Execute uma redefinição de fábrica segura nos roteadores de borda SD-WAN

Contents

Introdução

Este documento descreve o procedimento de redefinição de fábrica seguro para Cisco Catalyst SD-WAN Edge Routers executando Cisco IOS® XE.

Background

Uma redefinição de fábrica retorna o dispositivo ao seu estado original de fabricação e é normalmente exigida como parte de fluxos de trabalho de descomissionamento, reimplantação ou correção de segurança.

Caution: Este artigo recomenda exclusivamente a opção `fatory-reset all secure`, que executa a limpeza de dados alinhada com NIST SP 800-88 Rev. 1. Este método torna os dados na mídia de armazenamento irrecuperáveis e fornece o mais alto nível de garantia de que os dados confidenciais foram removidos permanentemente.

Aplicabilidade

O comando `fatory-reset all secure` é suportado nestas plataformas que executam o Cisco IOS XE:

- Plataformas de borda Cisco Catalyst 8200 Series
- Plataformas de borda Cisco Catalyst 8300 Series
- Plataformas de borda Cisco Catalyst 8500 Series
- Roteadores de serviços de agregação Cisco ASR 1000 Series
- Roteadores de serviços integrados Cisco ISR 4000 Series
- Roteadores de serviços integrados Cisco ISR 1000 Series

Note: A opção `all secure` pode apenas ser usada em dispositivos autônomos. Verifique se a sua plataforma e a versão do Cisco IOS XE suportam a palavra-chave `secure` verificando `fatory-reset ?` no modo EXEC privilegiado antes de continuar.

Pré-requisitos

Antes de executar a redefinição de fábrica segura, verifique se estes pré-requisitos foram atendidos:

- Configuração de backup: Exporte e armazene com segurança todas as configurações, modelos e políticas de dispositivos do SD-WAN Manager (vManage) antes da redefinição.
- Imagens do software de backup: Certifique-se de ter uma cópia da imagem do software Cisco IOS XE carregada no bootflash antes de executar a reinicialização. Enquanto a opção `secure` retém a imagem de inicialização na flash na maioria das plataformas, certas plataformas limpam totalmente o flash de inicialização como parte do apagamento seguro. Como contingência, tenha sempre a imagem do Cisco IOS XE disponível em uma unidade USB ou servidor TFTP acessível para garantir a recuperação independentemente do comportamento da plataforma.
- Alimentação ininterrupta: Verifique se o dispositivo tem uma fonte de alimentação ininterrupta durante todo o processo de reinicialização. A perda de energia durante a

limpeza pode tornar o dispositivo irrecuperável.

- Conclua todos os procedimentos de ISSU: Se alguma operação de In-Service Software Upgrade (ISSU) estiver pendente ou em andamento, conclua-as antes de iniciar a redefinição de fábrica.
- Liberar licença HSEC: A licença HSEC deve ser liberada do dispositivo antes de executar a redefinição de fábrica. Devolva a licença HSECK9 conforme descrito na seção "Devolva a licença HSECK9" em: Configure a licença HSECK9 em Cisco Edge Routers
- Remover da malha SD-WAN: Invalide o certificado do dispositivo do vManage e remova o dispositivo da sobreposição do controlador antes de executar a redefinição.
- Acesso do console: Verifique se você tem acesso físico de console ao dispositivo. Após a redefinição, o dispositivo entra no modo ROMMON e as sessões VTY não estão disponíveis.

Tip: Confirme se a imagem do Cisco IOS XE está carregada no bootflash e se uma cópia de recuperação está disponível em USB ou TFTP antes de executar a redefinição de fábrica. Enquanto a opção `secure` retém a imagem de inicialização na maioria das plataformas, algumas plataformas limpam completamente o flash de inicialização durante o processo.

O que é apagado

O comando `fatory-reset all secure` remove permanentemente estes dados do dispositivo:

Categoria	Dados apagados
Software	Todas as imagens do software Cisco IOS XE (a imagem de inicialização atual é retida na memória flash na maioria das plataformas; no entanto, em certas plataformas, o bootflash é totalmente limpo)
Configuração	Configuração de inicialização, configuração de execução
Logs e diagnósticos	Informações de travamento, registros do sistema, OBFL (On-Board Failure Logging, Registro de falhas na placa)
Material de segurança	Credenciais e chaves relacionadas a FIPS, chaves PKI e certificados configurados pelo usuário
Armazenamento	Todos os dados do usuário em armazenamento removível (SATA, SSD, USB)
Licenciamento	Todas as licenças de dispositivos (requer novo registro)
ROMMON	Variáveis de ambiente ROMMON adicionadas pelo usuário

Note: Estes itens são retidos após a redefinição de fábrica segura:

- Certificados SUDI (Secure Unique Device Identifier) e chaves PKI associadas
- Valor do registro de configuração

- A imagem de inicialização atual (mantida na memória flash na maioria das plataformas; em determinadas plataformas, o bootflash é totalmente limpo — sempre com recuperação USB/TFTP preparada)

Procedimento: Redefinição de fábrica segura

aviso: Este procedimento é irreversível. Uma vez iniciados, todos os dados listados na tabela anterior são permanentemente destruídos. Verifique se todos os backups foram verificados antes de continuar.

Passo 1: Acessar o dispositivo através do console

Conecte-se ao dispositivo por meio de uma conexão de console física. O acesso SSH/VTY é perdido durante o processo de redefinição.

Passo 2: Entre no modo EXEC privilegiado

```
Device> enable
Device#
```

Passo 3: Execute o Secure Fatory Reset (Redefinição segura de fábrica)

Execute este comando para iniciar a redefinição de fábrica segura:

```
Device# factory-reset all secure
```

O sistema solicita a confirmação:

```
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
```

⚠ Verificar: No prompt de confirmação, verifique uma última vez se:

- Backup de todas as configurações
- A imagem de recuperação do Cisco IOS XE está disponível em USB ou TFTP
- O dispositivo foi removido da sobreposição de SD-WAN

Digite `y` ou pressione Enter para confirmar e continuar.

Passo 4: Aguarde a conclusão da limpeza

O dispositivo executa a limpeza de dados em todas as mídias de armazenamento. Esse processo pode levar um longo período, dependendo da capacidade de armazenamento. Não interrompa a alimentação durante esta operação.

Após a conclusão, o dispositivo é recarregado automaticamente e entra no modo ROMMON.

Passo 5: Restaurar variáveis de ambiente do ROMMON

Após a redefinição, as variáveis de ambiente que incluem `MAC_ADDRESS` e `SERIAL_NUMBER` podem ser apagadas. Execute uma redefinição de ROMMON para restaurá-los:

```
rommon 1> reset
```

✎ Note: A variável de ambiente de taxa BAUD retorna ao seu valor padrão (9600) após uma redefinição de fábrica. Se sua sessão de console foi configurada em uma taxa de baud diferente, você pode ajustar as configurações do emulador de terminal para 9600 baud para recuperar o acesso ao console.

Passo 6: Inicialize a imagem do software Cisco IOS XE

Na maioria das plataformas, a opção `secure` retém a imagem de inicialização na flash. Verifique sua presença com `dir bootflash:` do ROMMON. Se a imagem estiver disponível, inicialize diretamente:

```
rommon 2> boot bootflash:<image-filename>.bin
```

Comportamento específico da plataforma: Em determinadas plataformas de hardware, o processo de limpeza segura limpa totalmente o flash de inicialização, incluindo a imagem de inicialização. Nesses casos, faça a recuperação via USB ou TFTP.

Opção A — Recuperação via USB:

```
rommon 2> boot usbflash0:<image-filename>.bin
```

Opção B — Recuperação TFTP:

Defina as variáveis de ambiente ROMMON necessárias e, em seguida, inicie a transferência:

```
rommon 2> IP_ADDRESS=

rommon 3> IP_SUBNET_MASK=

rommon 4> DEFAULT_GATEWAY=

rommon 5> TFTP_SERVER=

rommon 6> TFTP_FILE=

     .bin
rommon 7> tftpboot
```

Verifique se a conectividade com o servidor TFTP está disponível através da interface de gerenciamento ou de um segmento de rede diretamente conectado. O ROMMON não suporta protocolos de roteamento, portanto, o servidor TFTP deve estar acessível através do gateway padrão configurado.

Tenha sempre uma imagem de recuperação preparada em USB ou um servidor TFTP acessível antes de iniciar a redefinição de fábrica para explicar esse comportamento.

Pós-reinicialização: Reintegração na malha SD-WAN

Depois que o dispositivo tiver sido restaurado com uma imagem limpa do Cisco IOS XE, use os procedimentos de onboarding SD-WAN padrão para trazer o dispositivo de volta à estrutura:

1. Configuração de bootstrap: Aplicar a configuração inicial do bootstrap (IP do sistema, ID do local, nome da organização, endereço vBond). Consulte Gerar arquivo de bootstrap usando CLI para obter o procedimento.
2. Instalação do certificado: Instale o certificado do dispositivo e a cadeia raiz de CA conforme exigido pela autoridade de certificação (Symantec/DigiCert, Cisco PKI ou Enterprise CA).
3. Conexões de controle: Verifique se as conexões de controle DTLS/TLS estão estabelecidas para vManage, vSmart e vBond.
4. Envio de modelo: No vManage, anexe o modelo de dispositivo ou grupo de configuração apropriado ao dispositivo.
5. Validação: Confirme se sessões BFD, rotas OMP e túneis de plano de dados estão operacionais.

Note: Após a reintegração, a licença HSEC (High Security) deve ser reaplicada manualmente via CLI para restaurar o throughput da criptografia. Conforme documentado em Gerenciamento de licenças HSEC no Cisco Catalyst SD-WAN, o SD-WAN Manager (vManage) não suporta a reinstalação de uma licença HSEC em um dispositivo. É necessário recarregar o dispositivo nos roteadores físicos para ativar a licença. Consulte Configuração da Licença HSECK9 em Cisco Edge Routers para obter o procedimento CLI manual.

Troubleshooting

Console sem resposta após reinicialização

Se o console parecer não responder após a conclusão da redefinição de fábrica, a taxa de baud provavelmente foi revertida para o padrão (9600). Ajuste o emulador de terminal para 9600 baud e reconecte.

O dispositivo não entra no ROMMON

Se o dispositivo não entrar no ROMMON após a conclusão da redefinição, verifique se o registro de configuração está definido corretamente. Na maioria dos casos, um ciclo de energia força o dispositivo a entrar no ROMMON quando nenhuma imagem inicializável estiver presente.

Variáveis de ambiente ausentes no ROMMON

Se as variáveis `MAC_ADDRESS` ou `SERIAL_NUMBER` estiverem ausentes após a redefinição, emita o comando `reset` no ROMMON para restaurar as variáveis de ambiente padrão de fábrica do

armazenamento de hardware.

Perguntas mais freqüentes

P: Por que a opção "segura" é recomendada em relação às opções padrão "todas" ou "3 etapas"?

R: A opção `fatory-reset all secure` executa a limpeza de dados mais completa disponível, alinhada com o NIST SP 800-88 Rev. 1. Ela torna os dados irrecuperáveis e retém a imagem de inicialização atual na memória flash, simplificando a recuperação. Em comparação, a opção `3 passos` executa um padrão de sobregravação de três passos (zeros, uns, aleatório) que leva aproximadamente três vezes mais tempo e também apaga a imagem de inicialização, exigindo uma recarga completa da imagem do USB ou TFTP. A opção `secure` é recomendada, pois oferece a limpeza mais completa com a menor sobrecarga operacional para recuperação.

P: Quanto tempo leva a restauração segura de fábrica?

R: A duração varia com base na capacidade total de armazenamento do dispositivo. Para dispositivos com armazenamento flash padrão (8-32 GB), o processo normalmente é concluído entre 15 e 45 minutos. Dispositivos com SSD ou armazenamento SATA maiores podem demorar mais. Importante: Não interrompa a alimentação durante esse processo. Planeje uma janela de manutenção que seja responsável pela redefinição mais o tempo de recarregamento e reintegração da imagem.

P: O dispositivo mantém sua identidade (número de série, SUDI) após a redefinição?

R: Yes. O certificado Secure Unique Device Identifier (SUDI) e suas chaves PKI associadas são armazenados em armazenamento protegido por hardware (chip TAm/ACT2) e não são apagados pela redefinição de fábrica. O número de série do dispositivo também é preservado no hardware. Isso significa que o dispositivo pode ser reintegrado à estrutura SD-WAN usando sua identidade original após a redefinição.

P: Preciso remover o dispositivo do Gerenciador de SD-WAN antes de executar a redefinição?

R: Yes. É altamente recomendável invalidar o certificado do dispositivo e remover o dispositivo da sobreposição de SD-WAN antes de executar a redefinição de fábrica. Isso garante a remoção total da infraestrutura do controlador, nenhuma entrada obsoleta no inventário de dispositivos do vManage e nenhuma conexão de controle órfã ou estado de túnel. Do vManage: Navegue até Configuration > Certificates > selecione o dispositivo > Invalidate e, em seguida, Send to Controllers. Depois, exclua o dispositivo da lista de dispositivos.

P: O que acontece com a licença HSEC após a redefinição de fábrica?

R: A licença HSEC (High Security) é removida durante a redefinição de fábrica. Sem ele, o dispositivo opera com produtividade de criptografia restrita. A licença HSEC deve ser liberada antes da redefinição de fábrica para que possa ser reutilizada posteriormente:

1. Antes de redefinir: Libere a licença por meio da `autorização inteligente de licença, volte para o local online` e remova a instância do produto da Smart License Central.
2. Após a reintegração: Reaplique manualmente a licença HSEC via CLI. Conforme documentado em Gerenciamento de licenças HSEC no Cisco Catalyst SD-WAN, o SD-WAN Manager (vManage) não suporta a reinstalação da licença HSEC.
3. Recarregar: É necessário recarregar os roteadores físicos para ativar a licença.
4. Verifique via `show license summary` e `show license authorization`.

Para obter o procedimento completo, consulte Configuração da Licença HSECK9 em Cisco Edge Routers e Gerenciamento de Licenças HSEC no Cisco Catalyst SD-WAN.

P: Posso executar a redefinição de fábrica segura remotamente (via SSH/VTY)?

R: Embora o comando possa ser emitido tecnicamente em uma sessão SSH/VTY, ele é fortemente desencorajado. O dispositivo inicia imediatamente a limpeza e a sessão remota é encerrada. Após a reinicialização, o dispositivo entra no modo ROMMON, onde não há conectividade IP disponível, nenhum acesso VTY é possível e o acesso ao console é necessário para a recuperação da imagem. Certifique-se sempre de que o acesso físico ao console esteja disponível antes de iniciar a redefinição de fábrica.

P: A redefinição de fábrica segura é apropriada para cenários de correção de segurança?

R: Yes. A reinicialização segura de fábrica é a abordagem recomendada quando um dispositivo deve ser retornado a um estado em boas condições após uma suspeita de comprometimento. Isso garante que todas as chaves, backdoors ou mecanismos de persistência plantados pelo invasor sejam permanentemente removidos, que nenhuma configuração residual ou dados de credenciais permaneçam e que o dispositivo esteja limpo para reintegração. Para redefinições de fábrica relacionadas à segurança, certifique-se de que novas credenciais (senhas, chaves, certificados) sejam geradas durante a reintegração e que nenhuma configuração de backup de pré-comprometimento seja restaurada no dispositivo.

P: Por que não usar "request platform software sdwan software reset" ou "request platform software sdwan config reset" em vez disso?

R: Esses comandos servem a uma finalidade diferente e não fornecem o mesmo nível de limpeza que `reinicializa todos os equipamentos de fábrica`. O comando `request platform software sdwan`

`software reset` redefine a sobreposição do software SD-WAN, mas não apaga as configurações, chaves, certificados ou armazenamento subjacentes do Cisco IOS XE — o dispositivo mantém seu estado de SO básico. O comando `request platform software sdwan config reset` redefine apenas a configuração SD-WAN, mas deixa a imagem do Cisco IOS XE, as credenciais locais, as chaves SSH e todos os outros dados intactos no disco. Nenhum comando executa a limpeza de dados na mídia de armazenamento. Se o objetivo for retornar o dispositivo a um estado totalmente limpo — principalmente após um incidente de segurança — esses comandos são insuficientes porque os dados residuais (chaves, credenciais, logs, arquivos plantados pelo invasor) podem permanecer na memória flash ou no SSD. Use `reinicialização de fábrica totalmente segura` quando o dispositivo tiver de estar limpo garantido no nível de armazenamento.

Referências

- Cisco Trustworthy Systems - Guia para Redefinição de Fábrica
- Configurar a licença HSECK9 nos Cisco Edge Routers
- Gerenciamento de licenças HSEC no Cisco Catalyst SD-WAN
- Gerar arquivo de bootstrap usando CLI — Guia de introdução da SD-WAN
- Atualize os controladores SD-WAN com o uso da GUI ou CLI do vManage

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.