AWS Cloud에 Firepower Management Center Virtual 구축

Amazon VPC(Amazon Virtual Private Cloud)를 통해 사용자가 정의한 가상 네트워크에서 AWS(Amazon Web Services) 리소스를 실행할 수 있습니다. 자체 데이터 센터에서 운영할 수 있는 기존 네트워크와 매우 유사한 이 가상 네트워크는 확장 가능한 AWS 인프라 사용 시의 이점도 제공합니다.

AWS Cloud에서 Firepower Management Center Virtual(FMCv)을 구축할 수 있습니다.

- FMCv 구축 및 AWS , 1 페이지
- AWS 구축에 대한 지침 및 제한 사항, 3 페이지
- AWS 환경 구성, 5 페이지
- Firepower Management Center Virtual 인스턴스 구축, 10 페이지

FMCv 구축 및 AWS

FMCv에는 업그레이드 **(6.6.0** 이상**)**에 **28GB RAM** 필요

FMCv 플랫폼이 업그레이드 중 수행할 새로운 메모리 검사를 도입했습니다. 가상 어플라이언스에 28GB 미만의 RAM을 할당하면 버전 6.6.0 이상으로의 FMCv 업그레이드가 실패합니다.

중요 버전 6.6.0 릴리스부터는 클라우드 기반 FMCv 구축(AWS, Azure)의 메모리 부족 인스턴스 유형이 완전히 사용되지 않습니다. 이전 Firepower 버전에서도 해당 인스턴스를 사용하여 새 FMCv 인스턴스를 생성할 수 없습니다. 기존 인스턴스는 계속 실행할 수 있습니다. 표 1: AWS 지원 인스턴스 FMCv, 2 페이지의 내용을 참조하십시오.

이 메모리 검사의 결과로 지원되는 플랫폼에서 더 낮은 메모리 인스턴스를 지원할 수 없게 됩니다.

다음 표에는 FMCv가 지원하는 AWS 인스턴스 유형, 즉 버전 6.5.x 이하가 지원하는 인스턴스 및 버전 6.6.0 이상이 지원하는 인스턴스가 요약되어 있습니다.

참고 Firepower 버전 6.6에서는 다음 표에 나와 있는 C5 인스턴스 유형에 대한 지원이 추가되었습니다. 인스턴스 유형이 클수록 AWS VM에 더 많은 CPU 리소스를 제공하여 성능을 높이고 일부는 더 많은 네트워크 인터페이스를 허용합니다.

표 *1: AWS* 지원 인스턴스 *FMCv*

플랫폼	버전 **6.6.0** 이상	버전 **6.5** 이하*
FMCv	c3.4xlarge: 16개의 vCPU, 30GB	c3.xlarge: 4개의 vCPU, 7.5GB
	c4.4xlarge: 16개의 vCPU, 30GB	c3.2xlarge: 8개의 vCPU, 15GB
	c5.4xlarge: 16개의 vCPU, 32GB	c4.xlarge: 4개의 vCPU, 7.5GB
	—	c4.2xlarge: 8개의 vCPU, 15GB
	* 버전 6.6.0이 릴리스된 후에는 이러한 인스턴스 유형은 FMCv가 더 이상 지원하지 않습니다. 버전 6.6.0부터는 최소 28GB RAM이 있는 인스턴스를 사용하여 FMCv(모든 버전)을 구축해야 합니다. 인스턴스 크기 조정, 2 페이지의 내용을 참조하십시오.	

사용되지 않는 인스턴스

현재 버전 6.5.x 이하 버전의 FMCv 구축을 계속 실행할 수 있지만 다음 인스턴스를 사용하여 새 FMCv 구축(모든 버전)을 시작할 수는 없습니다.

- c3.xlarge—vCPU 4개, 7.5GB(버전 6.6.0 이상 이후 FMCv에 대해 비활성화됨)
- c3.2xlarge—vCPU 8개, 15GB(버전 6.6.0 이상 이후 FMCv에 대해 비활성화됨)
- c4.xlarge-vCPU 4개, 7.5GB(버전 6.6.0 이상 이후 FMCv에 대해 비활성화됨)
- c4.2xlarge—vCPU 8개, 15GB(버전 6.6.0 이상 이후 FMCv에 대해 비활성화됨)

인스턴스 크기 조정

이전 버전의 FMCv(6.2.x, 6.3.x, 6.4.x, 6.5.x)에서 버전 6.6.0으로의 업그레이드 경로에 28GB RAM 메모리 검사가 포함되어 있으므로 현재 인스턴스 유형의 크기를 버전 6.6.0이 지원하는 크기로 조정해야 합니다(표 1: AWS 지원 인스턴스 FMCv, 2 페이지 참고).

현재 인스턴스 유형과 원하는 새 인스턴스 유형이 호환되는 경우 인스턴스의 크기를 조정할 수 있습니다. FMCv 구축의 경우:

- c3.xlarge 또는 c3.2xlarge의 크기를 c3.4xlarge 인스턴스 유형으로 조정합니다.
- c4.xlarge 또는 c4.2xlarge의 크기를 c4.4xlarge 인스턴스 유형으로 조정합니다.

인스턴스 크기를 조정하기 전에 다음 사항에 유의하십시오.

- 인스턴스 유형을 변경하기 전에 인스턴스를 중지해야 합니다.
- 현재 인스턴스 유형이 선택한 새 인스턴스 유형과 호환되는지 확인합니다.
- 이 인스턴스에 인스턴스 스토어 볼륨이있는 경우, 인스턴스가 중지되면 해당 인스턴스의 모든 데이터가 손실됩니다. 크기를 조정하기 전에 인스턴스 스토어 지원 인스턴스를 마이그레이션합니다.
- 탄력적 IP 주소를 사용하지 않는 경우 인스턴스를 중지하면 퍼블릭 IP 주소가 해제됩니다.

인스턴스 크기 조정 방법에 대한 지침은 AWS 문서 "Changing the Instance Type"(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html)을 참조하십시오.

AWS 솔루션 개요

AWS는 클라우드 컴퓨팅 플랫폼을 구성하는 원격 컴퓨팅 서비스(웹 서비스라고도 함) 컬렉션으로 Amazon.com에서 제공합니다. 이러한 서비스는 전 세계 11개 지역에서 운영됩니다. 일반적으로 FMCv를 구축할 때는 다음과 같은 AWS 서비스를 숙지해야 합니다.

- Amazon EC2(Elastic Compute Cloud) - Amazon의 데이터 센터에서 방화벽 등의 자체 애플리케이션 및 서비스를 실행하고 관리하기 위한 가상 컴퓨터를 임대할 수 있는 웹 서비스입니다.
- Amazon VPC(Virtual Private Cloud) - Amazon 퍼블릭 클라우드 내에 격리된 프라이빗 네트워크를 구성하는 데 사용할 수 있는 웹 서비스입니다. EC2 인스턴스는 VPC 내에서 실행할 수 있습니다.
- Amazon S3(Simple Storage Service) - 데이터 스토리지 인프라를 제공하는 웹 서비스입니다.

AWS에서 어카운트를 생성하고, AWS 마법사 또는 수동 컨피그레이션을 사용하여 VPC 및 EC2 구성 요소를 설정하고, AMI(Amazon Machine Image) 인스턴스를 선택합니다. AMI는 인스턴스 실행에 필요한 소프트웨어 컨피그레이션을 포함한 템플릿입니다.

참고 AMI 이미지는 AWS 환경이 아닌 곳에서 다운로드할 수 없습니다.

AWS 구축에 대한 지침 및 제한 사항

사전 요구 사항

AWS에서 FMCv와 관련이 있는 사전 요구 사항은 다음과 같습니다.

- Amazon 어카운트는 aws.amazon.com에서 생성할 수 있습니다.
- Cisco Smart Account는 Cisco Software Central(https://software.cisco.com/)에서 생성할 수 있습니다.
- FMCv에 라이선스를 부여합니다. 가상 플랫폼 라이선스에 대한 일반적인 지침은 Firepower Management Center Virtual 라이선스의 내용을 참조하십시오. 라이선스를 관리하는 방법에 대한

자세한 내용은 *Firepower Management Center* 설정 가이드의 "Firepower System 라이선싱"을 참조하십시오.

- FMCv 인터페이스 요구 사항:
  - 관리 인터페이스
- 통신 경로:
  - FMCv에 액세스하기 위한 공용/탄력적 IP
- FMCv 및 Firepower System 호환성에 대한 내용은 Cisco Firepower 호환성 가이드를 참조하십시오.

지침

AWS에서 FMCv와 관련이 있는 지침은 다음과 같습니다.

- VPC(Virtual Private Cloud)에서 구축
- 향상된 네트워킹(SR-IOV) - 사용 가능한 경우
- Amazon Marketplace에서 구축
- 인스턴스당 최대 4개의 vCPU
- L3 네트워크의 사용자 구축

제한 사항

AWS에서 FMCv와 관련이 있는 제한 사항은 다음과 같습니다.

- Cisco Firepower Management Center Virtual 어플라이언스에는 시리얼 번호가 없습니다. **System(**시스템**)** > **Configuration(**구성**)** 페이지에는 가상 플랫폼에 따라 **None(**없음**)** 또는 **Not Specified(**지정되지 않음**)** 중 하나가 표시됩니다.
- 모든 IP 주소 컨피그레이션(CLI 또는 Firepower Management Center의 컨피그레이션)은 AWS 콘솔에서 생성된 컨피그레이션과 일치해야 하며, 구축 중에 컨피그레이션 정보를 적어 두어야 합니다.
- IPv6은 현재 지원되지 않습니다.
- 부팅 후에는 인터페이스를 추가할 수 없습니다.
- 복제/스냅샷은 현재 지원되지 않습니다.
- 고가용성은 지원되지 않습니다.

AWS 환경 구성

AWS에 FMCv를 구축하려면 구축 관련 요구 사항과 설정을 사용하여 Amazon VPC를 구성해야 합니다. 대부분의 상황에서는 설정 마법사가 설정 과정을 안내합니다. AWS는 소개 정보에서 고급 기능에 이르기까지 서비스와 관련한 여러 가지 유용한 정보를 찾을 수 있는 온라인 설명서를 제공합니다. 자세한 내용은 AWS 시작하기를 참조하십시오.

AWS 설정을 더 세부적으로 제어할 수 있도록 인스턴스를 실행하기 전에 다음과 같은 섹션에서 FMCv의 VPC 및 EC2 구성을 안내합니다.

- VPC 생성, 5 페이지
- 인터넷 게이트웨이 추가, 6 페이지
- 서브넷 추가, 6 페이지
- 경로 테이블 추가, 7 페이지
- 보안 그룹 생성, 8 페이지
- 네트워크 인터페이스 생성, 8 페이지
- 탄력적 IP 생성, 9 페이지

VPC 생성

VPC(Virtual Private Cloud)는 AWS 어카운트 전용 가상 네트워크이며, AWS Cloud의 다른 가상 네트워크와 논리적으로 격리되어 있습니다. Firepower Management Center Virtual 인스턴스 등의 AWS 리소스를 VPC에서 실행할 수 있습니다. VPC의 IP 주소 범위를 선택하고, 서브넷을 생성하고, 라우트 테이블, 네트워크 게이트웨이, 보안 설정을 구성하여 VPC를 구성할 수 있습니다.

시작하기 전에

- AWS 어카운트를 생성합니다.
- Firepower Management Center Virtual 인스턴스에 AMI를 사용할 수 있는지 확인합니다.

단계 **1** aws.amazon.com에 로그인하고 지역을 선택합니다.

AWS는 여러 지역으로 나뉘며, 이 지역은 상호 격리되어 있습니다. 화면의 우측 상단에 지역이 표시됩니다. 한 지역의 리소스가 다른 지역에는 나타나지 않습니다. 원하는 지역에 있는지 정기적으로 확인합니다.

단계 **2** **Services(**서비스**)** > **VPC**를 클릭합니다.

단계 **3** **VPC Dashboard(VPC** 대시보드**)** > **Your VPCs(**사용 중인 **VPC)**를 클릭합니다.

단계 **4** **Create VPC(VPC** 생성**)**를 클릭합니다.

단계 **5** **Create VPC(VPC** 생성**)** 대화 상자에 다음 정보를 입력합니다.

a) VPC를 식별하기 위한 사용자 정의 **Name tag(**이름 태그**)**.
b) IP 주소의 **CIDR block(CIDR** 블록**)**. CIDR(Classless Inter-Domain Routing) 표기법은 IP 주소와 관련 라우팅 접두사를 축약한 표현입니다. 예를 들면 10.0.0.0/24와 같습니다.
c) **Tenancy(**테넌시**)** 설정을 Default(기본값)로 설정하면 이 VPC에서 실행되는 인스턴스가 실행 시에 지정된 테넌시 특성을 사용합니다.

단계 **6** VPC를 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 VPC에 인터넷 게이트웨이를 추가합니다.

인터넷 게이트웨이 추가

VPC를 인터넷에 연결하기 위해 인터넷 게이트웨이를 추가할 수 있습니다. VPC 외부의 IP 주소에 대한 트래픽을 인터넷 게이트웨이로 라우팅할 수 있습니다.

시작하기 전에

- FMCv 인스턴스용으로 VPC를 생성합니다.

단계 **1** **Services(**서비스**)** > **VPC**를 클릭합니다.
단계 **2** **VPC Dashboard(VPC** 대시보드**)** > **Internet Gateways(**인터넷 게이트웨이**)**를 클릭하고 **Create Internet Gateway(**인터넷 게이트웨이 생성**)**를 클릭합니다.
단계 **3** 게이트웨이 식별을 위한 사용자 정의 Name tag(이름 태그)를 입력한 후, 게이트웨이를 생성하려면 Yes, Create(예, 생성합니다)를 클릭합니다.
단계 **4** 이전 단계에서 생성한 게이트웨이를 선택합니다.
단계 **5** **Attach to VPC(VPC**에 연결**)**를 클릭하고 이전에 생성한 VPC를 선택합니다.
단계 **6** VPC에 게이트웨이를 연결하려면 **Yes, Attach(**예**,** 연결합니다**)**를 클릭합니다.

기본적으로 VPC에서 실행되는 인스턴스는 게이트웨이를 생성하여 VPC에 연결할 때까지 인터넷과 통신할 수 없습니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 VPC에 서브넷을 추가합니다.

서브넷 추가

Firepower Management Center Virtual 인스턴스를 연결할 수 있는 VPC의 IP 주소 범위를 세그먼트로 지정할 수 있습니다. 보안 및 운영 요구 사항에 따라 서브넷을 생성하여 인스턴스를 그룹화할 수 있

습니다. Firepower Threat Defense Virtual의 경우에는 트래픽용 서브넷과 관리용 서브넷을 모두 생성해야 합니다.

단계 **1** **Services(**서비스**)** > **VPC**를 클릭합니다.

단계 **2** **VPC Dashboard(VPC** 대시보드**)** > **Subnets(**서브넷**)**를 클릭하고 **Create Subnet(**서브넷 생성**)**을 클릭합니다.

단계 **3** **Create Subnet(**서브넷 생성**)** 대화 상자에 다음 정보를 입력합니다.

a) 서브넷을 식별하기 위한 사용자 정의 **Name tag(**이름 태그**)**.

b) 이 서브넷에 사용할 **VPC**.

c) 이 서브넷이 상주할 **Availability Zone(**가용성 영역**)**. Amazon이 해당 영역을 선택할 수 있게 하려면 No Preference(환경 설정 없음)를 선택합니다.

d) IP 주소의 **CIDR block(CIDR** 블록**)**. 서브넷의 IP 주소 범위는 VPC의 IP 주소 범위의 하위 집합이어야 합니다. 블록 크기는 /16 네트워크 마스크와 /28 네트워크 마스크 사이여야 합니다. 서브넷의 크기는 VPC의 크기와 같아도 됩니다.

단계 **4** 서브넷을 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **5** 필요한 서브넷 수만큼 위의 단계를 반복합니다. 관리 트래픽용으로 별도의 서브넷을 생성하고, 데이터 트래픽용으로 필요한 수만큼의 서브넷을 생성합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 VPC에 라우트 테이블을 추가합니다.

경로 테이블 추가

VPC용으로 구성한 게이트웨이에 라우트 테이블을 연결할 수 있습니다. 여러 서브넷을 단일 라우트 테이블과 연결할 수는 있지만, 각 서브넷은 한 번에 하나의 라우트 테이블에만 연결할 수 있습니다.

단계 **1** **Services(**서비스**)** > **VPC**를 클릭합니다.

단계 **2** **VPC Dashboard(VPC** 대시보드**)** > **Route Tables(**경로 테이블**)**를 클릭하고 **Create Route Tables(**경로 테이블 생성**)**를 클릭합니다.

단계 **3** 라우트 테이블 식별을 위한 사용자 정의 **Name tag(**이름 태그**)**를 입력합니다.

단계 **4** 드롭다운 목록에서 이 라우트 테이블을 사용할 **VPC**를 선택합니다.

단계 **5** 라우트 테이블을 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **6** 방금 생성한 라우트 테이블을 선택합니다.

단계 **7** **Routes(**라우트**)** 탭을 클릭하여 상세 정보 창에 라우트 정보를 표시합니다.

단계 **8** **Edit(**수정**)**, **Add another route(**다른 라우트 추가**)**를 차례로 클릭합니다.

a) **Destination(**대상**)** 열에 **0.0.0.0/0**을 입력합니다.

b) 위의 단계에서 생성한 인터넷 게이트웨이를 **Target(**대상**)** 열에서 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

단계 **10** **Subnet Associations(**서브넷 연결**)** 탭을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 **11** FMCv의 관리 인터페이스에 사용할 서브넷 옆의 확인란을 선택하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 보안 그룹을 생성합니다.

보안 그룹 생성

허용되는 프로토콜, 포트 및 소스 IP 범위를 지정하는 규칙을 사용하여 보안 그룹을 생성할 수 있습니다. 각 인스턴스에 할당할 수 있는 각기 다른 규칙을 사용해 여러 보안 그룹을 생성할 수 있습니다. 이 기능에 대해 잘 알지 못하는 경우 AWS의 보안 그룹 관련 상세 설명서를 참조하십시오.

단계 **1** **Services(**서비스**)** > **EC2**를 클릭합니다.

단계 **2** **EC2 Dashboard(EC2** 대시보드**)** > **Security Groups(**보안 그룹**)**를 클릭합니다.

단계 **3** **Create Security Group(**보안 그룹 생성**)**을 클릭합니다.

단계 **4** **Create Security Group(**보안 그룹 생성**)** 대화 상자에 다음과 같은 정보를 입력합니다.

a) 보안 그룹 식별을 위한 사용자 정의 **Security group name(**보안 그룹 이름**)**.

b) 이 보안 그룹에 대한 **Description(**설명**)**.

c) 이 보안 그룹과 연결된 **VPC**.

단계 **5** **Security group rules(**보안 그룹 규칙**)**를 구성합니다.

a) **Inbound(**인바운드**)** 탭을 클릭하고 **Add Rule(**규칙 추가**)**을 클릭합니다.

참고 AWS 외부에서 FMCv를 관리하려면 HTTPS 및 SSH 액세스가 필요합니다. 이에 따라 소스 IP 주소를 지정해야 합니다. 또한 AWS VPC 내에 FMCv와 FTDv를 모두 구성하는 경우에는 개인 IP 관리 서브넷 액세스를 허용해야 합니다.

b) **Outbound(**아웃바운드**)** 탭을 클릭한 다음, **Add Rule(**규칙 추가**)**을 클릭하여 아웃바운드 트래픽용 규칙을 추가하거나, 기본값인 **All traffic(**모든 트래픽**)**(**Type(**유형**)**의 경우) 및 **Anywhere(**모든 위치**)**(**Destination(**대상**)**의 경우)를 그대로 유지합니다.

단계 **6** 보안 그룹을 생성하려면 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 네트워크 인터페이스를 생성합니다.

네트워크 인터페이스 생성

고정 IP 주소를 사용하여 FMCv용 네트워크 인터페이스를 생성할 수 있습니다. 특정 구축에 필요한 만큼 네트워크 인터페이스(외부 및 내부)를 생성합니다.

단계 **1** **Services(**서비스**)** > **EC2**를 클릭합니다.

단계 **2** **EC2 Dashboard(EC2** 대시보드**)** > **Network Interfaces(**네트워크 인터페이스**)**를 클릭합니다.

단계 **3** **Create Network Interface(**네트워크 인터페이스 생성**)**를 클릭합니다.

단계 **4** **Create Network Interface(**네트워크 인터페이스 생성**)** 대화 상자에 다음 정보를 입력합니다.

a) 네트워크 인터페이스에 대한 사용자 정의 **Description(**설명**)**(선택 사항)

b) 드롭다운 목록에서 **Subnet(**서브넷**)**을 선택합니다. Firepower 인스턴스를 생성할 VPC의 서브넷을 선택해야 합니다.

c) **Private IP(**개인 **IP)** 주소를 입력합니다. **auto-assign(**자동 할당**)**보다는 고정 IP 주소를 사용하는 것이 좋습니다.

d) 하나 이상의 **Security groups(**보안 그룹**)**를 선택합니다. 보안 그룹의 필수 포트가 모두 열려 있는지 확인합니다.

단계 **5** 네트워크 인터페이스를 생성하려면 **Yes, Create(**예**,** 생성합니다**)**를 클릭합니다.

단계 **6** 방금 생성한 네트워크 인터페이스를 선택합니다.

단계 **7** 마우스 오른쪽 버튼을 클릭하고 **Change Source/Dest. Check(**소스/대상 확인 변경**)** 를 선택합니다.

단계 **8** **Disabled(**비활성화**)** 선택하고 **Save(**저장**)**를 클릭합니다.

생성하는 모든 네트워크 인터페이스에 대해 이 단계를 반복합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 탄력적 IP 주소를 생성합니다.

탄력적 IP 생성

인스턴스를 생성하면 공용 IP 주소가 인스턴스와 연결됩니다. 해당 공용 IP 주소는 인스턴스를 중지하고 시작할 때 자동으로 변경됩니다. 이 문제를 해결하려면 탄력적 IP 주소를 사용하여 인스턴스에 영구적 공용 IP 주소를 할당합니다. 탄력적 IP는 FMCv 및 기타 인스턴스에 대한 Remote Access에 사용되는 예약된 공용 IP입니다. 이 기능에 대해 잘 알지 못하는 경우 AWS의 탄력적 IP 관련 상세 설명서를 참조하십시오.

참고 최소한 FMCv용으로 탄력적 IP 주소를 1개 생성하고, Firepower Threat Defense Virtual 관리 및 진단 인터페이스용으로 탄력적 IP 주소를 2개 생성할 수 있습니다.

단계 **1** **Services(**서비스**)** > **EC2**를 클릭합니다.

단계 **2** **EC2 Dashboard(EC2** 대시보드**)** > **Elastic IPs(**탄력적 **IP)**를 클릭합니다.

단계 **3** **Allocate New Address(**새 주소 할당**)**를 클릭합니다.

필요한 수만큼의 탄력적/공용 IP에 대해 이 단계를 반복합니다.

단계 **4** 탄력적 IP를 생성하려면 **Yes, Allocate(**예**,** 할당합니다**)**를 클릭합니다.

단계 **5** 구축에 필요한 탄력적 IP 수만큼 위의 단계를 반복합니다.

다음에 수행할 작업

다음 섹션에 설명된 대로 FMCv를 구축합니다.

Firepower Management Center Virtual 인스턴스 구축

시작하기 전에

- AWS 환경 구성에 설명된 대로 AWS VPC 및 EC2 요소를 구성합니다.
- FMCv 인스턴스에 AMI를 사용할 수 있는지 확인합니다.

단계 **1** https://aws.amazon.com/marketplace(Amazon Marketplace)로 이동하여 로그인합니다.

단계 **2** Amazon Marketplace에 로그인한 후 Firepower Management Center Virtual용으로 제공된 링크를 클릭합니다.

참고 이전에 AWS를 사용했다면 로그아웃했다가 다시 로그인해야 링크가 작동합니다.

단계 **3** **Continue(**계속**)**를 클릭하고 **Manual Launch(**수동 실행**)** 탭을 클릭합니다.

단계 **4** **Accept Terms(**약관 동의**)**를 클릭합니다.

단계 **5** 원하는 지역에서 **Launch with EC2 Console(EC2** 콘솔로 실행**)**을 클릭합니다.

단계 **6** Firepower Management Center Virtual에서 지원하는 **Instance Type(**인스턴스 유형**)**을 선택합니다. 지원되는 인스턴스 유형은 FMCv 구축 및 AWS 를 참조하십시오.

단계 **7** 화면 하단의 **Next: Configure Instance Details(**다음**:** 인스턴스 상세 정보 구성**)** 버튼을 클릭합니다.

a) 이전에 생성한 VPC와 일치하도록 **Network(**네트워크**)**를 변경합니다.

b) 이전에 생성한 관리 서브넷과 일치하도록 **Subnet(**서브넷**)**을 변경합니다. IP 주소를 지정하거나 자동 생성을 사용할 수 있습니다.

c) **Advanced Details(**고급 상세 정보**)**에서 기본 로그인 정보를 추가합니다.

디바이스 이름과 비밀번호에 대한 요구 사항을 충족하도록 아래의 예시를 수정합니다.

샘플 로그인 구성:

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

주의 **Advanced Details(**고급 상세정보**)** 필드에 데이터를 입력할 때는 일반 텍스트만 사용하십시오. 텍스트 편집기에서 이 정보를 복사하는 경우에는 일반 텍스트로만 복사해야 합니다. 유니코드 데이터(공백 포함)를 **Advanced Details(**고급 상세정보**)** 필드에 복사하는 경우, 인스턴스가 손상될 수 있으며 인스턴스를 종료하고 다시 생성해야 합니다.

단계 **8** **Next: Add Storage(**다음**:** 스토리지 추가**)**를 클릭하여 스토리지 디바이스 설정을 구성합니다.

볼륨 Size (GiB)(크기(GiB))가 250GiB가 되도록 루트 볼륨 설정을 수정합니다. 볼륨 크기가 250GiB 미만이면 이벤트 스토리지가 제한되므로 해당 크기는 지원되지 않습니다.

단계 **9** **Next: Tag Instance(**다음**:** 인스턴스 태그 지정**)**를 클릭합니다.

태그는 대/소문자를 구별하는 키-값 쌍으로 구성됩니다. 예를 들어 **Key(**키**)** = Name, **Value(**값**)** = Management를 사용하여 태그를 정의할 수 있습니다.

단계 **10** **Next: Configure Security Group(**다음**:** 보안 그룹 구성**)**을 선택합니다.

단계 **11** **Select an existing Security Group(**기존 보안 그룹 선택**)**을 클릭하고 이전에 구성한 보안 그룹을 선택하거나 새 보안 그룹을 생성합니다. 보안 그룹 생성에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

단계 **12** **Review and Launch(**검토 및 실행**)**를 클릭합니다.

단계 **13** **Launch(**실행**)**를 클릭합니다.

단계 **14** 기존 키 쌍을 선택하거나 새 키 쌍을 생성합니다.

참고 기존 키 쌍을 선택하거나 새 키 쌍을 생성할 수 있습니다. 키 쌍은 AWS가 저장하는 공개 키와 사용자가 저장하는 개인 키 파일로 구성됩니다. 이 두 키를 함께 사용하면 인스턴스에 안전하게 연결할 수 있습니다. 키 쌍은 인스턴스에 연결하는 데 필요할 수도 있으므로 확인된 위치에 저장해야 합니다.

단계 **15** **Launch Instances(**인스턴스 실행**)**를 클릭합니다.

단계 **16** **EC2 Dashboard(EC2** 대시보드**)** > **Elastic IPs(**탄력적 **IP)**를 클릭하고 이전에 할당한 IP를 찾거나 새 IP를 할당합니다.

단계 **17** 탄력적 IP를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 **Associate Address(**주소 연결**)**를 선택합니다.

인스턴스 또는 네트워크 인터페이스를 찾아서 선택한 다음 Associate(연결)를 클릭합니다.

단계 **18** **EC2 Dashboard(EC2** 대시보드**)** > **Instances(**인스턴스**)**를 클릭합니다.

단계 **19** FMCv 인스턴스 상태는 "running(실행 중)"으로 표시되며, 몇 분만 지나면 상태 확인에서 "2/2 checks(2/2 확인)"에 대해 pass(통과)가 표시됩니다. 그러나 구축 및 초기 설정 프로세스를 완료하려면 약 30~40분이 걸립니다. 상태를 보려면 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Instance Settings(**인스턴스 설정**)** > **Get Instance Screenshot(**인스턴스 스크린샷 가져오기**)**을 선택합니다.

약 30~40분 후 설정이 완료되면 **Instance Screenshot(**인스턴스 스크린샷**)**에 "Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)(AWS용 Cisco Firepower Management Center vW.X.Y(빌드 ZZ)"와 비슷한 메시지가 표시되며, 그 다음에는 추가 출력이 몇 줄 표시될 수 있습니다.

그러면 SSH 또는 HTTP를 사용하여 새로 생성된 FMCv에 로그인할 수 있습니다. 실제 구축 시간은 지역별 AWS 로드에 따라 달라질 수 있습니다.

다음과 같이 SSH를 사용하여 FMCv에 액세스할 수 있습니다.

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

SSH 인증은 키 쌍으로 처리됩니다. 비밀번호는 필요하지 않습니다. 비밀번호를 입력하라는 메시지가 표시된다면 설정이 아직 실행 중인 것입니다.

다음과 같이 HTTPS를 사용하여 FMCv에 액세스할 수도 있습니다.

```
https//<Public_Elastic_IP>
```

참고 "system startup processes are still running(시스템 시작 프로세스가 아직 실행되고 있습니다)"가 표시된다면 설정이 아직 완료되지 않은 것입니다.

SSH 또는 HTTPS에서 응답이 없으면 다음 항목을 다시 확인하십시오.

- 구축이 완료되었는지 확인합니다. FMCv VM 인스턴스 스크린샷에 "Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)"(AWS용 Cisco Firepower Management Center vW.X.Y(빌드 ZZ))와 비슷한 메시지가 표시되며, 그 다음에는 추가 출력이 몇 줄 표시될 수 있습니다.
- 탄력적 IP가 있고, 해당 IP가 Firepower Management Center의 관리 네트워크 인터페이스(eni)에 연결되어 있으며, 해당 IP 주소에 연결되어 있는지 확인합니다.
- VPC와 연결된 인터넷 게이트웨이(igw)가 있는지 확인합니다.
- 관리 서브넷에 라우트 테이블이 연결되어 있는지 확인합니다.
- 관리 서브넷에 연결된 라우트 테이블에 인터넷 게이트웨이(igw)를 가리키는 "0.0.0.0/0"에 대한 라우트가 있는지 확인합니다.
- 연결에 사용하는 IP 주소에서 들어오는 SSH 및/또는 HTTPS를 보안 그룹이 허용하는지 확인합니다.

다음에 수행할 작업

정책 및 디바이스 설정 구성

Firepower Threat Defense Virtual을 설치하고 Management Center에 디바이스를 추가한 후에는 Firepower Management Center 사용자 인터페이스를 사용하여 AWS에서 실행 중인 Firepower Threat Defense Virtual의 디바이스 관리 설정을 구성하고 Firepower Threat Defense Virtual 디바이스를 사용하여 트래픽을 관리하기 위한 액세스 제어 정책 및 기타 관련 정책을 구성할 수 있습니다. 보안 정책은 Firepower Threat Defense Virtual에서 제공하는 Next Generation IPS 필터링 및 애플리케이션 필터링 등의 서비스를 제어합니다. Firepower Management Center를 사용하여 Firepower Threat Defense Virtual에서 보안 정책을 구성하십시오. 보안 정책 구성 방법에 대한 자세한 내용은 Firepower 설정 가이드 또는 Firepower Management Center의 온라인 도움말을 참조하십시오.

-