Aggiorna modalità Air-Gap appliance di analisi malware sicura

Sommario

- Introduzione
- Prerequisiti
  - Componenti usati
- Premesse
  - Limitazioni
  - Requisiti
  - Operazioni preliminari
  - Aggiornare un'appliance di analisi malware sicura offline (con airgapped)
    - Convenzioni di denominazione
    - Limitazioni
  - Linux/MAC - Download ISO
    - Requisiti
    - Componenti usati
    - Configurazione
    - Scaricare l'ISO utilizzando il comando Desync
  - Windows - Download ISO
    - Scaricare l'ISO utilizzando il comando Desync
  - Appliance di avvio da USB
    - Come trovare il dispositivo /dev corretto
    - status=opzione di avanzamento
  - Sequenza di avvio per unità disco rigido per aggiornamenti offline
    - Requisito:

Introduzione

In questa guida vengono descritte le procedure per l'aggiornamento di un'appliance di analisi malware protetto in modalità air-gap.

Nota:la manutenzione degli apparecchi in modalità air-gap può ridurne l'efficacia. Prima di procedere, considerare il compromesso tra sicurezza e funzionalità.

Prerequisiti

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

Cisco consiglia di familiarizzare con i seguenti argomenti:

- Sistema operativo basato su Windows 10 e Linux (ad esempio: CentOS, RedHat)
- RUFUS 2.17
- C220 M4, M510 e M520 M5, M610 e M620 M6 (modelli di appliance)

Le informazioni fornite in questo documento si basano sui dispositivi usati in un ambiente lab controllato con configurazioni predefinite. Se la rete è operativa, procedere con cautela e comprendere a fondo le potenziali implicazioni di qualsiasi comando prima di procedere.

Premesse

La maggior parte degli accessori di analisi malware sicuri si connette a Internet e utilizza il processo di aggiornamento online. Tuttavia, alcuni elettrodomestici sono mantenuti rigorosamente all'interno delle reti interne (air-gapped). Cisco sconsiglia questo approccio perché riduce l'efficacia. La presente guida illustra il processo di aggiornamento offline per gli utenti che devono eseguire la manutenzione di apparecchiature con interruzioni dell'aria.

Per gli aggiornamenti non in linea di Secure Malware Analytics, Cisco fornisce supporti di aggiornamento su richiesta. Seguire il processo di aggiornamento offline descritto in questo documento.

Supporti: I supporti di aggiornamento Airgap (offline) sono forniti dal supporto di analisi malware sicuro su richiesta. Si tratta di un file ISO che può essere copiato su un'unità USB o HDD (con dimensioni sufficienti).

Dimensioni:le dimensioni dei supporti di aggiornamento variano in base alle versioni supportate e possono aumentare in modo significativo con l'introduzione di nuove macchine virtuali. Per le versioni correnti, le dimensioni sono di circa 30 GB, incluso lo strumento desync, che consente aggiornamenti incrementali per le modifiche relative alla VM.

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 nell'accessorio il contenuto associato a tale versione successiva. 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.

Ganci 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.

Ripetere Se Necessario: Ciascun ciclo di avvio di tali supporti aggiorna quindi (o si prepara ad aggiornare) solo un passaggio verso la release di destinazione finale; per eseguire l'aggiornamento alla versione di destinazione desiderata, l'utente deve eseguire l'avvio tutte le volte che è necessario.

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 sulla versione per le 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 alla configurazione e alla 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 delle versioni degli accessori

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: Aggiornamento di TGA Airgap 2.16.2-2.17.2.

Questo supporto può essere utilizzato per un accessorio con una versione minima: 2.16.2 e aggiornare l'accessorio alla versione: 2.17.2 .

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

Le informazioni fornite in questo documento si basano su un sistema operativo Linux (ad esempio: CentOS, RedHat).

Le informazioni fornite in questo documento si basano sui dispositivi usati in un ambiente lab controllato con configurazioni predefinite. Se la rete è operativa, procedere con cautela e comprendere a fondo le potenziali implicazioni di qualsiasi comando prima di procedere.

Configurazione

Installare il linguaggio di programmazione GO

```
# wget https://go.dev/dl/go1.23.1.linux-amd64.tar.gz
# tar -xzf go1.23.1.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 localmente il contenuto del file Zip fornito dal supporto di Secure Malware Analytics includendo il file desync.linux e .caibx nella stessa directory del 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 di trovarsi nella directory.

```
# pwd
```

Passaggio 4. Una volta entrati nella 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 2.16.2 a 2.17.2 ISO:

```
# desync extract -k -s s3+https://s3.amazonaws.com/sma-appliance-airgap-update airgap-update-2.16.2ag-2
```

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 comporre l'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).

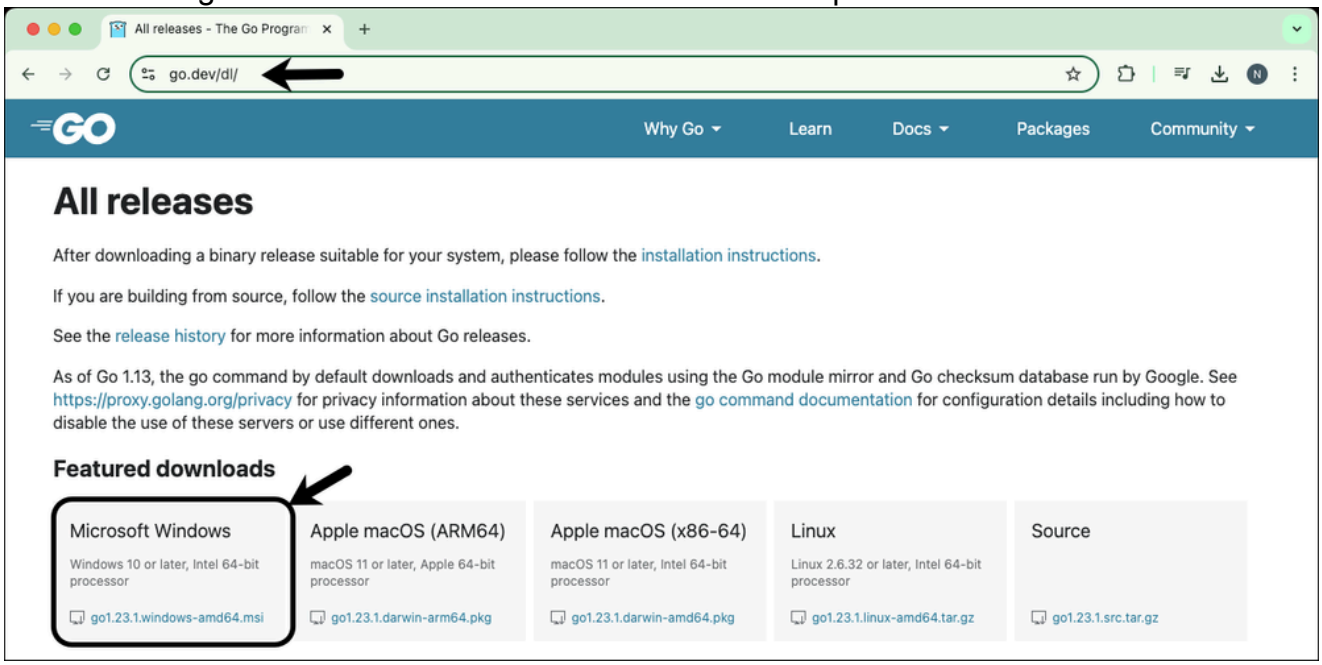
Inserire l'unità USB e accendere o riavviare l'accessorio. Nella schermata di avvio di Cisco, premere F6 per accedere al menu di avvio.

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
```

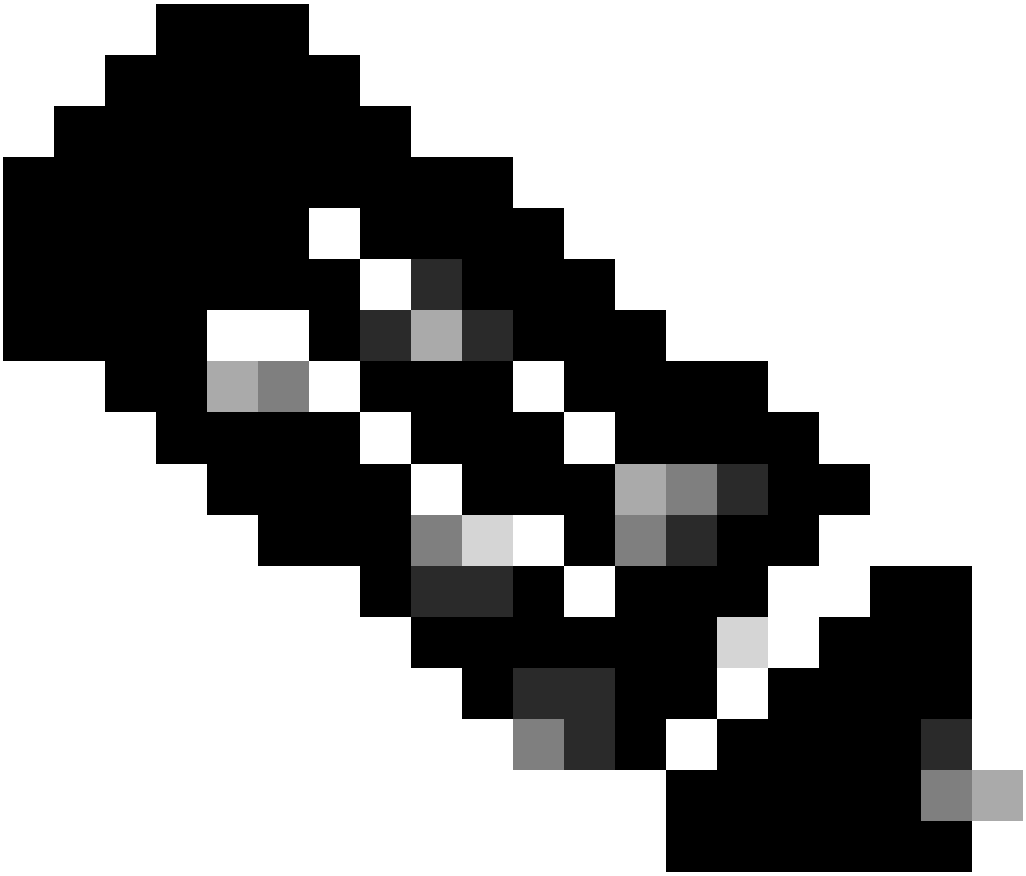
Scaricare l'ISO utilizzando il comando Desync

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

```
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 co

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



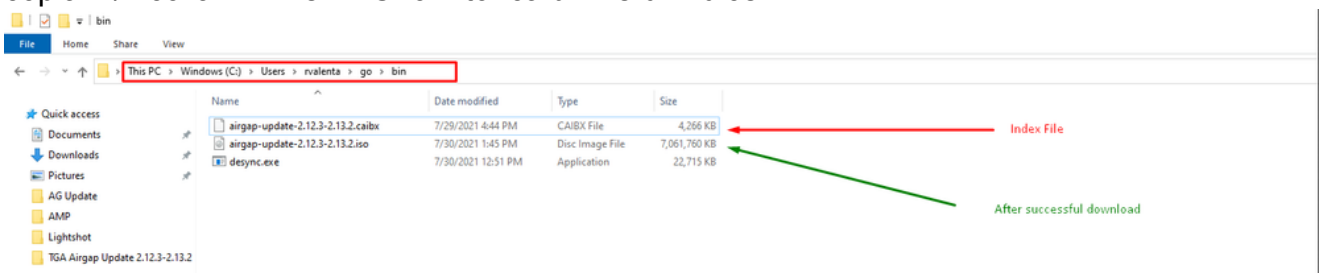
Nota: Se il comando git non funziona, è possibile scaricare e installare Git da qui: https://git-scm.com/download/win.

Quindi esegui sotto due comandi uno per uno:

```
cd desync/cmd/desync

go install
```

```
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. Passare a vai — > posizione contenitore. Ad esempio C:\Users\<nomeutente>\go\bin e copiarvi/incollarvi il file TAC fornito .caibx file di indice.

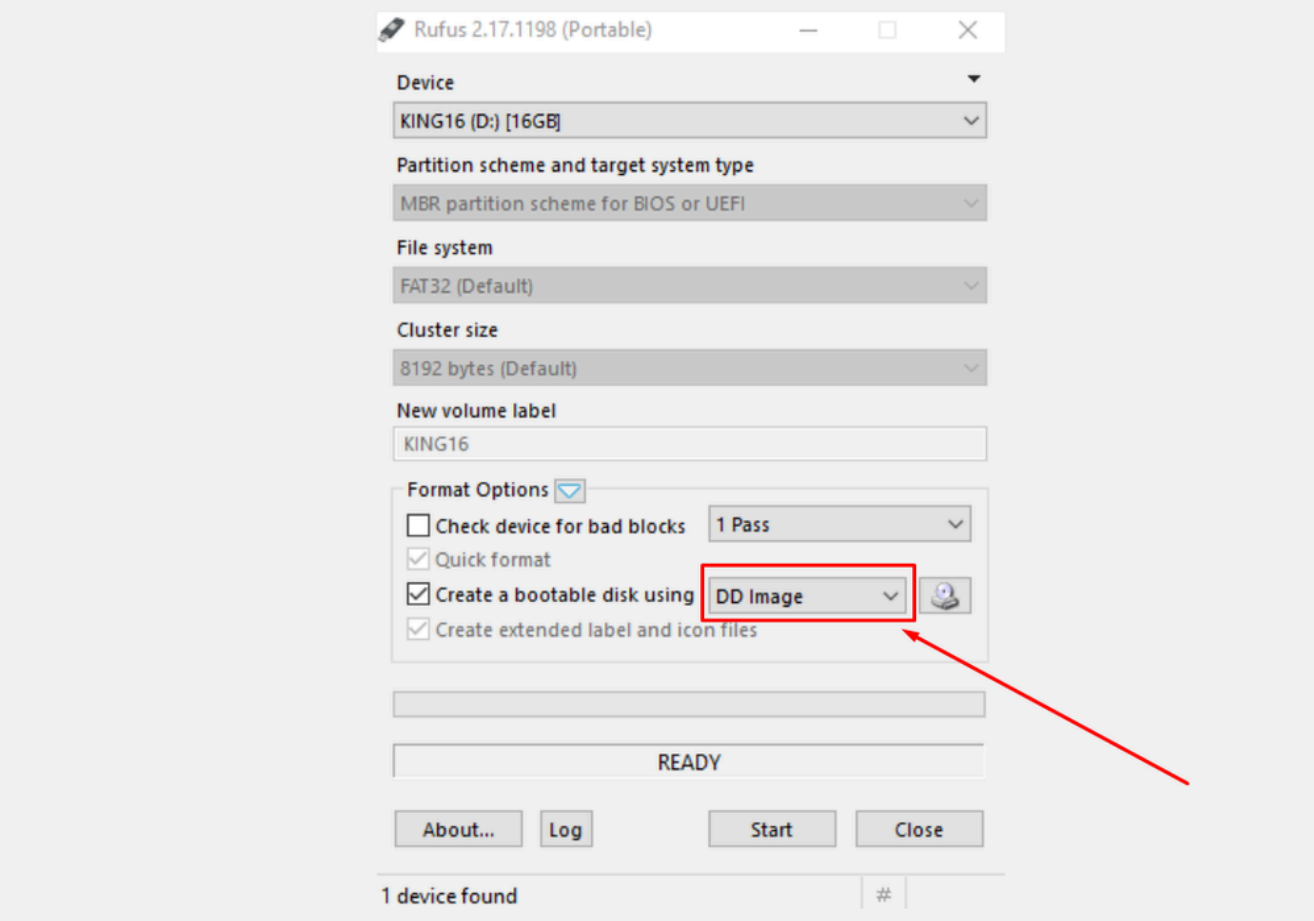


4. (Verifica) Tornare al prompt di CMD e selezionare la cartella go\bin ed eseguire i comandi di download. Il download dovrebbe procedere immediatamente. Attendere il completamento del download. L'intero file .ISO si trova nella stessa posizione del file .caibx copiato in precedenza file indice

```
\$HOME/go/bin/desync extract -k -s s3+https://s3.amazonaws.com/sma-appliance-airgap-update airgap-
```

```
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>_
```

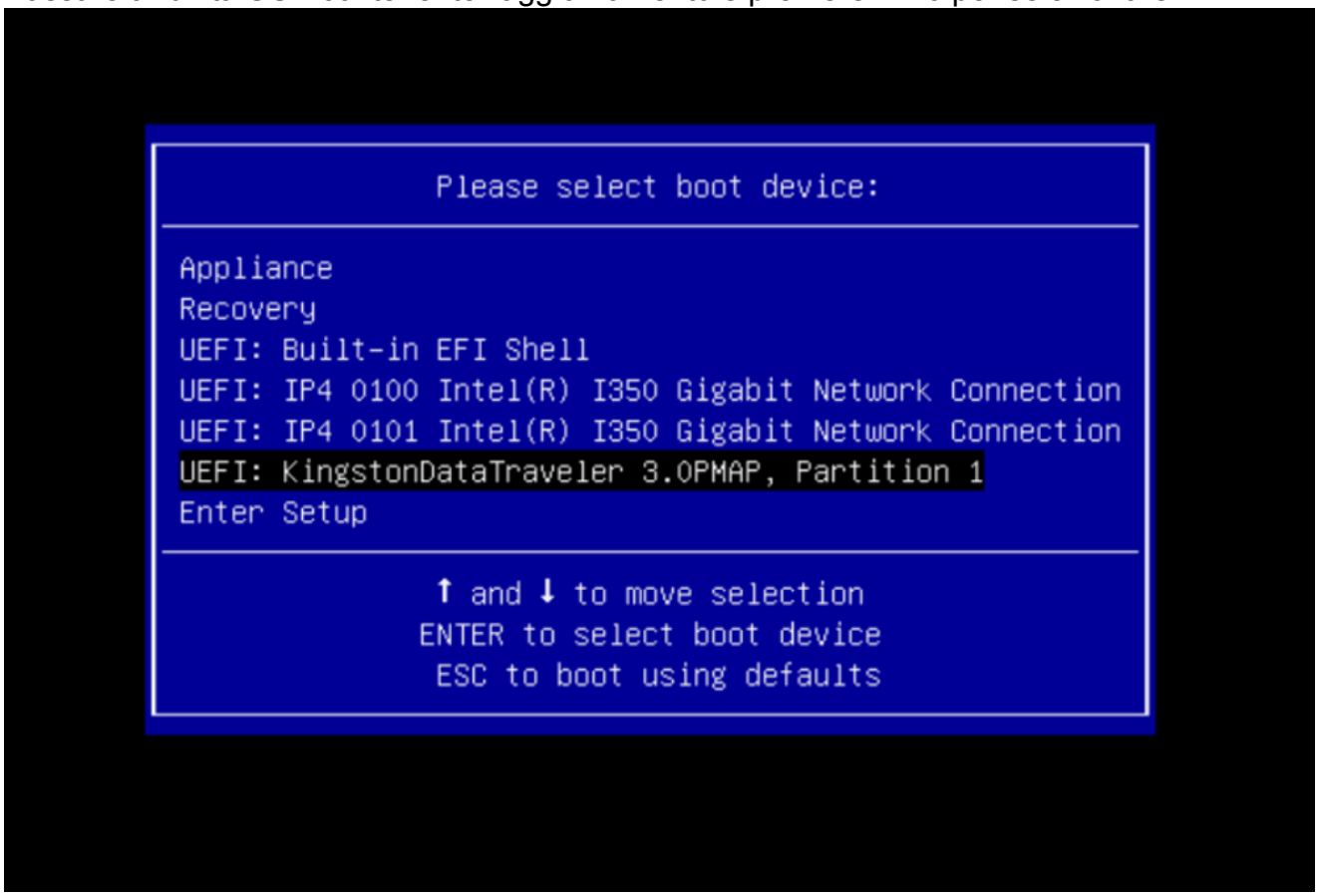
Per la creazione di questo USB di ripristino specifico, è fondamentale utilizzare Rufus versione 2.17, in quanto consente di utilizzare opzioni di aggiunta essenziali. In questo repository sono disponibili tutte le versioni di RUFUS.



Appliance di avvio da USB

1. Inserire l'USB, riavviare l'accessorio, e premere rapidamente F6 nella schermata di avvio di Cisco per accedere al menu di avvio.

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



   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.

3. 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 il riavvio aggiuntivo come parte dell'aggiornamento, che è realizzato con il 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 possono essere utilizzate 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. Ciò 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 relativa al processo di aggiornamento offline TGA, il comando informato 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 b
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 th
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: Una volta restituito il comando "dd", l'operazione di scrittura sul dispositivo di blocco non è stata completata, ma è stata rilevata 11 secondi dopo il ritorno.
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 a blocchi consentono a un'applicazione di leggere/scrivere in blocchi di dati di dimensioni diverse; read()/write() vengono applicati alle cache di pagina (buffer) e non direttamente al 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" rispetto al mancato utilizzo dell'opzione; ma, se è abilitato, assicura 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 b
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: Prendere in considerazione questo flag (oflag=sync) del comando "dd" quando si lavora su questo tipo di richiesta.

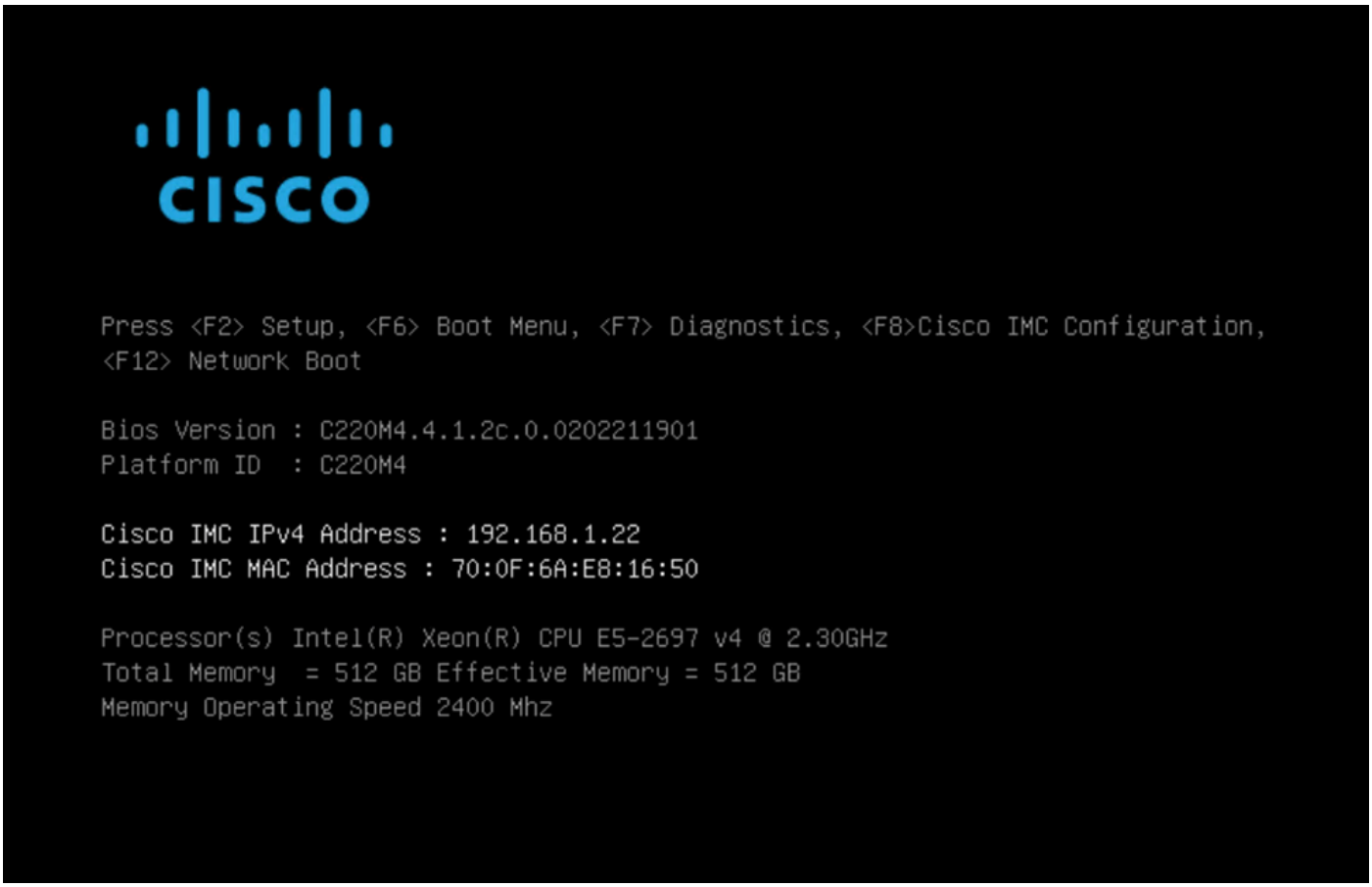
Sequenza di avvio per unità disco rigido per aggiornamenti offline

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.

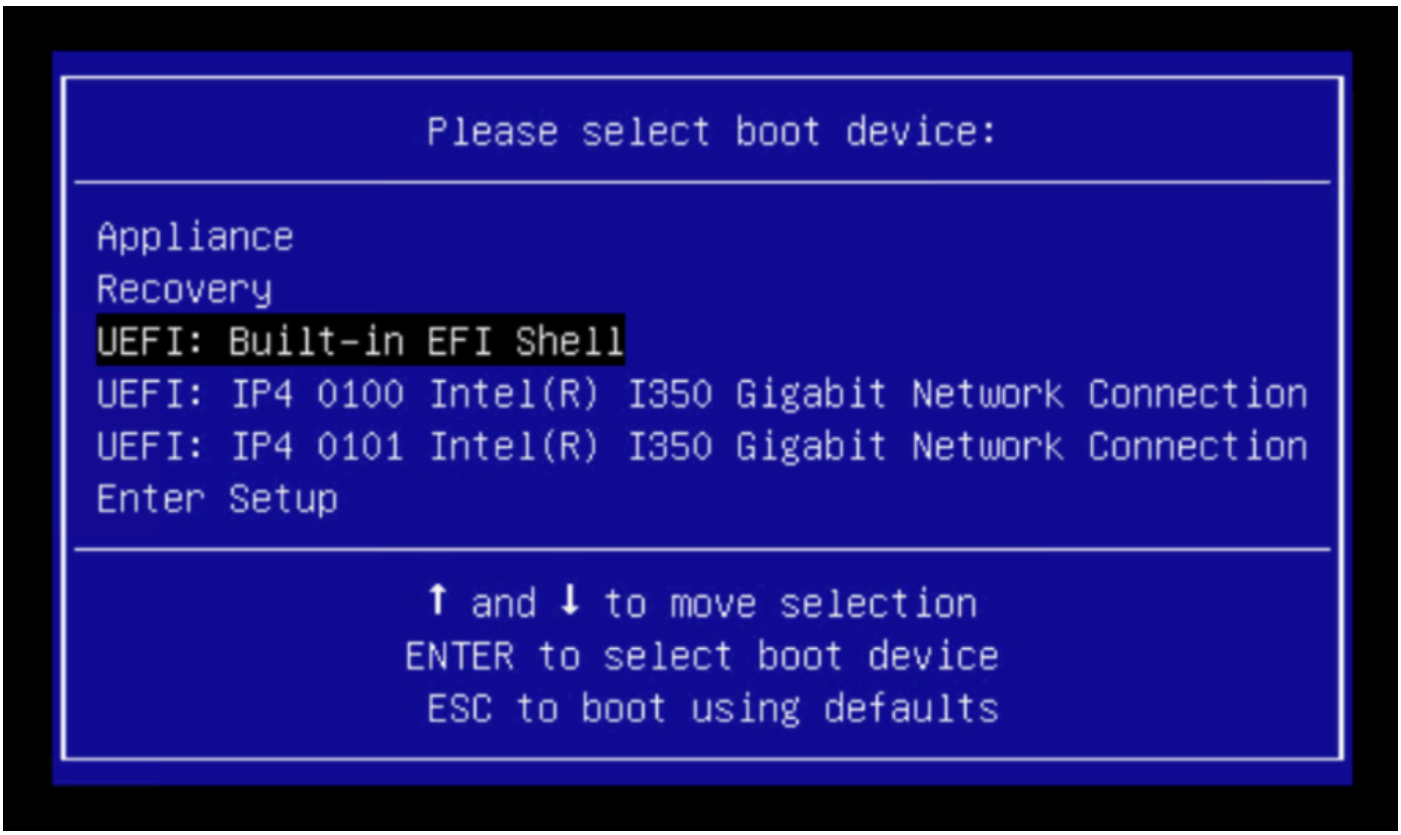
Una volta caricato il supporto sull'HDD/USB utilizzando la formattazione "DD", è necessario collegarlo all'accessorio TGA e riavviare il dispositivo.

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 l'accesso alla shell EFI, si noterà che le partizioni rilevate in questo caso sono 3 file system: 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

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 solo fs0: e fs1: sono disponibili e non è presente alcun fs2:, verificare che il supporto di avvio (file system di aggiornamento) sia stato scritto in modalità dd e sia stato collegato correttamente.
- I supporti di avvio (file system di aggiornamento) devono avere sempre un numero inferiore rispetto ai supporti di ripristino e devono essere sempre l'uno accanto all'altro; è possibile stabilire se l'unità collegata tramite USB si trova all'inizio dell'estremità che potrebbe cambiare (quindi, se prende la posizione anteriore in fs0: o la posizione posteriore a fs2:) devono essere identificate
- 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"

```
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)
```

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: Si tratta del file system di avvio principale.

```
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: File system di avvio dell'immagine di ripristino.

```
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)
```

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).