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, 7 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, 7 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.