Aktualisieren des Air-Gap-Modus der Appliance für sichere Malwareanalysen

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Aktualisierung des Air-Gap-Modus der Secure Malware Analytics Appliance beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse von Eingaben über die Befehlszeile in Windows- und Unix/Linux-Umgebungen

- Kenntnisse der Malware-Analyse-Appliance
- Kenntnisse des Cisco Integrated Management Controller (IMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die meisten Appliances für sichere Malware-Analyse sind mit dem Internet verbunden und verwenden daher den Online-Aktualisierungsprozess. In einigen Fällen werden Secure Malware Analytics-Appliances jedoch nur innerhalb interner Netzwerke verwaltet, d. h. "Air-Gap". Wir raten davon ab, die Appliance "Air-Gap" zu verwenden, da dies die Effektivität der Appliance beeinträchtigt. Dieser Kompromiss kann jedoch erforderlich sein, um zusätzliche Sicherheits- oder gesetzliche Anforderungen zu erfüllen.

Für Benutzer, die ihre Secure Malware Analytics-Appliances ohne Internetverbindung ausführen, bieten wir den in diesem Dokument beschriebenen Offline-Aktualisierungsprozess an. Aktualisierungsmedien werden auf Anfrage vom Secure Malware Analytics Support bereitgestellt. Details hierzu finden Sie weiter unten.

Medien: Aktualisierungsmedien für Airgap (offline) werden vom Secure Malware Analytics Support als ISO bereitgestellt und können entweder auf ein USB-Medium oder eine HDD (Festplatte) kopiert werden, wenn eine entsprechende Größe verfügbar ist.

Größe: Die Größe hängt von den Versionen ab, die von den Update-Medien unterstützt werden, kann jedoch bei Einführung neuer VMs zwischen Quell- und Zielversion häufig mehrere Dutzend Gigabyte betragen. Bei den aktuellen Versionen sind es möglicherweise ca. 30 GB, da das Desync-Tool bei der inkrementellen Aktualisierung der VM-bezogenen Änderungen hilft.

Upgrade-Bootzyklus: Jedes Mal, wenn das airgap-Aktualisierungsmedium gebootet wird, bestimmt es die nächste Version, auf die aktualisiert werden soll, und kopiert den mit dieser nächsten Version verknüpften Inhalt auf die Appliance. Eine bestimmte Version kann auch eine Paketinstallation initiieren, wenn für diese Version keine erforderlichen Prüfungen vorhanden sind, die ausgeführt werden müssen, während die Appliance ausgeführt wird. Wenn die Version solche Prüfungen enthält oder Teile des Aktualisierungsprozesses überschreiben, die solche Prüfungen hinzufügen könnten, gilt das Update erst, wenn sich der Benutzer bei OpAdmin anmeldet und das

Update mit OpAdmin > Operations > Update Appliance aufruft.

Vorinstallationshaken: Je nachdem, ob Vorinstallationshaken für das jeweilige Upgrade vorhanden sind, wird das Upgrade entweder sofort ausgeführt oder die Appliance wird wieder in den regulären Betriebsmodus gestartet, damit der Benutzer die übliche Administrationsoberfläche betreten und das Upgrade von Hand starten kann.

Bei Bedarf wiederholen: Jeder dieser Medien-Bootzyklen führt daher nur einen Schritt in Richtung der letztendlichen Zielversion durch (oder bereitet sich auf die Aktualisierung vor); der Benutzer muss so oft booten, wie es für die Aktualisierung auf die gewünschte Zielversion erforderlich ist.

Einschränkungen

CIMC-Medien werden für Air-Gap-Updates nicht unterstützt.

Aufgrund von Lizenzbeschränkungen bei verwendeten Drittanbieterkomponenten sind Upgrade-Medien für 1.x-Versionen nach dem Ende der Lebensdauer der UCS M3-Hardware nicht mehr verfügbar. Daher ist es wichtig, dass die UCS M3-Appliances vor dem EOL ausgetauscht oder aktualisiert werden.

Anforderungen

Migrationen: Wenn die Versionshinweise für die abgedeckten Versionen Szenarien umfassen, in denen eine Migration vor der Installation der nächsten Version zwingend erforderlich ist, muss der Benutzer diese Schritte vor einem Neustart befolgen, um zu vermeiden, dass die Appliance in einen unbrauchbaren Zustand versetzt wird.

Hinweis: Insbesondere die erste Version 2.1.x, die neuer als 2.1.4 ist, führt mehrere Datenbankmigrationen aus. Es ist gefährlich, fortzufahren, bis diese Migrationen abgeschlossen sind. Weitere Informationen finden Sie im Migrationshinweis zur Threat Grid Appliance 2.1.5.

Wenn die airgap-Upgrade-Medien ab einer Version vor 2.1.3 einen von der individuellen Lizenz abgeleiteten Verschlüsselungsschlüssel verwenden und daher für jede Appliance angepasst werden müssen. (Der einzige sichtbare Effekt für Benutzer besteht darin, dass Secure Malware Analytics für die Unterstützung von Originalversionen vor 2.1.3 die Lizenzen benötigt, die zuvor auf diesen Appliances installiert wurden, und die Medien auf den Appliances funktionieren, die nicht in der Liste aufgeführt sind, für die sie erstellt wurden.)

Ab Version 2.1.3 oder später sind die AirGap-Medien allgemein gehalten, und Kundeninformationen sind nicht erforderlich.

Vorbereitungen

- Sicherung. Sie müssen eine Sicherung Ihrer Appliance in Betracht ziehen, bevor Sie mit der Aktualisierung fortfahren.
- Überprüfen Sie in den Versionshinweisen für die zu aktualisierende Version, ob

Hintergrundmigrationen erforderlich sind, bevor Sie eine Aktualisierung auf die neuere Version planen.
- Überprüfen Sie die aktuelle Version Ihrer Appliance: OpAdmin > Operations > Update Appliance
- Lesen Sie den Versionsverlauf der Secure Malware Analytics Appliance in der Suchtabelle Build Number/Version (Build-Nummer/Version), die in allen Threat Grid Appliance-Dokumenten verfügbar ist: Versionshinweise, Migrationshinweise, Setup- und Konfigurationsanleitung und Administratoranleitung.

Aktualisieren einer Anwendung für sichere Offline-Malwareanalysen (Airgapped)

Erster Blick auf verfügbare Air Gap Version auf dieser Seite: Appliance Version Lookup Table

1. Erstellen Sie eine TAC-Support-Anfrage, um die Offline-Update-Medien zu erhalten. Diese Anforderung muss die Seriennummer der Einheit sowie die Build-Nummer der Einheit enthalten.

2. TAC Support liefert ein aktualisiertes ISO basierend auf Ihrer Installation.

3. Brennen Sie das ISO-Image auf einen bootfähigen USB-Anschluss. Beachten Sie, dass USB das einzige unterstützte Gerät/die einzige unterstützte Methode für Offline-Updates ist.

Namenskonventionen

Dies ist der aktualisierte Dateiname ex: TGA Airgap Update 2.13.2-2.14.0.

Dies würde bedeuten, dass dieses Medium für eine Appliance mit der Mindestversion 2.13.2 verwendet werden kann und die Appliance auf die Version 2.14.0 aktualisiert werden kann.

Einschränkungen

- CIMC-Medien werden für Air-Gap-Updates nicht unterstützt.
- Aufgrund von Lizenzbeschränkungen bei verwendeten Drittanbieterkomponenten sind Upgrade-Medien für 1.x-Versionen nach dem Ende der Lebensdauer der UCS M3-Hardware nicht mehr verfügbar. Daher ist es wichtig, dass die UCS M3-Appliances vor dem EOL ausgetauscht oder aktualisiert werden.

Linux/MAC - ISO-Download

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Ein Linux-Rechner mit Internetzugang, um die ISO-Datei herunterzuladen und das bootfähige USB-Installationslaufwerk zu erstellen.
- Die Anweisungen zum Herunterladen von Airgap werden vom Secure Malware Analytics Support bereitgestellt.
- GO-Programmiersprache. Herunterladen

- Die .caibx Indexdatei (enthalten in der vom TAC Support bereitgestellten ZIP-Datei).
- Desync Tool (in der vom Secure Malware Analytics Support bereitgestellten ZIP-Datei enthalten).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer CentOS Linux-Version 7.6.1810 (Core).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Installieren der GO-Programmiersprache

```
# 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
```

Führen Sie diese drei Befehle nach der Installation aus, falls der Befehl desync nicht fehlschlägt.

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

Sie können die GO-Version wie folgt überprüfen:

```
# go version
```

ISO mit dem Desync-Befehl herunterladen

Schritt 1: Kopieren Sie den Inhalt der Zip-Datei, die von Secure Malware Analytics Support bereitgestellt wird, einschließlich der Dateien desync.linux und .caibx lokal auf dem Computer in dasselbe Verzeichnis.

Schritt 2: Wechseln Sie in das Verzeichnis, in dem Sie die Dateien gespeichert haben:

Beispiel:

```
# cd MyDirectory/TG
```

Schritt 3: Führen Sie den Befehl pwd aus, um sicherzustellen, dass Sie sich im Verzeichnis befinden.

```
# pwd
```

Schritt 4: Sobald Sie sich im Verzeichnis befinden, das den Befehl desync.linux und die Datei .caibx enthält, führen Sie den Befehl Ihrer Wahl aus, um den Download-Prozess zu starten.

Hinweis: Dies sind die Beispiele für verschiedene ISO-Versionen. Lesen Sie dazu die Datei .caibx aus den Anweisungen des Secure Malware Analytics-Supports.

Für Version 2.1.3 bis 2.4.3.2 ISO:

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

Für Version 2.4.3.2 bis 2.5 ISO:

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

Für Version 2.5 bis 2.7.2ag ISO:

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

Sobald der Download beginnt, wird eine Statusleiste angezeigt.

Hinweis: Die Download-Geschwindigkeit und die Größe der Upgrade-Medien in Ihrer Umgebung können sich auf die Zeit für die ISO-Erstellung auswirken.
Bitte vergleichen Sie das MD5 der heruntergeladenen Datei mit dem verfügbaren Paket, das vom Support zur Verfügung gestellt wird, um die Integrität des heruntergeladenen ISO zu

---

überprüfen.

Nach Abschluss des Downloads werden die ISOs im gleichen Verzeichnis erstellt.

Schließen Sie den USB-Stick an den Computer an, und führen Sie den Befehl dd aus, um das bootfähige USB-Laufwerk zu erstellen.

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

<MY_USB> ist der Name Ihres USB-Sticks (lassen Sie die spitzen Klammern weg).

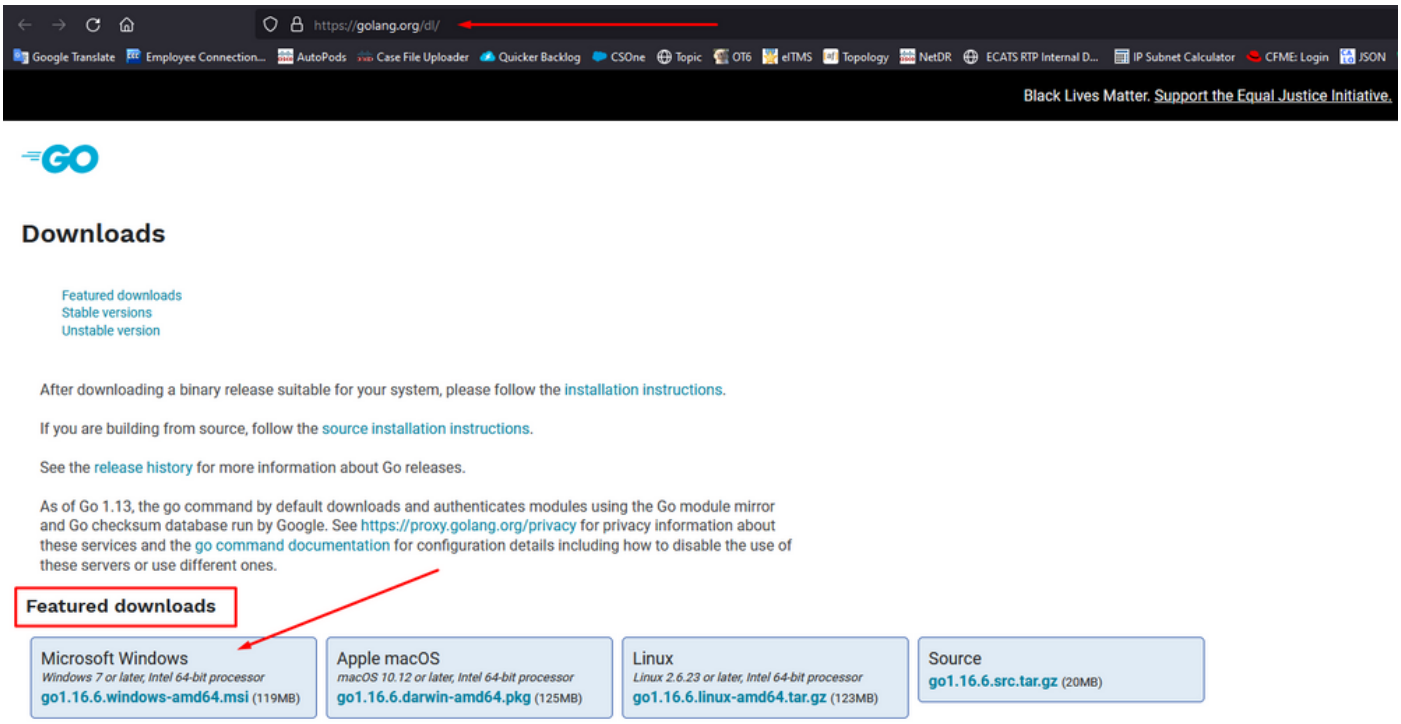
Legen Sie das USB-Laufwerk ein, und schalten Sie die Einheit ein, oder starten Sie sie neu. Drücken Sie auf dem Cisco Bootbildschirm die F6-Taste, um das Startmenü aufzurufen.

Tipp:
Führen Sie den Download außerhalb der Geschäftszeiten oder außerhalb der Geschäftszeiten aus, da dies die Bandbreite beeinträchtigen kann.
Um das Werkzeug zu stoppen, schließen Sie entweder das Terminal oder drücken Sie Strg+c/Strg+z.
Um fortzufahren, führen Sie den gleichen Befehl aus, um den Download fortzusetzen.

Windows - ISO-Download

Installieren der GO-Programmiersprache

#1: Die erforderliche GO-Programmiersprache herunterladen. Installieren von https://golang.org/dl/ In meinem Fall wähle ich die Version mit den Funktionen aus. Starten Sie den CMD neu und testen Sie mit



Schließen Sie den CMD-Befehl run, und öffnen Sie ihn erneut, um Folgendes zu überprüfen:

```
go version
```

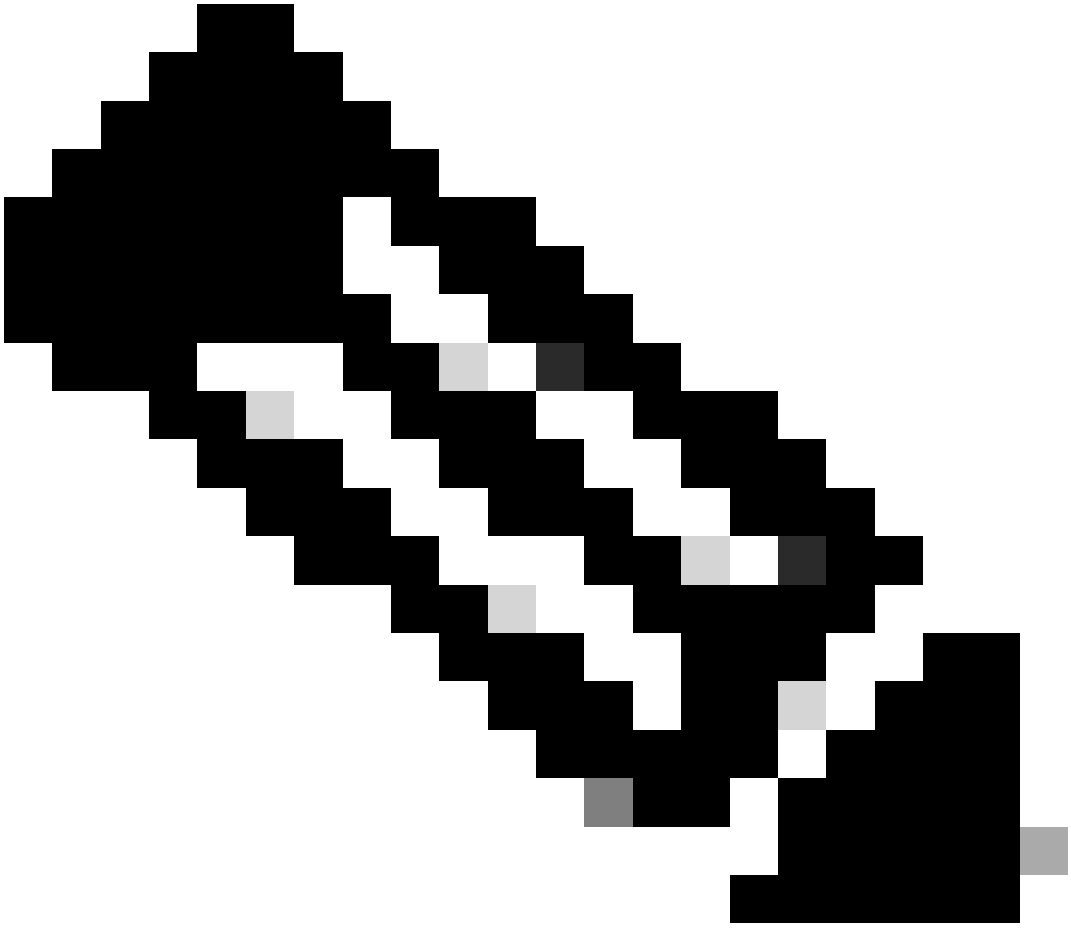
ISO mit dem Desync-Befehl herunterladen

#2: Installieren Sie das Tool DESYNC. Nach der Ausführung des Befehls werden Sie eine Reihe von Download-Aufforderungen bemerken. Etwa nach 2-3 Minuten sollte der Download erfolgen.

```
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
```



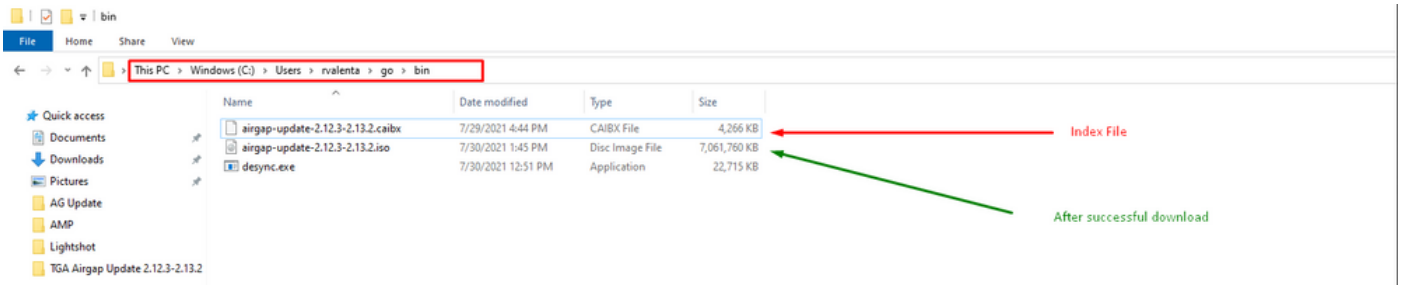
Hinweis: Wenn der Befehl git nicht funktioniert, können Sie Git hier herunterladen und installieren: https://git-scm.com/download/win.

Führen Sie dann die folgenden beiden Befehle nacheinander aus:

```
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: Navigieren Sie zu go — > bin location. In meinem Fall war dies C:\Users\rvalenta\go\bin, und kopieren/einfügen Sie dort die TAC provided.caibx Indexdatei.



Überprüfung

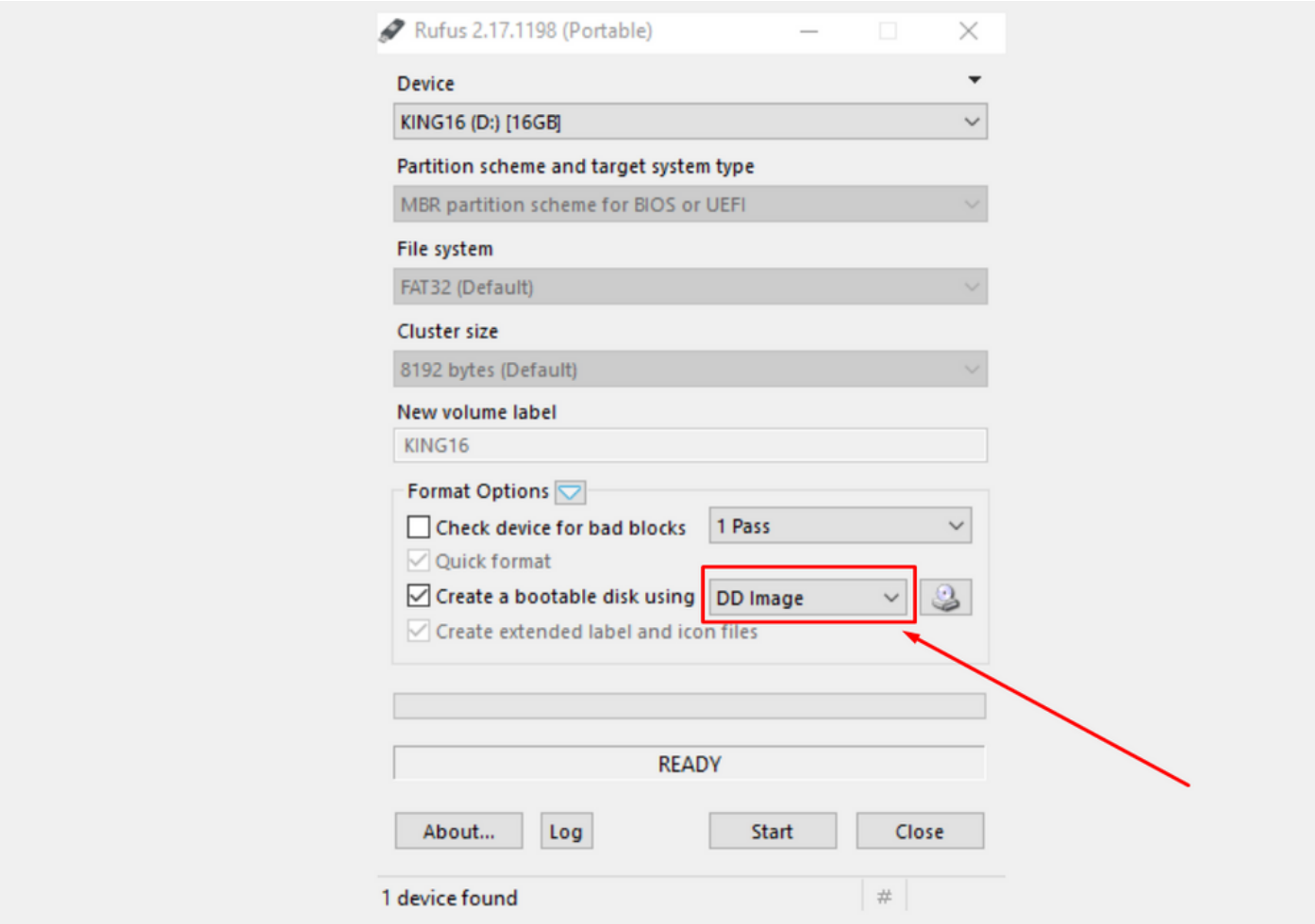
#4: Wechseln Sie zurück zur CMD-Eingabeaufforderung, navigieren Sie zum Ordner go\bin, und führen Sie die Download-Befehle aus. Sie sollten sofort sehen, dass der Download fortgesetzt wird. Warten Sie, bis der Download abgeschlossen ist. Sie sollten nun die gesamte .ISO-Datei am gleichen Speicherort wie die zuvor kopierte .caibx Indexdatei haben

```
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>
```

Verwenden Sie dann RUFUS, um einen bootfähigen USB-Anschluss zu erstellen. Dies ist sehr wichtig, um Version 2.17 zu verwenden. Dies ist die letzte Version, wo Sie dd Optionen verwenden können, die sehr wichtig ist, um diese spezifische USB-Wiederherstellung zu erstellen.

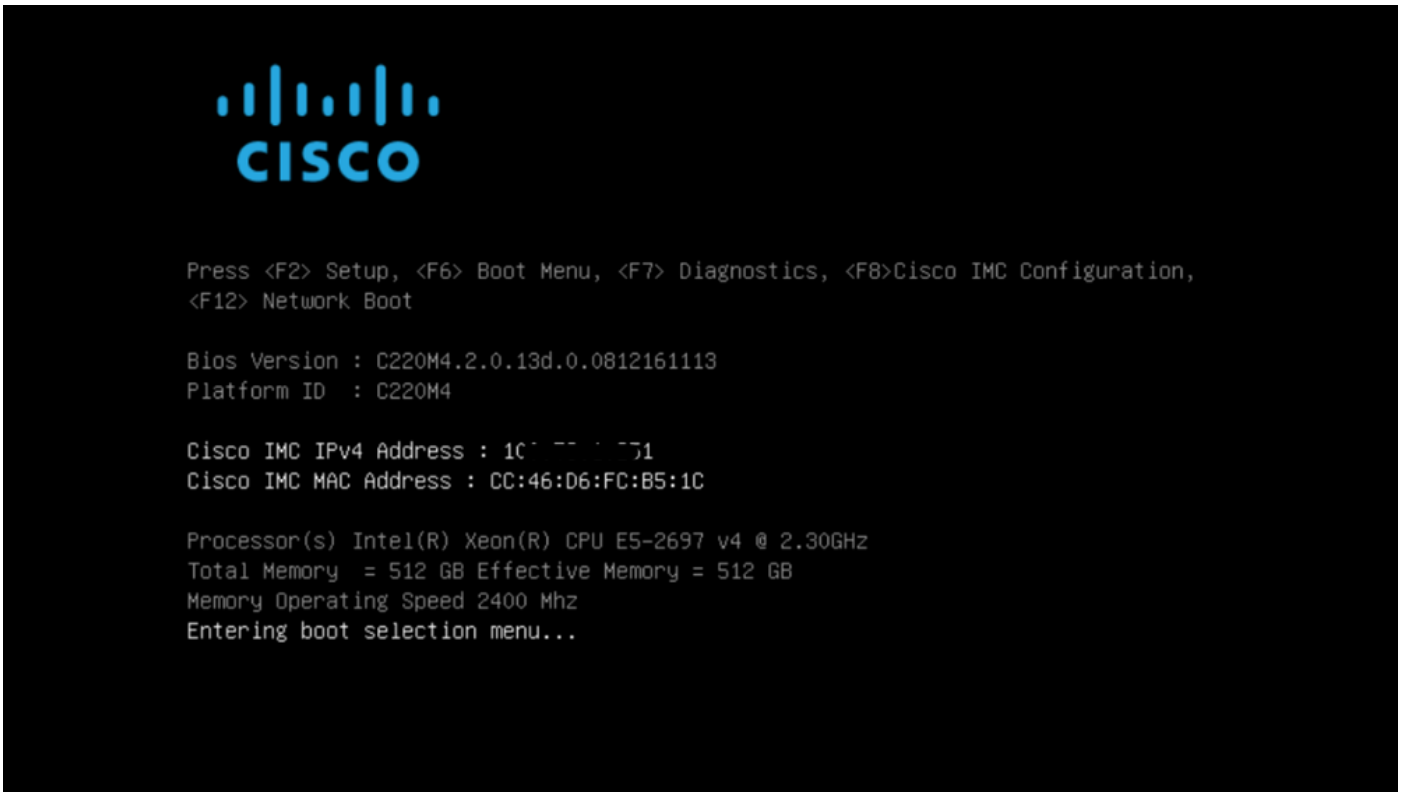
Sie können alle Versionen dieses Projektarchivs RUFUS REPOSITORY finden Falls diese Dateien nicht mehr verfügbar sind, schließe ich in diesem Dokument auch Installationsprogramme für vollständige und portable Versionen ein.



Einheit über USB booten

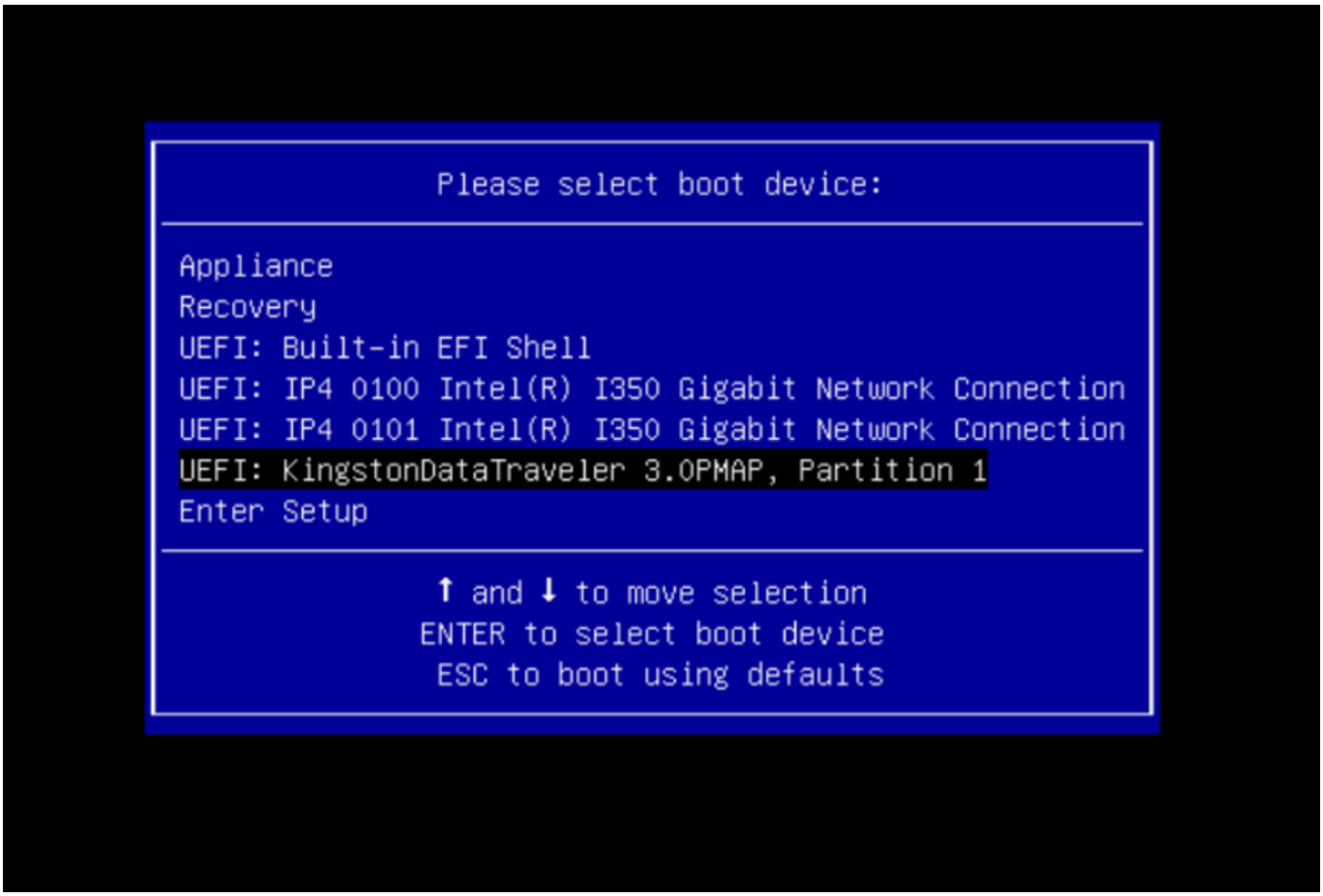
Legen Sie das USB-Laufwerk ein, und schalten Sie die Einheit ein, oder starten Sie sie neu. Wählen Sie auf dem Cisco Bootbildschirm die Option "F6" aus, um in das Boot-Menü zu wechseln. Du musst schnell sein! Sie haben nur wenige Sekunden, um diese Auswahl zu treffen. Wenn Sie es verpassen, müssen Sie neu starten und es erneut versuchen.

Abbildung 1: Drücken von F6, um das Startmenü aufzurufen



Navigieren Sie zu dem USB-Laufwerk, das die Aktualisierung enthält, und drücken Sie die Eingabetaste, um Folgendes auszuwählen:

Abbildung 2: Auswählen des Update-USB



Das Aktualisierungsmedium bestimmt die nächste Version im Aktualisierungspfad und kopiert den Inhalt für diese Version auf die Appliance. Die Appliance führt das Upgrade entweder sofort aus oder führt einen Neustart in den regulären Betriebsmodus durch, sodass Sie OpAdmin aufrufen und das Upgrade manuell starten können.

Sobald der ISO-Bootvorgang abgeschlossen ist, starten Sie die Secure Malware Analytics-Appliance wieder in den Betriebsmodus.

Melden Sie sich bei der Benutzeroberfläche des Portals an, und prüfen Sie, ob Warnungen bezüglich eines sicheren Upgrades usw. vorliegen, bevor Sie fortfahren.

Navigieren Sie zur OpAdmin-Schnittstelle, und wenden Sie die Updates an, wenn sie nicht automatisch während des Neustarts angewendet wurden: OpAdmin > Operations > Update Appliance HINWEIS: Der Update-Prozess umfasst zusätzliche Neustarts als Teil des Updates, das über das USB-Medium erfolgt. Sie müssen z. B. die Schaltfläche Reboot (Neustart) auf der Installationsseite verwenden, nachdem Updates installiert wurden.

Wiederholen Sie den Vorgang bei Bedarf für jede USB-Version.

So finden Sie das richtige /dev-Gerät

Mit dem USB immer noch nicht an den Endpunkt angeschlossen führen Sie den Befehl "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$
```

Nachdem der USB-Stick angeschlossen wurde.

```
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$
```

Dies bestätigt, dass das USB-Gerät in /dev "/dev/sdb" ist.

Weitere Möglichkeiten zur Bestätigung, nachdem der USB-Stick angeschlossen wurde:

Der Befehl dmesg liefert einige Informationen. Nachdem der USB angeschlossen wurde, führen Sie den Befehl dmesg aus. | grep -iE 'usb|attached'.

```
xsilenc3x@Alien15:~/testarea/usb$ dmesg | grep -iE 'usb|attached'
[842717.663757] usb 1-1.1: new high-speed USB device number 13 using xhci_hcd
[842717.864505] usb 1-1.1: New USB device found, idVendor=0781, idProduct=5567
```

```
[842717.864510] usb 1-1.1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[842717.864514] usb 1-1.1: Product: Cruzer Blade
[842717.864517] usb 1-1.1: Manufacturer: SanDisk
[842717.864519] usb 1-1.1: SerialNumber: 4C530202420924105393
[842717.865608] usb-storage 1-1.1:1.0: USB Mass Storage device detected
[842717.866074] scsi host1: usb-storage 1-1.1:1.0
[842718.898700] sd 1:0:0:0: Attached scsi generic sg1 type 0
[842718.922265] sd 1:0:0:0: [sdb] Attached SCSI removable disk  <-------
xsilenc3x@Alien15:~/testarea/usb$
```

Der Befehl fidsk liefert Informationen über die Größe, die verwendet werden können, um zu bestätigen: 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$
```

Hinweis: Denken Sie daran, die USB-Einbindung vor der Ausführung des Befehls "dd" aufzuheben.

Bestätigen Sie, dass das USB-Gerät aus dem Beispiel eingebunden ist.

```
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
```

Um die Bereitstellung des USB-Geräts aufzuheben, verwenden Sie sudo umount /dev/sdb1.

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

Überprüfen Sie erneut, ob das Gerät nicht als "montiert" wahrgenommen wird.

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

status=progress-Option

oflag=sync- und status=progress-Optionen im Befehl dd.

Beim Schreiben mehrerer Datenblöcke liefert die Option "status=progress" Informationen über die aktuellen Schreibvorgänge. Dies ist nützlich, um zu bestätigen, ob der Befehl "dd" derzeit in den Seitencache schreibt; er kann verwendet werden, um den Fortschritt und die gesamte Zeit in Sekunden aller Schreibvorgänge anzuzeigen.

Wenn "dd" nicht verwendet wird, liefert es keine Informationen über den Fortschritt, sondern nur die Ergebnisse der Schreibvorgänge, bevor "dd" zurückgegeben wird:

```
[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]$
```

Bei Verwendung werden die Echtzeitinformationen zu den Schreibvorgängen jede Sekunde aktualisiert.

```
[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]
```

Hinweis: In der offiziellen Dokumentation für das TGA Offline-Upgrade lautet der Befehl: dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M

Nach einigen Tests wird das folgende Beispiel beobachtet.

Sobald eine Datei von 10MB mit "dd" mit dem Gerät /dev/zero erstellt wurde.

1M x 10 = 10M (10240 kB + vorherige Systemdaten in Dirty File Page Caches = 10304 kB —> dies wird im Dirty Page Cache am Ende von "dd" wahrgenommen).

```
[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

Hinweis: Nach der Rückkehr des Befehls "dd" wurde der Schreibvorgang auf das Blockgerät nicht abgeschlossen, sondern 11 Sekunden nach der Rückkehr wahrgenommen.
Wenn dies der "dd"-Befehl bei der Erstellung des bootfähigen USB mit dem TGA ISO, UND ich hatte den USB vom Endpunkt entfernt, bevor diese 11 Sekunden = ich hätte eine beschädigte ISO in der bootfähigen USB.

Erläuterung:

Blockierungsgeräte ermöglichen einen gepufferten Zugriff auf Hardwaregeräte. Dies bietet eine Abstraktionsebene für Anwendungen, wenn mit Hardwaregeräten gearbeitet wird.

Blockgeräte ermöglichen es einer Anwendung, Daten in Blöcken unterschiedlicher Größe zu lesen/schreiben. Diese Read()/Writes()-Funktion wird auf die Seitencaches (Puffer) und nicht direkt auf das Blockgerät angewendet.
Der Kernel (und nicht die Anwendung, die den Lese-/Schreibvorgang ausführt) verwaltet die Verschiebung der Daten von den Puffern (Seiten-Caches) zu den Blockgeräten.

Daher:

Die Anwendung (in diesem Fall "dd") hat keine Kontrolle über die Leerung der Puffer, wenn sie nicht angewiesen wird.

Die Option "oflag=sync" erzwingt synchrones physikalisches Schreiben (durch den Kernel), nachdem jeder Ausgabeblock (durch "dd" bereitgestellt) im Seiten-Cache platziert wurde.

oflag=sync vermindert die "dd"-Leistung im Vergleich zur Nichtverwendung der Option; wenn sie jedoch aktiviert ist, stellt sie sicher, dass nach jedem write()-Aufruf von "dd" ein physisches Schreiben auf das Blockgerät erfolgt.

Test : Mit der Option "oflag=sync" des Befehls "dd" wurden alle Schreibvorgänge mit den schmutzigen Seitencachedaten bei der Rückgabe des Befehls "dd" abgeschlossen:

```
[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]$
```

Es verbleiben keine Daten vom Schreibvorgang im Cache der unsauberen Seite.
Der Schreibvorgang wurde durchgeführt, bevor (oder zum gleichen Zeitpunkt) der Befehl "dd" zurückgegeben wurde (nicht 11 Sekunden nach dem vorherigen Test).
Jetzt bin ich sicher, dass nach dem Befehl "dd" gab es keine Daten im Dirty Page Cache in Bezug auf den Schreibvorgang = keine Probleme in der bootfähigen USB-Erstellung (wenn die ISO-Prüfsumme richtig ist).

Hinweis: Berücksichtigen Sie dieses Flag (oflag=sync) des Befehls "dd", wenn Sie mit dieser Art von Fall arbeiten.

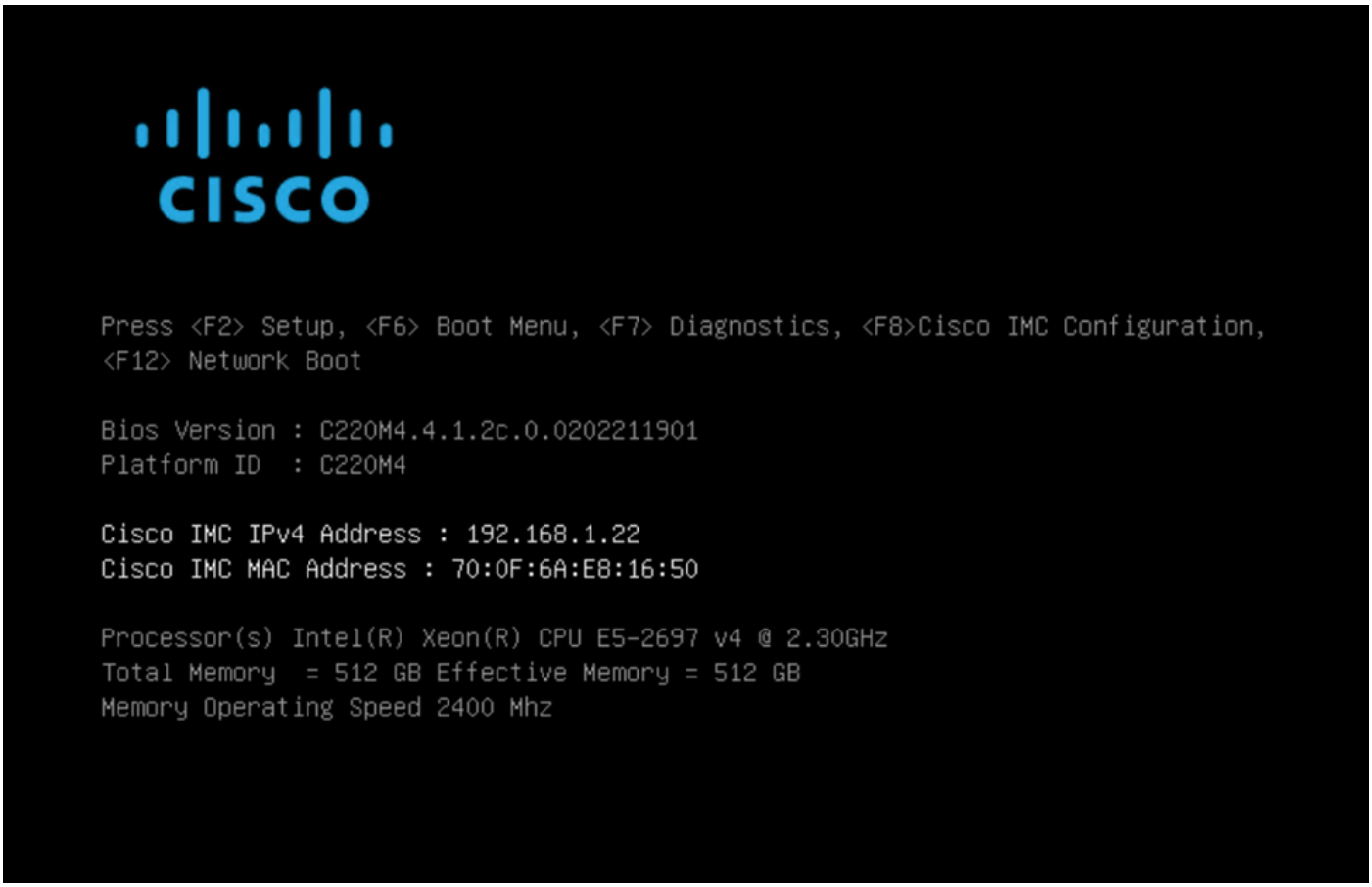
Bootreihenfolge für Festplattenlaufwerke für Offline-Upgrades

Anforderung:

Wir müssen sicherstellen, dass die HDD mit der Option "DD" formatiert wird, die jedes verfügbare Tool verwendet, und die Medien sollten anschließend auf das Laufwerk kopiert werden. Wenn wir diese Formatierung nicht verwenden, können wir diese Medien nicht lesen.

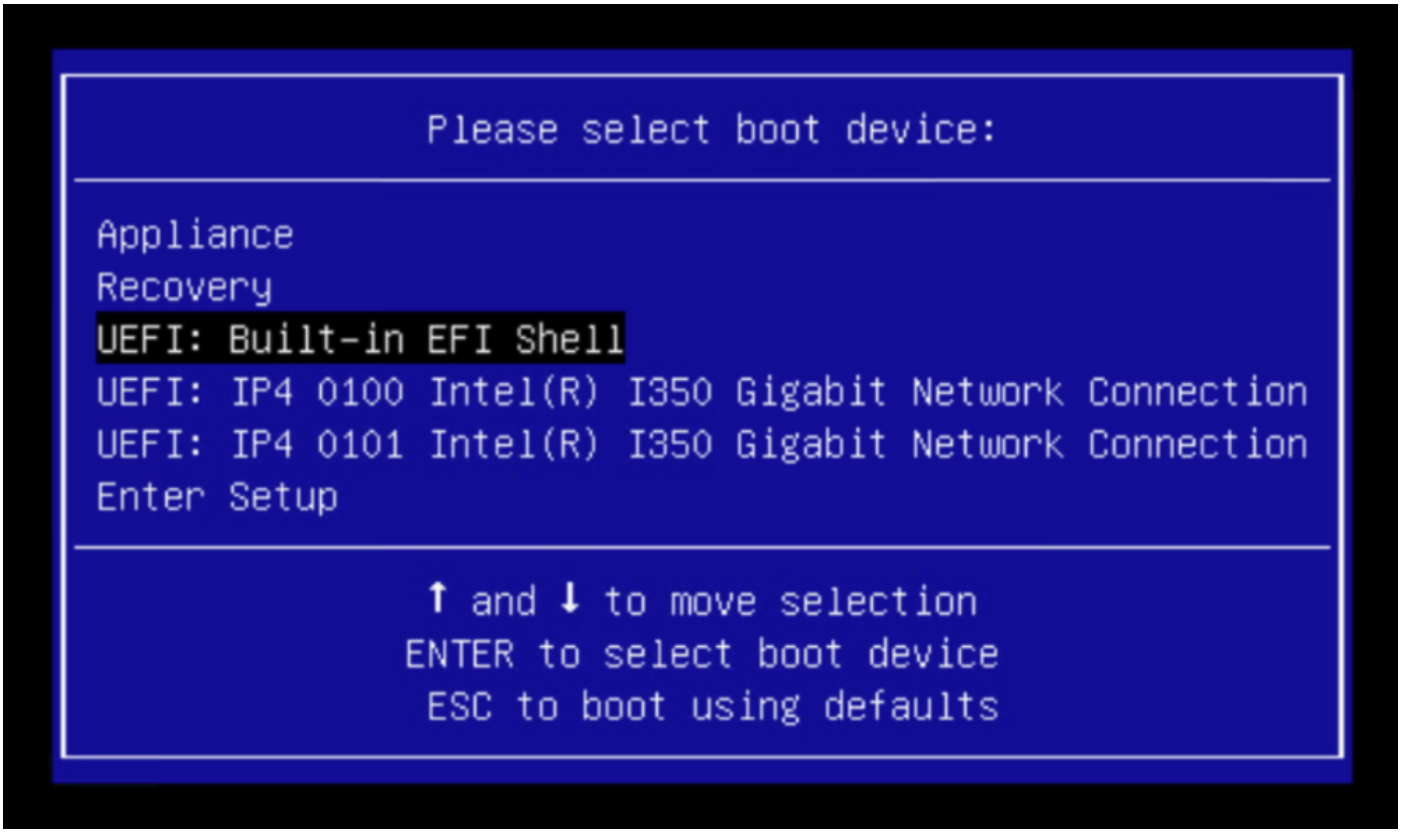
Sobald wir die Medien auf der Festplatte/USB mit der "DD"-Formatierung geladen haben, müssen wir diese an die TGA-Appliance anschließen und das Gerät neu starten.

Dies ist der Standardbildschirm zur Auswahl des Startmenüs. Wir müssen "F6" drücken, um das Gerät zu booten und das Boot-Medium auszuwählen.

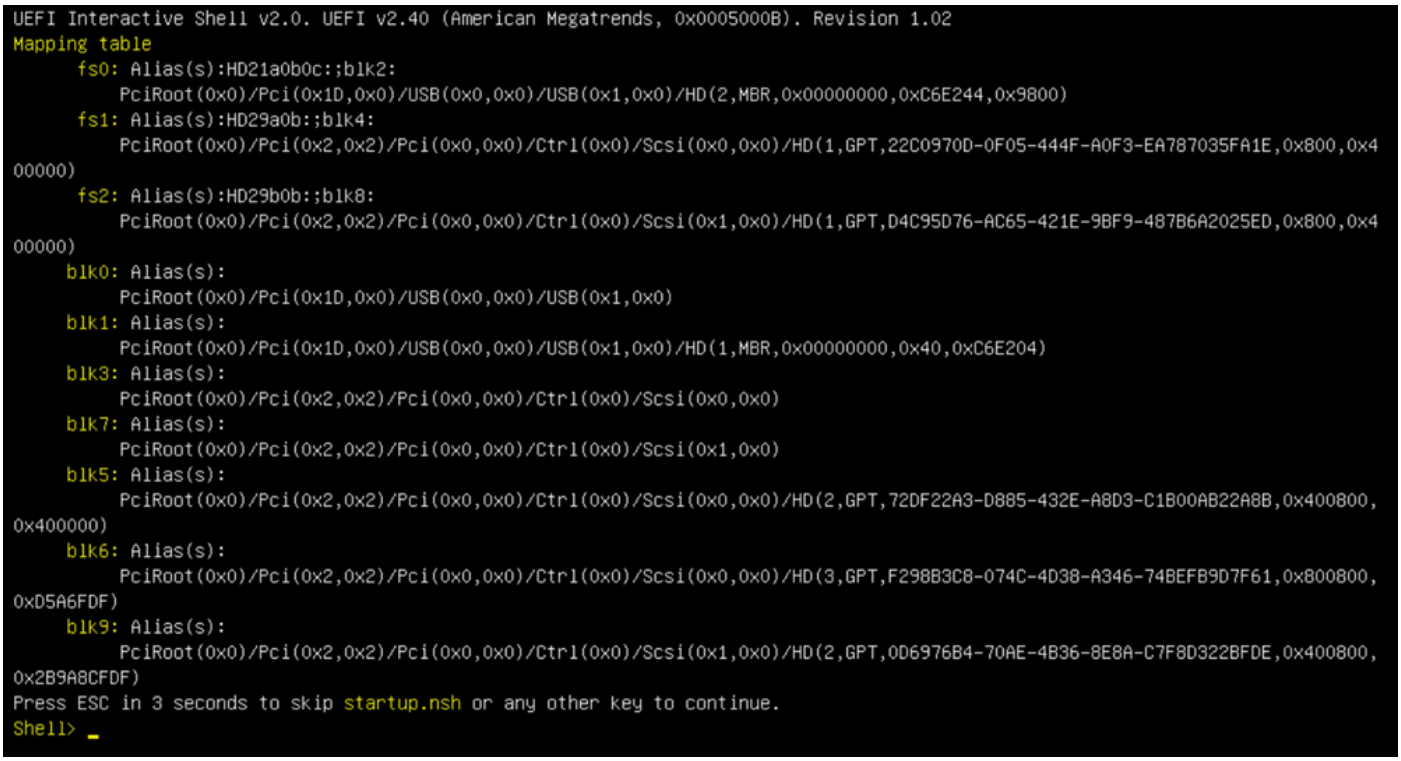


Sobald das Gerät unsere Eingabe erkennt, wird es aufgefordert, in das Boot-Auswahlmenü zu wechseln.

Dies ist die Eingabeaufforderung, die sich zwischen verschiedenen TGA-Modellen unterscheiden kann. Idealerweise würden wir die Option sehen, mit dem Boot-Medium (Upgrade-Dateisystem) aus diesem Menü selbst zu booten, aber wenn es nicht gesehen wird, müssen wir uns in der "EFI Shell" anmelden.



Sie müssten "ESC" drücken, bevor das Skript "startup.sh" beendet wird, um in die EFI-Shell zu wechseln. Einmal, melden wir uns bei der EFI Shell, würden wir feststellen, dass die Partitionen in diesem Fall erkannt werden 3 Dateisysteme: fs0:, fs1:, fs2.



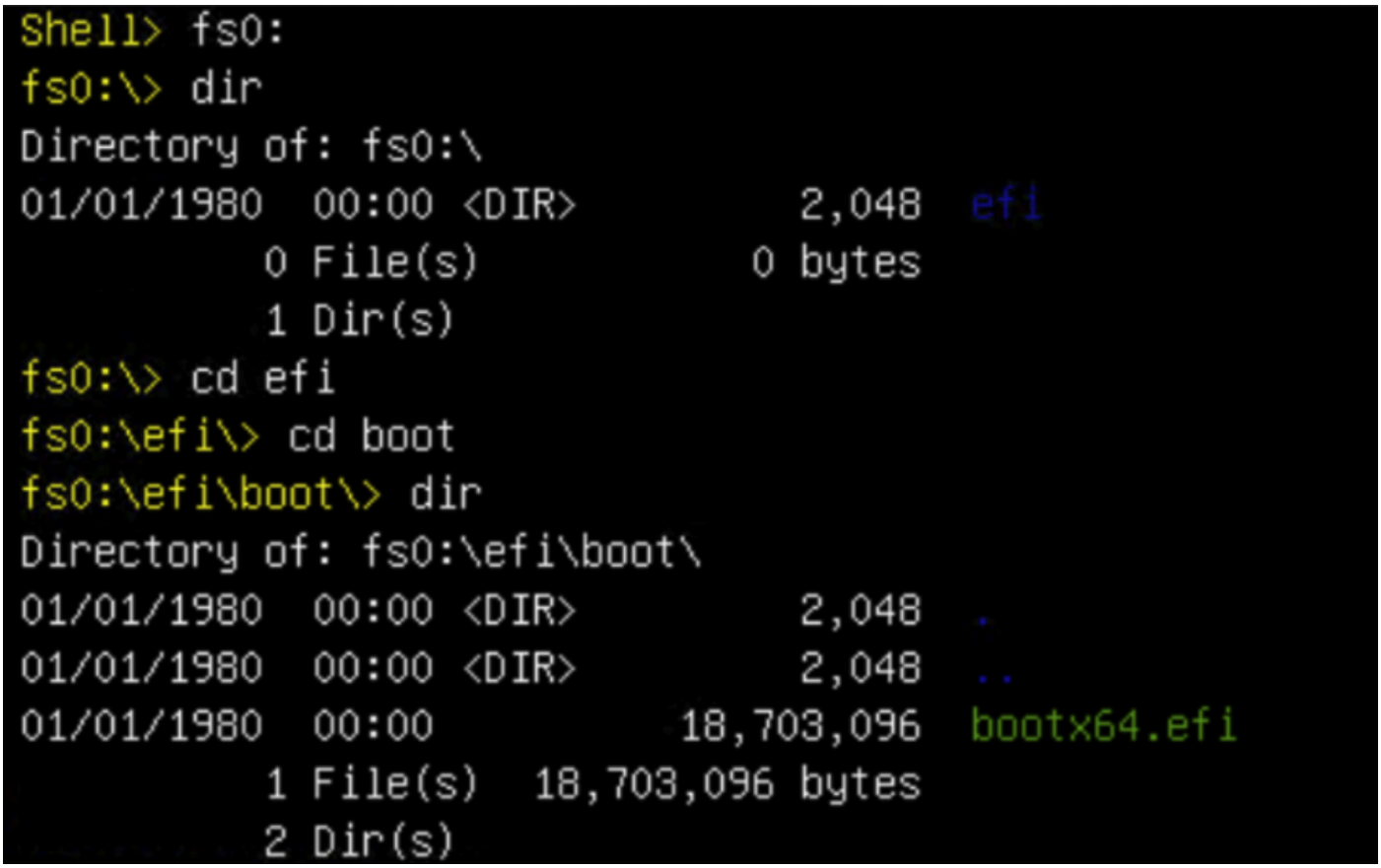
Wichtig

Identifizieren des richtigen Dateisystems:

- Wie im obigen Screenshot gezeigt, können Sie sehen, dass "fs0:" das einzige Medium ist, das "USB" in seinem Pfad hat, und daher können wir sicher sein, dass dieses Dateisystem das Boot-Medium enthalten würde (Upgrade-Dateisystem).

Bei fehlenden Dateisystemen:

- Wenn nur fs0: und fs1: verfügbar sind und fs2: nicht vorhanden ist, stellen Sie sicher, dass das Boot-Medium (Upgrade-Dateisystem) im Modus "dd" geschrieben wurde und erfolgreich verbunden ist.
- Boot-Medien (Upgrade-Dateisystem) sollten immer eine niedrigere Nummer als die Wiederherstellungsmedien haben, und sie sollten immer nebeneinander sein; es ist, ob das USB-Laufwerk am Anfang des Endes ist, das sich wahrscheinlich ändern wird (also ob es die vordere Position bei fs0: oder die hintere Position bei fs2:) müsste identifiziert werden
- In diesem Fall ist im Screenshot unten die richtige ".efi"-Datei, wie sie sich unter der "\efi\boot"-Partition befindet und die Namenskonvention "bootx64.efi" hat

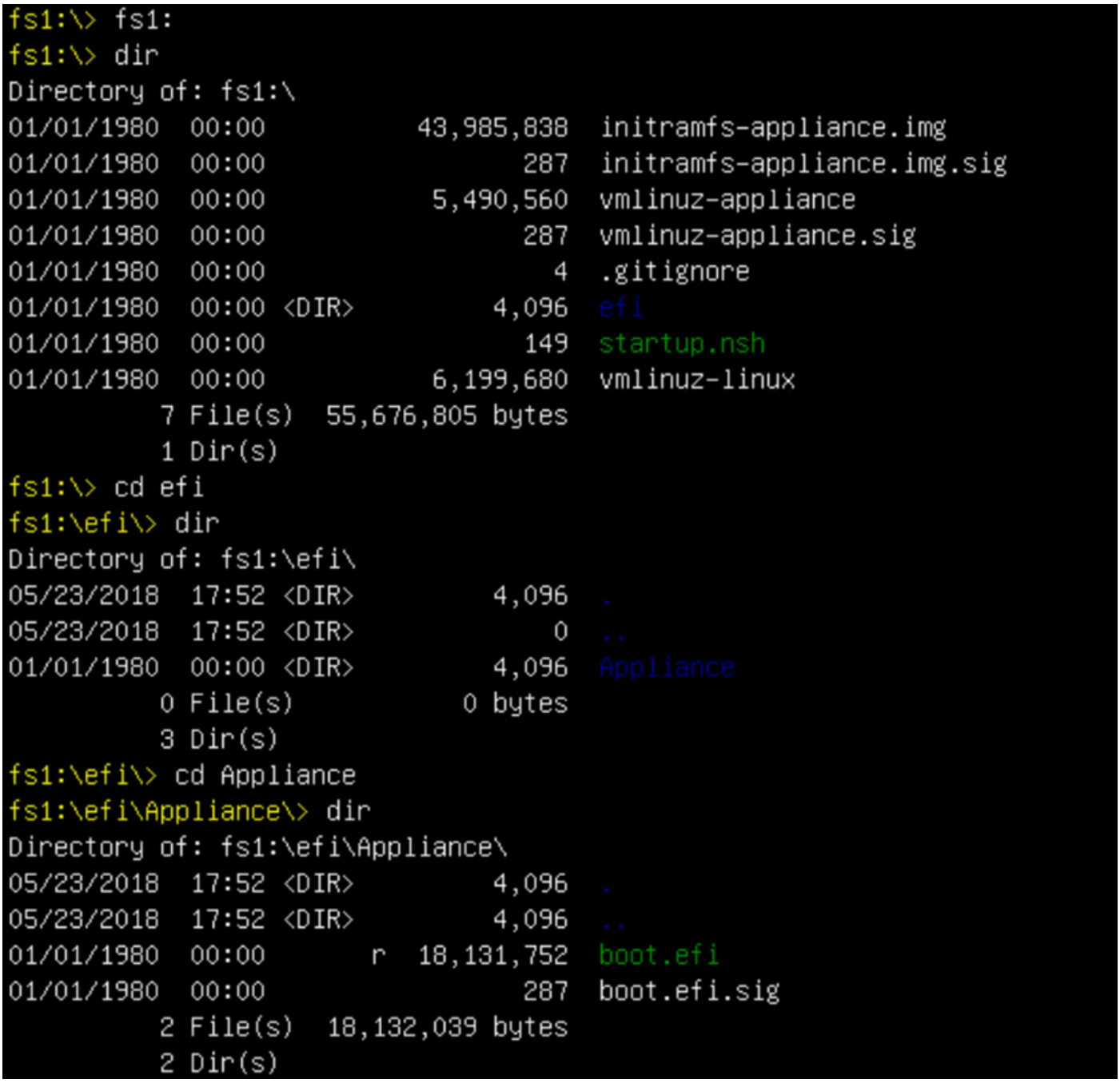


Um das Gerät im Boot-Medium (Upgrade-Dateisystem) zu booten, müssen wir die Datei "bootx64.efi" ausführen:

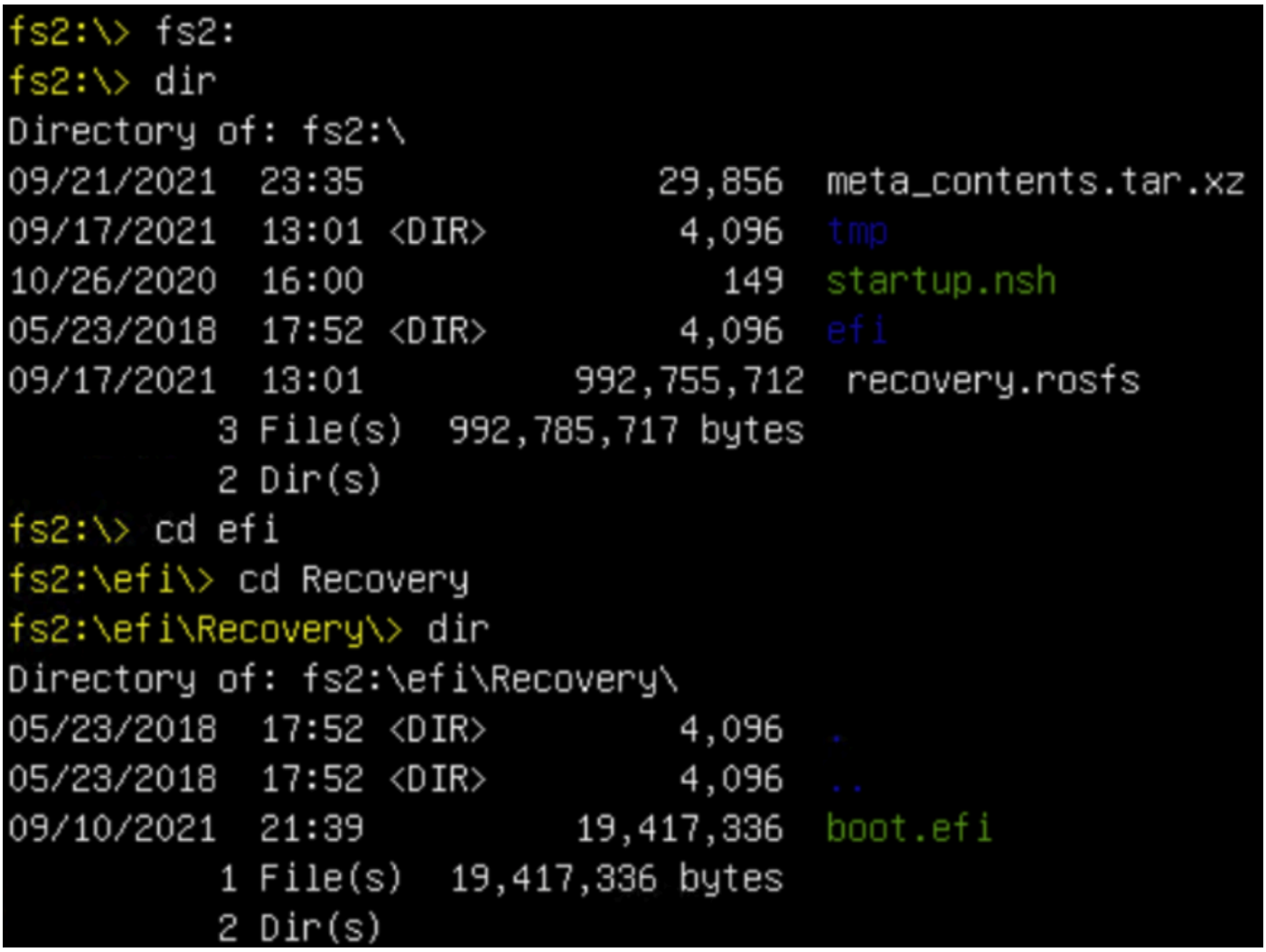
```
fs0:\efi\boot\bootx64.efi
```

Zu Ihrer Referenz haben wir die Inhalte der anderen Dateisysteme sowie unten angezeigt:

fs1: Dies ist das Haupt-Boot-Dateisystem.



fs2: Dies ist das Boot-Dateisystem des Recovery-Images.



Verschiedene Anweisungen:

Um das richtige Dateisystem zu überprüfen, das das gemountete Boot-Medium enthält. Wir können dies tun, indem wir die verschiedenen Dateisysteme durchsuchen und die ".efi"-Bootdatei überprüfen

---

Hinweis: Die Reihenfolge der eigentlichen Boot-Medien (Upgrade-Dateisystem), die in diesem Fall "fs0:" ist, kann auch mit anderen Geräten variieren.
Der Name und der Pfad können variieren, aber in allen modernen Bildern sollte dies der gleiche sein.

Checkliste, die helfen kann, das richtige Boot-Medium zu finden (Upgrade-Dateisystem):

- Wenn der Root eines Dateisystems "vmlinuz-appliance" enthält, ist dies nicht das Boot-Medium (Upgrade-Dateisystem).
- Wenn der Root eines Dateisystems "meta_contents.tar.xz" enthält, ist dies nicht das Boot-Medium (Upgrade-Dateisystem).
- Wenn ein Dateisystem nicht "efi\boot\bootx64.efi" enthält, ist es nicht das Boot-Medium (Upgrade-Dateisystem).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.