Oracle Cloud Infrastructure에 Firepower Management Center Virtual 구축

OCI(Oracle Cloud Infrastructure)는 Oracle에서 제공하는 고 가용성 호스팅 환경에서 애플리케이션을 실행할 수 있는 퍼블릭 클라우드 컴퓨팅 서비스입니다. OCI는 Oracle의 자율 서비스, 통합 보안 및 서버리스 컴퓨팅을 결합하여 엔터프라이즈 애플리케이션에 실시간 탄력성을 제공합니다.

OCI에서 Cisco Firepower Management Center Virtual(FMCv)을 구축할 수 있습니다.

FMCv 구축 및 OCI

Cisco Firepower Management Center Virtual (FMCv) 물리적 Cisco와 동일한 소프트웨어를 실행하여 가상 폼 팩터에서 검증된 보안 기능을 제공합니다. FMCv은 퍼블릭 OCI에서 구축될 수 있습니다. 그런 다음 가상 및 물리적 Firepower 디바이스를 관리하도록 구성할 수 있습니다.

OCI 컴퓨팅 셰이프

셰이프는 인스턴스 수에 할당되는 CPU 수, 메모리 양 및 기타 리소스를 결정하는 템플릿입니다. FMCv는 다음 OCI 셰이프 유형을 지원합니다.

표 *1:* 지원되는 컴퓨팅 셰이프 ***FMCv***

셰이프 유형	속성	
	oCPU	**RAM(GB)**
VM.Standard2.4	4	60GB

참고 지원되는 셰이프 유형은 예고 없이 변경될 수 있습니다.

- OCI에서 1 oCPU는 vCPU 2개와 같습니다.
- FMCv에는 1 개의 인터페이스가 필요합니다.

OCI에서 계정을 생성하고, Oracle Cloud Marketplace에서 Cisco Firepower Management Center virtual(FMCv) 제품을 사용하여 컴퓨팅 인스턴스를 실행한 다음 OCI 셰이프를 선택합니다.

OCI에서 FMCv 사전 요건

- https://www.oracle.com/cloud/에서 OCI 계정 생성
- Cisco Smart Account는 Cisco Software Central(https://software.cisco.com/)에서 생성할 수 있습니다.
  - Firepower Management Center의 보안 서비스에 대해 모든 라이선스 권한을 구성합니다.
  - 라이선스를 관리하는 방법에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 "Firepower System 라이선싱"을 참조하십시오.
- 인터페이스 요구 사항:
  - 관리 인터페이스 - Firepower Threat Defense 디바이스를 Firepower Management Center에 연결하는 데 사용되는 인터페이스입니다.
- 통신 경로:
  - FMCv에 대한 관리 액세스를 위한 공용 IP
- Firepower Management Center Virtual 및 Firepower System 호환성에 대해서는 Cisco Firepower Compatibility를 참조하십시오.

FMCv 및 OCI에 대한 지침 및 제한

지원 기능

- OCI VCN(Virtual Cloud Network)에 구축
- 인스턴스당 최대 8개의 vCPU
- 라우팅 모드(기본값)
- 라이선싱 – BYOL만 지원됨

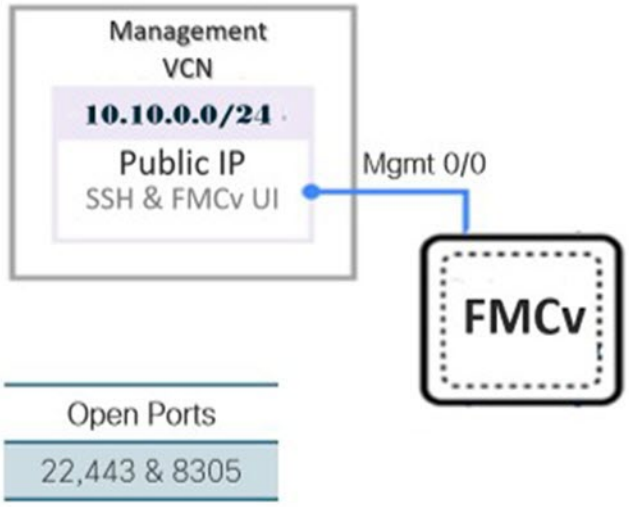
지원되지 않는 기능

- IPv6
- FMCv 네이티브 HA
- 자동 확장
- 투명 / 인라인 / 패시브 모드
- 멀티컨텍스트 모드

OCI의 FMCv에 대한 네트워크 토폴로지 예

다음 그림에는 OCI에 서브넷 1 개가 구성된 FMCv의 일반적인 토폴로지가 나와 있습니다.

그림 *1: OCI*에서의 *FMCv* 구축 토폴로지 예



OCI에 FMCv 구축

VCN(Virtual Cloud Network) 구성

FMCv 구축을 위해 VCN(Virtual Cloud Network)을 구성합니다.

시작하기 전에

참고 탐색 메뉴에서 서비스를 선택하면 왼쪽의 메뉴에 컴파트먼트 목록이 포함됩니다. 컴파트먼트는 리소스에 대한 액세스를 보다 쉽게 제어할 수 있도록 구성하는 데 도움이 됩니다. 테넌시가 프로비저닝되면 루트 컴파트먼트가 Oracle에 의해 생성됩니다. 관리자는 루트 컴파트먼트에서 더 많은 컴파트먼트를 생성한 다음 액세스 규칙을 추가하여 어떤 사용자가 보고 액세스할 수 있는지 제어할 수 있습니다. 자세한 내용은 Oracle 문서 "Managing Compartments"을 참조하십시오.

단계 **1** OCI에 로그인하고 지역을 선택합니다.

OCI는 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** **Networking(**네트워킹**)** > **Virtual Cloud Networks(**가상 클라우드 네트워크**)**를 선택하고 **Create VCN(VCN** 생성**)**을 클릭합니다.

단계 **3** VCN에 대한 설명이 포함된 이름(예: *FMCv-Management*)을 입력합니다.

단계 **4** VCN의 **CIDR** 블록을 입력합니다.

단계 **5** **Create VCN(VCN** 생성**)**을 클릭합니다.

다음에 수행할 작업

다음 절차를 계속 진행하여 관리 VCN을 완료할 수 있습니다.

네트워크 보안 그룹 생성

네트워크 보안 그룹은 vNIC에 적용되는 vNIC 집합과 보안 규칙 집합으로 구성됩니다.

단계 **1** **Networking(**네트워킹**)** > **Virtual Cloud Networks(**가상 클라우드 네트워크**)** > **Virtual Cloud Network Details(**가상 클라우드 네트워크 세부 사항**)** > **Network Security Groups(**네트워크 보안 그룹**)**를 선택하고 **Create Network Security Group(**네트워크 보안 그룹 생성**)**을 클릭합니다.

단계 **2** 네트워크 보안 그룹을 설명하는 **Name(**이름**)**(예: *FMCv-Mgmt-Allow-22-443-8305*)을 입력합니다.

단계 **3** **Next(**다음**)**를 클릭합니다.

단계 **4** 보안 규칙을 추가합니다.

a) SSH 액세스를 위해 TCP 포트 22를 허용하는 규칙을 추가합니다.

b) HTTPS 액세스를 위해 TCP 포트 443을 허용하는 규칙을 추가합니다.

c) TCP 포트 8305를 허용하는 규칙을 추가합니다.

FMCv를 통해 Firepower 디바이스 FMCv를 관리할 수 있습니다. HTTPS 연결을 위해 포트 8305를 열어야 합니다. Firepower Management Center 자체에 액세스하려면 포트 443이 필요합니다.

단계 **5** **Create(**생성**)**를 클릭합니다.

인터넷 게이트웨이 생성

관리 서브넷에 액세스를 개방하려면 인터넷 게이트웨이가 필요합니다.

단계 **1** **Networking(**네트워킹**)** > **Virtual Cloud Networks(**가상 클라우드 네트워크**)** > **Virtual Cloud Network Details(**가상 클라우드 네트워크 세부 사항**)** > **Internet Gateways(**인터넷 게이트웨이**)**를 선택하고 **Create Internet Gateway(**인터넷 게이트웨이 생성**)**를 클릭합니다.

단계 **2** 인터넷 게이트웨이의 설명 이름(예: *FMCv-IG*)을 입력합니다.

단계 **3** **Create Internet Gateway(**인터넷 게이트웨이 생성**)**를 클릭합니다.

단계 **4** 인터넷 게이트웨에 라우트 추가

a) **Networking(**네트워킹**)** > **Virtual Cloud Networks(**가상 클라우드 네트워크**)** > **Virtual Cloud Network Details(**가상 클라우드 네트워크 세부 사항**)** > **Route Tables(**라우트 테이블**)**를 선택합니다.
b) 경로 규칙을 추가하려면 기본 경로 테이블에 대한 링크를 클릭합니다.
c) 경로 규칙 추가를 클릭합니다.
d) **Target Type(**대상 유형**)** 드롭 다운에서 **Internet Gateway(**인터넷 게이트웨이**)**를 선택합니다.
e) 대상 CIDR 블록을 입력합니다(예: 0.0.0.0/0).
f) **Target Internet Gateway(**대상 인터넷 게이트웨이**)** 드롭 다운에서 생성한 게이트웨이를 선택합니다.
g) 경로 규칙 추가를 클릭합니다.

서브넷 생성

각 VCN에는 최소한 하나의 서브넷이 있습니다. 관리 VCN에 대한 관리 서브넷을 생성합니다.

단계 **1** **Networking(**네트워킹**)** > **Virtual Cloud Networks(**가상 클라우드 네트워크**)** > **Virtual Cloud Network Details(**가상 클라우드 네트워크 세부 사항**)** > **Subnets(**서브넷**)**를 선택하고 **Create Subnet(**서브넷 생성**)**를 클릭합니다.

단계 **2** 서브넷을 설명하는 이름(예: *Management(*관리*)*)을 입력합니다.

단계 **3** 서브넷 유형을 선택합니다(권장 기본값 **Regional(**지역별**)**은 유지).

단계 **4** **CIDR** 블록을 입력합니다(예: 10.10.0.0/24). 서브넷의 내부(비 공용) IP 주소는 이 CIDR 블록에서 가져옵니다.

단계 **5** **Route Table(**경로 테이블**)** 드롭 다운에서 이전에 생성한 경로 테이블 중 하나를 선택합니다.

단계 **6** 서브넷의 서브넷 액세스를 선택합니다.

관리 서브넷의 경우 공용 서브넷이어야 합니다.

단계 **7** **DHCP** 옵션을 선택합니다.

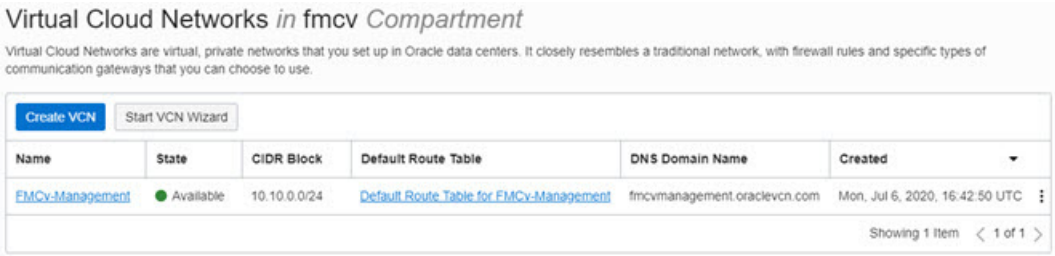
단계 **8** 이전에 생성한 보안 목록을 선택합니다.

단계 **9** **Create Subnet(**서브넷 생성**)**을 클릭합니다.

다음에 수행할 작업

관리 VCN을 구성하고 나면 FMCv를 시작할 수 있습니다. FMCv VCN 컨피그레이션의 예는 다음 그림을 참조하십시오.

그림 *2: FMCv* 가상 클라우드 네트워크



OCI에서 FMCv 인스턴스 생성

Oracle Cloud Marketplace에서 Cisco Firepower Management Center Virtual(FMCv)-BYOL 제품을 사용하여 컴퓨팅 인스턴스를 통해 OCI에 FMCv를 구축합니다. CPU 수, 메모리 양, 네트워크 리소스 등의 특성에 따라 가장 적합한 시스템 형태를 선택합니다.

단계 **1** OCI포털에 로그인합니다.

화면의 우측 상단에 지역이 표시됩니다. 원하는 지역에 있는지 정기적으로 확인합니다.

단계 **2** **Marketplace(**마켓플레이스**)** > **Applications(**애플리케이션**)**을 선택합니다.

단계 **3** "Cisco Firepower Management Center virtual(FMCv)"의 마켓플레이스를 검색하고 제품을 선택합니다.

단계 **4** 이용 약관을 검토하고, 제가 검토한 후 **Oracle** 이용 약관 및 파트너 이용 약관에 동의함 확인란을 선택합니다.

단계 **5** **Launch Instance(**인스턴스 실행**)**를 클릭합니다.

단계 **6** 인스턴스를 설명하는 **Name(**이름**)**(예: *Cisco-FMCv*)을 입력합니다.

단계 **7** **Change Shape(**셰이프 변경**)**를 클릭하고 CPU 수, RAM 크기, FMCv에 필요한 인터페이스 수를 포함하는 셰이프를 선택합니다(예: VM.Standard2.4 (OCI 컴퓨팅 셰이프, 1 페이지 참조)).

단계 **8** **Virtual Cloud Network(**가상 클라우드 네트워크**)** 드롭 다운에서 Management VCN (관리 VCN)을 선택합니다.

단계 **9** **Subnet(**서브넷**)** 드롭 다운에서 관리 서브넷이 자동으로 채워지지 않은 경우 선택합니다.

단계 **10** **Use Network Security Groups to Network Traffic(**트래픽을 제어하기 위해 네트워크 보안 그룹 사용**)**을 선택하고 관리 VCN에 대해 구성한 보안 그룹을 선택합니다.

단계 **11** **Assign a Public Ip Address(**공용 **IP** 주소 할당**)** 라디오 버튼을 클릭합니다.

단계 **12** **Add SSH keys(SSH** 키 추가**)**에서 **Paste Public Keys(**공개 키 붙여 넣기**)** 라디오 버튼을 클릭하고 SSH 키를 붙여 넣습니다.

Linux 기반 인스턴스는 비밀번호 대신 SSH 키 쌍을 사용하여 원격 사용자를 인증합니다. 키 쌍은 개인 키와 공개 키로 구성됩니다. 인스턴스를 생성할 때 개인 키를 컴퓨터에 보관하고 공개 키를 제공해야 합니다. 지침은 Linux 인스턴스에서 키 쌍 관리를 참조하십시오.

단계 **13** **Show Advanced Options(**고급 옵션 표시**)** 링크를 클릭하여 옵션을 확장합니다.

단계 **14** **Initialization Script(**초기화 스크립트**)**에서 **Paste Cloud-Init Script(**클라우드 초기화 스크립트**)** 라디오 버튼을 클릭하여 FMCv을 위한 day0 컨피그레이션을 제공합니다. day0 컨피그레이션은 FMCv의 첫 번째 부팅 중에 적용됩니다.

다음 예는 **Cloud-Init Script(Cloud-Init** 스크립트**)** 필드에서 복사하여 붙여넣을 수 있는 샘플 day0 컨피그레이션을 보여줍니다.

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

단계 **15** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

FMCv 인스턴스를 모니터링합니다. **Create(**생성**)** 버튼을 클릭하면 상태가 Provisionin (프로비저닝)으로 표시됩니다. 상태를 모니터링하는 것이 중요합니다. FMCv 부팅이 완료되었음을 나타내는 FMCv 인스턴스가 Provisioning(프로비저닝)에서 Running(실행 중) 상태로 전환되는지 확인합니다.

OCI에서 FMCv 인스턴스에 액세스

SSH(Secure Shell) 연결을 사용하여 실행중인 인스턴스에 연결할 수 있습니다.

- 대부분의 UNIX 스타일 시스템에는 기본적으로 SSH 클라이언트가 포함되어 있습니다.
- Windows 10 및 Windows Server 2017 시스템에는 Oracle Cloud Infrastructure에서 생성된 SSH 키를 사용하여 인스턴스를 생성한 경우 필요한 OpenSSH 클라이언트가 포함되어야 합니다.
- 다른 Windows 버전의 경우 http://www.putty.org에서 무료 SSH 클라이언트인 PuTTY를 다운로드할 수 있습니다.

사전 요건

인스턴스에 연결하려면 다음 정보가 필요합니다.

- 해당 인스턴스의 퍼블릭 IP 주소 콘솔의 Instance Details(인스턴스 세부 사항) 페이지에서 해당 주소를 가져올 수 있습니다. Navigation(탐색) 메뉴를 엽니다. **Core Infrastructure(**코어 인프라**)**에서 **Compute(**계산**)**로 이동하여 **Instances(**인스턴스**)**를 클릭합니다. 그런 다음 인스턴스를 선택합니다. 또는 Core Services API ListVnicAttachments 및 GetVnic 작업을 사용할 수 있습니다.
- 인스턴스의 사용자 이름 및 비밀번호입니다.
- 인스턴스를 시작할 때 사용한 SSH 키 쌍의 개인 키 부분에 대한 전체 경로입니다.

  키 쌍에 대한 자세한 내용은 Linux 인스턴스에서 키 쌍 관리를 참조하십시오.

참고 Day0 컨피그레이션을 추가하지 않을 경우 기본 자격 증명(admin/Admin123)을 사용하여 FMCv인스턴스에 로그인할 수 있습니다.

첫 번째 로그인 시도 시 비밀번호를 설정하라는 메시지가 표시됩니다.

PuTTY를 사용해서 FMCv 인스턴스 연결

PuTTY를 사용하여 Windows 시스템에서 FMCv 인스턴스에 연결하려면:

단계 1 PuTTY를 엽니다.

단계 2 **Category(**범주**)** 창에서 **Session(**세션**)**을 선택하고 다음을 입력합니다.

- 호스트 이름 또는 **IP** 주소**:**

  <username>@<public-ip-address>

  여기서 각 항목은 다음을 나타냅니다.

  <username>은 FMCv 인스턴스의 사용자 이름입니다.

  <public-ip-address>은 콘솔에서 검색한 인스턴스 공용 IP 주소입니다.

- 포트**:** 22
- 연결 유형**:** SSH

단계 3 **Category(**카테고리**)** 창에서 **Window(**창**)**를 확장한 다음 **Translation(**변환**)**을 선택합니다.

단계 4 **Remote character set(**원격 문자 집합**)** 드롭 다운 목록에서 **UTF-8**을 선택합니다.

Linux 기반 인스턴스의 기본 로캘 설정은 UTF-8이며, 이 설정이 동일한 로캘을 사용하도록 PuTTY를 구성합니다.

단계 5 **Category(**카테고리**)** 창에서 **Connection(**연결**)**, **SSH**를 차례로 확장한 다음 **Auth(**인증**)**를 클릭합니다.

단계 6 **Browse(**찾아보기**)**를 클릭한 다음 개인 키를 선택합니다.

단계 7 **Open(**열기**)**을 클릭하여 세션을 시작합니다.

인스턴스에 처음 연결하는 경우에는 서버의 호스트 키가 레지스트리에 캐시되지 않는다는 메시지가 표시될 수 있습니다. **Yes(**예**)**를 클릭하여 연결을 계속합니다.

SSH를 사용해서 FMCv 인스턴스 연결

Unix 스타일 시스템에서 인스턴스에 연결하려면 SSH를 사용하여 FMCv 인스턴스에 로그인합니다.

단계 1 다음 명령을 사용해서 파일 권한을 설정해서 본인만 파일을 읽을 수 있도록 합니다.

```
$ chmod 400 <private_key>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

단계 **2** 다음 SSH 명령을 사용해서 인스턴스에 액세스합니다.

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

<username>은 FMCv 인스턴스를 위한 사용자 이름입니다.

<public-ip-address>는 콘솔에서 가져온 인스턴스 IP 주소입니다.

OpenSSH를 사용해서 FMCv 인스턴스 연결

Windows 시스템에서 FMCv 인스턴스에 연결하려면 OpenSSH를 사용하여 인스턴스에 로그인합니다.

단계 **1** 이 키 쌍을 처음 사용하는 경우에는 파일 읽기만 가능하도록 파일 권한을 설정해야 합니다.

다음을 수행합니다.

a) Windows Explorer에서 개인 키 파일로 이동하여 파일을 마우스 오른쪽 버튼으로 클릭한 다음 **Properties(**속성**)**를 클릭합니다.
b) **Security(**보안**)** 탭에서 **Advanced(**고급**)**를 클릭합니다.
c) 소유자가 사용자 계정인지 확인하십시오.
d) **Disable Inheritance(**상속 비활성화**)**를 클릭한 다음 이 개체에 대해 상속된 권한을 명시적 권한으로 변환을 선택합니다.
e) 사용자 계정이 아닌 각 권한 항목을 선택하고 **Remove(**제거**)**를 클릭합니다.
f) 사용자 계정에 대한 액세스 권한이 모든 권한인지 확인합니다.
g) 변경 내용을 저장합니다.

단계 **2** 인스턴스에 연결하려면 Windows PowerShell을 열고 다음 명령을 실행합니다.

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

<username>은 FMCv 인스턴스를 위한 사용자 이름입니다.

<public-ip-address>는 콘솔에서 가져온 인스턴스 IP 주소입니다.