Atualizar Modo de Intervalo de Ar do Secure Malware Analytics Appliance

Contents

Introdução

Este guia descreve os procedimentos para atualizar um Secure Malware Analytics Appliance no modo air-gap.

Nota:A manutenção dos dispositivos no modo de isolamento de ar pode diminuir sua eficácia. Considere a compensação entre segurança e funcionalidade antes de continuar.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico das entradas através da linha de comando no ambiente Windows e Unix/Linux

- Conhecimento do Malware Analytic Appliance
- Conhecimento do Cisco Integrated Management Controller (IMC)

Componentes Utilizados

A Cisco recomenda familiaridade com os seguintes tópicos:

- SO baseado em Windows 10 e Linux (por exemplo: CentOS, RedHat)
- RUFUS 2,17
- C220 M4, M510 e M520 M5, M610 e M620 M6 (modelos de dispositivo)

As informações neste documento são baseadas em dispositivos em um ambiente de laboratório controlado com configurações padrão. Se sua rede estiver ativa, tenha cuidado e compreenda completamente as possíveis implicações de qualquer comando antes de continuar.

Informações de Apoio

A maioria dos dispositivos Secure Malware Analytics se conecta à Internet e usa o processo de atualização on-line. No entanto, alguns dispositivos são mantidos estritamente dentro de redes internas (com isolamento de ar). A Cisco não recomenda essa abordagem, pois ela reduz a eficácia. Este guia fornece o processo de atualização off-line para aqueles que precisam manter dispositivos com isolamento de ar.

Para atualizações offline do Secure Malware Analytics, a Cisco fornece mídia de atualização mediante solicitação. Siga o processo de atualização offline descrito neste documento.

Mídia: A mídia de atualização do Airgap (off-line) é fornecida pelo Secure Malware Analytics Support mediante solicitação. É um arquivo ISO que pode ser copiado para uma unidade USB ou HDD (com tamanho suficiente).

Tamanho:O tamanho da mídia de atualização varia de acordo com as versões suportadas e pode aumentar significativamente com a introdução de novas máquinas virtuais. Para versões atuais, o tamanho é de aproximadamente 30 GB, incluindo a ferramenta de dessincronização, que permite atualizações incrementais para alterações relacionadas à VM.

Ciclo de inicialização de atualização: cada vez que a mídia de atualização do airgap é inicializada, ela determina a próxima versão para a qual atualizar e copia o conteúdo associado à próxima versão para o equipamento. Uma determinada versão também pode iniciar a instalação de um pacote se essa versão não tiver nenhuma verificação de pré-requisito que deva ser executada enquanto o equipamento estiver em execução. Se a versão incluir tais verificações ou uma substituição para partes do processo de atualização que poderiam adicionar tais verificações, a atualização não será realmente aplicada até que o usuário faça login no OpAdmin e chame a atualização com OpAdmin > Operações > Atualizar aplicativo.

Ganchos de pré-instalação: dependendo da presença de algum gancho de pré-instalação para essa atualização específica, ele executa a atualização imediatamente ou reinicializa o equipamento de volta em seu modo de operação normal para permitir que o usuário entre na

interface administrativa normal e inicie a atualização manualmente.

Repetir Conforme Necessário: Cada ciclo de inicialização de mídia faz o upgrade (ou se prepara para o upgrade) de apenas uma etapa em direção à release de destino final; o usuário deve inicializar quantas vezes forem necessárias para fazer o upgrade para a release de destino desejada.

Limitações

A mídia do CIMC não é suportada para atualizações air-gapped.

Devido a restrições de licenciamento em componentes de terceiros usados, a mídia de atualização para versões 1.x não estará mais disponível depois que o hardware do UCS M3 atingir o EOL (fim da vida útil). Portanto, é essencial que os dispositivos UCS M3 sejam substituídos ou atualizados antes do EOL.

Requisitos

Migrações: se as notas de versão das versões abordadas incluírem cenários em que a migração é obrigatória para ocorrer antes da próxima versão ser instalada, o usuário deverá seguir estas etapas antes de reinicializar novamente para evitar colocar o dispositivo em um estado inutilizável.

Nota:A primeira versão 2.1.x mais recente que a 2.1.4, em particular, executa várias migrações de banco de dados. Não é seguro continuar até que essas migrações sejam concluídas. Para obter mais informações, consulte a Nota de migração do Threat Grid Appliance 2.1.5.

Se estiver começando em uma versão anterior à 2.1.3, a mídia de atualização do airgap usará uma chave de criptografia derivada da licença individual e, portanto, precisará ser personalizada para cada dispositivo. (O único efeito visível ao usuário é que com a mídia criada para suportar versões de origem anteriores à 2.1.3, o Secure Malware Analytics precisa das licenças instaladas nesses dispositivos com antecedência, e a mídia não funcionará em nenhum dispositivo que não esteja na lista para a qual foi criado.)

Se começar com a versão 2.1.3 ou posterior, a mídia de airgap é genérica e as informações do cliente não são necessárias.

Antes de Começar

- Fazer backup. Você deve considerar o backup do equipamento antes de continuar com a atualização.
- Revise as Notas de versão da versão a ser atualizada para verificar se há alguma migração de segundo plano necessária antes de planejar a atualização para a versão mais recente
- Verifique a versão atual do seu equipamento: OpAdmin > Operações > Atualizar equipamento

- Revise o histórico de versão do dispositivo Secure Malware Analytics na Tabela de Pesquisa de Número de Compilação/Versão, que está disponível em todos os documentos do dispositivo Threat Grid: Notas de Versão, Notas de Migração, Guia de Configuração e Configuração e Guia do Administrador.

Atualize um dispositivo seguro de análise de malware off-line (sem interrupção)

Primeira verificação disponível versão Air Gapped nesta página: Tabela de pesquisa da versão do dispositivo

1. Abra uma Solicitação de Suporte do TAC para obter a Mídia de Atualização Offline. Essa solicitação deve incluir o número de série do equipamento, bem como o número de compilação do equipamento.

2. Suporte do TAC forneça um ISO atualizado com base na sua instalação.

3. Grave a imagem ISO em um USB inicializável. Observe que USB é o único dispositivo/método suportado para atualizações offline.

Convenções de nomeação

Este é o nome de arquivo atualizado ex: TGA Airgap Update 2.16.2-2.17.2.

Isso significa que essa mídia pode ser usada para um dispositivo que executa uma versão mínima: 2.16.2 e atualiza o dispositivo para a versão: 2.17.2.

Limitações

- A mídia do CIMC não é suportada para atualizações air-gapped.
- Devido a restrições de licenciamento em componentes de terceiros usados, a mídia de atualização para versões 1.x não estará mais disponível depois que o hardware do UCS M3 atingir o EOL (fim da vida útil). Portanto, é essencial que os dispositivos UCS M3 sejam substituídos ou atualizados antes do EOL.

Linux/MAC - Download do ISO

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Uma máquina Linux com acesso à Internet para baixar o ISO e criar a unidade de instalação USB inicializável.
- As Instruções para download do Airgap são fornecidas pelo Secure Malware Analytics Support.
- IR Linguagem de programação. Download
- O arquivo de índice .caibx (incluído no arquivo zip fornecido pelo suporte do TAC).
- Desync Tool (incluída no arquivo zip fornecido pelo Secure Malware Analytics Support).

Componentes Utilizados

As informações neste documento são baseadas em um sistema operacional baseado em Linux (por exemplo: CentOS, RedHat).

As informações neste documento são baseadas em dispositivos em um ambiente de laboratório controlado com configurações padrão. Se sua rede estiver ativa, tenha cuidado e compreenda completamente as possíveis implicações de qualquer comando antes de continuar.

Configurar

Instalar a linguagem de programação 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
```

Execute esses três comandos após a instalação, caso contrário, o comando desync falhará

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

Você pode verificar a versão GO por:

```
# go version
```

Faça o download do ISO usando o comando Desync

Etapa 1. Copie o conteúdo do arquivo Zip fornecido pelo Secure Malware Analytics Support, incluindo os arquivos desync.linux e .caibx, no mesmo diretório local na máquina.

Etapa 2. Altere para o diretório no qual você armazenou os arquivos:

Exemplo:

```
# cd MyDirectory/TG
```

Etapa 3. Execute o comando pwd para garantir que você esteja dentro do diretório.

```
# pwd
```

Etapa 4. Quando estiver dentro do diretório que inclui o comando desync.linux e o arquivo .caibx , execute o comando de sua escolha para iniciar o processo de download.

Observação: estes são os exemplos de diferentes versões do ISO. Consulte o arquivo .caibx a partir das instruções fornecidas pelo Secure Malware Analytics Support.

Para as versões 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
```

Para as versões 2.4.3.2 a 2.5 ISO:

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

Para a versão 2.5 a 2.7.2ag ISO:

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

Quando o download for iniciado, uma barra de progresso será exibida.

Observação: a velocidade de download e o tamanho da mídia de atualização em seu ambiente podem afetar o tempo de composição do ISO.
Certifique-se de comparar o MD5 do arquivo baixado com o pacote disponível fornecido pelo suporte para validar a integridade do ISO baixado.

Quando o download estiver concluído, os ISOs serão criados no mesmo diretório.

Conecte o USB à máquina e execute o comando dd para criar a unidade USB inicializável.

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

Onde <MY_USB> é o nome da sua chave USB (deixe fora os sinais de maior e menor).

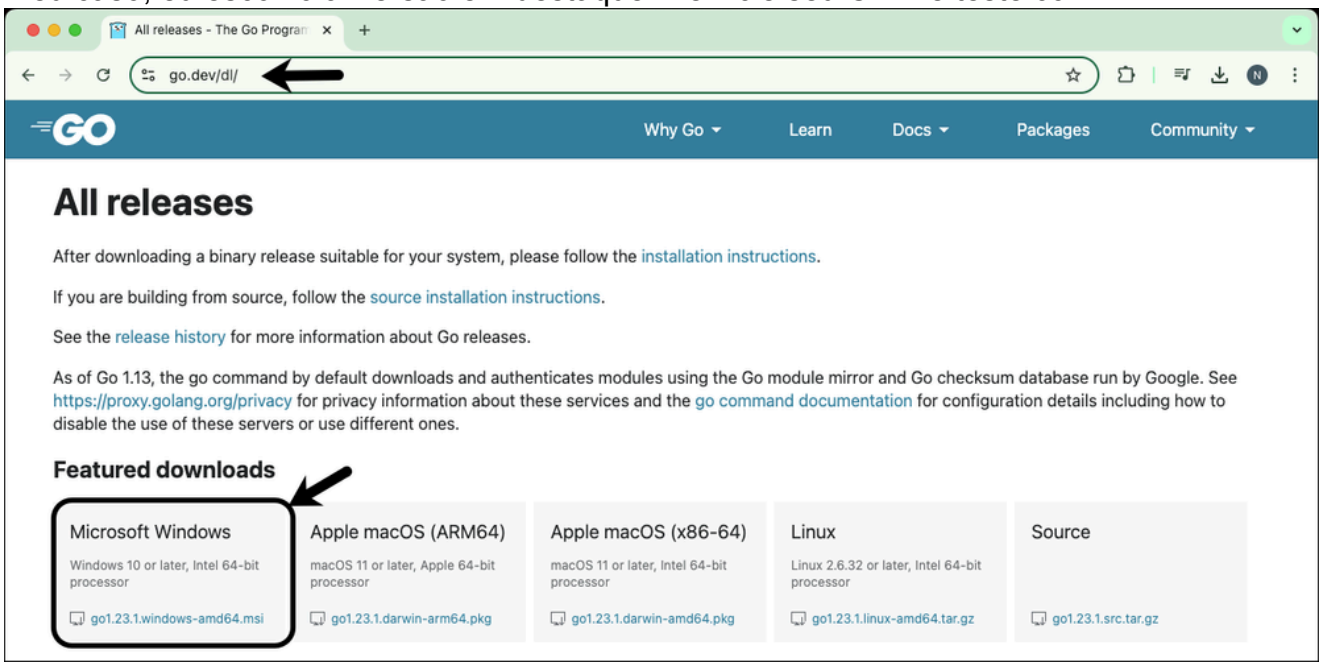
Insira a unidade USB e ligue ou reinicialize o dispositivo. Na tela de inicialização da Cisco, pressione F6 para entrar no Menu de inicialização.

Tip:
Execute o download após o horário comercial ou fora do horário de pico, pois ele pode afetar a largura de banda.
Para parar a ferramenta, feche o terminal ou pressione Ctrl+c/Ctrl+z.
Para continuar, execute o mesmo comando para continuar o download.

Windows - Download de ISO

Instalar a linguagem de programação GO

1. É necessário baixar a linguagem de programação GO. Instalar de https://golang.org/dl/ No meu caso, eu escolho a Versão em destaque. Reinicie seu CMD e teste com



   Feche e reabra o comando run do CMD para verificar:

```
go version
```

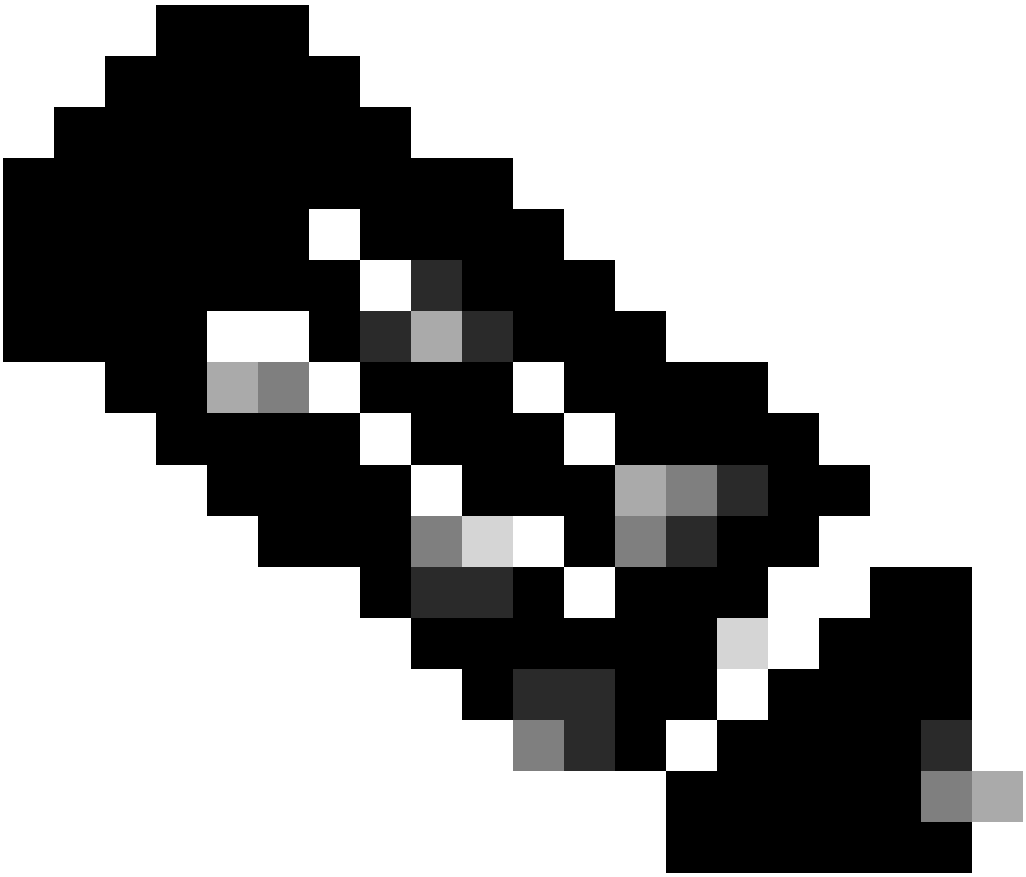
   Faça o download do ISO usando o comando Desync

2. Instale o DESSINC ferramenta. Após a execução do comando, você pode observar vários prompts de download. Aproximadamente após 2-3 minutos, o download deve ser feito.

```
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
```



> Observação: se o comando git não estiver funcionando, você poderá baixar e instalar o Git aqui: https://git-scm.com/download/win.

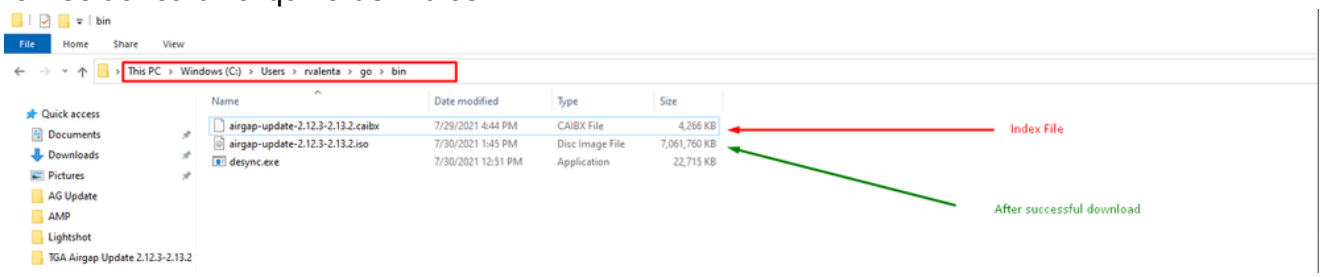
Em seguida, execute abaixo de dois comandos, um por um:

```
cd desync/cmd/desync
```

```
go install
```

```
C:\Users\rvalenta>go install github.com/folbricht/desync/cmd/desync@latest
go: downloading github.com/folbricht/tempfile v0.0.1
go: downloading github.com/go-ini/ini v1.62.0
go: downloading github.com/minio/minio-go/v6 v6.0.57
go: downloading github.com/pkg/errors v0.9.1
go: downloading github.com/sirupsen/logrus v1.7.0
go: downloading github.com/spf13/cobra v1.1.1
go: downloading github.com/spf13/pflag v1.0.5
go: downloading golang.org/x/crypto v0.0.0-20201221181555-eec23a3978ad
go: downloading github.com/sirupsen/logrus v1.8.1
go: downloading gopkg.in/cheggaaa/pb.v1 v1.0.28
go: downloading github.com/spf13/cobra v1.2.1
go: downloading github.com/minio/minio-go v1.0.0
go: downloading cloud.google.com/go v0.72.0
go: downloading github.com/DataDog/zstd v1.4.5
go: downloading github.com/boljen/go-bitmap v0.0.0-20151001105940-23cd2fb0ce7d
go: downloading github.com/dchest/siphash v1.2.2
go: downloading github.com/hanwen/go-fuse v1.0.0
go: downloading github.com/klauspost/compress v1.11.4
go: downloading github.com/DataDog/zstd v1.4.8
go: downloading github.com/hanwen/go-fuse/v2 v2.0.3
go: downloading github.com/pkg/sftp v1.12.0
go: downloading golang.org/x/crypto v0.0.0-20210711020723-a769d52b0f97
go: downloading github.com/minio/minio-go v6.0.14+incompatible
go: downloading github.com/pkg/sftp v1.13.2
go: downloading github.com/pkg/xattr v0.4.3
go: downloading golang.org/x/sync v0.0.0-20201207232520-09787c993a3a
go: downloading google.golang.org/api v0.36.0
go: downloading github.com/hanwen/go-fuse/v2 v2.1.0
go: downloading golang.org/x/sync v0.0.0-20210220032951-036812b2e83c
go: downloading github.com/mattn/go-runewidth v0.0.9
go: downloading golang.org/x/sys v0.0.0-20201201145000-ef89a241ccb3
```

3. Navegue até ir — > bin local. Por exemplo C:\Users\<username>\go\bin e copie/cole o TAC fornecido .caibx arquivo de índice.

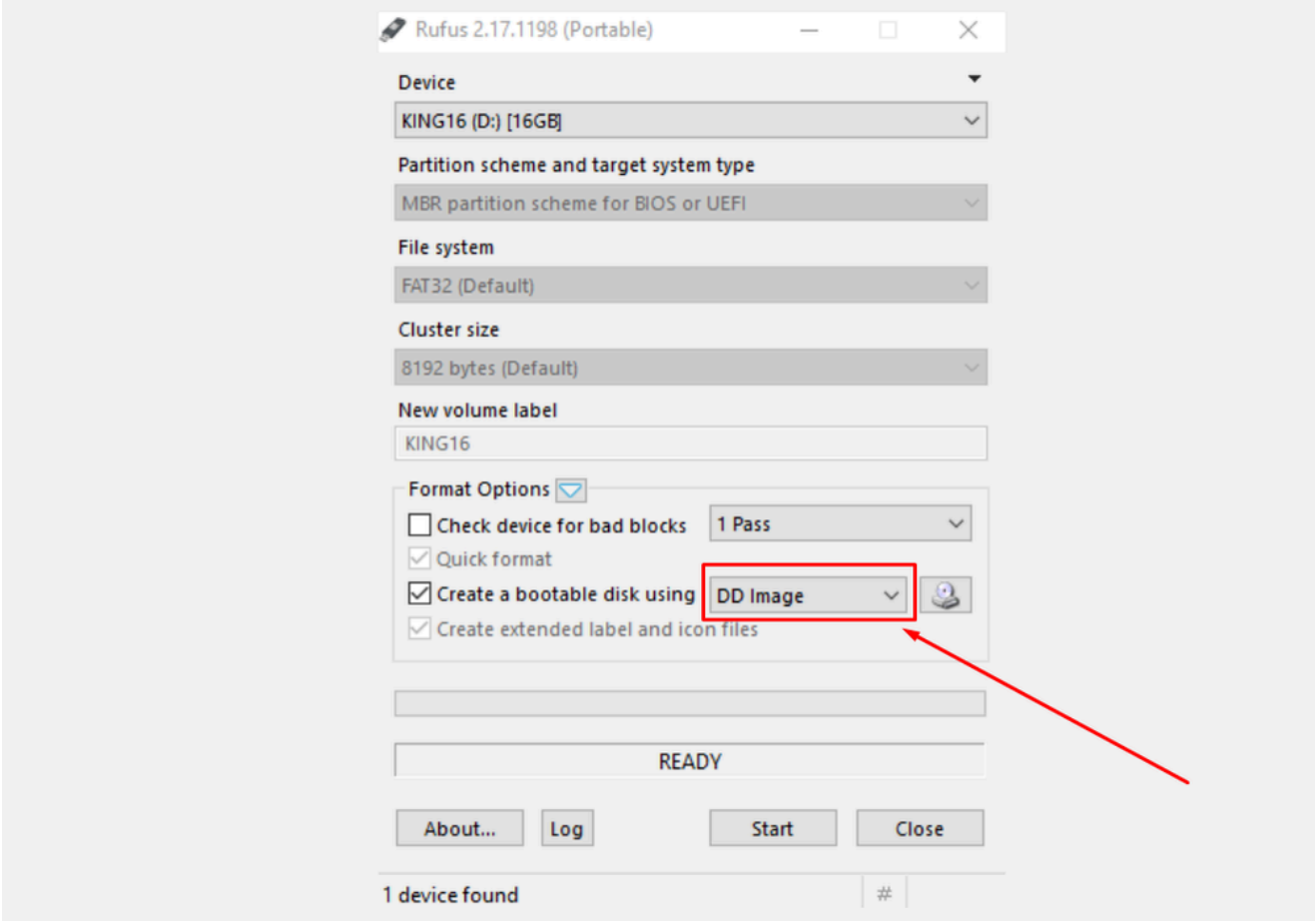


4. (Verificar) Volte para o prompt do CMD e navegue até a pasta go\bin e execute os comandos de download. Você deve ver imediatamente o download prosseguir. Aguarde a conclusão do download. Agora você deve ter o .ISO no mesmo local do arquivo copiado anteriormente .caibx arquivo de índice

```
\$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>_
```

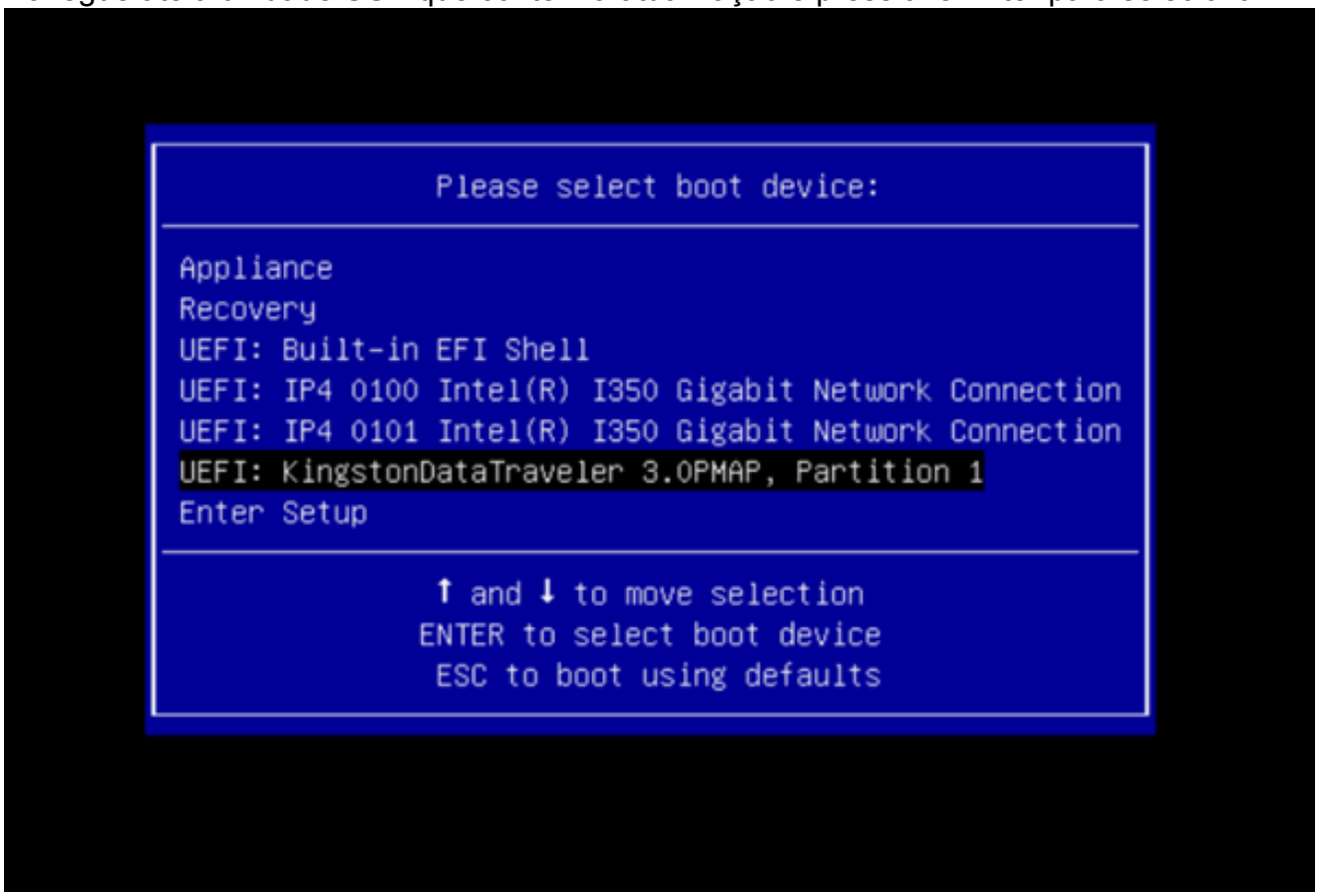
Para criar este USB de recuperação específica, é crucial usar Rufus versão 2.17, pois ele permite que você use opções dd essenciais. Você pode encontrar todas as versões do RUFUS neste repositório.



Dispositivo de inicialização a partir do USB

1. Insira o USB, reinicialize a ferramenta, e pressione rapidamente F6 na tela de inicialização da Cisco para entrar no Menu de inicialização.

2. Navegue até a unidade USB que contém a atualização e pressione Enter para selecionar.



   A mídia de atualização determina a próxima versão no caminho de atualização e copia o conteúdo dessa versão no equipamento. O equipamento executa a atualização imediatamente ou reinicializa em seu modo operacional regular para permitir que você entre no OpAdmin e inicie a atualização manualmente.

   Quando o processo de inicialização ISO estiver concluído, reinicialize o dispositivo Secure Malware Analytics novamente no modo de operação.

   Faça login na interface do usuário do portal e verifique se há avisos que informem se é seguro atualizar, etc., antes de continuar.

3. Navegue até a interface OpAdmin e aplique as atualizações, se elas não tiverem sido aplicadas automaticamente durante a reinicialização: OpAdmin > Operações > Atualizar dispositivo OBSERVAÇÃO: O processo de atualização inclui reinicializações adicionais como parte da atualização, que é feita a partir da mídia USB. Por exemplo, é necessário usar o botão Reinicializar na página de instalação após a instalação das atualizações. Repita conforme necessário para cada versão no USB.

Como encontrar o dispositivo /dev correto

Com a USB ainda não conectada ao endpoint, execute o comando "lsblk | grep -iE 'disk|part'.

```
xsilenc3x@Alien15:~/testarea/usb$ lsblk | grep -iE 'disk|part'
sda           8:0    0 931.5G  0 disk
```

```
├─sda1        8:1    0   128M  0 part
└─sda2        8:2    0 931.4G  0 part /media/DATA
nvme0n1     259:0    0 238.5G  0 disk
├─nvme0n1p1 259:1    0   650M  0 part
├─nvme0n1p2 259:2    0   128M  0 part
├─nvme0n1p3 259:3    0 114.1G  0 part
├─nvme0n1p4 259:4    0   525M  0 part /boot
├─nvme0n1p5 259:5    0   7.6G  0 part [SWAP]
├─nvme0n1p6 259:6    0  38.2G  0 part /
├─nvme0n1p7 259:7    0  62.7G  0 part /home
├─nvme0n1p8 259:8    0  13.1G  0 part
└─nvme0n1p9 259:9    0   1.1G  0 part
xsilenc3x@Alien15:~/testarea/usb$
```

Depois que o stick USB estiver conectado.

```
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$
```

Isso confirma que o dispositivo USB em /dev é "/dev/sdb".

Outras maneiras de confirmar, depois que o stick USB estiver conectado:

O comando dmesg fornece algumas informações. Após a conexão da USB, execute o comando 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$
```

O comando fidsk fornece informações sobre o tamanho, que podem ser usadas para confirmar: sudo fdisk -l /dev/sdb.

```
xsilenc3x@Alien15:~/testarea/usb$ sudo fdisk -l /dev/sdb
Disk /dev/sdb: 3.7 GiB, 4004511744 bytes, 7821312 sectors  <-------
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x63374e06

Device     Boot Start    End Sectors  Size Id Type
/dev/sdb1  *        0 675839  675840  330M  0 Empty
/dev/sdb2         116   8307    8192    4M ef EFI (FAT-12/16/32)
xsilenc3x@Alien15:~/testarea/usb$
```

 Observação: lembre-se de desmontar o USB antes de executar o comando "dd".

Confirmação de que o dispositivo USB do exemplo está montado.

```
xsilenc3x@Alien15:~/testarea/usb$ sudo mount -l | grep -i sdb
/dev/sdb1 on /media/xsilenc3x/ARCH_201902 type vfat (rw,nosuid,nodev,relatime,uid=1000,gid=1000,fmask=0
```

Para desmontar o dispositivo USB, use sudo umount /dev/sdb1.

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

Verifique novamente se o dispositivo não é visto como "montado".

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

status=opção de progresso

oflag=sync e status=opções de progresso no comando dd.

Ao gravar vários blocos de dados, a opção "status=progress" fornece informações sobre as

operações de gravação atuais. Isso é útil para confirmar se o comando "dd" está gravando no momento no cache de páginas; ele pode ser usado para mostrar o progresso e a quantidade completa de tempo em segundos de todas as operações de gravação.

Quando não usado, "dd" não fornece informações sobre o progresso, apenas os resultados das operações de gravação são fornecidos antes de "dd" retornar:

```
[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 usadas, as informações em tempo real sobre as operações de gravação são atualizadas a cada segundo.

```
[rootuser@centos8-01 tga-airgap]$ dd if=/dev/zero of=testfile.txt bs=1M count=8192 status=progress
8575254528 bytes (8.6 GB, 8.0 GiB) copied, 8 s, 1.1 GB/s <----------------
8192+0 records in
8192+0 records out
8589934592 bytes (8.6 GB, 8.0 GiB) copied, 8.03387 s, 1.1 GB/s
[rootuser@centos8-01 tga-airgap]
```

Observação: na documentação oficial do processo de atualização offline da TGA, o comando informado é: dd if=airgap-update.iso of=/dev/<MY_USB> bs=64M

Após alguns testes, o exemplo a seguir é observado.

Uma vez que um arquivo é criado de 10MB com "dd" usando o dispositivo /dev/zero.

1M x 10 = 10M (10240 kB + dados do sistema anterior em caches de página de arquivo sujo = 10304 kB —> isso é percebido no cache de página suja no final de "dd").

```
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && dd if=/dev/zero of=testfile.txt
count=10 status=progress && cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                92 kB
10+0 records in
10+0 records out
10485760 bytes (10 MB, 10 MiB) copied, 0.0138655 s, 756 MB/s
Dirty:             10304 kB <----- dirty page cache after "dd" returned | data still to be written to t
1633260775 <---- epoch time
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:             10372 kB
1633260778
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
```

```
Dirty:             10380 kB
1633260779
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:             10404 kB
1633260781
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:             10412 kB
1633260782
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:             10424 kB
1633260783
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:             10436 kB
1633260785
[rootuser@centos8-2 testarea]$ cat /proc/meminfo | grep -iE 'dirty' && date +%s
Dirty:                 0 kB  <--- data in the dirty page cache flushed = written to the block device
1633260786 <---- epoch time
[rootuser@centos8-2 testarea]$
```

1633260786 - 1633260775 = 11 seconds

Observação: depois que o comando "dd" retornou, a operação de gravação no dispositivo de bloco não foi concluída, ela foi percebida 11 segundos após o retorno.
Se esse fosse o comando "dd" ao criar o USB inicializável com o TGA ISO, E eu tivesse removido o USB do endpoint antes desses 11 segundos = Eu teria um ISO corrompido no USB inicializável.

Explicação:

Os dispositivos de bloco fornecem acesso em buffer aos dispositivos de hardware. Isso fornece uma camada de abstração para aplicativos ao trabalhar com dispositivos de hardware.

Os dispositivos de bloco permitem que um aplicativo leia/grave por blocos de dados de tamanhos diferentes; essa função read()/write() é aplicada nos caches de página (buffers) e não diretamente no dispositivo de bloco.
O kernel (e não o aplicativo que faz a leitura/gravação) gerencia a movimentação de dados dos buffers (caches de página) para os dispositivos de bloco.

Portanto:

O aplicativo (neste caso, "dd") não tem controle sobre a liberação dos buffers se não receber instruções.

A opção "oflag=sync" força a gravação física síncrona (pelo kernel) depois que cada bloco de saída (fornecido por "dd") é colocado no cache de páginas.
oflag=sync degrada o desempenho "dd" quando comparado a não usar a opção; mas, se estiver habilitado, ele garante uma gravação física no dispositivo de bloco após cada chamada write() de "dd".

Teste : Usando a opção "oflag=sync" do comando "dd" para confirmar que todas as operações de gravação com os dados de cache de página suja foram concluídas no retorno do 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]$
```

Nenhum dado restante da operação de gravação no cache de páginas sujas.
A operação de gravação foi aplicada antes (ou no mesmo instante) que o comando "dd" fosse retornado (não 11 segundos após o teste anterior).
Agora, tenho certeza de que após o retorno do comando "dd" não havia dados no cache de página suja relacionados à operação de gravação = nenhum problema na criação de USB inicializável (se o checksum ISO estiver correto).

Observação: leve em consideração este sinalizador (oflag=sync) do comando "dd" ao trabalhar neste tipo de caso.

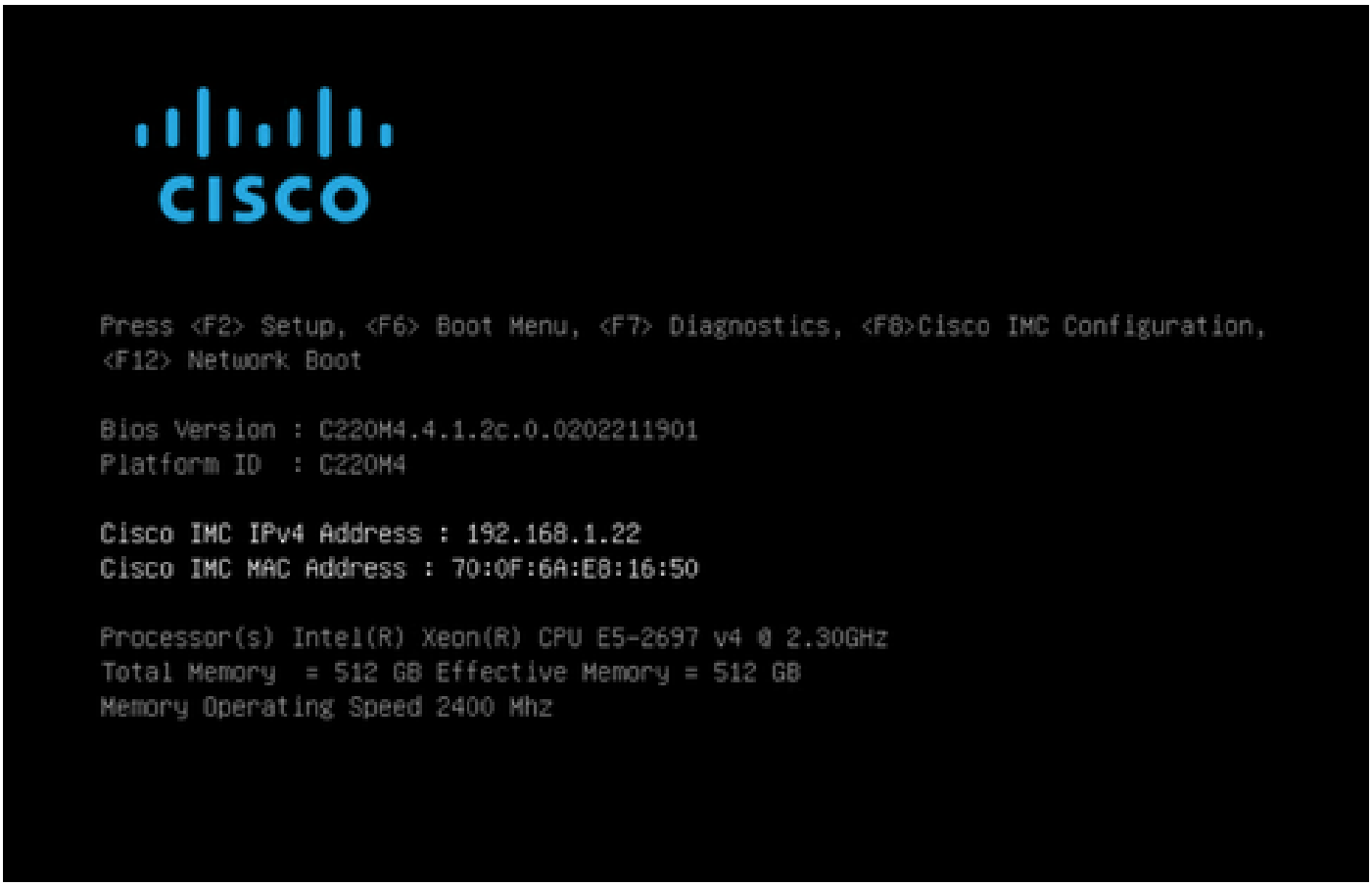
Sequência de inicialização para unidades de disco rígido para atualizações offline

Requisito:

Precisamos garantir que o disco rígido seja formatado usando a opção "DD" com qualquer ferramenta disponível e que a mídia seja copiada posteriormente para a unidade. Se não usarmos essa formatação, não poderemos ler essa mídia.

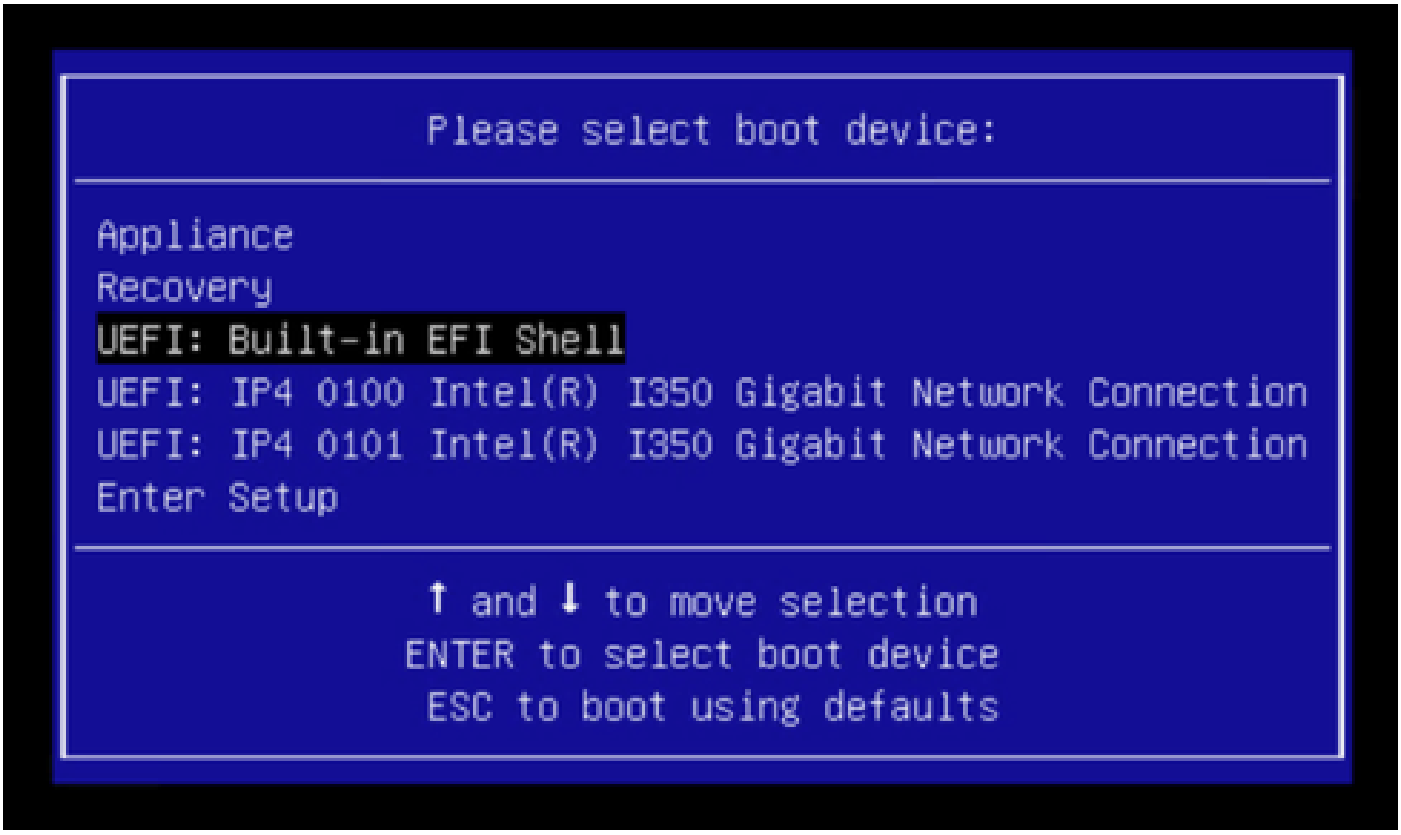
Uma vez que temos a mídia carregada no HDD/USB usando a formatação "DD", precisamos conectá-la ao dispositivo TGA e reiniciar o dispositivo.

Esta é a tela de seleção padrão do Menu de inicialização. Precisamos pressionar "F6" para inicializar o dispositivo e selecionar a mídia de inicialização

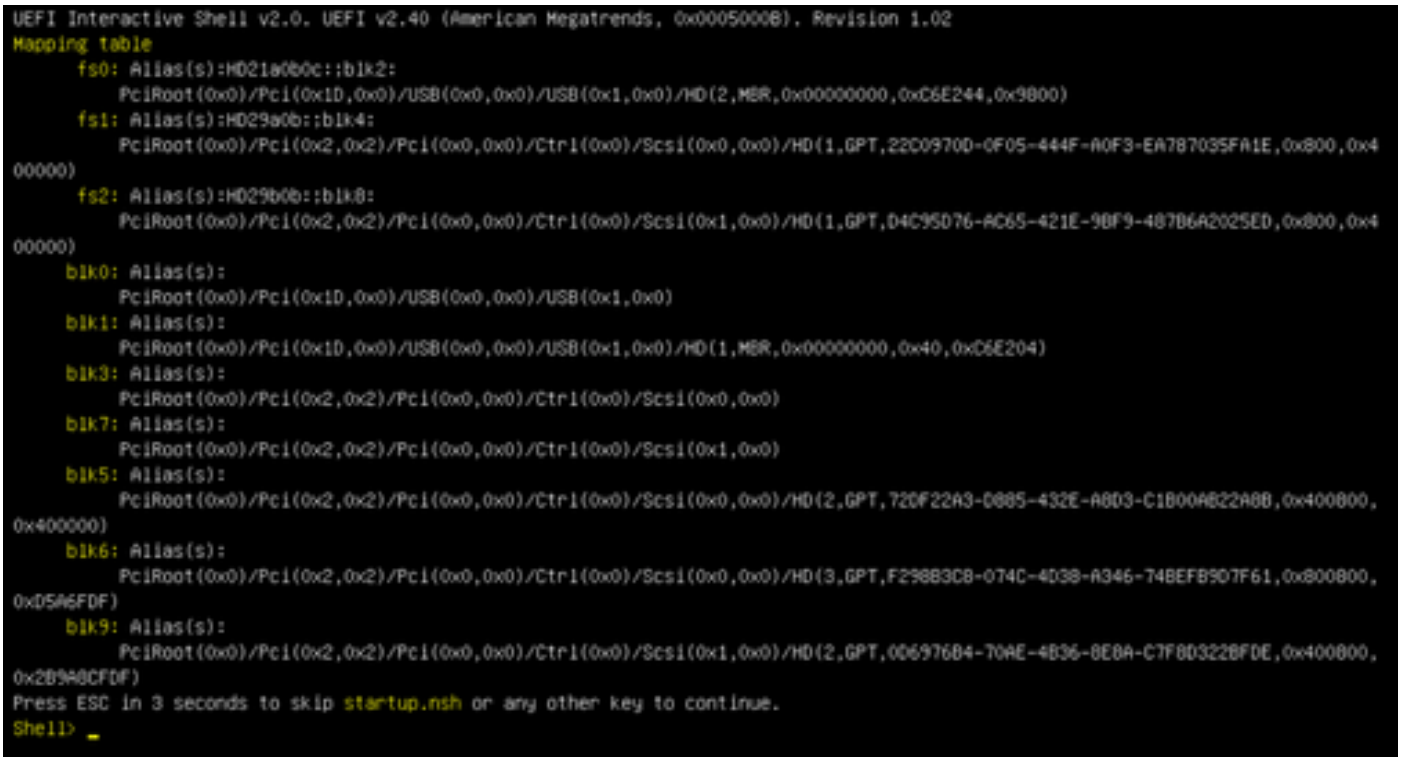


Uma vez que o dispositivo reconheça nossa entrada, ele solicitará que o dispositivo entre no menu de seleção de inicialização.

Esse é o prompt que pode diferir entre modelos TGA diferentes. Idealmente, veríamos a opção de inicializar usando a mídia de inicialização (sistema de arquivos de upgrade) a partir desse menu, mas se não for exibida, precisaremos fazer login na "EFI Shell".



Você teria que pressionar "ESC" antes que o script "startup.sh" terminasse para se mover para o EFI Shell. Depois de fazer login no EFI Shell, observamos que as partições detectadas nesse caso são 3 sistemas de arquivos: fs0:, fs1:, fs2.



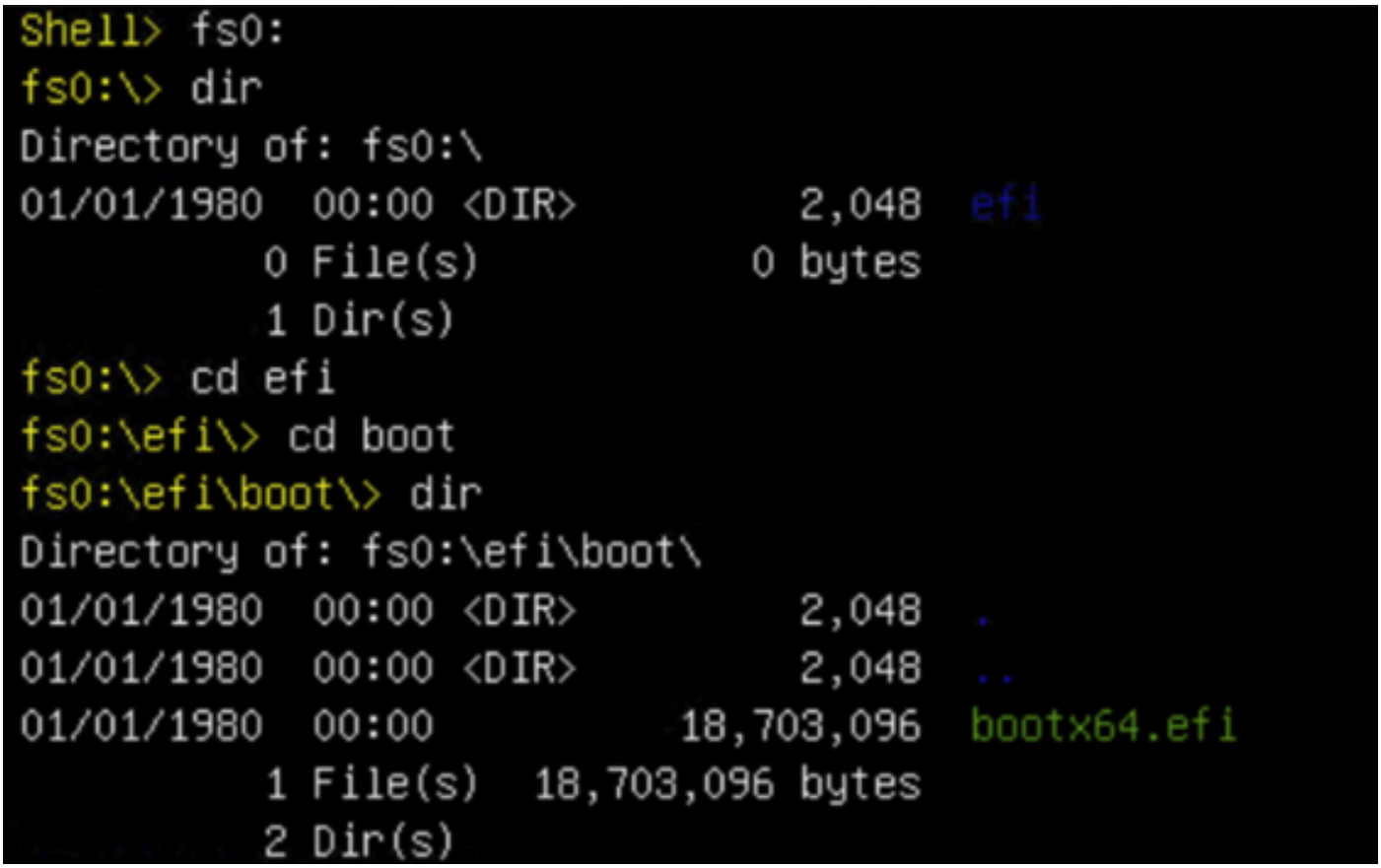
Importante

Identificando o sistema de arquivos correto:

- De acordo com a captura de tela acima, você poderia ver que "fs0:" é a única mídia com "USB" em seu caminho e, portanto, podemos ter certeza de que este sistema de arquivos conteria a mídia de inicialização (sistema de arquivos de atualização).

Em caso de perda de sistemas de arquivos:

- Se apenas fs0: e fs1: estiverem disponíveis e não houver fs2:, verifique se a mídia de inicialização (sistema de arquivos de atualização) foi gravada no modo dd e está conectada com êxito.
- A mídia de inicialização (sistema de arquivos de atualização) deve sempre ter um número menor do que a mídia de recuperação e devem estar sempre próximas uma da outra; é se a unidade conectada por USB está no início da extremidade que provavelmente será alterada (então, se ela ocupa a posição frontal em fs0: ou a posição traseira em fs2:) precisaria ser identificada
- Nesse caso, na captura de tela abaixo, está o arquivo ".efi" correto, pois ele está sob a partição "\efi\boot" e tem a convenção de nomenclatura de "bootx64.efi"

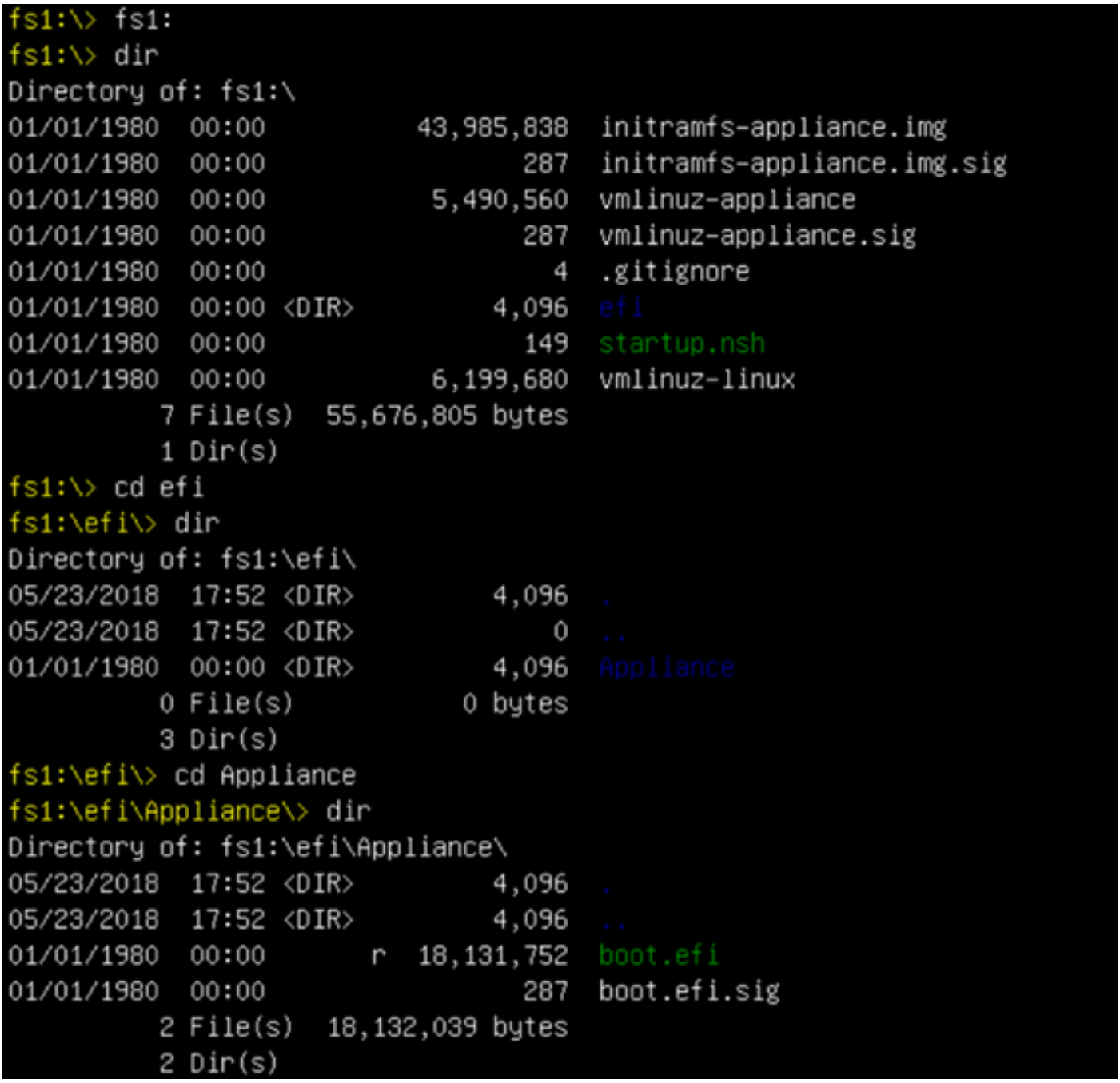


Para inicializar o dispositivo na mídia de inicialização (sistema de arquivos de upgrade), devemos executar o arquivo "bootx64.efi":

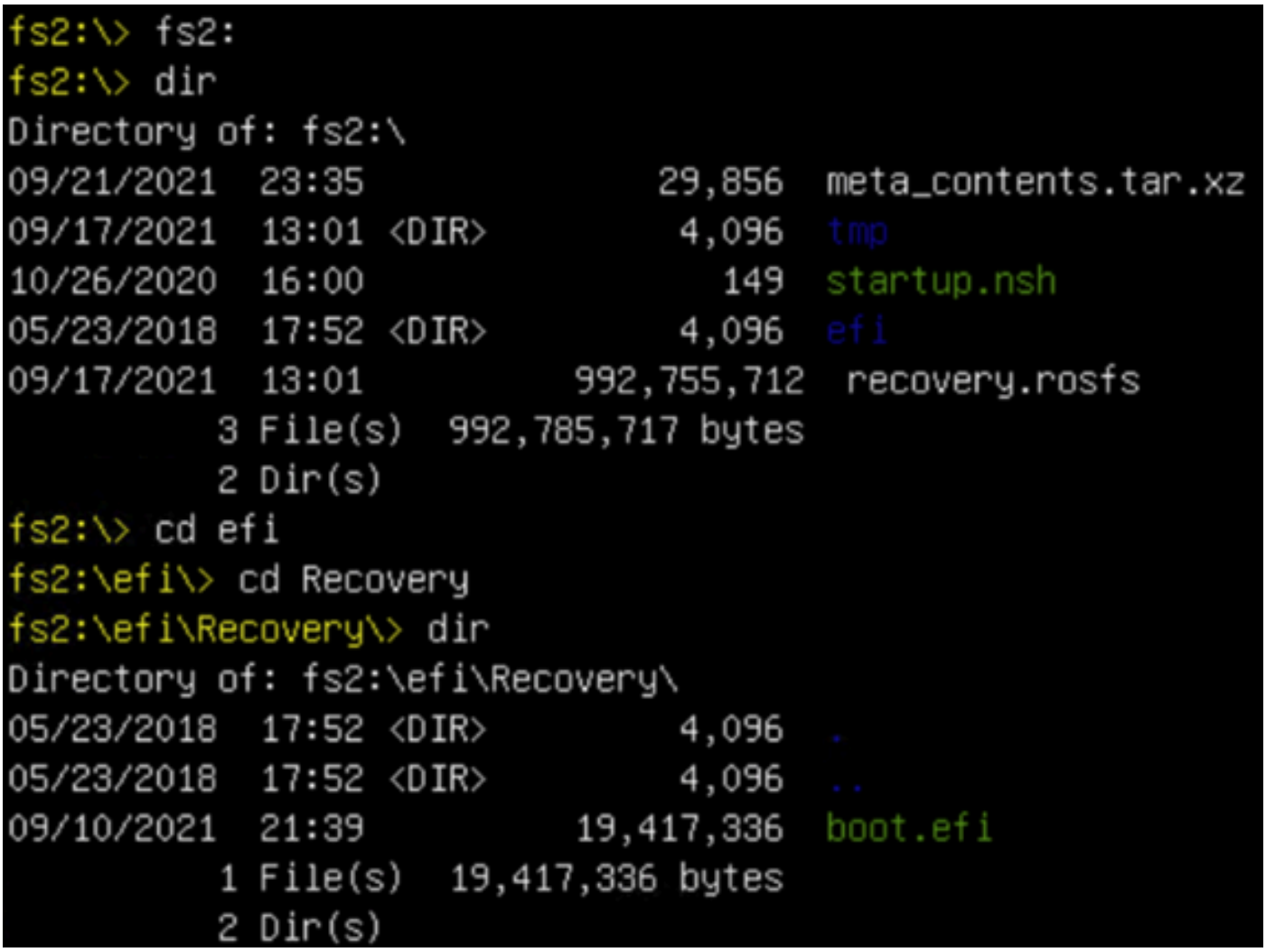
```
fs0:\efi\boot\bootx64.efi
```

Para sua referência, exibimos o conteúdo dos outros sistemas de arquivos também abaixo:

fs1: este é o sistema de arquivos de inicialização principal.



fs2: Este é o sistema de arquivos de inicialização da imagem de recuperação.



Instruções Diversas:

Para verificar o sistema de arquivos correto que contém a mídia de inicialização montada. Podemos fazer isso navegando pelos diferentes sistemas de arquivos e verificando o arquivo de inicialização ".efi"

Observação: a sequência da mídia de inicialização real (sistema de arquivos de atualização) que, neste caso, é "fs0:" também pode variar com outros dispositivos.
O nome e o caminho podem variar, mas em todas as imagens modernas, deve ser o mesmo.

Lista de verificação que pode ajudar a localizar a mídia de inicialização correta (atualizar o sistema de arquivos):

- Se a raiz de um sistema de arquivos contiver "vmlinuz-appliance", ela não será a mídia de inicialização (sistema de arquivos de upgrade).
- Se a raiz de um sistema de arquivos contiver "meta_contents.tar.xz", ela não será a mídia de inicialização (sistema de arquivos de upgrade).
- Se um sistema de arquivos não contiver "efi\boot\bootx64.efi", ele não será a mídia de inicialização (sistema de arquivos de upgrade).

Instalador de campo SMA 2.19.2
Para dispositivos SMA que foram corrompidos e/ou estão além do reparo, use o instalador de campo para reinstalar o software SMA. Observe que este pacote especial é destinado SOMENTE para fins de RECUPERAÇÃO. Utilizá-lo para uma atualização pode resultar em perda de dados irreversível.

Recuperação

Em caso de recuperação quando os TGAs ficam presos e uma vez que o GATE fornece esta imagem especial, precisamos usar uma versão específica do software bem conhecido chamado RUFUS. O RUFUS é amplamente usado para criar USBs inicializáveis. No caso dessa imagem específica, precisamos usar o RUFUS versão 2.17. É muito importante usar a versão 2.17. Esta é a última versão em que você pode usar opções dd que é muito importante na criação deste específico recuperar USB. Você pode encontrar todas as versões deste repositório repositório Rufus caso esses arquivos não estejam mais disponíveis Eu também incluir instaladores para versões completas e portáteis neste documento.

Senha para RUFUS_217.zip

Spoiler (Realce para ler)
C1sco!123
C1sco!123

Nota especial para a atualização off-line ISO TGA Airgap 2.x-2.12.3ag2 MUST_RESET [airgap-update-MUST_RESET-2.12.3ag2]

Se você estiver usando a Atualização TGA Airgap 2.x-2.12.3ag2 MUST_RESET para atualizar dispositivos que são mais antigos que 2.11.x, você DEVE REINICIAR dados [data-destroy] para fazer a atualização funcionar corretamente.

Esta mídia de atualização de airgap é uma construção única para permitir atualizações de versões 2.x ainda muito antigas diretamente para 2.12.3ag2; é especificamente testada para trabalhar com 2.2.3 e 2.5 como versões iniciais: versões mais recentes do que o acima são muito provável de funcionar; versões mais antigas do que o acima (mas mais recentes do que 2.0) pode plausivelmente funcionar.

- As atualizações de uma versão anterior à 2.11.x exigem uma redefinição de dados para funcionar corretamente. Isso ocorre porque o processo regular de upgrade envolve migrações de dados que não são mais incluídas além da próxima versão secundária. Pelo mesmo motivo, os backups criados em uma versão anterior à 2.11.x podem não ser restauráveis na compilação instalada por esta mídia ou podem causar comportamento defeituoso após serem restaurados.

- Se a atualização de uma versão que usa '/sandcastle' em vez de '/data' para armazenamento em massa (ou seja, uma versão mais antiga que 2.7), pode haver uma falha de inicialização temporária após a instalação dessa compilação. O estado do sistema quando isso ocorre é

como mostrado no arquivo chamado `airgap-update-MUST_RESET-2.12.3ag2-filesystem-rename-hang-screenshot.png` no mesmo diretório deste README. Quando essa tela é exibida por mais de 15 segundos sem alterações, é seguro reinicializar o sistema.

Pacotes de arquivos de índice ISO offline

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.