

# Update Secure Malware Analytics-applicatie met airgap-modus

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beperkingen](#)

[Vereisten](#)

[Voordat u begint](#)

[Update en offline \(Airgapped\) Secure Malware Analytics-applicatie](#)

[Naamgevingsconventies](#)

[Beperkingen](#)

[Linux/MAC - ISO Download](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Download de ISO met de opdracht Desync](#)

[Windows - ISO Download](#)

[Download de ISO met de opdracht Desync](#)

[Verifiëren](#)

[Boot-applicatie van USB](#)

[Het juiste /dev apparaat vinden](#)

[status=voortgangsoptie](#)

[Boot Sequence voor HDD-stations voor offline upgrades](#)

[Voorschrift:](#)

---

## Inleiding

In dit document worden de stappen beschreven voor het bijwerken van de Air-Gap-modus van Secure Malware Analytics.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ingangen via opdrachtregel in Windows- en Unix/Linux-omgeving
- Kennis van Malware Analytic Applicatie

- Kennis van Cisco geïntegreerde beheercontroller (IMC)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Windows 10 en CentOS-8
- RUFUS 2,17
- C220 M4 router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

De meeste Secure Malware Analytics-apparaten zijn aangesloten op het internet en maken dus gebruik van het online updateproces. In sommige gevallen worden Secure Malware Analytics-apparaten echter alleen binnen interne netwerken onderhouden, dat wil zeggen "met lucht ingekapseld". We raden niet aan om apparaten luchtdicht te houden omdat dit ze minder effectief maakt; deze uitruil kan echter nodig zijn om extra beveiligings- of regelgevingsvereisten te ondersteunen.

Voor gebruikers die hun Secure Malware Analytics-apparaten draaien zonder verbinding met internet, bieden wij het offline updateproces dat in dit document wordt beschreven. Upgrademedia worden op verzoek geleverd door Secure Malware Analytics Support; zie hieronder voor meer informatie.

Media: Airgap (offline) updatemedia wordt geleverd door Secure Malware Analytics Support als een ISO, die kan worden gekopieerd naar een USB-media of HDD (vaste schijf) als een van de geschikte grootte beschikbaar is.

Grootte: De grootte hangt af van welke versies de updatemedia steunt, maar het kan vaak verscheidene tientallen gigabytes zijn wanneer nieuwe VMs tussen bron en bestemmingsversies worden geïntroduceerd. Bij de huidige releases kan het ongeveer 30 GB zijn, omdat de desync-tool helpt bij het geleidelijk bijwerken van de VM-gerelateerde wijzigingen.

Upgradeopstartcyclus: elke keer dat de airgap-updatemedia wordt opgestart, wordt de volgende release bepaald om naar te upgraden en wordt de inhoud van de volgende release naar het apparaat gekopieerd. Een bepaalde release kan ook een pakketinstallatie starten als die release geen enkele noodzakelijke controles heeft die uitgevoerd moeten worden terwijl het apparaat in bedrijf is. Als de release zulke controles bevat of een overschrijving op delen van het updateproces die zulke controles kunnen toevoegen, dan is de update niet van toepassing totdat de gebruiker zich aanmeldt bij OpAdmin en de update aanhaalt met OpAdmin > Operations > Update applicatie.

Vóór de installatie gebruikte haken: afhankelijk van de vraag of er voor die specifieke upgrade voorafgaand aan de installatie haken aanwezig zijn, wordt de upgrade direct uitgevoerd of wordt het apparaat opnieuw opgestart in de normale bedrijfsmodus, zodat de gebruiker de gebruikelijke administratieve interface kan invoeren en de upgrade met de hand kan starten.

Herhaal zoals nodig: Elk van deze media bootcyclus verbetert (of bereidt zich voor om te upgraden) slechts één stap naar de uiteindelijke doelrelease; de gebruiker moet zo vaak als nodig opstarten om te upgraden naar de gewenste doelrelease.

## Beperkingen


CIMC-media worden niet ondersteund voor air-gapped updates.

Als gevolg van licentiebeperkingen op gebruikte componenten van derden zijn upgrademedia voor 1.x-releases niet langer beschikbaar nadat UCS M3-hardware EOL (end-of-life) heeft bereikt. Het is dus van cruciaal belang dat UCS M3-toestellen worden vervangen of verbeterd voordat ze worden afgestoten.

## Vereisten

Migraties: Als de release notities voor releases waarop de richtlijn betrekking heeft scenario's bevatten waarin migratie verplicht is voordat de volgende versie wordt geïnstalleerd, moet de gebruiker deze stappen volgen voordat hij opnieuw start om te voorkomen dat het apparaat in onbruikbare staat wordt geplaatst.

---

 **Opmerking:** De eerste 2.1.x release nieuwer dan 2.1.4, in het bijzonder, voert verschillende database migraties uit. Het is onveilig om door te gaan totdat deze migraties zijn voltooid. Raadpleeg de [Threat Grid-applicatie 2.1.5 Migratieopmerking voor](#) meer informatie.

---

Als wordt begonnen met een release voor 2.1.3, maakt airgap upgrade media gebruik van een coderingssleutel die is afgeleid van de individuele licentie en moet dus worden aangepast per apparaat. (Het enige door de gebruiker zichtbare effect is dat Secure Malware Analytics, met media die gebouwd zijn om pre-2.1.3 oorsprongversies te ondersteunen, eerst de licenties nodig heeft die op die apparaten zijn geïnstalleerd, en dat de media niet zullen werken op apparaten die niet voorkomen in de lijst waarvoor ze zijn gemaakt.)

Als het begin met release 2.1.3 of daarna, de airgap media is generiek en de klant informatie is niet nodig.

## Voordat u begint

- Reserve. U moet overwegen een back-up van uw apparaat te maken voordat u doorgaat met de update.
- Bekijk de Releaseopmerkingen voor de release die u wilt bijwerken om te controleren of er achtergrondmigraties vereist zijn voordat u de nieuwere release wilt bijwerken
- Controleer de huidige versie van uw apparaat: OpAdmin > Operations > Update applicatie

- Bekijk de geschiedenis van de Secure Malware Analytics-applicatie in de Build Number/Version Lookup Table, die beschikbaar is in alle [Threat Grid-applicatiedocumenten](#): Releaseopmerkingen, Migratieopmerkingen, Setup- en configuratiehandleiding en beheerdershandleiding.

## Update en offline (Airgapped) Secure Malware Analytics-applicatie

Eerste controle beschikbaar Air Gapped versie op deze pagina: [Applicatie Versie Lookup Tabel](#)

1. Open een TAC-ondersteuningsverzoek om de offline updatemedia te verkrijgen. Deze aanvraag moet het serienummer van het apparaat en het compilatienummer van het apparaat bevatten.
2. TAC Support levert een bijgewerkte ISO op basis van uw installatie.
3. Verbrand de ISO-afbeelding op een opstartbare USB. USB is het enige ondersteunde apparaat/de enige methode voor offline updates.

### Naamgevingsconventies

Dit is de bijgewerkte bestandsnaam ex: TGA Airgap Update 2.13.2-2.14.0.

Dit betekent dat deze media kunnen worden gebruikt voor een apparaat met een minimumversie: 2.13.2 en dat het apparaat kan worden opgewaardeerd naar versie: 2.14.0.

### Beperkingen

- CIMC-media worden niet ondersteund voor air-gapped updates.
- Als gevolg van licentiebeperkingen op gebruikte componenten van derden zijn upgrademedia voor 1.x-releases niet langer beschikbaar nadat UCS M3-hardware EOL (end-of-life) heeft bereikt. Het is dus van cruciaal belang dat UCS M3-toestellen worden vervangen of verbeterd voordat ze worden afgestoten.

## Linux/MAC - ISO Download

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een Linux-machine met internettoegang om de ISO te downloaden en de opstartbare USB-installatiedrive te maken.
- De Airgap Download Instructies worden geleverd door Secure Malware Analytics Ondersteuning.
- GO Programmeertaal. [Downloaden](#)
- Het bestand met de .caibx-index (opgenomen in het zip-bestand dat wordt geleverd door TAC Support).
- Desync Tool (opgenomen in het zipbestand dat wordt geleverd door Secure Malware Analytics Support).

## Gebruikte componenten

De informatie in dit document is gebaseerd op een CentOS Linux release 7.6.1810 (Core).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

### Installeer de GO Programmeertaal

```
# 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
```

Voer deze drie opdrachten uit nadat de installatie is voltooid, indien niet de opdracht desync mislukt

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

U kunt de GO-versie controleren door:

```
# go version
```

## Download de ISO met de opdracht Desync

Stap 1. Kopieer de inhoud van het zip-bestand dat wordt geleverd door Secure Malware Analytics Support, inclusief het bestand desync.linux en .caibx in dezelfde map lokaal op het apparaat.

Stap 2. Wijzing in de map naar waar u de bestanden hebt opgeslagen:

Voorbeeld:


```
# cd MyDirectory/TG
```

Stap 3. Voer de pwd-opdracht uit om er zeker van te zijn dat u zich in de map bevindt.

```
# pwd
```

Stap 4. Zodra u binnen de map die de opdracht desync.linux en het .caibx-bestand omvat, voert u de opdracht van uw keuze uit om het downloadproces te starten.

---

 **Opmerking:** Dit zijn de voorbeelden voor verschillende ISO-versies. Raadpleeg het .caibx bestand vanuit de instructies van Secure Malware Analytics Support.

---

Voor versie 2.1.3 tot en met 2.4.3.2 van ISO:

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

Voor versie 2.4.3.2 tot en met 2.5 ISO:


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

Voor versie 2.5 tot en met 2.7.2ag ISO:

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

Zodra de download begint, wordt er een voortgangsbalk weergegeven.

---

 **Opmerking:** de downloadsnelheid en de grootte van de upgrademedia in uw omgeving kunnen invloed hebben op de tijd om de ISO te maken.  
Vergelijk de MD5 van het gedownloade bestand met de bundel die wordt geleverd door ondersteuning om de integriteit van de gedownloade ISO te valideren.

---

Zodra de download is voltooid, worden de ISO's in dezelfde directory aangemaakt.

Sluit de USB-stick aan op de machine en voer de dd-opdracht uit om de opstartbare USB-drive te maken.

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

Waar <MY\_USB> de naam van uw USB-stick is (laat de haakjes los).

Plaats de USB-stick en schakel het apparaat in of herstart het. Druk op F6 om het opstartmenu in te voeren op het scherm om Cisco op te starten.



Tip:

Draai de download na kantooruren of off-peakuren aangezien het bandbreedte zou kunnen beïnvloeden.

Sluit de terminal of druk op Ctrl+c/Ctrl+z om het gereedschap te stoppen.

Als u wilt doorgaan, voert u dezelfde opdracht uit om de download te hervatten.

## Windows - ISO Download

Installeer de GO Programmeertaal

#1: Download de vereiste GO programmeertaal. Installeer via <https://golang.org/dl/> In mijn geval kies ik de Getoonde Versie. Start uw CMD opnieuw en test met

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**

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

Sluit de CMD-run en open deze opnieuw om te verifiëren:

```
go version
```

```
C:\Users\rvalenta>go version  
go version go1.16.6 windows/amd64
```

Download de ISO met de opdracht Desync

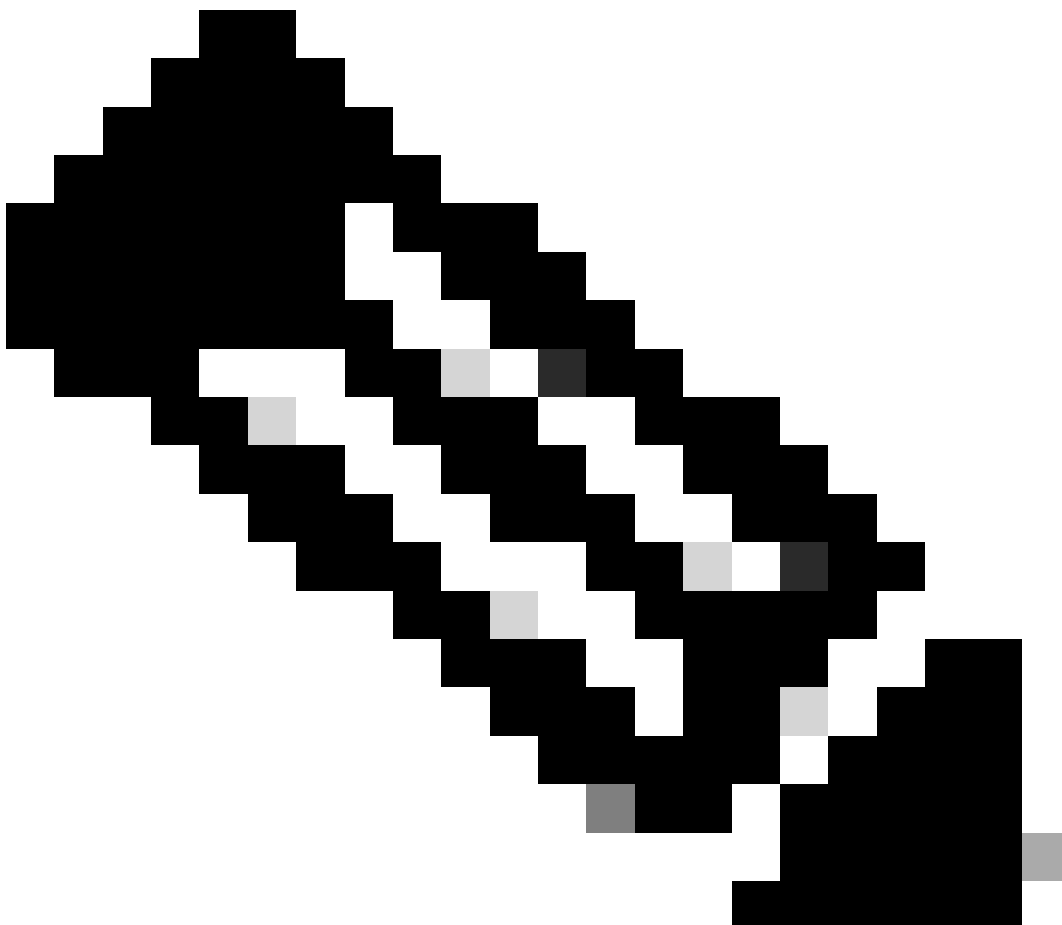
#2: Installeer het DESYNC-programma. Na de uitvoering van de opdracht, kunt u een hoop download aanwijzingen opmerken. Ruwweg na 2-3 minuten moet de download gedaan worden.

```
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
```

---



Opmerking: als git commando niet werkt dan kunt u downloaden en installeren Git van

---



hier: <https://git-scm.com/download/win>.

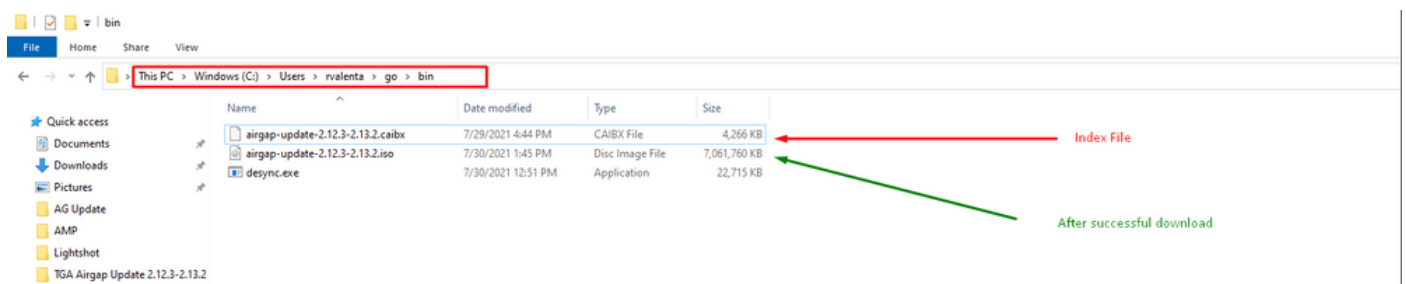
Dan loop onder twee bevelen één voor één:

```
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-eec23a3978ad
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: Navigeren om te gaan —> bin locatie. In mijn geval was het C:\Users\rvalenta\go\bin en kopieer/plak daar TAC verstrekte .caibx indexbestand.



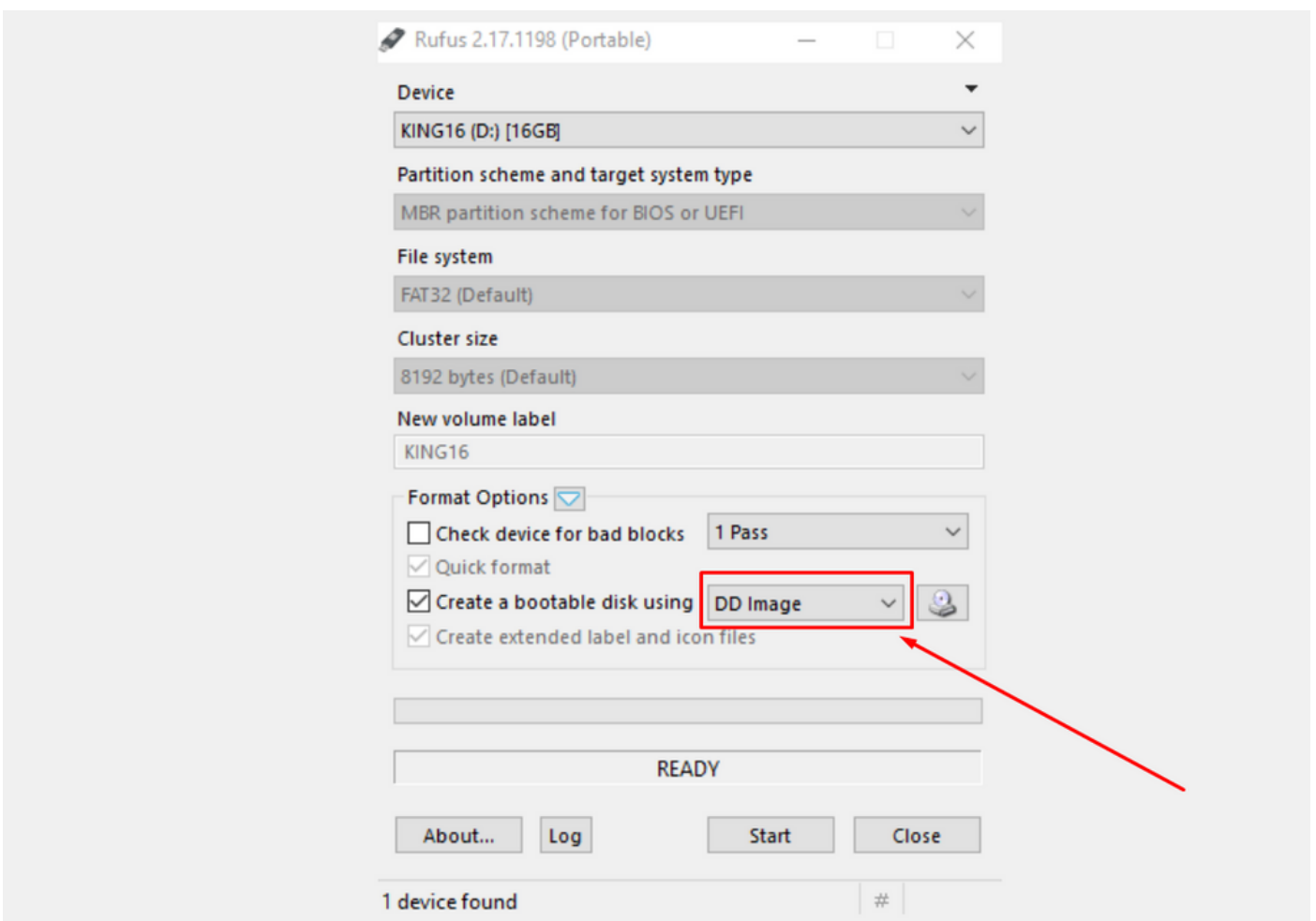
Verifiëren

#4: Ga terug naar de CMD-prompt en navigeer naar de map go\bin en voer de downloadopdrachten uit. U moet onmiddellijk zien dat de download verdergaat. Wacht tot de download is voltooid. U moet nu het gehele .ISO bestand op dezelfde locatie hebben als het eerder gekopieerde indexbestand .caibx

```
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>
```

Gebruik dan RUFUS om een opstartbare USB te maken. Dit is erg belangrijk om versie 2.17 te gebruiken. Dit is de laatste versie waar u add-opties kunt gebruiken die zeer belangrijk is om dit specifieke herstel USB te maken. U kunt alle versies van deze repository [RUFUS REPOSITORY](#) vinden Als deze bestanden niet meer beschikbaar zijn, neem ik ook installateurs voor volledige en draagbare versies op in dit document.



## Boot-applicatie van USB

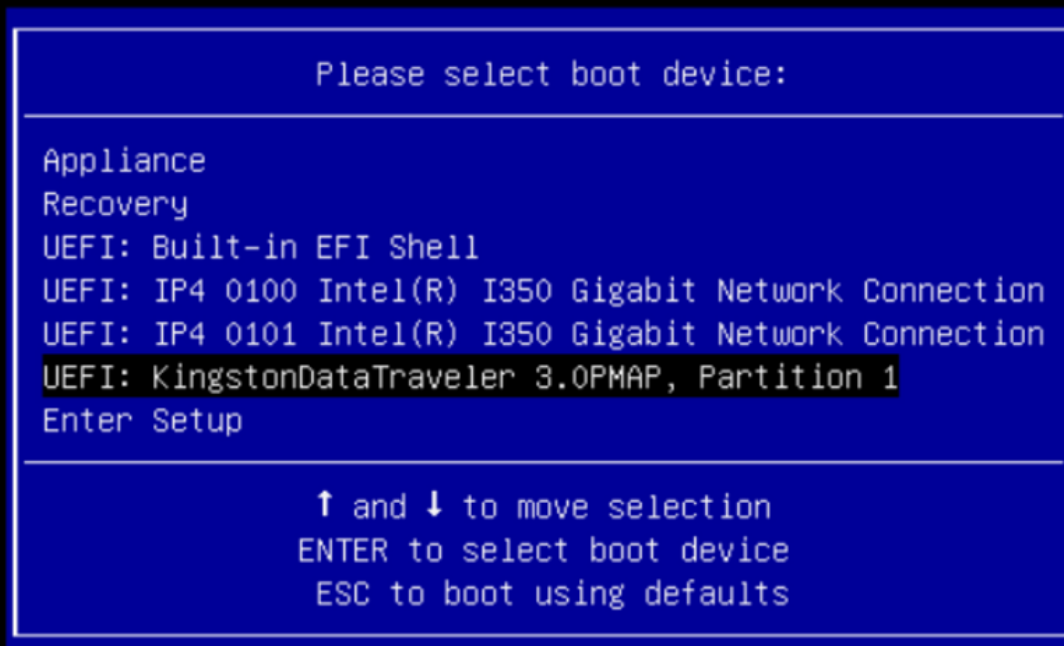
Plaats de USB-stick en schakel het apparaat in of herstart het. Selecteer "F6" in het opstartmenu van Cisco op het opstartscherm. Je moet snel zijn! Je hebt maar een paar seconden om deze selectie te maken. Als je het mist, moet je opnieuw opstarten en opnieuw proberen.

Afbeelding 1 - Druk op F6 om het opstartmenu in te voeren



Navigeer naar het USB-station met de update en druk op Enter om te selecteren:

Afbeelding 2 - Selecteer de Update USB



De updatemedia bepaalt de volgende release in het upgradepad en kopieert de inhoud voor die release naar het apparaat. Het apparaat voert de upgrade direct uit of start de normale werking opnieuw op, zodat u de OpAdmin kunt invoeren en handmatig kunt starten.

Wanneer het opstartproces van de ISO is voltooid, start u het Secure Malware Analytics-apparaat opnieuw op in de bedrijfsmodus.

Meld u aan bij de portal UI en controleer voordat u verdergaat of er waarschuwingen zijn die aangeven of het veilig is om te upgraden, enzovoort.

Navigeer naar de OpAdmin-interface en pas de updates toe, als ze niet automatisch werden toegepast tijdens de reboot: OpAdmin > Operations > Update-applicatie **OPMERKING:** Het updateproces omvat extra reboots als onderdeel van de update, die is gemaakt van de USB-media. U moet bijvoorbeeld de knop Reboot op de installatiepagina gebruiken nadat er updates zijn geïnstalleerd.

Herhaal dit voor elke versie op de USB stick.

Het juiste /dev apparaat vinden

Als de USB nog steeds niet is aangesloten op het eindpunt, voer dan de opdracht "sblk | 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$
```

Nadat de USB-stick is aangesloten.

```
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$
```

Dit bevestigt dat het USB-apparaat in /dev "/dev/sdb" is.

Andere manieren om te bevestigen, nadat de USB-stick is aangesloten:

Het commando dmesg geeft wat informatie. Nadat de USB-stick is aangesloten, voert u de opdracht dmesg uit | grep -iE 'usb|attach'.

```
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$
```


De commando `fdisk` geeft informatie over de grootte, die kan worden gebruikt om te bevestigen:  
`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$
```

---

 **Opmerking:** Vergeet niet om de USB-stick te ontkoppelen voor de uitvoering van de opdracht "dd".

---

Bevestiging dat het USB-apparaat van het voorbeeld is gemonteerd.

```
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,umask=0
```

Om het USB-apparaat te ontkoppelen gebruikt u `sudo umount /dev/sdb1`.

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

Controleer of de voorziening niet als "gemonteerd" wordt ervaren.

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

status=voortgangsoptie

oflag=sync en status=progress opties in de opdracht toevoegen.

Bij het schrijven van talrijke gegevensblokken geeft de optie "status=progress" informatie over de huidige schrijfbewerkingen. Dit is handig om te bevestigen of de opdracht "dd" momenteel aan het paginacache schrijft; het kan worden gebruikt om de voortgang en de volledige hoeveelheid tijd in seconden van alle schrijfbewerkingen te tonen.

Indien niet gebruikt, geeft "dd" geen informatie over de voortgang, alleen de resultaten van de schrijfbewerkingen worden gegeven voordat "dd" teruggeeft:

```
[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]$
```

Bij gebruik wordt real-time informatie over de schrijfbewerkingen elke seconde bijgewerkt.

```
[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]
```



Opmerking: In de officiële documentatie voor het offline TGA-upgradeproces wordt de volgende opdracht gegeven: `dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M`

---

Na enkele testen wordt het volgende voorbeeld waargenomen.

Zodra een bestand van 10MB is gemaakt met "dd" met behulp van apparaat /dev/zero.


1M x 10 = 10M (10240 kB + vorige systeemgegevens in vuile bestandspaginacaches = 10304 kB  
—> dit wordt waargenomen in het vuile paginacache aan het einde van "dd").

```
[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
```

---

 **Opmerking:** Nadat de opdracht "dd" is teruggegeven, is de schrijfbewerking op het blokapparaat niet voltooid, maar 11 seconden na de terugkeer wordt deze waargenomen. Als dit de opdracht "dd" was bij het maken van de opstartbare USB met de TGA ISO, EN ik had de USB verwijderd van het eindpunt voor die 11 seconden = ik zou een beschadigde ISO in de opstartbare USB.

---

Uitleg:

Blokapparaten bieden gebufferde toegang tot hardwareapparaten. Dit biedt een laag van abstractie aan toepassingen wanneer het werken met hardwareapparaten.

Blokapparaten maken het mogelijk om een toepassing te lezen/schrijven met gegevensblokken van verschillende grootte; deze read()/writes() wordt toegepast op de pagina-caches (buffers) en niet direct op het blok-apparaat.

De kernel (en niet de toepassing die het lezen/schrijven doet) beheert de beweging van gegevens van de buffers (pagina-caches) naar de blokapparaten.

Daarom:

De applicatie (in dit geval "dd") heeft geen controle over de flush van de buffers als dit niet geïnstrueerd wordt.

De optie "oflag=sync" dwingt synchroon fysiek schrijven (door de kernel) na elk uitvoerblok (geleverd door "dd") wordt in het paginacache geplaatst.

oflag=sync vermindert de "dd" prestaties in vergelijking met het niet gebruiken van de optie; maar



als deze optie is ingeschakeld, zorgt het ervoor dat fysiek naar het blok apparaat wordt geschreven na elke schrijf() aanroep van "dd".

Test: Het gebruik van de optie "oflag=sync" van de opdracht "dd" om te bevestigen dat alle schrijfbewerkingen met de vuile paginacache gegevens waren voltooid bij de terugkeer van de opdracht "dd":


```
[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]$
```

Er blijven geen gegevens over van de schrijfhandeling in het vuile paginacache.

De schrijfhandeling werd toegepast voor (of op hetzelfde moment) de opdracht "dd" werd teruggegeven (niet 11 seconden na de vorige test).

Nu ben ik er zeker van dat na de "dd" opdracht teruggegeven was er geen gegevens in het vuile paginacache met betrekking tot de schrijfhandeling = geen problemen in de bootable USB-creatie (als de ISO-checksum correct is).

---

 Opmerking: houd rekening met deze vlag (oflag=sync) van de opdracht "dd" wanneer u aan dit soort case werkt.

---

## Boot Sequence voor HDD-stations voor offline upgrades

Voorschrift:

We moeten ervoor zorgen dat de vaste schijf met behulp van alle beschikbare gereedschappen wordt geformatteerd met de optie "DD" en dat de media nadien naar het station worden gekopieerd. Als we deze opmaak niet gebruiken, kunnen we deze media niet lezen.

Zodra de media zijn geladen op de HDD/USB met behulp van de "DD"-opmaak, moeten we die aansluiten op de TGA-applicatie en het apparaat opnieuw opstarten.

Dit is het standaardscherm voor de selectie van het opstartmenu. We moeten op "F6" drukken om het apparaat op te starten om de opstartmedia te selecteren



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

Zodra het apparaat onze input herkent, zou het vragen dat het apparaat zou invoeren het laarsselectie menu.



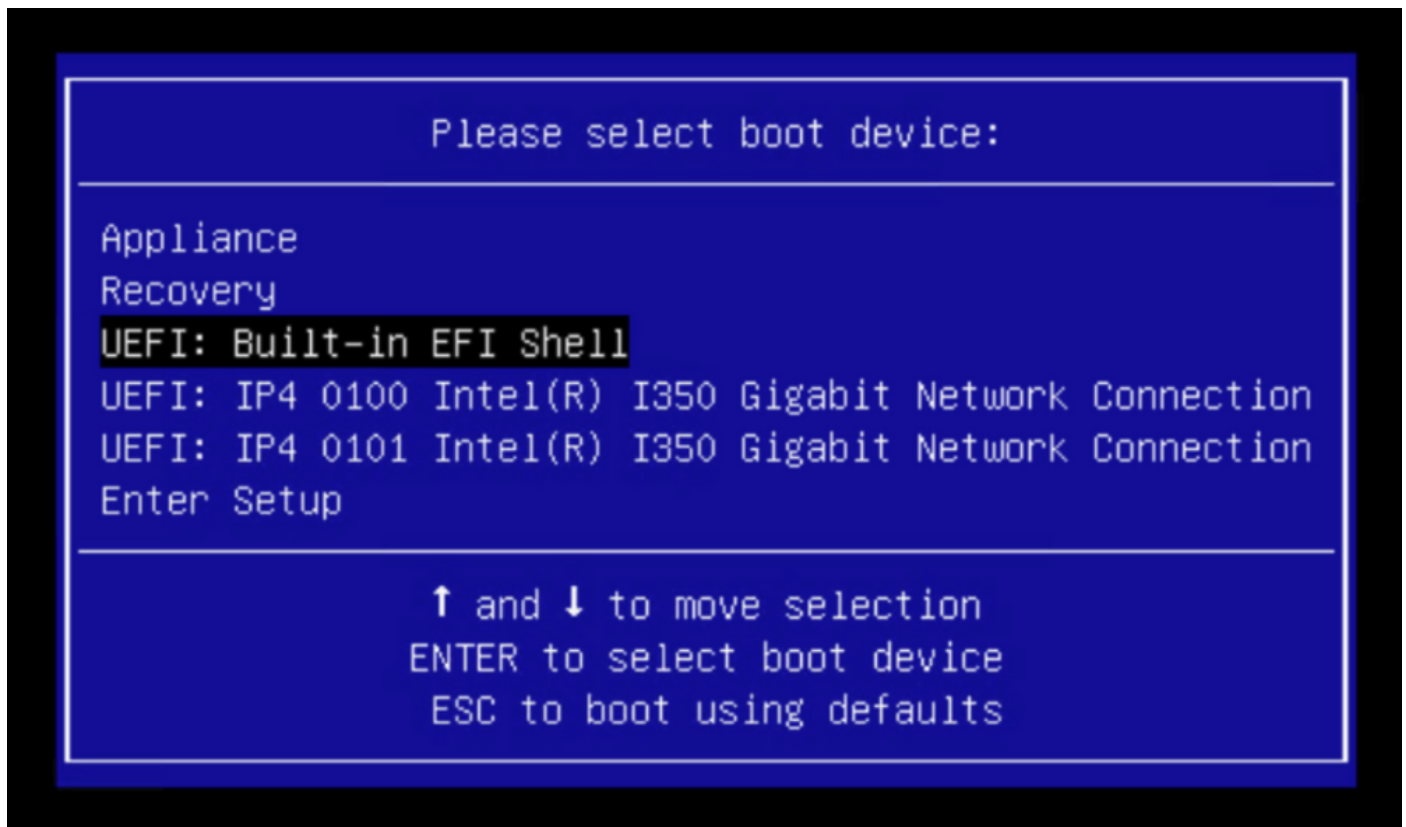
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,  
<F12> Network Boot

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...

Dit is de prompt die kan verschillen tussen verschillende TGA-modellen. Idealiter zouden we de optie zien om te starten met behulp van de boot media (upgrade bestandssysteem) van dit menu zelf, maar als het niet wordt gezien, moeten we inloggen in de "EFI Shell".



Je zou op "ESC" moeten drukken voordat het "startup.sh" script klaar is om naar de EFI Shell te gaan. Zodra we inloggen in de EFI Shell, zouden we merken dat de in dit geval gedetecteerde partities 3 bestandssystemen zijn: 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,
0x400000)
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,
0x05A6FDF)
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> _

```

## Belangrijk

Het juiste bestandssysteem identificeren:

- Volgens de bovenstaande screenshot, zou je kunnen zien dat "fs0:" is de enige media met "USB" in hun pad en daarom kunnen we er zeker van zijn dat dit bestandssysteem de boot media (upgrade bestandssysteem) zou bevatten.

Bij ontbrekende bestandssystemen:

- Als alleen fs0: en fs1: beschikbaar zijn en er geen fs2:, controleer dan of de opstartmedia (upgrade-bestandssysteem) in de dd-modus zijn geschreven en met succes zijn verbonden.
- Boot media (upgrade bestandssysteem) moeten altijd een lager aantal hebben dan de herstelmedia, en ze moeten altijd naast elkaar staan; het is of de USB-aangesloten schijf aan het begin van het einde is dat waarschijnlijk zal veranderen (dus, of het de voorpositie bij fs0: of de achterpositie bij fs2:) zou moeten worden geïdentificeerd
- In dit geval in de screenshot hieronder, is het juiste ".efi" bestand zoals het onder de "efi\boot" partitie is en heeft de naamgevingsconventie van "bootx64.efi"

```
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)
```

Om het apparaat in de opstartmedia (upgrade bestandssysteem) op te starten, moeten we het bestand "bootx64.efi" uitvoeren:

```
fs0:\efi\boot\bootx64.efi
```

Voor uw referentie, hebben we de inhoud van de andere bestands systemen weergegeven, evenals hieronder:

fs1: Dit is het belangrijkste systeem van de laarsfilesysteem.

```

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: Dit is het herstelimage bootfilesysteem.

```

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)

```

Diverse instructies:

Om het juiste bestandssysteem te verifiëren dat de opstartmedia bevat. Dit kunnen we doen door door door de verschillende bestandssystemen te bladeren en het ".efi" opstartbestand te controleren

---

 **Opmerking:** De volgorde van de feitelijke opstartmedia (upgrade bestandssysteem) die in dit geval "fs0:" is, kan ook variëren met andere apparaten. De naam en het pad kunnen variëren, maar in alle moderne afbeeldingen moet dit hetzelfde zijn.

---

Checklist die kan helpen de juiste opstartmedia te vinden (upgrade bestandssysteem):

- Als de wortel van een bestandssysteem "vmlinuz-toestel" bevat, is het niet de opstartmedia (upgrade filesystem).
- Als de wortel van een filesystem "meta\_content.tar.xz" bevat, is het niet de laarsmedia (upgrade filesystem).
- Als een bestandssysteem geen "efi\boot\bootx64.efi" bevat, is het niet de opstartmedia (upgrade filesystem).

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.