Firepower Threat Defense Virtual Auto Scale for AWS 구축

이 문서에서는 AWS에서 FTDv Auto Scale Manager 용 서버리스 구성 요소를 구축하는 방법을 설명합니다.

중요 구축을 시작하기 전에 전체 문서를 읽어보십시오. 구축을 시작하기 전에 전제 조건이 충족되었는지 확인합니다.

AWS의 FTDv 용 Auto Scale 솔루션

다음 섹션에서는 AWS에서 Auto Scale 솔루션의 구성 요소가 FTDv에서 작동하는 방식을 설명합니다.

Auto Scale 솔루션

Cisco는 람다, 자동 확장 그룹, ELB(Elastic Load Balancing), Amazon S3 버킷, SNS 및 CloudWatch를 비롯한 여러 AWS 서비스를 사용하여 FTDv 방화벽의 자동 확장 그룹을 구축하기 위한 CloudFormation 템플릿 및 스크립트를 제공합니다.

FTDv AWS의 Auto Scale은 완전한 서버리스 방식으로 구현되는 만큼(즉, 이 기능의 자동화와 관련된 헬퍼 VM 없음) AWS 환경의 FTDv 인스턴스에 수평 자동 확장 기능을 추가합니다.

FTDv Auto Scale 솔루션은 다음을 제공하는 CloudFormation 템플릿 기반 구축입니다.

- 완전 자동화된 FTDv 인스턴스 등록 및 FMC 등록 취소
- 확장된 FTDv 인스턴스에 자동으로 적용되는 NAT 정책, 액세스 정책 및 경로

- 로드 밸런서 및 다중 가용성 영역 지원
- Auto Scale 기능 활성화 및 비활성화 지원
- FMC에서만 작동합니다. Firepower Device Manager는 지원되지 않습니다.

Auto Scale(버전 **6.7)** 개선 사항

- Custom Metric Publisher(맞춤형 메트릭 게시자)-새로운 람다 함수가 Auto Scale 그룹에 있는 모든 FTDv 인스턴스의 메모리 사용량에 대해 2분마다 FMC를 폴링한 다음 해당 값을 CloudWatch Metric에 게시합니다. 자세한 내용은 입력 매개변수, 9 페이지를 참조하십시오.
- 메모리 소비를 기반으로 하는 새로운 확장 정책을 사용할 수 있습니다.
- SSH 및 FMC에 대한 보안 터널용 FTDv 개인 IP 연결
- FMC 컨피그레이션 검증
- ELB에서 추가 수신 대기 포트 열기 지원
- 단일 스택 구축으로 수정되었습니다. 모든 람다 함수 및 AWS 리소스는 간소화된 구축을 위해 단일 스택에서 구축됩니다.

지원되는 소프트웨어 플랫폼

FTDv Auto Scale 솔루션은 FMC에서 관리하는 FTDv에 적용 가능하며 소프트웨어 버전과 무관합니다. Cisco Firepower Compatibility Guide는 운영 체제 및 호스팅 환경 요구 사항을 포함해서 Cisco Firepower 소프트웨어 및 하드웨어 호환성에 대한 내용을 제공합니다.

- Firepower Management Centers: Virtual 표는 Firepower 호환성 그리고 AWS의 FMCv에 대한 가상 호스팅 환경 요건을 제시합니다.
- Firepower Threat Defense Virtual Compatibility 표는 Firepower 호환성 그리고 AWS의 FTDv에 대한 가상 호스팅 환경 요건을 제시합니다.

참고 AWS Auto Scale 솔루션 구축을 위해 AWS에서 FTDv에 대해 지원되는 최소 Firepower 버전은 버전 6.4입니다. 메모리 기반 확장을 사용하려면 FMC에서 버전 6.6 이상을 실행해야 합니다.

Auto Scale 사용 사례

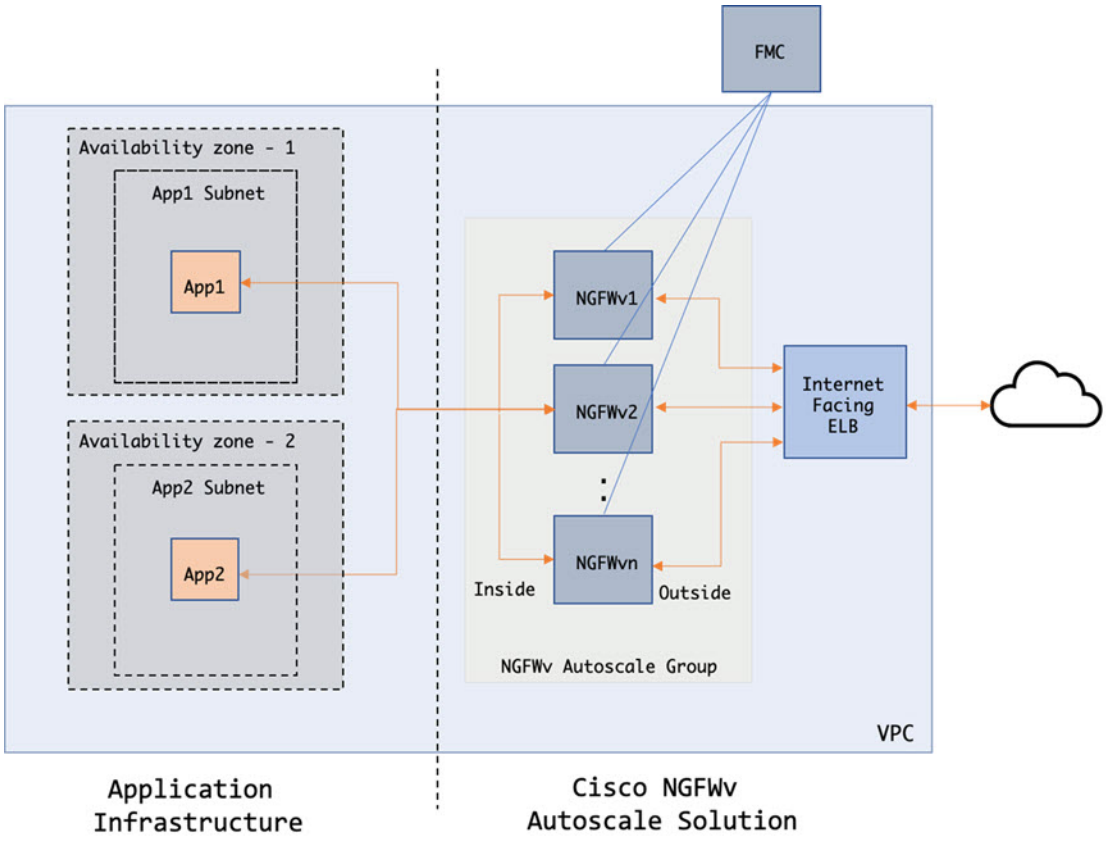
이 FTDv AWS Auto Scale 솔루션의 사용 사례는 그림 1: FTDv Auto Scale 사용 사례 다이어그램, 3 페이지에 제시되어 있습니다. AWS 로드 밸런서는 인바운드 시작 연결만 허용하므로 외부에서 생성된 트래픽만 Cisco FTDv 방화벽을 통해 내부로 전달할 수 있습니다.

참고 보안 포트에는 SSL 서버 인증서, 8 페이지 전제 조건에 설명된 대로 SSL / TLS 인증서가 필요합니다.

인터넷 연결 로드 밸런서는 Network Load Balancer 또는 Application Load Balancer일 수 있습니다. 두 경우 모두 모든 AWS 요건 및 조건이 적용됩니다. 사용 사례 다이어그램에 나와 있는 것처럼 점선의 오른쪽은 FTDv 템플릿을 통해 구축됩니다. 왼쪽은 완전히 사용자 정의된 것입니다.

참고 애플리케이션 시작 아웃 바운드 트래픽은 FTDv를 통과하지 않습니다.

그림 *1: FTDv Auto Scale* 사용 사례 다이어그램



트래픽에 대한 포트 기반 분기가 가능합니다. 이는 NAT 규칙을 통해 수행할 수 있습니다. FMC에서 개체, 디바이스 그룹, NAT 규칙, 액세스 정책의 구성, 15 페이지를 참조하십시오. 예를 들어 인터넷 연결 LB DNS, 포트 80의 트래픽은 Application-1로 라우팅될 수 있습니다. 포트: 88 트래픽을 애플리케이션-2로 라우팅할 수 있습니다.

Auto Scale 솔루션 작동 방식

FTDv 인스턴스를 확장 및 축소하기 위해 Auto Scale Manager라는 외부 엔터티가 메트릭을 모니터링하고, FTDv 인스턴스를 추가 또는 삭제하도록 자동 확장 그룹에 명령하고, 관리 FMC에 FTDv 디바이스를 등록 및 등록 취소하고, FTDv 인스턴스를 구성합니다.

Auto Scale Manager는 AWS 서버리스 아키텍처를 사용하여 구현되며 AWS 리소스, FTDv, FMC . Cisco는 Auto Scale Manager 구성 요소의 구축을 자동화하기 위해 CloudFormation 템플릿을 제공합니다. 이 템플릿은 전체 솔루션이 작동하는 데 필요한 기타 리소스도 구축합니다.

참고 서버리스 Auto Scale 스크립트는 CloudWatch 이벤트에서만 호출되므로 인스턴스가 시작될 때만 실행됩니다.

Auto Scale 솔루션 구성 요소

다음 구성 요소가 Auto Scale 솔루션을 구성합니다.

CloudFormation 템플릿

CloudFormation 템플릿은 AWS의 Auto Scale 솔루션에 필요한 리소스를 구축하는 데 사용됩니다. 템플릿은 다음으로 구성됩니다.

- 자동 확장 그룹, 로드 밸런서, 보안 그룹 및 기타 기타 구성 요소
- 템플릿은 사용자 입력에 따라 구축을 맞춤화합니다.

참고 템플릿에는 사용자 입력을 검증하는 데 제한이 있으므로 구축 중에 입력을 검증하는 것은 사용자의 책임입니다.

람다 함수

Auto Scale은 Python으로 개발한 람다 함수의 집합으로서 라이프사이클 후크, SNS, CloudWatch 이벤트/경보 이벤트에서 트리거됩니다. 기본 기능은 다음과 같습니다.

- 인스턴스에 Diag, Gig0/0 및 Gig 0/1 인터페이스를 추가/제거합니다.
- 로드 밸런서의 대상 그룹에 Gig0/1 인터페이스를 등록합니다.
- FMC에 새 FTDv를 등록합니다.
- FMC를 통해 새 FTDv를 구성하고 구축합니다.
- FMC에서 확장된 FTDv를 등록취소(제거)합니다.
- FMC에서 메모리 메트릭을 게시합니다.

람다 함수는 Python 패키지 형식으로 고객에게 제공됩니다.

라이프 사이클 후크

- 라이프 사이클 후크는 인스턴스에 대한 라이프 사이클 변경 알림을 가져오는 데 사용됩니다.
- 인스턴스 시작의 경우 라이프 사이클 후크를 사용하여 FTDv 인스턴스에 인터페이스를 추가하고 대상 그룹에 외부 인터페이스 IP를 등록할 수 있는 람다 함수를 트리거합니다.
- 인스턴스가 종료되는 경우, 라이프사이클 후크를 사용하여 대상 그룹에서 FTDv 인스턴스의 등록을 취소하는 람다 함수를 트리거합니다.

간편 알림 서비스**(SNS)**

- AWS의 SNS(Simple Notification Service)를 사용하여 이벤트를 생성합니다.
- AWS에는 서버리스 람다 함수에 적합한 오케스트레이터가 없다는 제한 때문에, 솔루션은 SNS를 일종의 기능 체인으로 사용하여 이벤트를 기반으로 람다 함수를 오케스트레이션합니다.

Auto Scale 솔루션 사전 요건

구축 파일 다운로드

FTDv Auto Scale for AWS 솔루션을 시작하는 데 필요한 파일을 다운로드합니다. Firepower 버전의 구축 스크립트 및 템플릿은 GitHub 리포지토리에서 제공됩니다.

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

주의 Cisco에서 제공하는 자동 확장용 구축 스크립트 및 템플릿은 오픈 소스 예시로 제공되며 일반적인 Cisco TAC 지원 범위에서는 다루지 않습니다. GitHub에서 정기적으로 업데이트 및 ReadMe 지침을 확인하십시오.

인프라 구성

복제/다운로드된 GitHub 리포지토리의 **infrastructure.yaml** 파일은 템플릿 폴더에 있습니다. 이 CFT는 버킷 정책을 통해 VPC, 서브넷, 경로, ACL, 보안 그룹, VPC 엔드 포인트 및 S3 버킷을 구축하는 데 사용할 수 있습니다. 이 CFT는 요구 사항에 맞게 수정할 수 있습니다.

다음 섹션에서는 이러한 리소스 및 해당 리소스가 Auto Scale에서 사용되는 방법에 대해 자세히 설명합니다. 이러한 리소스를 수동으로 구축하고 Auto Scale에서도 사용할 수 있습니다.

참고 **infrastructure.yaml** 템플릿은 VPC, 서브넷, ACL, 보안 그룹, S3 버킷 및 VPC 엔드 포인트만 구축합니다. SSL 인증서, 람다 레이어 또는 KMS 키 리소스는 생성하지 않습니다.

VPC

애플리케이션 요구 사항에 따라 VPC를 생성해야 합니다. VPC에는 인터넷에 대한 경로가 연결된 하나 이상의 서브넷이 있는 인터넷 게이트웨이가 있어야 합니다. 보안 그룹, 서브넷 등에 대한 요구 사항은 해당 섹션을 참조하십시오.

서브넷

필요할 경우 애플리케이션 요구 사항에 따라 서브넷을 생성할 수 있습니다. FTDv VM에는 사용 사례에 나와 있는 것처럼 작동하기 위해 3개의 서브넷이 필요합니다.

참고 다중 가용성 영역 지원이 필요한 경우 서브넷은 AWS 클라우드 내의 영역 속성이므로 각 영역에 서브넷이 필요합니다.

외부 서브넷

외부 서브넷에는 인터넷 게이트웨이에 대한 기본 경로가 '0.0.0.0/0'이어야 합니다. 여기에는 FTDv의 외부 인터페이스가 포함되며 인터넷 연결 NLB도 이 서브넷에 포함됩니다.

내부 서브넷

이는 NAT/인터넷 게이트웨이가 있거나 없는 애플리케이션 서브넷과 유사할 수 있습니다. FTDv 상태 프로브의 경우 포트 80을 통해 AWS 메타 데이터 서버(169.254.169.254)에 연결할 수 있어야 합니다.

참고 이 AutoScale 솔루션에서 로드 밸런서 상태 프로브는 inside/Gig0/0 인터페이스를 통해 AWS 메타 데이터 서버로 리디렉션됩니다. 그러나 로드 밸런서에서 FTDv로 전송되는 상태 프로브 연결을 제공하는 고유한 애플리케이션을 사용하여 이를 변경할 수 있습니다. 이 경우 상태 프로브 응답을 제공하려면 AWS Metadata Server 개체를 해당 애플리케이션 IP 주소로 교체해야 합니다.

관리 서브넷

이 서브넷에는 FTDv 관리 인터페이스가 포함되어 있습니다. 이 서브넷에서 FMC를 사용하는 경우 FTDv에 EIP(Elastic IP Address)를 할당하는 것은 선택 사항입니다. 진단 인터페이스도 이 서브넷에 있습니다.

람다 서브넷

AWS 람다 함수를 사용하려면 NAT 게이트웨이가 기본 게이트웨이인 두 개의 서브넷이 필요합니다. 이렇게 하면 VPC 전용의 람다 함수가 생성됩니다. 람다 서브넷은 다른 서브넷만큼 넓을 필요는 없습니다. 람다 서브넷에 대한 모범 사례는 AWS 설명서를 참조하십시오.

애플리케이션 서브넷

Auto Scale 솔루션에서 이 서브넷에 적용되는 제한은 없지만, 애플리케이션이 VPC 외부에서 아웃 바운드 연결을 필요로 하는 경우 서브넷에 각각의 경로가 구성되어 있어야 합니다. 이는 아웃 바운드에서 시작된 트래픽이 로드 밸런서를 통과하지 않기 때문입니다. AWS Elastic Load Balancing User Guide를 참조하십시오.

보안 그룹

제공된 Auto Scale 그룹 템플릿에서 모든 연결이 허용됩니다. Auto Scale 솔루션이 작동하려면 다음 연결만 필요합니다.

표 *1:* 필수 포트

포트	사용	서브넷
8305	FMC-FTDv 보안 터널 연결	관리 서브넷
상태 프로브 포트 (기본값: 8080)	인터넷 연결 로드 밸런서 상태 프로브	외부, 내부 서브넷
애플리케이션 포트	애플리케이션 데이터 트래픽	외부, 내부 서브넷

FMC 인스턴스의 보안 그룹 또는 **ACL**

람다 함수와 FMC 간의 HTTPS 연결을 허용합니다. 람다 함수는 NAT 게이트웨이를 기본 경로로 사용하는 람다 서브넷에서 유지되므로 FMC는 NAT 게이트웨이 IP 주소에서 인바운드 HTTPS 연결을 가질 수 있어야 합니다.

Amazon S3 버킷

Amazon Simple Storage Service(Amazon S3)는 업계 최고의 확장성, 데이터 가용성, 보안 및 성능을 제공하는 개체 스토리지 서비스입니다. 방화벽 템플릿 및 애플리케이션 템플릿 모두에 필요한 모든 파일을 S3 버킷에 담을 수 있습니다.

템플릿이 구축되면 S3 버킷의 Zip 파일을 참조하는 람다 함수가 생성됩니다. 따라서 사용자 계정에서 S3 버킷에 액세스할 수 있어야 합니다.

SSL 서버 인증서

인터넷 연결 로드 밸런서가 TLS / SSL을 지원해야 하는 경우 인증서 ARN이 필요합니다. 자세한 내용은 다음 링크를 참조하십시오.

- 서버 인증서 작업
- 테스트를 위한 개인 키 및 자체 서명 인증서 생성
- 자체 서명 SSL 인증서로 AWS ELB 생성(서드 파티 링크)

ARN의 예: arn:aws:iam::[AWS 계정]:server-certificate/[인증서 이름]

람다 레이어

autoscale_layer.zip은 Linux 환경(예: Python 3.6이 설치된 Ubuntu 18.04)에서 생성 할 수 있습니다.

```
#!/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
```

결과 ***autoscale_layer.zip*** 파일을 *lambda-python-files* 폴더에 복사해야 합니다.

KMS 마스터 키

이는 FMC 및 FTDv 비밀번호가 암호화된 형식인 경우 필요합니다. 그렇지 않으면 이 구성 요소가 필요하지 않습니다. 비밀번호는 여기에 제공된 KMS만 사용하여 암호화해야 합니다. KMS ARN이 CFT에 입력된 경우 비밀번호를 암호화해야 합니다. 그렇지 않으면 비밀번호는 일반 텍스트여야 합니다.

마스터 키 및 암호화에 대한 자세한 내용은 AWS 문서 Creating keys 및 the AWS CLI Command Reference에서 비밀번호 암호화 및 KMS에 대한 내용을 참조하십시오.

예:

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

```
}
$
```

CiphertextBlob 키의 값을 비밀번호로 사용해야 합니다.

Python 3 환경

make.py 파일은 복제된 리포지토리의 최상위 디렉토리에 있습니다. 이렇게하면 python 파일을 Zip 파일로 압축하고 대상 폴더에 복사합니다. 이러한 작업을 수행하려면 Python 3 환경을 사용할 수 있어야 합니다.

Auto Scale 구축

준비

애플리케이션이 구축되었거나 구축 계획을 사용할 수 있어야 합니다.

입력 매개변수

다음 입력 매개 변수는 구축 전에 수집해야 합니다.

표 ***2: Auto Scale*** 입력 매개 변수

파라미터	허용되는 값 / 유형	설명
PodNumber	문자열 허용되는 패턴: '^\d{1,3}$'	Pod 번호입니다. 이는 Auto Scale 그룹 이름(FTDv-Group-Name)의 접미사입니다. 예를 들어 이 값이 '1'인 경우 그룹 이름은 *FTDv-Group-Name-1*이 됩니다. 숫자는 한 자릿수 이상 세 자릿수 이하여야 합니다. 기본값: 1
AutoscaleGrpNamePrefix	문자열	Auto Scale 그룹 이름 접두사입니다. Pod 번호는 접미사로 추가됩니다. 최대 문자수: 18자 예: Cisco-FTDv-1
NotifyEmailID	문자열	Auto Scale 이벤트가 이 이메일 주소로 전송됩니다. 구독 이메일 요청을 수락해야 합니다. 예: admin@company.com

파라미터	허용되는 값 / 유형	설명
VpcId	문자열	디바이스를 구축해야 하는 VPC ID입니다. 이는 AWS 요건에 따라 구성해야 합니다. 유형: AWS::EC2::VPC::Id "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
LambdaSubnets	목록	람다 함수가 구축될 서브넷 유형: List<AWS::EC2::Subnet::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
LambdaSG	목록	람다 함수의 보안 그룹 유형: List<AWS::EC2::SecurityGroup::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
S3BktName	문자열	파일의 S3 버킷 이름입니다. 이는 AWS 요건에 따라 사용자 계정에서 구성해야 합니다. "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
LoadBlancerType	문자열	인터넷 연결 로드 밸런서의 유형(“애플리케이션”또는 “네트워크”)입니다. 예: application
LoadBlancerSG	문자열	로드 밸런서의 보안 그룹 네트워크 로드 밸런서의 경우에는 사용되지 않습니다. 그러나 보안 그룹 ID를 제공해야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.

파라미터	허용되는 값 / 유형	설명
LoadBlancerPort	정수	로드 밸런서 포트 이 포트는 선택한 로드 밸런서 유형에 따라 프로토콜로 HTTP / HTTPS 또는 TCP / TLS를 사용하여 LB에서 열립니다. 포트가 유효한 TCP 포트인지 확인합니다. 이 포트는 로드 밸런서 리스너를 생성하는 데 사용됩니다. 기본값: 80
SSL인증서	문자열	보안 포트 연결을 위한 SSL 인증서의 ARN입니다. 지정하지 않으면 로드 밸런서에서 열린 포트는 TCP / HTTP가 됩니다. 지정된 경우 로드 밸런서에서 열린 포트는 TLS / HTTPS입니다.
TgHealthPort	정수	이 포트는 상태 프로브의 대상 그룹에서 사용됩니다. FTDv에서 이 포트에 도착하는 상태 프로브는 AWS 메타 데이터 서버로 라우팅되며 트래픽에 사용해서는 안 됩니다. 유효한 TCP 포트여야 합니다. 애플리케이션 자체가 상태 프로브에 응답하도록 하려면 FTDv에 따라 NAT 규칙을 변경할 수 있습니다. 이 경우 애플리케이션이 응답하지 않으면 FTDv가 비정상 상태로 표시되고 비정상 인스턴스 임계 값 알람으로 인해 삭제됩니다. 예: 8080
AssignPublicIP	부울	"true"로 선택된 경우 공용 IP가 할당됩니다. BYOL 유형 FTDv의 경우 https://tools.cisco.com에 연결해야 합니다. 예: true
인스턴스 유형	문자열	AMI(Amazon Machine Image)는 인스턴스의 크기와 필요한 메모리 양을 결정하는 다양한 인스턴스 유형을 지원합니다. FTDv을 지원하는 AMI 인스턴스 유형만 사용해야 합니다. Firepower 릴리스 노트 를 참조하십시오. 예: c4.2xlarge
LicenseType	문자열	FTDv 라이선스 유형(BYOL 또는 PAYG) 관련 AMI ID가 동일한 라이선싱 유형인지 확인합니다. 예: BYOL

파라미터	허용되는 값 / 유형	설명
AmiId	문자열	FTDv AMI ID(유효한 Cisco FTDv AMI ID) 유형: AWS::EC2::Image::Id 영역 및 원하는 이미지 버전에 따라 올바른 AMI ID를 선택하십시오. Auto Scale 기능은 Firepower 버전 6.4 이상, BYOL / PAYG 이미지를 지원합니다. 두 경우 모두 AWS 마켓플레이스에서 라이선스를 수락해야 합니다. BYOL의 경우 컨피그레이션 JSON의 'licenseCaps' 키를 'BASE', 'MALWARE', 'THREAT', 'URLFilter' 등의 기능으로 업데이트하십시오.
NoOfAZs	정수	FTDv가 1 ~ 3의 범위에 걸쳐 있어야 하는 가용성 영역의 수입니다. ALB 구축의 경우 AWS에 필요한 최소값은 2입니다. 예: 2
ListOfAzs	쉼표로 구분된 문자열	쉼표로 구분된 영역의 목록(순서대로) 참고 나열되는 순서가 중요합니다. 서브넷 목록은 동일한 순서로 제공되어야 합니다. "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오. 예: us-east-1a, us-east-1b, us-east-1c
MgmtInterfaceSG	문자열	FTDv 관리 인터페이스의 보안 그룹입니다. 유형: List<AWS::EC2::SecurityGroup::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
InsideInterfaceSG	문자열	FTDv 내부 인터페이스의 보안 그룹입니다. 유형: AWS::EC2::SecurityGroup::Id "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.

파라미터	허용되는 값 / 유형	설명
OutsideInterfaceSG	문자열	FTDv 외부 인터페이스의 보안 그룹입니다. 유형: AWS::EC2::SecurityGroup::Id "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오. 예: sg-0c190a824b22d52bb
MgmtSubnetId	쉼표로 구분된 목록	쉼표로 구분된 관리 서브넷 ID 목록입니다. 목록은 해당 가용 영역과 동일한 순서여야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
InsideSubnetId	쉼표로 구분된 목록	쉼표로 구분된 inside/Gig0/0 ID 목록입니다. 목록은 해당 가용 영역과 동일한 순서여야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
OutsideSubnetId	쉼표로 구분된 목록	쉼표로 구분된 outside/Gig0/1 ID 목록입니다. 목록은 해당 가용 영역과 동일한 순서여야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "*infrastructure.yaml*" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에이 값이 지정됩니다. 해당 값을 사용하십시오.
KmsArn	문자열	기존 KMS의 ARN(대기시 암호화 할 AWS KMS 키) 지정된 경우 FMC 및 FTDv 비밀번호를 암호화해야 합니다. 비밀번호 암호화는 지정된 ARN만 사용하여 수행해야 합니다. 암호화된 비밀번호 생성 예 : "aws kmscrypt --key-id<KMS ARN> --plaintext<password> ". 표시된 대로 생성된 비밀번호를 사용하십시오. 예: arn:aws:kms:us-east-1:[AWS 계정]:key/7d586a25-5875-43b1-bb68-a452e2f6468e

파라미터	허용되는 값 / 유형	설명
ngfwPassword	문자열	모든 FTDv 인스턴스에는 기본 비밀번호가 표시되며, 이 비밀번호는 Launch Template(시작 템플릿)(Autoscale Group)의 *Userdata(*사용자 데이터*)* 필드에 입력됩니다. 이 입력은 FTDv에 액세스할 수 있게 되면 비밀번호를 새로 입력한 비밀번호로 변경합니다. KMS ARN이 사용되지 않는 경우 일반 텍스트 비밀번호를 사용하십시오. KMS ARN을 사용하는 경우 암호화된 비밀번호를 사용해야 합니다. 예: Cisco123789! or AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	숫자 문자열	람다 함수와 FTDv 관리 인터페이스 모두에 연결할 수 있는 관리 FMC의 IP 주소입니다. 예: 10.10.17.21
fmcOperationsUsername	문자열	관리 FMC에서 생성된 네트워크 관리자 이상의 권한이 있는 사용자. 자세한 내용은 Firepower Management Center Configuration Guide에서 사용자 및 역할 생성에 대한 내용을 참조하세요. 예: apiuser-1
fmcOperationsPassword	문자열	KMS ARN이 언급되지 않은 경우 일반 텍스트 비밀번호를 사용하십시오. 언급된 경우 암호화된 비밀번호를 사용해야 합니다. 예: Cisco123@ or AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQRnCAajB
fmcDeviceGrpName	문자열	FMC 디바이스 그룹 이름 예: AWS-Cisco-NGFW-VMs-1
fmcPublishMetrics	부울	"TRUE"로 설정된 경우, 제공된 디바이스 그룹에 등록된 FTDv 센서의 메모리 소비량을 가져 오기 위해 2분마다 한 번씩 실행되는 람다 함수가 생성됩니다. 허용되는 값: TRUE, FALSE 예: true

파라미터	허용되는 값 / 유형	설명
fmcMetricsUsername	문자열	AWS CloudWatch에 대한 메트릭 게시의 고유한 FMC 사용자 이름입니다. 자세한 내용은 Firepower Management Center Configuration Guide에서 사용자 및 역할 생성에 대한 내용을 참조하세요. "fmcPublishMetrics"가 "FALSE"로 설정된 경우 이 입력을 제공할 필요가 없습니다. 예: publisher-1
fmcMetricsPassword	문자열	AWS CloudWatch에 메트릭 게시를 위한 FMC 비밀번호입니다. KMS ARN이 언급되지 않은 경우 일반 텍스트 비밀번호를 사용하십시오. 언급된 경우 암호화된 비밀번호를 사용해야 합니다. "fmcPublishMetrics"가 "FALSE"로 설정된 경우 이 입력을 제공할 필요가 없습니다. 예: Cisco123789!
CpuThresholds	쉼표로 구분된 정수	CPU 하한 임계값 및 CPU 상한 임계값 최소값은 0이고 최대값은 99입니다. 기본값: 10, 70 하한 임계값은 상한 임계값보다 작아야 합니다. 예: 30, 70
MemoryThresholds	쉼표로 구분된 정수	하위 MEM 임계값 및 상위 MEM 임계값 최소값은 0이고 최대값은 99입니다. 기본값: 40, 70 하한 임계값은 상한 임계값보다 작아야 합니다. "fmcPublishMetrics" 매개 변수가 "FALSE"이면 아무런 효과가 없습니다. 예: 40, 50

FMC에서 개체, 디바이스 그룹, NAT 규칙, 액세스 정책의 구성

전체 기능을 갖춘 별도 서버의 다중 디바이스 관리자인 Firepower Management Center(FMC)를 사용해 FTDv를 관리할 수 있습니다. FTDv는 FDTv 가상 시스템에 할당한 관리 인터페이스의 FMC에 등록하고 통신합니다. 자세한 내용은 Firepower Management Center를 이용한 Firepower Threat Defense Virtual 관련 정보를 참조하십시오.

FTDv 컨피그레이션에 사용되는 모든 개체는 사용자가 생성해야 합니다.

중요 디바이스 그룹을 생성하고 규칙을 적용해야 합니다. 디바이스 그룹에 적용된 모든 컨피그레이션은 FTDv 인스턴스로 푸시됩니다.

개체

다음 개체를 생성합니다.

표 *3: FTDv* 관리를 위한 *FMC* 컨피그레이션 개체

개체 유형	이름	값
Host(호스트)	aws-metadata-server	169.254.169.254
포트	health-check-port	8080 / 필요에 따라 다른 포트
Zone	내부 / 다른 이름	—
Zone	외부 / 다른 이름	—

NAT 정책

일반적인 NAT 규칙은 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환(PAT)이라고 합니다. NAT 정책에 대한 자세한 내용은 Firepower Management Center로 Firepower Threat Defense Virtual 관리의 NAT 구성를 참조하십시오.

NAT 정책에는 하나의 필수 규칙이 필요합니다.

- 소스 영역: 외부 영역
- 대상 영역: 내부 영역
- 원본 소스: any-ipv4
- 원본 소스 포트 - 원본/기본
- 원본 대상: 인터페이스
- 원본 대상 포트: 8080/ 또는 사용자가 구성한 상태 포트
- 변환된 소스: any-ipv4
- 변환된 소스 포트: 원본/기본
- 변환된 대상: aws-metadata-server
- 변환된 대상 포트: 80 / HTTP

마찬가지로 모든 데이터 트래픽 NAT 규칙을 추가할 수 있으므로 이 컨피그레이션이 FTDv 디바이스로 푸시됩니다.

중요 생성된 NAT 정책은 디바이스 그룹에 적용해야 합니다. 람다 함수의 FMC 검증에서 이를 확인합니다.

액세스 정책

액세스 제어를 내부에서 외부로 향하는 트래픽을 허용하도록 구성합니다. 모든 필수 정책이 포함된 액세스 정책을 생성할 수 있습니다. 이 포트의 트래픽에 도달할 수 있도록 상태 포트 개체를 허용해야 합니다. 액세스 정책에 대한 자세한 내용은 Firepower Management Center로 Firepower Threat Defense Virtual 관리의 액세스 제어 구성를 참조하십시오.

컨피그레이션 JSON 파일 업데이트

Configuration.json 파일은 GitHub 리포지토리에서 가져온 아카이브 Zip의 일부인 ***lambda_python_files*** 폴더에 있습니다. JSON 키는 변경할 수 없습니다. FTDv VM의 모든 고정 경로는 JSON 파일에서 구성해야 합니다.

고정 경로 컨피그레이션의 예는 다음을 참조하십시오.

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

JSON 파일의 모든 값은 기본 FTDv 비밀번호를 제외하고 요구 사항에 따라 수정할 수 있습니다.

Amazon Simple Storage Service(S3)로 파일 업로드

대상 디렉토리의 모든 파일을 Amazon S3 버킷에 업로드해야 합니다. 원할 경우 CLI를 사용하여 대상 디렉토리의 모든 파일을 Amazon S3 버킷에 업로드할 수 있습니다.

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

스택 구축

구축을 위한 모든 전제 조건이 완료되면 AWS CloudFormation 스택을 생성할 수 있습니다.

대상 디렉토리의 *deploy_ngfw_autoscale.yaml* 파일을 사용합니다.

입력 매개변수, 9 페이지에 수집된 매개 변수를 제공합니다.

구축 검증

템플릿 구축이 완료되면, 람다 함수 및 CloudWatch 이벤트가 생성되었는지 검증해야 합니다. 기본적으로 Auto Scale 그룹에는 최소 및 최대 인스턴스 수가 0입니다. 원하는 인스턴스 수를 사용하여 AWS EC2 콘솔에서 Auto Scale그룹을 편집해야 합니다. 그러면 새 FTDv 인스턴스가 트리거됩니다.

인스턴스를 하나만 실행하고 그 워크플로우를 확인하고 예상대로 작동하는지에 대한 동작을 검증하는 것이 좋습니다. FTDv의 실제 요구 사항을 구축한 후에는 동작에 대해 확인할 수도 있습니다. AWS Scaling 정책에서 FTDv 인스턴스가 제거되지 않도록 최소 인스턴스 수를 축소 보호로 표시 할 수 있습니다.

Auto Scale 유지 보수 작업

확장 프로세스

이 항목에서는 Auto Scale 그룹에 대해 하나 이상의 확장 프로세스를 일시 중지한 다음 다시 시작하는 방법을 설명합니다.

확장 작업 시작 및 중지

스케일 아웃/인 작업을 시작하고 중지하려면 다음 단계를 수행합니다.

- AWS Dynamic Scaling의 경우 - 다음 링크를 참조하여 스케일 아웃 작업을 활성화하거나 비활성화할 수 있습니다.

  확장 프로세스 일시 중단 및 다시 시작

상태 모니터

CloudWatch Cron 작업은 60분마다 Health Doctor 모듈의 Auto Scale Manager 람다를 트리거합니다.

- 유효한 FTDv VM에 속한 비정상적인 IP가 있는 경우 FTDv가 1시간 이상 경과하면 해당 인스턴스가 삭제됩니다.
- 해당 IP가 유효한 FTDv VM에 있지 않으면 대상 그룹에서 IP만 제거됩니다.

상태 모니터는 디바이스 그룹, 액세스 정책 및 NAT 규칙에 대한 FMC 컨피그레이션도 검증합니다. IP/인스턴스 상태가 비정상이거나 FMC 검증에 실패하면 상태 모니터가 사용자에게 이메일을 전송합니다.

상태 모니터 비활성화

상태 모니터를 비활성화하려면 ***constant.py***에서 상수를 "True"로 지정합니다.

상태 모니터 활성화

상태 모니터를 활성화하려면 ***consist.py***에서 상수를 "False"로 지정합니다.

라이프 사이클 후크 비활성화

라이프 사이클 후크를 비활성화해야 하는 경우는 드물지만 비활성화되면 인스턴스에 인터페이스를 추가하지 않습니다. 또한 일련의 FTDv 인스턴스 구축이 실패할 수 있습니다.

Auto Scale Manager 비활성화

Auto Scale Manager를 비활성화하려면 각 CloudWatch 이벤트 "notify-instance-launch" 및 "notify-instance-terminate"를 비활성화해야 합니다. 이 기능을 비활성화하면 새 이벤트에 대해 람다가 트리거되지 않습니다. 그러나 이미 실행중인 람다 작업은 계속 진행됩니다. Auto Scale Manager는 갑자기 중지되지 않습니다. 스택 삭제 또는 리소스 삭제로 인해 갑자기 중지하려고 시도하면 무한 상태가 발생할 수 있습니다.

로드 밸런서 대상

AWS로드 밸런서는 둘 이상의 네트워크 인터페이스가 있는 인스턴스에 대해 인스턴스 유형 대상을 허용하지 않으므로 Gigabit0/1 인터페이스 IP는 대상 그룹에서 대상으로 구성됩니다. 그러나 현재 AWS Auto Scale 상태 확인은 IP가 아닌 인스턴스 유형 대상에 대해서만 작동합니다. 또한 이러한 IP는 대상 그룹에서 자동으로 추가되거나 제거되지 않습니다. 따라서 Auto Scale 솔루션은 이러한 두 작업을 모두 프로그래밍 방식으로 처리합니다. 그러나 유지 보수 또는 문제 해결의 경우에는 수동으로 수행해야 하는 상황이 있을 수 있습니다.

대상 그룹에 대상 등록

로드 밸런서에 FTDv 인스턴스를 등록하려면 Gigabit0/1 인스턴스 IP(외부 서브넷)를 대상 그룹의 대상으로 추가해야 합니다. Register or Deregister Targets by IP Address를 참조하십시오.

대상 그룹에서 대상 등록 취소

로드 밸런서에 FTDv 인스턴스를 등록 취소하려면 Gigabit0/1 인스턴스 IP(외부 서브넷)를 대상 그룹에서 삭제해야 합니다. Register or Deregister Targets by IP Address를 참조하십시오.

인스턴스 스탠바이

AWS는 Auto Scale 그룹에서 인스턴스 재부팅을 허용하지 않지만 사용자가 인스턴스를 스탠바이 상태로 설정하고 이러한 작업을 수행할 수 있도록 허용합니다. 그러나 이는 로드 밸런서 대상이 인스턴스 유형인 경우에 가장 적합합니다. 그러나 복수의 네트워크 인터페이스 때문에 FTDv VM은 인스턴스 유형 대상으로 구성할 수 없습니다.

인스턴스를 스탠바이 상태로 설정

인스턴스가 스탠바이 상태가 되면 대상 그룹의 해당 IP는 상태 프로브가 실패할 때까지 계속 동일한 상태로 유지됩니다. 따라서 인스턴스를 스탠바이 상태로 설정하기 전에 대상 그룹에서 각 IP를 등록 취소하는 것이 좋습니다. 자세한 내용은 대상 그룹에서 대상 등록 취소, 19 페이지를 참조하십시오.

IP가 제거되면 Temporarily Removing Instances from Your Auto Scaling Group을 참조하십시오.

스탠바이에서 인스턴스 제거

마찬가지로 인스턴스를 스탠바이 상태에서 실행 중 상태로 이동할 수 있습니다. 스탠바이 상태에서 제거한 후에는 인스턴스의 IP를 대상 그룹 대상에 등록해야 합니다. 대상 그룹에 대상 등록, 19 페이지의 내용을 참조하십시오.

문제 해결 또는 유지 보수를 위해 인스턴스를 스탠바이 상태로 설정하는 방법에 대한 자세한 내용은 AWS 뉴스 블로그를 참조하십시오.

Auto Scale 그룹에서 인스턴스 제거/분리

Auto Scale 그룹에서 인스턴스를 제거하려면 먼저 스탠바이 상태로 이동해야 합니다. "Put Instances on Stand-by"를 참조하십시오. 인스턴스가 스탠바이 상태가 되면 제거하거나 분리할 수 있습니다. Detach EC2 Instances from Your Auto Scaling Group을 참조하십시오.

FMC 측에는 변경 사항이 없습니다. 필요한 변경은 수동으로 수행해야 합니다.

인스턴스 종료

인스턴스를 종료하려면 스탠바이 상태로 설정해야 합니다. 인스턴스 스탠바이, 19 페이지을 참조하십시오. 인스턴스가 스탠바이 상태가 되면 종료를 진행할 수 있습니다.

인스턴스 축소 보호

Auto Scale 그룹에서 특정 인스턴스가 실수로 제거되는 것을 방지하기 위해 축소(scale in) 보호로 설정할 수 있습니다. 인스턴스가 축소(Scale-In) 보호 상태에 있을 경우 해당 인스턴스는 축소 이벤트로 인해 종료되지 않습니다.

인스턴스를 축소 보호 상태로 전환하려면 다음 링크를 참조하십시오.

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

중요 상태가 양호한 최소 인스턴스 수(대상 IP는 EC2 인스턴스가 아니라 정상이어야 함)를 축소 보호하는 것이 좋습니다.

자격 증명 및 등록 **ID** 변경

컨피그레이션의 변경 사항은 이미 실행중인 인스턴스에 자동으로 반영되지 않습니다. 변경 사항은 향후 디바이스에만 반영됩니다. 이러한 변경 사항은 기존 디바이스에 수동으로 푸시해야 합니다.

FMC 사용자 이름 및 비밀번호 변경

FMC IP, 사용자 이름 또는 비밀번호를 변경하는 경우, 각각의 변경은 Auto Scale Manager 람다 함수 및 맞춤형 메트릭 게시자 람다 함수 환경 변수에서 수행해야 합니다. Using AWS Lambda Environment Variables을 확인하십시오.

다음 번에 람다가 실행되면 변경된 환경 변수를 참조합니다.

참고 환경 변수는 람다 함수에 직접 제공됩니다. 여기에는 비밀번호 복잡성 확인이 없습니다.

FTDv 관리자 비밀번호 변경

FTDv 비밀번호를 변경하려면 사용자가 실행중인 인스턴스에 대해 각 디바이스에서 비밀번호를 수동으로 변경해야 합니다. 새 FTDv 디바이스를 온보딩할 경우, FTDv 비밀번호는 람다 환경 변수에서 가져옵니다. Using AWS Lambda Environment Variables을 확인하십시오.

등록 및 **NAT ID** 변경

새 FTDv 디바이스를 다른 등록 및 NAT ID로 온보딩하려면 FMC 등록을 위해 이 정보를 Configuration.json 파일에서 변경해야 합니다. Configuration.json 파일은 람다 리소스 페이지에 있습니다.

액세스 정책 및 NAT 정책 변경

액세스 정책 또는 NAT 정책에 대한 모든 변경 사항은 디바이스 그룹 할당을 통해 향후 인스턴스에 자동으로 적용됩니다. 그러나 기존 FTDv 인스턴스를 업데이트하려면 컨피그레이션 변경 사항을 수동으로 푸시하고 FMC에서 구축해야 합니다.

AWS 리소스 변경

Auto Post Group, Launch Configuration(컨피그레이션 시작), CloudWatch 이벤트, 확장 정책 등 AWS 사후 구축에서 여러 가지 사항을 변경할 수 있습니다. 리소스를 CloudFormation 스택으로 가져 오거나 기존 리소스에서 새 스택을 생성할 수 있습니다.

AWS 리소스에서 수행되는 변경 사항을 관리하는 방법에 대한 자세한 내용은 Bringing Existing Resources Into CloudFormation Management를 참조하십시오.

CloudWatch 로그 수집 및 분석

CloudWatch 로그를 내보내려면 Export Log Data to Amazon S3 Using the AWS CLI를 참조하십시오.

Auto Scale 문제 해결 및 디버깅

AWS CloudFormation 콘솔

AWS CloudFormation 콘솔에서 CloudFormation 스택에 대한 입력 매개 변수를 확인할 수 있습니다. 그러면 웹 브라우저에서 직접 스택을 생성, 모니터링, 업데이트 및 삭제할 수 있습니다.

필요한 스택으로 이동하여 매개 변수 탭을 확인합니다. 또한 람다 함수 환경 변수 탭에서 람다 함수에 대한 입력을 확인할 수도 있습니다. *configuration.json* 파일은 Auto Scale Manager 람다 함수 자체에서도 볼 수 있습니다.

AWS CloudFormation 콘솔에 대한 자세한 내용은 *AWS CloudFormation User Guide*를 참조하십시오.

Amazon Cloudwatch 로그

개별적인 람다 함수의 로그를 볼 수 있습니다. AWS 람다는 사용자를 대신하여 람다 함수를 자동으로 모니터링하며 Amazon CloudWatch를 통해 메트릭을 보고합니다. 함수에서 장애를 해결하는 데 도움이 되도록 람다는 함수에서 처리한 모든 요청을 기록하고, 코드에서 생성된 로그를 Amazon CloudWatch Logs를 통해 자동으로 저장합니다.

람다 콘솔, CloudWatch 콘솔, AWS CLI 또는 CloudWatch API를 사용하여 람다에 대한 로그를 볼 수 있습니다. CloudWatch 콘솔을 통해 로그 그룹에 액세스하고 액세스하는 방법에 대한 자세한 내용은 *Amazon CloudWatch User Guide*의 모니터링 시스템, 애플리케이션 및 맞춤형 로그 파일을 참조하십시오.

로드 밸런서 상태 확인 실패

로드 밸런서 상태 확인에는 프로토콜, ping 포트, ping 경로, 응답 시간 초과, 상태 확인 간격 등의 정보가 포함됩니다. 상태 확인 간격 내에 200 응답 코드를 반환하는 인스턴스는 정상 상태로 간주됩니다.

일부 또는 모든 인스턴스의 현재 상태가 `OutOfService`이고 설명 필드에 `인스턴스가 최소한 비정상 상태 임계 횟수 이상 실패했다`는 메시지가 표시되면 인스턴스가 로드 밸런서 상태 검사에 실패한 것입니다.

FMC 컨피그레이션에서 상태 프로브 NAT 규칙을 확인해야 합니다. 자세한 내용은 Troubleshoot a Classic Load Balancer: Health checks를 참조하십시오.

트래픽 문제

FTDv 인스턴스의 트래픽 문제를 해결하려면 로드 밸런서 규칙, NAT 규칙 및 FTDv 인스턴스에 구성된 고정 경로를 확인해야 합니다.

또한 보안 그룹 규칙 등 구축 템플릿에 제공된 AWS 가상 네트워크 / 서브넷 / 게이트웨이 세부 정보도 확인해야 합니다. Troubleshooting EC2 instances와 같은 AWS 설명서를 참조할 수도 있습니다.

FMC 연결에 실패함

관리 연결이 중단된 경우 FMC 컨피그레이션 및 자격 증명을 확인해야 합니다. *Firepower Management Center Configuration Guide*의 "디바이스 관리 요구 사항 및 사전 요구 사항"을 참조하십시오.

디바이스 등록 실패 FMC

디바이스가 FMC에 등록하지 못하면 FMC 컨피그레이션에 결함이 있는지/ 연결할 수 없는지 또는 FMC에 새 디바이스를 수용할 수 있는 용량이 있는지 확인해야 합니다. *Firepower Management Center Configuration Guide*에서 "FMC에 디바이스 추가"를 참조하십시오.

SSH 실패 FTDv

SSH를 FTDv로 연결할 수 없는 경우 템플릿을 통해 복잡한 비밀번호가 FTDv에 전달되었는지 확인합니다.