AWS 用の Firepower Threat Defense Virtual Auto Scale の展開

このドキュメントでは、FTDv Auto Scale Manager のサーバレスコンポーネントを AWS に導入する方法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。

- AWS での FTDv の Auto Scale ソリューション （1 ページ）
- Auto Scale ソリューションの前提条件 （5 ページ）
- Auto Scale の展開 （10 ページ）
- Auto Scale メンテナンスタスク （20 ページ）
- Auto Scale のトラブルシューティングとデバッグ （24 ページ）

AWS での FTDv の Auto Scale ソリューション

次のセクションでは、Auto Scale ソリューションのコンポーネントが AWS の FTDv でどのように機能するか説明します。

Auto Scale ソリューションについて

シスコでは、Lambda、Auto Scaling グループ、Elastic Load Balancing（ELB）、Amazon S3 バケット、SNS、CloudWatch などの複数の AWS サービスを使用して、FTDv ファイアウォールの Auto Scaling グループを導入するための CloudFormation テンプレートとスクリプトを提供しています。

AWS の FTDv Auto Scale は、AWS 環境の FTDv インスタンスに水平 Auto Scaling 機能を追加する、完全なサーバレス実装です（つまり、この機能の自動化に関与するヘルパー VM はありません）。

FTDv Auto Scale ソリューションは、以下の内容を提供する CloudFormation テンプレートベースの導入です。

- FMC による FTDv 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 FTDv 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のサポート。
- FMC でのみ動作。Firepower Device Manager はサポートされていません。

Auto Scale の機能拡張（バージョン 6.7）

- カスタム指標パブリッシャ：新しい Lambda 関数は、Auto Scale グループ内のすべての FTDv インスタンスのメモリ消費量について FMC を 2 分ごとにポーリングし、その値を CloudWatch メトリックにパブリッシュします。詳細については、入力パラメータ （10 ページ）を参照してください。
- メモリ消費に基づく新しいスケーリングポリシーを使用できます。
- FMC への SSH およびセキュアトンネル用の FTDv プライベート IP 接続。
- FMC の設定検証。
- ELB でより多くのリスニングポートを開くためのサポート。
- シングルスタック展開に変更。すべての Lambda 関数と AWS リソースは、合理化された展開のためにシングルスタックから展開されます。

サポートされるソフトウェア プラットフォーム

FTDv Auto Scale ソリューションは、FMC によって管理される FTDv に適用可能で、ソフトウェアバージョンに依存しません。Cisco Firepower 互換性ガイド [英語] を参照してください。このガイドには、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、Cisco Firepower 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。

- Firepower Management Centers: Virtual 表には、AWS 上の FMCv における Firepower の互換性および仮想ホスティング環境の要件が一覧表示されています。
- Firepower Threat Defense Virtual Compatibility 表には、AWS 上の FTDv における Firepower の互換性および仮想ホスティング環境の要件が一覧表示されています。

（注） AWS Auto Scale ソリューションを導入するために、AWS 上の FTDv でサポートされる Firepower の最小バージョンはバージョン 6.4 です。 メモリベースのスケーリングを使用するには、FMC がバージョン 6.6 以降を実行している必要があります。

Auto Scale の導入例

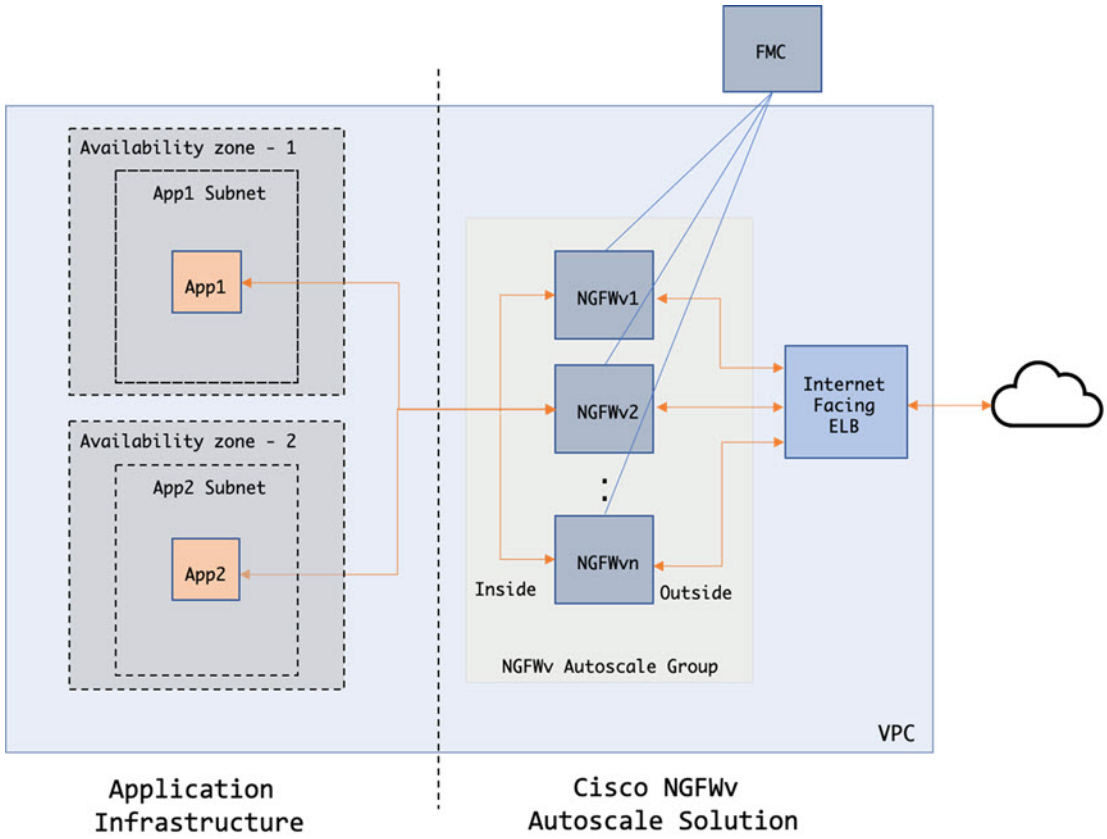
この FTDv AWS Auto Scale ソリューションの導入例は、図 1 : FTDv Auto Scale の導入例の図 （3 ページ）に示されています。AWS ロードバランサはインバウンドで開始された接続のみを許可するため、外部で生成されたトラフィックのみが Cisco FTDv ファイアウォール経由で内部を通過できます。

（注） 前提条件のSSL サーバ証明書 （8 ページ）で説明されているように、セキュアなポートには SSL/TLS 証明書が必要です。

インターネットに面したロードバランサは、ネットワークロードバランサまたはアプリケーション ロードバランサです。いずれの場合も、AWS のすべての要件と条件が適用されます。導入例の図に示されているように、点線の右側部分は FTDv テンプレートを介して展開されます。左側は完全にユーザ定義の部分です。

（注） アプリケーションが開始したアウトバウンドトラフィックは FTDv を通過しません。

図 *1 : FTDv Auto Scale* の導入例の図



トラフィックのポートベースの分岐が可能です。この分岐は、NAT ルールによって実現できます。FMC でのオブジェクト、デバイスグループ、NAT ルール、アクセスポリシーの設定（17 ページ）を参照してください。たとえば、インターネットに面した LB DNS、ポート：80 のトラフィックは、アプリケーション 1 にルーティングでき、ポート：88 のトラフィックはアプリケーション 2 にルーティングできます。

Auto Scale ソリューションの仕組み

FTDv インスタンスをスケールインおよびスケールアウトするには、Auto Scale Manager と呼ばれる外部エンティティがメトリックをモニタし、Auto Scale グループに FTDv インスタンスの追加または削除を指示し、FTDv デバイスを管理 FMC に登録および登録解除して、FTDv インスタンスを設定します。

Auto Scale Manager は、AWS サーバレスアーキテクチャを使用して実装され、AWS リソース、FTDv、および FMC と通信します。シスコでは、Auto Scale Manager コンポーネントの導入を自動化する CloudFormation テンプレートを提供しています。このテンプレートにより、包括的なソリューションが機能するために必要なその他のリソースも展開されます。

（注） サーバレス Auto Scale スクリプトは CloudWatch イベントによってのみ呼び出されるため、インスタンスの起動時にのみ実行されます。

Auto Scale ソリューションのコンポーネント

Auto Scale 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。

CloudFormation テンプレート

CloudFormation テンプレートは、AWS の 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。テンプレートの構成は次のとおりです。

- Auto Scale グループ、ロードバランサ、セキュリティグループ、およびその他のコンポーネント。
- 展開をカスタマイズするためのユーザ入力を取り込むテンプレート。

（注） テンプレートのユーザ入力の検証には限界があるため、展開時に入力を検証するのはユーザの責任です。

Lambda 関数

Auto Scale ソリューションは、Python で開発された一連の Lambda 関数で、ライフサイクルフック、SNS、CloudWatch イベントやアラームイベントからトリガーされます。基本的な機能は次のとおりです。

- インスタンスに対して Diag、Gig0/0、および Gig 0/1 インターフェイスを追加/削除します。
- ロードバランサのターゲットグループに Gig0/1 インターフェイスを登録します。
- 新しい FTDv を FMC に登録します。
- FMC を介して新しい FTDv を設定し展開します。
- スケールインした FTDv を FMC から登録解除（削除）します。
- FMC からメモリメトリックをパブリッシュします。

Lambda 関数は、Python パッケージの形式でお客様に提供されます。

ライフサイクルフック

- ライフサイクルフックは、インスタンスに関するライフサイクルの変更通知を取得するために使用されます。
- インスタンス起動の場合、ライフサイクルフックを使用して、FTDv インスタンスにインターフェイスを追加し、ターゲットグループに外部インターフェイス IP を登録できる Lambda 関数をトリガーします。
- インスタンス終了の場合、ライフサイクルフックを使用して Lambda 関数をトリガーし、ターゲットグループから FTDv インスタンスを登録解除します。

Simple Notification Service（SNS）

- AWS の Simple Notification Service（SNS）を使用してイベントが生成されます。
- AWS にはサーバレス Lambda 関数に適した Orchestrator がないという制限があるため、ソリューションは、イベントに基づいて Lambda 関数をオーケストレーションするための一種の関数チェーンとして SNS を使用します。

Auto Scale ソリューションの前提条件

展開ファイルのダウンロード

FTDv Auto Scale for AWS 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。Firepower バージョン用の展開スクリプトとテンプレートは、次の GitHub リポジトリから入手できます。

- https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/aws

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。

インフラストラクチャ設定

複製/ダウンロードされた GitHub リポジトリでは、**infrastructure.yaml** ファイルはテンプレートフォルダにあります。この CFT は、バケットポリシーを使用して VPC、サブネット、ルート、ACL、セキュリティグループ、VPC エンドポイント、および S3 バケットを展開するために使用できます。この CFT は、要件に合わせて変更できます。

次のセクションでは、これらのリソースと Auto Scale での使用について詳しく説明します。これらのリソースを手動で展開し、Auto Scale で使用することもできます。

（注） **infrastructure.yaml** テンプレートは、VPC、サブネット、ACL、セキュリティグループ、S3 バケット、および VPC エンドポイントのみを展開します。SSL 証明書、Lambda レイヤ、または KMS キーリソースは作成されません。

VPC

アプリケーション要件に応じて VPC を作成する必要があります。VPC には、インターネットへのルートがある少なくとも 1 つのサブネットを持つインターネットゲートウェイがあることが想定されます。セキュリティグループ、サブネットなどの要件については、該当するセクションを参照してください。

サブネット

サブネットは、アプリケーションの要件に応じて作成できます。導入例に示されているように、FTDv VM の動作には 3 つのサブネットが必要です。

（注） 複数の可用性ゾーンのサポートが必要な場合、サブネットは AWS クラウド内のゾーンプロパティであるため、各ゾーンにサブネットが必要です。

外部サブネット

外部サブネットには、インターネットゲートウェイへの「0.0.0.0/0」のデフォルトルートが必要です。このサブネットには、FTDv の外部インターフェイスが含まれ、インターネットに面した NLB も含まれます。

内部サブネット

これは、NAT/インターネットゲートウェイの有無にかかわらず、アプリケーションサブネットに似ています。FTDv 正常性プローブでは、ポート 80 経由で AWS メタデータサーバ（169.254.169.254）に到達できる必要があることに注意してください。

（注） この AutoScale ソリューションでは、ロードバランサの正常性プローブが inside/Gig0/0 インターフェイスを介して AWS メタデータサーバにリダイレクトされます。ただし、ロードバランサから FTDv に送信される正常性プローブ接続を提供する独自のアプリケーションでこれを変更できます。この場合、AWS メタデータ サーバ オブジェクトをそれぞれのアプリケーションの IP アドレスに置き換えて、正常性プローブ応答を提供する必要があります。

管理サブネット

このサブネットには、FTDv 管理インターフェイスが含まれます。 このサブネットで FMC を使用している場合、FTDv への Elastic IP アドレス（EIP）の割り当ては任意です。（6.7 以前）診断インターフェイスもこのサブネット上にあります。

Lambda サブネット

AWS Lambda 関数では、デフォルトゲートウェイとして NAT ゲートウェイを持つ 2 つのサブネットが必要です。これにより、Lambda 関数が VPC に対してプライベートになります。Lambda サブネットは、他のサブネットと同じ幅である必要はありません。Lambda サブネットのベストプラクティスについては、AWS のドキュメントを参照してください。

アプリケーションサブネット

Auto Scale ソリューションからこのサブネットに課せられる制限はありませんが、アプリケーションに VPC 外部のアウトバウンド接続が必要な場合は、サブネット上にそれぞれのルートが設定されている必要があります。これは、アウトバウンドで開始されたトラフィックがロードバランサを通過しないためです。AWS Elastic Load Balancing ユーザガイド [英語] を参照してください。

セキュリティ グループ

提供された Auto Scale グループテンプレートでは、すべての接続が許可されます。Auto Scale ソリューションを機能させるために必要なのは、次の接続だけです。

表 *1 :* 必須のポート

ポート	使用方法	Subnet
8305	FMC から FTDv へのセキュアなトンネル接続	管理サブネット

ポート	使用方法	Subnet
正常性プローブポート（デフォルト：8080）	インターネットに面したロードバランサの正常性プローブ	外部サブネット、内部サブネット
アプリケーションポート	アプリケーションデータ トラフィック	外部サブネット、内部サブネット

FMC インスタンスのセキュリティグループまたは ACL

Lambda 関数と FMC 間の HTTPS 接続を許可します。Lambda 関数は、NAT ゲートウェイをデフォルトルートとして持つ Lambda サブネットに保持されるため、FMC は NAT ゲートウェイ IP アドレスからのインバウンド HTTPS 接続を持つことができます。

Amazon S3 バケット

Amazon Simple Storage Service（Amazon S3）は、業界をリードする拡張性、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクト ストレージ サービスです。ファイアウォール テンプレートとアプリケーション テンプレートの両方に必要なすべてのファイルを S3 バケットに配置できます。

テンプレートが展開されると、S3 バケット内の Zip ファイルを参照して Lambda 関数が作成されます。したがって、S3 バケットはユーザアカウントにアクセス可能である必要があります。

SSL サーバ証明書

インターネットに面したロードバランサが TLS/SSL をサポートしている必要がある場合、証明書 ARN が必要です。詳細については、次のリンクを参照してください。

- サーバ証明書の使用
- テスト用の秘密キーと自己署名証明書の作成
- 自己署名 SSL 証明書を使用した AWS ELB の作成（サードパーティリンク）

ARN の例：arn:aws:iam::[AWS Account]:server-certificate/[Certificate Name]

Lambda レイヤ

autoscale_layer.zip は、Python 3.6 がインストールされた Ubuntu 18.04 などの Linux 環境で作成できます。

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.6 ./layer/
source ./layer/bin/activate
```

```
pip3 install pycrypto==2.6.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
echo "Copy from ./layer directory to ./python\n"
mkdir -p ./python/.libs_cffi_backend/
cp -r ./layer/lib/python3.6/site-packages/* ./python/
cp -r ./layer/lib/python3.6/site-packages/.libs_cffi_backend/* ./python/.libs_cffi_backend/
zip -r autoscale_layer.zip ./python
```

作成された ***autoscale_layer.zip*** ファイルは、*lambda-python-files* フォルダにコピーする必要があります。

KMS マスターキー

これは、FMC および FTDv パスワードが暗号化形式の場合に必要です。それ以外の場合、このコンポーネントは必要ありません。パスワードは、ここで提供される KMS のみを使用して暗号化する必要があります。KMS ARN が CFT で入力される場合、パスワードを暗号化する必要があります。それ以外の場合、パスワードはプレーンテキストである必要があります。

マスターキーと暗号化の詳細については、パスワードの暗号化と KMS に関する AWS のドキュメントのキーの作成 [英語] と AWS CLI コマンドリファレンス [英語] を参照してください。

例：

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN'
{
    "KeyId": "KMS-ARN",
    "CiphertextBlob":
"AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQRnCAFwfXhXHJAHL8tcVmDqurALAAAAajBoBgkqhki
G9w0BBwagWzBZAgEAMFQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
+wxpWKtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
}
$
```

CiphertextBlob キーの値をパスワードとして使用する必要があります。

Python 3 環境

make.py ファイルは、複製されたリポジトリの最上位ディレクトリにあります。これにより、python ファイルが Zip ファイルに圧縮され、ターゲットフォルダにコピーされます。これらのタスクを実行するには、Python 3 環境が使用可能である必要があります。

Auto Scale の展開

準備

アプリケーションが展開されているか、アプリケーションの展開プランが利用可能である必要があります。

入力パラメータ

導入前に、次の入力パラメータを収集する必要があります。

表 *2 : Auto Scale* 入力パラメータ

パラメータ	使用できる値/タイプ	説明
PodNumber	文字列 許可パターン：'^\d{1,3}$'	これはポッド番号です。Auto Scale グループ名（FTDv-Group-Name）の末尾に追加されます。たとえば、この値が「1」の場合、グループ名は *FTDv-Group-Name-1.* になります。 1 桁以上 3 桁以下の数字である必要があります。 デフォルト：1
AutoscaleGrpNamePrefix	文字列	これは Auto Scale グループ名プレフィックスです。ポッド番号がサフィックスとして追加されます。 最大：18 文字 例：Cisco-FTDv-1
NotifyEmailID	文字列	Auto Scale イベントはこの電子メールアドレスに送信されます。サブスクリプション電子メール要求を受け入れる必要があります。 例：admin@company.com
VpcId	文字列	デバイスを展開する必要がある VPC ID。これは、AWS の要件に従って設定する必要があります。 タイプ：AWS::EC2::VPC::Id 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。

パラメータ	使用できる値/タイプ	説明
LambdaSubnets	リスト（List）	Lambda 関数が展開されるサブネット。 タイプ：List<AWS::EC2::Subnet::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
LambdaSG	リスト（List）	Lambda 機能のセキュリティグループ。 タイプ：List<AWS::EC2::SecurityGroup::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
S3BktName	文字列	ファイルの S3 バケット名。これは、AWS の要件に従ってアカウントに設定する必要があります。 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
LoadBalancerType	文字列	インターネットに面したロードバランサのタイプ（「アプリケーション」または「ネットワーク」）。 例：アプリケーション
LoadBalancerSG	文字列	ロードバランサのセキュリティグループ。ネットワークロードバランサの場合は使用されません。ただし、セキュリティグループ ID を指定する必要があります。 タイプ：List<AWS::EC2::SecurityGroup::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。

パラメータ	使用できる値/タイプ	説明
LoadBalancerPort	整数（Integer）	ロードバランサポート。このポートは、選択したロードバランサタイプに基づいて、プロトコルとして HTTP/HTTPS または TCP/TLS を使用して LB で開きます。 ポートが有効な TCP ポートであることを確認します。これはロードバランサリスナーの作成に使用されます。 デフォルト：80
SSL認証	文字列	セキュアポート接続の SSL 証明書の ARN。指定しない場合、ロードバランサで開かれるポートは TCP/HTTP になります。指定した場合、ロードバランサで開かれるポートは TLS/HTTPS になります。
TgHealthPort	整数	このポートは、正常性プローブのターゲットグループによって使用されます。FTDv のこのポートに到達する正常性プローブは、AWS メタデータサーバにルーティングされるため、トラフィックには使用しないでください。このポートは有効な TCP ポートである必要があります。 アプリケーション自体が正常性プローブに応答するようにする場合は、それに応じて FTDv の NAT ルールを変更できます。このような場合、アプリケーションが応答しないと、FTDv は Unhealthy インスタンスのしきい値アラームにより、非正常としてマークされ、削除されます。 例：8080
AssignPublicIP	ブール値	「true」を選択すると、パブリック IP が割り当てられます。BYOL タイプの FTDv の場合、これは https://tools.cisco.com に接続するために必要です。 例：TRUE

パラメータ	使用できる値/タイプ	説明
InstanceType	文字列	Amazon マシンイメージ（AMI）は、さまざまなインスタンスタイプをサポートしています。インスタンスタイプによって、インスタンスのサイズと必要なメモリ容量が決まります。 FTDv をサポートする AMI インスタンスタイプのみを使用する必要があります。『Firepower リリースノート（Firepower Release Notes）』『』を参照してください。 例：c4.2xlarge
LicenseType	文字列	FTDv ライセンスタイプ（BYOL または PAYG）。関連する AMI ID が同じライセンスタイプであることを確認します。 例：BYOL
AmiId	文字列	FTDv AMI ID（有効な Cisco FTDv AMI ID）。 タイプ：AWS::EC2::Image::Id リージョンとイメージの目的のバージョンに応じて、正しい AMI ID を選択してください。Auto Scale 機能は、Firepower バージョン 6.4+、BYOL/PAYG イメージをサポートします。いずれの場合も、AWS マーケットプレイスでライセンスに同意する必要があります。 BYOL の場合、設定 JSON ファイルの「licenseCaps」キーを「BASE」、「MALWARE」、「THREAT」、「URLFilter」などの機能で更新してください。
NoOfAZs	整数（Integer）	FTDv を展開する必要がある可用性ゾーンの数（1 ー 3）。ALB 導入の場合、AWS で必要な最小値は 2 です。 例：2。

パラメータ	使用できる値/タイプ	説明
ListOfAzs	カンマ区切り文字列	ゾーンの順序のカンマ区切りリスト。 （注） ゾーンのリスト順は重要です。サブネットリストは同じ順序で指定する必要があります。 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 例：us-east-1a、us-east-1b、us-east-1c
MgmtInterfaceSG	文字列	FTDv管理インターフェイスのセキュリティグループ。 タイプ：List<AWS::EC2::SecurityGroup::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
InsideInterfaceSG	文字列	FTDv内部インターフェイスのセキュリティグループ。 タイプ：AWS::EC2::SecurityGroup::Id 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
OutsideInterfaceSG	文字列	FTDv外部インターフェイスのセキュリティグループ。 タイプ：AWS::EC2::SecurityGroup::Id 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。 例：sg-0c190a824b22d52bb

パラメータ	使用できる値/タイプ	説明
MgmtSubnetId	カンマ区切りリスト	管理サブネットIDのカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。 タイプ：List<AWS::EC2::SecurityGroup::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
InsideSubnetId	カンマ区切りリスト	内部/Gig0/0サブネットIDのカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。 タイプ：List<AWS::EC2::SecurityGroup::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
OutsideSubnetId	カンマ区切りリスト	外部/Gig0/1サブネットIDのカンマ区切りリスト。リストは、対応する可用性ゾーンと同じ順序にする必要があります。 タイプ：List<AWS::EC2::SecurityGroup::Id> 「*infrastructure.yaml*」ファイルを使用してインフラストラクチャを展開すると、スタックの出力セクションにこの値が設定されます。その値を使用してください。
KmsArn	文字列	既存の KMS の ARN（保存時に暗号化するための AWS KMS キー）。指定した場合は、FMC および FTDv のパスワードを暗号化する必要があります。パスワードの暗号化は、指定されたARNのみを使用して実行する必要があります。 暗号化パスワードの生成例： " aws kms encrypt --key-id <KMS ARN> --plaintext <password> ". 次のような生成されたパスワードを使用してください。 例：arn:aws:kms:us-east-1:[AWS Account]:key/7d586a25-5875-43b1-bb68-a452e2f6468e

パラメータ	使用できる値/タイプ	説明
ngfwPassword	文字列	すべてのFTDvインスタンスには、起動テンプレート（自動スケールグループ）の [ユーザデータ（Userdata）] フィールドに入力されたデフォルトのパスワードが設定されています。 この入力により、FTDvにアクセスできるようになると、パスワードが新しく提供されたパスワードに変更されます。 KMS ARN が使用されていない場合は、プレーンテキストのパスワードを使用してください。KMS ARNが使用されている場合は、暗号化されたパスワードを使用する必要があります。 例：Cisco123789! または AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	数値文字列	Lambda 関数と FTDv 管理インターフェイスの両方に到達可能な管理 FMC の IP アドレス。 例：10.10.17.21
fmcOperationsUsername	文字列	管理 FMC で作成された Network-Admin 以上の特権ユーザ。ユーザおよびロールの作成については、『Firepower Management Center Configuration Guide』を参照してください。 例：apiuser-1
fmcOperationsPassword	文字列	KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。 例：Cisco123@ または AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQRnCAajB
fmcDeviceGrpName	文字列	FMC のデバイスグループ名。 例：AWS-Cisco-NGFW-VMs-1
fmcPublishMetrics	ブール値	「TRUE」に設定すると、指定されたデバイスグループ内の登録済み FTDv センサーのメモリ消費量を取得するために、2 分に 1 回実行される Lambda 関数が作成されます。 使用可能な値：TRUE、FALSE 例：TRUE

パラメータ	使用できる値/タイプ	説明
fmcMetricsUsername	文字列	AWS CloudWatch にメトリックを公開するための一意の FMC ユーザ名。ユーザおよびロールの作成については、『Firepower Management Center Configuration Guide』を参照してください。 「fmcPublishMetrics」が「FALSE」に設定されている場合は、この入力を行う必要はありません。 例：publisher-1
fmcMetricsPassword	文字列	AWS CloudWatch にメトリックを公開するための FMC パスワード。KMS ARN が記載されていない場合は、プレーンテキストのパスワードを使用してください。記載されている場合は、暗号化されたパスワードを使用する必要があります。 「fmcPublishMetrics」が「FALSE」に設定されている場合は、この入力を行う必要はありません。 例：Cisco123789!
CpuThresholds	カンマ区切り整数	CPU しきい値の下限と CPU しきい値の上限。最小値は 0 で、最大値は 99 です。 デフォルト：10、70 しきい値の下限はしきい値の上限よりも小さくする必要があります。 例：30、70
MemoryThresholds	カンマ区切り整数	MEM しきい値の下限と MEM しきい値の上限。最小値は 0 で、最大値は 99 です。 デフォルト：40、70 しきい値の下限はしきい値の上限よりも小さくする必要があります。「fmcPublishMetrics」パラメータが「FALSE」の場合、影響はありません。 例：40、50

FMC でのオブジェクト、デバイスグループ、NAT ルール、アクセスポリシーの設定

別のサーバ上で実行されるフル機能のマルチデバイスマネージャである、Firepower Management Center（FMC）を使用して FTDv を管理できます。FTDv は、FTDv 仮想マシンに割り当てた管理インターフェイス上の FMC を登録して通信します。詳細については、Firepower Management Center を使用した Firepower Threat Defense Virtual についてを参照してください。

FTDv の設定に使用されるオブジェクトはすべて、ユーザが作成する必要があります。

重要 デバイスグループを作成し、ルールを適用する必要があります。デバイスグループに適用されたすべての設定が FTDv インスタンスにプッシュされます。

オブジェクト

次のオブジェクトを作成します。

表 *3 : FTDv* 管理用の *FMC* 設定オブジェクト

オブジェクト タイプ	名前	値
ホスト（Host）	aws-metadata-server	169.254.169.254
ポート	health-check-port	必要に応じて、8080 またはその他のポート
ゾーン	内部またはその他の名前	—
ゾーン	外部またはその他の名前	—

NAT ポリシー

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。NAT ポリシーの詳細については、Firepower Management Center を使用した Firepower Threat Defense Virtual の管理のNAT の設定を参照してください。

NAT ポリシーには 1 つの必須ルールが必要です。

- 送信元ゾーン（Source Zone）：外部ゾーン
- 宛先ゾーン（Dest Zone）：内部ゾーン（Inside Zone）
- Original-sources：any-ipv4
- 元の送信元ポート（Original source port）：元/デフォルト（Original/default）
- 元の宛先（Original Destinations）：インターフェイス（Interface）
- Original-destination-port：8080 またはユーザが設定する正常性ポート
- 変換済み送信元（Translated-sources）：any-ipv4
- 変換済み送信元ポート：元/デフォルト
- Translated-destination：aws-metadata-server
- 変換済み宛先ポート（Translated-destination-port）：80/HTTP

同様に、この設定が FTDv デバイスにプッシュされるように、データトラフィック NAT ルールを追加できます。

重要　作成された NAT ポリシーはデバイスグループに適用する必要があります。 Lambda 関数からの FMC 検証でこれを検証します。

アクセス ポリシー

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。必要なすべてのポリシーを含むアクセスポリシーを作成できます。このポートのトラフィックが到達できるように、正常性ポートオブジェクトを許可する必要があります。アクセスポリシーの詳細については、Firepower Management Center を使用した Firepower Threat Defense Virtual の管理のアクセス制御の設定を参照してください。

設定 JSON ファイルの更新

Configuration.json ファイルは、GitHub リポジトリから取得したアーカイブ Zip の一部である ***lambda_python_files*** フォルダにあります。JSON キーは変更しないでください。FTDv VM のスタティックルートは、JSON ファイルで設定する必要があります。

スタティックルートの設定例については、次を参照してください。

```
{
  "interface": "inside",
  "network": "any-ipv4",
  "gateway": "",
  "metric": "1"
}
```

JSON ファイルのすべての値は、デフォルトの FTDv パスワードを除き、要件に応じて変更できます。

Amazon Simple Storage Service（S3）へのファイルのアップロード

target ディレクトリ内のすべてのファイルを Amazon S3 バケットにアップロードする必要があります。必要に応じて、CLI を使用して、*target* ディレクトリ内のすべてのファイルを Amazon S3 バケットにアップロードできます。

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

スタックの展開

展開のすべての前提条件が完了すると、AWS CloudFormation スタックを作成できます。

target ディレクトリ内の *deploy_ngfw_autoscale.yaml* ファイルを使用します。

入力パラメータ （10 ページ）で収集されたパラメータを入力します。

展開の検証

テンプレートの展開が成功したら、Lambda 関数と CloudWatch イベントが作成されていることを検証する必要があります。デフォルトでは、Auto Scale グループのインスタンスの最小数と最大数はゼロです。AWS EC2 コンソールで必要な数のインスタンスを使用して、Auto Scale グループを編集する必要があります。これにより、新しい FTDv インスタンスがトリガーされます。

1 つのインスタンスのみを起動してワークフローを確認し、そのインスタンスが期待どおりに動作しているかどうかを検証することを推奨します。その後に FTDv の実際の要件を展開でき、動作を確認することもできます。AWS スケーリングポリシーによる削除を回避するために、最小数の FTDv インスタンスをスケールイン保護としてマークできます。

Auto Scale メンテナンスタスク

スケーリングプロセス

このトピックでは、Auto Scale グループの 1 つ以上のスケーリングプロセスを一時停止してから再開する方法について説明します。

スケールアクションの開始と停止

スケールアクションを開始および停止するには、次の手順を実行します。

- AWS 動的スケーリングの場合：スケールアウトアクションを有効化または無効化する方法については、次のリンクを参照してください。

  スケーリングプロセスの一時停止と再開

ヘルスモニタ

60 分ごとに、CloudWatch Cron ジョブは、Health Doctor モジュールの Auto Scale Manager Lambda をトリガーします。

- 有効な FTDv VM に属する異常な IP がある場合、FTDv の展開時間が 1 時間を超えると、そのインスタンスは削除されます。
- それらの IP が有効な FTDv VM の IP ではない場合、IP だけがターゲットグループから削除されます。

ヘルスモニタは、デバイスグループ、アクセスポリシー、および NAT ルールの FMC 構成も検証します。IP/インスタンスが正常でない場合、または FMC 検証が失敗した場合、ヘルスモニタはユーザに電子メールを送信します。

正常性モニタの無効化

ヘルスモニタを無効にするには、***constant.py*** で constant を「True」に設定します。

正常性モニタの有効化

ヘルスモニタを有効にするには、***constant.py*** で固定値を「False」に設定します。

ライフサイクルフックの無効化

まれに、ライフサイクルフックを無効にする必要があります。無効にすると、インスタンスに追加のインターフェイスが追加されません。また、FTDv インスタンスの展開に連続して失敗することがあります。

Auto Scale Manager の無効化

Auto Scale Manager を無効化するには、それぞれの CloudWatch イベント「notify-instance-launch」と「notify-instance-terminate」を無効化する必要があります。これらのイベントを無効にしても、新しいイベントの Lambda はトリガーされません。ただし、すでに実行されている Lambda アクションは続行されます。Auto Scale Manager が突然停止することはありません。スタックの削除またはリソースの削除による突然の停止を試みると、不定状態になる可能性があります。

ロードバランサのターゲット

AWS ロードバランサでは、複数のネットワーク インターフェイスを持つインスタンスに対してインスタンスタイプのターゲットが許可されないため、Gigabit0/1 インターフェイス IP はターゲットグループのターゲットとして設定されます。ただし、現在のところ、AWS Auto Scale の正常性チェックは、IP ではなく、インスタンスタイプのターゲットに対してのみ機能します。また、これらの IP はターゲットグループから自動的に追加されたり、削除されたりしません。したがって、Auto Scale ソリューションは、これら両方のタスクをプログラムで処理します。ただし、メンテナンスやトラブルシューティングの場合は、手動で実行する必要があることがあります。

ターゲットグループへのターゲットの登録

FTDv インスタンスをロードバランサに登録するには、Gigabit0/1 インスタンス IP（外部サブネット）をターゲットとしてターゲットグループに追加する必要があります。「IP アドレスによるターゲットの登録または登録解除」を参照してください。

ターゲットグループからのターゲットの登録解除

ロードバランサに対する FTDv インスタンスの登録を解除するには、Gigabit0/1 インスタンス IP（外部サブネット）をターゲットグループのターゲットとして削除する必要があります。「IP アドレスによるターゲットの登録または登録解除」を参照してください。

インスタンスのスタンバイ

AWS では、Auto Scale グループでのインスタンスの再起動は許可されませんが、ユーザはインスタンスをスタンバイ状態にして再起動アクションを実行できます。これは、ロードバランサのターゲットがインスタンスタイプの場合に最も機能しますが、FTDv VM は、複数のネットワーク インターフェイスがあるため、インスタンスタイプのターゲットとして設定できません。

インスタンスをスタンバイ状態にする

インスタンスがスタンバイ状態になると、正常性プローブが失敗するまで、ターゲットグループ内のそのインスタンスの IP は同じ状態のままになります。このため、インスタンスをスタンバイ状態にする前に、ターゲットグループからそれぞれの IP を登録解除することをお勧めします。詳細については、ターゲットグループからのターゲットの登録解除 （21 ページ）を参照してください。

IP が削除されたら、Auto Scaling グループからのインスタンスの一時的な削除 [英語] を参照してください。

スタンバイ状態からのインスタンスの削除

同様に、インスタンスをスタンバイ状態から実行状態に移行できます。スタンバイ状態から削除すると、インスタンスの IP がターゲットグループのターゲットに登録されます。「ターゲットグループへのターゲットの登録 （21 ページ）」を参照してください。

トラブルシューティングやメンテナンスのためにインスタンスをスタンバイ状態にする方法の詳細については、AWS ニュースブログ [英語] を参照してください。

Auto Scale グループからのインスタンスの削除または分離

Auto Scale グループからインスタンスを削除するには、まずインスタンスをスタンバイ状態に移行する必要があります。「インスタンスをスタンバイ状態にする」を参照してください。スタンバイ状態になったインスタンスは、削除または分離できます。「Auto Scaling グループからの EC2 インスタンスの分離」を参照してください。

FMC 側に変更はありません。必要な変更は手動で実行する必要があります。

インスタンスで終了

インスタンスを終了するには、スタンバイ状態にする必要があります。インスタンスのスタンバイ （22 ページ）を参照してください。インスタンスがスタンバイ状態になったら、終了できます。

インスタンスのスケールイン保護

Auto Scale グループから特定のインスタンスが誤って削除されないようにするために、そのインスタンスをスケールイン保護として作成できます。インスタンスがスケールイン保護されている場合、スケールインイベントが原因で終了することはありません。

インスタンスをスケールイン保護状態にするには、次のリンクを参照してください。

https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html

重要　正常（EC2インスタンスだけでなく、ターゲットIPが正常）なインスタンスの最小数をスケールイン保護として設定することをお勧めします。

ログイン情報と登録 ID の変更

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。

FMC ユーザ名とパスワードの変更

FMC の IP、ユーザ名、またはパスワードを変更する場合は、Auto Scale Manager Lambda 関数とカスタム指標パブリッシャ Lambda 関数の環境変数でそれぞれの変更を実行する必要があります。AWS Lambda 環境変数の使用 [英語] を参照してください。

Lambda の次回実行時に、変更された環境変数が参照されます。

（注）　環境変数は Lambda 関数に直接渡されます。パスワードの複雑さはチェックされません。

FTDv Admin パスワードを変更します。

FTDv パスワードを変更すると、インスタンスを実行するために各デバイスでパスワードを手動で変更する必要があります。新しい FTDv デバイスをオンボードする場合、FTDv パスワードは Lambda 環境変数から取得されます。AWS Lambda 環境変数の使用 [英語] を参照してください。

登録 ID と NAT ID の変更

新しいFTDvデバイスを異なる登録IDとNAT IDでオンボードする場合、FMC登録のために、Configuration.json ファイルでこの情報を変更する必要があります。Configuration.json ファイルは、[Lambda] リソースページにあります。

アクセスポリシーと NAT ポリシーの変更

アクセスポリシーまたは NAT ポリシーへの変更は、デバイスグループの割り当てにより、今後のインスタンスに自動的に適用されます。ただし、既存の FTDv インスタンスを更新するには、設定変更を手動でプッシュして、FMC から展開する必要があります。

AWS リソースに対する変更

AWS の導入後、Auto Scale グループ、起動設定、CloudWatch イベント、スケーリングポリシーなど、多くの項目を変更できます。CloudFormation スタックにリソースをインポートするか、既存のリソースから新しいスタックを作成できます。

AWS リソースで実行される変更を管理する方法の詳細については、既存のリソースを CloudFormation 管理に取り込む [英語] を参照してください。

CloudWatch ログの収集および分析

CloudWatch ログをエクスポートするには、AWS CLI を使用したログデータの Amazon S3 へのエクスポート [英語] を参照してください。

Auto Scale のトラブルシューティングとデバッグ

AWS CloudFormation コンソール

AWS CloudFormation コンソールで CloudFormation スタックへの入力パラメータを確認できます。これにより、Web ブラウザからスタックを直接作成、監視、更新、削除できます。

目的のスタックに移動し、[パラメータ（parameter）] タブを確認します。[Lambda関数環境変数（Lambda Functions environment variables）] タブで Lambda 関数への入力を確認することもできます。*configuration.json* ファイルは、Auto Scale Manager Lambda 関数自体でも表示できます。

AWS CloudFormation コンソールの詳細については、『AWS CloudFormation ユーザーガイド（AWS CloudFormation User Guide）』を参照してください。

Amazon CloudWatch ログ

個々の Lambda 関数のログを表示できます。AWS Lambda はお客様の代わりに Lambda 関数を自動的に監視し、Amazon CloudWatch を通じてメトリックを報告します。関数の障害のトラブルシューティングに役立つように、Lambda は関数によって処理されたすべての要求をログに記録し、Amazon CloudWatch ログを通じてコードによって生成されたログも自動的に保存します。

Lambda コンソール、CloudWatch コンソール、AWS CLI、または CloudWatch API を使用して、Lambda のログを表示できます。ロググループと CloudWatch コンソールを介したロググループへのアクセスの詳細については、『*Amazon CloudWatch* ユーザーガイド（*Amazon CloudWatch*

User Guide）』でモニタリングシステム、アプリケーション、およびカスタムログファイルについて参照してください。

ロードバランサのヘルスチェックの失敗

ロードバランサのヘルスチェックには、プロトコル、ping ポート、ping パス、応答タイムアウト、ヘルスチェック間隔などの情報が含まれます。ヘルスチェック間隔内に 200 応答コードを返す場合、インスタンスは正常と見なされます。

一部またはすべてのインスタンスの現在の状態が `OutOfService` であり、説明フィールドに「インスタンスがヘルスチェックの異常しきい値の数以上連続して失敗しました（Instance has failed at least the Unhealthy Threshold number of health checks consecutively）」というメッセージが表示された場合、インスタンスはロードバランサのヘルスチェックに失敗しています。

FMC 構成の正常性プローブ NAT ルールを確認する必要があります。詳細については、『Troubleshoot a Classic Load Balancer: Health checks』を参照してください。

トラフィックの問題

FTDv インスタンスのトラフィックの問題をトラブルシューティングするには、ロードバランサルール、NAT ルール、および FTDv インスタンスで設定されているスタティックルートを確認する必要があります。

セキュリティグループのルールなど、展開テンプレートで提供される AWS 仮想ネットワーク/サブネット/ゲートウェイの詳細も確認する必要があります。たとえば、「EC2 インスタンスのトラブルシューティング（Troubleshooting EC2 instances）」https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-troubleshoot.htmlなど、AWS のドキュメントを参照することもできます。

FMC への接続に失敗

管理接続が中断された場合は、FMC 構成とログイン情報を確認する必要があります。『*Firepower Management Center Configuration Guide*』の「Requirements and Prerequisites for Device Management」を参照してください。

デバイスが FMC への登録に失敗 FMC

デバイスが FMC に登録できない場合は、FMC 構成に障害があるか到達不能であるか、または FMC に新しいデバイスを収容するキャパシティがあるかどうかを判断する必要があります。『*Firepower Management Center Configuration Guide*』の「Add a Device to the FMC」を参照してください。

FTDv に SSH 接続不可能 FTDv

FTDv に SSH 接続できない場合は、テンプレートを介して複雑なパスワードが FTDv に渡されたかどうかを確認します。