Mettre à jour le mode Air-Gap du dispositif Secure Malware Analytics

Table des matières

- Introduction
- Conditions préalables
  - Composants utilisés
- Informations générales
  - Limites
  - Exigences
  - Avant de commencer
  - Mettre à jour une appliance Secure Malware Analytics hors ligne (avec interstice)
    - Conventions de nom
    - Limites
  - Linux/MAC - Téléchargement ISO
    - Exigences
    - Composants utilisés
    - Configurer
    - Téléchargez l'ISO à l'aide de la commande Desync
  - Windows - Téléchargement ISO
    - Téléchargez l'ISO à l'aide de la commande Desync
  - Appliance de démarrage depuis USB
    - Comment trouver le périphérique /dev correct
    - status=option de progression
  - Séquence de démarrage des disques durs pour les mises à niveau hors ligne
    - Conditions requises :

Introduction

Ce guide décrit les procédures de mise à jour d'une appliance Secure Malware Analytics en mode air-gap.

Remarque : le maintien des appareils en mode air-gap peut diminuer leur efficacité. Pensez à l'arbitrage entre la sécurité et la fonctionnalité avant de continuer.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base des entrées via la ligne de commande dans les environnements Windows et Unix/Linux

- Connaissance de Malware Analytic Appliance
- Connaissance de Cisco Integrated Management Controller (IMC)

Composants utilisés

Cisco recommande de se familiariser avec les sujets suivants :

- Système d'exploitation Windows 10 et Linux (par exemple : CentOS, RedHat)
- RUFUS 2.17
- C220 M4, M510 et M520 M5, M610 et M620 M6 (modèles d'appareil)

Les informations contenues dans ce document sont basées sur des périphériques dans un environnement de travaux pratiques contrôlé avec des configurations par défaut. Si votre réseau est actif, faites preuve de prudence et comprenez parfaitement les implications potentielles de toute commande avant de continuer.

Informations générales

La plupart des appliances Secure Malware Analytics se connectent à Internet et utilisent le processus de mise à jour en ligne. Cependant, certains appareils sont maintenus strictement au sein des réseaux internes (entrefer). Cisco ne recommande pas cette approche car elle réduit l'efficacité. Ce guide décrit le processus de mise à jour hors ligne pour les personnes qui doivent entretenir des appareils à air libre.

Pour les mises à jour Secure Malware Analytics hors ligne, Cisco fournit des supports de mise à jour sur demande. Suivez le processus de mise à jour hors connexion décrit dans ce document.

Média : Le support de mise à jour Airgap (hors ligne) est fourni sur demande par le support Secure Malware Analytics. Il s'agit d'un fichier ISO qui peut être copié sur un lecteur USB ou un disque dur (avec une taille suffisante).

Taille : la taille du support de mise à jour varie en fonction des versions prises en charge et peut augmenter considérablement avec l'introduction de nouvelles machines virtuelles. Pour les versions actuelles, la taille est d'environ 30 Go, y compris l'outil de désynchronisation, qui permet des mises à jour incrémentielles pour les modifications liées aux VM.

Cycle de démarrage de mise à niveau : Chaque fois que le support de mise à jour d'airgap est amorcé, il détermine la version suivante vers laquelle effectuer la mise à niveau et copie le contenu associé à cette version suivante sur l'appliance. Une version donnée peut également lancer l'installation d'un package si cette version ne comporte aucune vérification préalable qui doit être exécutée pendant l'exécution de l'appliance. Si la version inclut de telles vérifications ou un remplacement des parties du processus de mise à jour qui pourraient ajouter de telles vérifications, alors la mise à jour ne s'applique pas réellement jusqu'à ce que l'utilisateur se connecte à OpAdmin et appelle la mise à jour avec OpAdmin > Operations > Update Appliance.

Crochets de pré-installation : Selon qu'il existe des crochets de pré-installation pour cette mise à niveau spécifique, il exécute la mise à niveau immédiatement ou redémarre l'appliance dans son

mode de fonctionnement normal pour permettre à l'utilisateur d'accéder à l'interface d'administration habituelle et de démarrer cette mise à niveau manuellement.

Répétez L'Opération Si Nécessaire : Chaque cycle d'amorçage de ce type ne met à niveau (ou ne prépare à mettre à niveau) qu'une seule étape vers la version cible finale ; l'utilisateur doit démarrer autant de fois que nécessaire pour mettre à niveau vers la version de destination souhaitée.

Limites

Le support CIMC n'est pas pris en charge pour les mises à jour à intervalle d'air.

En raison des contraintes de licence sur les composants tiers utilisés, les supports de mise à niveau pour les versions 1.x ne sont plus disponibles après la fin de vie du matériel UCS M3. Il est donc essentiel que les appliances UCS M3 soient remplacées ou mises à niveau avant la fin de vie.

Exigences

Migrations : Si les notes de version des versions couvertes incluent des scénarios dans lesquels la migration doit obligatoirement avoir lieu avant l'installation de la version suivante, l'utilisateur doit suivre ces étapes avant de redémarrer à nouveau pour éviter de mettre son appliance dans un état inutilisable.

Remarque : la première version 2.1.x plus récente que 2.1.4, en particulier, exécute plusieurs migrations de base de données. Il n'est pas sûr de continuer tant que ces migrations ne sont pas terminées. Pour plus d'informations, consultez la note de migration de Threat Grid Appliance 2.1.5.

Si la mise à niveau d'airgap débute avec une version antérieure à la version 2.1.3, elle utilise une clé de cryptage dérivée de la licence individuelle et doit donc être personnalisée par appliance. (Le seul effet visible par l'utilisateur est qu'avec les supports conçus pour prendre en charge les versions d'origine antérieures à la version 2.1.3, Secure Malware Analytics a besoin des licences installées sur ces appareils au préalable, et les supports ne fonctionneront sur aucun appareil ne figurant pas dans la liste pour laquelle ils ont été créés.)

Si vous commencez avec la version 2.1.3 ou une version ultérieure, le support airgap est générique et aucune information client n'est nécessaire.

Avant de commencer

- Sauvegarde. Vous devez envisager de sauvegarder votre appliance avant de poursuivre la mise à jour.
- Consultez les notes de version de la version à mettre à jour pour vérifier si des migrations en arrière-plan sont requises avant de planifier une mise à jour vers la version la plus récente
- Vérifiez la version actuelle de votre appliance : OpAdmin > Opérations > Mettre à jour

l'appliance
- Consultez l'historique des versions de l'appliance Secure Malware Analytics dans la table de recherche des numéros de build/versions, disponible dans tous les documents de l'appliance Threat Grid : Notes de version, Notes de migration, Guide de configuration et d'installation et Guide de l'administrateur.

Mettre à jour une appliance Secure Malware Analytics hors ligne (avec interstice)

Première vérification disponible Air Gapped version à cette page : Table de recherche des versions des appliances

1. Ouvrez une demande d'assistance TAC pour obtenir le support de mise à jour hors ligne. Cette demande doit inclure le numéro de série de l'appliance ainsi que le numéro de version de l'appliance.

2. L'assistance TAC fournit un ISO mis à jour en fonction de votre installation.

3. Gravez l'image ISO sur un USB amorçable. Notez que USB est le seul périphérique/méthode pris en charge pour les mises à jour hors connexion.

Conventions de nom

Il s'agit du nom de fichier mis à jour ex : Mise à jour Airgap TGA 2.16.2-2.17.2.

Cela signifie que ce support peut être utilisé pour une appliance exécutant une version minimale : 2.16.2 et mettre à niveau l'appliance vers la version : 2.17.2 .

Limites

- Le support CIMC n'est pas pris en charge pour les mises à jour à intervalle d'air.
- En raison des contraintes de licence sur les composants tiers utilisés, les supports de mise à niveau pour les versions 1.x ne sont plus disponibles après la fin de vie du matériel UCS M3. Il est donc essentiel que les appliances UCS M3 soient remplacées ou mises à niveau avant la fin de vie.

Linux/MAC - Téléchargement ISO

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Une machine Linux avec accès Internet pour télécharger l'ISO et créer le lecteur d'installation USB amorçable.
- Les instructions de téléchargement d'Airgap sont fournies par le support Secure Malware Analytics.
- Langage de programmation GO. Télécharger
- Le fichier d'index .caibx (inclus dans le fichier zip fourni par le support TAC).

- Outil de désynchronisation (inclus dans le fichier zip fourni par le support Secure Malware Analytics).

Composants utilisés

Les informations contenues dans ce document sont basées sur un système d'exploitation Linux (par exemple : CentOS, RedHat).

Les informations contenues dans ce document sont basées sur des périphériques dans un environnement de travaux pratiques contrôlé avec des configurations par défaut. Si votre réseau est actif, faites preuve de prudence et comprenez parfaitement les implications potentielles de toute commande avant de continuer.

Configurer

Installer le langage de programmation 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
```

Exécutez ces trois commandes après l'installation, sinon la commande desync échoue

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

Vous pouvez vérifier la version GO en procédant comme suit :

```
# go version
```

Téléchargez l'ISO à l'aide de la commande Desync

Étape 1. Copiez le contenu du fichier Zip fourni par Secure Malware Analytics Support, y compris le fichier desync.linux et .caibx dans le même répertoire localement sur la machine.

Étape 2. Accédez au répertoire dans lequel vous avez stocké les fichiers :

Exemple :

```
# cd MyDirectory/TG
```

Étape 3. Exécutez la commande pwd pour vous assurer que vous êtes à l’intérieur du répertoire.

```
# pwd
```

Étape 4. Une fois que vous êtes à l'intérieur du répertoire qui inclut la commande desync.linux et le fichier .caibx, exécutez la commande de votre choix pour commencer le processus de téléchargement.

Remarque : Voici des exemples pour différentes versions ISO, veuillez vous référer au fichier .caibx à partir des instructions fournies par le support Secure Malware Analytics.

Pour les versions 2.16.2 à 2.17.2 ISO :

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

Pour les versions 2.4.3.2 à 2.5 ISO :

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

Pour les versions 2.5 à 2.7.2ag ISO :

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

Une fois le téléchargement démarré, une barre de progression s'affiche.

Remarque : La vitesse de téléchargement et la taille du support de mise à niveau dans votre environnement peuvent avoir un impact sur le temps de composition de l'ISO.
Assurez-vous de comparer le MD5 du fichier téléchargé à celui disponible avec le bundle fourni par le support pour faire valider l'intégrité de l'ISO téléchargé.

Une fois le téléchargement terminé, les fichiers ISO sont créés dans le même répertoire.

Branchez l'USB sur la machine et exécutez la commande dd pour créer le lecteur USB amorçable.

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

Où <MY_USB> est le nom de votre clé USB (ne tenez pas compte des crochets).

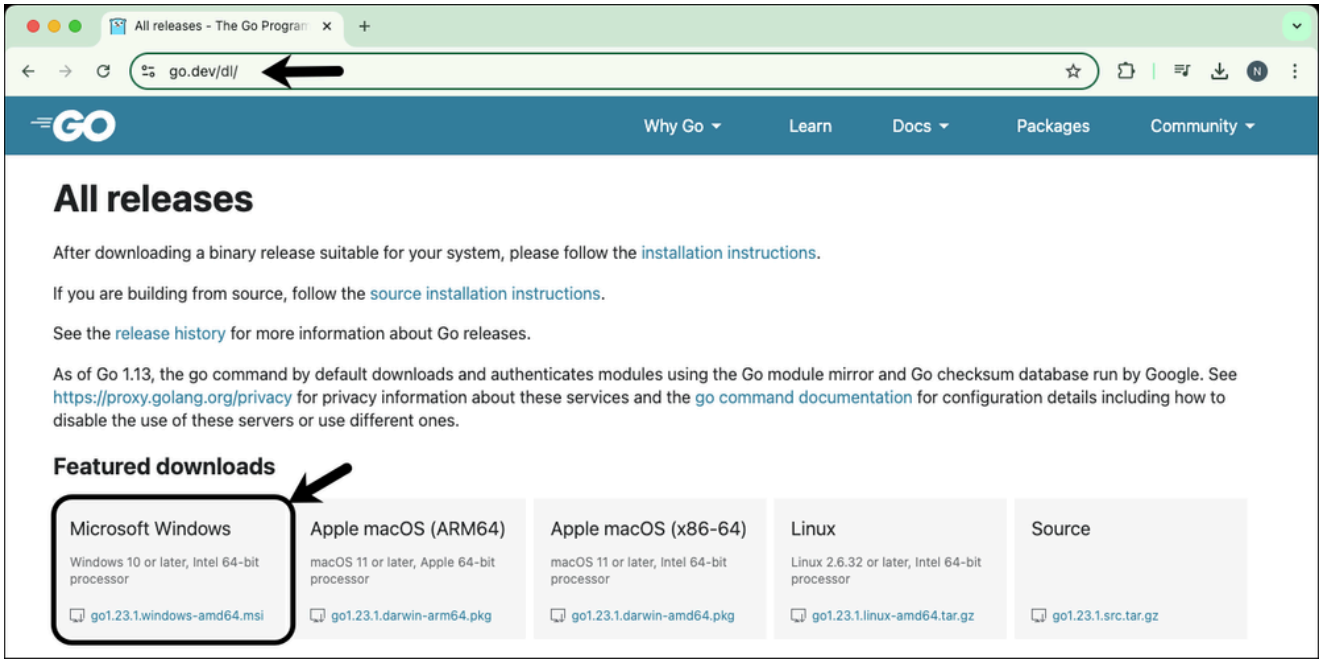
Insérez le lecteur USB et mettez sous tension ou redémarrez le périphérique. Dans l'écran de démarrage de Cisco, appuyez sur F6 pour entrer dans le menu de démarrage.

Conseil :
Exécutez le téléchargement après les heures de bureau ou les heures creuses car cela peut affecter la bande passante.
Pour arrêter l'outil, fermez le terminal ou appuyez sur Ctrl+c/Ctrl+z.
Pour continuer, exécutez la même commande pour reprendre le téléchargement.

Windows - Téléchargement ISO

Installer le langage de programmation GO

1. Téléchargez le langage de programmation GO requis. Installation à partir de https://golang.org/dl/ Dans mon cas, je sélectionne la version sélectionnée. Redémarrez votre CMD et testez avec



Fermez et rouvrez la commande CMD run pour vérifier :

```
go version
```

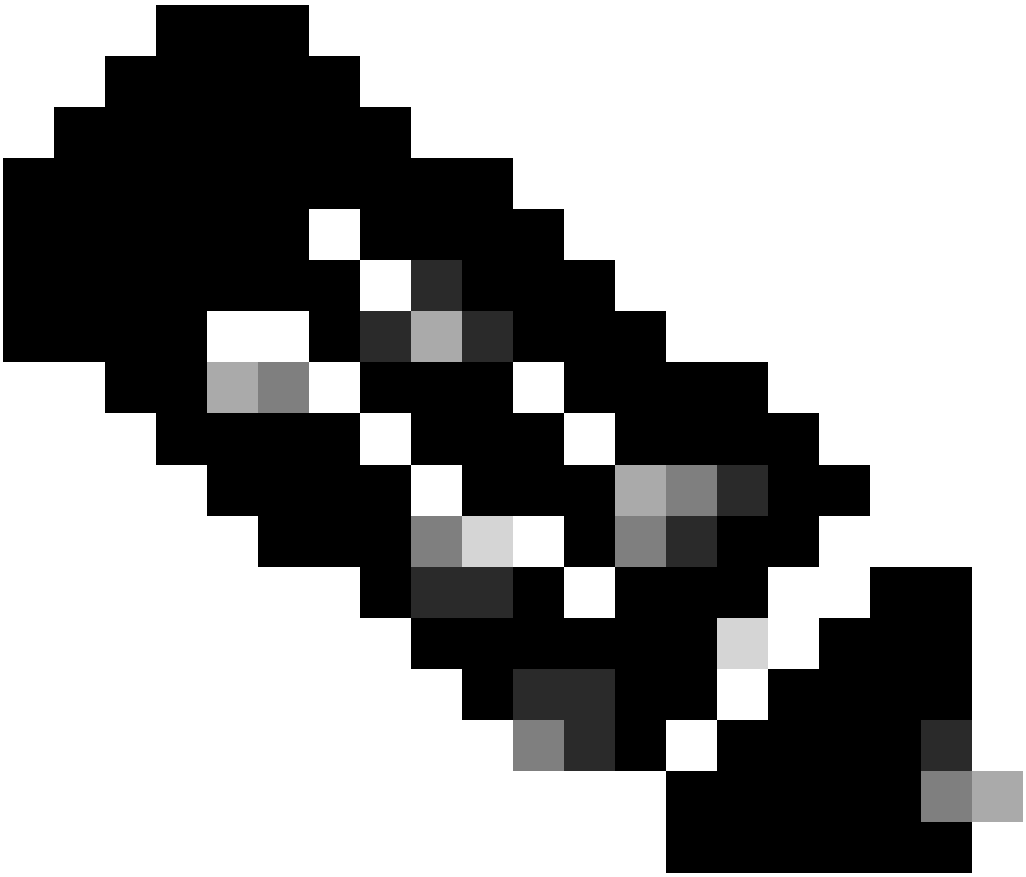
Téléchargez l'ISO à l'aide de la commande Desync

2. Installation de DESYNC outil. Après l'exécution de la commande, vous pouvez remarquer un tas d'invites de téléchargement. Environ après 2-3 minutes, le téléchargement devrait être fait.

```
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
```

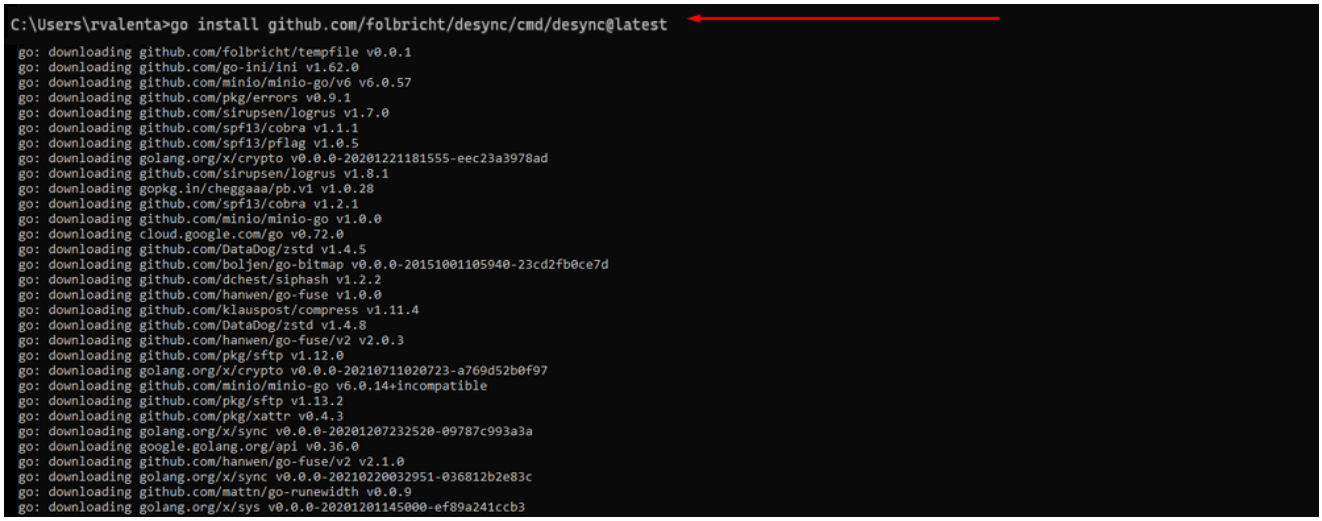


Remarque : Si la commande git ne fonctionne pas, vous pouvez télécharger et installer Git à partir d'ici : https://git-scm.com/download/win.

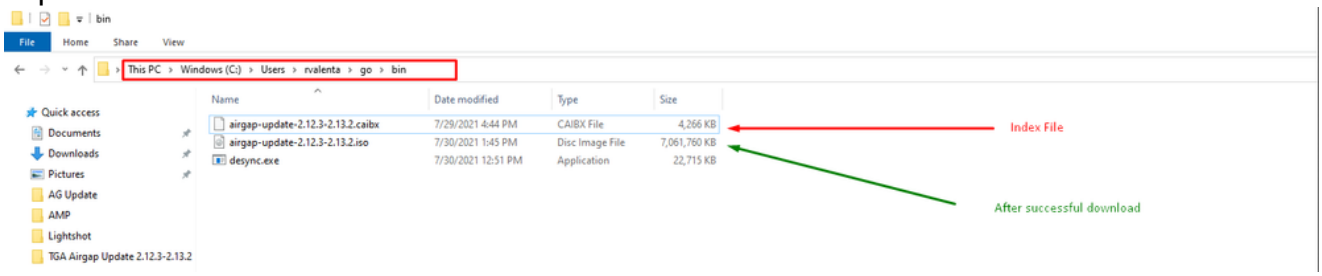
Exécutez ensuite les deux commandes ci-dessous une par une :

```
cd desync/cmd/desync

go install
```

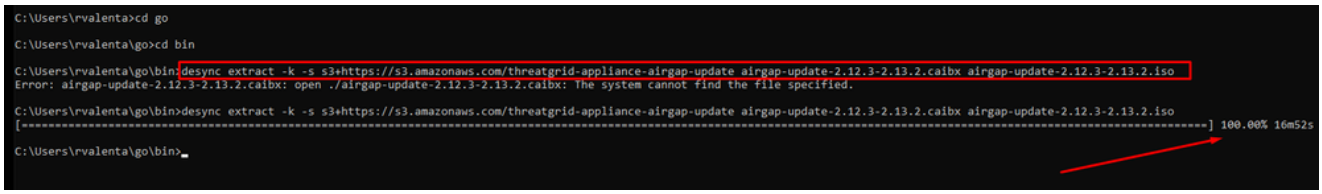


3. Naviguez jusqu'à go — > bin location. Par exemple C:\Users\<username>\go\bin et copier/coller le TAC fourni .caibx fichier index.

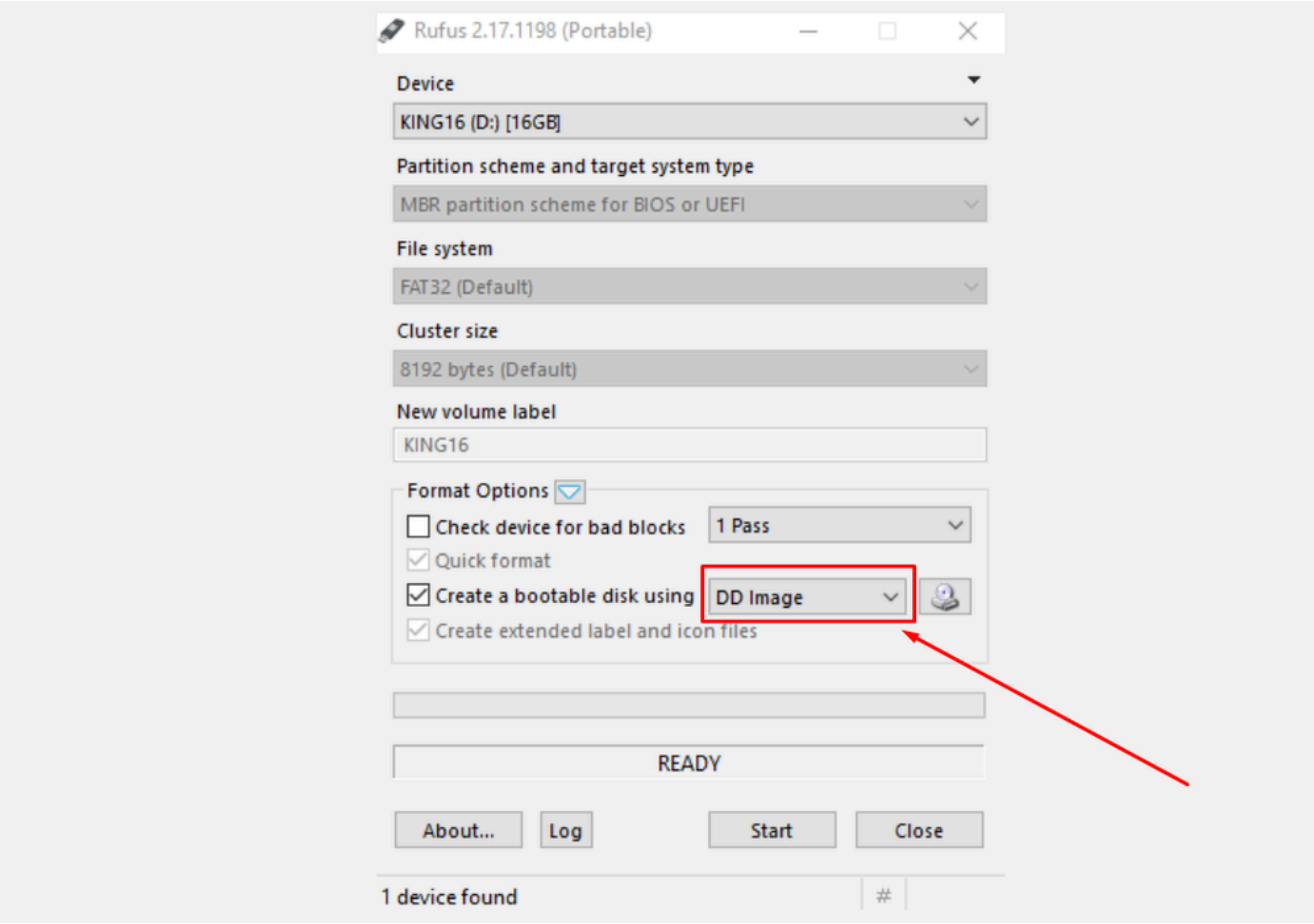


4. (Vérifiez) Retournez à l'invite CMD et accédez au dossier go\bin et exécutez les commandes de téléchargement. Vous devriez voir immédiatement le téléchargement se poursuivre. Attendez la fin du téléchargement. Le fichier .ISO entier doit maintenant se trouver au même emplacement que le fichier .caibx copié précédemment fichier index

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



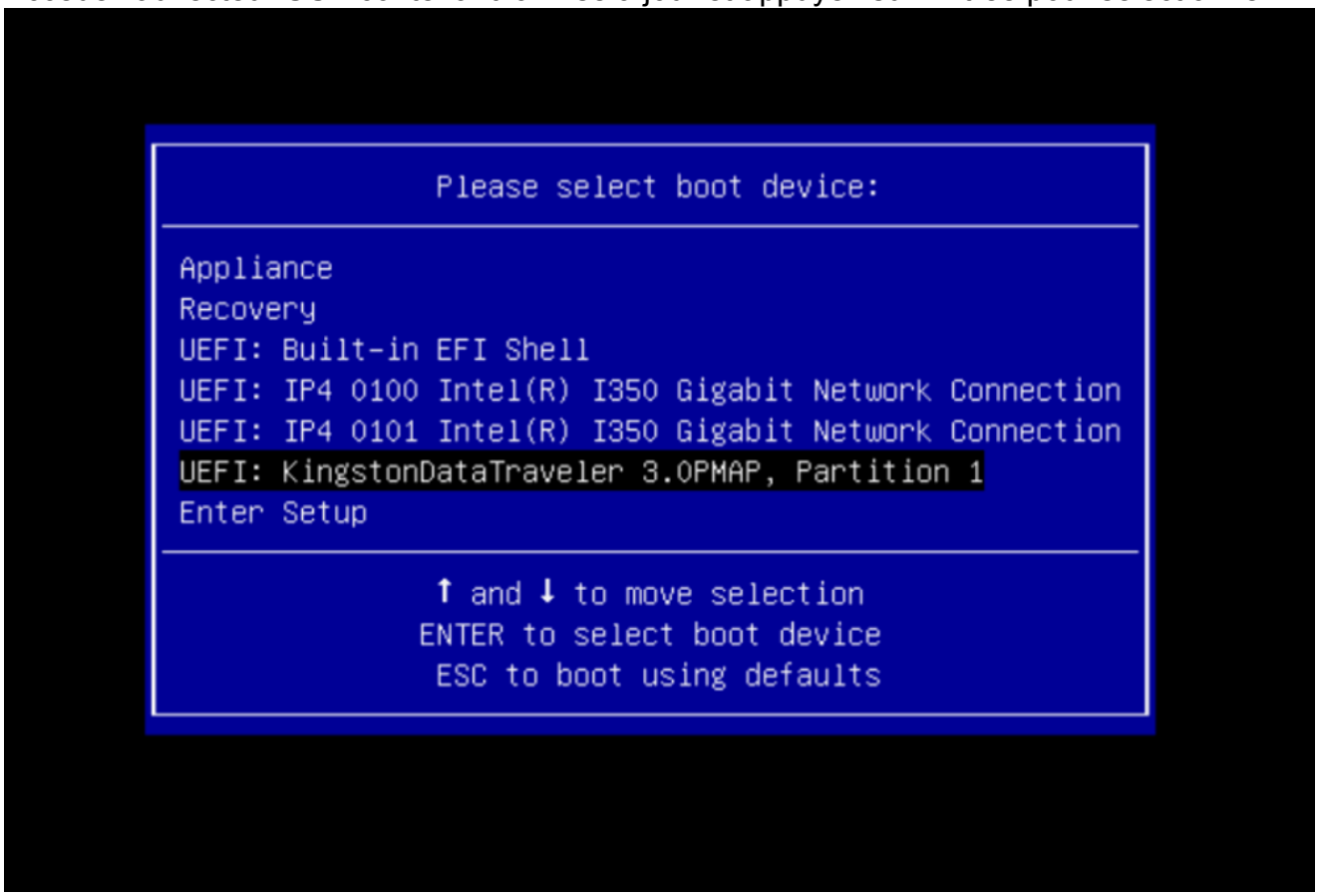
Pour créer cette récupération spécifique USB, il est crucial d'utiliser Rufus version 2.17, car il vous permet d'utiliser des options d'ajout essentielles. Vous pouvez trouver toutes les versions de RUFUS dans ce référentiel.



Appliance de démarrage depuis USB

1. Insérez l'USB, redémarrez l'appliance, et appuyez rapidement sur F6 à l'écran de démarrage de Cisco pour accéder au menu de démarrage.

2. Accédez au lecteur USB contenant la mise à jour et appuyez sur Entrée pour sélectionner.



Le support de mise à jour détermine la version suivante dans le chemin de mise à niveau et copie le contenu de cette version sur l'appliance. La solution matérielle-logicielle exécute la mise à niveau immédiatement ou redémarre en mode de fonctionnement normal pour vous permettre d'entrer dans OpAdmin et de démarrer cette mise à niveau manuellement.

Une fois le processus de démarrage ISO terminé, redémarrez l'appliance Secure Malware

Analytics en mode de fonctionnement.

Connectez-vous à l'interface utilisateur du portail et vérifiez si des avertissements indiquent que la mise à niveau est sans danger, etc., avant de continuer.

3. Accédez à l'interface OpAdmin et appliquez les mises à jour, si elles n'ont pas été appliquées automatiquement lors du redémarrage : OpAdmin > Operations > Update Appliance REMARQUE : Le processus de mise à jour inclut des redémarrages supplémentaires dans le cadre de la mise à jour, effectuée à partir du support USB. Par exemple, il est nécessaire d'utiliser le bouton Redémarrer de la page d'installation après l'installation des mises à jour.
   Répétez l'opération pour chaque version sur le périphérique USB.

Comment trouver le périphérique /dev correct

L'USB n'étant toujours pas connecté au terminal, exécutez la commande « lsblk | grep -iE 'disque|partie'.

```
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$
```

Une fois la clé USB branchée.

```
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$
```

Ceci confirme que le périphérique USB dans /dev est "/dev/sdb".

Autres moyens de confirmer, après la connexion de la clé USB :

La commande dmesg fournit des informations. Une fois l'USB connecté, exécutez la commande dmesg | 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$
```

La commande fidsk fournit des informations sur la taille, qui peuvent être utilisées pour confirmer : 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$
```

✎ Remarque : N'oubliez pas de démonter l'USB avant d'exécuter la commande « dd ».

Confirmez que le périphérique USB de l'exemple est monté.

```
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
```

Pour démonter le périphérique USB, utilisez sudo umount /dev/sdb1.

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

Vérifiez à nouveau que le périphérique n'est pas considéré comme « monté ».

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

status=option de progression

oflag=sync et status=progress dans la commande dd.

Lors de l'écriture de nombreux blocs de données, l'option "status=progress" fournit des informations sur les opérations d'écriture en cours. Ceci est utile pour confirmer si la commande "dd" est en train d'écrire dans le cache de page ; il peut être utilisé pour afficher la progression et la durée totale en secondes de toutes les opérations d'écriture.

Lorsqu'il n'est pas utilisé, "dd" ne fournit pas d'informations sur la progression, seuls les résultats des opérations d'écriture sont fournis avant que "dd" ne retourne :

```
[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]$
```

Lorsqu'elles sont utilisées, les informations en temps réel sur les opérations d'écriture sont mises à jour toutes les secondes.

```
[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]
```

✎ Remarque : Dans la documentation officielle du processus de mise à niveau hors ligne de la

---

TGA, la commande qui est indiquée est : dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M

Après quelques tests, on observe l'exemple suivant.

Une fois qu'un fichier de 10 Mo est créé avec "dd" en utilisant le périphérique /dev/zero.

1M x 10 = 10M (10240 kB + données système précédentes dans les caches de pages de fichiers sales = 10304 kB —> c'est ce qui est perçu dans le cache de pages sales à la fin de "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
```

Remarque : Après le retour de la commande « dd », l'opération d'écriture sur le périphérique de bloc n'était pas terminée, elle était perçue 11 secondes après le retour.
Si c'était la commande "dd" lors de la création de l'USB amorçable avec le TGA ISO, ET j'avais retiré l'USB du point d'extrémité avant ces 11 secondes = J'aurais un ISO corrompu dans l'USB amorçable.

Explication:

Les périphériques de type bloc fournissent un accès en mémoire tampon aux périphériques matériels. Cela fournit une couche d'abstraction aux applications lors de l'utilisation de périphériques matériels.

Les périphériques de bloc permettent à une application de lire/écrire des blocs de données de différentes tailles ; cette fonction read()/write() est appliquée sur les caches de page (tampons) et non directement sur le périphérique de bloc.
Le noyau (et non l'application effectuant la lecture/écriture) gère le mouvement des données des tampons (caches de pages) vers les unités de bloc.

Par conséquent :

L'application (en l'occurrence "dd") n'a pas le contrôle du vidage des tampons si elle n'est pas chargée de le faire.

L'option "oflag=sync" force l'écriture physique synchrone (par le noyau) après que chaque bloc de sortie (fourni par "dd") est placé dans le cache de page.
oflag=sync dégrade la performance "dd" par rapport à la non utilisation de l'option ; mais, si elle est activée, elle assure une écriture physique sur le périphérique bloc après chaque appel write() de "dd".

Test : L'utilisation de l'option "oflag=sync" de la commande "dd" pour confirmer toutes les opérations d'écriture avec les données du cache de pages modifiées a été effectuée au retour de la commande "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]$
```

Il ne reste aucune donnée de l'opération d'écriture dans le cache des pages modifiées.
L'opération d'écriture a été appliquée avant (ou au même instant) le retour de la commande "dd" (pas 11 secondes après comme le test précédent).
Maintenant, je suis sûr qu'après le retour de la commande "dd" il n'y avait aucune donnée dans le cache de la page sale liée à l'opération d'écriture = aucun problème dans la création USB amorçable (si la somme de contrôle ISO est correcte).

✎ Remarque : Tenez compte de cet indicateur (oflag=sync) de la commande "dd" lorsque vous

---

travaillez sur ce type de cas.

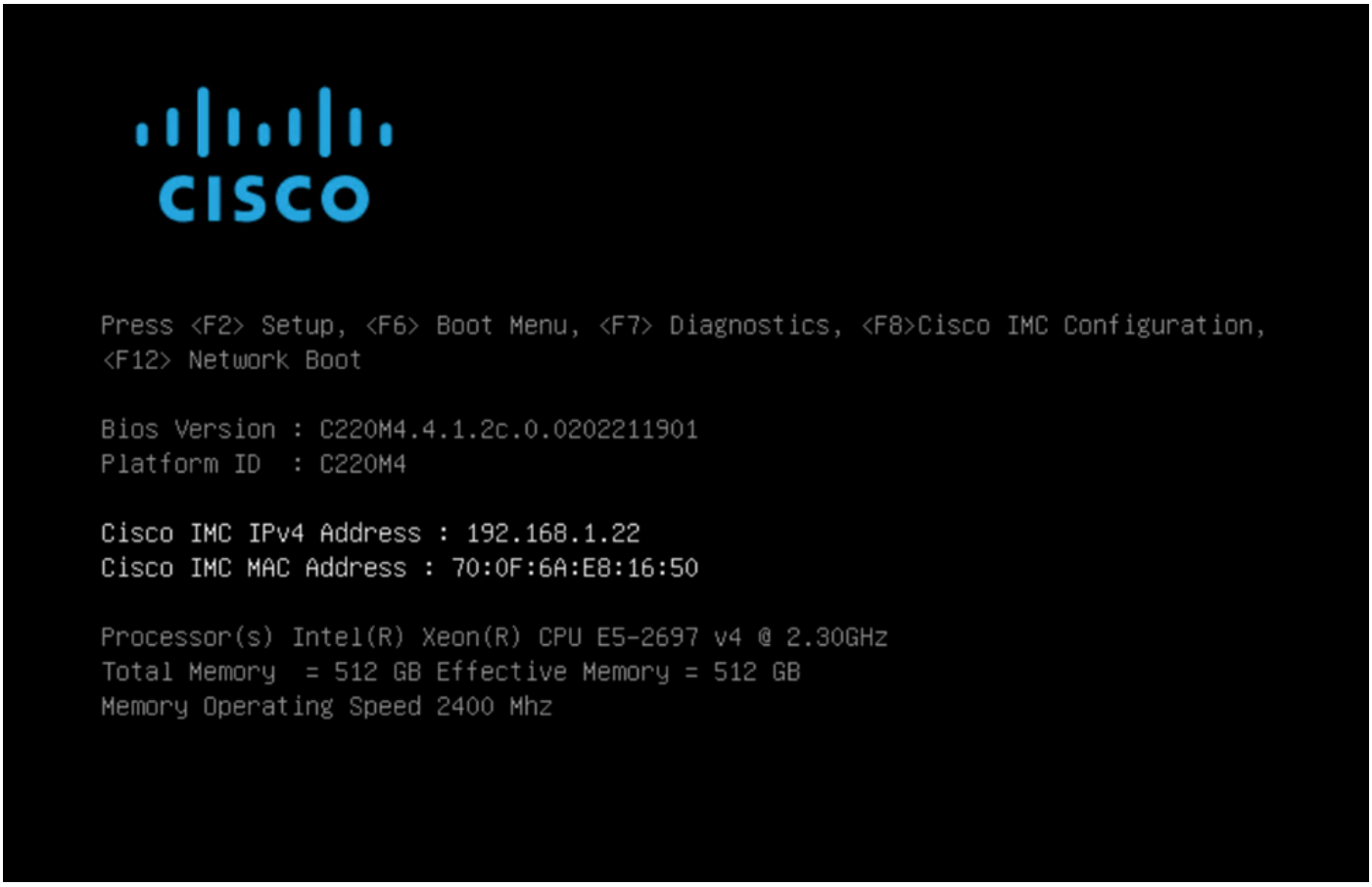
Séquence de démarrage des disques durs pour les mises à niveau hors ligne

Conditions requises :

Nous devons nous assurer que le disque dur est formaté à l'aide de l'option « DD » à l'aide de n'importe quel outil disponible et que le support doit être copié par la suite sur le lecteur. Si nous n'utilisons pas cette mise en forme, nous ne pourrons pas lire ce média.

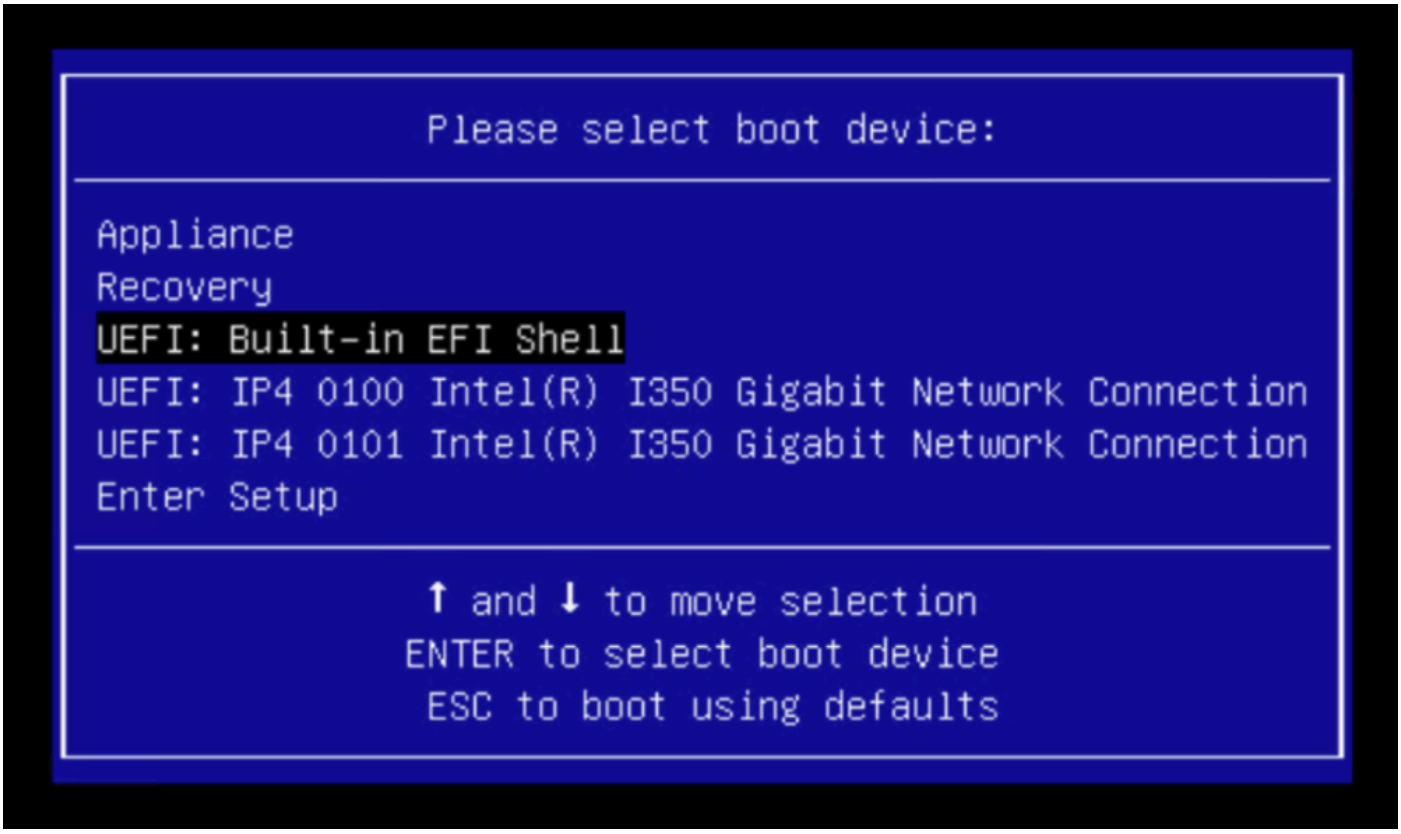
Une fois que le support est chargé sur le disque dur/l'unité USB à l'aide du formatage « DD », nous devons le connecter à l'appliance TGA et redémarrer le périphérique.

Il s'agit de l'écran de sélection du menu de démarrage par défaut. Nous devons appuyer sur « F6 » pour démarrer le périphérique et sélectionner le média de démarrage



Une fois que le périphérique reconnaît notre entrée, il vous invite à entrer dans le menu de sélection du démarrage.

Il s'agit de l'invite qui peut différer entre les différents modèles TGA. Idéalement, nous verrions l'option de démarrage à l'aide du média de démarrage (upgrade filesystem) à partir de ce menu lui-même, mais s'il n'est pas vu, nous devons nous connecter au « shell EFI ».



Vous devez appuyer sur « ESC » avant que le script « startup.sh » ne se termine pour accéder à l'environnement de ligne de commande EFI. Une fois que nous nous connectons au shell EFI, nous remarquons que les partitions détectées dans ce cas sont 3 systèmes de fichiers : 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> _
```

Important

Identification du système de fichiers approprié :

- Comme dans la capture d'écran ci-dessus, vous pourriez voir que «fs0:» est le seul média avec «USB» dans leur chemin et donc nous pouvons être sûrs que ce système de fichiers contiendrait le média de démarrage (upgrade filesystem).

En cas de systèmes de fichiers manquants :

- Si seulement fs0 : et fs1 : sont disponibles et il n'y a pas de fs2 :, vérifiez que le média de démarrage (système de fichiers de mise à niveau) a été écrit en mode dd et est correctement connecté.
- Le support d'amorçage (système de fichiers de mise à niveau) doit toujours avoir un numéro inférieur à celui du support de récupération et être toujours à côté l'un de l'autre ; c'est si le lecteur USB est au début de la fin qui est susceptible de changer (donc, s'il prend la position avant à fs0 : ou la position arrière à fs2 :) doit être identifiée
- Dans le cas présent, dans la capture d'écran ci-dessous, il s'agit du fichier « .efi » correct, tel qu'il se trouve sous la partition « \efi\boot » et la convention de nom est « 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)
```

Afin de démarrer le périphérique dans le support de démarrage (système de fichiers de mise à niveau), nous devons exécuter le fichier « bootx64.efi » :

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

Pour référence, nous avons affiché le contenu des autres systèmes de fichiers ainsi que ci-dessous :

fs1 : Il s'agit du système de fichiers de démarrage principal.

```
fs1:\> fs1:
fs1:\> dir
Directory of: fs1:\
01/01/1980  00:00          43,985,838  initramfs-appliance.img
01/01/1980  00:00                 287  initramfs-appliance.img.sig
01/01/1980  00:00           5,490,560  vmlinuz-appliance
01/01/1980  00:00                 287  vmlinuz-appliance.sig
01/01/1980  00:00                   4  .gitignore
01/01/1980  00:00 <DIR>         4,096  efi
01/01/1980  00:00                 149  startup.nsh
01/01/1980  00:00           6,199,680  vmlinuz-linux
          7 File(s)  55,676,805 bytes
          1 Dir(s)
fs1:\> cd efi
fs1:\efi\> dir
Directory of: fs1:\efi\
05/23/2018  17:52 <DIR>         4,096  .
05/23/2018  17:52 <DIR>             0  ..
01/01/1980  00:00 <DIR>         4,096  Appliance
          0 File(s)           0 bytes
          3 Dir(s)
fs1:\efi\> cd Appliance
fs1:\efi\Appliance\> dir
Directory of: fs1:\efi\Appliance\
05/23/2018  17:52 <DIR>         4,096  .
05/23/2018  17:52 <DIR>         4,096  ..
01/01/1980  00:00       r  18,131,752  boot.efi
01/01/1980  00:00                 287  boot.efi.sig
          2 File(s)  18,132,039 bytes
          2 Dir(s)
```

fs2 : Il s'agit du système de fichiers de démarrage de l'image de récupération.

```
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)
```

Instructions diverses :

Pour vérifier le système de fichiers correct qui contient le support de démarrage monté. Nous pouvons le faire en parcourant les différents systèmes de fichiers et en vérifiant le fichier de démarrage « .efi »

✎ Remarque : La séquence du support de démarrage réel (système de fichiers de mise à niveau), dans ce cas « fs0: », peut également varier avec d'autres périphériques.
Le nom et le chemin peuvent varier, mais dans toutes les images modernes, cela devrait être le même.

Liste de contrôle permettant de localiser le support de démarrage approprié (système de fichiers de mise à niveau) :

- Si la racine d'un système de fichiers contient « vmlinuz-appliance », ce n'est pas le média de démarrage (upgrade filesystem).
- Si la racine d'un système de fichiers contient «meta_contents.tar.xz», ce n'est pas le média de démarrage (upgrade filesystem).
- Si un système de fichiers ne contient pas « efi\boot\bootx64.efi », il ne s'agit pas du support de démarrage (système de fichiers de mise à niveau).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.