



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, 1 페이지](#)
- [Firepower Management Center Virtual 라이선스, 3 페이지](#)
- [가상 어플라이언스 성능 정보, 4 페이지](#)
- [Firepower Management Center Virtual 구축 패키지 다운로드, 5 페이지](#)

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 페이지](#)의 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 할당된 IP 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 연결을 위한 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 정보](#)를 참조하십시오.

하이퍼바이저 및 버전 지원

하이퍼바이저 및 버전 지원에 대한 내용은 [Cisco Firepower 호환성](#)을 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Standard_D3_v2 에서 Standard_D4_v2 로 	Azure 포털 또는 PowerShell을 사용합니다. 크기를 조정하기 전에 인스턴스를 중지할 필요는 없지만 중지하면 크기가 더 표시될 수 있습니다. 크기를 조정하면 실행 중인 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](#)의 내용을 참조하십시오.
- KVM 하이퍼바이저를 실행하는 Linux 서버에서 Firepower Management Center Virtual을 구축하려면 [KVM을 사용하여 Firepower Management Center Virtual 구축](#)의 내용을 참조하십시오.
- AWS에서 Firepower Management Center Virtual을 구축하려면 [AWS Cloud에 Firepower Management Center Virtual 구축](#)의 내용을 참조하십시오.

- Azure에서 Firepower Management Center Virtual을 구축하려면 [Firepower Management Center Virtual On the Microsoft Azure Cloud 구축](#)의 내용을 참조하십시오.

