

Secure Malware Analytics Appliance Air-Gap 모드 업데이트

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[제한 사항](#)

[요구 사항](#)

[시작하기 전에](#)

[오프라인\(Airgapped\) Secure Malware Analytics Appliance 업데이트](#)

[명명 규칙](#)

[제한 사항](#)

[Linux/MAC - ISO 다운로드](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[Desync 명령을 사용하여 ISO 다운로드](#)

[Windows - ISO 다운로드](#)

[Desync 명령을 사용하여 ISO 다운로드](#)

[다음을 확인합니다.](#)

[USB에서 어플라이언스 부팅](#)

[올바른 /dev 디바이스를 찾는 방법](#)

[status=progress 옵션](#)

[오프라인 업그레이드를 위한 HDD 드라이브의 부팅 순서](#)

[요구 사항:](#)

소개

이 문서에서는 Secure Malware Analytics Appliance Air-Gap 모드를 업데이트하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows 및 Unix/Linux 환경에서 명령줄을 통한 입력에 대한 기본 지식
- 악성코드 분석 어플라이언스에 대한 지식

- Cisco IMC(Integrated Management Controller)에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows 10 및 CentOS-8
- RUFUS 2.17
- C220 M4

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

대부분의 Secure Malware Analytics 어플라이언스는 인터넷에 연결되어 온라인 업데이트 프로세스를 사용합니다. 그러나 경우에 따라 Secure Malware Analytics 어플라이언스는 내부 네트워크, 즉 "에어 갭(air-gapped)" 내에서 엄격하게 관리됩니다. 어플라이언스를 에어 갭(air-gapped)으로 유지하는 것은 효율성이 떨어지므로 권장하지 않습니다. 그러나 추가적인 보안 또는 규정 요건을 지원하려면 이러한 절충이 필요할 수 있습니다.

인터넷에 연결되지 않은 상태에서 Secure Malware Analytics 어플라이언스를 실행하는 사용자의 경우 이 문서에 설명된 오프라인 업데이트 프로세스를 제공합니다. 요청 시 Secure Malware Analytics Support에서 업데이트 미디어를 제공합니다. 자세한 내용은 아래를 참조하십시오.

미디어: Airgap(오프라인) 업데이트 미디어는 Secure Malware Analytics Support에서 ISO로 제공됩니다. USB 미디어 또는 HDD(Hard Disk Drives)에 복사한 다음 적절한 크기로 사용할 수 있습니다.

크기: 업데이트 미디어에서 지원하는 버전에 따라 크기가 달라지지만, 새 VM이 소스 릴리스와 대상 릴리스 사이에 도입되면 수십 기가바이트가 될 수 있습니다. 현재 릴리스에서는 desync 틀이 VM 관련 변경 사항을 점진적으로 업데이트하는 데 도움이 되므로 약 30GB일 수 있습니다.

업그레이드 부팅 주기: Airgap 업데이트 미디어가 부팅될 때마다 업그레이드할 다음 릴리스를 결정하고 해당 다음 릴리스와 연결된 콘텐츠를 어플라이언스에 복사합니다. 어플라이언스가 실행되는 동안 해당 릴리스에 실행되어야 하는 필수 구성 요소 검사가 없는 경우 지정된 릴리스에서도 패키지 설치를 시작할 수 있습니다. 릴리스에 그러한 확인 사항 또는 그러한 확인을 추가할 수 있는 업데이트 프로세스의 일부에 대한 재정의가 포함된 경우, 사용자가 OpAdmin에 로그인하고 OpAdmin > Operations > Update Appliance로 업데이트를 호출할 때까지 업데이트가 실제로 적용되지 않습니다.

사전 설치 후크: 특정 업그레이드에 대한 사전 설치 후크가 있는지 여부에 따라, 업그레이드를 즉시 실행하거나 어플라이언스를 일반 운영 모드로 다시 부팅하여 사용자가 일반적인 관리 인터페이스로 들어가 직접 업그레이드를 시작할 수 있도록 합니다.

필요 시 반복: 이러한 각 미디어 부팅 사이클은 최종 대상 릴리스를 향해 한 단계만 업그레이드하거나 업그레이드를 준비합니다. 사용자는 원하는 대상 릴리스로 업그레이드하기 위해 필요한 만큼 부팅해야 합니다.


제한 사항

CIMC 미디어는 air-gapped 업데이트에서 지원되지 않습니다.

사용된 타사 구성 요소의 라이선싱 제약으로 인해 UCS M3 하드웨어가 EOL(단종)된 후에는 1.x 릴리스의 업그레이드 미디어를 더 이상 사용할 수 없습니다. 따라서 EOL 전에 UCS M3 어플라이언스를 교체하거나 업그레이드해야 합니다.

요구 사항

마이그레이션: 지원되는 릴리스에 대한 릴리스 노트에 다음 버전이 설치되기 전에 마이그레이션이 필요한 시나리오가 포함된 경우, 사용자는 어플라이언스를 사용할 수 없는 상태로 만들지 않으려면 다시 재부팅하기 전에 다음 단계를 따라야 합니다.

 참고: 특히 2.1.4 이후 버전의 첫 2.1.x 릴리스에서는 여러 데이터베이스 마이그레이션이 실행됩니다. 이러한 마이그레이션이 완료될 때까지 계속하는 것은 안전하지 않습니다. 자세한 내용은 [Threat Grid Appliance 2.1.5 마이그레이션 메모를 참조하십시오](#).

2.1.3 이전 릴리스부터 Airgap 업그레이드 미디어는 개별 라이선스에서 파생된 암호화 키를 사용하므로 어플라이언스 단위로 사용자 정의해야 합니다. 사용자가 볼 수 있는 유일한 효과는 2.1.3 이전 오리지널 버전을 지원하도록 작성된 미디어를 사용하는 경우, Secure Malware Analytics는 해당 어플라이언스에 미리 라이선스를 설치해야 하며, 미디어가 작성된 목록에 없는 어플라이언스에서는 작동하지 않는다는 것입니다.

릴리스 2.1.3 이상부터는 Airgap 미디어가 일반적이므로 고객 정보가 필요하지 않습니다.

시작하기 전에

- 백업. 업데이트를 진행하기 전에 어플라이언스 백업을 고려해야 합니다.
- 업데이트하려는 릴리스의 릴리스 정보를 검토하여 새 릴리스로 업데이트하기 전에 필요한 백그라운드 마이그레이션이 있는지 확인합니다
- 어플라이언스의 현재 버전을 확인합니다. OpAdmin > Operations > Update Appliance
- 모든 [Threat Grid 어플라이언스 문서](#)에서 사용할 수 있는 빌드 번호/버전 조회 테이블에서 Secure Malware Analytics 어플라이언스 버전 기록(릴리스 정보, 마이그레이션 정보, 설정 및 컨피그레이션 설명서, 관리자 설명서)을 검토합니다.

오프라인(Airgapped) Secure Malware Analytics Appliance 업데이트

이 페이지에서 사용 가능한 Air Gapped 버전을 먼저 확인합니다. [어플라이언스 버전 조회 테이블](#)

1. 오프라인 업데이트 미디어를 받으려면 TAC 지원 요청을 엽니다. 이 요청에는 어플라이언스 일련 번호와 어플라이언스 빌드 번호가 포함되어야 합니다.
2. TAC Support는 설치를 기반으로 업데이트된 ISO를 제공합니다.
3. 부팅 가능 USB에 ISO 이미지를 굽습니다. USB는 오프라인 업데이트를 위해 지원되는 유일한 장치/방법입니다.

명명 규칙

업데이트된 파일 이름(예: TGA Airgap Update 2.13.2-2.14.0)입니다.

따라서 이 미디어는 최소 버전 2.13.2를 실행하는 어플라이언스에 사용할 수 있으며 어플라이언스를 버전 2.14.0으로 업그레이드할 수 있습니다.

제한 사항

- CIMC 미디어는 air-gapped 업데이트에서 지원되지 않습니다.
- 사용된 타사 구성 요소의 라이선싱 제약으로 인해 UCS M3 하드웨어가 EOL(단종)된 후에는 1.x 릴리스용 업그레이드 미디어를 더 이상 사용할 수 없습니다. 따라서 EOL 전에 UCS M3 어플라이언스를 교체하거나 업그레이드해야 합니다.

Linux/MAC - ISO 다운로드

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISO를 다운로드하고 부팅 가능 USB 설치 드라이브를 만들 수 있는 인터넷 액세스 권한이 있는 Linux 시스템입니다.
- Airgap 다운로드 지침은 Secure Malware Analytics Support에서 제공합니다.
- GO 프로그래밍 언어. [다운로드](#)
- .caibx 인덱스 파일(TAC 지원에서 제공하는 zip 파일에 포함됨).
- Desync Tool(Secure Malware Analytics Support에서 제공하는 zip 파일에 포함됨).

사용되는 구성 요소

이 문서의 정보는 CentOS Linux 릴리스 7.6.1810(핵심)을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

GO 프로그래밍 언어 설치

```
# wget https://dl.google.com/go/go1.12.2.linux-amd64.tar.gz
# tar -xzf go1.12.2.linux-amd64.tar.gz
# mv go /usr/local
```

desync 명령이 실패하지 않는 경우 설치 후 다음 세 명령을 실행합니다

```
# export GOROOT=/usr/local/go
# export GOPATH=$HOME/Projects/Proj1
# export PATH=$GOPATH/bin:$GOROOT/bin:$PATH
```

GO 버전은 다음 방법으로 확인할 수 있습니다.

```
# go version
```

Desync 명령을 사용하여 ISO 다운로드

1단계. Secure Malware Analytics Support에서 제공하는 Zip 파일의 내용(desync.linux 및 .caibx 파일 포함)을 시스템의 동일한 디렉토리에 로컬로 복사합니다.

2단계. 파일을 저장한 디렉토리로 변경합니다.


예:

```
# cd MyDirectory/TG
```

3단계. pwd 명령을 실행하여 디렉토리 안에 있는지 확인합니다.

```
# pwd
```

4단계. desync.linux 명령 및 .caibx 파일이 포함된 디렉토리 내에 있으면 선택한 명령을 실행하여 다운로드 프로세스를 시작합니다.

 참고: 여러 ISO 버전에 대한 예입니다. Secure Malware Analytics Support에서 제공하는 지침에서 .caibx 파일을 참조하십시오.

버전 2.1.3~2.4.3.2 ISO의 경우:

```
# desync extract -k -s s3+https://s3.amazonaws.com/threatgrid-appliance-airgap-update airgap-update-2.1
```


버전 2.4.3.2~2.5 ISO의 경우:

```
# desync extract -k -s s3+https://s3.amazonaws.com/threatgrid-appliance-airgap-update airgap-update-2.4
```

버전 2.5~2.7.2ag ISO의 경우:

```
# desync extract -k -s s3+https://s3.amazonaws.com/threatgrid-appliance-airgap-update airgap-update-2.5
```

다운로드가 시작되면 진행 표시줄이 표시됩니다.

 참고: 환경에서 다운로드 속도 및 업그레이드 미디어의 크기는 ISO 작성 시간에 영향을 줄 수 있습니다.
다운로드한 파일의 MD5를 지원에서 제공한 번들과 함께 사용 가능한 파일과 비교하여 다운로드한 ISO의 무결성을 검증하십시오.


다운로드가 완료되면 동일한 디렉토리에 ISO가 생성됩니다.

USB를 컴퓨터에 플러그인하고 dd 명령을 실행하여 부팅 가능 USB 드라이브를 만듭니다.

```
# dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M
```

여기서 <MY_USB>는 USB 키의 이름입니다(꺾쇠 괄호는 제외).

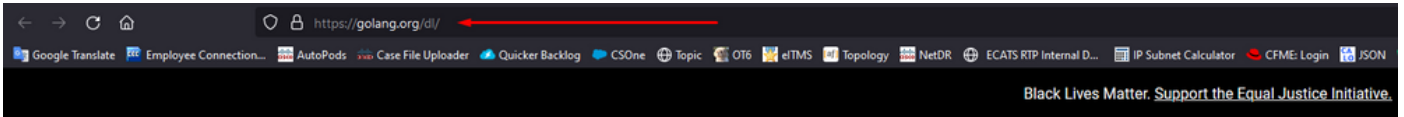
USB 드라이브를 삽입하고 어플라이언스를 켜거나 재부팅합니다. Cisco 부팅 화면에서 F6 키를 눌러 Boot Menu(부팅 메뉴)로 들어갑니다.

 **팁:**
다운로드가 대역폭에 영향을 미칠 수 있으므로 업무 시간 또는 사용량이 적은 시간 후에 다운로드를 실행합니다.
도구를 중지하려면 터미널을 닫거나 Ctrl+c/Ctrl+z를 누릅니다.
계속하려면 동일한 명령을 실행하여 다운로드를 다시 시작하십시오.

Windows - ISO 다운로드

GO 프로그래밍 언어 설치

#1: 필요한 GO 프로그래밍 언어를 다운로드합니다. <https://golang.org/dl/>에서 [설치](#) 내 경우에는 Featured Version을 선택합니다. CMD를 다시 시작하고



Downloads

Featured downloads
Stable versions
Unstable version

After downloading a binary release suitable for your system, please follow the [installation instructions](#).

If you are building from source, follow the [source installation instructions](#).

See the [release history](#) for more information about Go releases.

As of Go 1.13, the go command by default downloads and authenticates modules using the Go module mirror and Go checksum database run by Google. See <https://proxy.golang.org/privacy> for privacy information about these services and the [go command documentation](#) for configuration details including how to disable the use of these servers or use different ones.

Featured downloads

Microsoft Windows <i>Windows 7 or later, Intel 64-bit processor</i> go1.16.6.windows-amd64.msi (119MB)	Apple macOS <i>macOS 10.12 or later, Intel 64-bit processor</i> go1.16.6.darwin-amd64.pkg (125MB)	Linux <i>Linux 2.6.23 or later, Intel 64-bit processor</i> go1.16.6.linux-amd64.tar.gz (123MB)	Source go1.16.6.src.tar.gz (20MB)
---	--	---	---

CMD run 명령을 달았다가 다시 열어 다음을 확인합니다.

```
go version
```



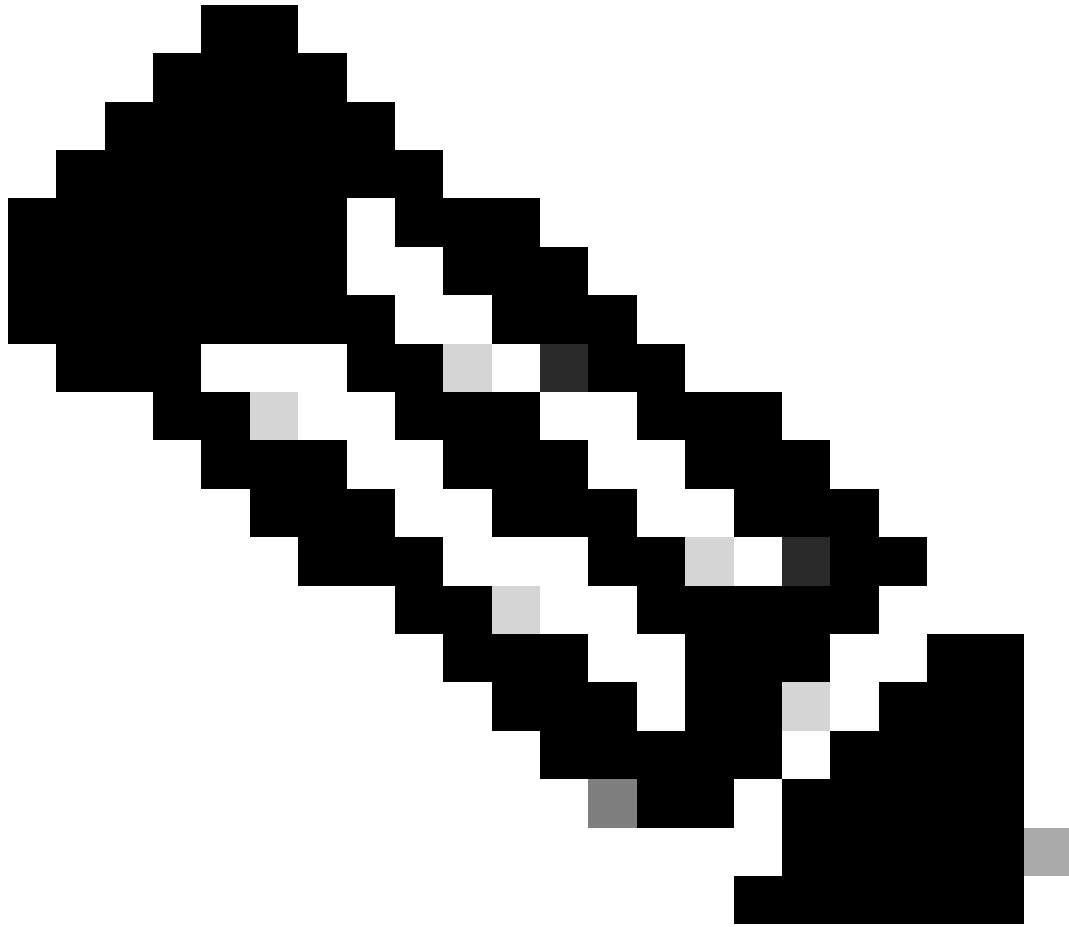
Desync 명령을 사용하여 ISO 다운로드

#2: DESYNC 도구를 설치합니다. 명령을 실행한 후 여러 다운로드 프롬프트를 확인할 수 있습니다. 대략 2-3분 후에 다운로드가 완료되어야 합니다.

```
go install github.com/folbricht/desync/cmd/desync@latest
```

In case desync is not working using above command then change directory to C drive and run this command

```
git clone https://github.com/folbricht/desync.git
```



참고: git 명령이 작동하지 않으면 <https://git-scm.com/download/win>에서 Git를 다운로드하여 설치할 수 [있습니다](#).

그런 다음 두 명령 아래에서 하나씩 실행합니다.

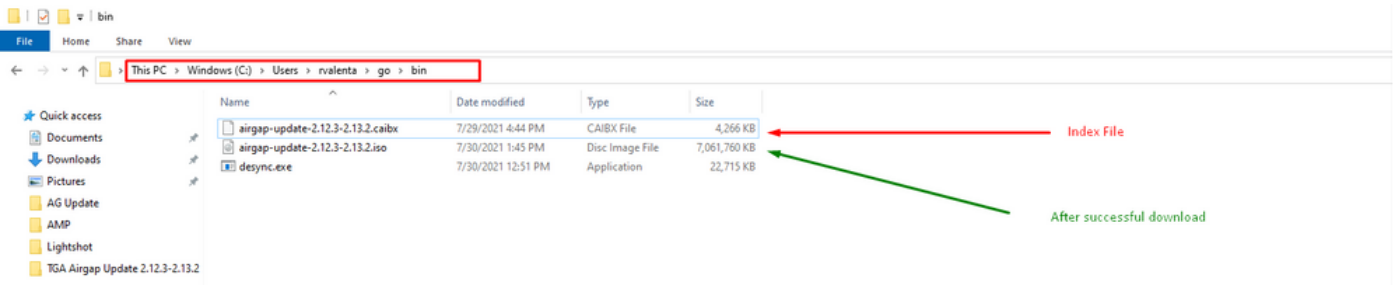
```
cd desync/cmd/desync
```

```
go install
```



```
C:\Users\rvalenta>go install github.com/folbricht/desync/cmd/desync@latest
go: downloading github.com/folbricht/tempfile v0.0.1
go: downloading github.com/go-ini/ini v1.62.0
go: downloading github.com/minio/minio-go/v6 v6.0.57
go: downloading github.com/pkg/errors v0.9.1
go: downloading github.com/sirupsen/logrus v1.7.0
go: downloading github.com/spf13/cobra v1.1.1
go: downloading github.com/spf13/pflag v1.0.5
go: downloading golang.org/x/crypto v0.0.0-20201221181555-ee23a3978ad
go: downloading github.com/sirupsen/logrus v1.8.1
go: downloading gopkg.in/cheggaaa/pb.v1 v1.0.28
go: downloading github.com/spf13/cobra v1.2.1
go: downloading github.com/minio/minio-go v1.0.0
go: downloading cloud.google.com/go v0.72.0
go: downloading github.com/DataDog/zstd v1.4.5
go: downloading github.com/boljen/go-bitmap v0.0.0-20151001105940-23cd2fb0ce7d
go: downloading github.com/dchest/siphash v1.2.2
go: downloading github.com/hanwen/go-fuse v1.0.0
go: downloading github.com/klauspost/compress v1.11.4
go: downloading github.com/DataDog/zstd v1.4.8
go: downloading github.com/hanwen/go-fuse/v2 v2.0.3
go: downloading github.com/pkg/sftp v1.12.0
go: downloading golang.org/x/crypto v0.0.0-20210711020723-a769d52b0f97
go: downloading github.com/minio/minio-go v6.0.14+incompatible
go: downloading github.com/pkg/sftp v1.13.2
go: downloading github.com/pkg/xattr v0.4.3
go: downloading golang.org/x/sync v0.0.0-20201207232520-09787c993a3a
go: downloading google.golang.org/api v0.36.0
go: downloading github.com/hanwen/go-fuse/v2 v2.1.0
go: downloading golang.org/x/sync v0.0.0-20210220032951-036812b2e83c
go: downloading github.com/mattn/go-runewidth v0.0.9
go: downloading golang.org/x/sys v0.0.0-20201201145000-ef89a241ccb3
```

#3: 이동 —> bin 위치로 이동합니다. 내 경우에는 C:\Users\rvalenta\go\bin이며 TAC에서 제공한 .caibx 인덱스 파일을 복사/붙여넣습니다.



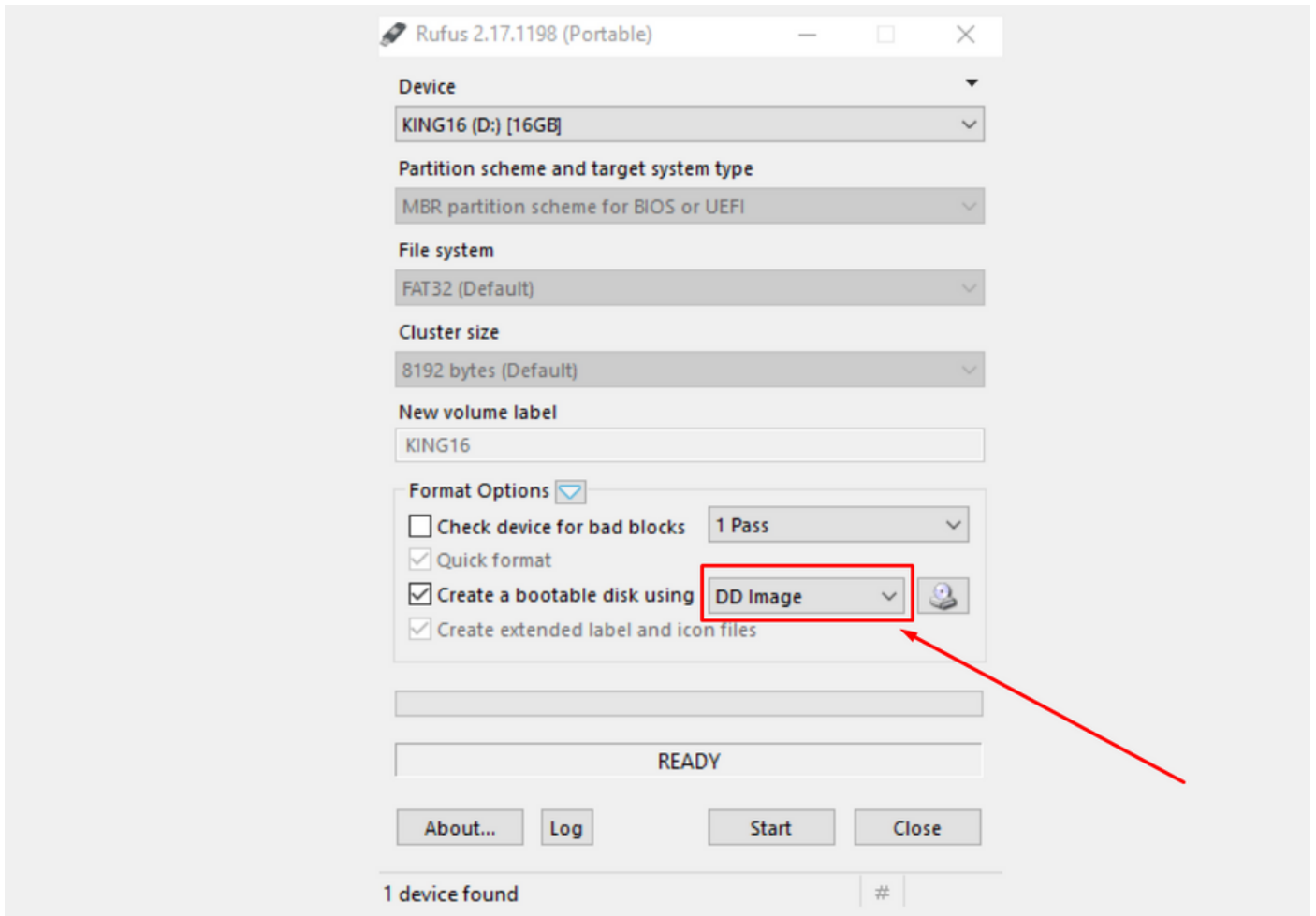
다음을 확인합니다.

#4: CMD 프롬프트로 돌아가서 go\bin 폴더로 이동하고 download 명령을 실행합니다. 다운로드가 진행되는 것을 즉시 확인할 수 있습니다. 다운로드가 완료될 때까지 기다립니다. 이제 전체 .ISO 파일이 이전에 복사한 .caibx 인덱스 파일과 같은 위치에 있어야 합니다

```
desync extract -k -s s3+https://s3.amazonaws.com/threatgrid-appliance-airgap-update airgap-update-2.12.
```

```
C:\Users\rvalenta>cd go
C:\Users\rvalenta>go>cd bin
C:\Users\rvalenta\go\bin>desync extract -k -s s3+https://s3.amazonaws.com/threatgrid-appliance-airgap-update airgap-update-2.12.3-2.13.2.caibx airgap-update-2.12.3-2.13.2.iso
Error: airgap-update-2.12.3-2.13.2.caibx: open ./airgap-update-2.12.3-2.13.2.caibx: The system cannot find the file specified.
C:\Users\rvalenta\go\bin>desync extract -k -s s3+https://s3.amazonaws.com/threatgrid-appliance-airgap-update airgap-update-2.12.3-2.13.2.caibx airgap-update-2.12.3-2.13.2.iso
[=====] 100.00% 16m52s
C:\Users\rvalenta\go\bin>
```

그런 다음 RUFUS를 사용하여 부팅 가능 USB를 만듭니다. 이는 버전 2.17을 사용하는 데 매우 중요합니다. 이 특정 복구 USB를 만드는 데 매우 중요한 dd 옵션을 사용할 수 있는 마지막 버전입니다. 이 저장소의 모든 버전을 찾을 수 있습니다 [RUFUS 저장소](#) 해당 파일을 더 이상 사용할 수 없는 경우 이 문서에 있는 전체 및 휴대용 버전의 설치 프로그램도 포함됩니다.



USB에서 어플라이언스 부팅

USB 드라이브를 삽입하고 어플라이언스를 켜거나 재부팅합니다. Cisco 부팅 화면에서 "F6"을 선택하여 Boot Menu(부팅 메뉴)를 입력합니다. 빨리요! 이 항목을 선택할 수 있는 시간은 몇 초입니다. 놓치면 다시 부팅해서 다시 시도해야 합니다.

그림 1 - F6 키를 눌러 Boot 메뉴로 들어가기



Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

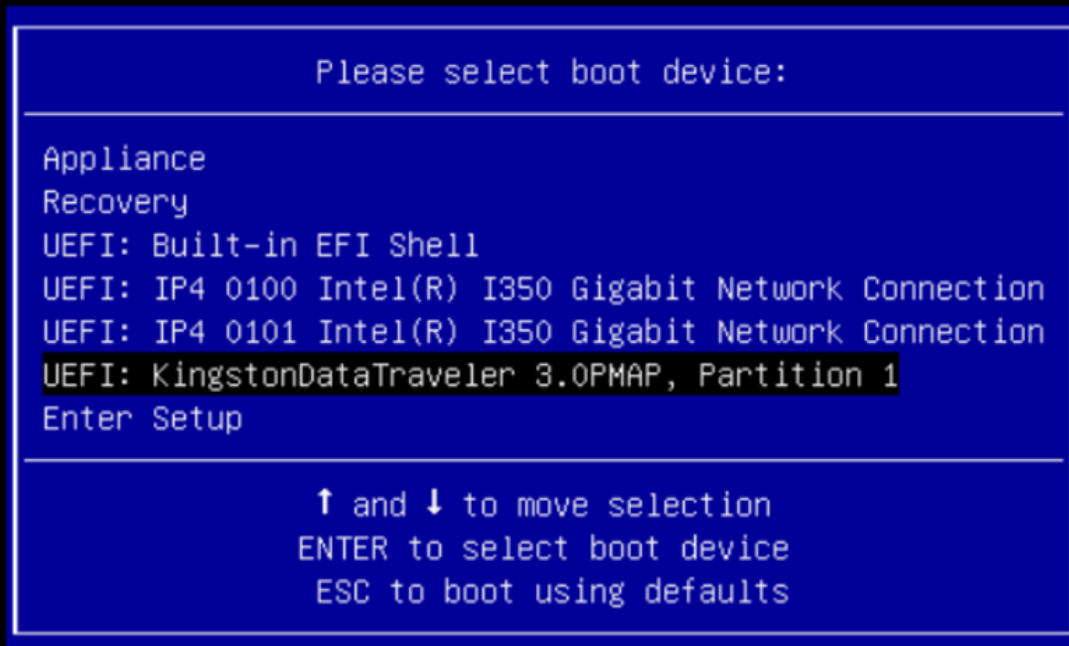
Bios Version : C220M4.2.0.13d.0.0812161113
Platform ID : C220M4

Cisco IMC IPv4 Address : 10.77.1.71
Cisco IMC MAC Address : CC:46:D6:FC:B5:1C

Processor(s) Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz
Total Memory = 512 GB Effective Memory = 512 GB
Memory Operating Speed 2400 Mhz
Entering boot selection menu...

업데이트가 포함된 USB 드라이브로 이동한 후 Enter를 눌러 다음을 선택합니다.

그림 2 - 업데이트 USB 선택



업데이트 미디어는 업그레이드 경로의 다음 릴리스를 결정하고 해당 릴리스에 대한 콘텐츠를 어플라이언스에 복사합니다. 어플라이언스는 업그레이드를 즉시 실행하거나 OpAdmin을 시작하고 수동으로 업그레이드를 시작할 수 있도록 일반 운영 모드로 다시 재부팅합니다.

ISO 부팅 프로세스가 완료되면 Secure Malware Analytics Appliance를 다시 작동 모드로 재부팅합니다.

계속하기 전에 포털 UI에 로그인하여 업그레이드 등의 안전 여부를 알리는 모든 경고를 확인합니다

재부팅 중에 업데이트가 자동으로 적용되지 않은 경우 OpAdmin 인터페이스로 이동하여 업데이트를 적용합니다. OpAdmin > Operations > Update Appliance 참고: 업데이트 프로세스에는 업데이트의 일부로 USB 미디어로 이루어진 추가 재부팅이 포함됩니다. 예를 들어, 업데이트를 설치한 후 설치 페이지에서 Reboot(재부팅) 버튼을 사용해야 합니다.

USB의 각 버전에 대해 필요에 따라 반복합니다.

올바른 /dev 디바이스를 찾는 방법

USB가 엔드포인트에 여전히 연결되지 않은 상태에서 "lsblk" 명령을 실행합니다. | grep -iE 'disk|part'.

```

xsilenc3x@Alien15:~/testarea/usb$ lsblk | grep -iE 'disk|part'
sda            8:0    0 931.5G  0 disk
├─sda1         8:1    0  128M  0 part
└─sda2         8:2    0 931.4G  0 part /media/DATA
nvme0n1       259:0    0 238.5G  0 disk
├─nvme0n1p1   259:1    0   650M  0 part
├─nvme0n1p2   259:2    0   128M  0 part
├─nvme0n1p3   259:3    0  114.1G  0 part
├─nvme0n1p4   259:4    0   525M  0 part /boot
├─nvme0n1p5   259:5    0    7.6G  0 part [SWAP]
├─nvme0n1p6   259:6    0   38.2G  0 part /
├─nvme0n1p7   259:7    0   62.7G  0 part /home
├─nvme0n1p8   259:8    0   13.1G  0 part
└─nvme0n1p9   259:9    0    1.1G  0 part
xsilenc3x@Alien15:~/testarea/usb$

```

USB 스틱이 연결된 후

```

xsilenc3x@Alien15:~/testarea/usb$ lsblk | grep -iE 'disk|part'
.sda            8:0    0 931.5G  0 disk
├─sda1         8:1    0  128M  0 part
└─sda2         8:2    0 931.4G  0 part /media/DATA
sdb            8:16    1   3.7G  0 disk
├─sdb1         8:17    1   3.7G  0 part /media/xsilenc3x/ARCH_201902 <----- not observed when the USB was not
nvme0n1       259:0    0 238.5G  0 disk
├─nvme0n1p1   259:1    0   650M  0 part
├─nvme0n1p2   259:2    0   128M  0 part
├─nvme0n1p3   259:3    0  114.1G  0 part
├─nvme0n1p4   259:4    0   525M  0 part /boot
├─nvme0n1p5   259:5    0    7.6G  0 part [SWAP]
├─nvme0n1p6   259:6    0   38.2G  0 part /
├─nvme0n1p7   259:7    0   62.7G  0 part /home
├─nvme0n1p8   259:8    0   13.1G  0 part
└─nvme0n1p9   259:9    0    1.1G  0 part
xsilenc3x@Alien15:~/testarea/usb$

```

이렇게 하면 /dev의 USB 디바이스가 "/dev/sdb"임을 확인합니다.

USB 스틱이 연결된 후 확인하는 다른 방법:

dmesg 명령은 일부 정보를 제공합니다. USB가 연결된 후 명령 dmesg를 실행합니다 | grep -iE 'usb|attached'.

```

xsilenc3x@Alien15:~/testarea/usb$ dmesg | grep -iE 'usb|attached'
[842717.663757] usb 1-1.1: new high-speed USB device number 13 using xhci_hcd
[842717.864505] usb 1-1.1: New USB device found, idVendor=0781, idProduct=5567
[842717.864510] usb 1-1.1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[842717.864514] usb 1-1.1: Product: Cruzer Blade
[842717.864517] usb 1-1.1: Manufacturer: SanDisk
[842717.864519] usb 1-1.1: SerialNumber: 4C530202420924105393


```

```
[842717.865608] usb-storage 1-1.1:1.0: USB Mass Storage device detected
[842717.866074] scsi host1: usb-storage 1-1.1:1.0
[842718.898700] sd 1:0:0:0: Attached scsi generic sg1 type 0
[842718.922265] sd 1:0:0:0: [sdb] Attached SCSI removable disk <-----
xsilenc3x@Alien15:~/testarea/usb$
```

fdisk 명령은 크기에 대한 정보를 제공하며, 이를 확인하는 데 사용할 수 있습니다. `sudo fdisk -l /dev/sdb`.

```
xsilenc3x@Alien15:~/testarea/usb$ sudo fdisk -l /dev/sdb
Disk /dev/sdb: 3.7 GiB, 4004511744 bytes, 7821312 sectors <-----
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x63374e06

Device      Boot Start    End Sectors  Size Id Type
/dev/sdb1   *            0 675839   675840  330M 0 Empty
/dev/sdb2             116    8307    8192     4M ef EFI (FAT-12/16/32)
xsilenc3x@Alien15:~/testarea/usb$
```

 참고: "dd" 명령을 실행하기 전에 USB를 마운트 해제해야 합니다.

예제의 USB 장치가 장착되었는지 확인합니다.

```
xsilenc3x@Alien15:~/testarea/usb$ sudo mount -l | grep -i sdb
/dev/sdb1 on /media/xsilenc3x/ARCH_201902 type vfat (rw,nosuid,nodev,relatime,uid=1000,gid=1000,fmask=0
```

USB 디바이스를 마운트 해제하려면 `sudo umount /dev/sdb1`을 사용합니다.

```
xsilenc3x@Alien15:~/testarea/usb$ sudo umount /dev/sdb1
```

디바이스가 "마운트된" 것으로 인식되지 않는지 다시 확인하십시오.

```
xsilenc3x@Alien15:~/testarea/usb$ sudo mount -l | grep -i sdb
```

`status=progress` 옵션

dd 명령의 oflag=sync 및 status=progress 옵션


수많은 데이터 블록을 쓸 때 "status=progress" 옵션은 현재 쓰기 작업의 정보를 제공합니다. 이 명령은 "dd" 명령이 현재 페이지 캐시에 기록 중인지 확인하는 데 유용합니다. 이 명령을 사용하여 모든 쓰기 작업의 진행률과 전체 시간을 초 단위로 표시할 수 있습니다.

사용하지 않는 경우 "dd"는 진행 상황에 대한 정보를 제공하지 않으며, 쓰기 작업의 결과만 "dd"가 반환되기 전에 제공됩니다.

```
[rootuser@centos8-01 tga-airgap]$ dd if=/dev/zero of=testfile.txt bs=1M count=8192
8192+0 records in
8192+0 records out
8589934592 bytes (8.6 GB, 8.0 GiB) copied, 5.03493 s, 1.7 GB/s
[rootuser@centos8-01 tga-airgap]$
```

사용되는 경우 쓰기 작업에 대한 실시간 정보가 매초마다 업데이트됩니다.

```
[rootuser@centos8-01 tga-airgap]$ dd if=/dev/zero of=testfile.txt bs=1M count=8192 status=progress
8575254528 bytes (8.6 GB, 8.0 GiB) copied, 8 s, 1.1 GB/s <-----
8192+0 records in
8192+0 records out
8589934592 bytes (8.6 GB, 8.0 GiB) copied, 8.03387 s, 1.1 GB/s
[rootuser@centos8-01 tga-airgap]
```

 참고: TGA 오프라인 업그레이드 프로세스에 대한 공식 문서에서 제공되는 명령은 다음과 같습니다. dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M

몇 가지 테스트 후 다음 예가 관찰됩니다.

/dev/zero 디바이스를 사용하여 "dd"로 10MB의 파일이 생성되면

1M x 10 = 10M(10240kB + 더티 파일 페이지 캐시의 이전 시스템 데이터 = 10304kB → "dd"가 끝나면 더티 페이지 캐시에서 인식되는 데이터입니다.)

```
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && dd if=/dev/zero of=testfile.txt
count=10 status=progress && cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                92 kB
10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.0138655 s, 756 MB/s
Dirty:                10304 kB <----- dirty page cache after "dd" returned | data still to be written to t
1633260775 <---- epoch time
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                10372 kB
1633260778
```


```

[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                10380 kB
1633260779
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                10404 kB
1633260781
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                10412 kB
1633260782
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                10424 kB
1633260783
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                10436 kB
1633260785
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                0 kB <--- data in the dirty page cache flushed = written to the block device
1633260786 <---- epoch time
[rootuser@centos8-2 testarea]$
```


1633260786 - 1633260775 = 11 seconds


```

---

 참고: "dd" 명령이 반환된 후 블록 디바이스에 대한 쓰기 작업이 완료되지 않았으며 반환 11초 후에 인식되었습니다.  
TGA ISO를 사용하여 부팅 가능 USB를 만들 때 "dd" 명령이었고 11초 전에 엔드포인트에서 USB를 제거한 경우 = 부팅 가능 USB에서 손상된 ISO가 있을 수 있습니다.

---

## 설명:

블록 디바이스는 하드웨어 디바이스에 대한 버퍼링된 액세스를 제공합니다. 이는 하드웨어 장치로 작업할 때 애플리케이션에 추상화 계층을 제공합니다.

블록 디바이스를 사용하면 애플리케이션이 서로 다른 크기의 데이터 블록으로 읽기/쓰기를 수행할 수 있습니다. 이 read()/writes()는 페이지 캐시(버퍼)에 적용되며 블록 디바이스에 직접 적용되지 않습니다.

읽기/쓰기를 수행하는 애플리케이션이 아닌 커널은 버퍼(페이지 캐시)에서 블록 디바이스로의 데이터 이동을 관리합니다.

따라서

애플리케이션(이 경우 "dd")은 지침 없이 버퍼 플러시를 제어할 수 없습니다.

"oflag=sync" 옵션은 각 출력 블록("dd"에서 제공됨)이 페이지 캐시에 배치된 후 커널에서 동기식으로 물리적 쓰기를 강제로 수행합니다.

oflag=sync는 옵션을 사용하지 않는 경우와 비교할 때 "dd" 성능을 저하시키지만, 활성화된 경우 "dd"에서 각 write()를 호출한 후 블록 디바이스에 대한 물리적 쓰기를 보장합니다.

테스트 : " dd " 명령의 " oflag=sync " 옵션을 사용하여 더티 페이지 캐시 데이터가 있는 모든 쓰기 작업이 " dd " 명령의 반환에서 완료되었음을 확인합니다.




```
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && dd if=/dev/zero of=testfile.txt
count=10 oflag=sync status=progress && cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty: 60 kB
10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.0841956 s, 125 MB/s
Dirty: 68 kB <---- No data remaining in the dirty page cache after "dd" returned
1633260819
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty: 36 kB
1633260821
[rootuser@centos8-2 testarea]$
```

더티 페이지 캐시의 쓰기 작업에서 남아 있는 데이터가 없습니다.

"dd" 명령이 반환되기 전에(또는 동시에) 쓰기 작업이 적용되었습니다(이전 테스트에서 11초 후에). 이제 "dd" 명령이 반환된 후 쓰기 작업과 관련된 더티 페이지 캐시에 데이터가 없었음을 확인합니다. 즉, 부팅 가능 USB 생성에 문제가 없습니다(ISO 체크섬이 올바른 경우).

---

 참고: 이 유형의 사례에서 작업할 때는 "dd" 명령의 이 플래그(oflag=sync)를 고려해야 합니다.

---

## 오프라인 업그레이드를 위한 HDD 드라이브의 부팅 순서

요구 사항:

사용 가능한 모든 도구를 사용하여 "DD" 옵션을 사용하여 HDD를 포맷하고 나중에 미디어를 드라이브에 복사해야 합니다. 이 서식을 사용하지 않으면 이 미디어를 읽을 수 없습니다.

일단 "DD" 형식을 사용하여 HDD/USB에 미디어를 로드한 다음 TGA 어플라이언스에 연결하고 디바이스를 다시 시작해야 합니다.

이것이 기본 Boot Menu(부팅 메뉴) 선택 화면입니다. 디바이스를 부팅하여 부팅 미디어를 선택하려면 "F6"을 눌러야 합니다



Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,  
<F12> Network Boot

Bios Version : C220M4.4.1.2c.0.0202211901  
Platform ID : C220M4

Cisco IMC IPv4 Address : 192.168.1.22  
Cisco IMC MAC Address : 70:0F:6A:E8:16:50

Processor(s) Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz  
Total Memory = 512 GB Effective Memory = 512 GB  
Memory Operating Speed 2400 Mhz

디바이스가 입력을 인식하면 디바이스에서 부팅 선택 메뉴를 입력하라는 프롬프트가 표시됩니다.



Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,  
<F12> Network Boot

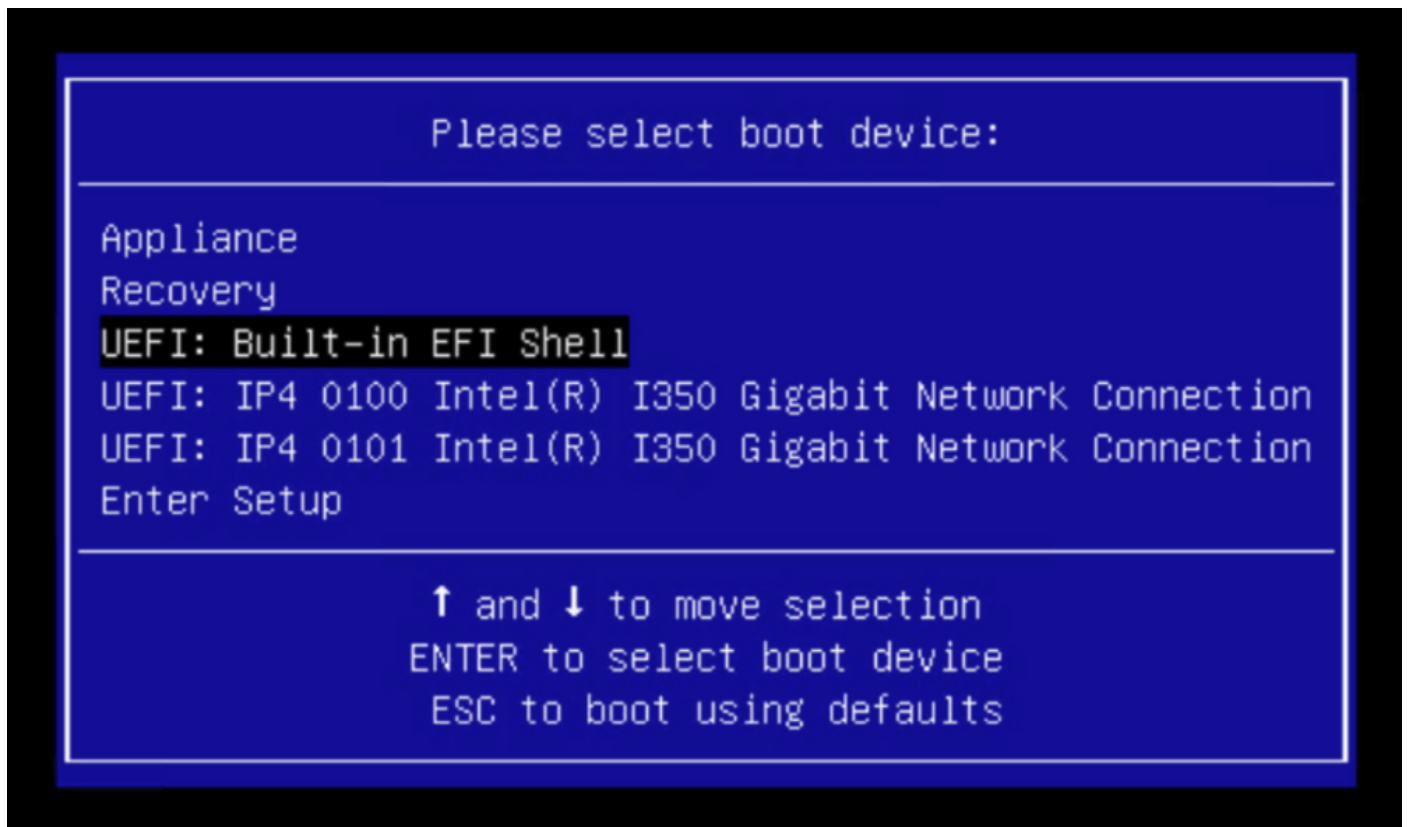
Bios Version : C220M4.4.1.2c.0.0202211901  
Platform ID : C220M4

Cisco IMC IPv4 Address : 192.168.1.22  
Cisco IMC MAC Address : 70:0F:6A:E8:16:50

Processor(s) Intel(R) Xeon(R) CPU E5-2697 v4 @ 2.30GHz  
Total Memory = 512 GB Effective Memory = 512 GB  
Memory Operating Speed 2400 Mhz  
Entering boot selection menu...

이것은 서로 다른 TGA 모델 간에 다를 수 있는 프롬프트입니다. 이상적으로는 이 메뉴 자체에서 부

트 미디어(파일 시스템 업그레이드)를 사용하여 부팅하는 옵션이 표시되지만 표시되지 않으면 "EFI 셸"에 로그인해야 합니다.



"startup.sh" 스크립트가 EFI 셸로 이동하기 전에 "ESC"를 눌러야 합니다. 일단 EFI 셸에 로그인하면 이 경우에 탐지된 파티션은 3개의 파일 시스템입니다. fs0:, fs1:, fs2.

```
UEFI Interactive Shell v2.0. UEFI v2.40 (American Megatrends, 0x0005000B). Revision 1.02
Mapping table
fs0: Alias(s):HD21a0b0c::blk2:
 PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x1,0x0)/HD(2,MBR,0x00000000,0xC6E244,0x9800)
fs1: Alias(s):HD29a0b::blk4:
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(1,GPT,22C0970D-0F05-444F-A0F3-EA787035FA1E,0x800,0x4
00000)
fs2: Alias(s):HD29b0b::blk8:
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)/HD(1,GPT,D4C95D76-AC65-421E-9BF9-487B6A2025ED,0x800,0x4
00000)
blk0: Alias(s):
 PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x1,0x0)
blk1: Alias(s):
 PciRoot(0x0)/Pci(0x1D,0x0)/USB(0x0,0x0)/USB(0x1,0x0)/HD(1,MBR,0x00000000,0x40,0xC6E204)
blk3: Alias(s):
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)
blk7: Alias(s):
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)
blk5: Alias(s):
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(2,GPT,72DF22A3-D885-432E-A8D3-C1B00AB22A8B,0x400800,
0x4000000)
blk6: Alias(s):
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(3,GPT,F298B3C8-074C-4D38-A346-74BEFB9D7F61,0x800800,
0xD5A6FDF)
blk9: Alias(s):
 PciRoot(0x0)/Pci(0x2,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x1,0x0)/HD(2,GPT,0D6976B4-70AE-4B36-8E8A-C7F8D322BFDE,0x400800,
0x2B9A8CFDF)
Press ESC in 3 seconds to skip startup.nsh or any other key to continue.
Shell> _
```

## 중요

올바른 파일 시스템 식별:

- 위 스크린샷에 따르면 "fs0:"이 경로에 "USB"가 있는 유일한 미디어임을 알 수 있으므로 이 파일 시스템에 부팅 미디어(업그레이드 파일 시스템)가 포함되어 있음을 확인할 수 있습니다.

파일 시스템이 누락된 경우:

- fs0: 및 fs1:만 사용할 수 있고 fs2:가 없는 경우 부팅 미디어(업그레이드 파일 시스템)가 dd 모드에서 작성되었으며 성공적으로 연결되었는지 확인합니다.
- 부팅 미디어(업그레이드 파일 시스템)는 항상 복구 미디어보다 작은 숫자를 가져야 하며 항상 서로 옆에 있어야 합니다. USB 연결 드라이브가 끝 시작 부분에 있어야 변경되기 쉽습니다(따라서 fs0:의 앞쪽 위치 또는 fs2:의 뒷쪽 위치).
- 아래 스크린샷의 경우, "\efi\boot" 파티션 아래에 있는 올바른 ".efi" 파일이며 명명 규칙이 "bootx64.efi"입니다.

```
Shell> fs0:
fs0:\> dir
Directory of: fs0:\
01/01/1980 00:00 <DIR> 2,048 efi
 0 File(s) 0 bytes
 1 Dir(s)
fs0:\> cd efi
fs0:\efi> cd boot
fs0:\efi\boot> dir
Directory of: fs0:\efi\boot\
01/01/1980 00:00 <DIR> 2,048 .
01/01/1980 00:00 <DIR> 2,048 ..
01/01/1980 00:00 18,703,096 bootx64.efi
 1 File(s) 18,703,096 bytes
 2 Dir(s)
```

부팅 미디어(업그레이드 파일 시스템)에서 디바이스를 부팅하려면 "bootx64.efi" 파일을 실행해야 합니다.

fs0:\efi\boot\bootx64.efi

참고로, 다른 파일 시스템의 내용도 아래와 같이 표시해 드렸습니다.

fs1: 기본 부팅 파일 시스템입니다.

```
fs1:\> fs1:
fs1:\> dir
Directory of: fs1:\
01/01/1980 00:00 43,985,838 initramfs-appliance.img
01/01/1980 00:00 287 initramfs-appliance.img.sig
01/01/1980 00:00 5,490,560 vmlinuz-appliance
01/01/1980 00:00 287 vmlinuz-appliance.sig
01/01/1980 00:00 4 .gitignore
01/01/1980 00:00 <DIR> 4,096 efi
01/01/1980 00:00 149 startup.nsh
01/01/1980 00:00 6,199,680 vmlinuz-linux
 7 File(s) 55,676,805 bytes
 1 Dir(s)
fs1:\> cd efi
fs1:\efi\> dir
Directory of: fs1:\efi\
05/23/2018 17:52 <DIR> 4,096 .
05/23/2018 17:52 <DIR> 0 ..
01/01/1980 00:00 <DIR> 4,096 Appliance
 0 File(s) 0 bytes
 3 Dir(s)
fs1:\efi\> cd Appliance
fs1:\efi\Appliance\> dir
Directory of: fs1:\efi\Appliance\
05/23/2018 17:52 <DIR> 4,096 .
05/23/2018 17:52 <DIR> 4,096 ..
01/01/1980 00:00 r 18,131,752 boot.efi
01/01/1980 00:00 287 boot.efi.sig
 2 File(s) 18,132,039 bytes
 2 Dir(s)
```

fs2: 이것은 복구 이미지 부트 파일 시스템입니다.


```

fs2:\> fs2:
fs2:\> dir
Directory of: fs2:\
09/21/2021 23:35 29,856 meta_contents.tar.xz
09/17/2021 13:01 <DIR> 4,096 tmp
10/26/2020 16:00 149 startup.nsh
05/23/2018 17:52 <DIR> 4,096 efi
09/17/2021 13:01 992,755,712 recovery.rosfs
 3 File(s) 992,785,717 bytes
 2 Dir(s)
fs2:\> cd efi
fs2:\efi\> cd Recovery
fs2:\efi\Recovery\> dir
Directory of: fs2:\efi\Recovery\
05/23/2018 17:52 <DIR> 4,096 .
05/23/2018 17:52 <DIR> 4,096 ..
09/10/2021 21:39 19,417,336 boot.efi
 1 File(s) 19,417,336 bytes
 2 Dir(s)

```

기타 지침:

마운트된 부트 미디어가 포함된 올바른 파일 시스템을 확인합니다. 여러 파일 시스템을 탐색하고 ".efi" 부트 파일을 확인하여 이를 수행할 수 있습니다

 참고: 실제 부팅 미디어(업그레이드 파일 시스템)의 시퀀스(이 경우 "fs0:")는 다른 디바이스에도 다를 수 있습니다. 이름과 경로는 다를 수 있지만 모든 현대 이미지에서는 동일해야 합니다.

올바른 부트 미디어(업그레이드 파일 시스템)를 찾는 데 도움이 되는 체크리스트:

- 파일 시스템의 루트에 "vmlinuz-appliance"가 포함되어 있으면 부팅 미디어(업그레이드 파일 시스템)가 아닙니다.
- 파일 시스템의 루트에 "meta\_contents.tar.xz"가 포함되어 있으면 부트 미디어(업그레이드 파일 시스템)가 아닙니다.
- 파일 시스템에 "efi\boot\bootx64.efi"가 없으면 부트 미디어(파일 시스템 업그레이드)가 아닙니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.