Aggiorna modalità Air-Gap di Secure Malware Analytics Appliance

Sommario

Introduzione

In questo documento viene descritto come aggiornare la modalità Air-Gap di Secure Malware Analytics Appliance.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base degli input tramite riga di comando in ambiente Windows e Unix/Linux
- Conoscenza di Malware Analytic Appliance

- Conoscenza di Cisco Integrated Management Controller (IMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La maggior parte degli accessori di analisi malware sicuri è connessa a Internet e pertanto utilizza il processo di aggiornamento online. Tuttavia, in alcuni casi gli appliance Secure Malware Analytics vengono mantenuti rigorosamente all'interno delle reti interne, ovvero "air-gapped". Non è consigliabile mantenere gli accessori con interruzioni di corrente perché in questo modo risultano meno efficaci; tuttavia, questo compromesso potrebbe essere necessario per supportare ulteriori requisiti di sicurezza o normativi.

Per gli utenti che eseguono i propri accessori di analisi malware sicuro non connessi a Internet, è disponibile il processo di aggiornamento offline descritto in questo documento. Il supporto per l'aggiornamento è fornito dal supporto di analisi malware sicuro su richiesta. Per ulteriori informazioni, vedere di seguito.

Supporti: i supporti di aggiornamento Airgap (offline) vengono forniti dal supporto di analisi malware sicuro come ISO, che può essere copiato su un supporto USB o su un disco rigido (unità disco rigido) se sono disponibili dischi di dimensioni adeguate.

Dimensioni: le dimensioni dipendono dalle versioni supportate dai supporti di aggiornamento, ma spesso possono essere diverse decine di gigabyte quando vengono introdotte nuove VM tra le versioni di origine e di destinazione. Con le versioni correnti, potrebbe essere di circa 30 GB poiché lo strumento di desincronizzazione aiuta ad aggiornare le modifiche relative alla VM in modo incrementale.

Ciclo di avvio dell'aggiornamento: ogni volta che il supporto di aggiornamento airgap viene avviato, determina la versione successiva a cui eseguire l'aggiornamento e copia il contenuto associato a tale versione nell'accessorio. Una determinata release può inoltre avviare l'installazione di un pacchetto se non dispone di controlli dei prerequisiti che devono essere eseguiti mentre l'accessorio è in esecuzione. Se la release include tali controlli o una sostituzione a parti del processo di aggiornamento che potrebbero aggiungere tali controlli, l'aggiornamento non viene effettivamente applicato fino a quando l'utente non accede a OpAdmin e richiama

l'aggiornamento con OpAdmin > Operazioni > Aggiorna accessorio.

Hook di preinstallazione: a seconda che siano presenti o meno hook di preinstallazione per l'aggiornamento specifico, l'aggiornamento viene eseguito immediatamente oppure l'accessorio viene riavviato nella normale modalità operativa per consentire all'utente di accedere all'interfaccia amministrativa e avviare manualmente l'aggiornamento.

Ripeti se necessario: ogni ciclo di avvio di questi supporti aggiorna (o si prepara per l'aggiornamento) solo un passaggio verso l'eventuale release di destinazione; l'utente deve avviare tutte le volte necessarie per eseguire l'aggiornamento alla release di destinazione desiderata.

Limitazioni

I supporti CIMC non sono supportati per gli aggiornamenti con interruzioni di connessione.

A causa dei vincoli imposti dalle licenze sui componenti di terze parti utilizzati, i supporti di aggiornamento per le versioni 1.x non saranno più disponibili dopo che l'hardware UCS M3 ha raggiunto la fine del ciclo di vita. È pertanto fondamentale che gli accessori UCS M3 siano sostituiti o aggiornati prima della fine del ciclo di vita.

Requisiti

Migrazioni: se le note di rilascio relative alle versioni considerate includono scenari in cui è obbligatorio eseguire la migrazione prima dell'installazione della versione successiva, l'utente deve eseguire la procedura seguente prima di riavviare il sistema per evitare di rendere inutilizzabile l'accessorio.

Nota:la prima release 2.1.x successiva alla 2.1.4, in particolare, esegue diverse migrazioni di database. Non è sicuro continuare fino al completamento di queste migrazioni. Per ulteriori informazioni, vedere la nota sulla migrazione di Threat Grid Appliance 2.1.5.

Se i supporti airgap sono stati creati con una versione precedente alla 2.1.3, usano una chiave di crittografia derivata dalla licenza individuale e devono quindi essere personalizzati per singola appliance. (L'unico effetto visibile all'utente è che con i supporti creati per supportare le versioni di origine precedenti alla 2.1.3, Secure Malware Analytics richiede preventivamente le licenze installate su tali accessori e i supporti non funzioneranno su accessori non inclusi nell'elenco per cui è stato creato).

Se si inizia con la release 2.1.3 o successive, il supporto airgap è generico e non sono necessarie informazioni sul cliente.

Operazioni preliminari

- Backup. Prima di procedere con l'aggiornamento, è necessario eseguire un backup dell'accessorio.
- Esaminare le Note sulla versione da aggiornare per verificare se sono necessarie migrazioni

in background prima di pianificare l'aggiornamento alla nuova versione
- Verificare la versione corrente dell'accessorio: OpAdmin > Operazioni > Aggiorna accessorio
- Esaminare la cronologia delle versioni dell'appliance Secure Malware Analytics nella tabella di ricerca numero build/versione, disponibile in tutti i documenti dell'appliance Threat Grid: note sulla versione, note sulla migrazione, guida di installazione e configurazione e guida dell'amministratore.

Aggiornare un'appliance di analisi malware sicura offline (con airgapped)

Controllare prima la versione Air Gapped disponibile in questa pagina: Tabella di ricerca della versione dell'accessorio

1. Aprire una richiesta di assistenza TAC per ottenere il supporto di aggiornamento offline. La richiesta deve includere il numero di serie dell'accessorio e il numero di build dell'accessorio.

2. Il supporto TAC fornisce un ISO aggiornato in base all'installazione.

3. Masterizzare l'immagine ISO su una porta USB avviabile. Si noti che USB è l'unico dispositivo/metodo supportato per gli aggiornamenti offline.

Convenzioni di denominazione

Questo è il nome file aggiornato: TGA Airgap Update 2.13.2-2.14.0.

Questo significa che il supporto può essere utilizzato per un accessorio con una versione minima: 2.13.2 e aggiornare l'accessorio alla versione: 2.14.0.

Limitazioni

- I supporti CIMC non sono supportati per gli aggiornamenti con interruzioni di connessione.
- A causa dei vincoli delle licenze sui componenti di terze parti utilizzati, i supporti di aggiornamento per le versioni 1.x non sono più disponibili dopo che l'hardware UCS M3 ha raggiunto la fine del ciclo di vita. È pertanto fondamentale che gli accessori UCS M3 siano sostituiti o aggiornati prima della fine del ciclo di vita.

Linux/MAC - Download ISO

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Un computer Linux con accesso a Internet per scaricare l'ISO e creare l'unità di installazione USB avviabile.
- Le istruzioni per il download dell'airgap sono fornite dal supporto per l'analisi sicura dei malware.
- Linguaggio di programmazione GO. Scarica
- Il file di indice .caibx (incluso nel file zip fornito dal supporto TAC).

- Strumento di dissincronizzazione (incluso nel file zip fornito dal supporto di analisi malware protetto).

Componenti usati

Il riferimento delle informazioni contenute in questo documento è una versione di CentOS Linux 7.6.1810 (Core).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Installare il linguaggio di programmazione 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
```

Eseguire questi tre comandi dopo l'installazione, se il comando desync non ha esito positivo

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

È possibile verificare la versione GO eseguendo le operazioni seguenti:

```
# go version
```

Scaricare l'ISO utilizzando il comando Desync

Passaggio 1. Copiare il contenuto del file Zip fornito dal supporto di analisi malware sicuro, inclusi i file desync.linux e .caibx nella stessa directory localmente sul computer.

Passaggio 2. Passare alla directory in cui sono stati memorizzati i file:

Esempio:

```
# cd MyDirectory/TG
```

Passaggio 3. Eseguire il comando pwd per verificare che l'utente si trovi all'interno della directory.

```
# pwd
```

Passaggio 4. Una volta all'interno della directory che include il comando desync.linux e il file .caibx, eseguire il comando desiderato per avviare il processo di download.

Nota: questi sono gli esempi di diverse versioni ISO. Fare riferimento al file .caibx dalle istruzioni fornite dal supporto di analisi malware sicuro.

Per le versioni da 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
```

Per le versioni da 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
```

Per le versioni da 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 volta avviato il download, viene visualizzata una barra di avanzamento.

Nota: la velocità di download e le dimensioni dei supporti di aggiornamento nell'ambiente in uso possono influire sul tempo necessario per la composizione dell'ISO.
Accertarsi di confrontare l'MD5 del file scaricato con quello disponibile con il bundle fornito dal supporto per verificare l'integrità dell'ISO scaricato.

Una volta completato il download, gli ISO vengono creati nella stessa directory.

Collegare l'USB al computer ed eseguire il comando add per creare l'unità USB avviabile.

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

Dove <MY_USB> è il nome della chiave USB (non utilizzare le parentesi angolari).

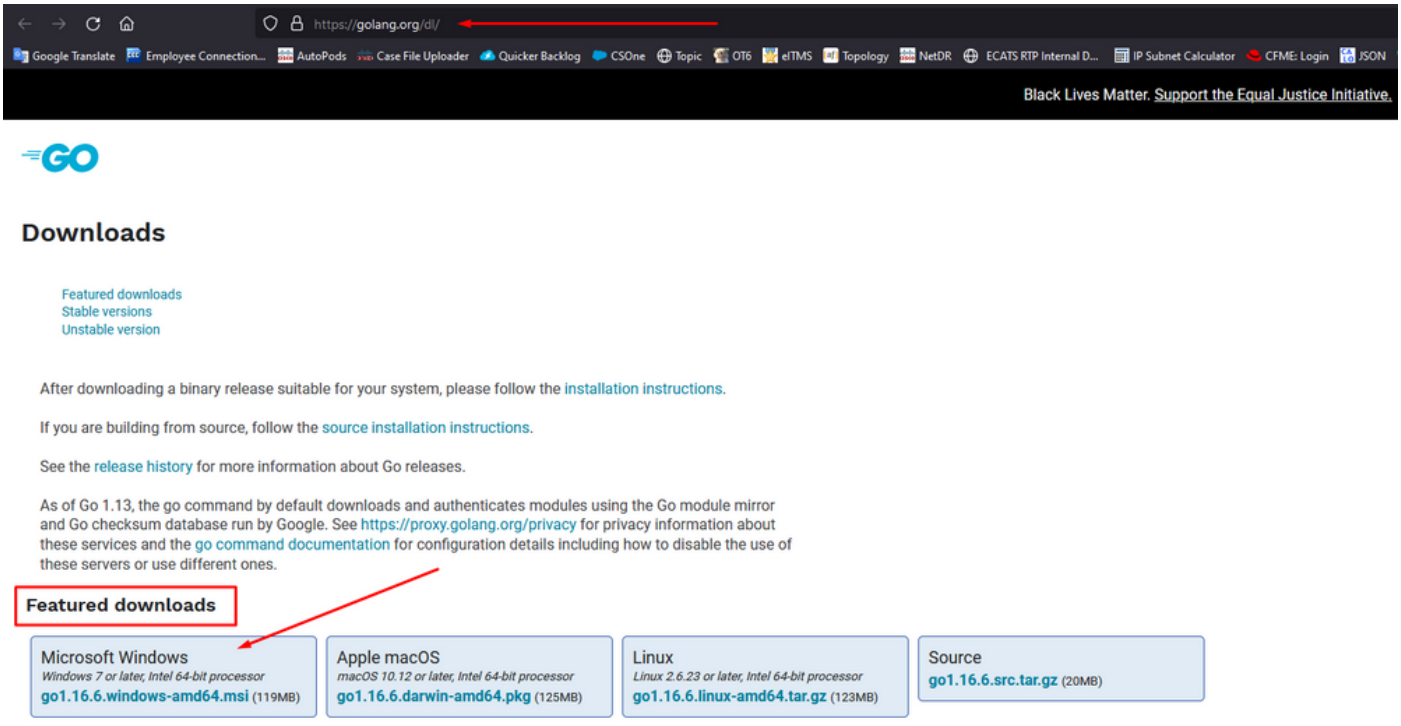
Inserire l'unità USB e accendere o riavviare l'accessorio. Nella schermata di avvio di Cisco, premere F6 per accedere al menu di avvio.

Suggerimento:
Eseguire il download dopo l'orario di ufficio o fuori orario di punta in quanto potrebbe influire sulla larghezza di banda.
Per arrestare lo strumento, chiudere il terminale o premere Ctrl+c/Ctrl+z.
Per continuare, eseguire lo stesso comando per riprendere il download.

Windows - Download ISO

Installare il linguaggio di programmazione GO

#1: Scarica il linguaggio di programmazione GO richiesto. Installa da https://golang.org/dl/ Nel mio caso scelgo la Versione in Vetrina. Riavviare il CMD e provare con



Chiudere e riaprire il comando CMD run per verificare:

```
go version
```

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

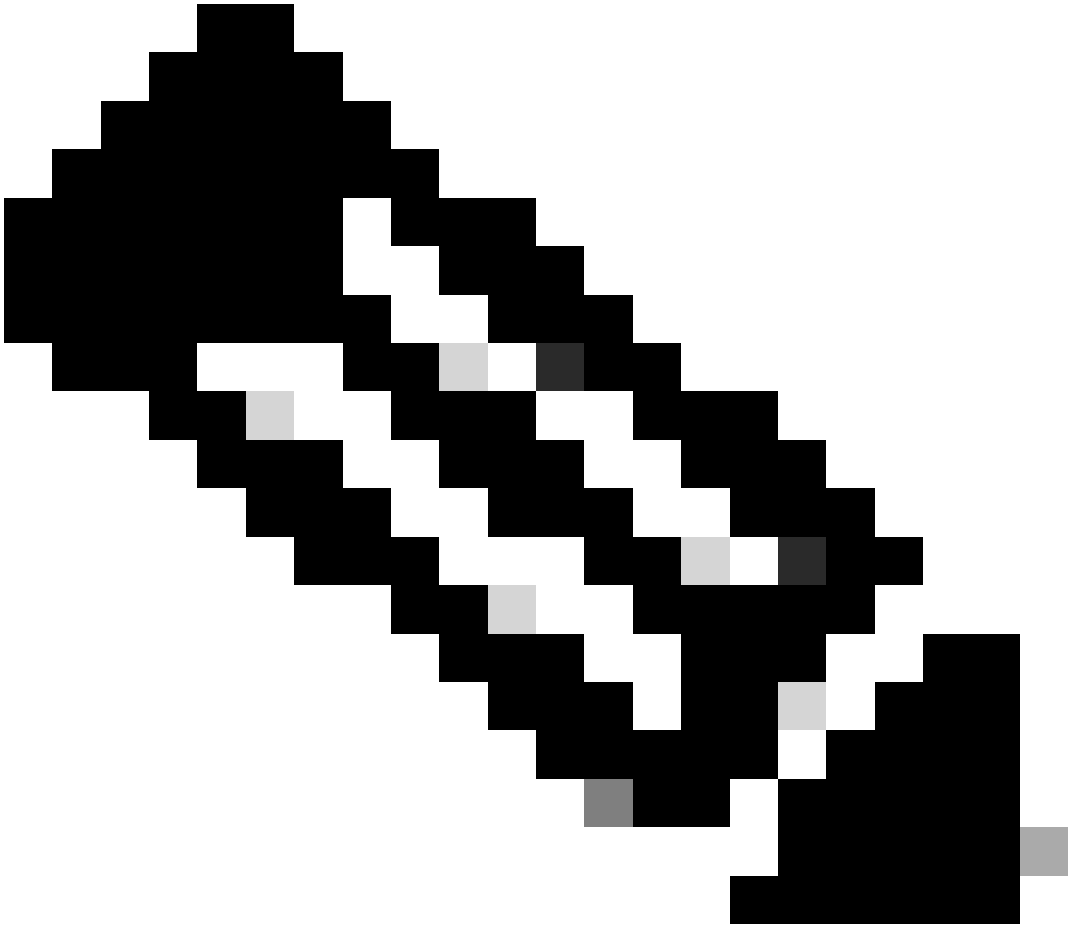
Scaricare l'ISO utilizzando il comando Desync

#2: Installare lo strumento DESYNC. Dopo l'esecuzione del comando, è possibile notare una serie di richieste di download. Dopo circa 2-3 minuti, il download dovrebbe essere completato.

```
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
```

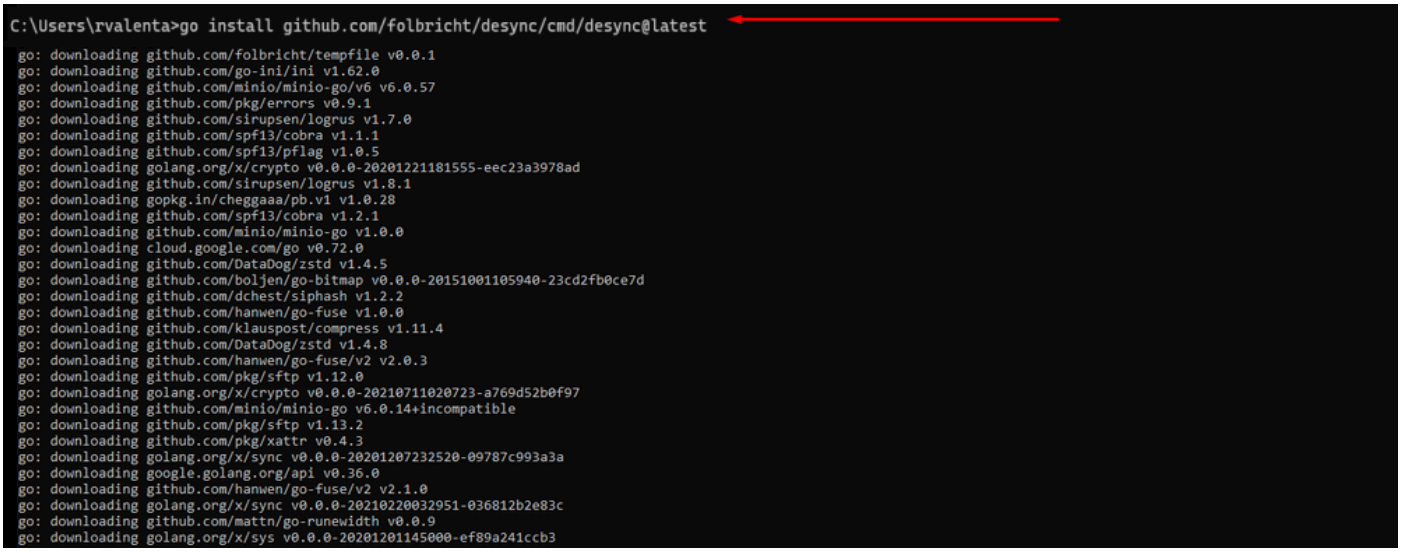


Nota: se il comando git non funziona, è possibile scaricare e installare Git da qui: https://git-scm.com/download/win.

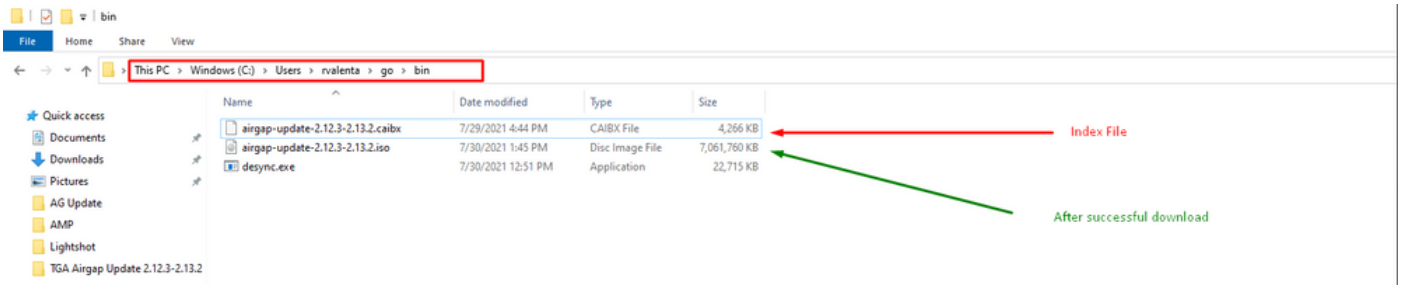
Quindi esegui sotto due comandi uno per uno:

```
cd desync/cmd/desync

go install
```



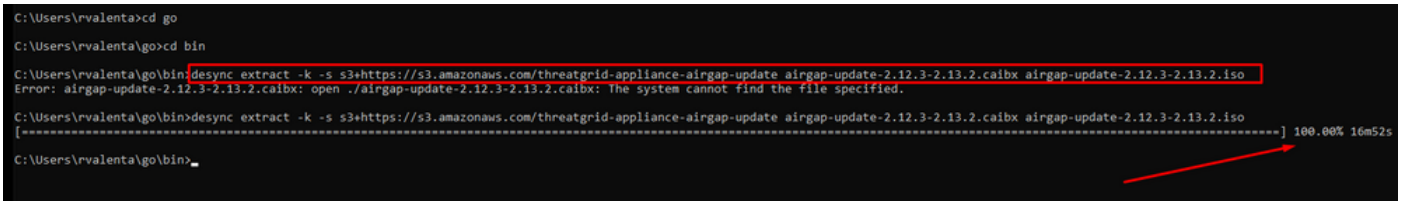
#3: Passa a vai — > posizione contenitore. Nel mio caso era C:\Users\rvalenta\go\bin e copia / incolla lì TAC fornito .caibx file di indice.



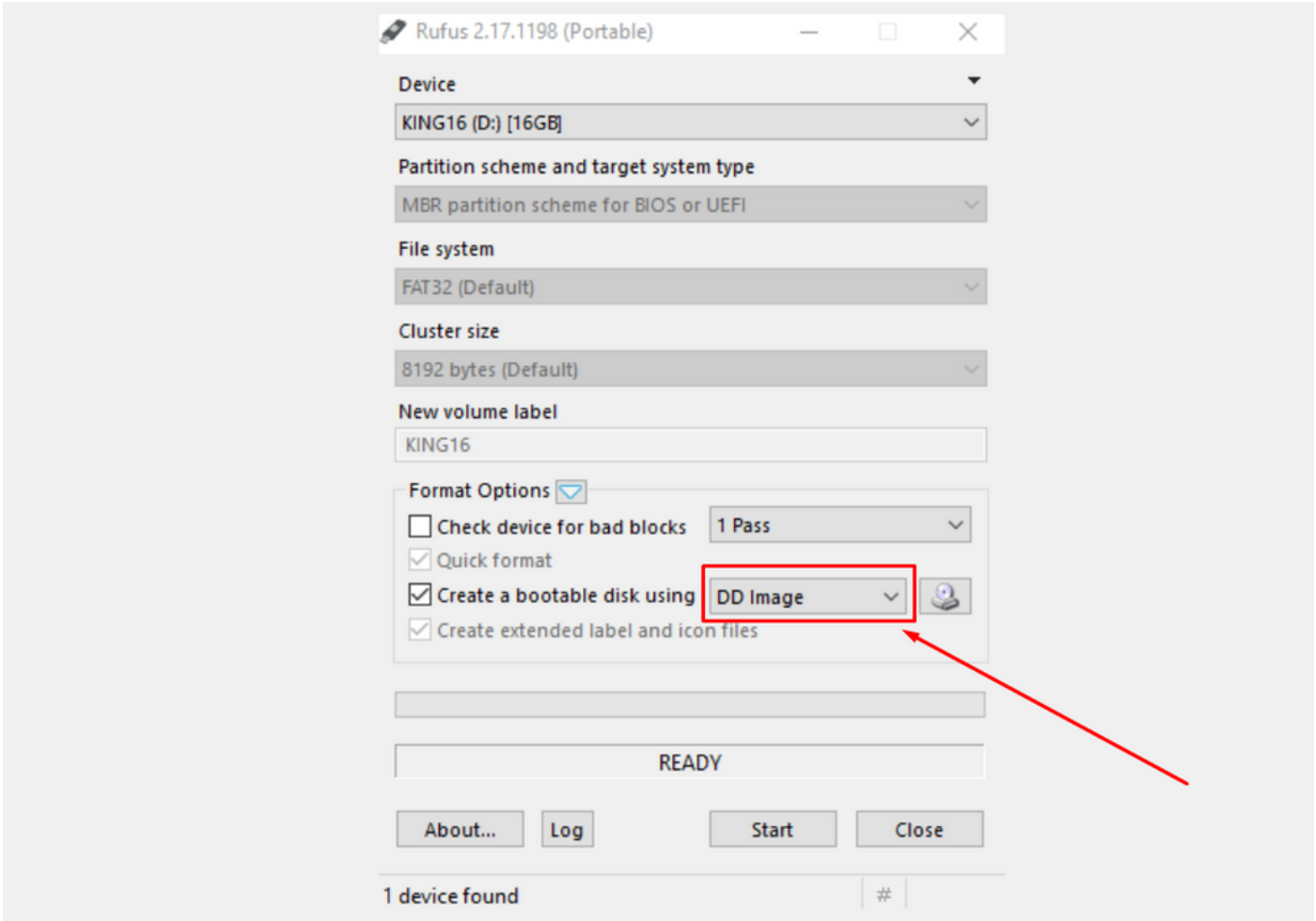
Verifica

#4: Tornare al prompt di CMD e selezionare la cartella go\bin ed eseguire i comandi di download. Il download dovrebbe procedere immediatamente. Attendere il completamento del download. A questo punto, l'intero file .ISO si trova nella stessa posizione del file di indice .caibx copiato in precedenza

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



Quindi utilizzare RUFUS per creare un USB avviabile. È molto importante utilizzare la versione 2.17. Questa è l'ultima versione in cui è possibile utilizzare opzioni aggiuntive che è molto importante per creare questo USB di ripristino specifico. È possibile trovare tutte le versioni di questo repository RUFUS REPOSITORY Nel caso in cui tali file non siano più disponibili, in questo documento sono inclusi anche i programmi di installazione per le versioni complete e portabili.



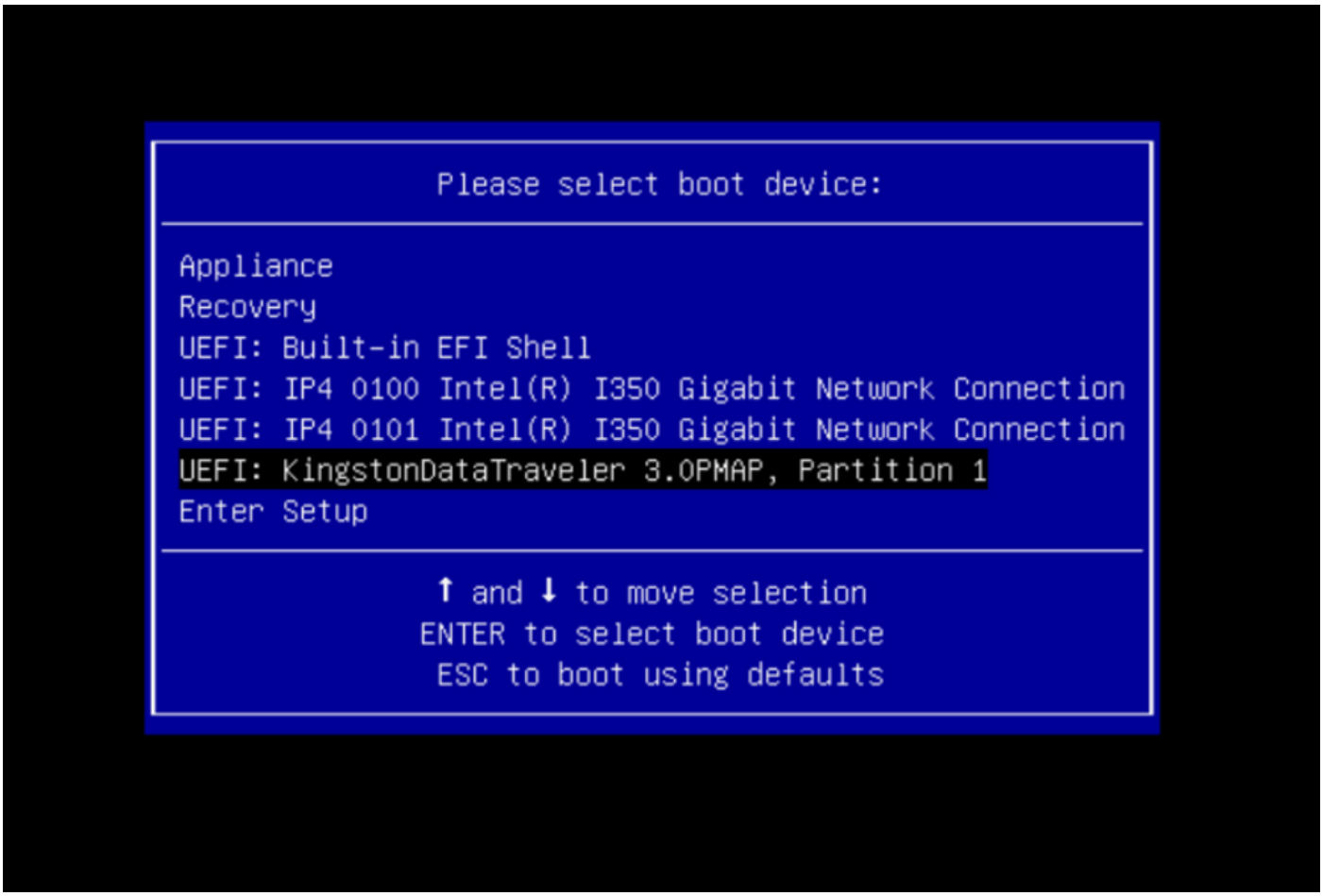
Appliance di avvio da USB

Inserire l'unità USB e accendere o riavviare l'accessorio. Nella schermata di avvio di Cisco, selezionare "F6" per accedere al menu di avvio. Devi essere veloce! Hai solo pochi secondi per effettuare questa selezione. Se non riesci a vederlo, riavvia il sistema e riprova.

Figura 1 - Premere F6 per accedere al menu di avvio

Passare all'unità USB contenente l'aggiornamento e premere Invio per selezionare:

Figura 2 - Selezione dell'USB di aggiornamento



Il supporto di aggiornamento determina la versione successiva nel percorso di aggiornamento e copia il contenuto di tale versione nell'accessorio. L'accessorio esegue l'aggiornamento immediatamente oppure riavvia il sistema nella normale modalità operativa per consentire l'accesso a OpAdmin e l'avvio manuale dell'aggiornamento.

Al termine del processo di avvio ISO, riavviare l'appliance Secure Malware Analytics per tornare alla modalità operativa.

Prima di procedere, accedere all'interfaccia utente del portale e verificare la presenza di eventuali avvisi che indicano se è sicuro eseguire l'aggiornamento, ecc.

Passare all'interfaccia OpAdmin e applicare gli aggiornamenti, se non sono stati applicati automaticamente durante il riavvio: OpAdmin > Operazioni > Aggiorna accessorio NOTA: il processo di aggiornamento include riavvii aggiuntivi come parte dell'aggiornamento, che viene eseguito dal supporto USB. È ad esempio necessario utilizzare il pulsante Riavvia nella pagina di installazione dopo l'installazione degli aggiornamenti.

Ripetere l'operazione per ogni versione sulla porta USB.

Come trovare il dispositivo /dev corretto

Con l'USB ancora non collegato all'endpoint, eseguire il comando "lsblk | grep -iE 'disco|parte'.

```
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$
```

Dopo aver collegato la chiavetta 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$
```

Ciò conferma che il dispositivo USB in /dev è "/dev/sdb".

Altri modi per confermare, dopo il collegamento della chiavetta USB:

Il comando dmesg fornisce alcune informazioni. Dopo aver collegato l'USB, eseguire il comando dmesg | grep -iE 'usb|allegato'.

```
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$
```

Il comando fidsk fornisce informazioni sulle dimensioni che è possibile utilizzare per confermare: 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: ricordarsi di smontare l'USB prima di eseguire il comando "dd".

Confermare che il dispositivo USB dell'esempio è montato.

```
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
```

Per smontare il dispositivo USB, utilizzare sudo umount /dev/sdb1.

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

Ricontrolla il dispositivo non percepito come "montato".

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

status=opzione di avanzamento

oflag=sync e status=progress nel comando add.

Quando si scrivono numerosi blocchi di dati, l'opzione "status=progress" fornisce informazioni sulle operazioni di scrittura correnti. Questo comando è utile per verificare se il comando "dd" sta scrivendo nella cache delle pagine; può essere utilizzato per visualizzare lo stato di avanzamento e l'intero periodo di tempo in secondi di tutte le operazioni di scrittura.

Se non viene utilizzato, "dd" non fornisce informazioni sull'avanzamento, ma solo i risultati delle operazioni di scrittura vengono forniti prima che "dd" restituisca:

```
[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]$
```

Quando vengono utilizzate, le informazioni in tempo reale sulle operazioni di scrittura vengono aggiornate ogni secondo.

```
[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: nella documentazione ufficiale per il processo di aggiornamento offline TGA il comando indicato è : dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M

Dopo alcuni test, si osserva il seguente esempio.

Una volta creato un file di 10 MB con "dd" usando il dispositivo /dev/zero.

1M x 10 = 10M (10240 kB + dati di sistema precedenti nelle cache dirty file page = 10304 kB —> questo è ciò che viene percepito nella cache dirty page alla fine di "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: dopo la restituzione del comando "dd", l'operazione di scrittura sul dispositivo di blocco non è stata completata ed è stata rilevata 11 secondi dopo la restituzione.
Se questo fosse il comando "dd" durante la creazione dell'USB avviabile con TGA ISO, E avessi rimosso l'USB dall'endpoint prima di quei 11 secondi = avrei un ISO danneggiato nell'USB avviabile.

Spiegazione:

I dispositivi bloccati consentono l'accesso con buffer ai dispositivi hardware. Questo fornisce un livello di astrazione alle applicazioni quando si lavora con dispositivi hardware.

I dispositivi di blocco consentono a un'applicazione di eseguire operazioni di lettura/scrittura in blocchi di dati di dimensioni diverse; queste operazioni di lettura()/scrittura() vengono eseguite nelle cache di pagina (buffer) e non direttamente nel dispositivo di blocco.
Il kernel (e non l'applicazione che esegue le operazioni di lettura/scrittura) gestisce lo spostamento dei dati dai buffer (cache di pagina) ai dispositivi di blocco.

Pertanto:

L'applicazione (in questo caso "dd") non ha il controllo sullo svuotamento dei buffer se non è indicato.

L'opzione "oflag=sync" forza la scrittura fisica sincrona (da parte del kernel) dopo che ogni blocco di output (fornito da "dd") è inserito nella cache della pagina.

oflag=sync peggiora le prestazioni "dd" se confrontate con il non utilizzo dell'opzione; ma, se è abilitata, garantisce una scrittura fisica sul dispositivo di blocco dopo ogni chiamata write() da "dd".

Test : l'utilizzo dell'opzione "oflag=sync" del comando "dd" per confermare tutte le operazioni di scrittura con i dati della cache della pagina dirty è stato completato alla restituzione del 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]$
```

Nessun dato rimane dall'operazione di scrittura nella cache delle pagine dirty.
L'operazione di scrittura è stata applicata prima (o nello stesso istante) del comando "dd" restituito (non 11 secondi dopo il test precedente).
Ora sono sicuro che dopo il comando "dd" restituito non c'erano dati nella cache di pagina dirty relativi all'operazione di scrittura = nessun problema nella creazione USB avviabile (se il checksum ISO è corretto).

Nota: tenere in considerazione questo flag (oflag=sync) del comando "dd" quando si lavora su questo tipo di richiesta.

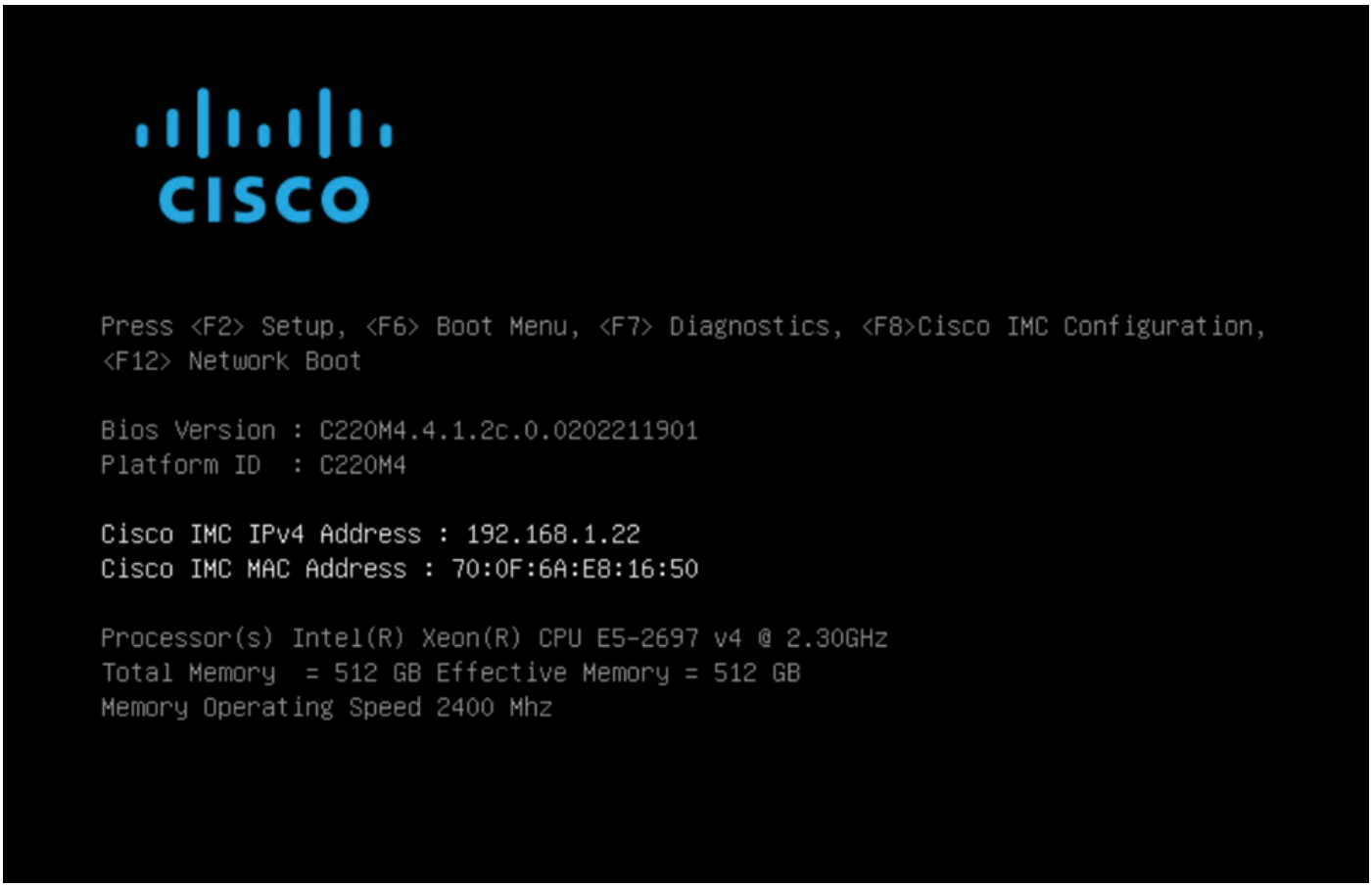
Sequenza di avvio per unità disco rigido per aggiornamenti offline

Requisito:

È necessario verificare che l'HDD sia formattato utilizzando l'opzione "DD" utilizzando qualsiasi strumento disponibile e che il supporto venga successivamente copiato sull'unità. Se non utilizzassimo questa formattazione, non saremmo in grado di leggere questo supporto.

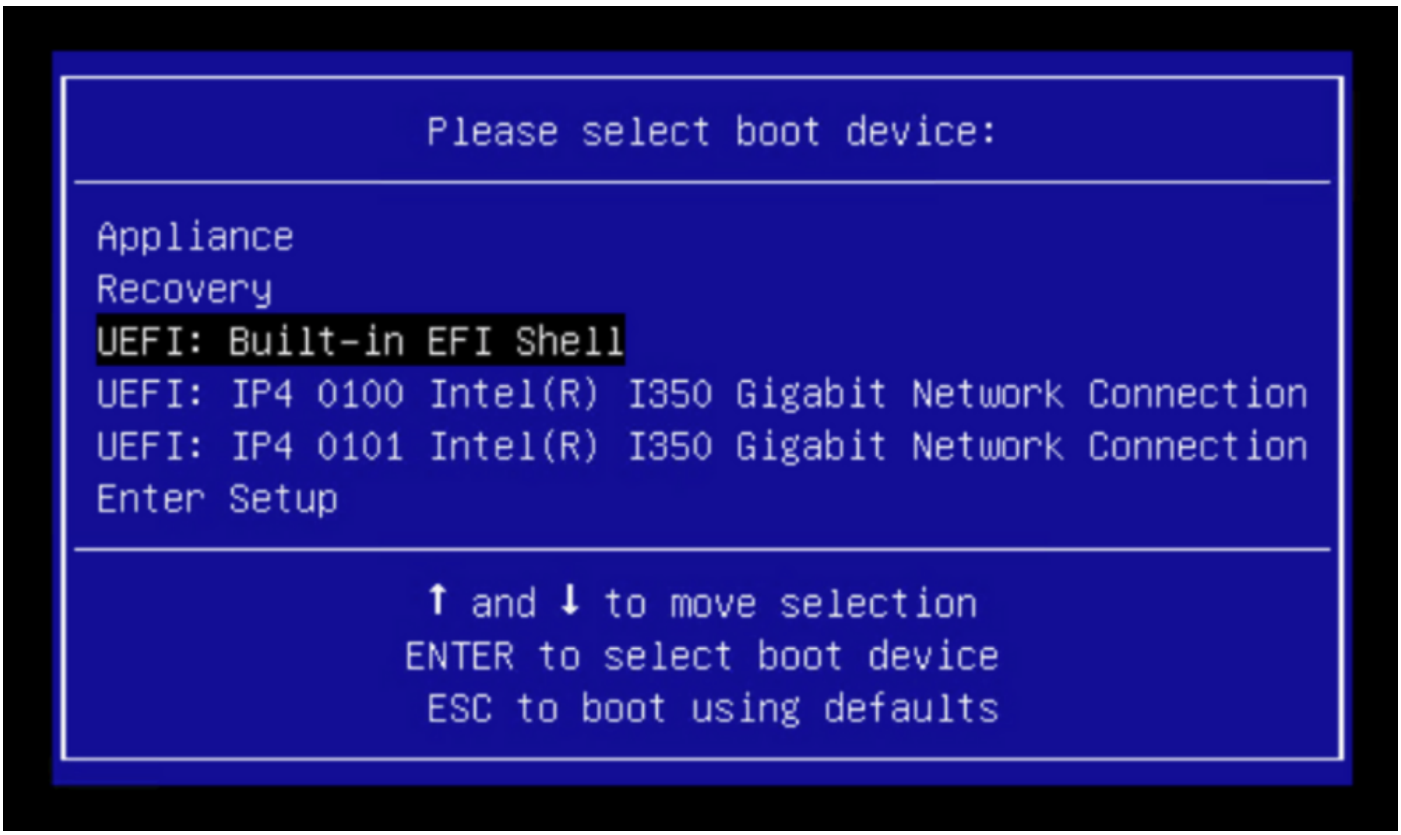
Una volta caricato il supporto sull'HDD/USB utilizzando la formattazione "DD", è necessario collegarlo all'accessorio TGA e riavviare il dispositivo.

Questa è la schermata di selezione predefinita del menu di avvio. È necessario premere "F6" per avviare il dispositivo e selezionare il supporto di avvio

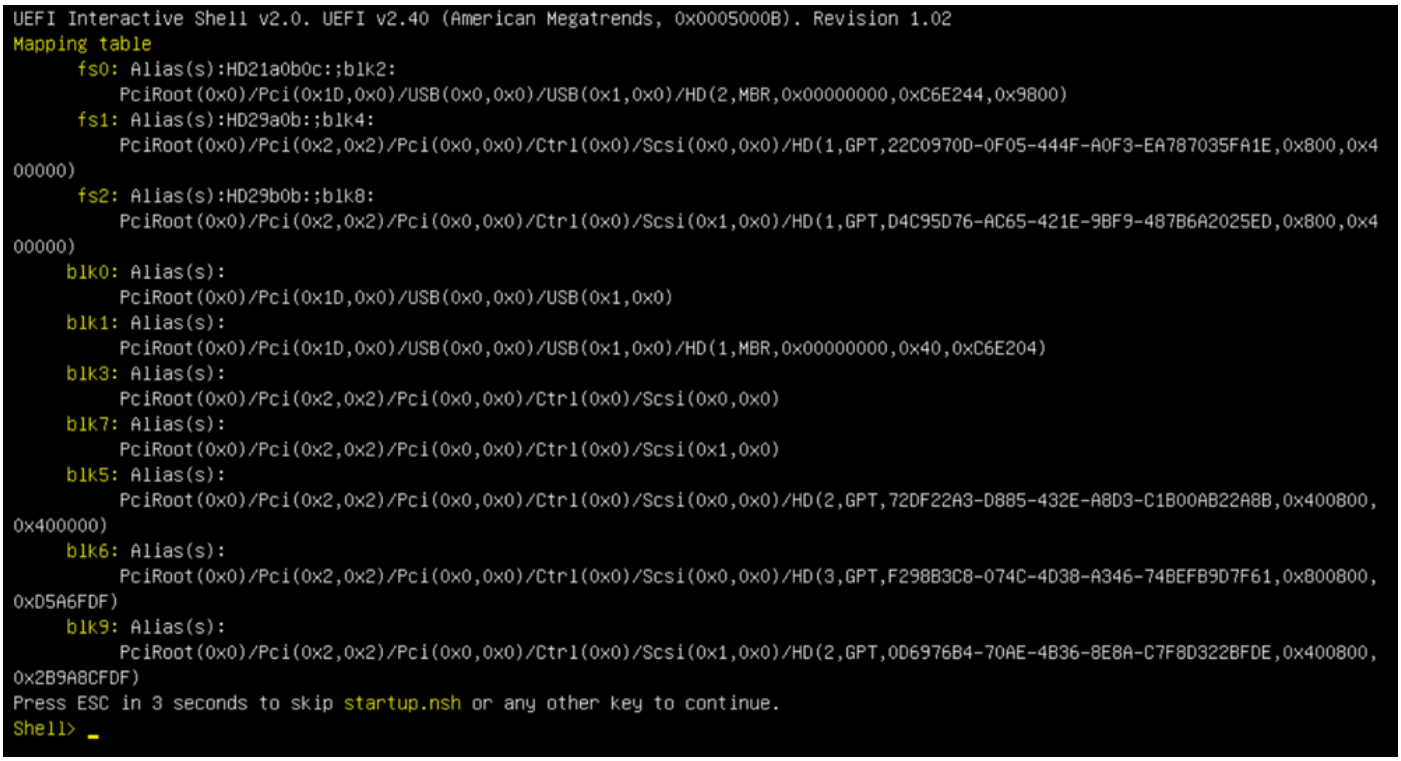


Una volta riconosciuto l'input, il dispositivo richiederebbe di accedere al menu di selezione di avvio.

Questo prompt può variare a seconda del modello TGA. Idealmente, l'opzione di avvio dovrebbe essere visualizzata utilizzando il supporto di avvio (aggiornamento del file system) da questo menu, ma se non è visibile, è necessario accedere alla "shell EFI".



È necessario premere "ESC" prima che lo script "startup.sh" termini per spostarsi nella shell EFI. Una volta eseguito il login alla shell EFI, si noterà che le partizioni rilevate in questo caso sono 3 file system: fs0:, fs1:, fs2.



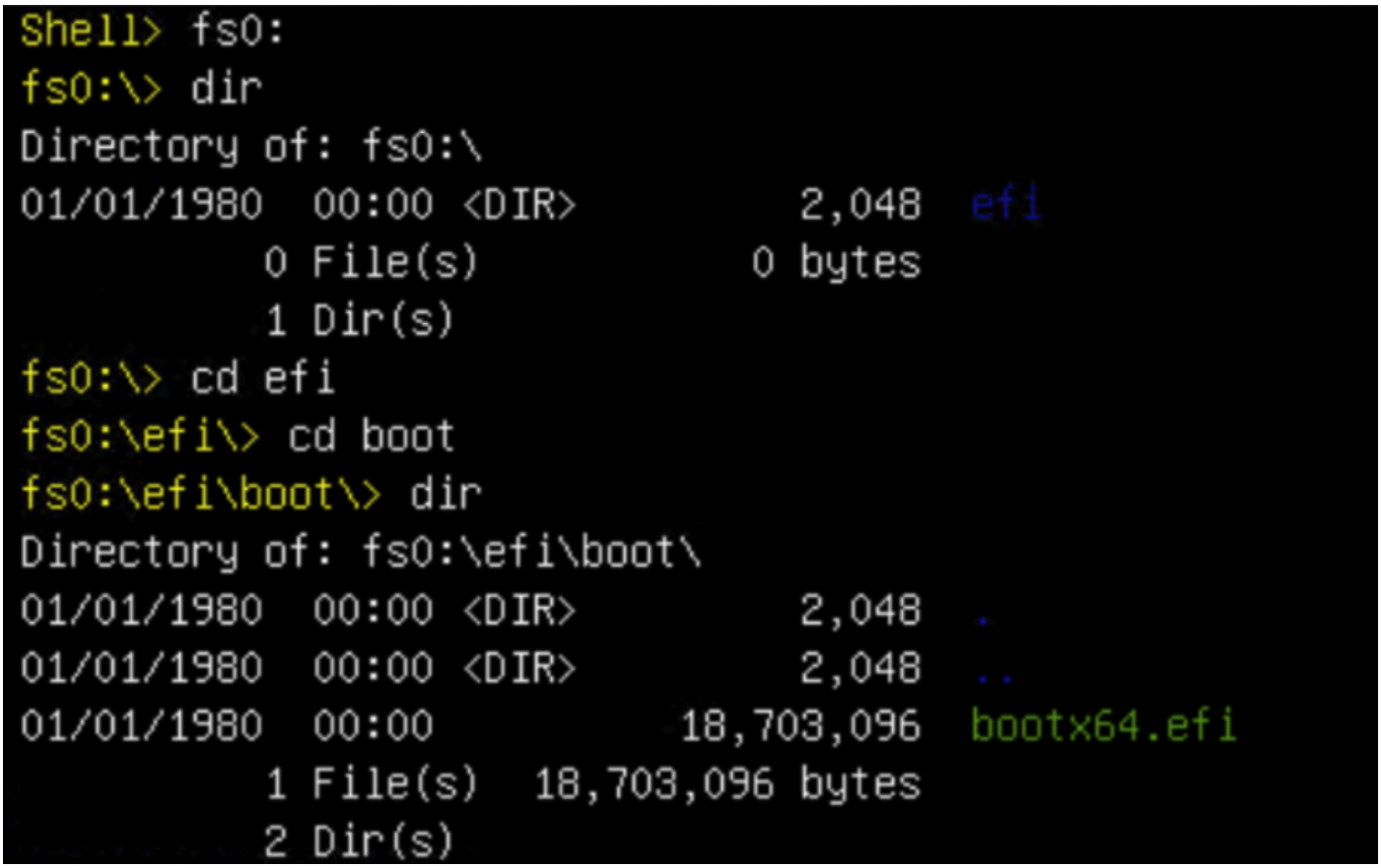
Importante

Identificazione del file system corretto:

- Come per la schermata precedente, si potrebbe vedere che "fs0:" è l'unico supporto con "USB" nel loro percorso e quindi possiamo essere sicuri che questo file system contiene il supporto di avvio (aggiornamento file system).

In caso di file system mancanti:

- Se sono disponibili solo fs0: e fs1: e non è presente fs2:verificare che il supporto di avvio (file system di aggiornamento) sia stato scritto in modalità dd e sia connesso correttamente.
- I supporti di avvio (file system di aggiornamento) devono sempre avere un numero inferiore rispetto ai supporti di ripristino e devono essere sempre l'uno accanto all'altro; è infatti necessario identificare se l'unità collegata tramite USB si trova all'inizio della parte finale che potrebbe cambiare (quindi, se si trova in posizione anteriore a fs0: o in posizione posteriore a fs2:)
- In questo caso, nello screenshot sottostante, è il file ".efi" corretto, in quanto si trova nella partizione "\efi\boot" e ha la convenzione di denominazione "bootx64.efi"

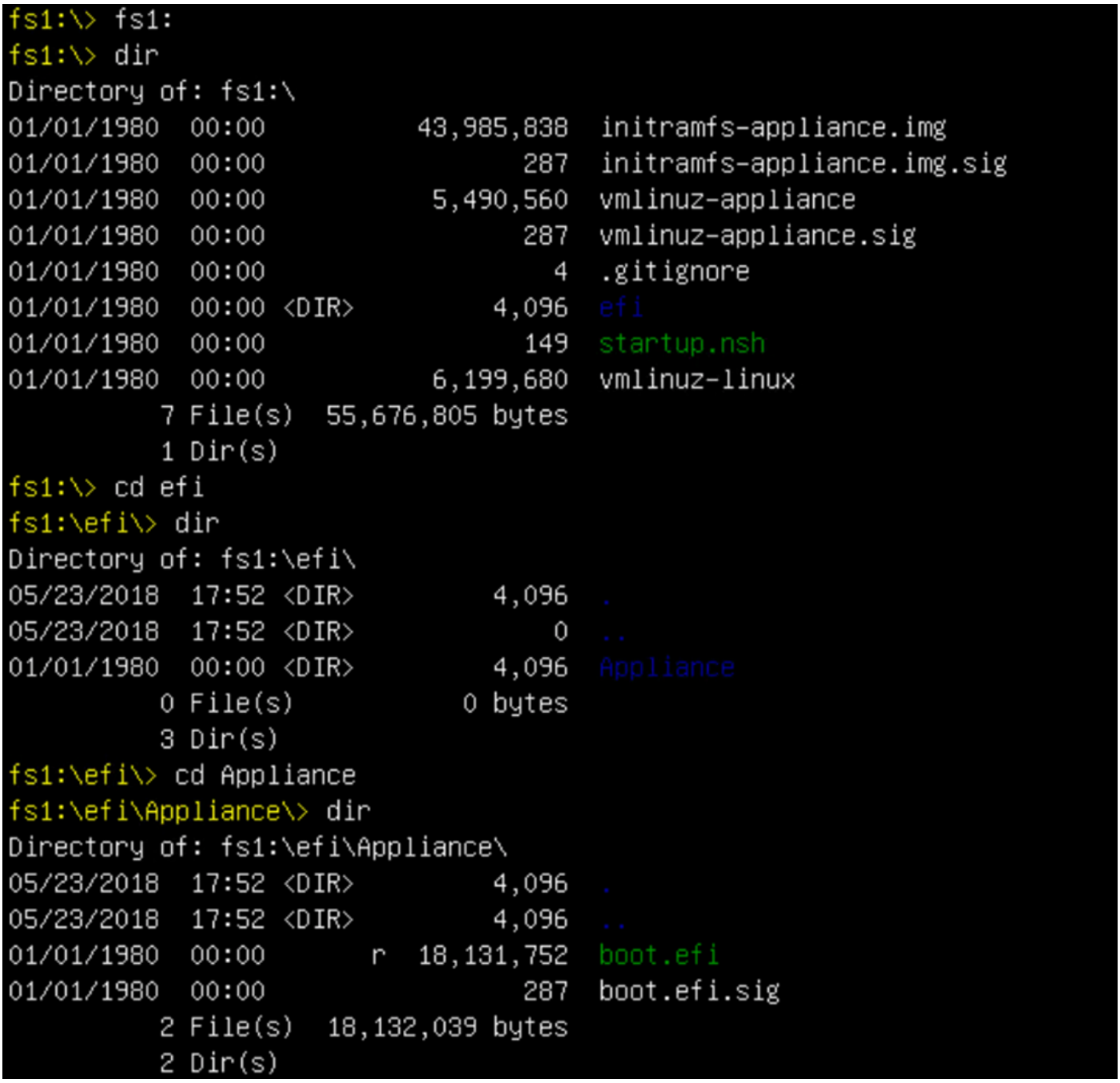


Per avviare il dispositivo nel supporto di avvio (aggiornamento del file system), è necessario eseguire il file "bootx64.efi":

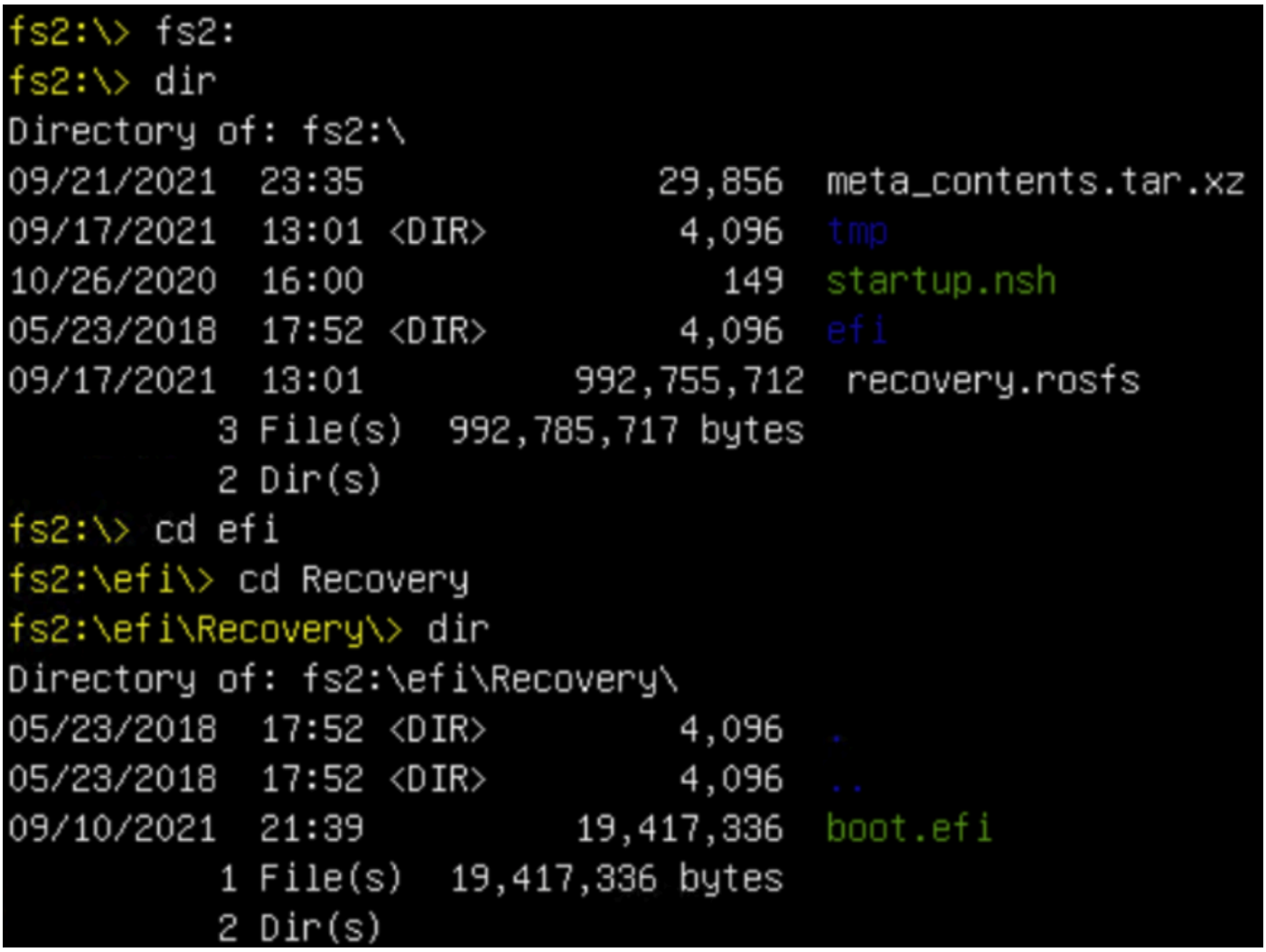
```
fs0:\efi\boot\bootx64.efi
```

Per riferimento, sono stati visualizzati i contenuti degli altri file system:

fs1: è il file system di avvio principale.



fs2: file system di avvio dell'immagine di ripristino.



Istruzioni varie:

Per verificare il file system corretto che contiene il supporto di avvio montato. A tale scopo, è possibile esplorare i diversi file system e verificare il file di avvio ".efi"

✎ Nota: la sequenza del supporto di avvio effettivo (file system di aggiornamento) che in questo caso è "fs0:" può variare anche con altri dispositivi.
Il nome e il percorso potrebbero variare, ma in tutte le immagini moderne, questo dovrebbe essere lo stesso.

Elenco di controllo che consente di individuare il supporto di avvio corretto (aggiornamento del file system):

- Se la radice di un file system contiene "vmlinuz-appliance", non è il supporto di avvio (aggiornamento del file system).
- Se la radice di un file system contiene "meta_contents.tar.xz", non è il supporto di avvio (aggiorna il file system).
- Se un file system non contiene "efi\boot\bootx64.efi", non è il supporto di avvio (aggiornare il file system).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).