

# Actualizar el modo Air-Gap de Secure Malware Analytics Appliance

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Limitaciones](#)

[Requirements](#)

[Antes de comenzar](#)

[Actualizar un dispositivo de análisis de malware seguro sin conexión \(Airgapped\)](#)

[Convenciones para la asignación de nombres](#)

[Limitaciones](#)

[Linux/MAC - Descarga de ISO](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Descargue el ISO mediante el comando Desync](#)

[Windows - Descarga de ISO](#)

[Descargue el ISO mediante el comando Desync](#)

[Verificación](#)

[Arranque del dispositivo desde USB](#)

[Cómo encontrar el dispositivo /dev correcto](#)

[status=opción de progreso](#)

[Secuencia de arranque para unidades de disco duro para actualizaciones fuera de línea](#)

[Requisito:](#)

---

## Introducción

Este documento describe los pasos para actualizar el modo Air-Gap de Secure Malware Analytics Appliance.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de entradas a través de la línea de comandos en entornos Windows y Unix/Linux

- Conocimiento del dispositivo de análisis de malware
- Conocimientos de Cisco Integrated Management Controller (IMC)

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Windows 10 y CentOS-8
- RUFUS 2,17
- C220 M4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

La mayoría de los dispositivos Secure Malware Analytics están conectados a Internet y, por tanto, utilizan el proceso de actualización en línea. Sin embargo, en algunos casos, los appliances de Secure Malware Analytics se mantienen estrictamente dentro de las redes internas, es decir, "sin protección". No recomendamos mantener los dispositivos aislados al aire, ya que de este modo se reduce su eficacia; sin embargo, esta disyuntiva puede ser necesaria para cumplir requisitos de seguridad o normativos adicionales.

Para aquellos usuarios que ejecuten sus dispositivos Secure Malware Analytics sin conexión a Internet, proporcionamos el proceso de actualización sin conexión descrito en este documento. El soporte de Secure Malware Analytics proporciona medios de actualización a petición, consulte a continuación para obtener más información.

**Medios:** El soporte de Secure Malware Analytics proporciona medios de actualización Airgap (sin conexión) como un ISO, que se puede copiar en un medio USB o HDD (unidades de disco duro) si hay disponibles unidades de tamaño adecuado.

**Tamaño:** El tamaño depende de las versiones que admita el medio de actualización, pero a menudo puede ser de varias decenas de gigabytes cuando se introducen nuevas VM entre las versiones de origen y destino. Con las versiones actuales, podría rondar los 30 GB, ya que la herramienta desync ayuda a actualizar los cambios relacionados con la VM de forma incremental.

**Ciclo de inicio de actualización:** cada vez que se inicia el medio de actualización de AirGap, determina la siguiente versión a la que se debe actualizar y copia el contenido asociado a esa siguiente versión en el dispositivo. Una versión determinada también puede iniciar la instalación de un paquete si dicha versión no tiene ninguna comprobación de requisitos previos que se deba ejecutar mientras el dispositivo se está ejecutando. Si la versión incluye dichas comprobaciones o una sustitución en partes del proceso de actualización que podrían agregar dichas comprobaciones, la actualización no se aplicará realmente hasta que el usuario inicie sesión en

OpAdmin e invoque la actualización con OpAdmin > Operations > Update Appliance.

Ganchos de preinstalación: en función de si hay algún gancho de preinstalación para esa actualización específica, ejecuta la actualización inmediatamente o reinicia el dispositivo en su modo de funcionamiento normal para permitir al usuario entrar en la interfaz administrativa habitual e iniciar la actualización manualmente.

Repetir según sea necesario: cada ciclo de arranque de medios de este tipo actualiza (o prepara la actualización) solo un paso hacia la versión final de destino; el usuario debe arrancar tantas veces como sea necesario para actualizar a la versión de destino deseada.

## Limitaciones


El medio CIMC no es compatible con las actualizaciones por espacios de aire.

Debido a las limitaciones de licencia de los componentes de terceros utilizados, los medios de actualización para las versiones 1.x ya no están disponibles después de que el hardware UCS M3 haya alcanzado el fin de vida útil (EOL). Por lo tanto, es fundamental que los appliances UCS M3 se sustituyan o actualicen antes de la fase EOL.

## Requirements

Migraciones: si las notas de la versión de las versiones incluidas incluyen situaciones en las que es obligatorio que la migración se realice antes de instalar la siguiente versión, el usuario debe seguir estos pasos antes de reiniciar de nuevo para evitar que el dispositivo quede en un estado inutilizable.

---

 Nota: La primera versión 2.1.x más reciente que la 2.1.4, en particular, ejecuta varias migraciones de bases de datos. No es seguro continuar hasta que se completen estas migraciones. Para obtener más información, consulte la [nota de migración de Threat Grid Appliance 2.1.5](#).

---

Si a partir de una versión anterior a la 2.1.3, el medio de actualización airgap utiliza una clave de cifrado derivada de la licencia individual y, por lo tanto, debe personalizarse por dispositivo. (El único efecto visible para el usuario es que, con medios creados para admitir versiones de origen anteriores a la 2.1.3, Secure Malware Analytics necesita las licencias instaladas en esos dispositivos de antemano y los medios no funcionarán en ningún dispositivo que no esté en la lista para la que se creó.)

Si se empieza con la versión 2.1.3 o posterior, el medio de ventilación es genérico y no se necesita información del cliente.

## Antes de comenzar

- Copia de seguridad. Debe considerar la posibilidad de realizar una copia de seguridad del dispositivo antes de continuar con la actualización.
- Revise las notas de la versión de la versión que desea actualizar para comprobar si hay

- alguna migración en segundo plano necesaria antes de actualizar a la versión más reciente
- Verifique la versión actual de su dispositivo: OpAdmin > Operations > Update Appliance
  - Revise el historial de versiones del dispositivo Secure Malware Analytics en la tabla de búsqueda de número de compilación/versión, que está disponible en todos los [documentos del dispositivo Threat Grid](#): Release Notes, Migration Notes, Setup and Configuration Guide y Administrator's Guide.

## Actualizar un dispositivo de análisis de malware seguro sin conexión (Airgapped)

En primer lugar, compruebe la versión de Air Gapped disponible en esta página: [Tabla de Consulta de la Versión del Dispositivo](#)

1. Abra una solicitud de asistencia del TAC para obtener los medios de actualización sin conexión. Esta solicitud debe incluir el número de serie del dispositivo, así como el número de compilación del dispositivo.
2. El soporte del TAC proporciona una ISO actualizada basada en su instalación.
3. Grabe la imagen ISO en un USB de arranque. Tenga en cuenta que USB es el único dispositivo/método compatible para las actualizaciones sin conexión.

### Convenciones para la asignación de nombres

Este es el nombre de archivo actualizado, por ejemplo: TGA Airgap Update 2.13.2-2.14.0.

Esto significa que este medio se puede utilizar para un dispositivo que ejecuta una versión mínima: 2.13.2 y actualizar el dispositivo a la versión: 2.14.0.

### Limitaciones

- El medio CIMC no es compatible con las actualizaciones por espacios de aire.
- Debido a las limitaciones de licencia de los componentes de terceros utilizados, los medios de actualización para las versiones 1.x ya no estarán disponibles después de que el hardware UCS M3 haya alcanzado el fin de vida útil (EOL). Por lo tanto, es fundamental que los appliances UCS M3 se sustituyan o actualicen antes de la fase EOL.

## Linux/MAC - Descarga de ISO

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Una máquina Linux con acceso a Internet para descargar el ISO y crear la unidad de instalación USB de arranque.
- Las instrucciones de descarga de Airgap las proporciona Secure Malware Analytics Support.
- lenguaje de programación GO. [Descargar](#)
- El archivo de índice .caibx (incluido en el archivo zip proporcionado por el Soporte del TAC).

- Herramienta de desincronización (incluida en el archivo zip proporcionado por Secure Malware Analytics Support).

## Componentes Utilizados

La información de este documento se basa en una versión 7.6.1810 (Core) de CentOS Linux.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

### Instalación del lenguaje de programación GO

```
# 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
```

Ejecute estos tres comandos después de la instalación, si no falla el comando desync

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

Puede verificar la versión GO de la siguiente manera:

```
# go version
```

Descargue el ISO mediante el comando Desync

Paso 1. Copie el contenido del archivo Zip proporcionado por Secure Malware Analytics Support, incluidos los archivos desync.linux y .caibx en el mismo directorio localmente en el equipo.

Paso 2. Cambie al directorio en el que almacenó los archivos:

Ejemplo:


```
# cd MyDirectory/TG
```

Paso 3. Ejecute el comando `pwd` para asegurarse de que está dentro del directorio.

```
# pwd
```

Paso 4. Una vez que esté dentro del directorio que incluye el comando `desync.linux` y el archivo `.caibx`, ejecute el comando de su elección para comenzar el proceso de descarga.

---

 Nota: Estos son los ejemplos para las diferentes versiones de ISO; consulte el archivo `.caibx` de las instrucciones proporcionadas por Secure Malware Analytics Support.

---

Para las versiones 2.1.3 a 2.4.3.2 ISO:

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

Para las versiones 2.4.3.2 a 2.5 ISO:


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

Para las versiones 2.5 a 2.7.2ag ISO:

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

Una vez que comienza la descarga, se muestra una barra de progreso.

---

 Nota: La velocidad de descarga y el tamaño del medio de actualización en su entorno pueden afectar al tiempo de composición de la ISO. Asegúrese de comparar el MD5 del archivo descargado con el disponible con el paquete proporcionado por el soporte para validar la integridad del ISO descargado.

---

Una vez completada la descarga, los ISO se crean en el mismo directorio.

Conecte el USB a la máquina y ejecute el comando `dd` para crear la unidad USB de arranque.

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

Donde <MY\_USB> es el nombre de la llave USB (no entre paréntesis angulares).

Introduzca la unidad USB y encienda o reinicie el equipo. En la pantalla de inicio de Cisco, presione F6 para ingresar al Menú de inicio.

 Consejo:

Ejecute la descarga después de las horas de oficina o fuera de las horas pico, ya que podría afectar al ancho de banda.

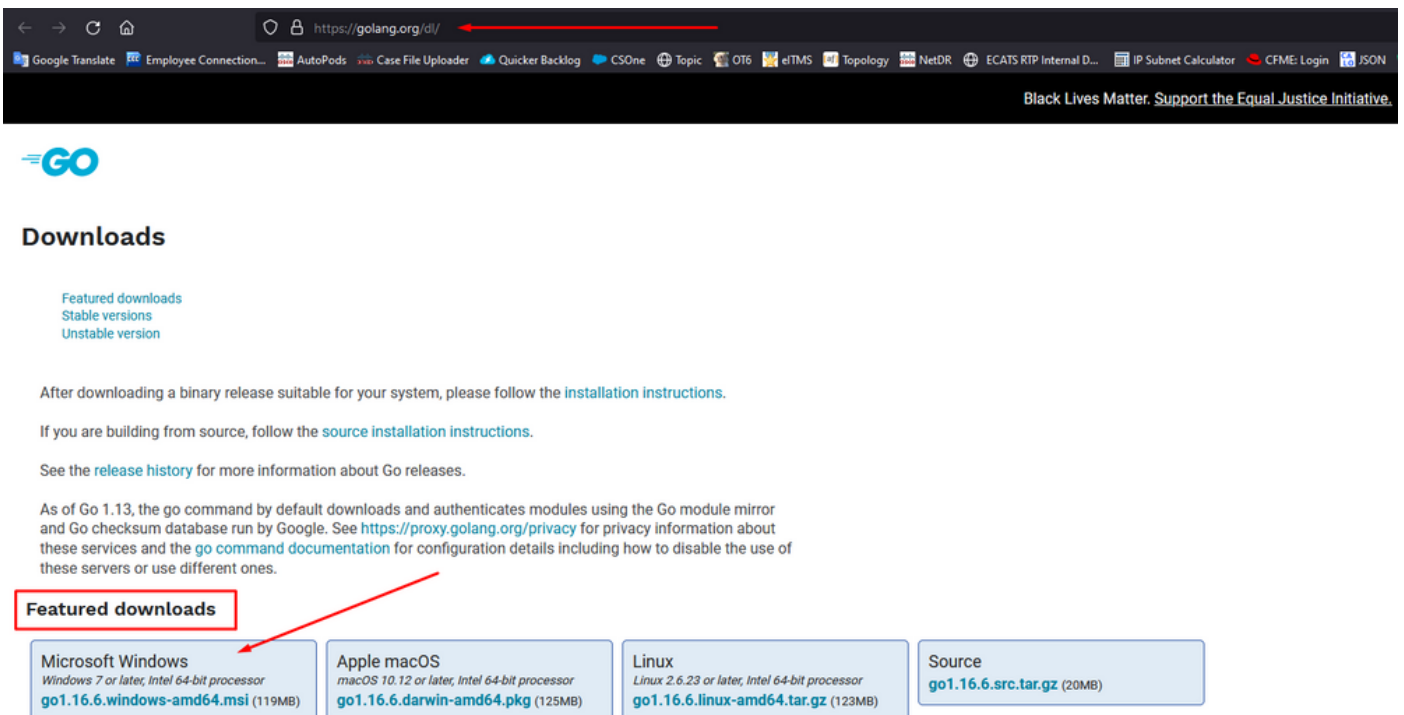
Para detener la herramienta, cierre el terminal o presione Ctrl+c/Ctrl+z.

Para continuar, ejecute el mismo comando para reanudar la descarga.

## Windows - Descarga de ISO

### Instalación del lenguaje de programación GO

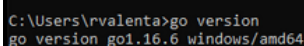
#1: Descargue el lenguaje de programación GO necesario. Instalar desde <https://golang.org/dl/> En mi caso elijo la versión destacada. Reinicie el CMD y pruébelo con



The screenshot shows the Golang download page. The browser address bar is <https://golang.org/dl/>. The page has a navigation bar with various links and a footer with a Black Lives Matter message. The main content area is titled "Downloads" and includes links for "Featured downloads", "Stable versions", and "Unstable version". Below this, there are instructions for downloading and installing Go. A red box highlights the "Featured downloads" section, and a red arrow points to the "Microsoft Windows" download button. The download buttons are for "Microsoft Windows" (119MB), "Apple macOS" (125MB), "Linux" (123MB), and "Source" (20MB).

Cierre y vuelva a abrir el comando CMD run para verificar:

```
go version
```



The terminal screenshot shows the command `go version` being executed in a Windows Command Prompt. The output is `go version go1.16.6 windows/amd64`. A red arrow points to the output text.

Descargue el ISO mediante el comando Desync

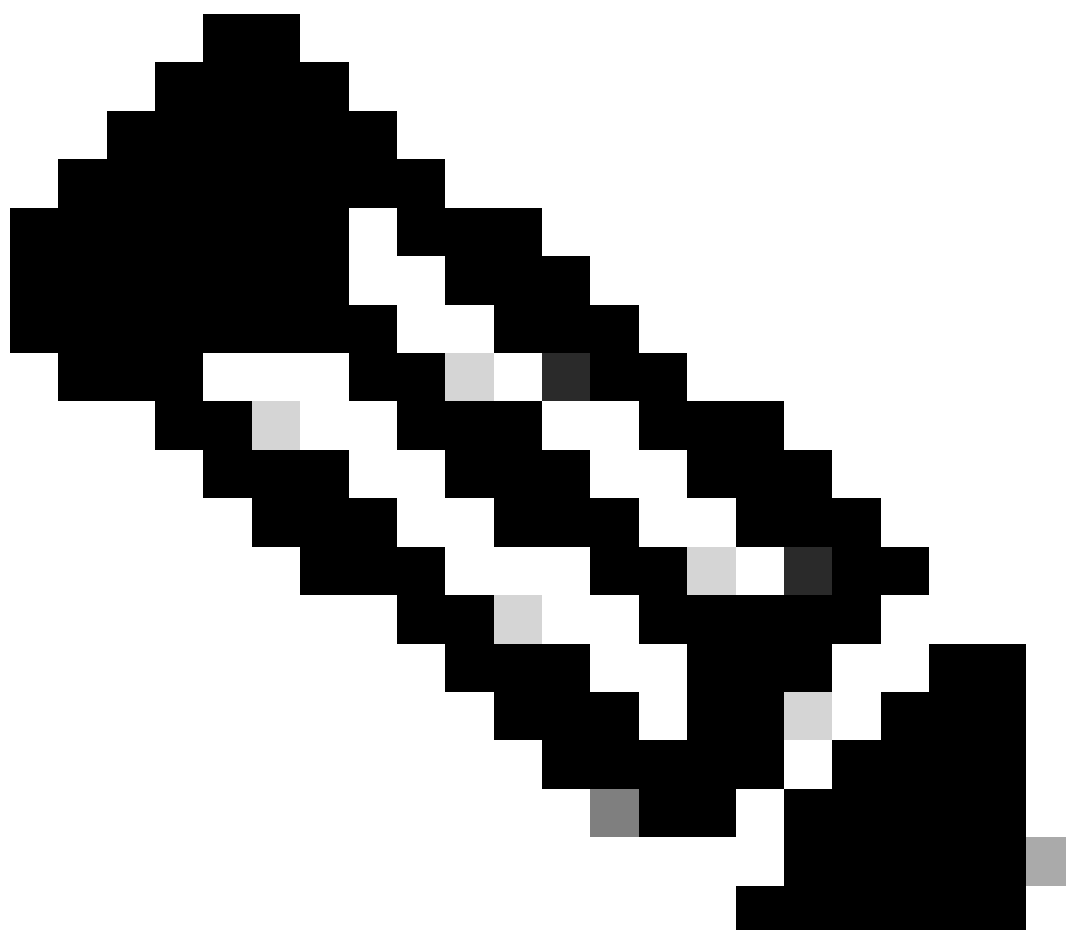
#2: Instale la herramienta DESYNC. Después de la ejecución del comando, puede observar un montón de mensajes de descarga. Aproximadamente después de 2-3 minutos, la descarga debe realizarse .

```
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
```

---





Nota: Si el comando git no funciona, puedes descargar e instalar Git desde aquí:  
<https://git-scm.com/download/win>.

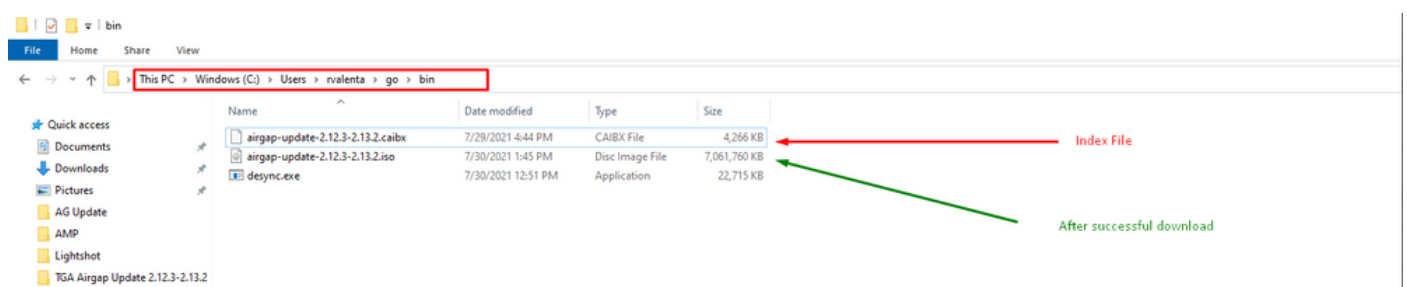
Luego ejecute debajo de dos comandos uno por uno :

```
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: Navegue hasta ir —> ubicación de ubicación. En mi caso, era C:\Users\rvalenta\go\bin y copie y pegue allí el archivo de índice .caibx proporcionado por el TAC.



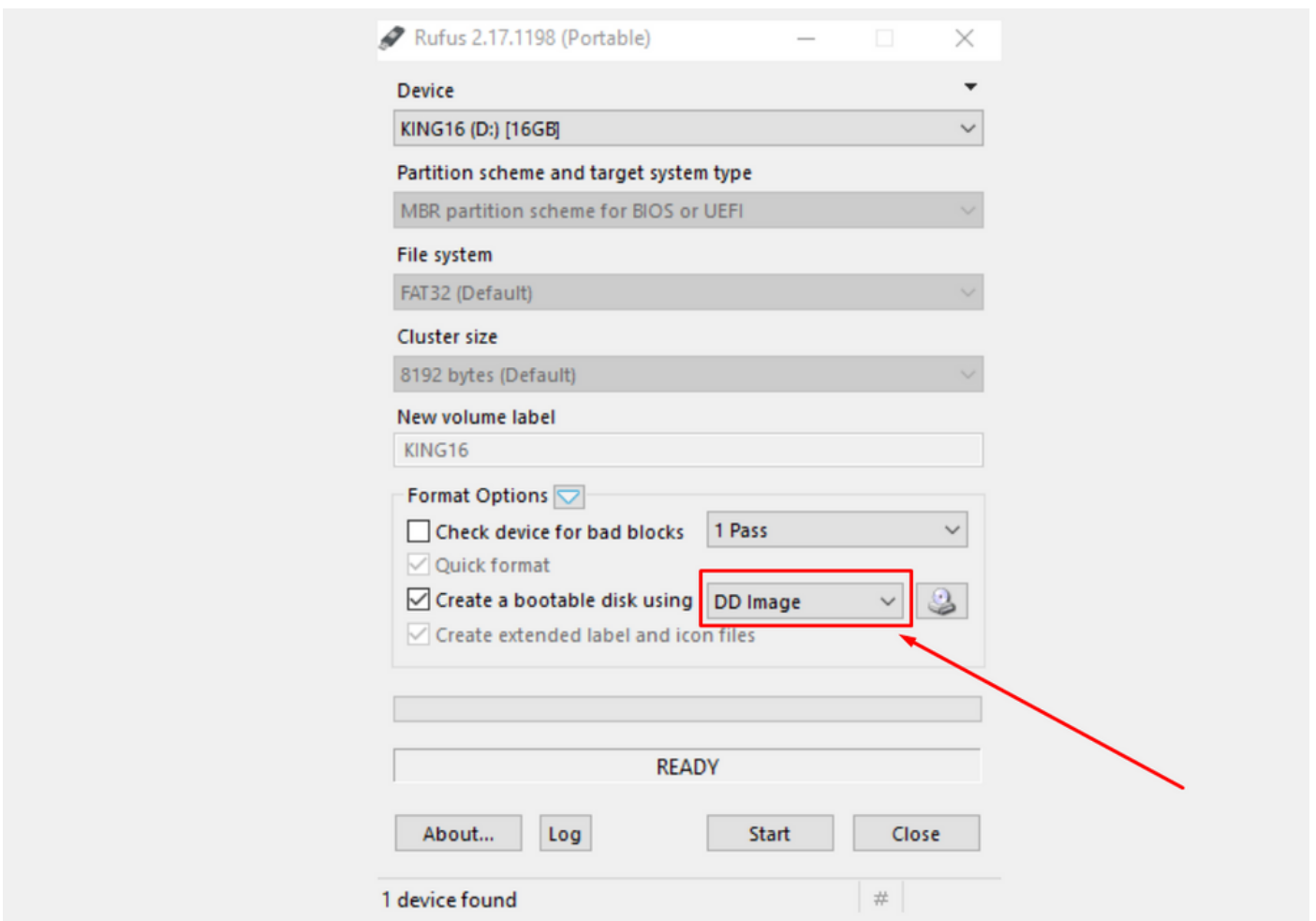
## Verificación

#4: Vuelva al mensaje de CMD y navegue hasta la carpeta go\bin y ejecute los comandos de descarga. Debería ver inmediatamente cómo continúa la descarga. Espere a que se complete la descarga. Ahora debe tener el archivo .ISO completo en la misma ubicación que el archivo de índice .caibx copiado anteriormente

```
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>
```

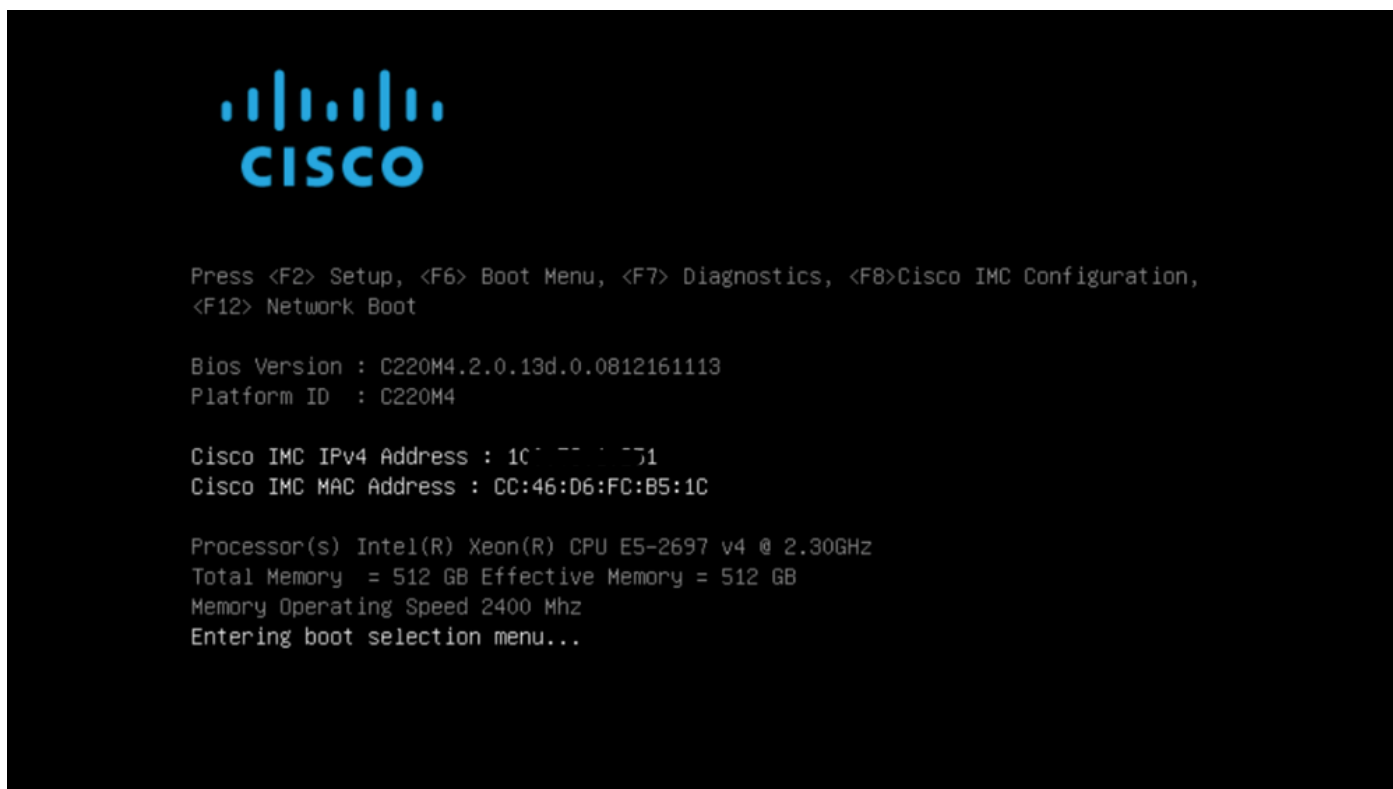
A continuación, utilice RUFUS para crear un USB de arranque. Esto es muy importante para utilizar la versión 2.17. Esta es la última versión en la que puede utilizar dd options que es muy importante para crear este USB de recuperación específica. Puede encontrar todas las versiones de este repositorio [RUFUS REPOSITORY](#) En caso de que esos archivos ya no estén disponibles, también incluyo instaladores para versiones completas y portátiles en este documento.



## Arranque del dispositivo desde USB

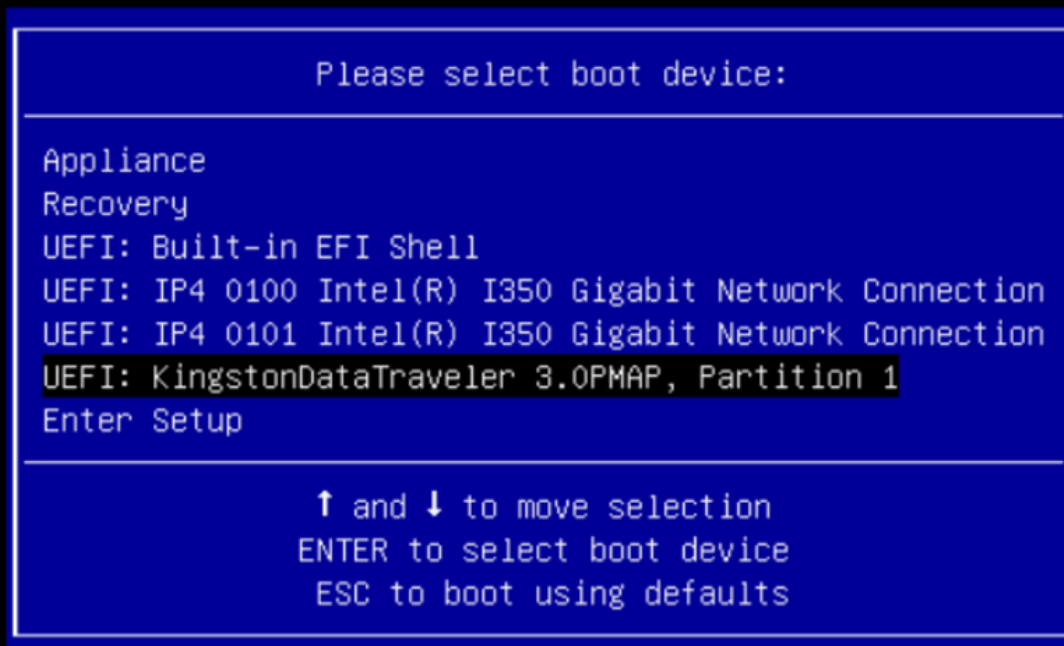
Introduzca la unidad USB y encienda o reinicie el equipo. En la pantalla de arranque de Cisco, seleccione "F6" para acceder al menú de arranque. ¡Debes ser rápido! Solo dispone de unos segundos para realizar esta selección. Si no lo encuentra, debe reiniciar e intentarlo de nuevo.

Figura 1: Pulse F6 para acceder al menú de inicio



Desplácese hasta la unidad USB que contiene la actualización y pulse Intro para seleccionar:

Figura 2: Seleccione Update USB (Actualizar USB)



El medio de actualización determina la siguiente versión en la ruta de actualización y copia el contenido de esa versión en el dispositivo. El dispositivo ejecuta la actualización inmediatamente o se reinicia de nuevo en su modo de funcionamiento normal para permitirle introducir OpAdmin e iniciar la actualización manualmente.

Una vez finalizado el proceso de arranque ISO, reinicie el dispositivo Secure Malware Analytics de nuevo en modo de funcionamiento.

Inicie sesión en la interfaz de usuario del portal y compruebe si hay advertencias que indiquen si es seguro actualizar, etc., antes de continuar.

Navegue hasta la interfaz de OpAdmin y aplique las actualizaciones, si no se aplicaron automáticamente durante el reinicio: OpAdmin > Operations > Update Appliance **NOTA:** El proceso de actualización incluye reinicios adicionales como parte de la actualización, que se realiza a partir de los medios USB. Por ejemplo, es necesario utilizar el botón Reiniciar en la página de instalación después de instalar las actualizaciones.

Repita este procedimiento según sea necesario para cada versión del dispositivo USB.

Cómo encontrar el dispositivo /dev correcto

Con el USB todavía no conectado al terminal ejecute el comando "lsblk | 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$
```

Una vez conectada la memoria USB.

```
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$
```

Esto confirma que el dispositivo USB en /dev es "/dev/sdb".

Otras formas de confirmar, después de conectar el dispositivo USB:

El comando dmesg proporciona cierta información. Una vez conectado el USB, ejecute el comando dmesg | grep -iE 'usb|attachment'.

```
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$
```

El comando `fdisk` proporciona información sobre el tamaño, que se puede utilizar para confirmar:  
`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$
```



Nota: Recuerde desmontar el USB antes de ejecutar el comando "dd".

---

Confirmación de que el dispositivo USB del ejemplo está montado.

```
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
```

Para desmontar el dispositivo USB utilice `sudo umount /dev/sdb1`.

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

Vuelva a comprobar si el dispositivo no se considera "montado".

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

status=opción de progreso

oflag=sync y status=progress en el comando dd.

Cuando se escriben numerosos bloques de datos, la opción "status=progress" proporciona información sobre las operaciones de escritura actuales. Esto es útil para confirmar si el comando "dd" está escribiendo actualmente en la caché de páginas; se puede utilizar para mostrar el progreso y la cantidad completa de tiempo en segundos de todas las operaciones de escritura.

Cuando no se utiliza, "dd" no proporciona información sobre el progreso, sólo se proporcionan los resultados de las operaciones de escritura antes de que "dd" devuelva:

```
[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]$
```

Cuando se utiliza, la información en tiempo real sobre las operaciones de escritura se actualiza cada segundo.

```
[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]
```



Nota: En la documentación oficial para el proceso de actualización offline de TGA, el comando que se informa es : dd if=airgap-update.iso of=/dev/<MY\_USB> bs=64M

---

Después de algunas pruebas, se observa el siguiente ejemplo.

Una vez creado un archivo de 10MB con "dd" usando el dispositivo /dev/zero.

1M x 10 = 10M (10240 kB + datos anteriores del sistema en cachés de páginas de archivos dañadas = 10304 kB → esto es lo que se percibe en la caché de páginas dañadas al final de "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

---

 Nota: Después de que el comando "dd" regresó, la operación de escritura en el dispositivo de bloqueo no se completó, se percibió 11 segundos después del retorno. Si este fuera el comando "dd" al crear el USB de arranque con el TGA ISO, Y yo había eliminado el USB del terminal antes de esos 11 segundos = Yo tendría un ISO dañado en el USB de arranque.

---

#### Explicación:

Los dispositivos de bloqueo proporcionan acceso almacenado en búfer a los dispositivos de hardware. Esto proporciona una capa de abstracción para las aplicaciones cuando se trabaja con dispositivos de hardware.

Los dispositivos de bloqueo permiten que una aplicación lea/escriba por bloques de datos de diferentes tamaños; este read()/write() se aplica en las memorias caché de páginas (búferes) y no directamente en el dispositivo de bloqueo.

El núcleo ( y no la aplicación que hace la lectura/escritura ) administra el movimiento de datos desde los búferes (memorias caché de páginas) a los dispositivos de bloque.

Por lo tanto:

La aplicación (en este caso "dd") no tiene control sobre el vaciado de los búferes si no se le indica.



La opción "oflag=sync" fuerza la escritura física sincrónica (por parte del núcleo) después de colocar cada bloque de salida (proporcionado por "dd") en la memoria caché de la página. oflag=sync degrada el rendimiento "dd" en comparación con no utilizar la opción; pero, si está activada, garantiza una escritura física en el dispositivo de bloqueo después de cada llamada write() desde "dd".

Prueba: el uso de la opción "oflag=sync" del comando "dd" para confirmar todas las operaciones de escritura con los datos de caché de páginas dañadas se completó al volver el comando "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]$
```

No quedan datos de la operación de escritura en la caché de páginas dañadas.

La operación de escritura se aplicó antes (o en el mismo instante) de que regresara el comando "dd" (no 11 segundos después de la prueba anterior).

Ahora estoy seguro de que después de que el comando "dd" regresó no había datos en la memoria caché de la página corrupta relacionados con la operación de escritura = no hay problemas en la creación de arranque USB (si la suma de comprobación ISO es correcta).

---

 Nota: Tenga en cuenta este indicador (oflag=sync) del comando "dd" cuando trabaje en este tipo de caso.

---

## Secuencia de arranque para unidades de disco duro para actualizaciones fuera de línea

Requisito:

Debemos asegurarnos de que el disco duro esté formateado con la opción "DD" utilizando cualquier herramienta disponible y que los medios se copien después en la unidad. Si no utilizamos este formato, no podríamos leer este medio.

Una vez que tengamos los medios cargados en el disco duro/USB usando el formato "DD", necesitamos conectarlo al dispositivo TGA y reiniciar el dispositivo.

Esta es la pantalla de selección predeterminada del menú de arranque. Necesitamos presionar

"F6" para iniciar el dispositivo y seleccionar el medio de arranque



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

Una vez que el dispositivo reconoce nuestra entrada, se le solicitará que entre en el menú de selección de arranque.



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...

Este es el mensaje que puede diferir entre diferentes modelos TGA. Idealmente, veríamos la opción de arrancar usando el medio de arranque (upgrade filesystem) desde este mismo menú, pero si no se ve, necesitamos iniciar sesión en el "Shell de EFI".

Please select boot device:

Appliance

Recovery

**UEFI: Built-in EFI Shell**

UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection

UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection

Enter Setup

↑ and ↓ to move selection  
ENTER to select boot device  
ESC to boot using defaults

Tendría que pulsar "ESC" antes de que el script "startup.sh" finalice para pasar al shell de EFI. Una vez que iniciamos sesión en el shell de EFI, nos daríamos cuenta de que las particiones detectadas en este caso son 3 sistemas de archivos: 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,
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> _
```

## ¡Importante

Identificación del sistema de archivos correcto:

- Según la captura de pantalla anterior, usted podría ver que "fs0:" es el único medio con "USB" en su trayectoria y por lo tanto podemos estar seguros de que este sistema de archivos contendría el medio de arranque (upgrade filesystem).

En caso de que falten sistemas de archivos:

- Si sólo fs0: y fs1: están disponibles y no hay fs2:, verifique que el medio de arranque (sistema de archivos de actualización) se haya escrito en modo dd y que se haya conectado correctamente.
- Los medios de arranque (sistema de archivos de actualización) siempre deben tener un número menor que los medios de recuperación, y siempre deben estar uno al lado del otro; es si la unidad conectada al USB está al principio del fin que es probable que cambie (por lo tanto, si toma la posición frontal en fs0: o la posición trasera en fs2:) tendría que ser identificado
- En este caso, en la captura de pantalla siguiente, aparece el archivo ".efi" correcto, ya que se encuentra en la partición "\efi\boot" y tiene la convención de nomenclatura "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)
```

Para arrancar el dispositivo en el medio de arranque (upgrade filesystem), debemos ejecutar el archivo "bootx64.efi":

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

Para su referencia, hemos mostrado el contenido de los otros sistemas de archivos a continuación:

fs1: Este es el sistema de archivos de arranque principal.

```

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: Este es el sistema de archivos de arranque de la imagen de recuperación.

```


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)

```

Instrucciones varias:

Para verificar el sistema de archivos correcto que contiene el medio de arranque montado. Podemos hacerlo explorando los diferentes sistemas de archivos y verificando el archivo de inicio ".efi"

---

 Nota: La secuencia del medio de arranque real (sistema de archivos de actualización) que en este caso es "fs0:" también puede variar con otros dispositivos. El nombre y la ruta pueden variar, pero en todas las imágenes modernas, esto debe ser el mismo.

---

Lista de comprobación que puede ayudar a localizar el medio de arranque correcto (actualizar el sistema de archivos):

- Si la raíz de un sistema de archivos contiene "vmlinuz-appliance", no es el medio de arranque (upgrade filesystem).
- Si la raíz de un sistema de archivos contiene "meta\_contents.tar.xz", no es el medio de arranque (upgrade filesystem).
- Si un sistema de archivos no contiene "efi\boot\bootx64.efi", no es el medio de arranque (sistema de archivos de actualización).

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).