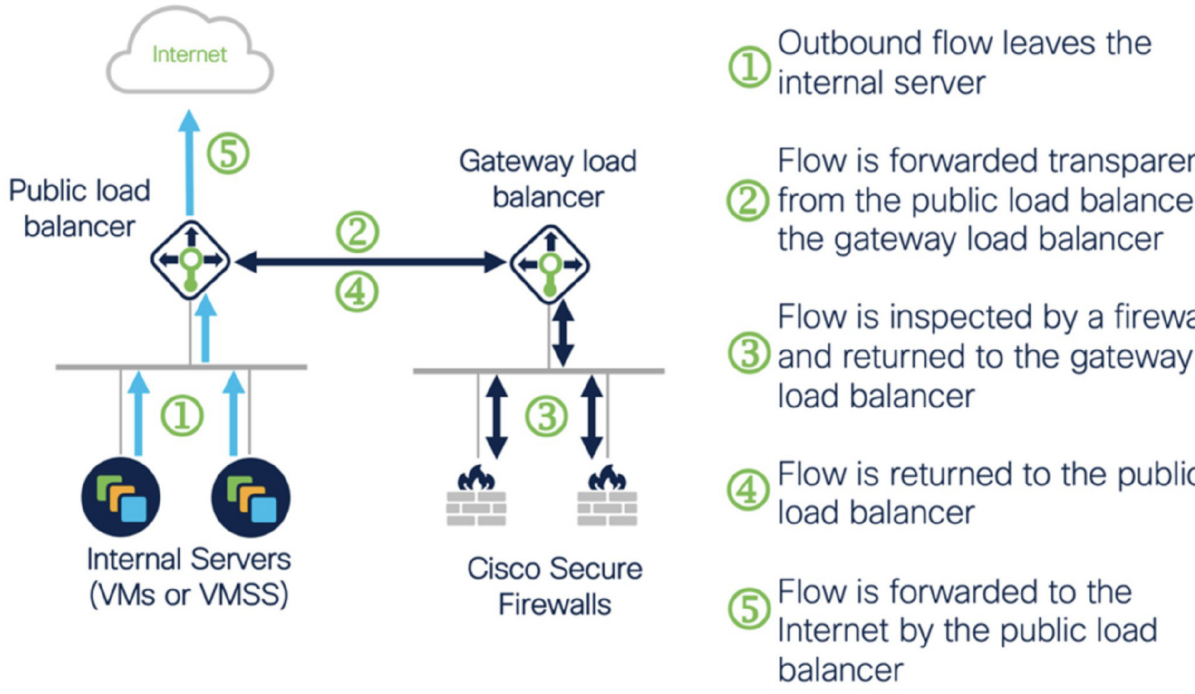
着信トラフィックの導入例とトポロジ

次の図は、着信トラフィックのトラフィックフローを示しています。



発信トラフィックの導入例とトポロジ

次の図は、発信トラフィックのトラフィックフローを示しています。

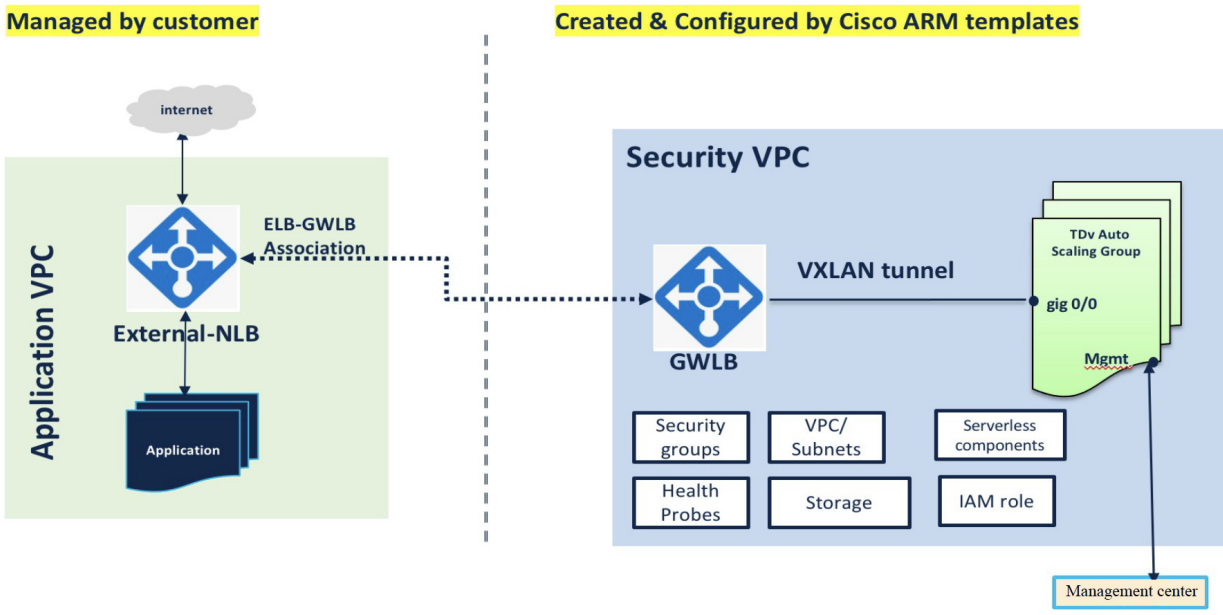


（注） Management Center を展開して設定するには、『Cisco Secure Firewall Management Center Device Configuration Guide』の手順を参照してください。展開された Management Center を使用して、Threat Defense Virtual インスタンスを管理します。

アプリケーション VPC とセキュリティ VPC 間のトラフィックフロー

次の図では、トラフィックは既存のトポロジからファイアウォールにリダイレクトされ、外部ロードバランサによる検査が行われます。その後、トラフィックは新しく作成された GWLB にルーティングされます。ELB にルーティングされるトラフィックはすべて GWLB に転送されます。

次に、GWLB は VXLAN でカプセル化されたトラフィックを Threat Defense Virtual インスタンスに転送します。GWLB は、入力トラフィックと出力トラフィックに 2 つの別個の VXLAN トンネルを使用するため、2 つの Threat Defense Virtual アソシエーションを作成する必要があります。Threat Defense Virtual は、VXLAN でカプセル化されたトラフィックのカプセル化を解除して検査し、GWLB にルーティングします。その後、GWLB はトラフィックを ELB に転送します。



スコープ

このドキュメントでは、Threat Defense Virtual Auto Scale for Azure ソリューションと、Azure GWLB ソリューションを使用した Auto Scale のサーバーレスコンポーネントを展開する詳細な手順について説明します。

重要

- 導入を開始する前に、ドキュメント全体をお読みください。
- 導入を開始する前に、前提条件を満たしていることを確認します。
- ここに記載されている手順と実行順序に従っていることを確認します。

導入パッケージのダウンロード

サンドイッチトポロジを使用した Threat Defense Virtual Auto Scale for Azure ソリューションは、Azure が提供するサーバーレス インフラストラクチャ（Logic App、Azure 関数、ロードバランサ、仮想マシンスケールセットなど）を使用する Azure Resource Manager（ARM）テンプレートベースの展開です。

Azure GWLB ソリューションを使用した Threat Defense Virtual Auto Scale は、GWLB、ネットワーク インフラストラクチャ、Threat Defense Virtual 自動スケーリンググループ、サーバーレスコンポーネント、および他の必要なリソースを作成する ARM テンプレートベースの展開です。

両方のソリューションの展開手順はほぼ同じです。

Threat Defense Virtual Auto Scale for Azure ソリューションの起動に必要なファイルをダウンロードします。該当するバージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

注目

Auto Scale 用のシスコ提供の導入スクリプトおよびテンプレートは、オープンソースの例として提供されており、通常の Cisco TAC サポートの範囲内ではカバーされないことに注意してください。更新と ReadMe の手順については、GitHub を定期的に確認してください。

ASM_Function.zip パッケージの作成方法については、「ソースコードからの Azure 関数の構築（74 ページ）」を参照してください。

Auto Scale ソリューションのコンポーネント

Threat Defense Virtual Auto Scale for Azure ソリューションは、次のコンポーネントで構成されています。

Azure 関数（Function App）

Function App とは一連の Azure 関数です。基本的な機能は次のとおりです。

- Azure メトリックを定期的に通信またはプローブします。
- Threat Defense Virtual の負荷をモニターし、スケールイン/スケールアウト操作をトリガーします。

- Management Center で Threat Defense Virtual を新規登録します。
- Management Center を使用して新しい Threat Defense Virtual を設定します。
- スケールインした Threat Defense Virtual を Management Center から登録解除（削除）します。

関数は、圧縮された Zip パッケージの形式で提供されます（「Azure Function App パッケージの構築 （36 ページ）」を参照）。関数は、特定のタスクを実行するために可能な限り独立しており、拡張機能や新しいリリースのサポートのために必要に応じてアップグレードできます。

Orchestrator（Logic App）

Auto Scale Logic App は、ワークフロー、つまり一連のステップの集合です。Azure 関数は独立したエンティティであり、相互に通信できません。この Orchestrator は、関数の実行を順序付けし、関数間で情報を交換します。

- Logic App は、Auto Scale Azure 関数間で情報をオーケストレーションおよび受け渡すために使用されます。
- 各ステップは、Auto Scale Azure 関数または組み込みの標準ロジックを表します。
- Logic App は JSON ファイルとして提供されます。
- Logic App は、GUI または JSON ファイルを使用してカスタマイズできます。

仮想マシンスケールセット（VMSS）

VMSS は、Threat Defense Virtual デバイスなどの同種の仮想マシンの集合です。

- VMSS では、新しい同一の VM をセットに追加できます。
- VMSS に追加された新しい VM は、ロードバランサ、セキュリティグループ、およびネットワーク インターフェイスに自動的に接続されます。
- VMSS には組み込みの Auto Scale 機能があり、Threat Defense Virtual for Azure では無効になっています。
- VMSS で Threat Defense Virtual インスタンスを手動で追加したり、削除したりしないでください。

Azure Resource Manager（ARM）テンプレート

ARM テンプレートは、Threat Defense Virtual Auto Scale for Azure ソリューションに必要なリソースを展開するために使用されます。

Threat Defense Virtual Auto Scale for Azure：ARM テンプレート **azure_ftdv_autoscale.json** は、以下を含む Auto Scale Manager コンポーネントへの入力情報を提供します。

- Azure Function App

- Azure Logic App
- 仮想マシンスケールセット（VMSS）
- 内部および外部ロードバランサ。
- 展開に必要なセキュリティグループおよびその他のコンポーネント。

Threat Defense Virtual Auto Scale for Azure GWLB：ARM テンプレート **azure_ftdv_autoscale_with_GWLB.json** は、以下を含む Auto Scale Manager コンポーネントへの入力情報を提供します。

- Azure Function App
- Azure Logic App
- 仮想マシン（VM）または仮想マシンスケールセット（VMSS）
- ネットワーキング インフラストラクチャ
- ゲートウェイロードバランサ
- 展開に必要なセキュリティグループおよびその他のコンポーネント

重要 ユーザー入力の検証に関しては、ARM テンプレートには限界があるため、展開時に入力を検証する必要があります。

前提条件

Azure のリソース

リソース グループ

このソリューションのすべてのコンポーネントを展開するには、既存または新しく作成されたリソースグループが必要です。

（注） 後で使用するために、リソースグループ名、リソースグループが作成されたリージョン、および Azure サブスクリプション ID を記録します。

ネットワーキング

仮想ネットワークが使用可能または作成済みであることを確認します。サンドイッチテクノロジーを使用した Auto Scale 展開では、ネットワークリソースの作成、変更、管理は行われません。 ただし、Azure GWLB を使用した Auto Scale の展開では、ネットワーク インフラストラクチャが作成されることに注意してください。

Threat Defense Virtual には 4 つのネットワークインターフェイスが必要なため、仮想ネットワークには次の 4 つのサブネットが必要です。

1. 管理トラフィック
2. 診断トラフィック
3. 内部トラフィック
4. 外部トラフィック

サブネットが接続されているネットワーク セキュリティ グループで、次のポートを開く必要があります。

- SSH（TCP/22）

  ロードバランサと Threat Defense Virtual 間の正常性プローブに必要です。

  サーバーレス機能と Threat Defense Virtual 間の通信に必要です。

- TCP/8305

  Threat Defense Virtual と Management Center 間の通信に必要です。

- HTTPS（TCP/443）

  サーバーレスコンポーネントと Management Center 間の通信に必要です。

- アプリケーション固有のプロトコルまたはポート

  ユーザーアプリケーションに必要です（TCP/80 など）。

（注） 仮想ネットワーク名、仮想ネットワーク CIDR、 4 つすべてのサブネットの名前、および外部と内部のサブネットのゲートウェイ IP アドレスを記録します。

Azure Function App パッケージの構築

Threat Defense Virtual Auto Scale ソリューションでは、*ASM_Function.zip* アーカイブファイルを作成する必要があります。このファイルから、圧縮された ZIP パッケージの形式で一連の個別の Azure 関数が提供されます。

ASM_Function.zip パッケージの作成方法については、「ソースコードからの Azure 関数の構築（74 ページ）」を参照してください。

関数は、特定のタスクを実行するために可能な限り独立しており、拡張機能や新しいリリースのサポートのために必要に応じてアップグレードできます。

Management Center の準備

Threat Defense Virtual を管理するには、フル機能のマルチデバイスマネージャである Management Center を使用します。Threat Defense Virtual は、Threat Defense Virtual マシンに割り当てた管理インターフェイス上の Management Center を登録して通信します。

デバイスグループを含め、Threat Defense Virtual の設定と管理に必要なすべてのオブジェクトを作成します。そうすることで、複数のデバイスにポリシーを簡単に展開して、更新をインストールできます。デバイスグループに適用されたすべての設定が Threat Defense Virtual インスタンスにプッシュされます。

後続の項では、Management Center を準備するための基本的な手順の概要を説明します。詳細については、完全な『Firepower Management Center Configuration Guide』を参照してください。Management Center を準備する際は、次の情報を必ず記録してください。

- Management Center のパブリック IP アドレス。
- Management Center のユーザー名/パスワード。
- セキュリティポリシー名。
- 内部および外部のセキュリティ ゾーン オブジェクト名。
- デバイスグループ名。

Management Center の新規ユーザーの作成

Auto Scale Manager だけが使用する管理者権限を持つ Management Center で新規ユーザーを作成します。

重要 他の Management Center セッションとの競合を防ぐために、Threat Defense Virtual Auto Scale ソリューション専用の Management Center ユーザーアカウントを持つことが重要です。

ステップ 1 管理者権限を持つ Management Center で新しいユーザーを作成します。**[システム（System）]** > **[ユーザー（Users）]** の順にクリックし、[ユーザーの作成（Create User）] をクリックします。

ユーザー名は、次のように Linux に対して有効である必要があります。

- 英数字、ハイフン（-）、およびアンダースコア（_）が使用可で、最大 32 文字
- すべて小文字
- 最初の文字にハイフン（-）は使用不可、すべて数字は不可、ピリオド（.）、アット マーク（@）、またはスラッシュ（/）は使用不可

ステップ 2 使用環境に必要なユーザーオプションを入力します。詳細については、「Cisco Secure Firewall Management Center アドミニストレーション ガイド」を参照してください。

アクセス制御の設定

内部から外部へのトラフィックを許可するアクセス制御を設定します。アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理する詳細な方法が提供されます。ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』の「アクセス制御のベストプラクティス」を参照してください。

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] に一意の名前を入力し、オプションで [説明（Description）] を入力します。

ステップ 4 導入のセキュリティ設定とルールについては、『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』を参照してください。

ライセンスの設定

すべてのライセンスは、Management Center によって Threat Defense に提供されます。オプションで、次の機能ライセンスを購入できます。

- **Cisco Secure Firewall Threat Defense の IPS**：セキュリティ インテリジェンスと Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense のマルウェア防御**：マルウェア防御
- **Cisco Secure Firewall Threat Defense の URL フィルタリング**：URL フィルタリング
- **RA VPN**：AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

（注） IPS、マルウェア防御、または URL フィルタリングライセンスをご購入の場合、1 年、3 年、または 5 年間アップデートを利用するには、該当するサブスクリプション ライセンスも必要です。

始める前に

- Cisco Smart Software Manager にマスター アカウントを持ちます。

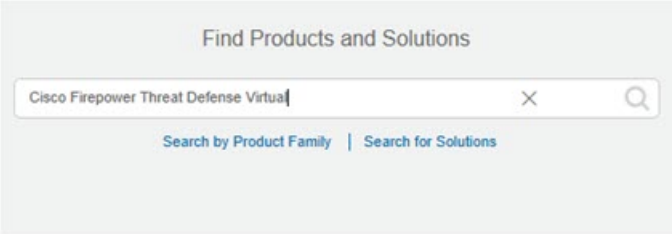
  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

- （輸出コンプライアンス フラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *3:* ライセンス検索



（注） PID が見つからない場合は、注文に手動で PID を追加できます。

ステップ 2 まだ設定していない場合は、スマート ライセンシング サーバーに Management Center を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細な手順については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

セキュリティ ゾーン オブジェクトの作成

展開用の内部および外部セキュリティ ゾーン オブジェクトを作成します。

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]** を選択します。
ステップ 2 オブジェクトタイプのリストから、[インターフェイス（Interface）] を選択します。
ステップ 3 **[追加（Add）] > [セキュリティゾーン（Security Zone）]** をクリックします。
ステップ 4 [名前（Name）]（inside、outside など）を入力します。
ステップ 5 [インターフェイスタイプ（Interface Type）] として [ルーテッド（Routed）] を選択します。
ステップ 6 [保存（Save）] をクリックします。

デバイスグループの作成

デバイス グループにより、複数デバイスへのポリシーの割り当てとインストール更新が簡単にできます。

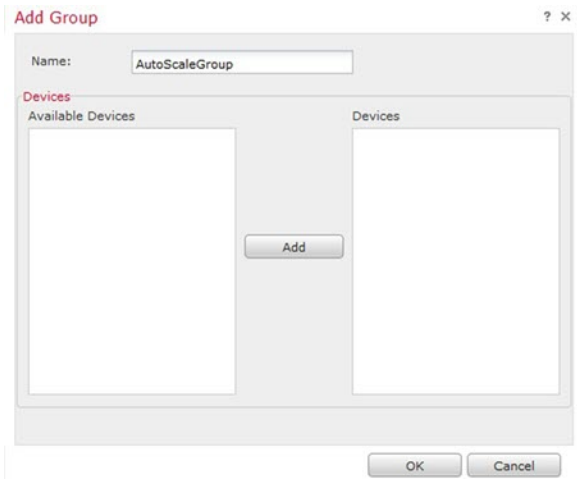
ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

図 *4 : Device Management*

ステップ 2 [追加（Add）] ドロップダウン メニューから、[グループの追加（Add Group）] を選択します。

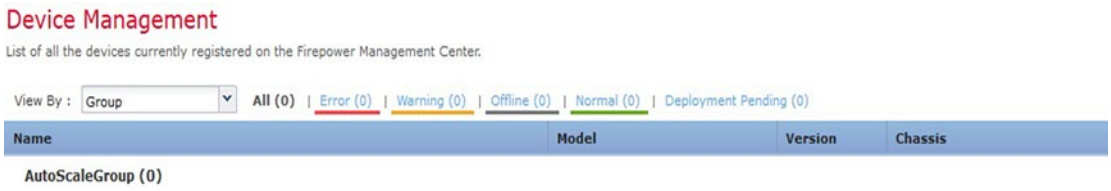
ステップ 3 名前を入力します。 例：AutoScaleGroup。

図 *5 :* デバイスグループの追加



ステップ 4 [OK] をクリックして、デバイス グループを追加します。

図 *6 :* 追加されたデバイスグループ



セキュアシェルアクセスの設定

Threat Defense デバイス用のプラットフォーム設定では、互いに関連しないさまざまな機能を設定して、いくつかのデバイス間でその値を共有できます。Threat Defense Virtual Auto Scale for Azure には、内部ゾーンと外部ゾーン、および自動スケールグループ用に作成されたデバイスグループで SSH を許可するための Threat Defense プラットフォーム設定ポリシーが必要です。

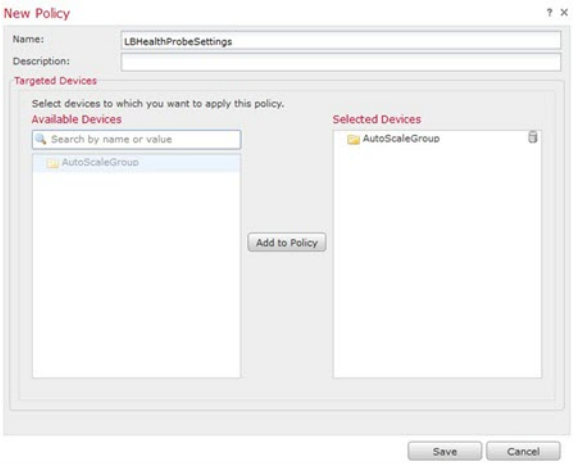
これは、Threat Defense Virtual のデータインターフェイスがロードバランサからの正常性プローブに応答するために必要です。

始める前に

デバイスへのSSH接続を許可するホストまたはネットワークを定義するネットワークオブジェクトが必要です。手順の一部としてオブジェクトを追加できますが、IPアドレスのグループを特定するためにオブジェクトグループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。例として、次の手順の azure-utility-ip（168.63.129.16）オブジェクトを参照してください。

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシー（例：LBHealthProbeSettings）を作成または編集します。

図 *7 : Threat Defense* プラットフォーム設定ポリシー



ステップ 2 [セキュア シェル（Secure Shell）] を選択します。

ステップ 3 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

a) [追加（Add）] をクリックして新しいルールを追加するか、[編集（Edit）] をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

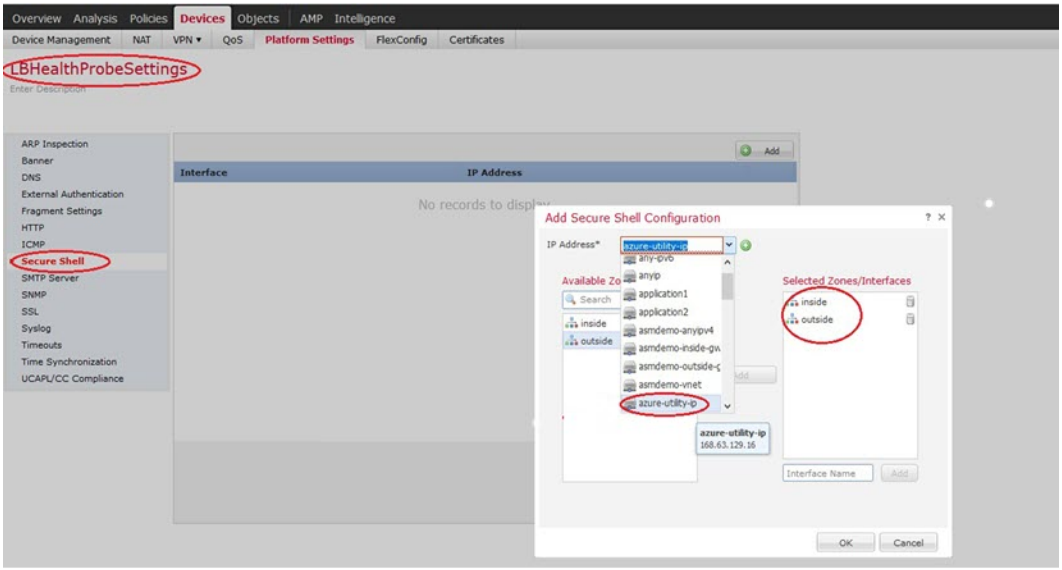
- [IPアドレス（IP Address）]：SSH接続を許可するホストまたはネットワークを特定するネットワークオブジェクト（例：azure-utility-ip（168.63.129.16））。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- [セキュリティ ゾーン（Security Zones）]：SSH 接続を許可するインターフェイスを含むゾーンを追加します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。セキュリティゾーンは、Management Center の [オブジェクト（Objects）] ページで作成できます。セキュリティゾーンの詳細については、『Cisco

Secure Firewall Management Center デバイス コンフィギュレーション ガイド』 を参照してください。

（注） Azure Gateway Load Balancer を使用した Auto Scale の導入例では、内部インターフェイスは使用されません。

- [OK] をクリック

図 *8 : Threat Defense Virtual Auto Scale* の *SSH* アクセス



ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

（注） **SSH アクセス**を使用する代わりに、TCP ポート 443 を正常性プローブ用に設定することもできます。この設定を行うには、[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] > [HTTPアクセス（HTTP Access）] に移動し、 [HTTPサーバーの有効化（Enable HTTP Server）] チェックボックスをオンにして、[ポート（Port）] フィールドに [443] と入力します。この設定を内部インターフェイスと外部インターフェイスに関連付けます。ARM テンプレートの正常性プローブポートも 443 に変更する必要があります。HTTP アクセスの構成の詳細については、『Configuring HTTP』[英語] を参照してください。

NAT の設定

NAT ポリシーを作成し、外部インターフェイスからアプリケーションにトラフィックを転送するために必要な NAT ルールを作成し、このポリシーを Auto Scale 用に作成したデバイスグループにアタッチします。

（注） サンドイッチトポロジを使用して自動スケールを構成する場合にのみ、NAT を構成する必要があります。

ステップ 1 **[デバイス（Devices）] > [NAT]** の順に選択します。

ステップ 2 [新しいポリシー（New Policy）] ドロップダウン リストで、[Threat Defense NAT] を選択します。

ステップ 3 [名前（Name）] に一意の名前を入力します。

ステップ 4 必要に応じて、[説明（Description）] を入力します。

ステップ 5 NAT ルールを設定します。NAT ルールの作成および NAT ポリシーの適用方法のガイドラインについては、『Cisco Secure Firewall Management Center デバイス コンフィギュレーション ガイド』の「Configure NAT for Threat Defense」の手順を参照してください。次の図に、基本的なアプローチを示します。

図 *9 : NAT* ポリシーの例

（注） 変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。

ステップ 6 [保存（Save）] をクリックします。

入力パラメータ

次の表に、テンプレートパラメータおよび例を示します。各パラメータの値を決めたら、Azure サブスクリプションに ARM テンプレートを展開するときに、各パラメータを使用して Threat Defense Virtual デバイスを作成できます。「Auto Scale ARM テンプレートの展開 （54 ページ）」を参照してください。Azure GWLB ソリューションを使用した Auto Scale では、テンプレートで追加の入力パラメータを設定する必要があるため、ネットワーク インフラストラクチャも作成されます。パラメータの意味は一目瞭然なので説明を省略します。

表 *2:* テンプレートパラメータ

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
resourceNamePrefix	文字列*（3 ～ 10 文字）	すべてのリソースは、このプレフィックスを含む名前で作成されます。 注：小文字のみを使用してください。 例：ftdv	新規作成
virtualNetworkRg	文字列	仮想ネットワークのリソースグループの名前。 例：cisco-virtualnet-rg	既存
virtualNetworkName	文字列	仮想ネットワーク名（作成済み） 例：cisco-virtualnet	既存
virtualNetworkCidr	CIDR 形式 x.x.x.x/y	仮想ネットワークの CIDR（作成済み）	既存
mgmtSubnet	文字列	管理サブネット名（作成済み） 例：cisco-mgmt-subnet	既存
diagSubnet	文字列	診断サブネット名（作成済み） 例：cisco-diag-subnet	既存
insideSubnet	文字列	内部サブネット名（作成済み） 例：cisco-inside-subnet	既存
internalLbIp	文字列	内部サブネットの内部ロードバランサの IP アドレス（作成済み）。 例：1.2.3.4	既存
insideNetworkGatewayIp	文字列	内部サブネットのゲートウェイ IP アドレス（作成済み）	既存

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
outsideSubnet	文字列	外部サブネット名（作成済み） 例：cisco-outside-subnet	既存
outsideNetworkGatewayIp	文字列	外部サブネットゲートウェイ IP（作成済み）	既存
deviceGroupName	文字列	Management Center のデバイスグループ（作成済み）	既存
insideZoneName	文字列	Management Center の内部ゾーン名（作成済み）	既存
outsideZoneName	文字列	Management Center の外部ゾーン名（作成済み）	既存
softwareVersion	文字列	Threat Defense Virtual バージョン（展開時にドロップダウンから選択）	既存
vmSize	文字列	Threat Defense Virtual インスタンスのサイズ（展開時にドロップダウンから選択）	該当なし
ftdLicensingSku	文字列	Threat Defense Virtual ライセンスモード（PAYG/BYOL） 注：PAYG はバージョン 6.5+ でサポートされています。	該当なし
licenseCapability	カンマ区切り文字列	BASE、MALWARE、URLFilter、THREAT	該当なし
ftdVmManagementUserName	文字列 *	Threat Defense Virtual VM 管理の管理者ユーザー名。 これは「admin」には**できません**。VM 管理者ユーザー名のガイドラインについては、「Azure」を参照してください。	新規作成

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
ftdVmManagementUserPassword	文字列 *	Threat Defense Virtual VM 管理の管理者ユーザーのパスワード。 パスワードの長さは 12 ー 72 文字で、小文字、大文字、数字、特殊文字を使用する必要があります。また、文字の繰り返しは 2 回までにする必要があります。 （注） テンプレートには、このパラメータのコンプライアンスチェック機能はありません。	新規作成
fmcIpAddress	文字列 x.x.x.x	Management Center のパブリック IP アドレス（作成済み）	既存
fmcUserName	文字列	管理権限を持つ Management Center ユーザー名（作成済み）	既存
fmcPassword	文字列	前述の Management Center ユーザー名の Management Center パスワード（作成済み）	既存
policyName	文字列	Management Center で作成されたセキュリティポリシー（作成済み）	既存

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：設定された期間に、いずれかの Threat Defense Virtual の平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。 **POLICY-2**：設定された期間に、Auto Scale グループ内のすべての Threat Defense Virtual デバイスの平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。 どちらの場合も、スケールインロジックは同じままです。設定された期間に、すべての Threat Defense Virtual デバイスの平均負荷がスケールインしきい値を下回るとスケールインがトリガーされます。	該当なし
scalingMetricsList	文字列	スケーリングの決定に使用されるメトリック。 許可：CPU CPU、メモリ デフォルト：CPU	該当なし
cpuScaleInThreshold	文字列	CPU メトリックのスケールインしきい値（パーセント単位）。 デフォルト：10 Threat Defense Virtualメトリック（CPU 使用率）がこの値を下回ると、スケールインがトリガーされます。 「Auto Scale ロジック （70 ページ）」を参照してください。	該当なし

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
cpuScaleOutThreshold	文字列	CPU メトリックのスケールアウトしきい値（パーセント単位）。 デフォルト：80 Threat Defense Virtualメトリック（CPU 使用率）がこの値を上回ると、スケールアウトがトリガーされます。 「cpuScaleOutThreshold」は、常に「cpuScaleInThreshold」より**大きく**する必要があります。 「Auto Scale ロジック （70 ページ）」を参照してください。	該当なし
memoryScaleInThreshold	文字列	メモリメトリックのスケールインしきい値（パーセント単位）。 デフォルト：0 Threat Defense Virtualメトリック（CPU 使用率）がこの値を下回ると、スケールインがトリガーされます。 「Auto Scale ロジック （70 ページ）」を参照してください。	該当なし

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
memoryScaleOutThreshold	文字列	メモリメトリックのスケールアウトしきい値（パーセント単位）。 デフォルト：0 Threat Defense Virtualメトリック（CPU 使用率）がこの値を上回ると、スケールアウトがトリガーされます。 「memoryScaleOutThreshold」は、常に「memoryScaleInThreshold」より**大きく**する必要があります。 「Auto Scale ロジック （70 ページ）」を参照してください。	該当なし
minFtdCount	整数	任意の時点でスケールセットで使用可能な最小 Threat Defense Virtual インスタンス数。 例：2。	該当なし
maxFtdCount	整数	スケールセットで許可される最大 Threat Defense Virtual インスタンス数。 例：10 （注） この数は Management Center の容量によって制限されます。 Auto Scale ロジックではこの変数の範囲はチェックされないため、慎重に入力してください。	該当なし

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
metricsAverageDuration	整数	ドロップダウンから選択します。 この数値は、メトリックが平均化される時間（分単位）を表します。 この変数の値が 5（5 分）の場合、Auto Scale Manager がスケジュールされると、メトリックの過去 5 分間の平均がチェックされ、その結果に基づいてスケーリングの判断が行われます。 （注） Azure の制限により、有効な数値は 1、5、15、および 30 だけです。	該当なし

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
initDeploymentMode	BULK/STEP		

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
		主に最初の展開、またはスケールセットに Threat Defense Virtual インスタンスが含まれていない場合に適用されます。 BULK：Auto Scale Manager は、「minFtdCount」個の Threat Defense Virtual インスタンスを同時に展開しようとします。 （注） 起動は並行して行われますが、Management Center への登録は Management Center の制限により順次実行されます。 STEP：Auto Scale Manager は、スケジュールされた間隔ごとに「minFtdCount」個の Threat Defense Virtualデバイスを 1 つずつ展開します。 （注） STEP オプションでは、「minFtdCount」個のインスタンスが Management Center で起動および設定されて、動作可能になるまで時間がかかりますが、デバッグに役立ちます。 BULK オプションでは、（並行実行のため）「minFtdCount」個すべての Threat Defense Virtual を起動するのに 1 つ	

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
		の Threat Defense Virtual 起動と同じ時間がかかりますが、Management Center の登録は順次実行されます。 「minFtdCount」個の Threat Defense Virtual を展開するための合計時間 =（1 つの Threat Defense Virtual の起動時間 + 1 つの Threat Defense Virtual 登録および設定時間 * minFtdCount）。	
* Azure には、新しいリソースの命名規則に関する制限があります。制限を確認するか、またはすべて小文字を使用してください**スペースやその他の特殊文字は使用しないでください**。			

Auto Scale ソリューションの展開

導入パッケージのダウンロード

サンドイッチトポロジを使用した Threat Defense Virtual Auto Scale for Azure ソリューションは、Azure が提供するサーバーレス インフラストラクチャ（Logic App、Azure 関数、ロードバランサ、仮想マシンスケールセットなど）を使用する Azure Resource Manager（ARM）テンプレートベースの展開です。

Azure GWLB ソリューションを使用した Threat Defense Virtual Auto Scale は、GWLB、ネットワーク インフラストラクチャ、Threat Defense Virtual 自動スケーリンググループ、サーバーレスコンポーネント、および他の必要なリソースを作成する ARM テンプレートベースの展開です。

両方のソリューションの展開手順はほぼ同じです。

Threat Defense Virtual Auto Scale for Azure ソリューションの起動に必要なファイルをダウンロードします。該当するバージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

注目 Auto Scale 用のシスコ提供の導入スクリプトおよびテンプレートは、オープンソースの例として提供されており、通常の Cisco TAC サポートの範囲内ではカバーされないことに注意してください。更新と ReadMe の手順については、GitHub を定期的に確認してください。

ASM_Function.zip パッケージの作成方法については、「ソースコードからの Azure 関数の構築（74 ページ）」を参照してください。

Auto Scale ARM テンプレートの展開

サンドイッチトポロジを使用した Azure 用 Threat Defense Virtual Auto Scale：ARM テンプレート **azure_ftdv_autoscale.json** を使用して、Azure 用 Threat Defense Virtual Auto Scale に必要なリソースを展開します。特定のリソースグループ内では、ARM テンプレートを展開することで次の内容が作成されます。

- 仮想マシンスケールセット（VMSS）
- 外部ロードバランサ
- 内部ロードバランサ
- Azure Function App
- Logic App
- セキュリティグループ（データインターフェイスおよび管理インターフェイス用）

Azure GWLB を使用した Threat defense virtual Auto Scale：ARM テンプレート **azure_ftdv_autoscale_with_GWLB.json** を使用して、Azure GWLB ソリューションによる Threat Defense Virtual Auto Scale に必要なリソースを展開します。特定のリソースグループ内では、ARM テンプレートを展開することで次の内容が作成されます。

- 仮想マシン（VM）または仮想マシンスケールセット（VMSS）
- ゲートウェイロードバランサ
- Azure Function App
- Logic App
- ネットワーキング インフラストラクチャ
- 展開に必要なセキュリティグループおよびその他のコンポーネント

始める前に

- GitHub リポジトリ（https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure）から、ARM テンプレートをダウンロードします。

ステップ 1 複数の Azure ゾーンに Threat Defense Virtual インスタンスを展開する必要がある場合は、展開リージョンで使用可能なゾーンに基づいて、ARM テンプレートを編集します。

例：

```
        "zones": [
            "1",
            "2",
            "3"
        ],
```

この例は、3 つのゾーンを持つ「Central US」リージョンを示しています。

ステップ 2 外部ロードバランサで必要なトラフィックルールを編集します。この「json」配列を拡張することで、任意の数のルールを追加できます。サンドイッチトポロジを使用したAuto Scaleの導入例でのみ有効です。

例：

```
       {
        "type": "Microsoft.Network/loadBalancers",
        "name": "[variables('elbName')]",
        "location": "[resourceGroup().location]",
        "apiVersion": "2018-06-01",
        "sku": {
          "name": "Standard"
        },
        "dependsOn": [
          "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

        ],
        "properties": {
          "frontendIPConfigurations": [
            {
              "name": "LoadBalancerFrontEnd",
                "properties": {
                  "publicIPAddress": {
                    "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
                  }
                }
            }
          ],
          "backendAddressPools": [
            {
              "name": "backendPool"
            }
          ],
          "loadBalancingRules": [
            {
              "properties": {
                "frontendIPConfiguration": {
                 "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/frontendIpConfigurations/LoadBalancerFrontend')]"
                },
                "backendAddressPool": {
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
 '/backendAddressPools/BackendPool')]"
                },
                "probe": {
```

```
                "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/probes/lbprobe')]"
                },
                "protocol": "TCP",
                "frontendPort": "80",
                "backendPort": "80",
                "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
              },
              "Name": "lbrule"
            }
          ],
```

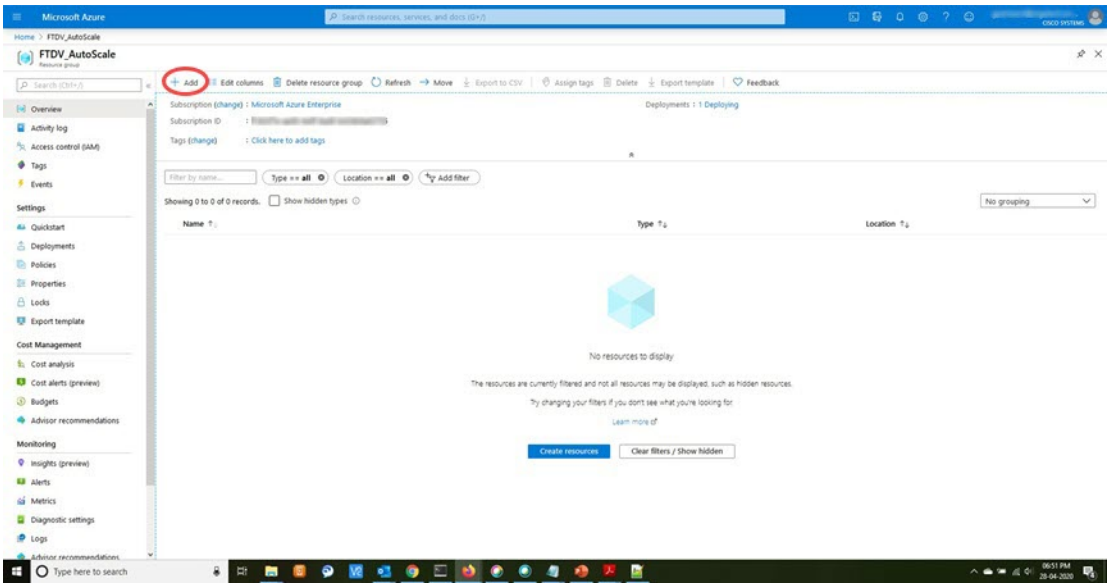
（注）　このファイルを編集しない場合は、導入後に Azure ポータルから編集することもできます。

ステップ 3　Microsoft アカウントのユーザー名とパスワードを使用して、Microsoft Azure ポータルにログインします。

ステップ 4　[リソースグループ（Resource Groups）] ブレードにアクセスするには、サービスのメニューから [リソースグループ（Resource groups）] をクリックします。サブスクリプション内のすべてのリソースグループがブレードに一覧表示されます。

新しいリソースグループを作成するか、既存の空のリソースグループを選択します。たとえば、*Threat Defense Virtual_AutoScale*。

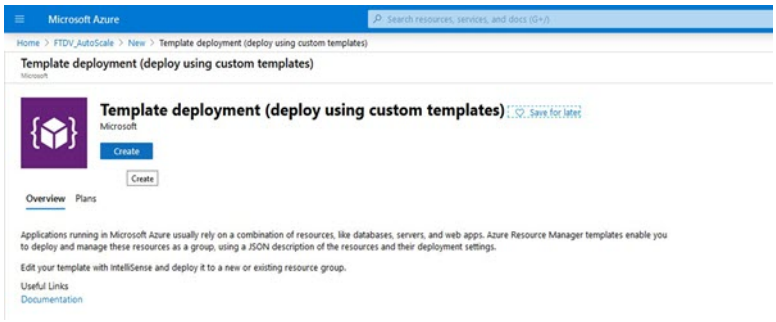
図 *10 : Azure* ポータル



ステップ 5　[リソースの作成（+）（Create a resource (+)）] をクリックして、テンプレート展開用の新しいリソースを作成します。[リソースグループの作成（Create Resource Group）] ブレードが表示されます。

ステップ 6　[マーケットプレイスの検索（Search the Marketplace）] で、「テンプレートの展開（カスタムテンプレートを使用した展開）（Template deployment (deploy using custom templates)）」と入力し、Enter を押します。

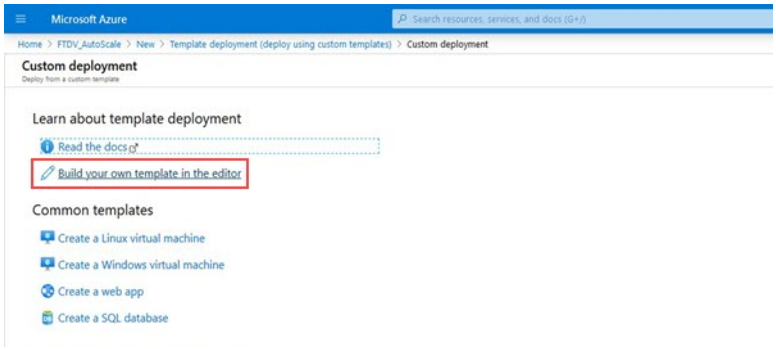
図 *11* : カスタムテンプレートの展開



ステップ 7 [作成（Create）] をクリックします。

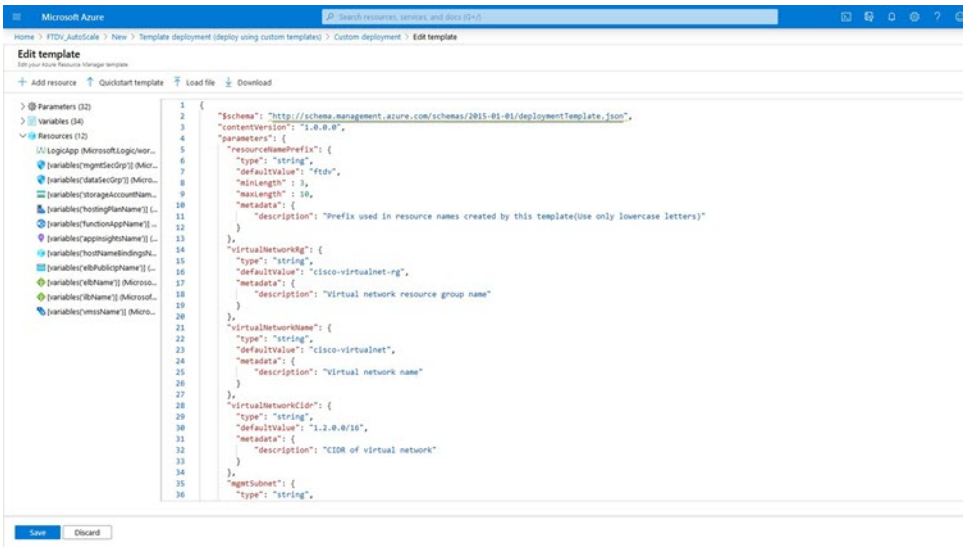
ステップ 8 テンプレートを作成するためのオプションは複数あります。[エディタで独自のテンプレートを作成する（Build your own template in editor）] を選択します。

図 *12* : 独自のテンプレートの作成



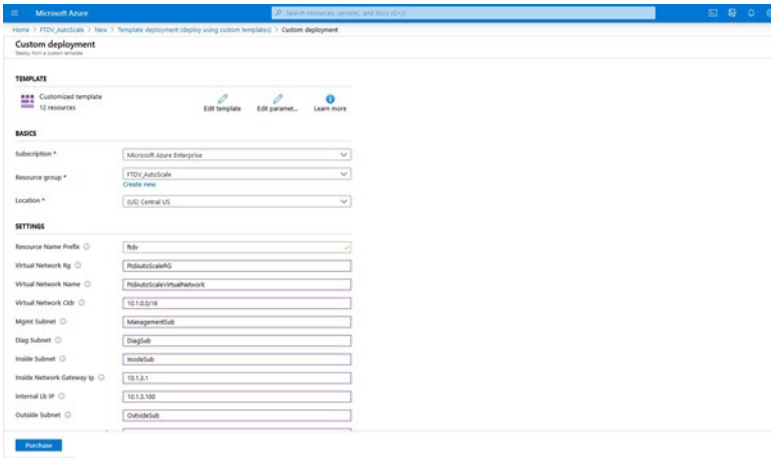
ステップ 9 [テンプレートの編集（Edit template）] ウィンドウで、すべてのデフォルトコンテンツを削除し、更新した *azure_ftdv_autoscale.json* からコンテンツをコピーして、[保存（Save）] をクリックします。

図 *13 : Edit Template*



ステップ 10 次のセクションで、すべてのパラメータを入力します。各パラメータの詳細については、「入力パラメータ （43 ページ）」を参照してください。次に、[購入（Purchase）] をクリックします。

図 *14 : ARM* テンプレートパラメータ

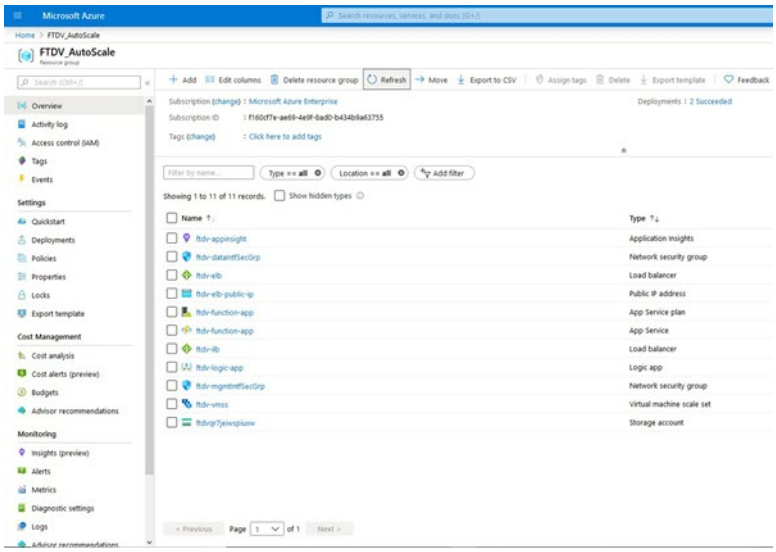


（注） [パラメータの編集（Edit Parameters）] をクリックして、JSON ファイルを編集するか、または事前入力されたコンテンツをアップロードできます。

ARM テンプレートの入力検証機能は限られているため、入力を検証するのはユーザーの責任です。

ステップ 11 テンプレートの展開が成功すると、Threat Defense Virtual Auto Scale for Azure ソリューションに必要なすべてのリソースが作成されます。次の図のリソースを参照してください。[タイプ（Type）]列には、Logic App、VMSS、ロードバランサ、パブリック IP アドレスなどの各リソースが示されます。

図 *15 : Threat Defense Virtual* 自動スケールテンプレートの展開



Azure Function App の展開

ARM テンプレートを展開すると、Azure によってスケルトン Function App が作成されます。このアプリは、Auto Scale Manager ロジックに必要な関数を使用して手動で更新および設定する必要があります。

始める前に

- ASM_Function.zip パッケージをビルドします。「ソースコードからの Azure 関数の構築（74 ページ）」を参照してください。

ステップ 1 ARM テンプレートを展開したときに作成した Function App に移動し、関数が存在しないことを確認します。ブラウザで次の URL にアクセスします。

https://<Function App Name>.scm.azurewebsites.net/DebugConsole

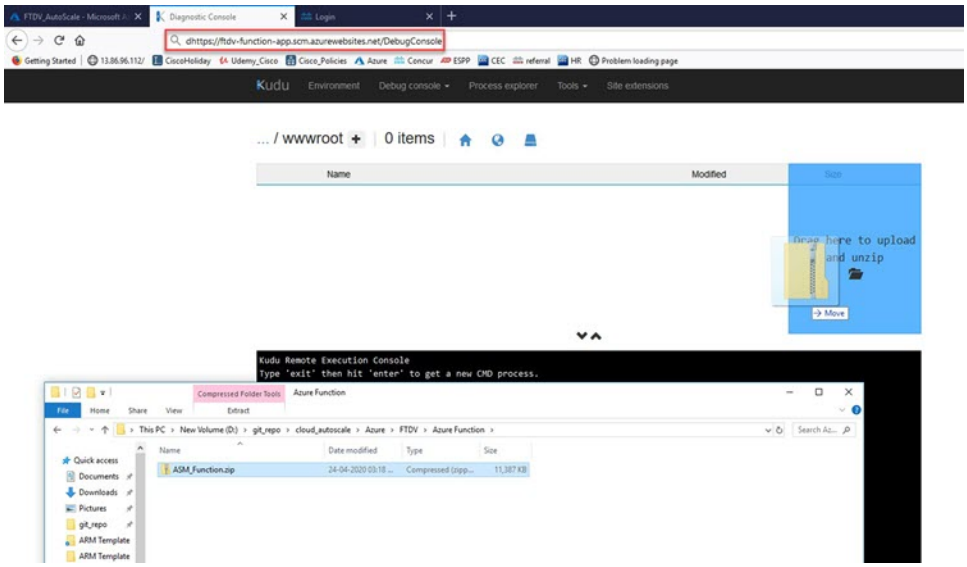
「Auto Scale ARM テンプレートの展開 （54 ページ）」の例の場合、次のようになります。

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

ステップ 2 ファイルエクスプローラで、site/wwwroot に移動します。

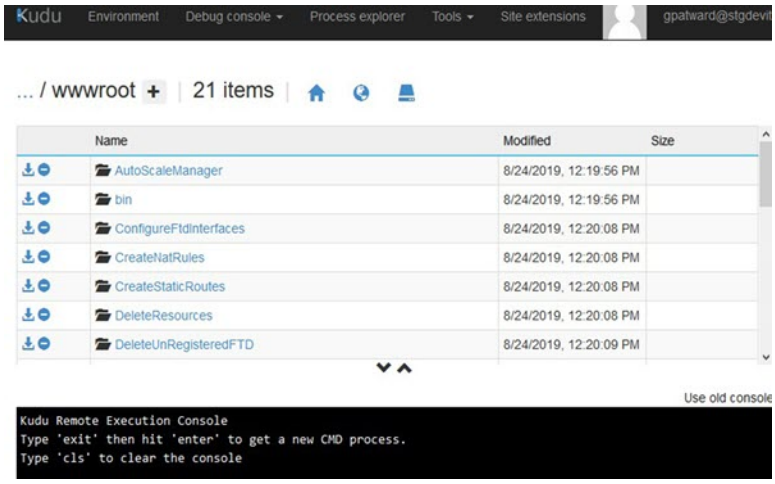
ステップ 3 ASM_Function.zip をファイルエクスプローラの右隅にドラッグアンドドロップします。

図 *16 : Threat Defense Virtual Auto Scale* 機能のアップロード



ステップ 4 アップロードが成功すると、すべてのサーバーレス関数が表示されます。

図 *17 : Threat Defense Virtual* のサーバーレス機能

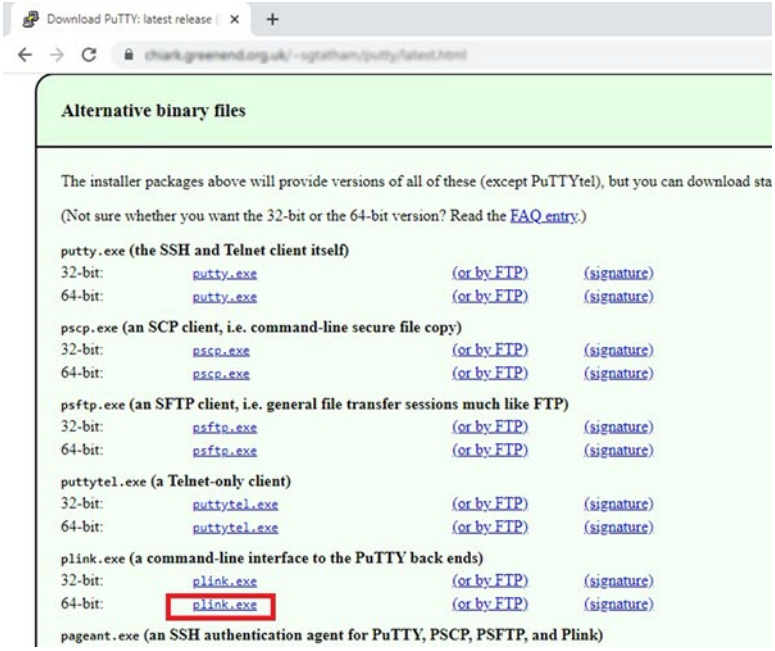


ステップ 5 PuTTY SSH クライアントをダウンロードします。

Azure 関数は、SSH 接続を介して Threat Defense Virtual にアクセスする必要があります。ただし、サーバーレスコードで使用されるオープンソースライブラリは、Threat Defense Virtual で使用される SSH キー交換アルゴリズムをサポートしていません。したがって、事前に構築された SSH クライアントをダウンロードする必要があります。

www.putty.org から PuTTY コマンドライン インターフェイスを PuTTY バックエンド（plink.exe）にダウンロードします。

図 *18 : PuTTY* のダウンロード



ステップ 6 SSH クライアントの実行ファイル **plink.exe** の名前を **ftdssh.exe** に変更します。

ステップ 7 **ftdssh.exe** をファイルエクスプローラの右隅（前のステップで **ASM_Function.zip** をアップロードした場所）にドラッグアンドドロップします。

ステップ 8 SSH クライアントが Function App とともに存在することを確認します。必要に応じてページを更新します。

設定の微調整

Auto Scale Manager を微調整したり、デバッグで使用したりするために使用できる設定がいくつかあります。これらのオプションは、ARM テンプレートには表示されませんが、Function App で編集できます。

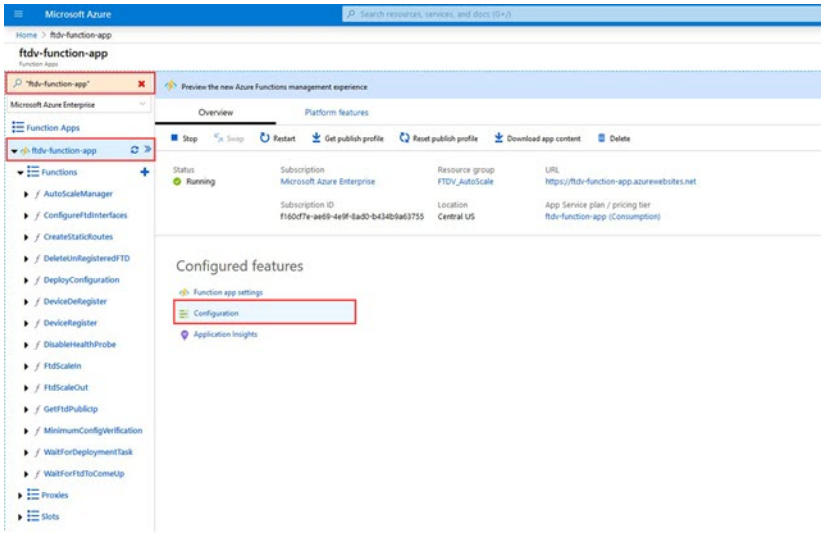
始める前に

（注） 設定はいつでも編集できます。設定を編集する場合は、次の手順に従います。

- Function App を無効にします。
- 既存のスケジュール済みタスクが終了するまで待ちます。
- 設定を編集して保存します。
- Function App を有効にします。

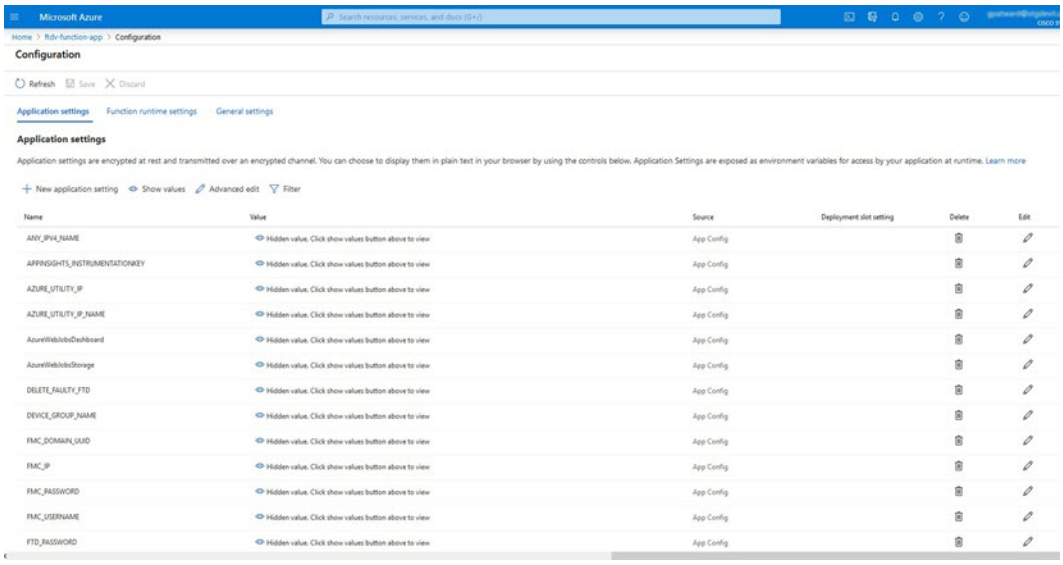
ステップ 1 Azure ポータルで、Threat Defense Virtual Function App を検索して選択します。

図 *19 : Threat Defense Virtual* 機能アプリケーション



ステップ 2 ここでは、ARM テンプレートを介して渡された設定も編集できます。変数名は、ARM テンプレートとは異なる場合がありますが、変数の目的は名前から簡単に識別できます。

図 *20 :* アプリケーションの設定



ほとんどのオプションは、名前を見ればわかります。次に例を示します。

- [構成名（Configuration Name）]：「DELETE_FAULTY_FTD」（[デフォルト値]（Default value ）]：YES）

スケールアウト中に、新しい Threat Defense Virtual インスタンスが起動し、Management Center に登録されます。登録が失敗した場合、このオプションに基づいて、Auto Scale Manager がその Threat Defense Virtual インスタンスを保持するか、削除するかを決定します。（[はい（Yes）]：障害のある Threat Defense Virtual を削除します。[いいえ（No）]：Management Center に登録できない場合でも、Threat Defense Virtual インスタンスを保持します）。

- Function App 設定では、Azure サブスクリプションにアクセスできるユーザーは、すべての変数（「password」などのセキュアな文字列を含んでいる変数を含む）をクリアテキスト形式で表示できます。

  この点に関するセキュリティ上の懸念がある場合（たとえば、Azure サブスクリプションが組織内の低い権限を持つユーザー間で共有されている場合）、ユーザーは Azure の Key Vault サービスを使用してパスワードを保護できます。この設定をすると、関数の設定でクリアテキストの「password」を入力する代わりに、ユーザーは、パスワードが保存されている Key Vault によって生成された、セキュアな識別子を入力する必要があります。

  （注） Azure のドキュメントを検索して、アプリケーションデータを保護するためのベストプラクティスを見つけてください。

仮想マシンスケールセットでの IAM ロールの設定

Azure Identity and Access Management（IAM）は、Azure Security and Access Control の一部として使用され、ユーザーの ID を管理および制御します。Azure リソースのマネージド ID は、Azure Active Directory で自動的にマネージド ID が Azure サービスに提供されます。

これにより、明示的な認証ログイン情報がなくても、Function App が仮想マシンスケールセット（VMSS）を制御できます。

ステップ 1 Azure ポータルで、VMSS に移動します。

ステップ 2 [アクセス制御（IAM）（Access control (IAM)）] をクリックします。

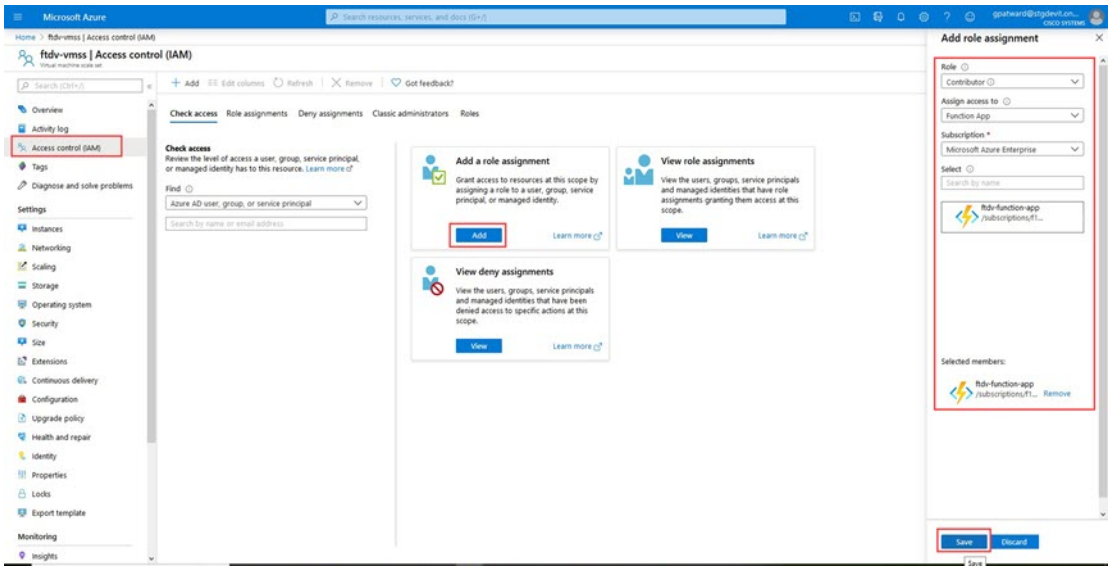
ステップ 3 [追加（Add）] をクリックしてロールの割り当てを追加します。

ステップ 4 [ロール割り当ての追加（Add role assignment）] ドロップダウンから、[共同作成者（Contributor）] を選択します。

ステップ 5 [アクセスの割り当て先（Assign access to）] ドロップダウンから、[Function App] を選択します。

ステップ 6 Threat Defense Virtual Function App を選択します。

図 *21 : AIM* ロールの割り当て



ステップ 7 [保存（**Save**）] をクリックします。

（注） まだ Threat Defense Virtual インスタンスが起動していないことも確認する必要があります。

Azure セキュリティグループの更新

ARM テンプレートは、管理インターフェイス用とデータインターフェイス用の 2 つのセキュリティグループを作成します。管理セキュリティグループは、Threat Defense Virtual 管理アクティビティに必要なトラフィックのみを許可します。ただし、データインターフェイスのセキュリティグループはすべてのトラフィックを許可します。

展開のトポロジとアプリケーションのニーズに基づいてセキュリティグループのルールを微調整します。

（注） データインターフェイスのセキュリティグループは、少なくともロードバランサからの SSH トラフィックを許可する必要があります。

Azure Logic App の更新

Logic App は、Auto Scale 機能の Orchestrator として機能します。ARM テンプレートによってスケルトン Logic App が作成されます。このアプリケーションを手動で更新して、Auto Scale Orchestrator として機能するために必要な情報を提供する必要があります。

ステップ 1 リポジトリから、LogicApp.txt ファイルをローカルシステムに取得し、次のように編集します。

重要　手順をすべて読んで理解してから続行してください。

手動の手順は、ARM テンプレートでは自動化されないため、Logic App のみ後で個別にアップグレードできます。

a) 必須: すべての「SUBSCRIPTION_ID」を検索し、サブスクリプション ID 情報に置き換えます。
b) 必須: すべての「RG_NAME」を検索し、リソースグループ名に置き換えます。
c) 必須: すべての「FUNCTIONAPPNAME」を検索し、Function App 名に置き換えます。

次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) （任意）トリガー間隔を編集するか、デフォルト値（5）のままにします。これは、Auto Scale 機能が定期的にトリガーされる時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
                    "frequency": "Minute",
                    "interval": 5
                },
```

e) （任意）ドレインする時間を編集するか、デフォルト値（5）のままにします。これは、スケールイン操作中にデバイスを削除する前に、Threat Defense Virtual から既存の接続をドレインする時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

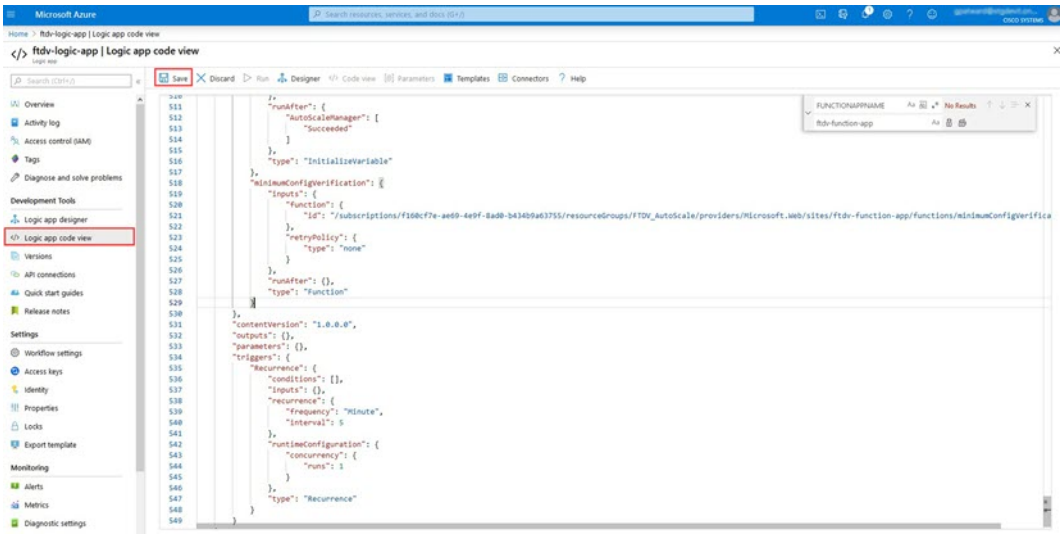
f) （任意）クールダウン時間を編集するか、デフォルト値（10）のままにします。これは、スケールアウト完了後に NO ACTION を実行する時間です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"actions": {
    "Branch_based_on_Scale-Out_or_Invalid_condition": {
        "actions": {
            "Cooldown_time": {
                "inputs": {
                    "interval": {
                        "count": 10,
                        "unit": "Second"
                    }
```

（注） これらの手順は、Azure ポータルからも実行できます。詳細については、Azure のドキュメントを参照してください。

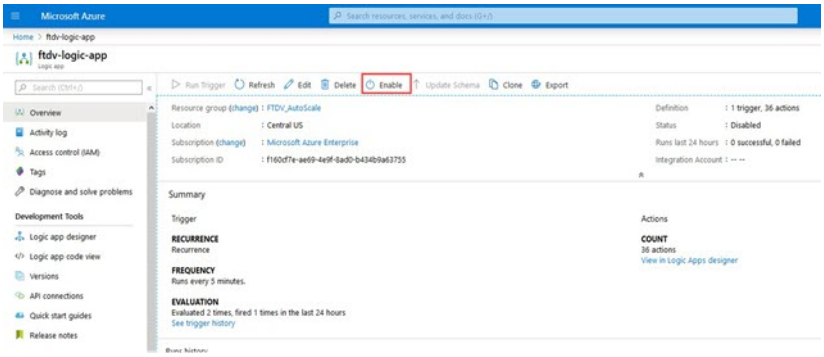
ステップ 2 [Logic Appコードビュー（Logic App code view）] に移動し、デフォルトの内容を削除して、編集した LogicApp.txt ファイルの内容を貼り付け、[保存（Save）] をクリックします。

図 *22 : Logic App* コードビュー



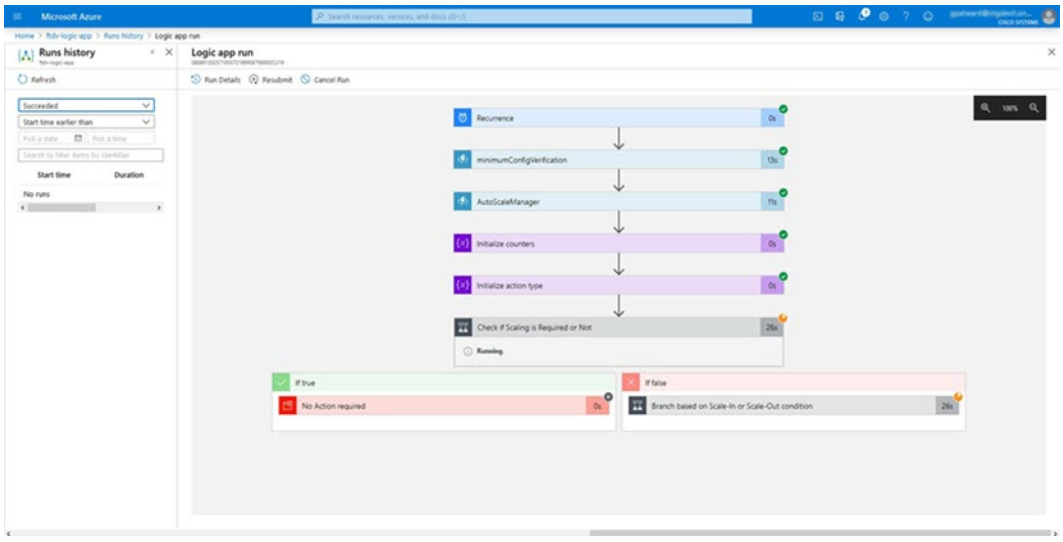
ステップ 3 Logic App を保存すると、[無効（Disabled）] 状態になります。Auto Scale Manager を起動する場合は、[有効化（Enable）] をクリックします。

図 *23 : Logic App* の有効化



ステップ 4 有効にすると、タスクの実行が開始されます。[実行中（Running）] ステータスをクリックしてアクティビティを表示します。

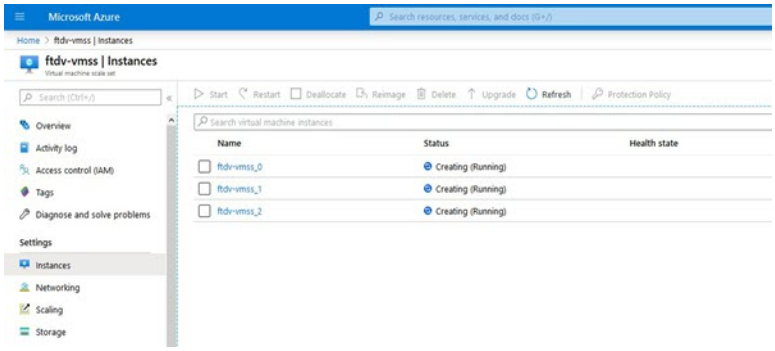
図 *24 : Logic App* の実行ステータス



ステップ 5 Logic App が起動すると、導入関連のすべての手順が完了します。

ステップ 6 Threat Defense Virtual インスタンスが作成されていることを VMSS で確認します。

図 *25 :* 稼働中の*Threat Defense Virtual* インスタンス



この例では、ARM テンプレートの展開で「'minFtdCount'」が「3」に設定され、「initDeploymentMode」が「BULK」に設定されているため、3 つの Threat Defense Virtual インスタンスが起動されます。

Threat Defense Virtualのアップグレード

Threat Defense Virtual アップグレードは、仮想マシンスケールセット（VMSS）のイメージアップグレードの形式でのみサポートされます。したがって、Threat Defense Virtual は Azure REST API インターフェイスを介してアップグレードします。

（注） 任意の REST クライアントを使用して Threat Defense Virtual をアップグレードできます。

始める前に

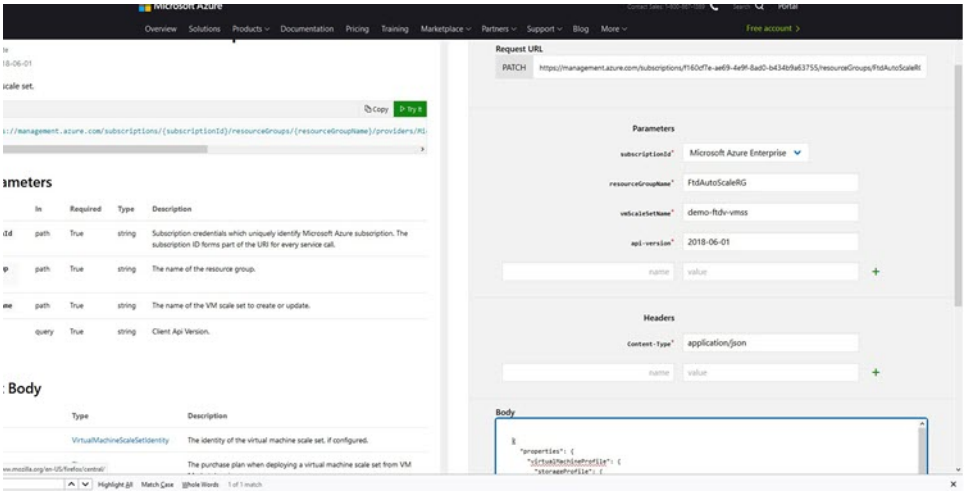
- 市場で入手可能な新しい Threat Defense Virtual イメージバージョンを取得します（例：650.32.0）。
- 元のスケールセットの展開に使用する SKU を取得します（例：ftdv-azure-byol）。
- リソースグループと仮想マシンスケールセット名を取得します。

ステップ 1 ブラウザで次の URL にアクセスします。

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

ステップ 2 [パラメータ（Parameters）] セクションに詳細を入力します。

図 *26 : Threat Defense Virtual*のアップグレード



ステップ 3 新しい Threat Defense Virtual イメージバージョン、SKU、トリガー RUN を含む JSON 入力を **[本文（Body）]** セクションに入力します。

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                    "imageReference": {
                          "publisher": "cisco",
                          "offer": "cisco-ftdv",
                          "sku": "ftdv-azure-byol",
                           "version": "650.32.0"
                    }
                },
            }
      }
}
```

ステップ 4 VMSS が変更を受け入れると、Azure から成功の応答が返ってきます。

新しいイメージは、スケールアウト操作の一環として起動される新しい Threat Defense Virtual インスタンスで使用されます。

- 既存の Threat Defense Virtual インスタンスは、スケールセットに存在している間、古いソフトウェアイメージを使用し続けます。
- 前述の動作を上書きし、既存の Threat Defense Virtual インスタンスを手動でアップグレードできます。これを行うには、VMSS の [アップグレード（Upgrade）] ボタンをクリックします。選択した Threat Defense Virtual インスタンスが再起動されて、アップグレードされます。アップグレードされた Threat Defense Virtual インスタンスは手動で再登録および再設定する必要があります。**この方法は推奨されません。**

Auto Scale ロジック

スケーリングメトリック

ARM テンプレートは、Threat Defense Virtual Auto Scale ソリューションに必要なリソースを展開するために使用されます。ARM テンプレートの展開中に、スケーリングメトリックに次のオプションがあります。

- CPU
- CPU、メモリ（バージョン 6.7 以降）。

（注） CPU メトリックは Azure から、メモリメトリックは Management Center から収集されます。

スケールアウトロジック

- **POLICY-1**：設定された期間に、**いずれか** Threat Defense Virtualの平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。「CPU、MEMORY」スケーリングメトリックを使用する場合、スケールアウトしきい値は、スケールセット内の**任意**の Threat Defense Virtual の平均 CPU **または**メモリ使用率です。
- **POLICY-2**：設定された期間に、**すべて**の Threat Defense Virtual デバイスの平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。「CPU、MEMORY」スケーリングメトリックを使用する場合、スケールアウトしきい値は、スケールセット内の**すべて**の Threat Defense Virtual デバイスの平均 CPU **または**メモリ使用率です。

スケールインロジック

- 設定された期間に、**すべて**の Threat Defense Virtual デバイスの CPU 使用率が設定されたスケールインしきい値を下回った場合。「CPU、MEMORY」スケーリングメトリックを使

用する場合、スケールセット内のすべての Threat Defense Virtual デバイスの CPU **および**メモリ使用率が、設定された期間に設定されたスケールインしきい値を下回ると、CPU の負荷が最小の Threat Defense Virtual が終了用に選択されます

注意

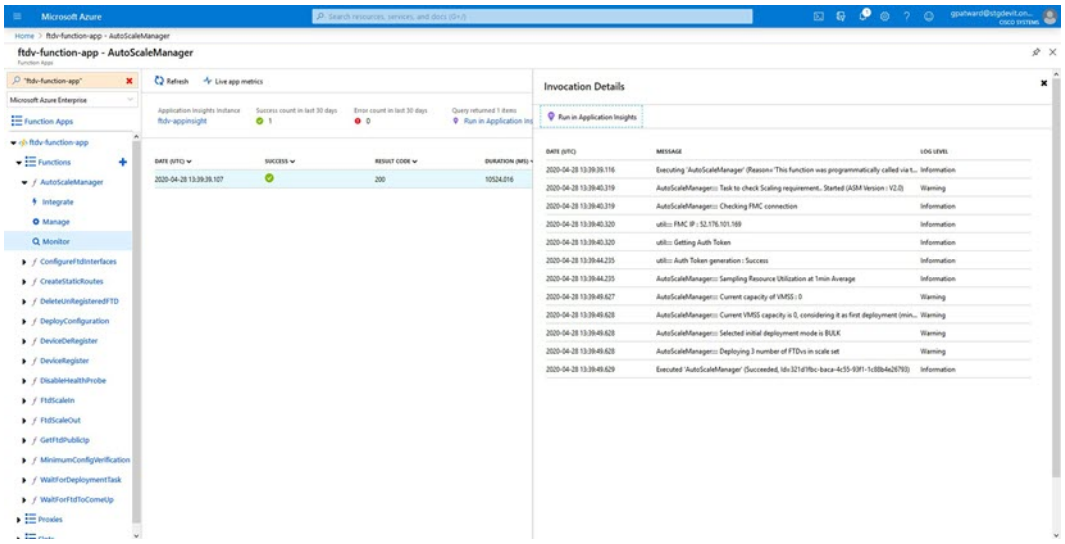
- スケールイン/スケールアウトは 1 つずつ行われます（つまり、一度に 1 つの Threat Defense Virtual だけがスケールインまたはスケールアウトされます）。
- Management Center から受信したメモリ消費量のメトリックは、経時的に計算された平均値ではなく、瞬間的なスナップショット/サンプル値です。したがって、スケーリングを決定する際にメモリメトリックだけを考慮することはできません。展開時にメモリのみのメトリックを使用するオプションはありません。

Auto Scale のロギングとデバッグ

サーバーレスコードの各コンポーネントには、独自のロギングメカニズムがあります。また、ログはアプリケーションインサイトにパブリッシュされます。

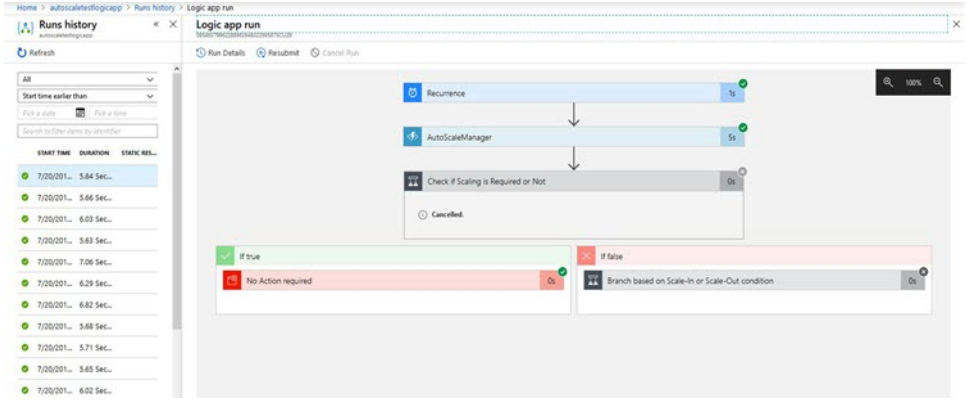
- 個々の Azure 関数のログを表示できます。

図 *27 : Azure* 関数ログ



- Logic App とその個々のコンポーネントの実行ごとに同様のログを表示できます。

図 *28 : Logic App* の実行ログ



- 必要な場合は、Logic App で実行中のタスクをいつでも停止または終了できます。ただし、現在実行中の Threat Defense Virtual デバイスが起動または終了すると、一貫性のない状態になります。
- 各実行または個々のタスクにかかった時間は、Logic App で確認できます。
- Function App は、新しい zip をアップロードすることでいつでもアップグレードできます。Logic App を停止し、すべてのタスクの完了を待ってから、Function App をアップグレードします。

Auto Scale のガイドラインと制約事項

Threat Defense Virtual Auto Scale for Azure を導入する場合は、次のガイドラインと制限事項に注意してください。

- （バージョン 6.6 以前）スケーリングの決定は、CPU 使用率に基づきます。
- （バージョン 6.7 以降）スケーリングの決定には、CPU のみの使用率、または CPU とメモリの使用率を使用できます。
- Management Center の管理が必要です。Device Manager はサポートされていません。
- Management Center にはパブリック IP アドレスが必要です。
- Threat Defense Virtual 管理インターフェイスは、パブリック IP アドレスを持つように設定されます。
- IPv4 だけがサポートされます。
- Threat Defense Virtual Auto Scale for Azure は、デバイスグループに適用され、スケールアウトされた Threat Defense Virtual インスタンスに伝播されるアクセスポリシー、NAT ポリシー、プラットフォーム設定などの設定のみをサポートします。Management Center を使用してデバイスグループの設定のみ変更できます。デバイス固有の設定はサポートされていません。

- ARM テンプレートの入力検証機能は限られているため、入力を正しく検証するのはユーザーの責任です。
- Azure 管理者は、Function App 環境内の機密データ（管理者ログイン情報やパスワードなど）をプレーンテキスト形式で確認できます。Azure Key Vault サービスを使用して、センシティブデータを保護できます。
- 設定の変更は、すでに実行中のインスタンスには自動的に反映されません。変更は新しいデバイスにのみ反映されます。このような変更は、既存のデバイスに手動でプッシュする必要があります。
- 既存のインスタンスの設定を手動で更新しているときに問題が発生した場合は、それらのインスタンスをスケーリンググループから削除し、新しいインスタンスに置き換えることを推奨します。

トラブルシューティング

次に、Threat Defense Virtual Auto Scale for Azure の一般的なエラーシナリオとデバッグのヒントを示します。

- Management Center への接続に失敗する：Management Center の IP またはログイン情報を確認してください。Management Center が障害状態または到達不能状態であるか確認します。
- Threat Defense Virtual に SSH 接続できない：複雑なパスワードがテンプレートを介して Threat Defense Virtual に渡されているか確認します。セキュリティグループで SSH 接続が許可されているか確認します。
- ロードバランサのヘルスチェックエラー：Threat Defense Virtual がデータインターフェイスの SSH に応答しているか確認します。セキュリティグループの設定を確認します。
- トラフィックの問題：ロードバランサルール、Threat Defense Virtual で設定された NAT ルールおよびスタティックルートを確認します。テンプレートとセキュリティグループルールで提供される Azure 仮想ネットワーク/サブネット/ゲートウェイの詳細を確認します。
- Threat Defense Virtual を Management Center に登録できない：新しい Threat Defense Virtual デバイスに対応するために Management Center の容量を確認します。ライセンスを確認します。Threat Defense Virtual バージョンの互換性を確認します。
- Logic App が VMSS にアクセスできない：VMSS の IAM ロール設定が正しいか確認します。
- Logic App の実行時間が長すぎる：スケールアウトされた Threat Defense Virtual デバイスで SSH アクセスを確認します。Management Center でデバイス登録の問題を確認します。Azure VMSS で Threat Defense Virtual デバイスの状態を確認します。
- サブスクリプション ID 関連の Azure 関数のスローエラー：アカウントでデフォルトのサブスクリプションが選択されていることを確認します。

- スケールイン操作の失敗：Azure でのインスタンスの削除には長時間かかることがあります。このような状況では、スケールイン操作がタイムアウトし、エラーが報告されますが、最終的にはインスタンスが削除されます。
- 設定を変更する前に、Logic App を無効にし、実行中のすべてのタスクが完了するまで待ちます。

Azure GWLB 展開を使用した Threat Defense Virtual 自動スケーリング中に問題が発生した場合のトラブルシューティングのヒントは次のとおりです。

- ELB と GWLB の関連付けを確認します。
- GWLB で正常性プローブのステータスを確認します。
- Threat Defense Virtual の物理インターフェイスおよび論理インターフェイスでトラフィックフローを確認して、VXLAN 設定を確認します。
- セキュリティグループのルールを確認します。

ソースコードからの Azure 関数の構築

システム要件

- Microsoft Windows デスクトップ/ラップトップ。
- Visual Studio（Visual Studio 2019 バージョン 16.1.3 でテスト済み）

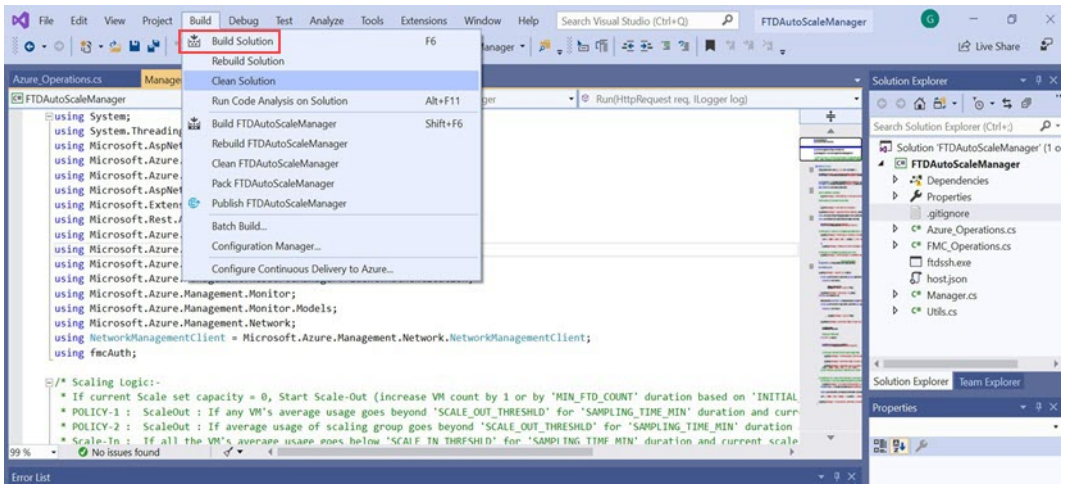
（注） Azure 関数は C# を使用して記述されます。

- 「Azure 開発」ワークロードを Visual Studio にインストールする必要があります。

Visual Studio を使用したビルド

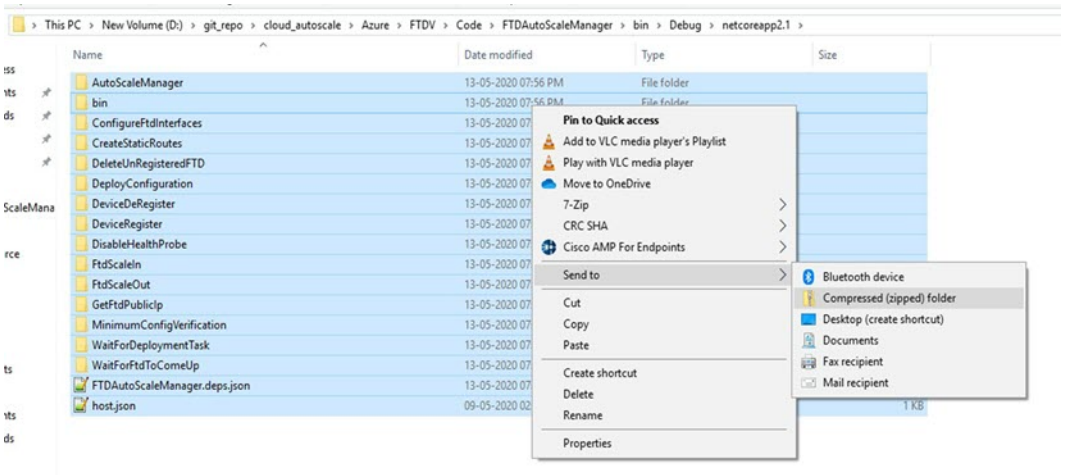
1. 「code」フォルダをローカルマシンにダウンロードします。
2. 「FTDAutoScaleManager」フォルダに移動します。
3. Visual Studio でプロジェクトファイル「FTDAutoScaleManager」を開きます。
4. クリーンアップしてビルドするには、Visual Studio の標準手順を使用します。

図 *29 : Visual Studio* ビルド



5. ビルドが正常にコンパイルされたら、**\bin\Release\netcoreapp2.1** フォルダに移動します。
6. すべての内容を選択し、**[送信先（Send to）]** > **[圧縮（ZIP）フォルダ（Compressed (zipped) folder）]** の順にクリックして、ZIP ファイルを ASM_Function.zip として保存します。

図 *30 : ASM_Function.zip* のビルド



Azure Virtual WAN への Cisco Secure Firewall Threat Defense Virtual の展開

Azure Virtual WAN での Threat Defense Virtual の概要

Microsoft Azure Virtual WAN では、「ハブアンドスポーク」アーキテクチャが採用されており、さまざまな仮想ネットワークとブランチロケーション全体のトラフィックを管理できます。Azure Virtual WAN 内では、Threat Defense Virtual と Azure Virtual ハブを統合することで、組織のオンプレミス（スポーク）ネットワーク（本社、ブランチ、リモートユーザーなど）から発信されたトラフィックがハブを通過し、Azure ネットワーク上の Vnet にアクセスする際の効率的な管理と検査が容易になります。統合し、Threat Defense Virtual 機能をファイアウォールとして使用することで、専用の接続チャネルを介したネットワークトラフィックの管理、検査、フィルタリング、およびルーティングが容易になります。

（注） Azure Virtual WAN では、インターフェイスが 3 つだけの Threat Defense Virtual 導入モデルがサポートされています。

Azure Virtual WAN ハブに Threat Defense Virtual を展開すると、次のような利点を得られます。

- ハブに接続された各スポークにファイアウォール ソリューションを実装する必要がない。
- 内部ロードバランサ（ILB）の Azure の組み込み機能を活用できる。
- 展開時の事前定義された設定によるインスタンスのスケーリング。

仮想 WAN ハブへの Threat Defense Virtual の展開については、「Azure Virtual WAN への Threat Defense Virtual の展開」を参照してください。

Azure Virtual WAN 上の Threat Defense Virtual を介したトラフィックルーティング

Azure Virtual WAN でのトラフィックのルーティング方法

Azure Virtual WAN は、ルーティングテーブルを常に更新および共有しながら、異なる Azure ネットワーク間でトラフィックを送信するための最適なルートを決定するのに役立つダイナミック ルーティング プロトコルであるボーダー ゲートウェイ プロトコル（BGP）を提供します。仮想 WAN ハブは、BGP エンドポイント（高可用性用）と自律システム番号（ASN）のセットを提供します。これらは、Management Center で Threat Defense Virtual の BGP ネイバーとして設定する必要があります。

スタティックルーティング方式を使用して、Threat Defense Virtual でルートを手動で設定することもできます。

Azure でのルーティングの詳細 については、Azure ドキュメントの「BGP および VPN Gateway について」を参照してください。

ルーティングインテント

ルーティングインテントは、検査のためにハブに展開された Threat Defense Virtual ファイアウォールにインターネット向けトラフィックとプライベートトラフィックを転送するプロセスを簡素化する、Azure Virtual WAN ハブのルーティング機能です。

詳細 については、Azure ドキュメントの Routing Intent [英語] を参照してください。

システム要件

スケーリング単位

最大スループットを実現するために必要なスケーリングは、Azure Virtual WAN ハブでの展開時に選択または設定する Threat Defense Virtual インスタンス（NVA）のサイズと数によって異なります。

例：**D3_V2** サイズの 2 つの Threat Defense Virtual インスタンスで 2.8 Gbps をサポートできる場合、NVA スループットは **Scale-Unit-4: 2.8 Gbps** として定義されます。

表 *3 :* インスタンスタイプに基づく *Threat Defense Virtual* スループットレベル

スケール単位	Threat Defense Virtual インスタンス	インスタンス タイプ	スループットのサポートレベル
4	2	Standard_D3_v2	3.2 Gbps
10	2	Standard_D4_v2	4.8 Gbps
20	2	Standard_D5_v2	12 Gbps
40	3	Standard_D5_v2	18 Gbps
60	4	Standard_D5_v2	24 Gbps
80	5	Standard_D5_v2	30 Gbps

制限事項

インターフェイス

Azure の制限により、NVA でサポートできるネットワーク インターフェイスは最大 3 つなので、Azure Virtual WAN ハブの Threat Defense Virtual では、展開用に 3 つ のインターフェイスがサポートされます。

（注） 3 つのインターフェイスモデルをサポートする Threat Defense Virtual バージョン 7.4.1 以降は、Azure Virtual WAN の展開と互換性があります。

Threat Defense Virtual ネットワーク インターフェイスの 3 つのサブネットは次のとおりです。

- **管理インターフェイス**：パブリック IP アドレスを使用して Threat Defense Virtual を Management Center に接続する**最初のインターフェイス**です。
- **外部インターフェイス（必須）**：Threat Defense Virtual を信頼できないパブリック IP アドレスに接続する **2 番目のインターフェイス**です。
- **内部インターフェイス（必須）**：Threat Defense Virtual を仮想 WAN ハブに接続し、信頼できるプライベート IP アドレス上のホストネットワーク内に接続する **3 番目のインターフェイス**です。

ネットワーク仮想アプライアンス（NVA）としての Threat Defense Virtual

次に、Azure Virtual WAN の NVA としての Threat Defense Virtual のネットワーク構成に関連する主な機能を示します。

- Azure Virtual WAN への Threat Defense Virtual の展開時に、Azure の内部で VNet とサブネットが作成されるため、展開完了後は、VNet とサブネットの変更や作成はできませんが、展開後にインスタンスに接続されている IP アドレスはすべて確認できます。
- インターフェイスごとにネットワーク セキュリティ グループのポートは選択できませんが、それらのポートは展開時に事前定義されます。管理インターフェイスでインターネットに接続できるのは、TCP ポート 443、8305、および 22 のみです。
- 内部インターフェイスでは、Azure Virtual WAN ハブとそのハブに接続されている内部ネットワーク内の通信のみ許可されます。

Azure Virtual WAN ハブの Threat Defense Virtual へのアクセス制限

管理対象リソースグループに対するマネージドアプリケーションとしてハブに展開されている Threat Defense Virtual インスタンスにアクセスするための承認が必要です。管理者は、この管理対象リソースグループへの限定または制限されたアクセス権を付与できます。

Azure マネージドアプリケーションは、マネージドアプリケーションへのアクセスを定義できるジャストインタイム（JIT）アクセス機能を提供します。JIT の詳細については、Azure のドキュメントの「Azure マネージドアプリケーションの概要」および「ジャストインタイム」を参照してください。

IP サポート

- IPv4 だけがサポートされます。

サポートされない機能

- Day-0/カスタムデータによるブートストラップはサポートされていません。
- Threat Defense Virtual は、Azure へのメトリックのストリーミングをサポートしていません。

- オペレーティング システム ディスクの交換による仮想マシンのアップグレードはサポートされていません。
- Threat Defense Virtual への SSH キーベースのログインはサポートされていません。
- PAYG はサポートされていません。

ライセンシング

シスコ スマート ライセンス アカウントを使用する BYOL。

ネットワーク トポロジ

Threat Defense Virtual は、Azure Virtual WAN ハブの NVA として、インターネット、ブランチ（サイト）、または VNet などのさまざまなオンプレミスネットワーク（スポーク）からハブを通過するネットワーク トラフィック ルーティングを検査します。

ネットワークトラフィックが通過するトラフィックルートは、次のトポロジに分類されます。

- East-West：ブランチからブランチ
- East-West：VNet から VNet
- North-South：ブランチからインターネット
- North-South：VNet からインターネット

（注） Threat Defense Virtual を介した**インターネットから VNet またはブランチへの**トラフィックは、Cisco Secure Firewall バージョン 7.4.1 ではサポートされていません。

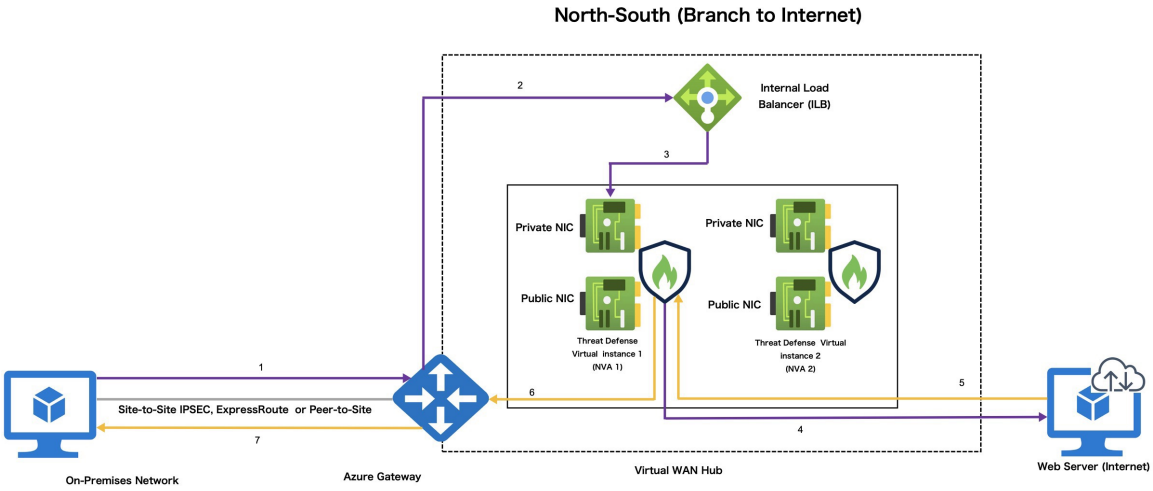
（注） Azure リージョン全体に複数のハブを展開し、仮想 WAN に接続できます。また、East-West および North-South トラフィック検査用の独自の Threat Defense Virtual を持つように各ハブを設定できます。

単一の仮想 WAN ハブでの Threat Defense Virtual による North-South トラフィック検査トポロジ

このトポロジは、次の間を移動するネットワークトラフィックを検査する Threat Defense Virtual を参照します。

- 仮想 WAN ハブに接続されているブランチと VNet、およびその逆。

図 *31 : Azure Virtual WAN* ハブの *Threat Defense Virtual North-South* トラフィック検査トポロジ



次の手順では、North-South トラフィック検査のトラフィックフロープロセスについて説明します。

1. オンプレミスネットワークで Azure ゲートウェイにトラフィックが送信されます。
2. ゲートウェイから ILB に転送されます。
3. ILB から Threat Defense Virtual（NVA）に送信されます。
4. NVA SNAT により PIP がインスタンス化され、インターネットに送信されます。
5. Web サーバーがインスタンス PIP Threat Defense Virtual（NVA）に応答すると、SNAT が取り消され、ゲートウェイに転送されます。
6. ゲートウェイからオンプレミスネットワークに転送されます。

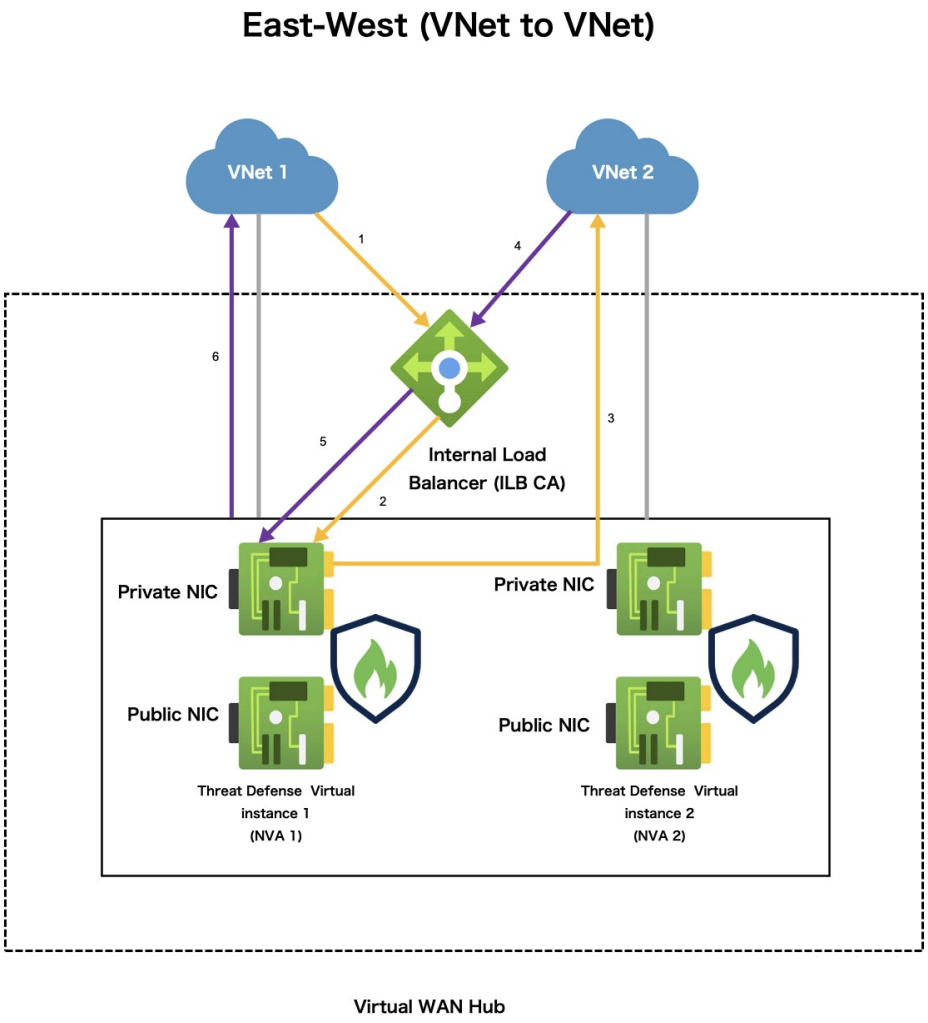
単一の仮想 WAN ハブでの Threat Defense Virtual による East-West トラフィック検査トポロジ

このトポロジは、次の間を移動するネットワークトラフィックを検査する Threat Defense Virtual を参照します。

- 仮想 WAN ハブに接続されているブランチと VNet、およびその逆。
- 仮想 WAN ハブに接続されたブランチまたは VNet へのインターネット。

図 *32 : Azure Virtual WAN* ハブの *Threat Defense Virtual East-West* トラフィック検査トポロジ

このトポロジは、Threat Defense Virtual を参照し、仮想 WAN ハブに接続されているサイト間（ブランチとブランチ）間と VNet 間を移動するネットワークトラフィックを検査します。



次の手順では、East-West トラフィック検査のトラフィックフロープロセスについて説明します。

1. VNet1 から ILB にトラフィックが送信されます。
2. ILB でアクティブなインスタンスが 1 つ選択されます。
3. Threat Defense Virtual（NVA）から宛先（VNet 2）に直接送信されます。
4. VNet から ILB にトラフィックが送信されます。
5. ILB から、適切な状態の Threat Defense Virtual（NVA）にトラフィックが完全に転送されます。
6. Threat Defense Virtual（NVA）から VNet 1 にトラフィックが返送されます。

Azure Virtual WAN への Threat Defense Virtual の展開

Azure マーケットプレイスで入手可能な Azure Virtual WAN 向け Cisco Secure Firewall Threat Defense Virtual サービスを使用して、Azure Virtual WAN ハブに Threat Defense Virtual を展開できます。

前提条件

- Microsoft Azure アカウント。https://azure.microsoft.com/en-us/ で 1 つ作成できます。
- 仮想 WAN にハブを作成します。Azure での仮想ハブの作成については、Azure のドキュメントの「ハブを作成する」を参照してください。
- 仮想 WAN ハブのアドレス空間は、/23 以下である必要があります。
- Cisco スマートアカウント。Cisco Software Central で作成できます。

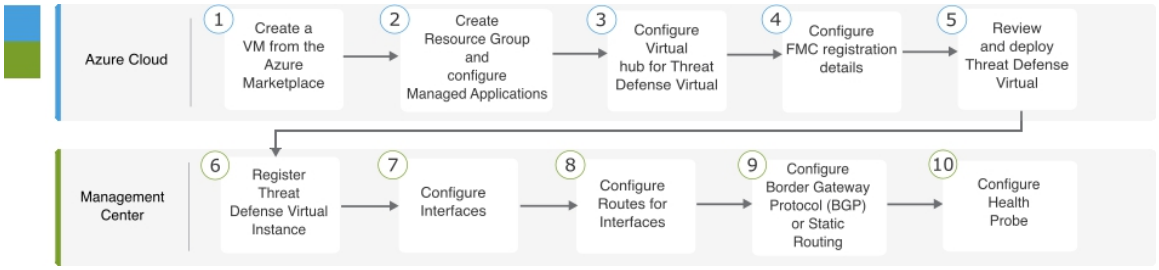
（注） Threat Defense Virtual インスタンスの展開後、そのインスタンスに接続されているすべてのパブリック IP とプライベート IP を確認できます。

通信パス

- 管理インターフェイス：Threat Defense Virtual を Management Center 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）：Threat Defense Virtual を内部ホストに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）：Threat Defense Virtual 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。

エンドツーエンドの手順

次のフローチャートは、ソリューションテンプレートを使用して Azure Virtual WAN に Threat Defense Virtual を展開する際のワークフローを示しています。



	ワークスペース	手順
1	Azure Cloud	ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：Azure マーケットプレイスで「Cisco Secure Firewall Threat Defense Virtual for Azure VWAN」を検索します。
2	Azure Cloud	ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：リソースグループを作成し、マネージドアプリケーションを設定します。
3	Azure Cloud	ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：仮想ハブと NVA の詳細を設定します。
4	Azure Cloud	ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：FMC 登録の詳細を設定します。
5	Azure Cloud	ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開：Threat Defense Virtual を確認して展開します。
6	Management Center または Device Manager	Management Center での Threat Defense Virtual インスタンスの登録：Threat Defense Virtual インスタンスを登録します。
7	Management Center または Device Manager	インターフェイスの設定：外部インターフェイスと内部インターフェイスを設定します。
8	Management Center または Device Manager	インターフェイスのルートの設定：ゲートウェイ IP アドレスを計算し、外部インターフェイスと内部インターフェイスのルートを設定します。
9	Management Center または Device Manager	トラフィックルーティングの設定：ボーダーゲートウェイプロトコル（BGP）またはスタティックルーティングを設定します。
10	Management Center または Device Manager	正常性プローブの設定：Threat Defense Virtual インスタンスの定期的なヘルスチェックを実行するために ILB を有効にするように正常性プローブを設定します。

ソリューションテンプレートを使用した Azure Virtual WAN への Threat Defense Virtual の展開

次の手順は、Azureマーケットプレイスで利用できるソリューションテンプレートを使用して、Azure Virtual WAN に Threat Defense Virtual を展開する方法を示しています。これは、Microsoft Azure Virtual WAN 環境で Threat Defense Virtual をセットアップする手順の概略です。

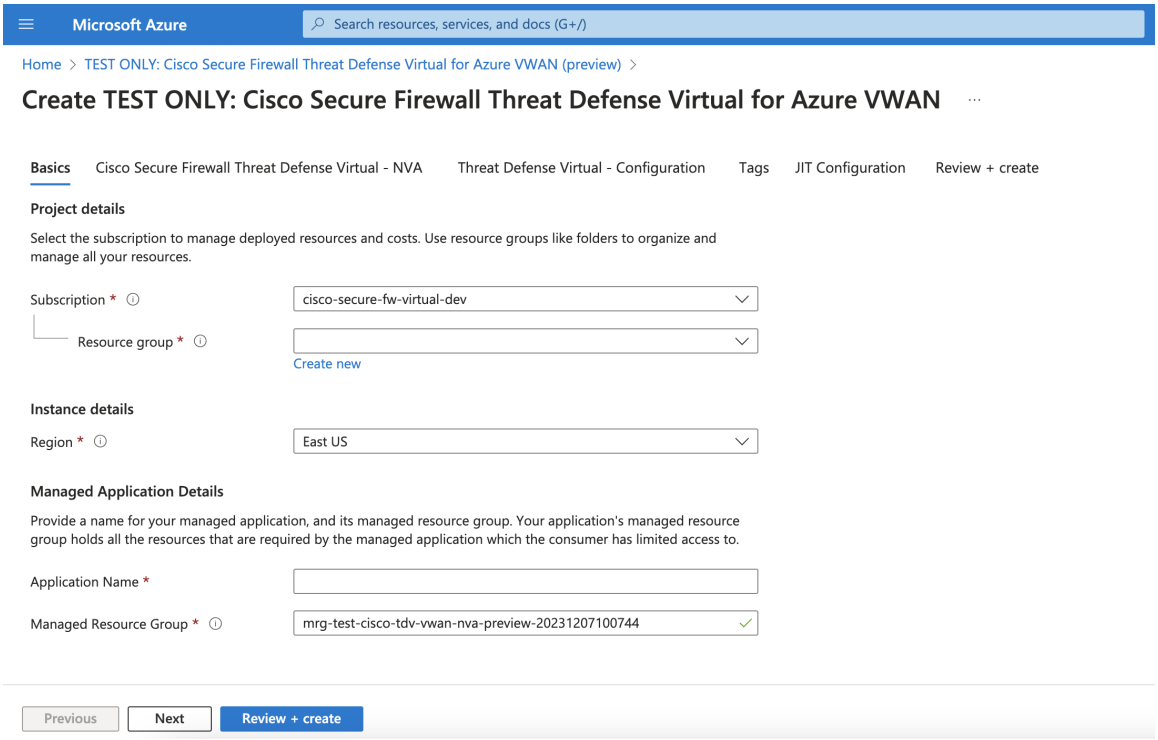
Azure のセットアップの詳細については、「Azure の使用を開始する」を参照してください。

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

Azure ポータルには、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が表示されます。

ステップ 2 [Azureマーケットプレイス（Azure Marketplace）]>[仮想マシン（Virtual Machines）] を順に選択します。

ステップ 3 マーケットプレイスで **Cisco Secure Firewall Threat Defense Virtual for Azure VWAN** を検索し、サービスを選択し、[作成（Create）] をクリックして [基本（Basics）] ページを表示します。



ステップ 4 [Basics] 設定を構成します。

a) サブスクリプションを選択します。

b) 新しい [リソースグループ（Resource Group）] を作成します。

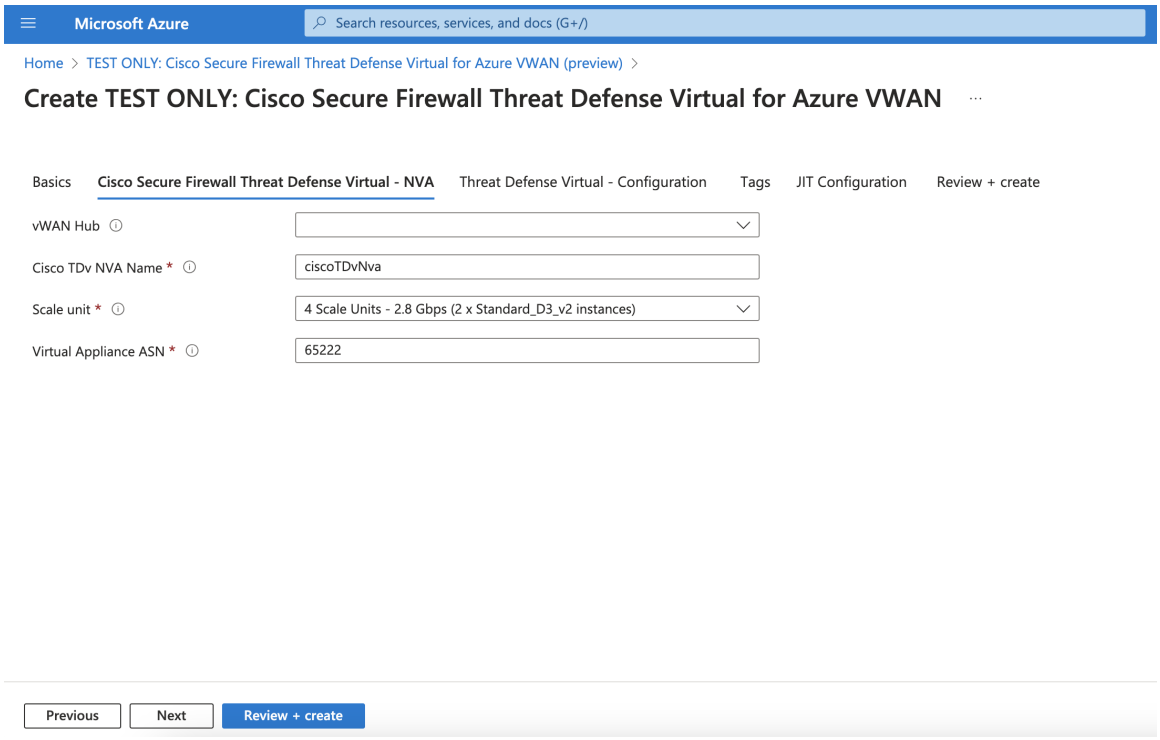
c) 仮想 WAN ハブの地理的な場所または地域を選択します。この展開で使用されるすべてのリソース（仮想 WAN ハブ、Threat Defense Virtual、ネットワーク、ストレージアカウントなど）に関して、同じ場所または地域を選択する必要があります。

ステップ 5 [マネージドアプリケーションの詳細（Managed Application Details）] の設定を設定します。

a) Threat Defense Virtual インスタンスを NVA として展開している管理対象リソースグループのマネージドアプリケーションの名前を入力します。

b) Threat Defense Virtual インスタンスを展開する管理対象リソースグループを選択します。

ステップ 6 [次へ（Next）] をクリックして、[Cisco Secure Firewall Threat Defense Virtual：NVA] ページを表示します。



ステップ 7 仮想ハブと NVA の詳細を設定します。

a) [vWANハブ（vWAN Hub）] ドロップダウンリストから仮想 WAN ハブを選択して、Threat Defense Virtual インスタンスを展開します。

b) 展開している Threat Defense Virtual インスタンスの適切な名前を入力します。

c) 展開する Threat Defense Virtual インスタンスの数を定義するスケール単位を選択します。

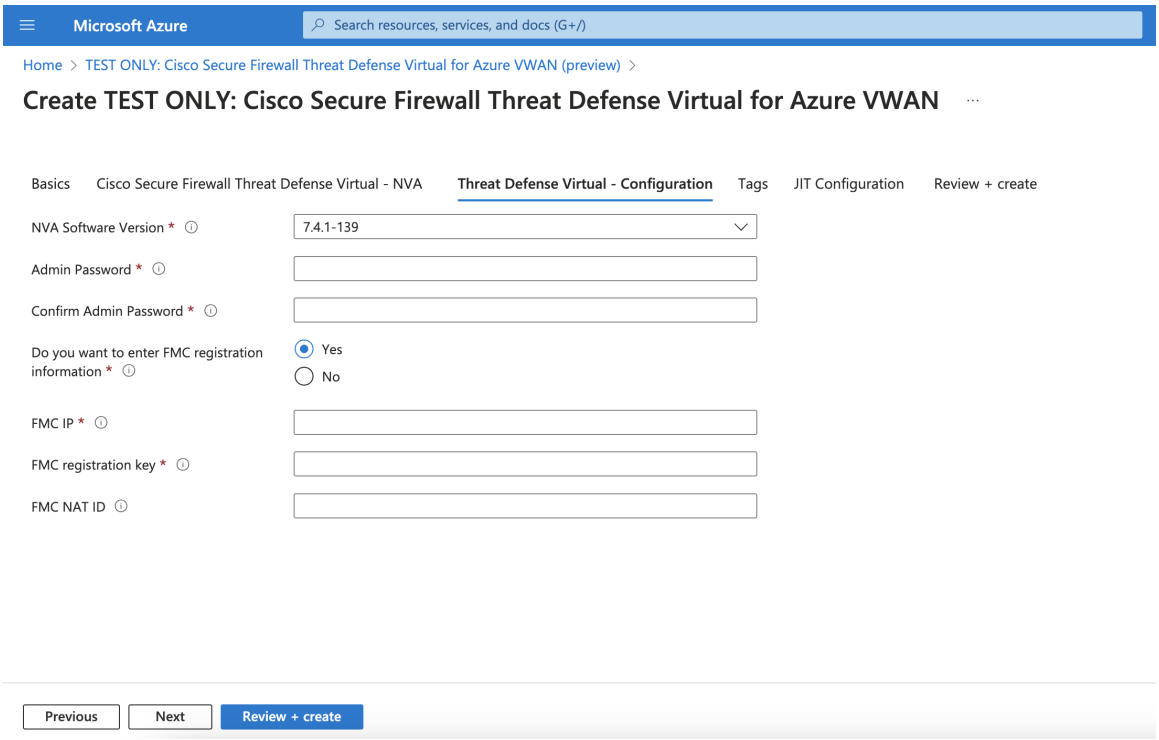
必要な NVA スループットレベルを実現するために必要なスケール単位を選択できます。たとえば、**4 つのスケール単位：2.8 Gbps（2 X Standard_D3_v2_instances）**を選択すると、「**スケール単位の数：スループットレベル（インスタンスタイプがある 2 つの Threat Defense Virtual**）が示唆されます。

（注） スケール単位では、ハブに展開している Threat Defense Virtual インスタンスの数と、関連付けられたインスタンスタイプを定義します。

d) [仮想アプライアンスASN（Virtual Appliance ASN）] を入力します。

（注） 入力する ASN 値は、64,512 ～ 65,534 の範囲内の値である必要があります。

ステップ 8 [次へ（Next）] をクリックして、[Threat Defense Virtual：設定（Threat Defense Virtual - Configuration）] ページを表示します。



ステップ 9 [NVAソフトウェアバージョン（NVA Software Version）] ドロップダウンリストから、適切な互換性のあるバージョンを選択します。

（注） このフィールドには、展開している対応する Threat Defense Virtual バージョンと互換性のある NVA ソフトウェアバージョンのリストが表示されます。リストから適切なバージョンを選択してください。

ステップ 10 Threat Defense Virtual インスタンスを含む管理対象リソースグループにアクセスするために必要な管理者パスワードを作成し、確認します。

ステップ 11 [はい（Yes）] をクリックして、[FMC登録情報（FMC registration information）] を入力します。

a) [FMC IP] アドレスを入力します。

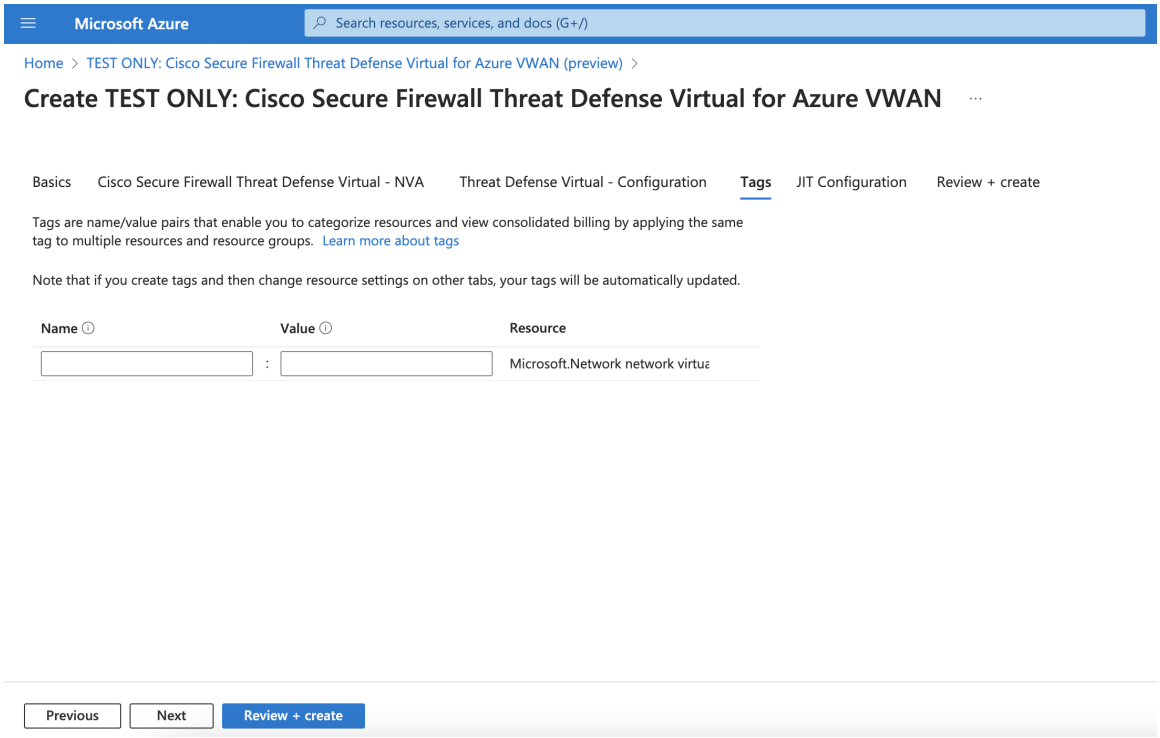
b) Threat Defense Virtual インスタンスを登録するための [FMC登録キー（FMC Registration Key）] を入力します。

（注）
- FMC 登録キーは、1 ～ 37 文字の英数字文字列である必要があります。このキーは、Threat Defense Virtual を追加するときに Management Center で入力します。

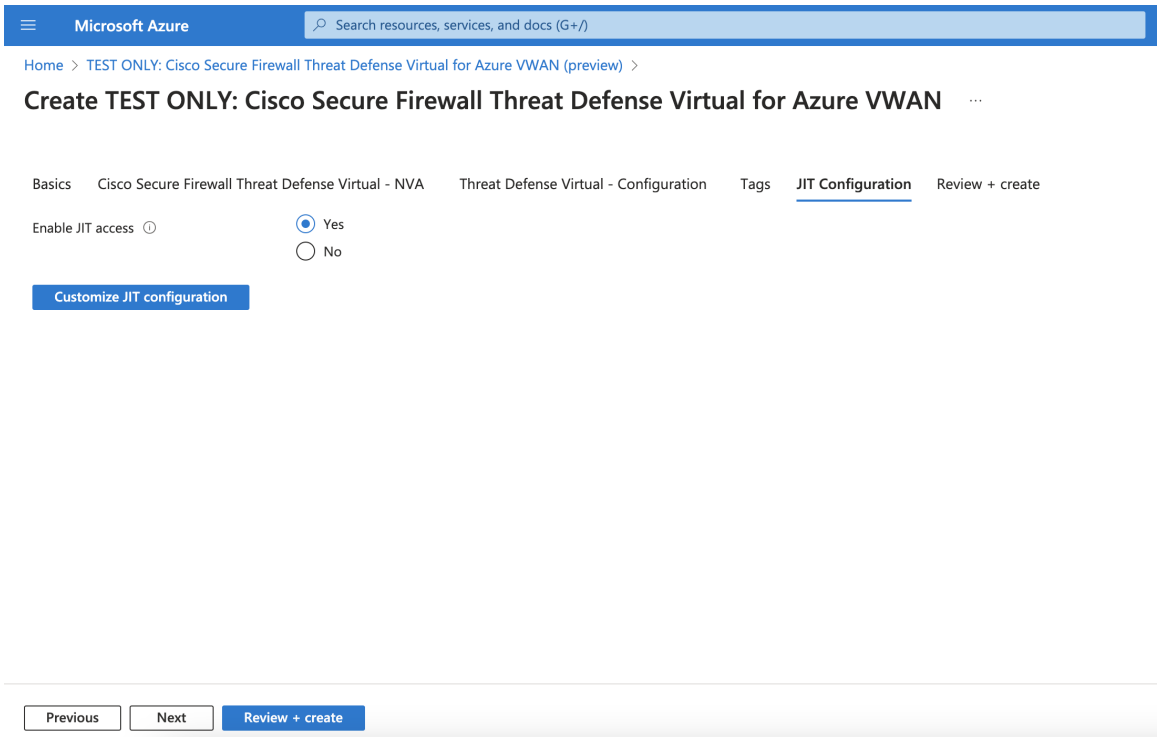
c) （任意）インスタンスの登録時に使用される Management Center NAT ID を入力します。

（注）
- NAT ID は 1 ～ 37 文字の英数字文字列である必要があり、Management Center とデバイス間の登録プロセス中に、一方で IP アドレスが指定されていない場合にのみ使用されます。NAT ID は基本的にワンタイムパスワードなので一意である必要があり、登録を待機している他のデバイスによって使用されないようにする必要があります。登録を成功させるには、Threat Defense Virtual を追加するときに、FMC で同じ NAT ID を指定してください。

ステップ 12 [次へ（Next）] をクリックして、[タグ（Tags）] を設定します。

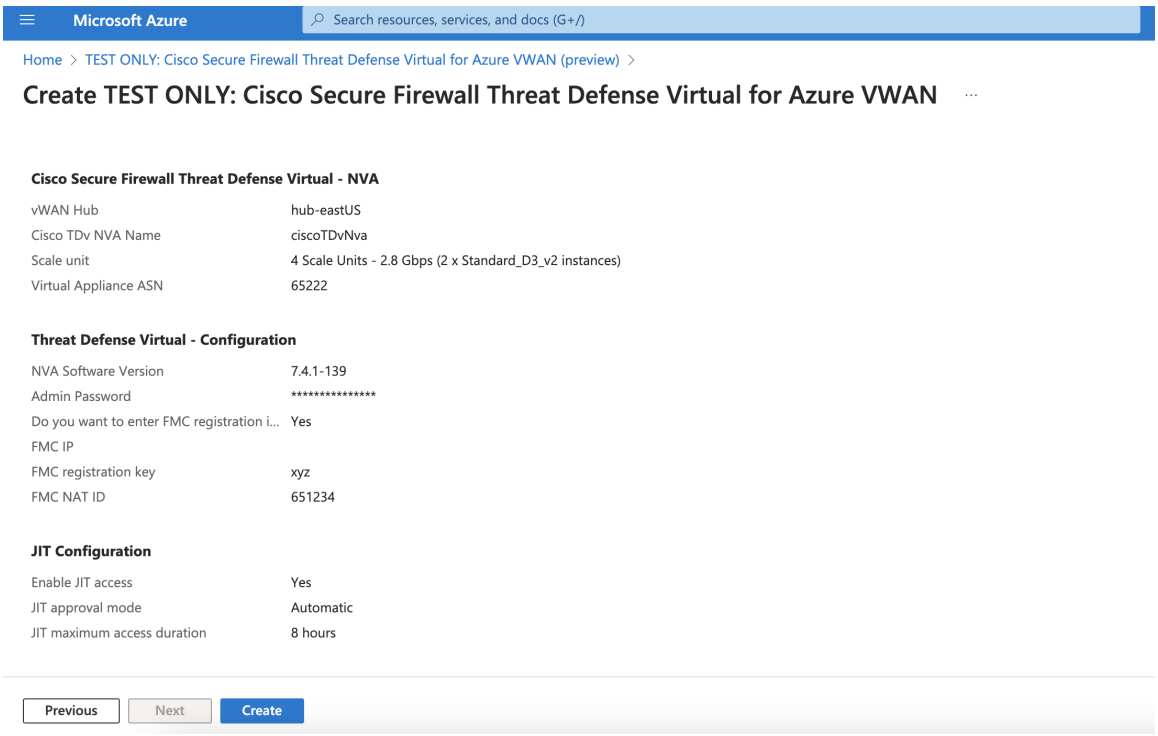


ステップ 13 [次へ（Next）] をクリックして、[JITの設定（JIT configuration）] ページを表示します。



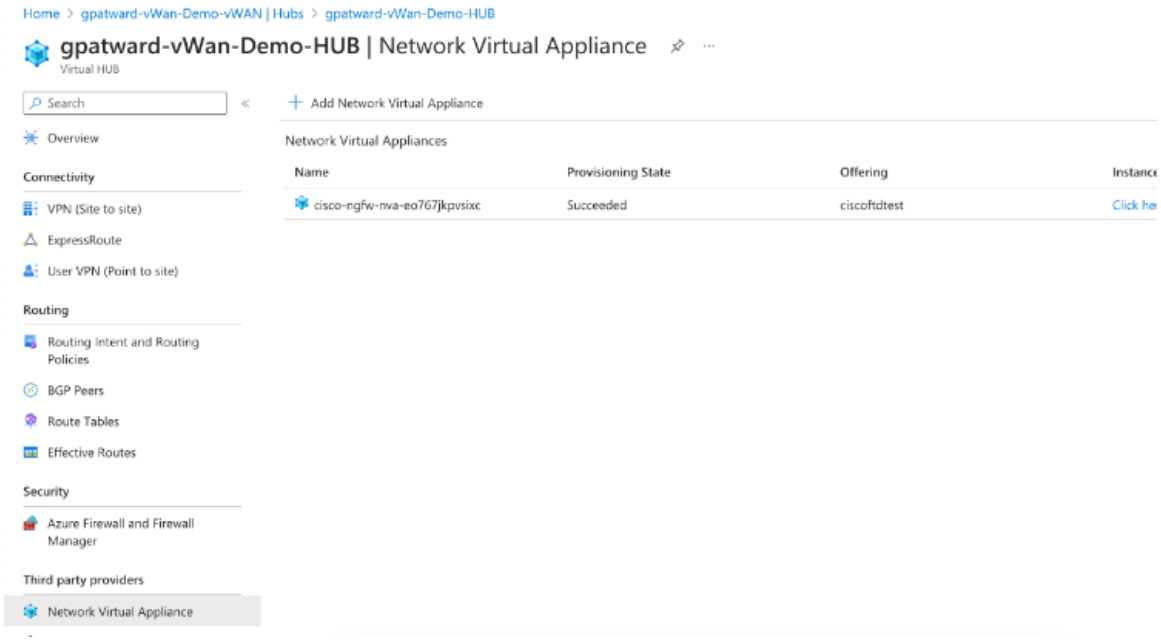
デフォルトでは、[JITアクセスの有効化（Enable JIT access）] オプションは [はい（Yes）] に設定されているため、Threat Defense Virtual インスタンスを管理およびトラブルシューティングするためのプロビジョニングアクセスの JIT が有効になります。

ステップ 14 [次へ（Next）] をクリックして、[確認と作成（Review+Create）] ページを表示します。



ステップ 15 展開する前に、サブスクリプション、NVA、Threat Defense Virtual、および JIT の設定の詳細を確認し、利用規約に同意してから [作成（Create）] をクリックして、仮想 WAN ハブに Threat Defense Virtual（NVA）を展開する必要があります。

ステップ 16 **[ホーム（Home）]> [セキュリティ（Security）]> [サードパーティプロバイダー（Third-party providers）]** の順に選択し、[ネットワーク仮想アプライアンス（Network Virtual Appliance）] をクリックして、ハブで作成された NVA を表示します。



ステップ 17 [NVA] をクリックして、展開されたすべての Threat Defense Virtual インスタンスを表示します。

インスタンスの管理パブリック IP アドレスを使用して Threat Defense Virtual にアクセスし、SSH を使用してログインできます。

（注） ハブに展開する各 Threat Defense Virtual インスタンスのパブリック IP アドレスは、Management Center でのインスタンスの登録に使用されます。

次のタスク

Management Center のハブに展開した Threat Defense Virtual インスタンスを登録して設定します。

Management Center での Threat Defense Virtual の設定

ハブに展開された各 Threat Defense Virtual インスタンスは、Management Center を介して設定します。

デバイスグループを含め、Threat Defense Virtual の設定と管理に必要なすべてのオブジェクトを作成すると、複数のデバイスにポリシーを簡単に展開して、更新をインストールできます。デバイスグループに適用されたすべての設定が Threat Defense Virtual インスタンスにプッシュされます。

ここでは、Management Center で Threat Defense Virtual インスタンスを設定するための基本的な手順の概要を示します。

詳細については、Cisco Secure Firewall Management Center デバイス 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。

Management Center での Threat Defense Virtual インスタンスの登録

仮想 WAN ハブに展開されているすべての Threat Defense Virtual インスタンスを、Management Center の共通のデバイスグループに登録する必要があります。登録すると、各インスタンスにポリシーと設定をすばやく展開できます。

始める前に

- Azure Virtual WAN ハブに展開されている各 Threat Defense Virtual インスタンスの管理パブリック IP アドレスが必要です。このアドレスは、Management Center にデバイスをセットアップして登録するために使用されます。
- Management Center でデバイスグループを作成します。「デバイスグループの追加」を参照してください。
- アクセス コントロール ポリシーを作成します。「基本的なアクセス コントロール ポリシーの作成」を参照してください。
- ハブに Threat Defense Virtual を展開中に作成された FMC 登録キー。

ステップ 1 Management Center にログインします。
ステップ 2 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
ステップ 3 **[追加（Add）]** > **[デバイス（Device）]**の順にクリックします。
ステップ 4 ハブに展開されている Threat Defense Virtual インスタンスのパブリック IP アドレスを入力します。
ステップ 5 Threat Defense Virtual インスタンスの表示名を指定します。
ステップ 6 ハブに Threat Defense Virtual を展開中に作成した Management Center の**登録キー**を入力します。
ステップ 7 [グループ（Group）] ドロップダウンリストから、Threat Defense Virtual インスタンスを追加するデバイスグループを選択します。
ステップ 8 [アクセスコントロールポリシー（Access Control Policy）] ドロップダウンリストから、Threat Defense Virtual インスタンスに適用するポリシーを選択します。
ステップ 9 必要に応じて、その他の詳細を入力します。
ステップ 10 [登録（Register）] をクリックします。
ステップ 11 他の Threat Defense Virtual インスタンスを登録するには、ステップ 1 ～ 10 を繰り返します。

次のタスク

Threat Defense Virtual インスタンスのインターフェイスを設定します。

インターフェイスの設定

Threat Defense Virtual インスタンスを登録したら、Management Center でそのインスタンスのインターフェイスを設定する必要があります。

Azure Virtual WAN では、次のように設定された **3 つの**インターフェイスのみサポートされます。

- パブリック IP を最初のインターフェイスとして使用する管理インターフェイス。
- パブリック IP を 2 番目のインターフェイスとして使用する外部インターフェイス。
- 3 番目のインターフェイス（プライベート IP のみを持つ）としてのプライベート IP を持つ内部インターフェイス。

ステップ 1 Management Center にログインします。
ステップ 2 [デバイス（Devices）] ページに移動します。
ステップ 3 登録した Threat Defense Virtual に対応する [編集（Edit）] アイコンをクリックします。
ステップ 4 インターフェイスに対応する [編集（Edit）] アイコンをクリックします。例：**GigbitEthernet0/0**。
ステップ 5 最初のインターフェイス の名前として **`outside`** を入力します。
ステップ 6 [有効（Enabled）] チェックボックスをオンにして、インターフェイスを有効にします。
ステップ 7 [セキュリティゾーン（Security Zone）] ドロップダウンリストから [外側（outside）] を選択します。
ステップ 8 [IPv4] メニューをクリックして、インターフェイスに IP のタイプを割り当てます。
ステップ 9 [IPタイプ（IP Type）] ドロップダウンリストから、[DHCPの使用（Use DHCP）] を選択して、DHCP から IP アドレスを取得するようにインターフェイスを設定します。
ステップ 10 [DHCPを使用してデフォルトルートを取得（Obtain default route using DHCP）] チェックボックスをオンにします。
ステップ 11 [デフォルトルートメトリック（Default route metric）] に **`1`** と入力します。
ステップ 12 [OK] をクリックしてコンフィギュレーションを保存します。
ステップ 13 ステップ 1 ～ 10 を繰り返して、内部インターフェイスを設定します。

次のタスク

インターフェイスのルートを設定します。

インターフェイスのルートの設定

ネットワークオブジェクトを作成し、ゲートウェイ IP アドレスを割り当てて、外部インターフェイスと内部インターフェイスのスタティックルートを設定します。

- 外部インターフェイスのルート設定では、すべてのパケットのデフォルトルートとしてゲートウェイ IP アドレスが使用されます。
- 内部インターフェイスのルート設定では、正常性プローブパケットおよびハブネットワーク範囲宛てのパケットのデフォルトルートとしてゲートウェイ IP アドレスが使用されます。

ゲートウェイ IP アドレスは、各インターフェイスの IP アドレスとサブネットマスクアドレスを使用して計算されます。

外部および内部インターフェイスのゲートウェイ IP アドレスの計算

ここでは、例を使用して外部インターフェイスと内部インターフェイスのゲートウェイ IP アドレスを計算するプロセスについて説明します。

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 3 ハブに展開した Threat Defense Virtual インスタンスにアクセスします。

ステップ 4 [>_Command] フィールドに、**`show interface GigbitEthernet 0/0`** と入力して外部インターフェイスの設定を取得するか、**`show interface GigbitEthernet 0/1`** と入力して内部インターフェイスの設定の詳細を取得します。

ステップ 5 ステップ 1 ～ 4 を繰り返して、内部インターフェイスまたは外部インターフェイスの IP アドレスとサブネットマスクアドレスを取得します。

ステップ 6 コマンドの結果から IP アドレスとサブネットマスクアドレスをメモします。

ステップ 7 次の例に従って、内部および外部のゲートウェイ IP アドレスを計算します。

- 外部インターフェイスのゲートウェイ IP アドレスを計算するには、次の手順を実行します。

  例：GigabitEthernet0/0（外部インターフェイス）の場合

  IP アドレス：**15.0.112.136**

  [サブネット マスク（Subnet mask）]：**255.255.255.128**

  したがって、ゲートウェイ IP アドレスは（このサブネットの最初の IP アドレス）**15.0.112.129** として計算されます。

- 内部インターフェイスのゲートウェイ IP アドレスを計算するには、次の手順を実行します。

  例：GigabitEthernet 0/1（内部インターフェイス）の場合

  IP アドレス：**15.0.112.10**

  [サブネット マスク（Subnet mask）]：**255.255.255.128**

  したがって、ゲートウェイ IP は（このサブネットの最初の IP アドレス）**15.0.112.1** として計算されます。

次のタスク

内部インターフェイスと外部インターフェイスのデフォルトルートを設定します。

外部インターフェイスのデフォルトルートの設定

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 3 Threat Defense Virtual インスタンスをクリックします。

ステップ 4 **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順にクリックします。

ステップ 5 [ルートを追加（Add Route）] をクリックします。

ステップ 6 [インターフェイス（Interface）] ドロップダウンリストから、[外部（Outside）] を選択します。

ステップ 7 [使用可能なネットワーク（Available Network）] で外部インターフェイスに [any-ipv4] を選択し、[追加（Add）] をクリックします。

ステップ 8 ゲートウェイの IP アドレスを入力します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) ネットワークオブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) 計算した外部インターフェイスのゲートウェイ IP アドレスを入力します。
e) [保存（Save）] をクリックします。

内部インターフェイスのデフォルトルートの設定

始める前に

Threat Defense Virtual の CIDR IP アドレスがハブに展開されている必要があります。このアドレスは、内部インターフェイスを設定するために必要です。

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。

ステップ 3 Threat Defense Virtual インスタンスをクリックします。

ステップ 4 **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順にクリックします。

ステップ 5 [ルートを追加（Add Route）] をクリックします。

ステップ 6 [インターフェイス（Interface）] ドロップダウンリストから、[内部（Inside）] を選択します。

ステップ 7 ネットワークオブジェクトを追加して、ハブの CIDR IP アドレスを使用して内部インターフェイスを設定します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) ネットワークオブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) ハブの CIDR IP アドレス（プライベートアドレス空間）を入力します。
e) [保存（Save）] をクリックします。

ステップ 8 ネットワークオブジェクトを追加して、ロードバランサの正常性プローブの IP アドレスを使用して内部インターフェイスを設定します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) ネットワークオブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) ロードバランサの正常性プローブの IP アドレスを入力します。例：**168.63.129.16**。

この IP アドレスは、標準アドレスまたは固定アドレスです。

ステップ 9 ゲートウェイの IP アドレスを入力します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) オブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) 計算した内部インターフェイスのゲートウェイ IP アドレスを入力します。
e) [保存（Save）] をクリックします。

トラフィックルーティングの設定

Threat Defense Virtual インスタンスとハブ間のデータ交換には、スタティックルーティングまたはボーダー ゲートウェイ プロトコル（BGP）を設定できます。これらは、仮想 WAN ハブのネットワークトラフィックに対して設定できる基本的に異なる 2 つのルーティング方法です。

BGP は、ハブと Threat Defense Virtual アプライアンス間のリアルタイムのトラフィック交換に基づいてルートを決定するダイナミック ルーティングプロトコルです。一方、スタティックルーティングでは、事前設定済みのルーティングプロトコルを使用してトラフィックが交換されます。

Azure Virtual WAN の詳細については、Microsoft Azure Virtual WAN のドキュメントを参照してください。

スタティック ルーティングの設定

ステップ 1 Management Center にログインします。
ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** の順に選択します。
ステップ 3 [Threat Defense Virtual] インスタンスをクリックします。
ステップ 4 **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** の順にクリックします。
ステップ 5 [ルートを追加（Add Route）] をクリックします。
ステップ 6 [インターフェイス（Interface）] ドロップダウンリストから、[外部（Outside）] を選択します。

内部インターフェイスを設定する場合は、[内部（Inside）] を選択します。

ステップ 7 ネットワークオブジェクトの IP アドレスを追加します。

a) [+] アイコンをクリックして、ネットワークオブジェクトを追加します。
b) オブジェクトの名前と説明を入力します。
c) [ホストネットワーク（Host Network）] をクリックします。
d) IP アドレスを入力します。
e) [保存（Save）] をクリックします。

BGP ルーティングの有効化

ステップ 1 Management Center にログインします。
ステップ 2 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。
ステップ 3 [Threat Defense Virtual] インスタンスをクリックします。
ステップ 4 [ルーティング（Routing）] メニューをクリックします。
ステップ 5 [全般設定（General Settings）] で [BGP] をクリックします。
ステップ 6 [BGPの有効化（Enable BGP）] チェックボックスをオンにします。
ステップ 7 仮想ハブの AS 番号を入力します。
ステップ 8 [保存（Save）] をクリックします。

次のタスク

BGP ネイバーを設定します。

BGP ネイバーの設定

ステップ 1 Management Center にログインします。
ステップ 2 **[BGP]** > **[IPv4]** > **[ネイバー（Neighbor）]** の順に選択します。
ステップ 3 [IPv4の有効化（Enable IPv4）] チェックボックスをオンにします。
ステップ 4 仮想ハブの自律システム（AS）番号を入力します。
ステップ 5 [ネイバー（Neighbor）] で [追加（Add）] をクリックします。
ステップ 6 メモした BGP エンドポイントの最初の IP アドレスを入力します。
ステップ 7 [有効なアドレス（Enabled address）] チェックボックスをオンにします。
ステップ 8 [リモートAS（Remote AS）] フィールドに AS 番号を入力します。
ステップ 9 [詳細（Advanced）] メニューの [接続検証の無効化（Disable Connection Verification）] チェックボックスをオンにします。
ステップ 10 [保存（Save）] をクリックします。
ステップ 11 ステップ 1 ～ 8 を繰り返して、BGP エンドポイントの 2 番目の IP アドレスを追加します。

次のタスク

BGP ルート設定を確認します。

BGP ルートの設定の確認

始める前に

BGP エンドポイントを設定後、Threat Defense Virtual と仮想 WAN ハブの間で BGP エンドポイントを介した接続が確立されているか確認する必要があります。

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**の順に選択します。

ステップ 3 [Threat Defense Virtual] インスタンスをクリックします。

ステップ 4 **[デバイス（Device）]** > **[全般（General）]** ウィジェットで [CLI] をクリックします。

ステップ 5 [>_Command] フィールドに **show route** と入力し、接続ステータスを表示して確認します。

（注） コード **B** は、Threat Defense Virtual との BGP エンドポイント接続ステータスを示します。

正常性プローブの設定

Threat Defense Virtual のステータスが安定していることを確認するには、内部ロードバランサ（ILB）に接続する内部インターフェイス（信頼済み）を設定する必要があります。ILB はTCP ポート 443 を介して定期的なヘルスチェックプローブを実行し、Threat Defense Virtual からの応答を確認します。

ステップ 1 Management Center にログインします。

ステップ 2 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[新しいポリシー（New Policy）]** > **[Threat Defense設定（Threat Defense Settings）]**の順に選択します。

ステップ 3 Threat Defense Virtual にロードバランサに接続するための**新しいポリシー**を追加します。

ステップ 4 追加した新しいポリシーを編集します。

ステップ 5 [HTTPサーバーの有効化（Enable HTTP Server）] チェックボックスをオンにし、[ポート（Port）] フィールドに **443** と入力します。

ステップ 6 [+追加（+ Add）] をクリックして、HTTP アドレスを設定します。

ステップ 7 正常性プローブの IP アドレス名を選択します。

ステップ 8 [使用可能なゾーン/インターフェイス（Available Zone/Interfaces）] から必要な IP アドレスを選択し、[追加（Add）] をクリックして [選択したゾーン/インターフェイス（Selected Zones/Interfaces）] に追加します。

ステップ 9 [OK] をクリック

ステップ 10 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**の順に選択します。

ステップ 11 [適用済みポリシー（Applied Policies）] ウィジェットの編集アイコンをクリックします。

ステップ 12 [プラットフォーム設定（Platform Settings）] ドロップダウンリストからこのポリシーを選択します。

ステップ 13 必要に応じてセキュリティポリシーを更新して適用します。

HTTP アクセスの設定の詳細については、Configuring HTTP を参照してください。

トラブルシューティング

次に、仮想 WAN での Threat Defense Virtual の一般的なエラーシナリオとデバッグのヒントを示します。

- トラフィックは Threat Defense Virtual にルーティングされません。
  - Management Center の正常性プローブチェックに対する Threat Defense Virtual の応答を確認します。
  - 内部インターフェイスと外部インターフェイスの派生ゲートウェイ IP アドレスが正しいか確認します。
  - スタティックルートを確認します。
- 非 RFC 1918 が Threat Defense Virtual に到達しない：ルーティングインテントでプライベートアドレスとして明示的に指定されている非 RFC 1918 の範囲を確認します。
- Threat Defense の展開エラー：Threat Defense Virtual の展開中に、**ハブプレフィックス長は 23 以下である必要がある（Hub Prefix Length should be less or equal to 23）**というエラーが表示された場合は、ハブのアドレス空間の CIDR が **/23** 以下であることを確認します。

Azure での IPv6 サポート対象 Secure Firewall Threat Defense Virtual の展開

この章では、Azure ポータルから IPv6 サポート対象の Threat Defense Virtual を展開する方法について説明します。

Azure での IPv6 をサポートする展開について

Threat Defense Virtual 製品は、7.3 以降、IPv4 と IPv6 の両方をサポートします。Azure では、仮想ネットワークを作成または使用する Marketplace サービスから Threat Defense Virtual を直接展開できますが、現在、Azure の制限により、Marketplace アプリケーション製品は、IPv4 ベースの VNet/サブネットのみを使用または作成するように制限されています。IPv6 アドレスを既存の VNet に手動で設定することはできますが、IPv6 サブネットで設定された VNet に新しい Threat Defense Virtual インスタンスを追加することはできません。Azure では、Marketplace を

介してリソースを展開する方法以外の代替アプローチを使用してサードパーティのリソースを展開するように、一定の制限を課しています。

シスコは現在、IPv6 アドレッシングをサポートするために Threat Defense Virtual を展開する 2 つの方法を提供しています。

次の 2 つの異なるカスタム IPv6 テンプレートが提供されます。

- [カスタムIPv6テンプレート（ARMテンプレート）（Custom IPv6 template (ARM template)）]：Azure 上の Marketplace イメージを内部的に参照する Azure Resource Manager（ARM）テンプレートを使用して、IPv6 設定の Threat Defense Virtual を展開するために提供されます。このテンプレートには、IPv6 サポート対象の Threat Defense Virtual を展開するように設定可能なリソースとパラメータ定義を含む JSON ファイルが含まれています。このテンプレートを使用するには、「Marketplace イメージ参照を含むカスタム IPv6 テンプレートを使用した Azure からの展開 （99 ページ）」を参照してください。

  プログラムによる展開は、PowerShell、Azure CLI、ARM テンプレート、または API を介してカスタムテンプレートを展開するために、Azure Marketplace 上の VM イメージへのアクセスを許可するプロセスです。VM へのアクセスを許可せずに、これらのカスタムテンプレートを VM に展開することは制限されています。このようなカスタムテンプレートを VM に展開しようとすると、次のエラーメッセージが表示されます。

  Legal terms have not been accepted for this item on this subscription. To accept legal terms ….and configure programmatic deployment for the Marketplace item …..

  次のいずれかの方法を使用して、Azure でのプログラムによる展開を有効にして、Marketplace イメージを参照するカスタム IPv6（ARM）テンプレートを展開できます。

  - **Azure ポータル**：カスタム IPv6 テンプレート（ARM テンプレート）を展開するために、Azure Marketplace で利用可能な Threat Defense Virtual の提供に対応するプログラムによる展開オプションを有効にします。
  - **Azure CLI**：CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

- **カスタム VHD イメージと IPv6 テンプレート（ARM テンプレート）**：Azure で VHD イメージと ARM テンプレートを使用して管理対象イメージを作成します。このプロセスは、VHD とリソーステンプレートを使用した Threat Defense Virtual の展開に似ています。このテンプレートは、展開中に管理対象イメージを参照し、IPv6 サポート対象の Threat Defense Virtual を展開するために Azure にアップロードして設定できる ARM テンプレートを使用します。VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開（106 ページ）を参照してください。

カスタム IPv6 テンプレートを使用した Marketplace イメージまたは VHD イメージを参照して、カスタム IPv6 テンプレート（ARM テンプレート）を使用して Threat Defense Virtual を展開するプロセス。

Threat Defense Virtual の展開に含まれる手順は次のとおりです。

表 *4:*

手順	プロセス
1	IPv6 サポート対象の Threat Defense Virtual の展開を計画している Azure で、Linux VM を作成します。
2	Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して Threat Defense Virtual を展開する場合に**のみ**、Azure ポータルまたは Azure CLI でプログラムによる展開オプションを有効にします。
3	展開のタイプに応じて、次のカスタムテンプレートをダウンロードします。 • Azure Marketplace 参照イメージを使用したカスタム IPv6 テンプレート。 カスタム IPv6（ARM）テンプレートを使用した VHD イメージ。
4	カスタム IPv6（ARM）テンプレートの IPv6 パラメータを更新します。 （注） Marketplace イメージバージョンに相当するソフトウェア イメージ バージョンのパラメータ値は、Marketplace イメージ参照でカスタム IPv6 テンプレートを使用して Threat Defense Virtual を展開する場合にのみ必要です。ソフトウェアバージョンの詳細を取得するには、コマンドを実行する必要があります。
5	Azure ポータルまたは Azure CLI を使用して ARM テンプレートを展開します。

Marketplaceイメージ参照を含むカスタムIPv6テンプレートを使用したAzureからの展開

Marketplaceイメージを参照し、カスタムIPv6テンプレート（ARMテンプレート）を使用してThreat Defense Virtual を展開するプロセス。

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 次の方法で、Azure ポータルまたは Azure CLI を使用してプログラムによる展開を有効にします。

Azure ポータルでこのオプションを有効にするには、次の手順を実行します。

a) [Azure（サービス）（Azure Services）] で [サブスクリプション（Subscriptions）] をクリックして、サブスクリプション ブレード ページを表示します。

b) 左側のペインで、[設定（Settings）] オプションの [プラグラムによる展開（Programmatic Deployment）] をクリックします。

VM に展開されたすべてのタイプのリソースが、関連するサブスクリプション製品とともに表示されます。

c) [ステータス（Status）] 列で、カスタム IPv6 テンプレートのプログラムによる展開のために取得する Threat Defense Virtual 製品に対応する [有効化（Enable）] ボタンをクリックします。

または

Azure CLI を使用してこのオプションを有効にするには、次の手順を実行します。

a) Linux VM に移動します。
b) 次の CLI コマンドを実行して、カスタム IPv6（ARM テンプレート）を展開するためのプログラムによる展開を有効にします。

コマンドの実行時に、イメージのサブスクリプションごとに 1 回だけ規約に同意する必要があります。

 # Accept terms

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # Review that terms were accepted (i.e., accepted=true)

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-ftdv'
- **<sku/plan>**：'ftdv-azure-byol'

以下は、BYOL サブスクリプションプランで展開するためのプログラムによる Threat Defense Virtual の展開を有効にするコマンドスクリプトの例です。

- **az vm image terms show -p cisco -f cisco-ftdv --plan ftdv-azure-byol**

ステップ 3 次のコマンドを実行して、Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得します。

az vm image list --all -p <publisher> -f <offer> -s <sku>

それぞれの説明は次のとおりです。

- **<publisher>**：'cisco'。
- **<offer>**：'cisco-ftdv'
- **<sku>**：'ftdv-azure-byol'

以下は、Threat Defense Virtual 用の Marketplace イメージバージョンに相当するソフトウェアバージョンの詳細を取得するコマンドスクリプトの例です。

az vm image list --all -p cisco -f cisco-ftdv -s ftdv-azure-byol

ステップ 4 表示される使用可能な Marketplace イメージバージョンのリストから、いずれかの Threat Defense Virtual バージョンを選択します。

Threat Defense Virtual の IPv6 サポート展開の場合は、Threat Defense Virtual バージョンを 73* 以上として選択する必要があります。

ステップ 5 Cisco GitHub リポジトリから Marketplace カスタム IPv6 テンプレート（ARM テンプレート）をダウンロードします。

ステップ 6 パラメータ テンプレート ファイル（JSON）で展開値を指定して、パラメータファイルを準備します。

次の表で、Threat Defense Virtual カスタム展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

パラメータ名	許可される値/タイプの例	説明
vmName	csf-tdv	Azure で Threat Defense Virtual VM に名前を付けます。
softwareVersion	730.33.0	Marketplaceイメージバージョンのソフトウェアバージョン。
billingType	BYOL	ライセンス方式はBYOLまたはPAYG です。 BYOL ライセンスはPAYG と比較して費用対効果が高いため、BYOLサブスクライブ展開を選択することをお勧めします。
adminUsername	hjohn	Threat Defense Virtual にログインするユーザー名。 管理者に割り当てられる予約名「admin」は使用できません。
adminPassword	E28@4OiUrhx!	管理者アカウントのパスワード。 パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。
vmStorageAccount	hjohnvmsa	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 文字の長

パラメータ名	許可される値/タイプの例	説明
		さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。
availabilityZone	0	展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。 可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。
customData	{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\":\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}	第 0 日構成で Threat Defense Virtual に表示されるフィールド。デフォルトでは、設定対象となる次の 3 つのキーと値のペアがあります。 • 「admin」ユーザーパスワード • Management Center Virtualホスト名 • 管理用の Management Center Virtual ホスト名または CSF-DM。 「ManageLocally : yes」：これにより、CSF-DM が Threat Defense Virtual マネージャとして使用されるように設定されます。 Management Center Virtual を Threat Defense Virtual マネージャとして設定し、Management Center Virtual で同じ設定をするのに必要なフィールドに入力することもできます。

パラメータ名	許可される値/タイプの例	説明
virtualNetworkResourceGroup	cisco-tdv-rg	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	cisco-tdv-vent	仮想ネットワークの名前。
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1Name	mgmt	管理サブネット名。
Subnet1Prefix	10.151.1.0/24	これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet1StartAddress	10.151.1.4	管理インターフェイスの IPv4 アドレス。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理インターフェイスの IPv6 アドレス。

パラメータ名	許可される値/タイプの例	説明
Subnet2Name	diag	データインターフェイス 1 のサブネット名。
Subnet2Prefix	10.151.2.0/24	これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet2StartAddress	10.151.2.4	データインターフェイス 1 の IPv4 アドレス。
subnet2v6StartAddress	ace:cab:deca:2222::6	データインターフェイス 1 の IPv6 アドレス。
Subnet3Name	inside	データインターフェイス 2 のサブネット名。
Subnet3Prefix	10.151.3.0/24	これはデータインターフェイス 2 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet3StartAddress	10.151.3.4	データインターフェイス 2 の IPv4 アドレス。
subnet3v6StartAddress	ace:cab:deca:3333::6	データインターフェイス 2 の IPv6 アドレス。

パラメータ名	許可される値/タイプの例	説明
Subnet4Name	outside	データインターフェイス 3 のサブネット名。
Subnet4Prefix	10.151.4.0/24	これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet4StartAddress	10.151.4.4	データインターフェイス 3 の IPv4 アドレス。
subnet4v6StartAddress	ace:cab:deca:4444::6	データインターフェイス 3 の IPv6 アドレス。
vmSize	Standard_D4_v2	Threat Defense Virtual VM のサイズ。Standard_D3_v2 がデフォルトです。。

ステップ 7 ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で Threat Defense Virtual ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』
- 『Deploy a local ARM template through CLI』

次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャーを有効にする（Enable Local Manager）] で [いいえ（No）] を選択した場合は、Secure Firewall Management Center を使用して Threat Defense Virtual を管理します。「Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center」を参照してください。

- [ローカルマネージャーを有効にする（Enable Local Manager）] で [はい（Yes）] を選択した場合は、Secure Firewall Device Manager を使用して Threat Defense VirtualThreat Defense VirtualThreat Defense VirtualThreat Defense Virtual を管理します。「Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall device manager」を参照してください。

  管理オプションを選択する方法の概要については、「How to Manage Your Secure Firewall Threat Defense Virtual Device」を参照してください。

VHD およびカスタム IPv6 テンプレートを使用した Azure からの展開

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 Threat Defense Virtual イメージを作成できます。このプロセスは、VHD とリソーステンプレートを使用した Threat Defense Virtual の展開に似ています。

始める前に

- Github の VHD および ARM の最新テンプレートを使用した Threat Defense Virtual 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。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。
- 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 ポータルによる Linux 仮想マシンの作成

- Azure サブスクリプションには、Threat Defense Virtual 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 シスコ ダウンロード ソフトウェア ページから Threat Defense Virtual 圧縮 VHD イメージ（*.bz2）をダウンロードします。

a) [製品（Products）] > [セキュリティ（Security）] > [ファイアウォール（Firewalls）] > **[次世代ファイアウォール（NGFW）（Next-Generation Firewalls (NGFW)）] > [Cisco Secure Firewall Threat Defense Virtual]** の順に選択します。

b) **[Firepower Threat Defense ソフトウェア（Firepower Threat Defense Software）]** 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、Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.vhd.bz2 です。

ステップ 2 「VHD およびリソーステンプレートを使用した Azure からの展開」の**ステップ 2** から**ステップ 8** の手順を実行します。

ステップ 3 [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 Threat Defense Virtual パラメータファイルを参照します。VHD およびカスタム IPv6（ARM）テンプレートを使用した Azure への Threat Defense Virtual の展開例は、Github を参照してください。ここでは、テンプレートとパラメータファイルの作成方法を確認できます。

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。

次の表で、Threat Defense Virtual 展開用のカスタム IPv6 テンプレートパラメータに入力する必要がある展開値について説明します。

パラメータ名	許可される値/タイプの例	説明
vmName	csf-tdv	Azure で Threat Defense Virtual VM に名前を付けます。
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group}/providers/Microsoft.Compute/images/{image-name}	展開に使用されるイメージの 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。
adminUsername	hjohn	Threat Defense Virtual にログインするユーザー名。 管理者に割り当てられる予約名「admin」は使用できません。
adminPassword	E28@4OiUrhx!	管理者アカウントのパスワード。 パスワードの組み合わせは、12 ～ 72 文字の英数字である必要があります。小文字、大文字、数字、特殊文字を組み合わせたパスワードにする必要があります。
vmStorageAccount	hjohnvmsa	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 文字の長さにする必要があります。小文字と数字のみを組み合わせたパスワードにする必要があります。

パラメータ名	許可される値/タイプの例	説明
availabilityZone	0	展開の可用性ゾーンを指定すると、指定した可用性ゾーンにパブリック IP と仮想マシンが作成されます。 可用性ゾーンの設定が必要ない場合は、「**0**」に設定します。選択した地域が可用性ゾーンをサポートしており、入力された値が正しいことを確認してください。（値は 0 ～ 3 の整数である必要があります）。
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	第 0 日構成で Threat Defense Virtual に表示されるフィールド。デフォルトでは、設定対象となる次の 3 つのキーと値のペアがあります。 • 「admin」ユーザーパスワード • CSF-MCv ホスト名 • 管理用の CSF-MCv ホスト名または CSF-DM。 「ManageLocally : yes」：これにより、CSF-DM が Threat Defense Virtual マネージャとして使用されるように設定されます。 CSF-MCv を Threat Defense Virtual マネージャとして設定し、CSF-MCv で同じ設定をするのに必要なフィールドに入力することもできます。
virtualNetworkResourceGroup	csf-tdv	仮想ネットワークを含むリソースグループの名前。virtualNetworkNewOrExisting が new の場合、この値はテンプレートの展開用に選択されたリソースグループと同じである必要があります。
virtualNetworkName	hjohn-vm-vn	仮想ネットワークの名前。

パラメータ名	許可される値/タイプの例	説明
virtualNetworkNewOrExisting	new	このパラメータによって、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用するかが決まります。
virtualNetworkAddressPrefixes	10.151.0.0/16	これは仮想ネットワークの IPv4 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	これは仮想ネットワークの IPv6 アドレスプレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1Name	mgmt-ipv6	管理サブネット名。
Subnet1Prefix	10.151.1.0/24	これは管理サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	これは管理サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet1StartAddress	10.151.1.4	管理インターフェイスの IPv4 アドレス。
subnet1v6StartAddress	ace:cab:deca:1111::6	管理インターフェイスの IPv6 アドレス。
Subnet2Name	diag	データインターフェイス 1 のサブネット名。
Subnet2Prefix	10.151.2.0/24	これはデータインターフェイス 1 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。

パラメータ名	許可される値/タイプの例	説明
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	これはデータインターフェイス 1 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet2StartAddress	10.151.2.4	データインターフェイス 1 の IPv4 アドレス。
subnet2v6StartAddress	ace:cab:deca:2222::6	データインターフェイス 1 の IPv6 アドレス。
Subnet3Name	inside	データインターフェイス 2 のサブネット名。
Subnet3Prefix	10.151.3.0/24	これはデータインターフェイス 2 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	これはデータインターフェイス 2 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet3StartAddress	10.151.3.4	データインターフェイス 2 の IPv4 アドレス。
subnet3v6StartAddress	ace:cab:deca:3333::6	データインターフェイス 2 の IPv6 アドレス。
Subnet4Name	outside	データインターフェイス 3 のサブネット名。
Subnet4Prefix	10.151.4.0/24	これはデータインターフェイス 3 サブネット IPv4 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。

パラメータ名	許可される値/タイプの例	説明
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	これはデータインターフェイス 3 サブネット IPv6 プレフィックスで、「virtualNetworkNewOrExisting」が「new」に設定されている場合にのみ必要です。
subnet4StartAddress	10.151.4.4	データインターフェイス 3 の IPv4 アドレス。
subnet4v6StartAddress	ace:cab:deca:4444::6	データインターフェイス 3 の IPv6 アドレス。
vmSize	Standard_D4_v2	Threat Defense Virtual VM のサイズ。Standard_D3_v2 がデフォルトです。。

ステップ 4 ARM テンプレートを使用して、Azure ポータルまたは Azure CLI で Threat Defense Virtual ファイアウォールを展開します。Azure での ARM テンプレートの展開については、次の Azure ドキュメントを参照してください。

- 『Create and deploy ARM templates by using the Azure portal』
- 『Deploy a local ARM template through CLI』

次のタスク

- Azure で Threat Defense Virtual の IP 設定を更新します。

Threat Defense Virtualイメージスナップショット

Azure ポータルでスナップショットイメージを使用して、Threat Defense Virtualを作成および展開できます。イメージスナップショットは、状態データのない、複製された Threat Defense Virtual イメージインスタンスです。

Threat Defense Virtualスナップショットの概要

Threat Defense Virtual インスタンスのスナップショットイメージを作成するプロセスは、Threat Defense Virtual および FSIC に対して実行される最初のブート手順をスキップすることにより、初期システムの初期化時間を最小限に抑えるのに役立ちます。スナップショットイメージは、事前に入力されたデータベースと Threat Defense Virtual 初期ブートプロセスで構成されます。

これにより、イメージは Management Center またはその他の管理センターのシステム ID に関連する一意の ID（UUID、シリアル番号）を再生成できます。このプロセスは、自動スケール展開に不可欠な Threat Defense Virtual の起動時間を短縮するのに役立ちます。

管理対象イメージからの Threat Defense Virtual スナップショットイメージの作成

Threat Defense Virtual のイメージスナップショットの作成は、Azure ポータルで Threat Defense Virtual インスタンスの既存の管理対象イメージを複製するプロセスです。

始める前に

Azure ポータルで Linux VM の Azure ストレージアカウント内のコンテナにサイズ変更した VHD イメージをアップロードして、Threat Defense Virtual バージョン 7.2 以降の管理対象イメージを作成しておく必要があります。サイズ変更した VHD イメージの作成については、「VHD およびリソーステンプレートを使用した Azure からの展開 （19 ページ）」を参照してください。

イメージスナップショットの準備をしている Threat Defense Virtual インスタンスを Management Center や Device Manager などのマネージャに登録しないでください。

ステップ 1 Threat Defense Virtual インスタンスの管理対象イメージを作成した Azure ポータルに移動します。

（注） 複製する予定の Threat Defense Virtual インスタンスが Management Center に登録されていないこと、または他のローカルマネージャに設定されていないこと、または設定が適用されていないことを確認します。

ステップ 2 [リソースグループ（Resource Group）] に移動し、Threat Defense Virtual インスタンスを選択します。

ステップ 3 Threat Defense Virtual インスタンスのナビゲーションページで [シリアルコンソール（Serial Console）] をクリックします。

ステップ 4 次のスクリプトを使用して、エキスパートシェルからプレスナップショット プロセスを実行します。

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

スクリプトで `prepare_snapshot` コマンドを使用すると、スクリプトの実行の確認を求める中間メッセージが表示されます。スクリプトを実行するには、[Y] を押します。

または、`root@firepower:/ngfw/var/common# prepare_snapshot -f` のように、このコマンドに `-f` を追加して、ユーザーの確認メッセージをスキップしてスクリプトを直接実行することもできます。

このスクリプトは、Threat Defense Virtual インスタンスに関連付けられたすべての回線設定、展開されたポリシー、設定されたマネージャ、UUID を削除します。処理が完了すると、Threat Defense Virtual インスタンスはシャットダウンされます。

ステップ 5 [キャプチャ（Capture）] をクリックします。

ステップ 6 [イメージの作成（Create an image）] ページで、既存のリソースグループを選択するか、[リソースグループ（Resource Group）] ドロップダウンリストから新しいリソースグループを作成します。

ステップ 7 [インスタンスの詳細（Instance Details）] セクションで [いいえ、管理対象イメージのみをキャプチャします（No, capture only a managed image）] をクリックして、管理対象イメージのみを作成します。

ステップ 8 Threat Defense Virtual インスタンスの管理対象イメージを使用して作成するスナップショットイメージの名前を指定します。

ステップ 9 [レビューと確認（Review+Create）] をクリックして、Threat Defense Virtual インスタンスの新しいスナップショットイメージを作成します。

次のタスク

スナップショットイメージを使用して Threat Defense Virtual インスタンスを展開します。「イメージスナップショットを使用した Threat Defense Virtual インスタンスの展開」を参照してください。

イメージスナップショットを使用した Threat Defense Virtual インスタンスの展開

始める前に

次のことを推奨します。

- Threat Defense Virtual インスタンスのスナップショットイメージが使用可能であることを確認します。

ステップ 1 Azure ポータルにログインします。

ステップ 2 新規に作成したスナップショットイメージのリソース ID をコピーします。

（注） Azure では、あらゆるリソース（スナップショットイメージ）がリソース ID に関連付けられています。新しい Threat Defense Virtual インスタンスを展開するには、スナップショットイメージのリソース ID が必要です。

a) Azure ポータルで、[イメージ（Images）] を選択します。
b) 管理対象イメージを使用して作成したスナップショット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** シンタックスは次の様に表されます。**/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>**

ステップ 3 スナップショットイメージを使用して Threat Defense Virtual インスタンスの展開を続行します。VHD およびリソーステンプレートを使用した Azure からの展開 （19 ページ） を参照してください。

（注） Threat Defense Virtual コンソールから CLI コマンド **show version** および **show snapshot detail** を実行すると、新しく展開された Threat Defense Virtual インスタンスのバージョンと詳細を確認できます。

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。