

Atualize a nuvem privada do ponto de extremidade seguro Air Gapped usando o dispositivo de armazenamento em massa USB

Contents

Introdução

Este documento descreve o guia passo a passo sobre como atualizar o software na nuvem privada de endpoint seguro usando armazenamento em massa USB.

Problema

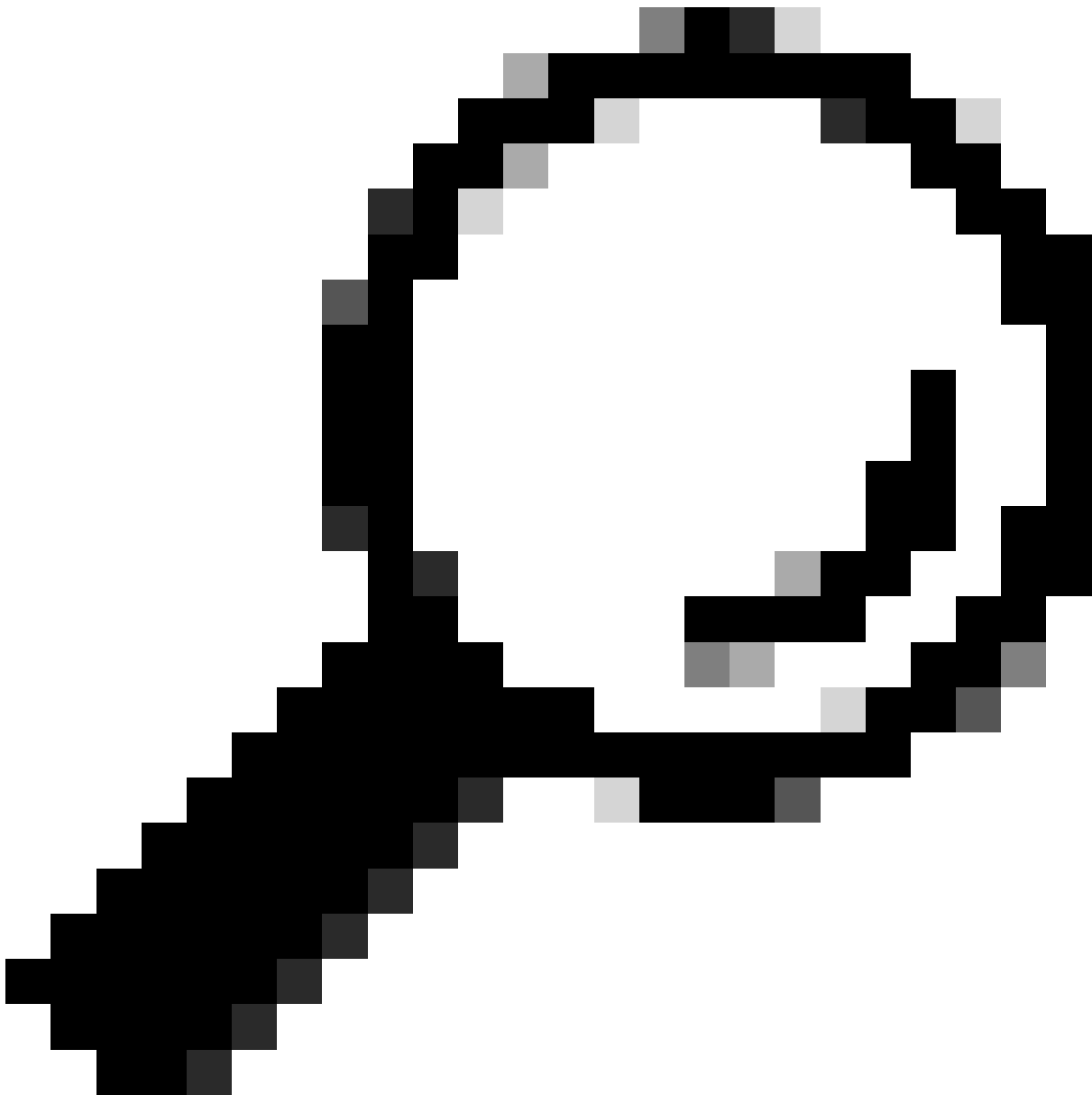
Em ambientes altamente seguros, os dispositivos "air-gapped" são essenciais para proteger dados e sistemas confidenciais de ameaças externas. Esses dispositivos operam sem nenhuma conexão de rede, garantindo que não haja comunicação direta ou indireta com redes não confiáveis. Embora esse isolamento forneça segurança excepcional, ele também apresenta desafios significativos quando se trata de manter e atualizar o software do dispositivo.

O principal problema está na atualização eficiente e segura de dispositivos com isolamento térmico sem comprometer seu status isolado ou postura de segurança. Os métodos de atualização tradicionais, que geralmente dependem da conectividade de rede, não são aplicáveis nesses cenários. Consequentemente, as empresas devem encontrar métodos alternativos para fornecer atualizações, garantir a conformidade com padrões de segurança e minimizar o tempo de inatividade durante o processo de atualização.

Enfrentar esses desafios exige um mecanismo de atualização bem definido, seguro e eficiente, adaptado às restrições exclusivas dos ambientes "air-gapped". Neste contexto, as atualizações através do armazenamento em massa USB apresentam uma solução viável que pode melhorar a capacidade de gerenciamento e a segurança da atualização de aparelhos com isolamento de ar.

Solução

1. Faça download do aplicativo amp-sync no portal OAdmin > Operações > Atualizar dispositivo > Faça download do amp-sync.



Dica: se você vir esta mensagem: "Este dispositivo de nuvem privada inclui um instantâneo Protect DB. É recomendável executar amp-sync com as opções -X e -M 20230821-1604 para economizar largura de banda" adicionar esses atributos ao final do comando amp-sync, por exemplo amp-sync all -X -M 20230821-1604.

-
2. Copie amp-sync para a máquina baseada em Linux e adicione privilégios de executável. Coloque-o na pasta em que você tem espaço suficiente (mais de 300 GB para todo o banco de dados).
 3. Há duas opções para executar amp-sync:
 - a. como processo principal:

```
amp-sync all
```

b. em segundo plano:

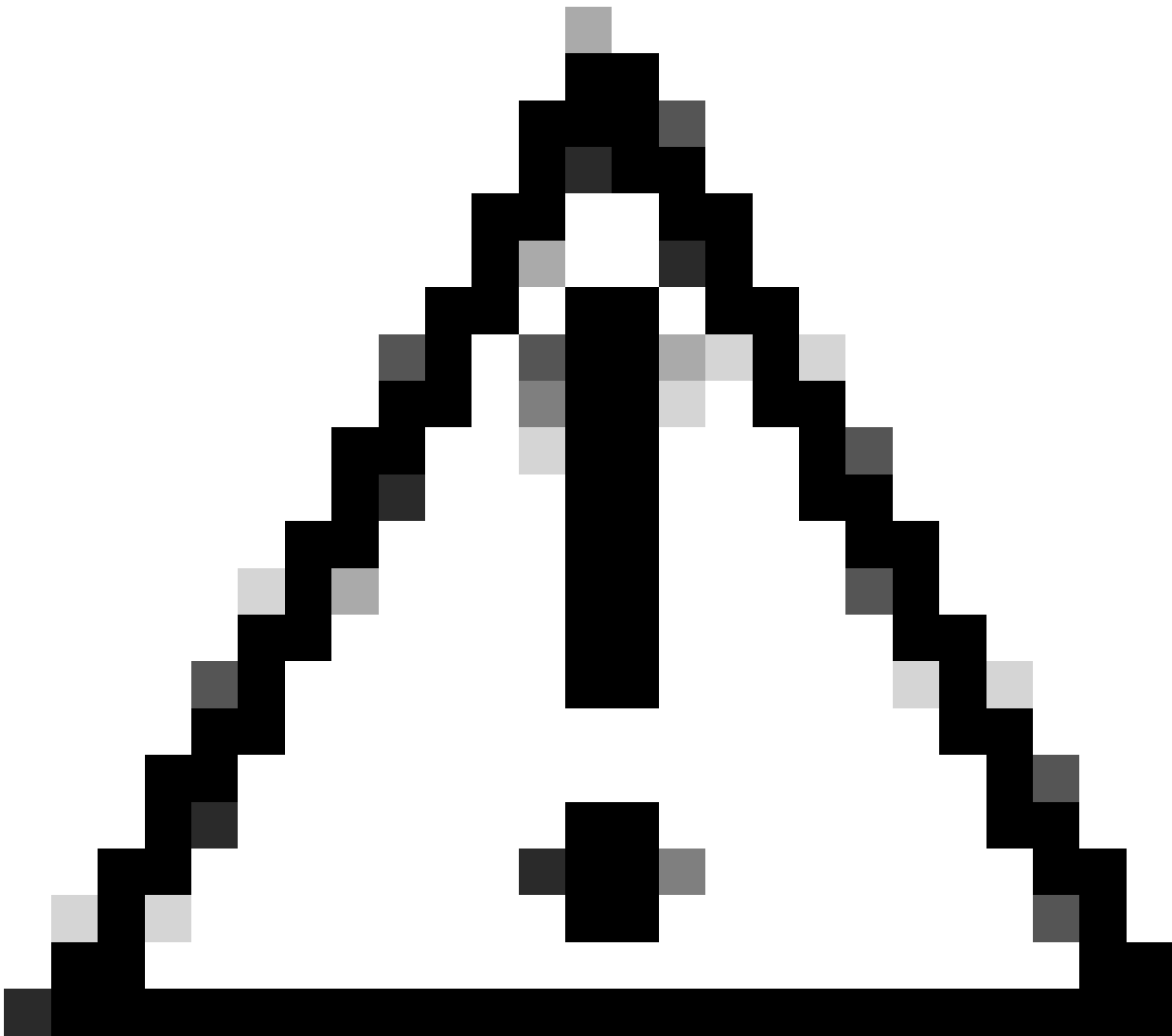
```
nohup amp-sync all &
```

para permitir que ele seja executado mesmo se a sessão SSH for desconectada. Isso é útil se todo o processo de download levar várias horas. Você pode examinar o status atual com o comando:

```
tail -f nohup.out
```

4. Copie a imagem ISO para o computador onde está conectado o armazenamento em massa USB.

5. Copie a imagem ISO para o armazenamento USB.



Cuidado: o armazenamento em massa USB deve ser formatado nos formatos ext2, ext3, ext4 ou XFS. Não há suporte para exFAT e NTFS. O FAT32, embora suportado em ambas as plataformas, tem a limitação de que um arquivo não pode ser maior que 4 GB.

6. Desconecte com segurança o armazenamento em massa USB e conecte-o ao dispositivo de nuvem privada.

7. Monte o armazenamento em massa USB e copie o arquivo ISO para a pasta /data/mount:

```
mkdir /mnt/usb  
mount /dev/sdd1 /mnt/usb  
cp /mnt/usb/PrivateCloud-4.2.1-Updates-2024-08-30-NOSNAP-D20230821-1604-prod.iso /data/mount
```

8. Vá para OAdmin > Operações > Montar ISO.

9. Selecione Tipo de Montagem como Local, Diretório Local como /data/mount e Arquivo ISO Local como o nome do arquivo nessa pasta do Diretório Local, por exemplo:

Mount an Update ISO

ISO Configuration		HELP
Mount Type	Local	
Local Directory	/data/mount	
Local ISO File	PrivateCloud-4.2.1-Updates-2024-08-30-NOSNAP-D20230821-1604-prod.iso	

✓ Mount

10. Clique em Montar e monitore as atualizações do Status de Montagem. Se o ISO foi montado com sucesso, você poderá ver uma saída semelhante:

Mount Status

Mounted ISO	
local /dev/loop0 /data/mount/PrivateCloud-4.2.1-Updates-2024-08-30-NOSNAP-D20230821-1604-prod.iso	Unmount

11. Vá para OAdmin > Operations > Update Device e clique em Check Update ISO e depois em Update Content ou/e Update Software.

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.