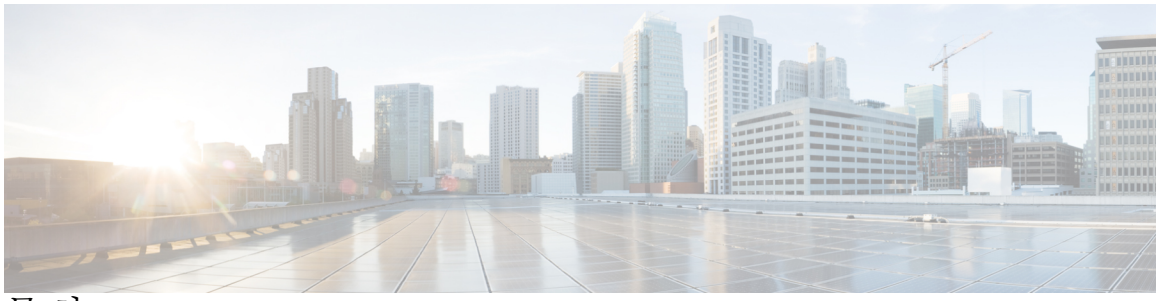
Cisco Firepower Management Center Virtual 시작 가이드

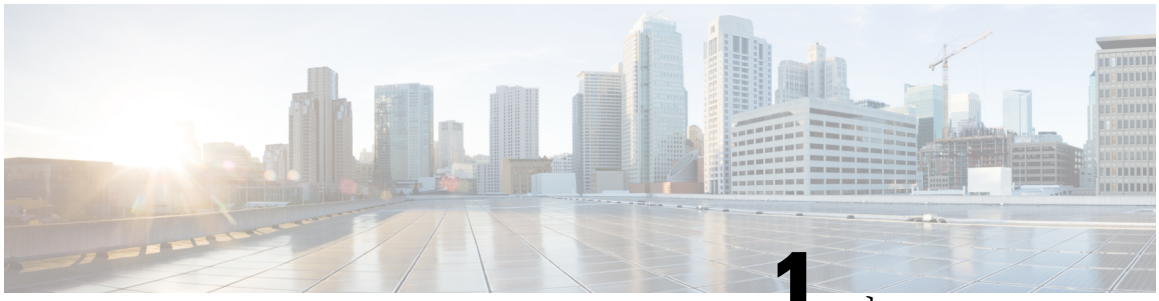
초판: 2015년 11월 10일

최종 변경: 2020년 12월 11일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

Cisco Firepower Management Center Virtual 어플라이언스 소개

Cisco FMCv(Firepower Management Center Virtual) 어플라이언스에서는 전체 방화벽 기능을 가상화된 환경으로 가져와 데이터 센터 트래픽과 다중 테넌트 환경을 보호합니다. Firepower Management Center Virtual은 물리적/가상 Firepower Threat Defense, Firepower NGIPS 및 FirePOWER 어플라이언스를 관리할 수 있습니다.

FMCv를 위한 플랫폼 및 지원

메모리 및 리소스 요구 사항

FMCv의 각 인스턴스가 최적의 성능을 발휘하도록 보장하려면 대상 플랫폼에 최소 리소스를(메모리 및 CPU 수, 디스크 공간) 할당해야 합니다.

중요 FMCv를 업그레이드할 때 최신 릴리스가 환경에 영향을 미치는지 여부에 대한 자세한 내용은 최신 Firepower 릴리스 노트를 참조하십시오. 최신 버전의 Firepower를 구축하려면 리소스를 늘려야 할 수 있습니다.

Firepower를 업그레이드할 때 Firepower 구축의 보안 기능 및 성능을 개선하는 데 도움이 되는 최신 기능 및 수정 사항을 추가합니다.

FMCv 업그레이드(6.6.0 이상)에 28GB RAM 필요

FMCv 플랫폼은 업그레이드 중에 새로운 메모리 검사를 도입했습니다. 가상 어플라이언스에 28GB 미만의 RAM을 할당하면 버전 6.6.0 이상으로의 FMCv 업그레이드가 실패합니다.

중요 기본 설정을 줄이지 않는 것이 좋습니다. 대부분의 FMCv 인스턴스의 경우 32GB RAM, FMCv 300의 경우 64GB가 필요합니다. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다.

이 메모리 검사의 결과로 지원되는 플랫폼에서 더 낮은 메모리 인스턴스를 지원할 수 없게 됩니다. 중요한 FMCv 업그레이드 정보는 가상 어플라이언스 성능 정보, 4 페이지의 내용을 참조하십시오.

FMCv 초기 설정(6.5.0 이상)

버전 6.5부터는 FMCv의 초기 설정 환경이 다음과 같이 개선되고 강화되었습니다.

- **DHCP on Management(**관리의 **DHCP)** - DHCP는 관리 인터페이스(eth0)에서 기본 모드로 활성화됩니다.

  FMCv 관리 인터페이스는 DHCP에서 할당한 IP4 주소를 수락하도록 사전 구성되어 있습니다. 시스템 관리자에게 문의해 DHCP가 FMCv에 할당하도록 구성된 IP 주소를 확인합니다. DHCP를 사용할 수 없는 상황이라면, FMC 관리 인터페이스는 IPv4 주소 192.168.45.45를 사용합니다.

- **Web interface URL(**웹 인터페이스 **URL)** - FMCv 웹 인터페이스의 기본 URL이 *https://<FMC-IP>:<port>/ui/login*으로 변경되었습니다.

- **Password reset(**비밀번호 재설정**)** - 시스템 보안 및 개인정보 보호를 위해 FMC에 처음 로그인하면 관리자 비밀번호를 변경해야 합니다. Change Password(비밀번호 변경) 마법사 화면이 표시되면 두 가지 옵션이 있습니다. **New Password(**새 비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 텍스트 상자에 새 비밀번호를 입력합니다. 비밀번호는 대화 상자에 나열된 기준을 준수해야 합니다.

- 네트워크 설정 - 이제 FMCv에 초기 설정을 완료하기 위한 설치 마법사가 포함되어 있습니다.
  - 정규화된 도메인 이름**(FQDN)** - 표시되는 기본값을 수락하거나 FQDN(syntax <hostname>.<domain>) 또는 호스트 이름을 입력합니다.
  - **IPV4** 연결을위한 부팅 프로토콜 - IP 주소 할당 방법으로 DHCP 또는 고정 / 수동을 선택합니다.
  - **DNS** 그룹 - FMCv의 기본 도메인 이름 서버 그룹은 Cisco Umbrella DNS입니다.
  - **NTP** 그룹 서버 - 기본 Network Time Protocol 그룹은 Sourcefire NTP 풀로 설정됩니다.

- **RAM** 요구 사항 - FMCv의 권장 RAM 크기는 32GB입니다.

- **FMCv-300 for VMware** - 최대 300개의 디바이스 관리를 지원하고 디스크 용량이 더 큰 VMware 플랫폼에서 새로운 크기의 FMCv 이미지를 사용할 수 있습니다.

지원되는 플랫폼

Cisco Firepower Management Center Virtual은 다음과 같은 플랫폼에서 구축할 수 있습니다.

- **VMware vSphere Hypervisor(ESXi)** - VMware ESXi에서 게스트 가상 머신으로 Firepower Management Center Virtual을 구축할 수 있습니다.
- **KVM(Kernel Virtualization Module)** - KVM 하이퍼바이저를 실행하는 Linux 서버에서 Firepower Management Center Virtual을 구축할 수 있습니다.
- **AWS(Amazon Web Services)** - AWS Cloud의 EC2 인스턴스에서 Firepower Management Center Virtual을 구축할 수 있습니다.
- **Microsoft Azure** - Azure Cloud에서 Firepower Management Center Virtual을 구축할 수 있습니다.

참고 고 가용성(HA) 컨피그레이션은 VMWare의 Firepower Management Center Virtual 구축에서만 지원됩니다. 고 가용성을 위한 시스템 요구 사항에 대한 자세한 내용은 *Firepower Management Center Configuration Guide*의 Firepower Management Center 고 가용성 정보를 참조하십시오.

하이퍼바이저 및 버전 지원

하이퍼바이저 및 버전 지원에 대한 내용은 Cisco Firepower 호환성을 참조하십시오.

Firepower Management Center Virtual 라이선스

Firepower Management Center Virtual 라이선스는 기능 라이선스가 아니라 플랫폼 라이선스입니다. 구매하는 가상 라이선스 버전에 따라 Firepower Management Center를 통해 관리할 수 있는 디바이스의 수가 결정됩니다. 예를 들어, 또는 2개의 디바이스, 10개의 디바이스, 25개의 디바이스 또는 300개의 디바이스를 관리할 수 있는 라이선스를 구매할 수 있습니다.

Firepower 기능 라이선스 정보

다양한 기능의 라이선스를 취득하여 조직에 가장 잘 맞는 Firepower System 구축을 생성할 수 있습니다. Firepower Management Center를 통해 이러한 기능 라이선스를 관리하고 디바이스에 할당할 수 있습니다.

참고 Firepower Management Center에서는 디바이스용 기능 라이선스를 관리하지만, Firepower Management Center를 사용하는 데는 기능 라이선스가 필요하지 않습니다.

Firepower 기능 라이선스는 디바이스 유형에 따라 달라집니다.

- 스마트 라이선스는 Firepower Threat Defense 및 Firepower Threat Defense Virtual 디바이스에 사용할 수 있습니다.
- 기본 라이선스는 7000 및 8000 Series, ASA FirePOWER 및 NGIPSv 디바이스에 사용할 수 있습니다.

기본 라이선스를 사용하는 디바이스를 기본 디바이스라고 할 때도 있습니다. 하나의 Firepower Management Center에서 기본 라이선스와 스마트 라이선스를 모두 관리할 수 있습니다.

"사용 권한" 기능 라이선스 외에도 여러 기능에 서비스 서브스크립션이 필요합니다. 사용 권한 라이선스는 만료되지 않지만 서비스 서브스크립션은 주기적으로 갱신해야 합니다.

각 플랫폼에서의 스마트 라이선스와 기본 라이선스를 비교한 자세한 내용은 Cisco Firepower System 기능 라이선스 문서를 참조하십시오.

스마트 라이선싱, 기본 라이선싱, 사용 권한 라이선스 및 서비스 서브스크립션에 대한 일반적인 질문에 대한 답변은 Firepower 라이선싱 문서에 대한 FAQ(자주 묻는 질문)를 참조하십시오.

가상 어플라이언스 성능 정보

가상 어플라이언스의 처리량과 처리 용량을 정확하게 예측하기란 불가능합니다. 다음을 포함한 여러 요소가 성능에 큰 영향을 미칩니다.

- 호스트의 메모리 양과 CPU 용량
- 호스트에서 실행되는 가상 머신의 총 개수
- 구축된 센싱 인터페이스의 수, 인터페이스 속도 및 네트워크 성능
- 각 가상 어플라이언스에 할당된 리소스의 양
- 호스트를 공유하는 다른 가상 어플라이언스의 활동 레벨
- 가상 디바이스에 적용된 정책의 복잡성

처리량이 만족스럽지 않을 경우 호스트를 공유하는 가상 어플라이언스에 할당된 리소스를 조정하십시오.

각각의 가상 어플라이언스를 만들 경우 호스트에 특정 양의 메모리, CPU, 하드 디스크 공간이 있어야 합니다. 기본 설정은 시스템 소프트웨어를 실행하는 데 필요한 최소 설정이므로 기본 설정을 줄이지 마십시오. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다.

FMCv 기본 및 최소 메모리 요구 사항

이제 모든 FMCv 구현에 동일한 RAM 요구 사항이 적용됩니다. 32GB 권장, 28GB 필수 (FMCv 300의 경우 64GB) 가상 어플라이언스에 28GB 미만을 할당하면 버전 6.6.0 이상으로의 업그레이드가 실패합니다. 업그레이드 후에는 메모리 할당량을 줄이면 상태 모니터에 경고가 표시됩니다.

이러한 새로운 메모리 요구 사항은 모든 가상 환경에서 균일한 요구 사항을 적용하고 성능을 개선하며 새로운 기능을 활용할 수 있도록 합니다. 기본 설정을 사용하는 것이 좋습니다. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다.

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 인스턴스를 계속 실행할 수 있습니다.

다음 표에는 메모리 부족 FMCv 구축의 업그레이드 전 요구 사항이 요약되어 있습니다.

표 *1:* 버전 *6.6.0* 이상 업그레이드를 위한 *FMCv* 메모리 요구 사항

플랫폼	사전 업그레이드 작업	세부정보
VMWare	최소 28GB / 32GB를 할당하는 것이 좋습니다.	먼저 가상 머신의 전원을 끕니다. 자세한 내용은 VMware 문서를 참조하십시오.
KVM	최소 28GB / 32GB를 할당하는 것이 좋습니다.	자세한 내용은 KVM 환경 설명서를 참조하십시오.
AWS	인스턴스 크기 조정: • c3.xlarge에서 c3.4xlarge로 • c3.2.xlarge에서 c3.4xlarge로 • c4.xlarge에서 c4.4xlarge로 • c4.2xlarge에서 c4.4xlarge로 또한 신규 구축을 위한 c5.4xlarge 인스턴스도 제공합니다.	크기를 조정하기 전에 인스턴스를 중지합니다. 이 작업을 수행하면 인스턴스 저장 볼륨의 데이터가 손실되므로 인스턴스 저장 기반 인스턴스를 먼저 마이그레이션하십시오. 또한 관리 인터페이스에 탄력적 IP 주소가 없는 경우 해당 공용 IP 주소가 사용됩니다. 자세한 내용은 Linux 인스턴스용 AWS 사용 설명서의 인스턴스 유형 변경에 대한 문서를 참조하십시오.
Azure	인스턴스 크기 조정: • Standard_D3_v2 에서 Standard_D4_v2로	Azure 포털 또는 PowerShell을 사용합니다. 크기를 조정하기 전에 인스턴스를 중지할 필요는 없지만 중지하면 크기가 더 표시될 수 있습니다. 크기를 조정하면 실행중인 가상 머신이 재시작됩니다. 지침은 Windows VM 크기 조정에 대한 Azure 설명서를 참조하십시오.

Firepower Management Center Virtual 구축 패키지 다운로드

Cisco.com에서 Firepower Management Center Virtual 구축 패키지를 다운로드할 수 있으며, 패치 및 핫픽스의 경우 Firepower Management Center 내에서 다운로드할 수 있습니다.

다음과 같이 Firepower Management Center Virtual 구축 패키지를 다운로드합니다.

단계 **1** Cisco 소프트웨어 다운로드 페이지로 이동합니다.

참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

단계 **2** **Browse all(**모두 찾아보기**)**을 클릭하여 Firepower Management Center Virtual 구축 패키지를 검색합니다.

단계 **3** **Security(**보안**)** > **Firewalls(**방화벽**)** > **Firewall Management(**방화벽 관리**)**를 선택하고 **Firepower Management Center Virtual Appliance(Firepower Management Center Virtual** 어플라이언스**)**를 선택합니다.

단계 **4** 사용 중인 *model(*모델*)* > **FireSIGHT System Software(FireSIGHT System** 소프트웨어**)** > *version(*버전*)*을 선택합니다.

다음 표에는 Cisco.com의 Firepower Management Center Virtual 소프트웨어에 대한 정보와 명명 규칙이 나와 있습니다.

모델	패키지 유형	패키지 이름
Firepower Management Center Virtual	Firepower 소프트웨어 설치: VMware	Cisco_Firepower_Management_Center_Virtual_VMware-*version*.**tar.gz**
	Firepower 소프트웨어 설치: KVM	Cisco_Firepower_Management_Center_Virtual-*version*.**qcow2**
	Firepower 소프트웨어 설치: AWS	클라우드 서비스에 로그인하여 Marketplace에서 구축합니다.
	Firepower 소프트웨어 설치: Azure	클라우드 서비스에 로그인하여 Marketplace에서 구축합니다.

단계 **5** 구축 패키지를 찾아 서버 또는 관리 컴퓨터에 다운로드합니다.

이름이 비슷한 패키지가 많으므로 정확한 패키지를 다운로드해야 합니다.

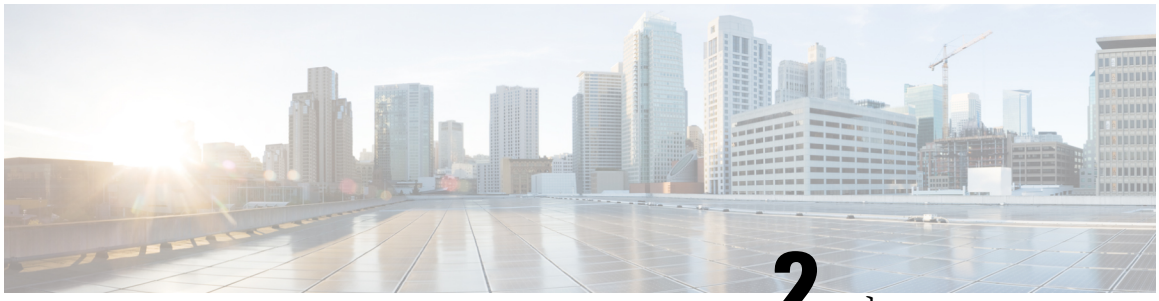
Cisco 지원 및 다운로드 사이트에서 바로 다운로드합니다. 이메일을 통해 구축 패키지를 전송하는 경우, 패키지가 손상될 수 있습니다.

다음에 수행할 작업

자신의 구축 플랫폼에 해당하는 장을 참조하십시오.

- VMware ESXi에서 게스트 가상 머신으로 Firepower Management Center Virtual을 구축하려면 VMware를 사용하여 Firepower Management Center Virtual 구축, 9 페이지의 내용을 참조하십시오.
- KVM 하이퍼바이저를 실행하는 Linux 서버에서 Firepower Management Center Virtual을 구축하려면 KVM을 사용하여 Firepower Management Center Virtual 구축, 23 페이지의 내용을 참조하십시오.

- AWS에서 Firepower Management Center Virtual을 구축하려면 AWS Cloud에 Firepower Management Center Virtual 구축, 35 페이지의 내용을 참조하십시오.
- Azure에서 Firepower Management Center Virtual을 구축하려면 Firepower Management Center Virtual On the Microsoft Azure Cloud 구축, 47 페이지의 내용을 참조하십시오.



2 장

VMware를 사용하여 Firepower Management Center Virtual 구축

VMware를 사용하여 Firepower Management Center Virtual(FMCv)을 구축할 수 있습니다.

Firepower Management Center Virtual에 대한 VMware 기능 지원

다음 표에는 FMCv에 지원되는 VMware 기능이 나와 있습니다.

표 *2: FMCv*에 대한 *VMware* 기능 지원

기능	설명	지원(예/아니요)	코멘트
Cold Clone	복제하는 동안 VM의 전원이 꺼집니다.	아니오	–
Hot add	추가하는 동안 VM이 실행됩니다.	아니오	–
Hot clone	복제하는 동안 VM이 실행됩니다.	아니오	–
Hot removal	제거하는 동안 VM이 실행됩니다.	아니오	–

기능	설명	지원(예/아니요)	코멘트
스냅샷	VM이 몇 초간 중지됩니다.	아니요	FMC와 매니지드 디바이스가 동기화되지 않는 상황이 발생할 수 있습니다. 스냅샷 지원, 15 페이지의 내용을 참조하십시오. .
일시 중지 및 재개	VM이 일시 중지되었다가 재개됩니다.	예	–
vCloud Director	VM의 자동 구축을 허용합니다.	아니오	–
VM 마이그레이션	마이그레이션하는 동안 VM의 전원이 꺼집니다.	예	–
vMotion	VM의 라이브 마이그레이션에 사용됩니다.	예	공유 스토리지를 사용합니다. vMotion 지원, 15 페이지을 참조하십시오.
VMware FT	VM의 HA에 사용됩니다.	아니오	–
VMware HA	ESXi 및 서버 장애에 사용됩니다.	예	–
VM 하트비트를 지원하는 VMware HA	VM 장애에 사용됩니다.	아니오	–
VMware vSphere 독립 실행형 Windows 클라이언트	VM을 구축하는 데 사용됩니다.	예	–
VMware vSphere Web Client	VM을 구축하는 데 사용됩니다.	예	–

호스트 시스템 요구 사항

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 기본 설정을 줄이지 않는 것이 좋습니다. 대부분 FMCv 인스턴스의 경우 32GB RAM, FMCv 300의 경우 64GB가 필요합니다. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다.

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

메모리 및 리소스 요구 사항

VMware ESX 및 ESXi 하이퍼바이저에서 호스팅되는 VMware vSphere 프로비저닝을 사용하여 Firepower Management Center Virtual을 구축할 수 있습니다. 하이퍼바이저 호환성에 대한 내용은 Cisco Firepower 호환성 가이드를 참조하십시오.

중요 FMCv를 업그레이드할 때 최신 릴리스가 환경에 영향을 미치는지에 대한 자세한 내용은 최신 Firepower 릴리스 노트를 확인하십시오. 최신 버전의 Firepower를 구축하려면 리소스를 늘려야 할 수 있습니다.

Firepower를 업그레이드할 때 Firepower 구축의 보안 기능 및 성능을 개선하는 데 도움이 되는 최신 기능 및 수정 사항을 추가합니다.

FMCv 구축에 사용되는 특정 하드웨어는 구축된 인스턴스 수 및 사용 요구 사항에 따라 달라질 수 있습니다. 생성하는 각 가상 어플라이언스는 호스트 머신에서 최소 리소스 할당(메모리, CPU 수 및 디스크 공간)을 필요로 합니다.

다음 표에는 FMCv 어플라이언스의 권고 및 기본 설정이 나와 있습니다.

중요 FMCv의 성능을 최적화하려면 충분한 메모리를 할당해야 합니다. FMCv의 메모리가 32GB 미만인 경우 시스템에 정책 구축 문제가 발생할 수 있습니다. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다. 기본 설정은 시스템 소프트웨어를 실행하는 데 필요한 최소 설정이므로 기본 설정을 줄이지 마십시오.

표 ***3: FMCv*** 기본 가상 어플라이언스 설정

설정	최소 필수 / 기본값	설정의 조정 가능 여부
메모리	28GB/32GB	제한 사항 있음 중요 FMCv 플랫폼은 업그레이드 중에 새로운 메모리 검사를 도입했습니다. 가상 어플라이언스에 28GB 미만의 RAM을 할당하면 버전 6.6.0 이상으로의 FMCv 업그레이드가 실패합니다.

설정	최소 필수 / 기본값	설정의 조정 가능 여부
가상 CPU	8 / 4	예, 최대 8개
하드 디스크 프로비저닝 크기	250 GB	아니요, 디스크 형식 선택 사항을 기준으로 함

표 ***4: FMCv300*** 기본 가상 어플라이언스 설정

설정	기본	설정의 조정 가능 여부
메모리	64GB	Yes(예)
가상 CPU	32	아니요
하드 디스크 프로비저닝 크기	2.2TB	아니요, 디스크 형식 선택 사항을 기준으로 함

VMware vCenter Server 및 ESXi 인스턴스를 실행하는 시스템은 특정 하드웨어 및 운영 체제 요구 사항을 충족해야 합니다. 지원되는 플랫폼의 목록을 보려면 VMware 온라인 호환성 가이드를 참조하십시오.

가상화 기술에 대한 지원

ESXi 호스트 역할을 하는 컴퓨터는 다음과 같은 요구 사항을 충족해야 합니다.

- Intel® VT(Virtualization Technology)든 AMD-V™(AMD Virtualization™) 기술이든 가상화 지원을 제공하는 64비트 CPU가 있어야 합니다.
- BIOS 설정에서 가상화를 활성화해야 합니다.

참고 Intel 및 AMD에서는 모두 CPU를 식별하고 기능을 결정하는 데 도움이 되는 온라인 프로세서 식별 유틸리티를 제공합니다. VT를 지원하는 CPU를 포함하는 여러 서버에서는 기본적으로 VT가 비활성화 상태일 수 있으므로 VT를 수동으로 활성화해야 합니다. 시스템에서 VT 지원을 활성화하는 방법에 대한 지침은 제조업체의 설명서를 참조하십시오.

- CPU가 VT를 지원하지만 이 옵션이 BIOS에 표시되지 않는 경우, 벤더에 문의하여 VT 지원을 활성화할 수 있게 해주는 BIOS 버전을 요청하십시오.
- 가상 디바이스를 호스팅하려면 컴퓨터에 Intel e1000 드라이버(예: PRO 1000MT 이중 포트 서버 어댑터 또는 PRO 1000GT 데스크톱 어댑터)와 호환되는 네트워크 인터페이스가 있어야 합니다.

CPU 지원 확인

Linux 명령줄을 사용하여 CPU 하드웨어에 대한 정보를 얻을 수 있습니다. 예를 들어, **/proc/cpuinfo** 파일에는 개별 CPU 코어에 대한 상세정보가 포함되어 있습니다. 해당 콘텐츠를 **less** 또는 **cat**과 함께 출력합니다.

다음 값에 대한 플래그 섹션을 확인할 수 있습니다.

- vmx — Intel VT 확장 프로그램
- svm — AMD-V 확장 프로그램

다음과 같은 명령을 실행하여 파일에 이러한 값이 있는지 빠르게 확인하려면 **grep**를 사용하십시오.

```
egrep "vmx|svm" /proc/cpuinfo
```

시스템에서 VT를 지원하는 경우, 플래그 목록에서 *vmx* 또는 *svm*을 확인할 수 있어야 합니다.

FMCv 및 VMware에 대한 지침 및 제한 사항

OVF 파일 지침

가상 어플라이언스는 OVF(Open Virtual Format) 패키징을 사용합니다. VI(가상 인프라) 또는 ESXi OVF 템플릿을 사용하여 가상 어플라이언스를 구축합니다. OVF 파일은 다음과 같은 구축 대상에 따라 선택합니다.

- vCenter에서의 구축 - Cisco_Firepower_Management_Center_Virtual_VMware-**VI**-*X.X.X-xxx*.ovf
- ESXi(vCenter 없음)에서의 구축 - Cisco_Firepower_Management_Center_Virtual_VMware-**ESXi**-*X.X.X-xxx*.ovf

여기서 *X.X.X-xxx*는 구축하려는 Firepower System 소프트웨어의 버전 및 빌드 번호입니다. 확인

- VI OVF 템플릿을 사용하여 구축할 경우, 설치 프로세스에서 FMCv 어플라이언스의 전체 초기 설정을 수행할 수 있습니다. 다음을 지정할 수 있습니다.
  - 관리자 계정의 새 비밀번호
  - 어플라이언스가 관리 네트워크에서 통신하도록 허용하는 네트워크 설정

  참고 VMware vCenter를 사용하여 이 가상 어플라이언스를 관리해야 합니다.
- ESXi OVF 템플릿을 사용하여 구축하는 경우 설치 후 Firepower System의 필수 설정을 구성해야 합니다. 이 가상 어플라이언스를 VMware vCenter를 사용하여 관리하거나 독립형 어플라이언스로 사용할 수 있습니다.

OVF 템플릿을 구축할 때 다음 정보를 제공합니다.

표 *5: VMware OFV* 템플릿 설정

설정	ESXi 또는 VI	조치
OVF 템플릿 가져오기/구축	모두	Cisco.com에서 다운로드한 OVF 템플릿을 찾습니다.
OVF 템플릿 세부 정보	모두	설치할 어플라이언스(FMCv) 및 구축 옵션(VI 또는 ESXi)을 확인합니다.
EULA 수락	VI만	OVF 템플릿에 포함된 라이선스 약관을 수락하려면 동의합니다.
이름 및 위치	모두	가상 어플라이언스에 고유하고 의미 있는 이름을 입력하고 어플라이언스의 인벤토리 위치를 선택합니다.
호스트 / 클러스터	모두	가상 어플라이언스를 구축할 호스트 또는 클러스터를 선택합니다.
리소스 풀	모두	컴퓨팅 리소스를 의미 있는 계층 구조로 설정하는 방식으로 호스트 또는 클러스터 내에서 컴퓨팅 리소스를 관리합니다. 가상 머신 및 하위 리소스 풀은 상위 리소스 풀의 리소스를 공유합니다.
스토리지	모두	가상 머신과 연결된 모든 파일을 저장할 데이터 저장소를 선택합니다.
디스크 형식	모두	가상 디스크를 저장할 형식(thick provision lazy zeroed, thick provision eager zeroed 또는 thin provision)을 선택합니다.
네트워크 매핑	모두	가상 어플라이언스의 관리 인터페이스를 선택합니다.
속성	VI만	가상 머신 초기 컨피그레이션 설정을 맞춤화합니다.

시간 및 시간 동기화

FMCv 및 관리되는 디바이스에서 시스템 시간을 동기화하려면 NTP(Network Time Protocol) 서버를 사용합니다. 일반적으로 FMCv 초기 컨피그레이션 중에 NTP 서버를 지정합니다. Firepower Management Center Virtual 초기 설정, 69 페이지에서 기본 NTP 서버에 대한 정보를 참조하십시오.

FMCv와 매니지드 디바이스에서 시스템 시간을 동기하하는 작업은 Firepower System의 성공적인 작업을 위해 반드시 필요합니다. VMware ESXi 서버에서의 FMCv의 NTP 설정과 일치하도록 NTP를 구성할 때 시간 동기화를 보장하기 위해 추가 단계를 수행할 수 있습니다.

vSphere Client를 사용하여 ESXi 호스트에서 NTP를 구성할 수 있습니다. 구체적인 지침은 VMware documentation를 참조하십시오. 또한 VMware KB 2012069에서는 vSphere Client를 사용하여 ESX / ESXi 호스트에서 NTP를 구성하는 방법을 설명합니다.

vMotion 지원

vMotion을 사용하려는 경우 공유 스토리지만 사용하는 것이 좋습니다. 호스트 클러스터가 있는 경우 구축하는 동안 특정 호스트에 로컬로 스토리지를 프로비저닝하거나 공유 호스트에 스토리지를 프로비저닝할 수 있습니다. 그러나 FMCv에서 다른 호스트에 대한 vMotion을 실행하려고 하는 경우, 로컬 스토리지를 사용하면 오류가 발생합니다.

스냅샷 지원

VMware 스냅샷은 지정된 시점의 가상 시스템 디스크 파일(VMDK)의 복사본입니다. 스냅샷은 가상 디스크에 대한 변경 로그를 제공하며, 장애 또는 시스템 오류가 발생하는 특정 시점으로 VM을 복원하는 데 사용할 수 있습니다. 스냅샷만으로는 백업을 제공하지 않으므로 백업으로 사용할 수 없습니다.

컨피그레이션 백업이 필요한 경우 Firepower Management Center(**System(**시스템**)** > **Tools(**도구**)** > **Backup/Restore(**백업/복원**)**)의 백업 및 복원 기능을 사용하십시오

ESXi의 VMware 스냅샷 기능은 VM 스토리지 용량을 소모하고 FMC 가상 어플라이언스의 성능에 영향을 줄 수 있습니다. 다음 VMware Knowledge Base 문서를 참조해 주십시오.

- vSphere 환경에서 스냅샷을 사용하기 위한 모범 사례(VMware KB 1025279).
- ESXi의 VM 스냅샷 이해(VMware KB 1015180)

HA(High Availability) 지원

VMware ESXi의 두 FMCv 가상 어플라이언스 간에 고 가용성(HA)을 설정할 수 있습니다.

- FMCv HA는 FMCv 모델과 FMCv 300 모두에서 지원됩니다.
- 고가용성 설정의 두 FMCv는 동일한 모델이어야 합니다. FMCv를 FMCv 300과 페어링할 수 없습니다.
- FMCv HA를 설정하려면 FMCv가 HA 컨피그레이션에서 관리하는 각 FTD 디바이스에 대해 추가 MCv(Firepower Management Center Virtual) 라이선스 권한이 필요합니다. 그러나 각 FTD 디바이스에 필요한 FTD 기능 라이선스 권한은 FMCv HA 컨피그레이션에 관계없이 변경되지 않습니다. 라이선싱에 대한 지침은 Firepower Management Center Configuration Guide의 고 가용성 쌍의 *FTD* 디바이스에 대한 라이선스 요건을 참조하십시오.
- FMCv HA 쌍을 분리하는 경우 추가 MCv(Firepower Management Center Virtual) 라이선스 권한이 릴리스되며 각 FTD 디바이스에 대해 하나의 권한만 있으면 됩니다.

고 가용성에 대한 지침은 *Firepower Management Center Configuration Guide*의 Firepower Management Center 고 가용성 설정을 참조하십시오.

INIT 리스포닝 오류 메시지 증상

ESXi 6 및 ESXi 6.5에서 실행 중인 FMCv 콘솔에 다음 오류 메시지가 표시될 수 있습니다.

```
"INIT: Id "fmcv" respawning too fast: disabled for 5 minutes"
```

해결 방법 — 디바이스 전원이 꺼져 있는 동안 시리얼 포트를 추가하려면 vSphere에서 가상 머신 설정을 수정합니다.

1. 가상 머신을 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings(**설정 수정**)**를 선택합니다.
2. Virtual Hardware(가상 하드웨어) 탭의 **New device(**새 디바이스**)** 드롭다운 메뉴에서 **Serial Port(**시리얼 포트**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

   시리얼 포트는 가상 디바이스 목록의 하단에 나타납니다.
3. **Virtual Hardware(**가상 하드웨어**)** 탭에서 **Serial port(**시리얼 포트**)**를 확장하고 연결 유형에서 **Use physical serial port(**물리적 시리얼 포트 사용**)**를 선택합니다.
4. **Connect at power on(**전원을 켤 때 연결**)** 확인란의 선택을 취소합니다.

   OK(확인**)**를 클릭하여 설정을 저장합니다.

제한 사항

다음은 VMware를 구축할 때의 제한 사항입니다.

- FMCv 어플라이언스에는 시리얼 번호가 없습니다. **System(**시스템**)** > **Configuration(**구성**)** 페이지에는 가상 플랫폼에 따라 **None(**없음**)** 또는 **Not Specified(**지정되지 않음**)** 중 하나가 표시됩니다.
- 가상 머신 복제는 지원되지 않습니다.
- 스냅샷을 사용한 가상 머신 복원은 지원되지 않습니다.
- VMware Workstation, Player, Server 및 Fusion은 OVF 패키징을 인식하지 않으며 지원되지 않습니다.

설치 패키지 다운로드

Cisco에서는 지원 사이트의 VMware ESX 및 ESXi 호스트 환경을 위해 패키지형 가상 어플라이언스를 압축된 아카이브(.tar.gz) 파일로 제공합니다. Cisco 가상 어플라이언스는 가상 하드웨어 버전 7을 사용하여 가상 머신으로 패키징됩니다. 각 아카이브에는 ESXi 또는 VI 구축 대상에 대한 매니페스트 파일 및 OVF 템플릿과 가상 머신 디스크 형식(vmdk) 파일이 포함되어 있습니다.

Cisco.com에서 Firepower Management Center Virtual 설치 패키지를 다운로드하고 로컬 디스크에 저장합니다. 항상 사용 가능한 최신 패키지를 사용하는 것이 좋습니다. 가상 어플라이언스 패키지는 보통 주 버전의 시스템 소프트웨어와 연결되어 있습니다(예: 6.1 또는 6.2).

단계 **1** Cisco 소프트웨어 다운로드 페이지로 이동합니다.

참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

단계 **2** **Browse all(**모두 찾아보기**)**을 클릭하여 Firepower Management Center Virtual 구축 패키지를 검색합니다.

단계 **3** **Security(**보안**) > Firewalls(**방화벽**) > Firewall Management(**방화벽 관리**)**를 선택하고 **Firepower Management Center Virtual Appliance(Firepower Management Center Virtual** 어플라이언스**)**를 선택합니다.

단계 **4** 다음의 명명 규칙을 사용하여 Firepower Management Center Virtual 어플라이언스용으로 다운로드할 VMware 설치 패키지를 찾습니다.

Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx.tar.gz

여기서 *X.X.X-xxx*는 다운로드할 설치 패키지의 버전 및 빌드 번호입니다.

단계 **5** 다운로드할 설치 패키지를 클릭합니다.

참고 사용자가 지원 사이트에 로그인되어 있는 동안 가상 어플라이언스를 주 버전으로 설치한 후 시스템 소프트웨어를 업데이트할 수 있도록 사용 가능한 모든 가상 어플라이언스 업데이트를 다운로드하는 것이 좋습니다. 또한 항상 어플라이언스에서 지원하는 최신 버전의 시스템 소프트웨어를 실행해야 합니다. Cisco Firepower Management Center Virtual의 경우 새로운 침입 규칙 및 VDB(Vulnerability Database) 업데이트도 모두 다운로드해야 합니다.

단계 **6** vSphere Client를 실행하는 서버 또는 워크스테이션에 액세스할 수 있는 위치로 설치 패키지를 복사합니다.

주의 아카이브 파일을 이메일로 전송하지 마십시오. 파일이 손상될 수 있습니다.

단계 **7** 선호하는 툴을 사용하여 설치 패키지 아카이브 파일의 압축을 풀고 설치 파일을 추출합니다. Cisco Firepower Management Center Virtual의 경우에는 다음과 같습니다.

- Cisco_Firepower_Management_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
- Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf
- Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf
- Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
- Cisco_Firepower_Management_Center_Virtual_VMware-VI-X.X.X-xxx.mf

여기서 *X.X.X-xxx*는 다운로드하려는 아카이브 파일의 버전 및 빌드 번호입니다.

참고 모든 파일을 동일한 디렉토리에 보관합니다.

다음에 수행할 작업

- 구축 대상(VI 또는 ESXi)을 결정하고 VMware vSphere를 사용하여 구축, 18 페이지 작업을 계속 진행합니다.

VMware vSphere를 사용하여 구축

VMware vSphere vCenter, vSphere Client, vSphere Web Client 또는 ESXi 하이퍼바이저(독립형 ESXi 구축의 경우)를 사용하여 Firepower Management Center Virtual을 구축할 수 있습니다. VI 또는 ESXi OVF 템플릿을 사용하여 구축할 수 있습니다.

- VI OVF 템플릿을 사용하여 구축하는 경우 VMware vCenter로 어플라이언스를 관리해야 합니다.
- ESXi OVF 템플릿을 사용하여 구축하는 경우 VMware vCenter로 어플라이언스를 관리하거나 독립형 ESXi 호스트에 어플라이언스를 구축할 수 있습니다. 둘 중 어떤 경우든지 설치 후 Firepower System의 필수 설정을 구성해야 합니다.

마법사의 각 페이지에서 설정을 지정한 다음 **Next**를 클릭하여 계속합니다. 사용자의 편의를 위해, 절차를 완료하기 전에 마법사의 마지막 페이지에서 설정을 확인할 수 있습니다.

단계 **1** vSphere Client에서 **File(**파일**)** > **Deploy OVF Template(OVF** 템플릿 구축**)**을 선택합니다.

단계 **2** 드롭다운 목록에서 Firepower Management Center Virtual을 구축하는 데 사용할 OVF 템플릿을 선택합니다.

- Cisco_Firepower_Management_Center_Virtual_VMware-VI-*X.X.X-xxx*.ovf
- Cisco_Firepower_Management_Center_Virtual_VMware-ESXi-*X.X.X-xxx*.ovf

여기서 *X.X.X-xxx*는 Cisco.com에서 다운로드한 설치 패키지의 버전 및 빌드 번호입니다.

단계 **3** **OVF Template Details(OVF** 템플릿 상세정보**)** 페이지를 확인하고 **Next(**다음**)**를 클릭합니다.

단계 **4** 라이선스 계약서가 OVF 템플릿(VI 템플릿 전용)과 함께 패키징된 경우, **End User License Agreement(**엔드 유저 라이선스 계약**)** 페이지가 나타납니다. 동의하여 라이선스 약관을 수락하고 **Next(**다음**)**를 클릭합니다.

단계 **5** (선택 사항) 이름을 수정하고 Firepower Management Center Virtual을 저장할 인벤토리 내의 폴더 위치를 선택한 후, **Next(**다음**)**를 클릭합니다.

참고 vSphere Client가 ESXi 호스트에 직접 연결된 경우, 폴더 위치를 선택하는 옵션이 나타나지 않습니다.

단계 **6** Firepower Management Center Virtual을 구축할 클러스터 또는 호스트를 선택하고 Next(다음)를 클릭합니다.

단계 **7** Firepower Management Center Virtual을 실행할 리소스 풀로 이동하여 해당 리소스 풀을 선택하고 **Next(**다음**)**를 클릭합니다.

이 페이지는 클러스터에 리소스 풀이 포함되어 있는 경우에만 나타납니다.

단계 **8** 가상 머신 파일을 저장할 스토리지 위치를 선택하고 **Next(**다음**)**를 클릭합니다.

이 페이지에서 이미 대상 클러스터 또는 호스트에 구성되어 있는 데이터 저장소에서 선택합니다. 가상 머신 컨피그레이션 파일 및 가상 디스크 파일은 해당 데이터 저장소에 저장되어 있습니다. 가상 머신과 모든 가상 디스크 파일을 수용할 만큼 큰 데이터 저장소를 선택합니다.

단계 **9** 가상 머신 가상 디스크를 저장할 디스크 형식을 선택하고 **Next(**다음**)**를 클릭합니다.

Thick Provisioned(씩 프로비저닝**)**를 선택할 경우, 모든 스토리지가 즉시 할당됩니다. **Thin Provisioned(**씬 프로비저닝**)**를 선택하면 데이터가 가상 디스크에 작성될 때 요청에 따라 스토리지가 할당됩니다.

단계 **10** Firepower Management Center Virtual 관리 인터페이스를 Network Mapping(네트워크 매핑) 화면의 VMware 네트워크와 연결합니다.

네트워크 매핑을 설정하려면 인프라에서 **Destination Networks(**대상 네트워크**)** 열을 마우스 오른쪽 버튼으로 클릭하여 네트워크를 선택하고 **Next(**다음**)**를 클릭합니다.

단계 **11** 사용자가 구성 가능한 속성이 OVF 템플릿(VI 템플릿 전용)과 함께 패키징된 경우, 구성 가능한 속성을 설정하고 **Next(**다음**)**를 클릭합니다.

단계 **12** **Ready to Complete(**완료 준비**)** 창에서 설정을 검토하고 확인합니다.

단계 **13** (선택 사항) **Power on after deployment(**구축 후 전원 켜기**)** 옵션을 선택하여 Firepower Management Center Virtual의 전원을 켠 다음, **Finish(**마침**)**를 클릭합니다.

참고: 구축 후 전원이 켜지지 않도록 선택하는 경우 나중에 VMware 콘솔에서 전원이 켜지도록 설정을 바꿀 수 있습니다. 가상 어플라이언스 초기화를 참조하십시오.

단계 **14** 설치가 완료되면 상태 창을 닫습니다.

단계 **15** 마법사를 완료하고 나면 vSphere Web Client에서 VM을 처리합니다. **Recent Tasks(**최근 작업**)** 창의 **Global Information(**전체 정보**)** 영역에서 "Initialize OVF deployment"(OVF 구축 초기화) 상태를 확인할 수 있습니다.

작업이 완료되면 Deploy OVF Template(OVF 템플릿 구축) 완료 상태가 표시됩니다.

그런 다음 인벤토리의 지정된 데이터 센터 아래에 Cisco Firepower Management Center Virtual 인스턴스가 표시됩니다. 새 VM을 부팅하는 데 최대 30분이 소요될 수 있습니다.

참고 Firepower Management Center Virtual을 Cisco Licensing Authority에 등록하려면 Firepower Management Center에 인터넷 액세스가 필요합니다. 구축 후 인터넷 액세스 및 성공적인 라이선스 등록을 위해 추가 컨피그레이션이 필요할 수 있습니다.

다음에 수행할 작업

- 가상 어플라이언스의 하드웨어 및 메모리 설정이 구축 요구 사항을 충족하는지 확인합니다. 가상 머신 속성 확인, 19 페이지의 내용을 참조하십시오.

가상 머신 속성 확인

VMware Virtual Machine Properties(VMware Virtual Machine 속성) 대화 상자를 사용하여 선택한 가상 머신에 대한 호스트 리소스 할당을 조정합니다. 이 탭에서 CPU, 메모리, 디스크 및 고급 CPU 리소스를 변경할 수 있습니다. 또한 가상 머신에 대한 전원 켜기 연결 설정, MAC 주소, 가상 이더넷 어댑터 컨피그레이션의 네트워크 연결을 변경할 수 있습니다.

단계 **1** 새 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음, 콘텍스트 메뉴에서 **Edit Settings(**설정 수정**)**를 선택하거나 기본 창의 **Getting Started(**시작하기**)** 탭에서 **Edit virtual machine settings(**가상 머신 설정 수정**)**를 클릭합니다.

단계 **2** **Memory(**메모리**)**, **CPU** 및 **Hard disk 1(**하드 디스크 **1)** 설정이 4페이지의 기본 가상 어플라이언스 설정에 설명된 대로 기본값 미만으로 설정되지 않았는지 확인합니다.

어플라이언스의 메모리 설정 및 가상 CPU 수가 창 왼쪽에 나열됩니다. 하드 디스크의 **Provisioned Size**를 보려면 **Hard disk 1**을 클릭합니다.

단계 **3** 선택적으로, 창 왼쪽에서 해당 설정을 클릭하여 메모리 및 가상 CPU의 수를 늘린 다음 창 오른쪽에서 변경 사항을 적용합니다.

단계 **4** **Network adapter 1** 설정이 다음과 같은지 확인하고, 필요한 경우 변경합니다.

a) **Device Status(**장치 상태**)** 아래에서 **Connect at power on(**전원이 켜진 상태에서 연결**)** 확인란을 활성화합니다.

b) **MAC Address(MAC** 주소**)** 아래에서 가상 어플라이언스 관리 인터페이스의 MAC 주소를 수동으로 설정합니다.

MAC 주소가 변경되거나 동적 풀의 다른 시스템과 충돌하지 않도록 MAC 주소를 가상 어플라이언스에 수동으로 할당합니다.

또한, 가상 Cisco Firepower Management Center의 경우 MAC 주소를 수동으로 설정하면 어플라이언스를 이미지로 다시 설치해야 할 경우 Cisco에서 라이선스를 다시 요청하지 않아도 됩니다.

c) **Network Connection(**네트워크 연결**)** 아래에서 **Network label(**네트워크 레이블**)**을 가상 어플라이언스의 관리 네트워크 이름으로 설정합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 가상 어플라이언스를 초기화합니다. 자세한 내용은 가상 어플라이언스 전원 켜기 및 초기화, 20 페이지를 참고하십시오.
- (선택 사항) 어플라이언스의 전원을 켜기 전에 추가 관리 인터페이스를 생성할 수 있습니다. 자세한 내용은 *VMware*용 *Cisco Firepower NGIPSv* 빠른 시작 가이드를 참조하십시오.

가상 어플라이언스 전원 켜기 및 초기화

가상 어플라이언스의 구축을 완료한 후, 처음으로 가상 어플라언스의 전원을 켜면 자동으로 초기화가 시작됩니다.

⚠

주의 시작 시간은 서버 리소스 가용성을 포함한 여러 요소에 따라 달라집니다. 초기화가 완료될 때까지 최대 40분이 소요될 수 있습니다. 초기화를 중단하지 마십시오. 초기화를 중단하면 어플라이언스를 삭제하고 다시 시작해야 할 수 있습니다.

단계 **1** 어플라이언스의 전원을 켭니다.

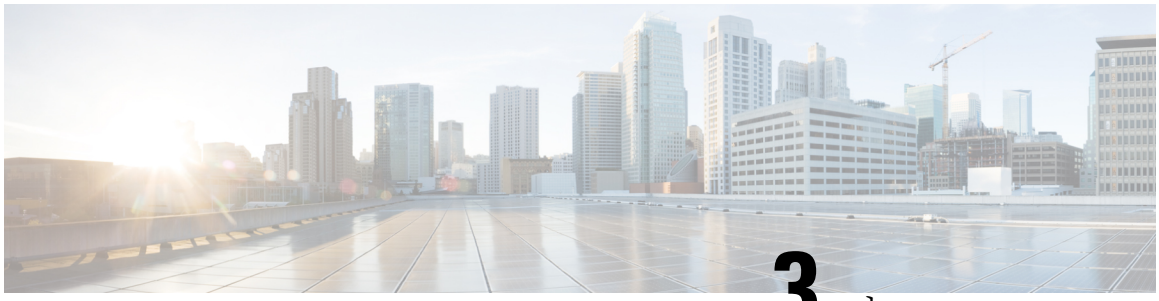
vSphere Client에 있는 인벤토리 목록에서 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음, 콘텍스트 메뉴에서 **Power(**전원**)** > **Power On(**전원 켜기**)**을 선택합니다.

단계 **2** VMware 콘솔 탭에서 초기화를 모니터링합니다.

다음에 수행할 작업

FMCv를 구축한 후, 새로운 어플라이언스가 신뢰할 수 있는 관리 네트워크와 통신하도록 구성하려면 설정 프로세스를 완료해야 합니다. VMware에서 ESXi OVF 템플릿을 사용하여 구축하는 경우 FMCv 설정은 2단계 프로세스로 진행됩니다.

- FMCv의 초기 설정을 완료하려면 Firepower Management Center Virtual 초기 설정, 69 페이지의 내용을 참조하십시오.
- FMCv 구축에서 필요한 다음 단계의 개요는 Firepower Management Center Virtual 초기 관리 및 구성, 77 페이지의 내용을 참조하십시오.



3 장

KVM을 사용하여 Firepower Management Center Virtual 구축

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

KVM을 사용한 구축 정보

KVM은 가상화 확장 프로그램(예: Intel VT)이 포함된 x86 하드웨어의 Linux용 전체 가상화 솔루션입니다. KVM은 로드 가능한 커널 모듈인 kvm.ko로 구성되어 있으며, 코어 가상화 인프라 및 kvm-intel.ko와 같은 프로세서별 모듈을 제공합니다.

FMCv 업그레이드(6.6.0 이상)에 28GB RAM 필요

FMCv 플랫폼은 업그레이드 중에 새로운 메모리 검사를 도입했습니다. 가상 어플라이언스에 28GB 미만의 RAM을 할당하면 버전 6.6.0 이상으로의 FMCv 업그레이드가 실패합니다.

중요 기본 설정을 줄이지 않는 것이 좋습니다. 대부분의 FMCv 인스턴스의 경우 32GB RAM, FMCv 300의 경우 64GB가 필요합니다. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다.

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

메모리 및 리소스 요구 사항

KVM을 사용하여 수정되지 않은 OS 이미지를 실행하는 여러 가상 머신을 실행할 수 있습니다. 각 가상 머신에는 네트워크 카드, 디스크, 그래픽 어댑터 등의 개인 가상화 하드웨어가 있습니다. 하이퍼바이저 호환성에 대한 내용은 Cisco Firepower 호환성 가이드를 참조하십시오.

중요 FMCv를 업그레이드할 때 최신 릴리스가 환경에 영향을 미치는지 여부에 대한 자세한 내용은 최신 Firepower 릴리스 노트를 참조하십시오. 최신 버전의 Firepower를 구축하려면 리소스를 늘려야 할 수 있습니다.

Firepower를 업그레이드할 때 Firepower 구축의 보안 기능 및 성능을 개선하는 데 도움이 되는 최신 기능 및 수정 사항을 추가합니다.

FMCv 구축에 사용되는 특정 하드웨어는 구축된 인스턴스 수 및 사용 요구 사항에 따라 달라질 수 있습니다. 생성하는 각 가상 어플라이언스는 호스트 머신에서 최소 리소스 할당(메모리, CPU 수 및 디스크 공간)을 필요로 합니다.

다음 표에는 FMCv 어플라이언스의 권고 및 기본 설정이 나와 있습니다.

- 프로세서
  - 4개의 vCPU 필요
- 메모리
  - 최소 필요 28 / 권장(기본값) 32GB RAM

    중요 FMCv 플랫폼은 업그레이드 중에 새로운 메모리 검사를 도입했습니다. 가상 어플라이언스에 28GB 미만의 RAM을 할당하면 버전 6.6.0 이상으로의 FMCv 업그레이드가 실패합니다.
- 네트워킹
  - virtio 드라이버 지원
  - 1개의 관리 인터페이스 지원
- 가상 머신별 호스트 스토리지
  - FMCv에는 250GB가 필요합니다.
  - virtio 및 scsi 블록 디바이스 지원
- 콘솔
  - 텔넷을 통해 터미널 서버 지원

KVM을 사용하는 구축에 대한 사전 요구 사항

- Cisco.com에서 Firepower Management Center Virtual qcow2 파일을 다운로드하고 이를 Linux 호스트에 둡니다.

  https://software.cisco.com/download/navigator.html

- Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.
- 이 문서에 나와 있는 샘플 구축의 경우, 사용자가 Ubuntu 18.04 LTS를 사용 중인 것으로 가정합니다. Ubuntu 18.04 LTS 호스트의 상위에 다음 패키지를 설치합니다.
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- 성능은 호스트 및 해당 컨피그레이션에 영향을 받습니다. 호스트를 조정하여 KVM에서 처리량을 극대화할 수 있습니다. 일반적인 호스트 조정 개념에 대한 내용은 Network Function Virtualization: Linux 및 Intel Architecture를 갖춘 Broadband Remote Access Server의 서비스 품질을 참조하십시오.
- Ubuntu 18.04 LTS에 유용한 최적화는 다음과 같습니다.
  - macvtap - 고성능 Linux 브리지로, Linux 브리지 대신 macvtap을 사용할 수 있습니다. Linux 브리지 대신 macvtap을 사용하려면 특정 설정을 구성해야 합니다.
  - Transparent Huge Pages - 메모리 페이지 크기를 늘리며 Ubuntu 18.04에서 기본적으로 설정됩니다.
  - Hyperthread 비활성화 - 두 개의 vCPU를 단일 코어로 줄입니다.
  - txqueuelength - 기본 txqueuelength를 4000 패킷으로 늘이고 삭제율을 줄입니다.
  - 고정 - qemu 및 vhost 프로세스를 특정 CPU 코어에 고정합니다. 특정 조건에서 고정 기능을 사용하면 성능이 대폭 향상됩니다.
- RHEL 기반 배포 최적화에 대한 자세한 내용은 Red Hat Enterprise Linux6 가상화 조정 및 최적화 가이드를 참조하십시오.

지침 및 제한 사항

- Firepower Management Center Virtual 어플라이언스에는 일련 번호가 없습니다. **System(**시스템**)** > **Configuration(**구성**)** 페이지에는 가상 플랫폼에 따라 **None(**없음**)** 또는 **Not Specified(**지정되지 않음**)** 중 하나가 표시됩니다.
- 중첩된 하이퍼바이저(VMware / ESXi에서 실행되는 KVM)는 지원되지 않습니다. 베어 메탈 KVM 구축만 지원됩니다.
- 가상 머신 복제는 지원되지 않습니다.
- 고가용성은 지원되지 않습니다.

Day 0 컨피그레이션 파일 준비

FMCv를 실행하기 전에 Day 0 구성 파일을 준비할 수 있습니다. Day 0 구성은 가상 머신이 구축될 때 적용되는 초기 구성 데이터가 포함된 텍스트 파일입니다. 이 초기 컨피그레이션은 사용자가 선택하는 작업 디렉토리의 "day0-config"라는 이름의 텍스트 파일에 위치하며, 이 파일은 최초 부팅 시 마운트되고 읽히는 day0.iso 파일로 조작됩니다.

참고 day0.iso 파일은 첫 부팅 시 사용할 수 있어야 합니다.

Day 0 컨피그레이션 파일을 사용하여 구축하는 경우, 프로세스를 통해 FMCv 어플라이언스의 전체 초기 설정을 수행할 수 있습니다. 다음을 지정할 수 있습니다.

- EULA 동의
- 시스템의 호스트 이름
- 관리자 계정의 새 관리자 비밀번호
- 어플라이언스가 관리 네트워크에서 통신하도록 허용하는 네트워크 설정. Day 0 구성 파일 없이 구축하는 경우, 실행 후 Firepower System의 필수 설정을 구성해야 합니다. 자세한 내용은 Day 0 구성 파일 없이 구축, 33 페이지의 내용을 참조하십시오.

  참고 이 예에서는 Linux를 사용하지만, Windows에도 유사한 유틸리티가 있습니다.

- 기본 Cisco Umbrella DNS 서버를 사용하려면 두 DNS 항목을 모두 비워 둡니다. 비 DNS 환경에서 작동하려면 두 항목을 모두 "None"(대/소문자 구분 안 함)으로 설정합니다.

단계 **1** "day0-config"라는 이름의 텍스트 파일에 FMCv 네트워크 설정에 대한 CLI 구성을 입력합니다.

예제:

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "Admin123",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",

    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

단계 **2** 텍스트 파일을 ISO 파일로 전환하여 가상 CD-ROM을 생성합니다.

예제:

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

또는

예제:

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

단계 **3** 이 작업을 반복하여 구축할 각 FMCv에 대해 고유한 기본 구성 파일을 생성합니다.

다음에 수행할 작업

- virt-install을 사용하는 경우, virt-install 명령에 다음 줄을 추가합니다.

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- virt-manager를 사용하는 경우, virt-manager GUI를 사용하여 가상 CD-ROM을 생성할 수 있습니다. Virtual Machine Manager를 사용하여 시작, 29 페이지의 내용을 참조하십시오.

실행 FMCv

다음 방법을 사용하여 KVM에서 FMCv를 실행할 수 있습니다.

- 구축 스크립트 사용 - virt-install 기반 구축 스크립트를 사용하여 FMCv를 실행합니다. 구축 스크립트를 사용하여 시작, 28 페이지의 내용을 참조하십시오.
- Virtual Machine Manager 사용 - KVM 게스트 가상 머신을 생성 및 관리하기 위한 그래픽 툴인 virt-manager를 사용하여 FMCv를 실행합니다. Virtual Machine Manager를 사용하여 시작, 29 페이지의 내용을 참조하십시오.
- OpenStack 사용 - OpenStack 환경을 사용하여 FMCv를 실행합니다. OpenStack을 사용하여 시작, 31 페이지의 내용을 참조하십시오.

Day 0 구성 파일 없이 FMCv를 구축하도록 선택할 수도 있습니다. 이 경우 어플라이언스의 CLI 또는 웹 인터페이스를 사용하여 초기 설정을 완료해야 합니다.

구축 스크립트를 사용하여 시작

virt-install 기반 구축 스크립트를 사용하여 Firepower Management Center Virtual을 실행할 수 있습니다.

시작하기 전에

환경에 가장 적합한 게스트 캐싱 모드를 선택하여 성능을 최적화할 수 있습니다. 사용 중인 캐시 모드는 데이터 손실 발생 여부에 영향을 미치며, 디스크 성능에도 영향을 줄 수 있습니다.

각 KVM 게스트 디스크 인터페이스에는 *writethrough*, *writeback*, *none*, *directsync* 또는 *unsafe* 캐시 모드 중 하나가 지정되어 있을 수 있습니다. *writethrough* 모드는 읽기 캐싱을 제공하고, *writeback*은 읽기 및 쓰기 캐싱을 제공하며, *directsync*는 호스트 페이지 캐시를 우회합니다. *unsafe*는 모든 콘텐츠를 캐시하고 게스트의 플러시 요청을 무시할 수 있습니다.

- *cache=writethrough*는 호스트에서 갑작스러운 전력 손실이 발생하는 경우 KVM 게스트 머신에서 파일 손상을 줄이는 데 도움이 됩니다. Writethrough 모드를 사용하는 것이 좋습니다.
- 그러나 *cache=writethrough*는 *cache=none*보다 더 많은 디스크 I/O 작성으로 인해 디스크 성능에도 영향을 줄 수 있습니다.
- *--disk* 옵션에서 캐시 파라미터를 제거하는 경우 기본값은 *writethrough*입니다.
- 캐시 옵션을 지정하지 않으면 VM을 생성하는 데 필요한 시간도 크게 줄일 수 있습니다. 이는 일부 오래된 RAID 컨트롤러의 디스크 캐싱 기능이 좋지 않기 때문입니다. 따라서 디스크 캐싱(*cache=none*)을 비활성화하여 기본값을 *writethrough*로 설정하면 데이터 무결성을 보장하는 데 도움이 됩니다.

단계 **1** "virt_install_fmc.sh"라는 이름의 virt-install 스크립트를 생성합니다.

Firepower Management Center Virtual 인스턴스의 이름은 이 KVM 호스트의 모든 기타 VM(가상 머신)에서 고유해야 합니다. Firepower Management Center Virtual은 1개의 네트워크 인터페이스를 지원할 수 있습니다. 가상 NIC는 Virtio여야 합니다.

예제:

```
virt-install \
    --connect=qemu:///system \
    --network network=default,model=virtio \
    --name=fmcv \
    --arch=x86_64 \
    --cpu host \
    --vcpus=4 \
    --ram=8192 \
    --os-type=linux \
    --virt-type=kvm \
    --import \
    --watchdog i6300esb,action=reset \
    --disk path=<fmc_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=writethrough \
    --disk path=<day0_filename>.iso,format=iso,device=cdrom \
    --console pty,target_type=serial \
    --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
    --force
```

단계 **2** virt_install 스크립트를 실행합니다.

예제:

```
/usr/bin/virt_install_fmc.sh
Starting install...
Creating domain...
```

VM의 콘솔을 표시하는 창이 나타납니다. VM이 부팅 중인 것으로 표시됩니다. VM이 부팅될 때까지 몇 분 정도 소요됩니다. VM이 부팅을 멈추면 콘솔 화면에서 CLI 명령을 발급할 수 있습니다.

Virtual Machine Manager를 사용하여 시작

Virtual Machine Manager라고도 알려져 있는 virt-manager를 사용하여 Firepower Management Center Virtual을 실행합니다. virt-manager는 게스트 가상 머신을 생성 및 관리하기 위한 그래픽 툴입니다.

단계 **1** virt-manager(**Applications(**애플리케이션**)** > **System Tools(**시스템 툴**)** > **Virtual Machine Manager**)를 시작합니다.

하이퍼바이저 선택 및/또는 루트 비밀번호 입력을 수행할지 묻는 메시지가 표시될 수 있습니다.

단계 **2** 왼쪽 상단 모서리에 있는 버튼을 클릭하여 **New VM(**새 **VM)** 마법사를 엽니다.

단계 **3** 다음과 같이 가상 머신 상세정보를 입력합니다.

a) 운영 체제에 대해서는 **Import existing disk image(**기존 디스크 이미지 가져오기**)**를 선택합니다.

이 방법을 사용하면 디스크 이미지(사전 설치, 부팅 가능 운영 체제 포함)를 가져올 수 있습니다.

b) 계속하려면 **Forward(**전달**)**를 클릭합니다.

단계 **4** 다음과 같이 디스크 이미지를 로드합니다.

a) **Browse...(**찾아보기**...)**를 클릭하여 이미지 파일을 선택합니다.

b) **OS type(OS** 유형**)**을 *Use Generic(*일반 사용*)*을 선택합니다.

c) 계속하려면 **Forward(**전달**)**를 클릭합니다.

단계 **5** 다음과 같이 메모리 및 CPU 옵션을 구성합니다.

a) *Memory (RAM)(*메모리*(RAM))*를 **8192**로 설정합니다.
b) **CPUs(CPU)**를 *4*로 설정합니다.
c) 계속하려면 **Forward(**전달**)**를 클릭합니다.

단계 **6** **Customize configuration before install(**설치 전에 구성 맞춤화**)** 상자를 선택하고, **Name(**이름**)**, 그 다음 **Finish(**마침**)**를 클릭합니다.

이렇게 하면 가상 머신의 하드웨어 설정을 추가, 제거 및 구성할 수 있게 해주는 또 다른 마법사가 열립니다.

단계 **7** CPU 구성을 수정합니다.

왼쪽 패널에서 프로세서를 선택하고 **Configuration(**구성**)** > **Copy host CPU configuration(**호스트 **CPU** 구성 복사**)**을 선택합니다.

이 작업을 수행하면 실제 호스트의 CPU 모델 및 구성이 가상 머신에 적용됩니다.

단계 **8** 8. 다음과 같이 가상 디스크를 구성합니다.

a) 왼쪽 패널에서 **Disk 1(**디스크 **1)**을 선택합니다.
b) **Advanced options(**고급 옵션**)**를 선택합니다.
c) **Disk bus(**디스크 버스**)**를 *Virtio*로 설정합니다.
d) **Storage format(**스토리지 형식**)**을 *qcow2*로 설정합니다.

단계 **9** 다음과 같이 시리얼 콘솔을 구성합니다.

a) 왼쪽 패널에서 **Console(**콘솔**)**을 선택합니다.
b) **Remove(**제거**)**를 선택하여 기본 콘솔을 제거합니다.
c) **Add Hardware(**하드웨어 추가**)**를 클릭하여 시리얼 디바이스를 추가합니다.
d) **Device Type(**디바이스 유형**)**의 경우 *TCP net console (tcp)(TCP* 넷 콘솔*(tcp))*을 선택합니다.
e) **Mode(**모드**)**의 경우 *Server mode (bind)(*서버 모드*(*바인딩*))*를 선택합니다.
f) **Host(**호스트**)**의 경우 IP 주소로 **0.0.0.0**을 그리고 고유한 **Port(**포트**)** 번호를 입력합니다.
g) **Use Telnet(**텔넷 사용**)** 상자를 선택합니다.
h) 디바이스 파라미터를 구성합니다.

단계 **10** 다음과 같이 KVM 게스트가 중단하거나 충돌할 때 자동으로 몇 가지 작업을 트리거할 수 있도록 워치도그 디바이스를 구성합니다.

a) **Add Hardware(**하드웨어 추가**)**를 클릭하여 워치도그 디바이스를 추가합니다.
b) **Model(**모델**)**의 경우 *default(*기본값*)*를 선택합니다.
c) **Action(**작업**)**의 경우 *Forcefully reset the guest(*게스트를 강제로 재설정*)*을 선택합니다.

단계 **11** 다음과 같이 가상 네트워크 인터페이스를 구성합니다.

macvtap을 선택하거나 공유 디바이스 이름을 지정합니다(브리지 이름 사용).

참고 기본적으로 Firepower Management Center Virtual 가상 인스턴스는 하나의 인터페이스에서 실행되며, 실행한 후 구성할 수 있습니다.

단계 **12** Day 0 구성 파일을 사용하여 구축하는 경우 다음과 같이 ISO에 대한 가상 CD-ROM을 생성합니다.

a) **Add Hardware(**하드웨어 추가**)**를 클릭합니다.
b) **Storage(**스토리지**)**를 선택합니다.
c) **Select managed or other existing storage(**매지니드 스토리지 또는 다른 기존 스토리지 선택**)**를 클릭하고 ISO 파일의 위치를 찾습니다.
d) **Device type(**디바이스 유형**)**의 경, *IDE CDROM*을 선택합니다.

단계 **13** 가상 머신의 하드웨어를 구성한 후 **Apply(**적용**)**를 클릭합니다.

단계 **14** virt-manager에 대해 **Begin installation(**설치 시작**)**을 클릭하여 지정된 하드웨어 설정으로 가상 머신을 생성합니다.

OpenStack을 사용하여 시작

OpenStack 환경에서 Firepower Management Center Virtual을 구축할 수 있습니다. OpenStack은 퍼블릭 및 프라이빗 클라우드용 클라우드 컴퓨팅 플랫폼을 구축 및 관리하기 위한 소프트웨어 툴 집합으로, KVM 하이퍼바이저와 긴밀하게 통합되어 있습니다.

OpenStack의 Day 0 구성 파일 정보

OpenStack은 부팅할 때 인스턴스에 연결되어 있는 특수 구성 드라이브(config-drive)를 통해 구성 데이터를 제공하는 것을 지원합니다. nova 부팅 명령을 사용하여 Day 0 구성이 있는 Firepower Management Center Virtual 인스턴스를 구축하려면 다음 줄을 포함하십시오.

```
--config-drive true --file day0-config=/home/user/day0-config \
```

--config-drive 명령이 활성화되어 있는 경우, nova 클라이언트가 호출되는 Linux 파일 시스템에서 발견된 =/home/user/day0-config 파일이 가상 CDROM에 있는 가상 머신에 전달됩니다.

참고 VM에서는 이름이 *day0-config*인 이 파일을 볼 수 있지만, OpenStack에서는 일반적으로 파일 콘텐츠를 /openstack/content/xxxx로 저장합니다. 여기서 xxxx는 할당된 4자리 숫자(예: /openstack/content/0000)입니다. 이 숫자는 OpenStack 배포별로 다를 수 있습니다.

커맨드 라인을 사용하여 OpenStack에서 시작

nova 부팅 명령을 사용하여 FMCv 인스턴스를 생성하고 부팅합니다.

프로시저

	명령 또는 동작	목적

단계 **1**	이미지, 버전, 인터페이스 및 Day 0 구성 정보를 사용하여 FMCv 인스턴스를 부팅합니다.
	예제:
	`local@maas:~$ nova boot \`
	`--image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \`
	`--flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \`
		FMCv에는 1개의 관리 인터페이스가 필요합니다.

	명령 또는 동작	목적
	`--nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \ --config-drive true --file day0-config=/home/local/day0-config \`	

대시보드를 사용하여 OpenStack에서 시작

Horizon은 OpenStack 대시보드로 Nova, Swift, Keystone 등의 OpenStack 서비스에 웹 기반 사용자 인터페이스를 제공합니다.

시작하기 전에

- Cisco.com에서 FMCv qcow2 파일을 다운로드하고 이를 로컬 MAAS 서버에 둡니다.
  https://software.cisco.com/download/navigator.html
- Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

단계 **1** Log In(로그인) 페이지에서 사용자 이름 및 비밀번호를 입력하고 **Sign In(**로그인**)**을 클릭합니다.

대시보드에서 볼 수 있는 탭과 기능은 로그인한 사용자의 액세스 권한 또는 역할에 따라 달라집니다.

단계 **2** 메뉴에서 **Admin(**관리**)** > **System Panel(**시스템 패널**)** > **Flavor(**버전**)**를 선택합니다.

가상 하드웨어 템플릿은 OpenStack에서 버전이라고 하며 디스크, RAM의 크기, 코어 수 등을 정의합니다.

단계 **3** 다음과 같이 **Flavor Info(**버전 정보**)** 창에서 필수 정보를 입력합니다.

a) **Name(**이름**)** - 인스턴스를 쉽게 식별할 수 있게 해주는 설명이 담긴 이름을 입력합니다. FMC-4vCPU-8GB와 같은 이름을 예로 들 수 있습니다.
b) **VCPUs(VCPU)** - 4를 선택합니다.
c) **RAM MB** - 8192를 선택합니다.

단계 **4** **Create Flavor(**버전 생성**)**를 선택합니다.

단계 **5** 메뉴에서 **Admin(**관리**)** > **System Panel(**시스템 패널**)** > **Images(**이미지**)**를 선택합니다.

단계 **6** 다음과 같이 Create An Image(이미지 생성) 창에서 필수 정보를 입력합니다.

a) **Name(**이름**)** - 이미지를 쉽게 식별할 수 있게 해주는 이름을 입력합니다. *FMC-Version-Build*와 같은 이름을 예로 들 수 있습니다.
b) **Description(**설명**)** - (선택 사항) 이 이미지 파일의 설명을 입력합니다.
c) **Browse(**찾아보기**)** - Cisco.com에서 이전에 다운로드한 Firepower Management Center Virtual qcow2 파일을 선택합니다.
d) **Format(**형식**)** - 형식 유형으로 *QCOW2-QEMU* 에뮬레이터를 선택합니다.
e) **Public(**퍼블릭**)** 상자를 선택합니다.

단계 **7** **Create Image(**이미지 생성**)**를 선택합니다.

새로 생성된 이미지를 확인합니다.

단계 **8** 메뉴에서 **Project(**프로젝트**)** > **Compute(**컴퓨팅**)** > **Instances(**인스턴스**)**를 선택합니다.

단계 **9** **Launch Instance(**인스턴스 실행**)**를 클릭합니다.

단계 **10** **Launch Instance(**인스턴스 실행**)** > **Details(**상세정보**)** 탭에서 필수 정보를 입력합니다.

a) **Instance Name(**인스턴스 이름**)** - 인스턴스를 쉽게 식별할 수 있게 해주는 이름을 입력합니다. *FMC-Version-Build* 와 같은 이름을 예로 들 수 있습니다.

b) **Flavor(**버전**)** - 이전에 3단계에서 생성한 버전을 선택합니다. 이 이미지 파일의 설명을 입력합니다.

c) **Instance Boot Source(**인스턴스 부팅 소스**)** - *Boot from image(*이미지에서 부팅*)*를 선택합니다.

d) **Image Name(**이미지 이름**)** - 이전에 6단계에서 생성한 이미지를 선택합니다.

단계 **11** **Launch Instance(**인스턴스 실행**)** > **Networking(**네트워킹**)** 탭에서 Firepower Management Center Virtual 인스턴스의 관리 네트워크를 선택합니다.

단계 **12** **Launch(**실행**)**를 클릭합니다.

클라우드의 컴퓨팅 노드에서 인스턴스가 시작됩니다. Instances(인스턴스) 창에서 새로 생성된 인스턴스를 확인합니다.

단계 **13** Firepower Management Center Virtual 인스턴스를 선택합니다.

단계 **14** **Console(**콘솔**)** 탭을 선택합니다.

단계 **15** 콘솔에서 가상 어플라이언스에 로그인합니다.

Day 0 구성 파일 없이 구축

모든 Firepower Management Center의 경우, 어플라이언스가 관리 네트워크에서 통신할 수 있도록 허용하는 설정 프로세스를 완료해야 합니다. Day 0 구성 파일 없이 구축하는 경우 FMCv 설정 시 다음과 같은 두 가지 단계의 프로세스를 수행하십시오.

- FMCv를 초기화한 다음, 어플라이언스가 관리 네트워크에서 통신하도록 구성하는 데 도움이 되는 어플라이언스 콘솔에서 스크립트를 실행합니다.
- 그런 다음, 관리 네트워크에서 컴퓨터를 사용하여 설정 프로세스를 완료하고 FMCv의 웹 인터페이스를 탐색합니다.

스크립트를 사용하여 네트워크 설정 구성

다음 절차에서는 CLI를 사용하여 FMCv에서 초기 설정을 완료하는 방법을 설명합니다.

단계 **1** 콘솔에서 FMCv 어플라이언스에 로그인합니다. 사용자 이름으로 **admin**, 비밀번호로 **Admin123**을 사용합니다.

단계 **2** admin 프롬프트에서 다음 스크립트를 실행합니다.

예제**:**

```
sudo /usr/local/sf/bin/configure-network
```

FMCv에 처음 연결할 때 포스트 부팅 구성에 대한 프롬프트가 표시됩니다.

단계 3 스크립트의 프롬프트에 따릅니다.

IPv4 및 IPv6 관리 설정을 차례로 구성(또는 비활성화)합니다. 네트워크 설정을 수동으로 지정하는 경우 IPv4 또는 IPv6 주소를 입력해야 합니다.

단계 4 설정이 올바른지 확인합니다.

단계 5 어플라이언스에서 로그아웃합니다.

다음에 수행할 작업

- 관리 네트워크에서 컴퓨터를 사용하여 설정 프로세스를 완료하고 FMCv의 웹 인터페이스를 탐색합니다.

웹 인터페이스를 사용하여 초기 설정 수행

다음 절차에서는 웹 인터페이스를 사용하여 FMCv에서 초기 설정을 완료하는 방법을 설명합니다.

단계 1 다음과 같이 브라우저에서 FMCv의 관리 인터페이스의 기본 IP 주소로 이동합니다.

예제:

```
https://192.168.45.45
```

단계 2 Firepower Management Center Virtual 어플라이언스에 로그인합니다. 사용자 이름으로 **admin**, 비밀번호로 **Admin123**을 사용합니다. 설정 페이지가 표시됩니다.

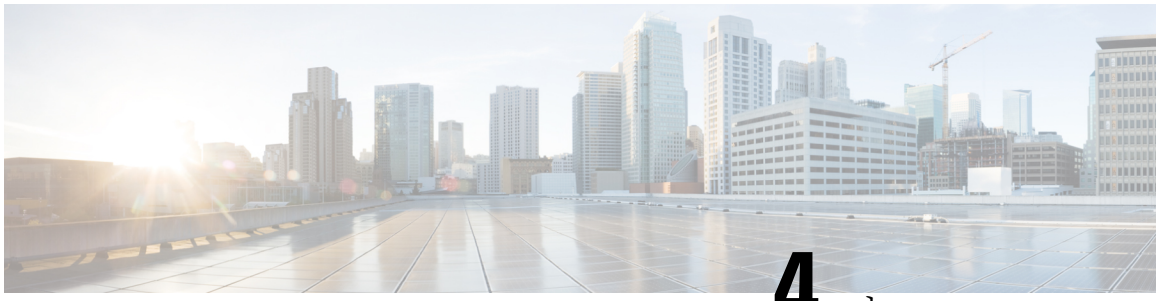
설정 페이지가 표시됩니다. 관리자 비밀번호를 변경하고 아직 수행하지 않은 경우 네트워크 설정을 지정한 후 EULA에 동의해야 합니다.

단계 3 완료되면 **Apply(**적용**)**를 클릭합니다. 선택 사항에 따라 FMCv가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 admin 사용자로 웹 인터페이스에 로그인된 것입니다.

선택 사항에 따라 FMCv가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 admin 사용자로 웹 인터페이스에 로그인된 것입니다.

다음에 수행할 작업

- FMCv의 초기 설정에 대한 자세한 내용은 Firepower Management Center Virtual 초기 설정, 69 페이지의 내용을 참조하십시오.
- FMCv 구축에서 필요한 다음 단계에 대한 개요는 Firepower Management Center Virtual 초기 관리 및 구성, 77 페이지 장을 참조하십시오.



4 장

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

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 6: AWS 지원 인스턴스 FMCv, 36 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 ***6: 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, 36 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 6: AWS 지원 인스턴스 FMCv, 36 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 라이선스, 3 페이지의 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, 39 페이지
- 인터넷 게이트웨이 추가, 40 페이지
- 서브넷 추가, 40 페이지
- 경로 테이블 추가, 41 페이지
- 보안 그룹 생성, 42 페이지
- 네트워크 인터페이스 생성, 42 페이지
- 탄력적 IP 생성, 43 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.

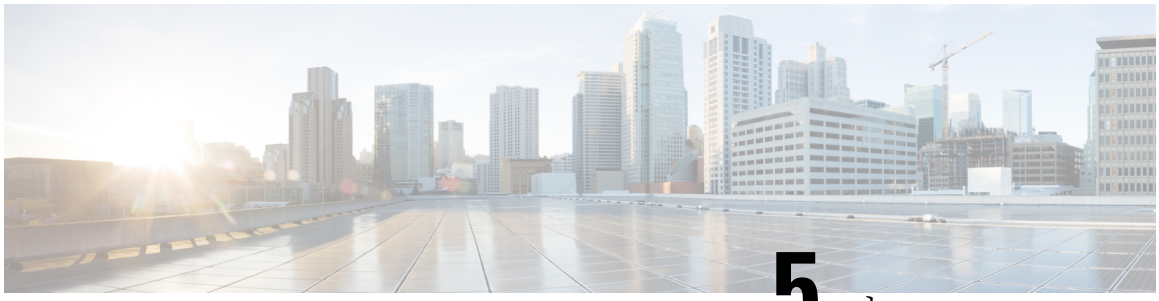
- 구축이 완료되었는지 확인합니다. FMCv VM 인스턴스 스크린샷에 "Cisco Firepower Management Center for AWS vW.X.Y (build ZZ)"(AWS용 Cisco Firepower Management Center vW.X.Y(빌드 ZZ))와 비슷한 메시지가 표시되며, 그 다음에는 추가 출력이 몇 줄 표시될 수 있습니다.
- 탄력적 IP가 있고, 해당 IP가 Firepower Management Center의 관리 네트워크 인터페이스(eni)에 연결되어 있으며, 해당 IP 주소에 연결되어 있는지 확인합니다.
- 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.

-



5 장

Firepower Management Center Virtual On the Microsoft Azure Cloud 구축

Microsoft Azure 퍼블릭 클라우드에 Firepower Management Center Virtual(FMCv)를 가상 시스템으로 구축할 수 있습니다.

중요 FMCv은(는) Cisco Firepower 소프트웨어 버전 6.4 이상으로 시작하는 Microsoft Azure에서 지원됩니다.

FMCv 구축 및 Azure 정보

Azure Marketplace에서 제공되는 솔루션 템플릿을 사용하여 Microsoft Azure에서 Firepower Management Center Virtual(FMCv)을 구축합니다. Azure 포털을 사용하여 FMCv를 구축할 때는 기존의 빈 리소스 그룹 및 스토리지 계정을 사용하거나 새로 생성할 수 있습니다. 솔루션 템플릿은 FMCv의 초기 설정을 제공하는 컨피그레이션 매개 변수 집합을 안내하며, 처음 부팅한 후 FMCv 웹 인터페이스에 로그인할 수 있습니다.

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 7: Azure 지원 인스턴스 대상 FMCv, 48 페이지의 내용을 참조하십시오.

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

FMCv는 Azure에서 리소스 관리자 구축 모드를 사용하여 VNet(Virtual Network)에 구축해야합니다. 표준 Azure 퍼블릭 클라우드 환경에서 FMCv를 구축할 수 있습니다. Azure Marketplace의 FMCv에서는 BYOL(Bring Your Own License) 모델을 지원합니다.

다음 표에는 FMCv가 지원하는 Azure 인스턴스 유형이 요약되어 있습니다. 즉, 버전 6.5.x 이하를 지원하는 인스턴스 및 버전 6.6.0 이상을 지원하는 인스턴스.

표 ***7: Azure*** 지원 인스턴스 대상 ***FMCv***

플랫폼	버전 **6.6.0** 이상	버전 **6.5** 이하*
FMCv	Standard_D4_v2: 8개의 vCPU, 28GB	Standard_D3_v2: 4개의 vCPU, 14GB
	—	Standard_D4_v2: 8개의 vCPU, 28GB
	* 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, 48 페이지의 내용을 참조하십시오.	

사용되지 않는 인스턴스

Standard_D3_v2를 사용해서 현재 6.5.x 이하 버전의 FMCv 구축을 계속 실행할 수 있지만 이 인스턴스를 사용하여 새 FMCv 구축(모든 버전)을 시작할 수는 없습니다.

인스턴스 크기 조정

이전 버전의 FMCv(6.2.x, 6.3.x, 6.4.x, 6.5.x)에서 버전 6.6.0으로의 업그레이드 경로에는 28GB RAM 메모리 검사가 포함되어 있으므로 Standard_D3_v2를 사용하는 경우 인스턴스 유형의 크기를 Standard_D4_v2로 조정합니다(표 7: Azure 지원 인스턴스 대상 FMCv, 48 페이지 참고).

Azure 포털 또는 PowerShell을 사용하여 인스턴스 크기를 조정할 수 있습니다. 가상 시스템이 현재 실행중인 경우 크기를 변경하면 가상 시스템이 재시작됩니다. 가상 시스템을 중지하면 추가 크기가 표시될 수 있습니다.

인스턴스 크기 조정 방법에 대한 지침은 Azure 설명서 "Resize a Windows VM"(https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm)을 참조하십시오.

사전 요건 및 시스템 요구 사항

Microsoft Azure에서 FMCv에 대한 지원은 Firepower 버전 6.4.0 릴리스의 새로운 기능입니다. Firepower Management Center Virtual 및 Firepower System 호환성에 대해서는 Cisco Firepower Threat Defense Virtual Compatibility를 참조하십시오.

Azure에서 FMCv를 구축하기 전에 다음을 확인합니다.

- Azure.com에서 계정을 생성합니다.

  Microsoft Azure에서 어카운트를 생성한 후에는 로그인하여 Cisco Firepower Management Center Virtual에 대한 시장을 검색하고 "Cisco Firepower Management Center (FMCv) BYOL" 제품을 선택할 수 있습니다.

- Cisco Smart Account는 Cisco Software Central에서 하나를 생성할 수 있습니다. (https://software.cisco.com/).

지침 및 제한 사항

지원 기능

- 지원되는 Azure 인스턴스
  - 표준 D3_v2 - 4개의 vCPU, 14GB 메모리, 250GB 디스크 크기
  - 표준 D4_v2 - 8개의 vCPU, 28GB 메모리, 400GB 디스크 크기
- 공용 IP 주소
  - 관리 0/0에는 공용 IP 주소가 할당됩니다.

라이선싱

Azure 퍼블릭 마켓플레이스의 FMCv는 BYOL(Bring Your Own License) 모델을 지원합니다. FMCv의 경우 이는 기능 라이선스가 아닌 플랫폼 라이선스입니다. 구매하는 가상 라이선스 버전에 따라 Firepower Management Center Virtual를 통해 관리할 수 있는 디바이스의 수가 결정됩니다. 예를 들어, 2개의 디바이스, 10개의 디바이스 또는 25개의 디바이스를 관리할 수 있는 라이선스를 구매할 수 있습니다.

- 라이선싱 모드:
  - 스마트 라이선스만 해당

라이선싱에 대한 자세한 내용은 *Firepower Management Center Configuration Guide*의 Firepower System 라이선싱을 참조하십시오. 유용한 링크를 포함하여 Firepower System용 기능 라이선스의 개요는 Cisco Firepower System 기능 라이선스를 참조하십시오.

시스템 종료 및 재시작

Azure 가상 머신 개요 페이지의 재시작 및 중지 컨트롤을 사용하여 FMCv VM의 전원을 켜지 마십시오. 이는 정상적인 종료 메커니즘이 아니며 데이터베이스 손상으로 이어질 수 있습니다.

FMCv의 웹 인터페이스에서 사용 가능한 **System(**시스템**)** > **Configuration(**컨피그레이션**)** 옵션을 사용하여 가상 어플라이언스를 종료하거나 재시작합니다.

FMCv의 명령줄 인터페이스에서 `shutdown(종료)` 및 `restart(재시작)` 명령을 사용하여 어플라이언스를 종료하거나 재시작합니다.

지원되지 않는 기능

- 라이선싱 모드:
  - PAYG(Pay As You Go) 라이선싱
  - PLR(Permanent License Reservation)
- 관리
  - Azure 포털 "비밀번호 재설정"기능
  - 콘솔 기반 비밀번호 복구: 사용자는 콘솔에 실시간으로 액세스할 수 없으므로 비밀번호를 복구할 수 없습니다. 비밀번호 복구 이미지는 부팅할 수 없습니다. 유일한 방법은 새 FMCv VM을 구축하는 것입니다.
- 고가용성(활성-대기)
- VM 가져오기/내보내기

구축 중에 생성된 리소스

Azure에서 FMCv를 구축할 때 다음 리소스가 생성됩니다.

- 단일 인터페이스의 Cisco FMCv VM(가상 머신)(서브넷이 1개인 신규 또는 기존 가상 네트워크 필요)
- 리소스 그룹

  FMCv는 항상 새 리소스 그룹에 구축됩니다. 그러나 다른 리소스 그룹의 기존 가상 네트워크에 연결할 수 있습니다.
- *vm name*-SSH-SecurityGroup으로 명명된 보안 그룹

  해당 보안 그룹은 VM의 Nic0에 연결됩니다.

  보안 그룹에는 SSH (TCP 포트 22) 및 Firepower Management Center 인터페이스 (TCP 포트 8305)의 관리 트래픽을 허용하는 규칙이 포함되어 있습니다. 구축 후에 이 값을 수정할 수 있습니다.
- 공용 IP 주소(구축 중에 선택한 값에 따라 이름이 지정됩니다)

공용 IP 주소가 VM Nic0과 연결되며, 이는 Management에 매핑됩니다.

참고 새로운 공용 IP를 만들거나 기존의 공용 IP를 선택할 수 있습니다. **NONE(**없음**)**을 선택할 수도 있습니다. 공용 IP 주소가 없으면 FMCv에 대한 모든 통신은 Azure 가상 네트워크 내에서 시작되어야 합니다.

- 해당 서브넷에 대한 라우팅 테이블(이미 있을 경우 업데이트됨)
- 선택된 스토리지 계정의 부팅 진단 파일

  부팅 진단 파일은 Blob(binary large object)에 포함됩니다.
- Blob과 컨테이너 VHD인 *vm name*-disk.vhd 및 *vm name*-<uuid>.status에 속한 선택된 스토리지 계정의 파일 2개
- 스토리지 계정(기존 스토리지 계정을 선택하지 않은 경우)

중요 VM을 삭제할 경우 이 리소스에서 유지할 것을 제외하고 각각을 개별적으로 삭제해야 합니다.

Firepower Management Center Virtual 구축

템플릿을 사용하여 Azure에서 Firepower Management Center Virtual를 구축할 수 있습니다. Cisco는 다음과 같은 두 가지 템플릿을 제공합니다.

- **Azure Marketplace**의 솔루션 템플릿 - Azure Marketplace에서 사용 가능한 솔루션 템플릿을 사용하여 Azure Portal을 사용하여 FMCv를 구축합니다. 기존 리소스 그룹 및 스토리지 어카운트를 사용하거나 새로 생성하여 가상 어플라이언스를 구축할 수 있습니다. 솔루션 템플릿을 사용하려면 솔루션 템플릿을 사용한 Azure Marketplace에서의 구축, 51 페이지를 참조하십시오.
- **GitHub** 리포지토리의 **ARM** 템플릿 - Cisco는 Marketplace 기반 구축 외에도 GitHub 리포지토리에서 ARM(Azure Resource Manager) 템플릿을 제공하여 Azure에 FMCv를 구축하는 프로세스를 간소화합니다. 매니지드 이미지와 두 개의 JSON 파일(템플릿 파일 및 매개 변수 파일)을 사용하여 FMCv를 위해 단일 리소스로 모든 리소스를 구축하고 프로비저닝할 수 있습니다.

솔루션 템플릿을 사용한 **Azure Marketplace**에서의 구축

Azure Marketplace에서 제공되는 솔루션 템플릿을 사용하여 Azure 포털에서 Firepower Management Center Virtual(FMCv)을 구축합니다. 다음 절차는 Microsoft Azure 환경에서 FMCv를 설정하는 상위 수준의 단계를 간략하게 정리한 것입니다. 자세한 Azure 설정 단계에 대한 자세한 내용은 Azure 시작하기를 참조하십시오.

Azure에서 FMCv를 구축할 경우 리소스, 공용 IP 주소, 경로 테이블과 같은 다양한 컨피그레이션이 자동으로 생성됩니다. 구축 후에 이 컨피그레이션을 추가로 관리할 수 있습니다. 이를테면 유휴 시간 초과 값을 낮게 설정된 기본값에서 변경할 수 있습니다.

단계 **1** Microsoft 계정 자격 증명을 사용하여 Azure 포털 (https://portal.azure.com)에 로그인합니다.

Azure 포털에서는 데이터 센터 위치와 상관없이 현재 계정 및 서브스크립션의 가상 요소를 보여줍니다.

단계 **2** **Create a Resource(**리소스 생성**)**를 클릭합니다.

단계 **3** Marketplace에서 "Cisco Firepower Management Center(FMCv)"를 검색하고 제품을 선택한 다음 **Create(**생성**)**을 클릭합니다.

단계 **4** 기본 설정을 구성합니다.

a) **Azure**의 **FMC VM** 이름 필드에 가상 머신의 이름을 입력합니다. 이 이름은 Azure 서브스크립션 내에서 고유해야 합니다.

주의 기존 이름을 사용하면 구축이 실패하므로 주의합니다.

b) (선택 사항)드롭 다운 목록에서 **FMC** 소프트웨어 버전을 선택합니다.

기본적으로 사용 가능한 최신 버전으로 설정해야 합니다.

c) 기본 계정의 사용자 이름 필드에 Azure 계정 관리자의 사용자 이름을 입력합니다.

이름 "admin"은 Azure에서 예약되어 있으므로 사용할 수 없습니다.

주의 여기에 입력된 사용자 이름은 FMCv 관리자 계정이 아닌 Azure 계정 용입니다. 이 사용자 이름을 사용하여 FMCv에 로그인하지 마십시오.

d) 권한 부여 유형을 비밀번호 또는 **SSH** 공용 키 중 하나로 선택합니다.

비밀번호를 선택할 경우 비밀번호를 입력하고 확인합니다. 비밀번호는 12자에서 72자 사이여야 하며 소문자 1개, 대문자 1개, 숫자 1개, '\'또는 '-'가 아닌 특수 문자 1개 중 3개를 포함해야 합니다.

SSH 공용 키를 선택하면, 원격 피어의 RSA 공용 키를 지정합니다.

e) FMCv의 **FMC** 호스트 이름을 입력합니다.

f) **Admin** 비밀번호를 입력합니다.

이는 FMCv를 구성하기 위해 관리자로서 FMCv 웹 인터페이스에 로그인할 때 사용할 비밀번호입니다.

g) 서브스크립션 유형을 선택합니다.

일반적으로 하나의 옵션만 나열됩니다.

h) 리소스 그룹을 생성합니다.

FMCv를 새 리소스 그룹에 구축해야 합니다. 기존 리소스 그룹에 구축하는 옵션은 기존 리소스 그룹이 비어 있는 경우에만 작동합니다.

그러나 나중 단계에서 네트워크 옵션을 구성할 때 다른 리소스 그룹의 기존 가상 네트워크에 FMCv를 연결할 수 있습니다.

i) 지리적 위치를 선택합니다.

이 구축에 사용된 모든 리소스에 대해 동일한 위치를 사용해야 합니다. FMCv, 네트워크, 스토리지 계정 등은 모두 동일한 위치를 사용해야 합니다.

j) **OK(**확인**)**를 클릭합니다.

단계 **5** 그런 다음 **Cisco FMCv Settings(Cisco FMCv** 설정) 아래에서 초기 컨피그레이션을 완료합니다.

a) 선택한 **Virtual machine size(**가상 머신 크기**)**를 확인하거나 **Change size(**크기 변경**)** 링크를 클릭하여 VM 크기 옵션을 확인합니다. **Select(**선택**)**를 클릭하여 확인합니다.

지원되는 가상 머신 크기만 표시됩니다.

b) 스토리지 계정을 구성합니다. 기존 스토리지 계정을 사용하거나 새로 만들 수 있습니다.

- 스토리지 계정의 **Name(**이름**)**을 입력한 다음 **OK(**확인**)**를 클릭합니다. 스토리지 계정 이름은 소문자와 숫자만 포함할 수 있습니다. 특수 문자는 포함할 수 없습니다.
- 이 릴리스부터 FMCv은 범용 표준 성능 스토리지만 지원합니다.

c) 공용 **IP** 주소를 구성합니다. 기존 IP를 사용하거나 새로 생성할 수 있습니다.

- **Create new(**새로 만들기**)**를 클릭하여 새 공용 IP 주소를 만듭니다. **Name(**이름**)** 필드에 IP 주소의 레이블을 입력하고 SKU 옵션으로 **Standard(**표준**)**를 선택한 다음 **OK(**확인**)**를 클릭합니다.

  참고 Azure는 이 단계에서 선택한 동적/고정 선택 항목에 관계 없이 동적 공용 IP 주소를 생성합니다. VM을 중지했다가 다시 시작하면 공용 IP가 변경될 수 있습니다. 고정 IP 주소를 선호할 경우 구축을 완료한 후에 포털에서 public-ip를 열고 동적 주소에서 고정 주소로 변경할 수 있습니다.

- 공용 IP 주소를 FMCv에 할당하지 않으려는 경우 **NONE(**없음**)**을 선택할 수 있습니다. 공용 IP 주소가 없으면 FMCv에 대한 모든 통신은 Azure 가상 네트워크 내에서 시작되어야 합니다.

d) 공용 IP의 레이블과 일치하는 **DNS** 레이블을 추가합니다.

FQDN(fully qualified domain name)은 DNS 레이블 + Azure URL이 됩니다. 즉 *<dnslabel>.<location>.cloupapp.azure.com*입니다.

e) 기존 가상 네트워크를 선택하거나 새로 만들고, **OK(**확인**)**를 클릭합니다.

f) FMCv에 대한 관리 서브넷을 구성합니다.

관리 서브넷 이름을 정의하고 관리 서브넷 접두사를 검토합니다. 권장되는 서브넷 이름은 "management"입니다.

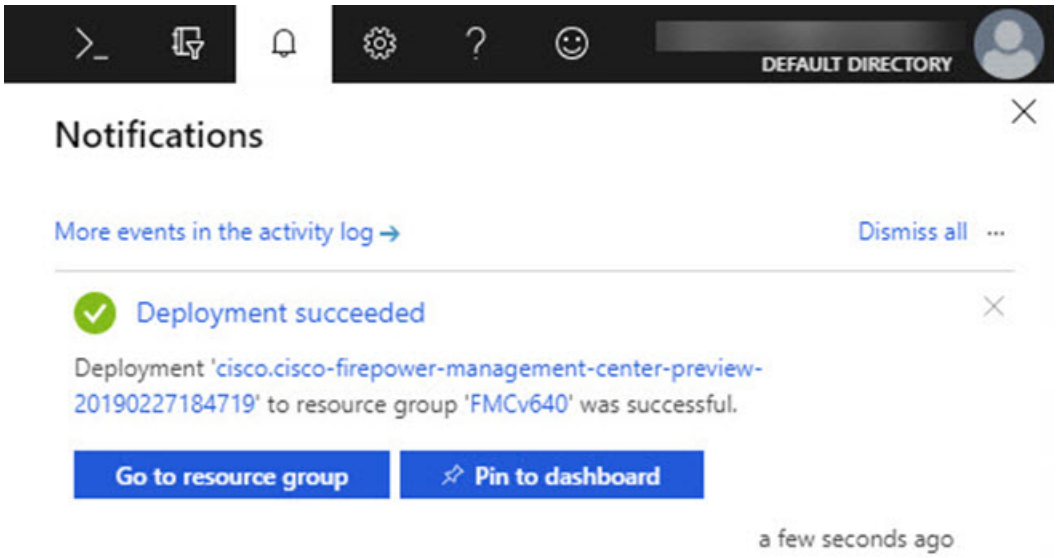
g) **OK(**확인**)**를 클릭합니다.

단계 **6** 컨피그레이션 요약을 본 다음 **OK(**확인**)**를 클릭합니다.

단계 **7** 이용 약관을 보고 **Create(**생성**)**를 클릭합니다.

단계 **8** 포털의 상단에서 알림(종 모양 아이콘)을 선택하여 구축 상태를 확인합니다.

그림 *1: Azure* 알림



여기에서 구축을 클릭하여 추가 세부 사항을 보거나 구축이 성공하면 리소스 그룹으로 이동할 수 있습니다. FMCv를 사용할 수 있을 때까지의 총 시간은 약 30분입니다. Azure에서는 구축 시간이 다양합니다. Azure가 FMCv VM이 실행 중임을 보고할 때까지 기다립니다.

단계 **9** (선택 사항) Azure는 부팅 진단 및 시리얼 콘솔을 포함하여 VM의 상태를 모니터링하는 데 도움이 되는 여러 도구를 제공합니다. 이러한 툴을 사용하면 가상 머신이 부팅될 때의 상태를 확인할 수 있습니다.

a) 왼쪽 메뉴에서 가상 머신을 선택합니다.

b) 목록에서 FMCv VM을 선택합니다. VM의 Overview(개요) 페이지가 열립니다.

c) **Support + troubleshooting(**지원 + 문제 해결**)** 섹션으로 스크롤하여 **Boot diagnostics(**부팅 진단**)** 또는 **Serial console(**시리얼 콘솔**)**을 선택합니다. 부팅 진단 스크린 샷 및 시리얼 로그가 있는 새 창이 열리거나 텍스트 기반 시리얼 콘솔이 열리고 연결이 시작됩니다.

부팅 진단 또는 시리얼 콘솔에 로그인 프롬프트가 표시되면 FMCv의 웹 인터페이스 준비 상태가 확인된 것입니다.

예제:

```
Cisco Firepower Management Center for Azure v6.4.0 (build 44)
FMCv64East login:
```

다음에 수행할 작업

- FMCv 구축에 성공했는지 확인하십시오. Azure 대시 보드에는 모든 관련 리소스(스토리지, 네트워크, 경로 테이블 등)와 함께 리소스 그룹 아래에 새 FMCv VM이 나열됩니다.

Firepower Management Center Virtual Deployment 확인

FMCv VM이 생성되면 Microsoft Azure 대시 보드가 리소스 그룹 아래에 새 FMCv VM을 나열합니다. 해당 스토리지 계정 및 네트워크 리소스도 생성 및 나열됩니다. 대시 보드는 Azure 자산의 통합보기를 제공하며 FMCv의 상태 및 성능을 한 눈에 쉽게 확인할 수 있는 평가를 제공합니다.

시작하기 전에

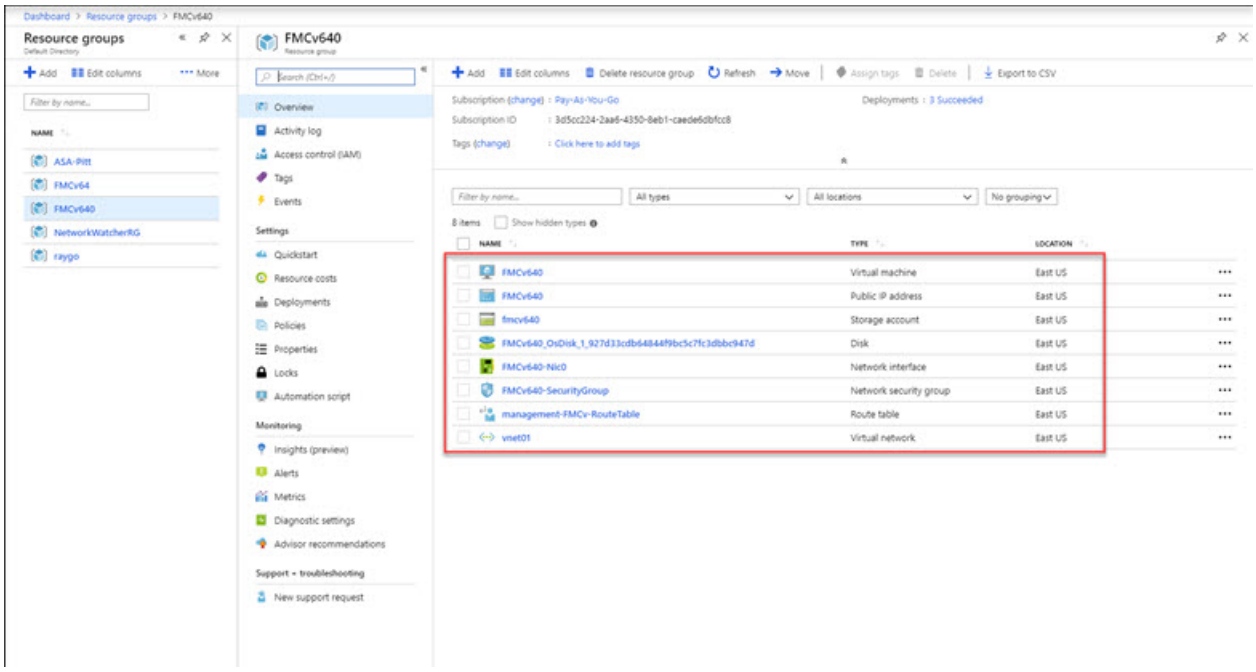
FMCv VM이 자동으로 시작됩니다. 구축 중에 Azure가 VM을 생성하는 동안 상태가 "Creating (생성)"으로 표시되고 구축이 완료되면 상태가 "Running (실행 중)"으로 변경됩니다.

참고 Azure에서는 구축 시간이 다르며 FMCv를 사용할 수 있을 때까지의 총 시간은 Azure 대시 보드에서 FMCv VM의 상태를 "Running (실행 중)"으로 표시하더라도 약 30분입니다.

단계 **1** 구축이 완료된 후 FMCv 리소스 그룹 및 해당 리소스를 보려면 왼쪽 메뉴 창에서 **Resource groups(**리소스 그룹**)**를 클릭하여 리소스 그룹 페이지에 액세스합니다.

다음 그림에는 Microsoft Azure 포털의 리소스 그룹 페이지 예가 나와 있습니다. FMCv VM과 해당 리소스를(스토리지 계정, 네트워크 리소스 등) 확인합니다.

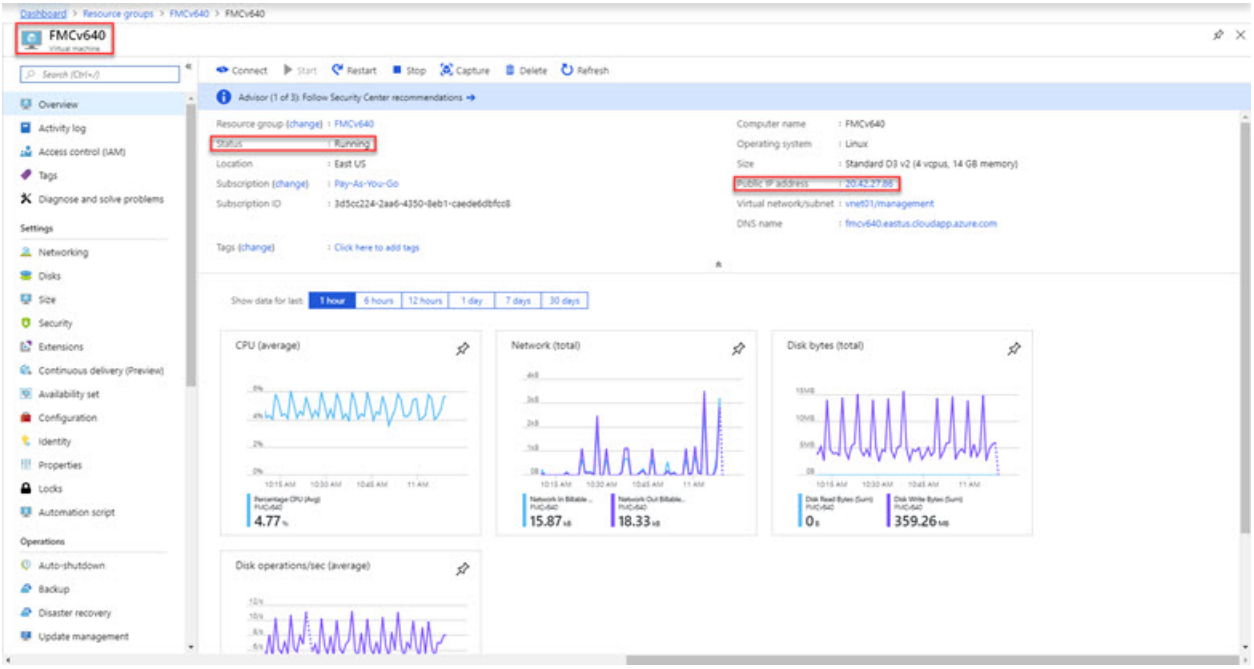
그림 ***2: Azure FMCv*** 리소스 그룹 페이지



단계 **2** 리소스 그룹과 연결된 FMCv VM의 세부 정보를 보려면 FMCv VM의 이름을 클릭합니다.

다음 그림에는 FMCv VM과 연결된 가상 머신 개요 페이지의 예가 나와 있습니다. 리소스 그룹 페이지에서 이 개요에 액세스할 수 있습니다.

그림 *3:* 가상 머신 개요



상태가 Running(실행 중)인지 확인합니다. Microsoft Azure 포털의 가상 머신 페이지에서 FMCv VM을 중지, 시작, 재시작 및 삭제할 수 있습니다. 이러한 컨트롤은 FMCv에 대한 정상 종료 메커니즘이 아닙니다. 정상 종료 정보는 지침 및 제한 사항, 49 페이지의 내용을 참조하십시오.

단계 **3** 가상 머신 페이지에서 FMCv에 할당된 공용 **IP** 주소를 찾습니다.

참고 IP 주소 위에 마우스를 올려 놓고 **Click to copy(**클릭하여 복사**)**를 선택하여 IP 주소를 복사할 수 있습니다.

단계 **4** 브라우저에서 **https://***public_ip*/로 이동합니다. 여기에서 *public_ip*는VM을 구축할 때 FMCv의 관리 인터페이스에 할당된 IP 주소입니다.

로그인 페이지가 나타납니다.

단계 **5** 사용자 이름으로 **admin**을 사용하고 VM 구축 시 지정한 관리자 계정의 비밀번호를 사용하여 로그인합니다.

다음에 수행할 작업

- 사용자를 생성하고 상태 및 시스템 정책을 검토하는 등 구축을 보다 쉽게 관리할 수 있는 몇 가지 관리 작업을 완료하는 것이 좋습니다. 시작 방법에 대한 개요는 Firepower Management Center Virtual 초기 관리 및 구성, 77 페이지를 참조하십시오.
- 또한 디바이스 등록 및 라이선싱 요건도 검토해야 합니다.

- Firepower 시스템 구성을 시작하는 방법에 대한 자세한 내용은 해당 소프트웨어 버전의 Firepower Management Center Configuration Guide 원본을 참조하십시오.

모니터링 및 문제 해결

이 섹션에는 Micosoft Azure에 구축 된 어플라이언스에 대한 일반적인 모니터링 및 문제 해결 지침이 포함되어 있습니다.Firepower Management Center Virtual 모니터링 및 문제 해결은 Azure의 VM 구축 또는 FMCv 어플라이언스 자체와 관련될 수 있습니다.

VM 구축의 **Azure** 모니터링

Azure는 **Support + Troubleshooting(**지원 + 문제 해결**)** 메뉴 아래에서 도구 및 리소스에 빠르게 액세스하여 문제를 진단하고 해결하고 추가 지원을 받을 수 있는 여러 도구를 제공합니다. 두 가지 주요 사항은 다음과 같습니다.

- 부팅 진단 - 부팅 시 FMCv VM의 상태를 확인할 수 있습니다. 부팅 진단은 VM과 스크린 샷에서 시리얼 로그 정보를 수집합니다. 이렇게 하면 시동 문제를 진단하는 데 도움이 됩니다.
- 시리얼 콘솔 - Azure 포털의 VM 시리얼 콘솔은 텍스트 기반 콘솔에 대한 액세스를 제공합니다. 이 직렬 연결은 가상 머신의 COM1 직렬 포트에 연결되어 FMCv에 할당된 공용 IP 주소를 사용하여의 FMCv의 명령 줄 인터페이스에 대한 직렬 및 SSH 액세스를 제공합니다.

FMCv 모니터링 및 로깅

트러블 슈팅 및 일반 로깅 작업은 현재 FMC 및 FMCv 모델과 동일한 절차를 따릅니다. 사용 중인 버전의 *Firepower Management Center Configuration Guide*에서 시스템 모니터링 및 문제 해결 섹션을 참조하십시오.

또한 Microsoft Azure Linux Agent(waagent)는 Linux 프로비저닝 그리고 Azure 패브릭 컨트롤러와의 VM 상호 작용을 관리합니다. 따라서 다음은 문제 해결을 위한 중요한 로그입니다.

- **/var/log/waagent.log** - 이 로그에는 Azure를 사용한 FMC 프로비저닝에서 오류가 발생합니다.
- **/var/log/firstboot.S07install_waagent** - 이 로그에는 waagent 설치의 오류가 발생합니다.

Azure 프로비저닝 실패

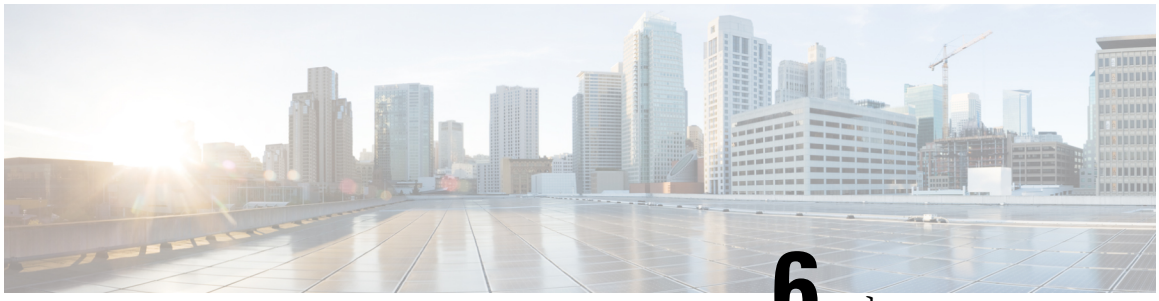
Azure Marketplace 솔루션 템플릿을 사용한 프로비저닝 오류는 드문 경우입니다. 그러나 프로비저닝 오류가 발생하는 경우 다음 사항에 유의하십시오.

- Azure는 가상 머신이 waagent와 함께 프로비저닝되는 데 20분의 시간 초과가 있으며, 이 시간이 초과되면 재부팅됩니다.
- FMC가 어떤 이유로든 프로비저닝하는 데 문제가 있는 경우, FMC 데이터베이스 초기화 중에 20분 타이머가 종료되는 경향이 있으며, 이로 인해 구축이 실패할 수 있습니다.
- 20분 내에 FMC가 프로비저닝되지 않으면 처음부터 다시 시작하는 것이 좋습니다.
- 문제 해결 정보는 */var/log/waagent.log*를 참조하십시오.

- 직렬 콘솔에 HTTP 연결 오류가 표시되는 경우, 이는 waagent가 패브릭과 통신할 수 없음을 나타냅니다. 재구축 시 네트워크 설정을 검토해야 합니다.

Microsoft Azure Cloud의 FMCv 히스토리

기능 이름	릴리스	기능 정보
Microsoft Azure 퍼블릭 클라우드에서 Firepower Management Center Virtual(FMCv)을 구축합니다.	6.4.0	초기 지원.



6 장

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 *8:* 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

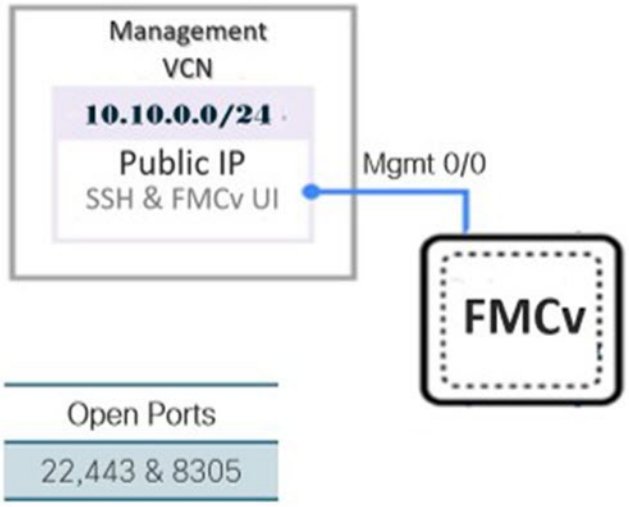
지원되지 않는 기능

- 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 *4: 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.

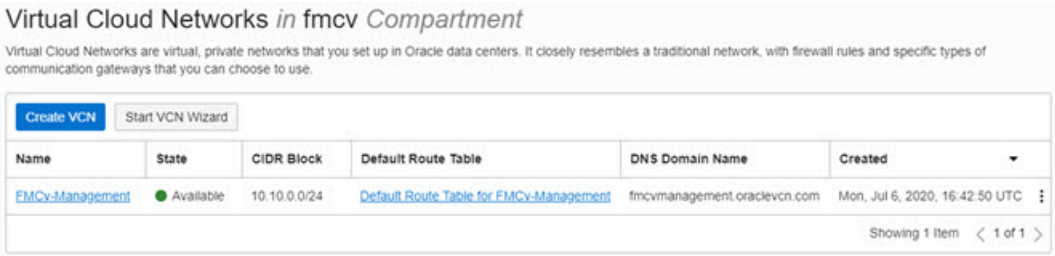
단계 **8** 이전에 생성한 보안 목록을 선택합니다.

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 *5: 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, 59 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.

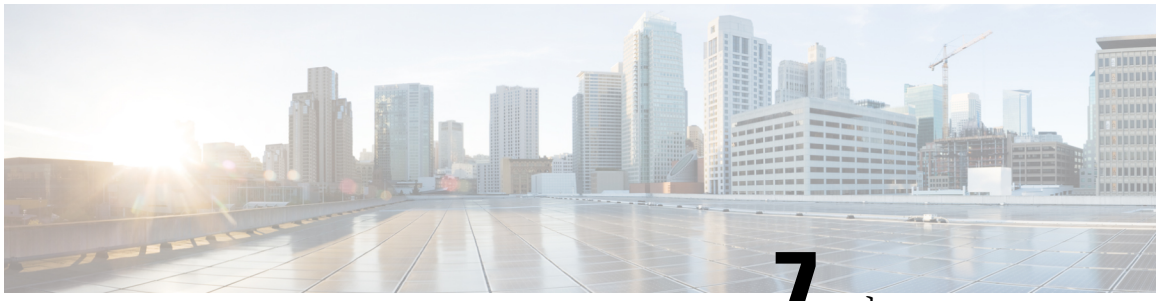
```
$ ssh –i <private_key> <username>@<public-ip-address>
```

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.



7 장

Firepower Management Center Virtual 초기 설정

이 장에서는 Firepower Management Center Virtual(FMCv) 어플라이언스를 구축한 후에 수행해야 하는 초기 설정 프로세스에 대해 설명합니다.

CLI(버전 6.5 이상)을 이용한 FMC 초기 설정

FMCv 구축이 끝나면 초기 설정을 위해 어플라이언스 콘솔에 액세스할 수 있습니다.웹 인터페이스를 사용하는 대신 CLI를 사용하여 초기 설정을 수행할 수 있습니다. 초기 구성 마법사를 완료해, 새 어플라이언스가 신뢰하는 관리 네트워크와 통신하도록 구성해야 합니다. 마법사를 완료하려면 최종 사용자 라이선스 계약(EULA)에 동의하고 관리자 비밀번호를 변경해야 합니다.

시작하기 전에

- FMCv 이(가) 관리 네트워크에서 통신하는 데 필요한 다음 정보가 있는지 확인합니다.
  - IPv4 관리 IP 주소

    FMC 관리 인터페이스는 DHCP에서 할당한 IP4 주소를 수락하도록 사전 구성되어 있습니다. 시스템 관리자에게 문의해 DHCP가 FMC MAC 주소에 할당하도록 구성된 IP 주소를 확인합니다. DHCP를 사용할 수 없는 상황이라면, FMC 관리 인터페이스는 IPv4 주소 192.168.45.45를 사용합니다.
  - 네트워크 마스크 및 기본 게이트웨이(DHCP를 사용하지 않는 경우)

단계 **1** 사용자 이름으로 **admin**을 사용하고 관리자 계정의 비밀번호로 **Admin123**을 사용하여 콘솔에서 FMCv 에 로그인합니다. 비밀번호는 대/소문자를 구분합니다.

단계 **2** 메시지가 표시되면 **Enter**를 눌러 최종 사용자 라이선스 계약(EULA)을 표시합니다.

단계 **3** EULA를 검토합니다. 메시지가 표시되면 예, **YES**를 입력하거나 **Enter**를 눌러 EULA에 동의합니다.

중요 EULA를 수락하지 않으면 마법사를 진행할 없습니다. 예, **YES** 또는 **Enter** 이외의 선택을 하면 시스템에서 로그아웃됩니다.

단계 **4** 시스템 보안 및 개인정보 보호를 위해, FMC에 처음 로그인하면 관리자 비밀번호를 변경해야 합니다. 새 비밀번호를 요구하는 메시지가 표시되면, 화면에 표시되는 제한을 준수하는 새 비밀번호를 입력하고 확인 메시지가 나오면 같은 메시지를 다시 입력하십시오.

참고 FMC은(는) 비밀번호를 비밀번호 크래킹 사전과 대조해, 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열과 일치하는지 확인합니다. 예를 들어 초기 구성 스크립트는 'abcdefg'나 'passw0rd' 같은 비밀번호는 거부합니다.

참고 초기 구성 프로세스가 끝나면 시스템은 사용자의 버전에 맞는 *Firepower Management Center* 구성 가이드에서 설명하는 강력한 비밀번호 요구 사항을 준수하는 값을 두 관리자 계정(웹 액세스용 계정과 CLI 액세스용 계정)에 설정합니다. 나중에 아무 관리자 계정의 비밀번호를 변경하면 두 계정의 비밀번호가 달라지며, 강력한 비밀번호 요건이 웹 인터페이스 관리자 계정에 적용되지 않게 됩니다.

단계 **5** 메시지에 응답하여 네트워크 설정을 구성합니다.

선택형 질문의 경우 선택지는 **(y/n)** 처럼 괄호 안에 나열됩니다. 기본값은 **[y]** 처럼 대괄호 안에 나열됩니다. 메시지에 응답할 때는 다음 사항에 유의하십시오.

- **Enter**키를 눌러 기본값을 수락합니다.
- 호스트 이름에는 FQDN(`<hostname>.<domain>`)이나 호스트 이름을 입력합니다. 필수 필드입니다.
- IPv4를 수동으로 구성한다면, 시스템은 IPv4 주소, 넷마스크 및 기본 게이트웨이를 묻습니다. DHCP를 선택하면 시스템은 DHCP를 사용하여 이러한 값을 할당합니다. DHCP를 사용하지 않기로 했다면 해당 필드의 값을 직접 입력해야 합니다. 점으로 구분되는 표준 10진수 표기법을 사용하십시오.
- DNS 서버 구성은 선택 사항입니다. DNS 서버를 지정하지 않으려면 **none (없음)** 을 입력하십시오. DNS 서버를 지정하려면 DNS 서버 1~2개에 대한 IPv4 서버를 지정해야 합니다. 주소 2개를 지정하려면 쉼표로 주소를 구분해야 합니다. (두 개 이상의 DNS 서버를 지정하는 경우 시스템은 추가 항목을 무시합니다.) FMC에서 인터넷에 액세스할 수 없는 경우 로컬 네트워크 외부에서 DNS를 사용할 수 없습니다.

  참고 평가 라이선스를 사용하는 경우 현재 DNS 지정은 선택 사항이지만 구축에 영구 라이선스를 사용하려면 DNS가 필요합니다.

- 네트워크에서 연결할 수 있는 하나 이상의 NTP 서버에 FQDN(Fully Qualified Domain Name)이나 IP 주소를 입력해야 합니다. (DHCP를 사용하지 않는 경우 NTP 서버에 대해 FQDN을 지정할 수 없습니다.) 서버 2개(기본 서버와 보조 서버)를 지정할 수도 있습니다. 두 서버는 쉼표로 구분해야 합니다. (두 개 이상의 DNS 서버를 지정하는 경우 시스템은 추가 항목을 무시합니다.) FMC에서 인터넷에 액세스할 수 없는 경우 로컬 네트워크 외부에서 NTP 서버를 사용할 수 없습니다.

예제**:**

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
```

```
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

단계 **6** 시스템에서 구성 선택 요약이 표시됩니다. 입력한 설정을 검토합니다.

예제:

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

단계 **7** 최종 프롬프트에서 설정을 확인할 수 있습니다.

- 설정이 올바른 경우, 설정을 적용한 후 계속하려면 **y**를 입력하고 **Enter** 키를 누릅니다.
- 설정이 잘못된 경우, **n**을 입력하고 **Enter** 키를 누릅니다. 시스템은 정보를 다시 요구하며, 가장 먼저 호스트 이름부터 입력해야 합니다.

예제:

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

단계 **8** 설정에 동의했다면 **exit(**종료**)**를 눌러 FMC CLI에서 나갑니다.

다음에 수행할 작업

- 방금 구성한 네트워크 정보를 사용하여 FMCv 웹 인터페이스에 연결할 수 있습니다.
- 초기 컨피그레이션 프로세스의 일부로서 FMC가 자동으로 구성하는 주별 유지 보수 활동을 검토합니다. 이러한 활동은 시스템을 최신 상태로 유지하고 데이터를 백업하기 위한 것입니다. 자동 초기 구성(버전 6.5 이상) 검토, 75 페이지을(를) 참조하십시오.
- 초기 설정이 끝나면 사용자의 버전에 맞는 Firepower Management Center 구성 가이드에서 설명하는 웹 인터페이스를 이용해, IPv6 주소 지정을 위한 FMC을(를) 구성할 수 있습니다.

웹 인터페이스(버전 6.5 이상)를 이용한 초기 설정

FMCv 구축 후 어플라이언스 웹 인터페이스에서 HTTPS를 사용하여 초기 설정을 수행할 수 있습니다.

처음으로 FMC 웹 인터페이스에 로그인하는 경우 FMC가 초기 구성 마법사를 제시하여 어플라이언스에 대한 기본 설정을 빠르고 쉽게 구성할 수 있도록 합니다. 이 마법사는 화면 3개와 팝업 대화상자 하나로 구성됩니다.

- 첫 번째 화면에서는 관리자 사용자의 비밀번호 기본값인 **Admin123**을 변경해야 합니다.
- 두 번째 화면에는 어플라이언스를 사용하기 전에 동의해야 하는 최종 사용자 라이선스 계약(EULA)이 표시됩니다.
- 세 번째 화면에서는 어플라이언스 관리 인터페이스에 대한 네트워크 설정을 변경할 수 있습니다. 이 페이지는 현재 설정이 미리 입력되어 있으며, 값을 변경해도 됩니다.
- 마법사는 사용자가 이 화면에서 입력한 값에 대한 유효성 검사를 수행하여 다음을 확인합니다.
  - 구문상 정확성
  - 입력한 값의 호환성(호환되는 IP 주소 및 게이트웨이, 또는 FQDN을 이용해 NTP 서버를 지정할 때 제공된 DNS 등)
  - FMCv 및 DNS와 NTP 서버 간의 네트워크 연결

  마법사는 이러한 테스트 결과를 화면에 실시간으로 표시하면, 따라서 사용자는 수정 사항을 적용하고 구성이 어떻게 보이는지 확인한 다음 화면 아래에 있는 **Finish(**완료**)**를 클릭하면 됩니다. NTP 및 DNS 연결 테스트는 비차단 방식입니다. 마법사가 연결 테스트를 완료하기 전에 **Finish(**완료**)**를 클릭해도 됩니다. **Finish(**완료**)**를 클릭했는데 시스템에서 연결 문제를 보고한다면, 마법사의 설정을 바꾸지 마십시오. 초기 설정 완료 후 웹 인터페이스를 이용해 연결을 구성해야 합니다.

  FMCv 미 브라우저 간의 기존 연결을 해제하는 구성 값을 입력했다면, 시스템은 연결성 테스트를 수행하지 않습니다. 이 경우 마법사에는 DNS나 NTP에 대한 연결 상태 정보를 표시하지 않습니다.
- 마법사 화면 3개를 모두 끝내면 팝업 대화상자가 나타나, 스마트 라이선싱을 쉽고 빠르게 설정할 수 있습니다(선택 사항).

초기 구성 마법사를 완료하고 스마트 라이선싱 대화상자를 입력하거나 무시하면, 시스템은 사용자의 버전에 대한 Firepower Management Center Configuration Guide의 '장치 관리 기본 사항'에서 설명하는 디바이스 관리 페이지를 표시합니다.

시작하기 전에

- FMC이(가) 관리 네트워크에서 통신하는 데 필요한 다음 정보가 있는지 확인합니다.
  - IPv4 관리 IP 주소

    FMC 관리 인터페이스는 DHCP에서 할당한 IP4 주소를 수락하도록 사전 구성되어 있습니다. 시스템 관리자에게 문의해 DHCP가 FMC MAC 주소에 할당하도록 구성된 IP 주소를 확인합니다. DHCP를 사용할 수 없는 상황이라면, FMC 관리 인터페이스는 IPv4 주소 192.168.45.45를 사용합니다.
  - 네트워크 마스크 및 기본 게이트웨이(DHCP를 사용하지 않는 경우)
- DHCP를 사용하지 않을 경우 다음 네트워크 설정을 사용하여 로컬 컴퓨터를 구성합니다.
  - IP 주소: 192.168.45.2
  - Netmask: 255.255.255.0

- 기본 게이트웨이: 192.168.45.1

이 컴퓨터상의 다른 네트워크 연결을 비활성화합니다.

단계 **1** 웹 브라우저를 사용하여 FMCv IP 주소인 *https://<FMC-IP>*로 이동합니다.

로그인 페이지가 나타납니다.

단계 **2** 사용자 이름으로 **admin**을 사용하고 관리자 계정의 비밀번호로 **Admin123**을 사용하여 FMCv에 로그인합니다. (비밀번호는 대/소문자를 구분합니다.)

단계 **3** **Change Password(**비밀번호 변경**)** 화면에서 다음을 수행합니다.

a) (선택 사항) **Show password(**비밀번호 표시**)** 확인란을 선택하면 이 화면을 이용하는 동안 비밀번호를 확인할 수 있습니다.

b) (선택 사항) **Generate Password(**비밀번호 생성**)** 버튼을 클릭하면 나열된 기준을 준수하는 비밀번호를 시스템이 대신 생성합니다. (이렇게 생성되는 비밀번호는 기억하기가 쉽지 않습니다. 이 옵션을 선택한다면 비밀번호를 기록해 두십시오.)

c) 원하는 비밀번호를 설정하려면 **New Password(**새 비밀번호**)**와 **Confirm Password(**비밀번호 확인**)** 텍스트 상자에 새 비밀번호를 입력합니다.

비밀번호는 대화 상자에 나열된 기준을 준수해야 합니다.

참고 FMC은(는) 비밀번호를 비밀번호 크래킹 사전과 대조해, 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열과 일치하는지 확인합니다. 예를 들어 초기 구성 스크립트는 'abcdefg'나 'passw0rd' 같은 비밀번호는 거부합니다.

참고 초기 구성 프로세스가 끝나면 시스템은 두 관리자 계정(웹 액세스용 계정과 CLI 액세스용 계정)에 같은 비밀번호 값을 설정합니다. 비밀번호는 사용자의 버전에 맞는 Firepower Management Center Configuration Guide에서 설명하는 강력한 비밀번호 요건을 충족해야 합니다. 나중에 아무 관리자 계정의 비밀번호를 변경하면 두 계정의 비밀번호가 달라지며, 강력한 비밀번호 요건이 웹 인터페이스 관리자 계정에 적용되지 않게 됩니다.

d) **Next(**다음**)**를 클릭합니다.

Change Password(비밀번호 변경**)** 화면에서 **Next(**다음**)**를 클릭하고 마법사는 새 관리자 비밀번호를 수락하면, 남은 마법사 작업을 수행하지 않아도 비밀번호가 웹 인터페이스와 CLI 관리자 계정 모두에 적용됩니다.

단계 **4** **User Agreement(**사용자 계약**)** 화면에서 EULA를 읽고 **Accept(**수락**)**을 클릭하여 계속 진행합니다.

Decline(거절**)**을 클릭하면 FMCv에서 로그아웃하게 됩니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** **Change Network Settings(**네트워크 설정 변경**)** 화면에서 다음을 수행합니다.

a) **FQDN(Fully Qualified Domain Name)**을 입력합니다. 기본값이 표시되면 네트워크 컨피그레이션과 호환되는 경우 이 값을 사용할 수 있습니다. 그렇지 않은 경우 정규화된 호스트 이름(syntax `<hostname>.<domain>`) 또는 호스트 이름을 입력합니다.

b) **Configure IPV4(IPV4** 구성**)** 옵션의 부트 프로토콜을 **Using DHCP(DHCP** 사용**)** 또는 **Using Static/Manual(**고정/수동 사용**)**로 선택합니다.

c) **IPV4 Address(IPV4** 주소**)**에 대해 표시되는 값을 수락하거나 새 값을 입력합니다. 점으로 구분된 10진수 형식(예: 192.168.45.45)을 사용합니다.

참고 초기 컨피그레이션 중에 IP 주소를 변경하는 경우 새 네트워크 정보를 사용하여 FMC에 다시 연결해야 합니다.

d) **Network Mask(**네트워크 마스크**)**에 대해 표시되는 값을 수락하거나 새 값을 입력합니다. 점으로 구분된 10진수 형식(예: 255.255.0.0)을 사용합니다.

참고 초기 컨피그레이션 중에 네트워크 마스크를 변경하는 경우 새 네트워크 정보를 사용하여 FMC에 다시 연결해야 합니다.

e) **Gateway(**게이트웨이**)**에 대해 표시된 값을 수락하거나 새 기본 게이트웨이를 입력합니다. 점으로 구분된 10진수 형식(예: 192.168.0.1)을 사용합니다.

참고 초기 컨피그레이션 중에 게이트웨이 주소를 변경하는 경우 새 네트워크 정보를 사용하여 FMC에 다시 연결해야 할 수 있습니다.

f) (선택 사항) **DNS Group(DNS** 그룹**)**에서 기본값인 **Cisco Umbrella DNS**를 수락합니다.

DNS 설정을 변경하려면 드롭다운 목록에서 **Custom DNS Servers(**사용자 지정 **DNS** 서버**)**를 선택하고, **Primary DNS(**기본 **DNS)** 및 **Secondary DNS(**보조 **DNS)**에 IPv4 주소를 입력합니다. FMC에서 인터넷에 액세스할 수 없는 경우 로컬 네트워크 외부에서 DNS를 사용할 수 없습니다. 드롭다운 목록에서 **Custom DNS Servers(**사용자 지정 **DNS** 서버**)**를 선택하고 **Primary DNS(**기본 **DNS)** 및 **Secondary DNS(**보조 **DNS)** 필드를 입력하지 않으면 DNS 서버를 구성하지 않습니다.

참고 NTP 서버를 지정하기 위해 IP 주소 대신 FQDN을 사용하는 경우 지금 DNS를 지정해야 합니다. 평가 라이선스를 사용하는 경우 DNS는 선택 사항이지만 구축에 영구 라이선스를 사용하려면 DNS가 필요합니다.

g) **NTP Group Servers(NTP** 그룹 서버**)**에는 기본값인 **Default NTP Servers(**기본 **NTP** 서버**)**를 수락할 수 있습니다. 이 경우 시스템은 **0.sourcefire.pool.ntp.org**를 기본 NTP 서버로, **1.sourcefire.pool.ntp.org**를 보조 NTP 서버로 사용합니다.

다른 NTP 서버를 구성하려면 드롭다운 목록에서 **Custom NTP Group Servers(**사용자 지정 **NTP** 그룹 서버**)**를 선택하고, 네트워크에서 연결할 수 있는 NTP 서버 하나 또는 두 개의 FQDN 또는 IP 주소를 입력합니다. FMC에서 인터넷에 액세스할 수 없는 경우 로컬 네트워크 외부에서 NTP 서버를 사용할 수 없습니다.

참고 초기 컨피그레이션 중에 네트워크 설정을 변경하는 경우 새 네트워크 정보를 사용하여 FMC에 다시 연결해야 합니다.

단계 **7** **Finish(**마침**)**를 클릭합니다.

마법사는 이 화면에서 입력한 값의 유효성 검사를 실시해 구문상 정확성, 입력한 값의 호환성, FMC와(과) DNS 및 NTP 서버 간의 네트워크 연결을 확인합니다. **Finish(**완료**)**를 클릭했는데 시스템에서 연결 문제를 보고한다면, 마법사의 설정을 바꾸지 마십시오. 초기 설정 완료 후 FMC 웹 인터페이스를 이용해 연결을 구성해야 합니다.

다음에 수행할 작업

- 스마트 라이선싱을 빠르고 쉽게 설정할 수 있는 팝업 대화상자가 표시됩니다. 이 대화상자 사용은 선택 사항입니다. FMCv에서 Firepower Threat Defense 디바이스를 관리하며 스마트 라이선싱이 익숙하시다면 이 대화상자를 사용하십시오. 그렇지 않다면 대화상자를 무시하고, 버전에 맞는 Firepower Management Center 구성 가이드의 'Firepower 시스템 라이선싱'을 참조하십시오.
- 초기 컨피그레이션 프로세스의 일부로서 FMC가 자동으로 구성하는 주별 유지 보수 활동을 검토합니다. 이러한 활동은 시스템을 최신 상태로 유지하고 데이터를 백업하기 위한 것입니다. 자동 초기 구성(버전 6.5 이상) 검토, 75 페이지을(를) 참조하십시오.
- 초기 구성 마법사를 완료하고 스마트 라이선싱 대화상자를 입력하거나 무시하면, 시스템은 *Firepower Management Center Configuration Guide*의 '장치 관리 기본 사항'에서 설명하는 디바이스 관리 페이지를 표시합니다.
- 초기 설정이 끝나면 사용자의 버전에 맞는 Firepower Management Center 구성 가이드에서 설명하는 웹 인터페이스를 이용해, IPv6 주소 지정을 위한 FMC을(를) 구성할 수 있습니다.

자동 초기 구성(버전 6.5 이상) 검토

(초기 구성 마법사나 CLI로 수행하는) 초기 구성 과정에서 FMC은(는) 유지관리 작업을 자동으로 구성해 시스템을 최신 상태로 유지하고 데이터를 백업합니다.

이러한 작업은 UTC 기준으로 예약되며, 따라서 사용자가 있는 곳의 날짜에 따라 지역적으로 실행됩니다. 또한 작업은 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받는다면, 예약된 작업은 현지 시간에 따라 여름에는 겨울보다 1시간 '후'에 실행됩니다

참고 자동 예약 구성을 검토하고 FMC가 그들을 성공적으로 설정하고 필요에 따라 조정했는지를 확인할 것을 강력하게 권장합니다.

- 주간 GeoDB 업데이트

  FMC에서는 GeoDB 업데이트가 매주 같은 무작위 선정 시간에 진행되도록 자동 예약됩니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 웹 인터페이스의 **System(**시스템**)** > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**> **Recurring Geolocation Updates(**반복 위치 업데이트**)**에서 이 자동 업데이트에 대한 구성을 볼 수 있습니다. 시스템이 업데이트를 구성하지 못하고 FMC이(가) 인터넷에 액세스할 수 있다면, 사용자의 버전에 맞는 Firepower Management Center 구성 가이드의 설명에 따라 정기 GeoDB 업데이트를 구성할 것을 강력하게 권장합니다.

- 주간 FMC 소프트웨어 업데이트

  FMC에서는 주간 작업을 자동으로 예약하여 FMC 및 매니지드 디바이스의 최신 소프트웨어를 다운로드합니다. 이 작업은 일요일 오전 2~3시 UTC에 진행되도록 예약됩니다. 따라서 날짜와 사용자의 위치에 따라 현지 시간 기준 토요일 오후에서 일요일 오후 사이에 진행될 수 있습니다.

웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 웹 인터페이스의 **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**에서 이 작업에 대한 구성을 볼 수 있습니다. 작업 예약이 실패하고 FMC이(가) 인터넷에 액세스할 수 있다면, 사용자의 버전에 맞는 Firepower Management Center 구성 가이드의 설명에 따른 소프트웨어 업데이트 다운로드 반복 작업 예약을 강력하게 권장합니다.

이 작업은 어플라이언스에서 현재 실행 중인 버전에 대한 소프트웨어 패치와 핫픽스 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.

- 주간 FMC 구성 백업

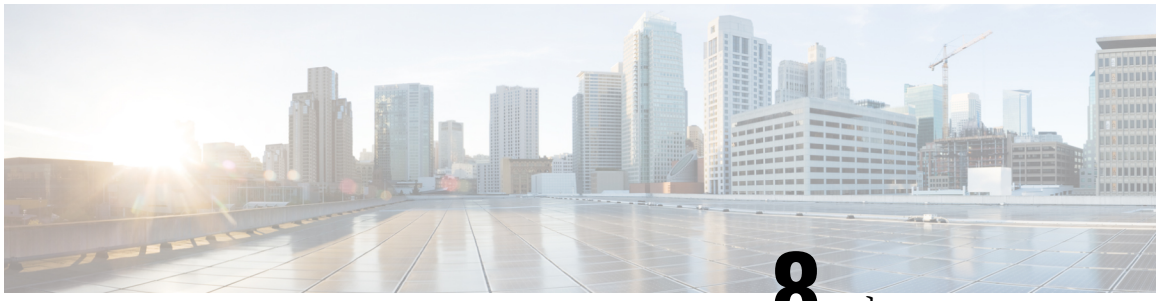
  FMC에서는 로컬에 저장한 구성 전용 백업을 월요일 오전 2시 UTC에 실행하도록 주간 작업을 자동 예약합니다. 따라서 날짜와 사용자의 위치에 따라 현지 시간 기준 토요일 오후에서 일요일 오후 사이에 진행될 수 있습니다 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 웹 인터페이스의 **System(**시스템**)** > **Tools(**툴**)** > **Scheduling(**예약**)**에서 이 작업에 대한 구성을 볼 수 있습니다. 작업 예약이 실패한다면, 사용자의 버전에 맞는 Firepower Management Center 구성 가이드의 설명에 따른 백업 실행 반복 작업 예약을 강력하게 권장합니다.

- 취약성 데이터베이스 업데이트

  버전 6.6 이상에서 FMC는 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 시스템을 최신 상태로 유지할 수 있도록 FMC가 인터넷에 액세스할 수 있다면 사용자의 버전에 맞는 Firepower Management Center Configuration Guide의 설명에 따라 VDB 업데이트 다운로드를 자동으로 반복할 수 있는 작업을 예약하는 것이 좋습니다.

- 일일 침입 규칙 업데이트

  버전 6.6 이상에서 FMC는 Cisco 지원 사이트에서 매일 자동 침입 규칙 업데이트를 구성합니다. FMC는 다음에 영향을 받는 정책을 구축하는 경우 영향을 받는 관리되는 디바이스에 자동으로 침입 규칙 업데이트를 구축합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 웹 인터페이스의 **System(**시스템**)** > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**에서 이 작업에 대한 구성을 볼 수 있습니다. 업데이트 구성에 실패하고 FMC가 인터넷에 액세스할 수 있다면 버전에 맞는 Firepower Management Center Configuration Guide의 설명에 따라 정기 침입 규칙 업데이트를 구성하는 것이 좋습니다.



8 장

Firepower Management Center Virtual 초기 관리 및 구성

Firepower Management Center Virtual(FMCv)의 초기 설정 프로세스를 완료하고 성공 여부를 확인한 후, 구축을 쉽게 관리할 수 있게 해주는 다양한 관리 작업을 완료하는 것이 좋습니다. 또한 라이선싱 등 초기 설정 시 건너뛴 작업을 완료해야 합니다. 다음 섹션에서 설명하는 작업에 대한 자세한 내용과 구축 구성을 시작하는 방법에 대한 내용은 사용 중인 버전에 대한 전체 Firepower Management Center 설정 가이드를 참조하십시오.

개인 사용자 계정

초기 설정을 완료하고 나면, 웹 인터페이스 사용자는 시스템에 단 1명만 남게 됩니다. 바로 관리자 역할 및 액세스 권한을 가진 관리자 사용자입니다. 해당 역할의 사용자는 시스템의 모든 메뉴 및 구성에 액세스할 수 있습니다. 보안 및 감사를 위해, 관리자 계정(및 관리자 역할)의 사용은 제한하는 것이 좋습니다. FMC GUI의 **System(**시스템**)** > **Users(**사용자**)** > **User(**사용자**)** 페이지에서 사용자 계정을 관리합니다.

참고 셸을 사용하여 FMC에 액세스하는 관리자 계정은 웹 인터페이스를 사용하여 FMC에 액세스하는 관리자 계정과 다르며, 다른 비밀번호를 사용할 수 있습니다.

시스템을 사용할 각 사용자에 대해 별도의 계정을 만든다면, 조직은 각 사용자의 작업과 각 사용자에 의한 변경 사항을 감사할 수 있을 뿐만 아니라 각 사용자와 관련된 사용자 액세스 역할을 제한할 수 있습니다. 이러한 조치는 대부분의 컨피그레이션 및 분석 작업을 수행하는 FMC에서 특히 중요합니다. 예를 들어, 분석가는 네트워크 보안을 분석하기 위해 이벤트 데이터에 대한 액세스가 필요할 수 있지만 구축 관리 기능에는 액세스가 필요하지 않을 수 있습니다.

시스템에는 웹 인터페이스를 사용하는 다양한 관리자 및 분석가에게 맞게 설계된 10개의 사전 정의된 사용자 역할이 있습니다. 또한 특수 액세스 권한을 가지는 맞춤형 사용자 역할을 생성할 수도 있습니다.

Device Registration

FMC에서는 현재 Firepower System에서 지원하는 모든 디바이스(물리적 또는 가상)를 관리할 수 있습니다.

- Firepower Threat Defense- 통합 차세대 방화벽 및 차세대 IPS 디바이스를 제공합니다.
- Firepower Threat Defense Virtual- 여러 하이퍼바이저 환경에서 작동하도록 설계된 64비트 가상 디바이스는 관리 오버헤드를 줄이고 운영 효율성을 높입니다.
- Cisco ASA with FirePOWER Services(또는 ASA FirePOWER 모듈) - 최우선 시스템 정책을 제공하고 검색 및 액세스 제어를 위해 Firepower System에 트래픽을 전달합니다. 그러나 FMC 웹 인터페이스를 사용하여 ASA FirePOWER 인터페이스를 구성할 수 없습니다. Cisco ASA with FirePOWER Services에는 시스템을 설치하고 기타 플랫폼별 관리 작업을 수행하는 데 사용할 수 있는 ASA 플랫폼에 대해 고유한 CLI 및 소프트웨어가 있습니다.
- 7000 및 8000 Series 어플라이언스 - Firepower System용으로 설계된 물리적 디바이스입니다. 7000 및 8000 Series 디바이스에는 다양한 처리량이 있지만 대부분의 동일한 기능을 공유합니다. 일반적으로 8000 Series 디바이스는 7000 시리즈 디바이스보다 강력하며, 8000 Series fastpath 규칙, 링크 어그리게이션 및 스태킹 등의 추가 기능도 지원합니다. 디바이스를 FMC에 등록하기 전에 반드시 디바이스에 원격 관리를 구성해야 합니다.
- NGIPSv - VMware VSphere 환경에 구축된 64비트 가상 디바이스입니다. NGIPSv 디바이스에서는 이중화 및 리소스 공유, 스위칭, 라우팅과 같은 시스템의 하드웨어 기반 기능을 지원하지 않습니다.

매니지드 디바이스를 FMC에 등록하려면 FMC GUI에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** 페이지를 사용해야 합니다. 사용자의 버전에 맞는 Firepower Management Center 구성 가이드에 있는 디바이스 관리 정보를 참조하십시오.

상태 및 시스템 정책

기본적으로, 모든 어플라이언스에는 초기 시스템 정책이 적용되어 있습니다. 시스템 정책은 메일 릴레이 호스트 기본 설정, 시간 동기화 설정 등 구축의 여러 어플라이언스에서 유사할 수 있는 설정을 관리합니다. FMC를 사용하여 FMC 자체와 FMC에서 관리하는 모든 디바이스에 동일한 시스템 정책을 적용하는 것이 좋습니다.

기본적으로, FMC에도 상태 정책이 적용되어 있습니다. 상태 정책은 상태 모니터링 기능에 포함되어 있으며 구축된 어플라이언스의 성능을 지속적으로 모니터링하는 기준을 제공합니다. FMC를 사용하여 여기에서 관리하는 모든 디바이스에 상태 정책을 적용하는 것이 좋습니다.

소프트웨어 및 데이터베이스 업데이트

구축을 시작하기 전에 어플라이언스에서 시스템 소프트웨어를 업데이트해야 합니다. 구축의 모든 어플라이언스에서 최신 버전의 Firepower System을 실행하는 것이 좋습니다. 구축 시 최신 버전을 사용하고 있는 경우 최신 침입 규칙 업데이트, VDB, GeoDB도 설치해야 합니다.

주의 Firepower System의 일부를 업데이트하기 전에 업데이트와 함께 제공되는 릴리스 노트 또는 권고 문구를 읽어야 합니다. 릴리스 정보에는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보가 제공됩니다.

FMC에서 **Firepower** 버전 **6.5** 이상을 실행한다면**,**

구성 중에 FMC에서는 다음 활동을 설정하여 시스템을 최신 상태로 유지하고 데이터를 백업합니다.

- 주간 자동 GeoDB 업데이트
- FMC 및 매니지드 디바이스의 최신 소프트웨어를 다운로드하는 주간 작업

중요 이 작업은 FMC에 대한 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.

- 로컬에 저장한 구성 전용 FMC 백업을 수행하는 주간 작업

FMC가 **Firepower** 버전 **6.6.** 이상을 사용하고 있을 경우 초기 구성의 일부로서 FMC가 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다.

웹 인터페이스 메시지 센터를 사용하면 이러한 활동의 상태를 확인할 수 있습니다. 시스템이 이러한 활동을 구성하지 못하고 FMC이(가) 인터넷에 액세스할 수 있다면, 사용자의 버전에 맞는 *Firepower Management Center* 구성 가이드의 설명에 따른 활동 구성을 강력하게 권장합니다.

자세한 내용은 자동 초기 구성(버전 6.5 이상) 검토, 75 페이지를 참고하십시오.