Consultoria de segurança do Catalyst SD-WAN de correção - maio de 2026

Contents

Introdução

Este documento descreve as etapas para identificar e corrigir vulnerabilidades de segurança críticas na SD-WAN com base nos avisos da PSIRT de 14 de maio de 2026.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Componentes de arquitetura e controle do Cisco Catalyst SD-WAN (vManage, vSmart, vBond)
- Procedimento de atualização do Cisco Catalyst SD-WAN
- Gerenciamento de casos do Cisco TAC e procedimentos de coleta de tecnologia administrativa

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Para obter informações detalhadas e as atualizações mais recentes, consulte a página oficial do PSIRT Advisory.

Essas recomendações estão disponíveis nos seguintes links:

- Vulnerabilidade de desvio de autenticação do controlador Cisco Catalyst SD-WAN
- Vulnerabilidades do Cisco Catalyst SD-WAN

Esses defeitos são abordados por estes avisos PSIRT:

- ID de bug da Cisco CSCwt50498
- ID de bug da Cisco CSCwt38739
- ID de bug da Cisco CSCwt38767
- ID de bug da Cisco CSCwt55544

Visão Geral do Fluxo de Trabalho de Correção

Note: Todos os controladores e gerentes SD-WAN são vulneráveis e exigem uma atualização imediata para todos os componentes de controle. No entanto, nem todos os controladores mostram evidências de comprometimento.

Ação necessária: Colete técnicos administrativos, atualize para uma versão fixa e abra um caso no Cisco TAC para que o TAC possa verificar seus técnicos administrativos em busca de indicadores de comprometimento.

TAC disponível para:

- Verifique os técnicos de administração que você fornece para obter indicadores de comprometimento
- Fornecer suporte à atualização se você encontrar problemas durante a atualização
- Guiá-lo através de correções adicionais se forem identificados indicadores de comprometimento

1. Coletar Admin-Techs - Executar admin-tech em todos os componentes de controle (vSmart, vManage, vBond) antes da atualização para garantir que nenhum dado de diagnóstico seja

perdido. Selecione as opções Log e Tech. O núcleo não é necessário.

Caution: Os técnicos de administração do vSmart não devem ser executados simultaneamente — execute-os um de cada vez. Todos os outros podem ser coletados em qualquer ordem

2. Atualizar para uma versão fixa - Atualizar todos os componentes de controle SD-WAN (vManage, vSmart, vBond) para uma versão de software fixa listada na tabela Versões de software fixo.

Note: Não espere pelos resultados da verificação do TAC antes de atualizar. Atualizar para uma versão fixa é a prioridade mais alta e fecha a vulnerabilidade. A verificação do TAC na Etapa 3 determina se alguma ação adicional é necessária após a atualização.

3. Abra um caso de TAC e faça upload de Admin-Techs para verificar indicadores de comprometimento - Abra um caso de TAC da Cisco e faça upload de todos os pacotes de registro de admin-tech coletados na Etapa 1. O TAC verifica os admin-techs para obter indicadores de comprometimento.
4. Se o comprometimento for identificado, siga as orientações do TAC - Se o TAC identificar indicadores de comprometimento em seu ambiente, preencha todas as orientações de correção fornecidas pelo TAC. Se nenhum indicador de comprometimento for encontrado, nenhuma ação além da atualização será necessária.

Passo 1: Coletar arquivos de administração técnica de todos os componentes de controle

obrigatório: Colete arquivos admin-tech de todos os componentes de controle antes da atualização para garantir que nenhum dado de diagnóstico seja perdido. Esses arquivos são usados pelo TAC na Etapa 3 para verificar seu ambiente em busca de indicadores de comprometimento.

Coleção:

Note: Para a geração de admin-tech, selecione as opções Log and Tech (Log e Tecnologia). O núcleo não é necessário.

1. Execute o admin-tech em TODOS os controladores (vSmarts) - não execute-os simultaneamente; coletar um de cada vez
2. Execute admin-tech em TODOS os gerentes (vManages)
3. Execute admin-tech em TODOS os Validadores (vBonds)

Note: Os técnicos administrativos do vSmart não devem ser executados simultaneamente — colete-os um de cada vez. Os técnicos de administração para gerentes e validadores podem ser coletados em qualquer ordem.

Coletar um Admin-Tech no ambiente SD-WAN e fazer upload para o caso TAC

Note: O TAC analisa esses arquivos para avaliar seu ambiente em busca de indicadores de comprometimento e orientar o caminho de correção apropriado.

Alternativa: Verificação manual (somente se não for possível coletar Admin-Tech)

Para aqueles que não podem compartilhar arquivos admin-tech, as etapas de verificação manual estão disponíveis. Essas etapas fornecem indicadores preliminares que devem ser documentados e compartilhados com o TAC.

Consulte a seção "Etapas de verificação manual" no final deste documento para obter os procedimentos detalhados. Documente todas as descobertas e forneça-as ao TAC em seu caso de suporte.

Passo 2: Atualizar para uma versão de software fixo

Depois de coletar os técnicos administrativos na Etapa 1, atualize todos os componentes de controle SD-WAN (vManage, vSmart e vBond) para uma versão de software fixa.

Importante: Não espere pelos resultados da verificação do TAC antes de atualizar. Atualizar para uma versão fixa é a prioridade mais alta e fecha a vulnerabilidade. A verificação do TAC na Etapa 3 determina se alguma ação adicional é necessária após a atualização.

Selecione a versão apropriada na tabela Versões de Software Fixo neste documento.

aviso: A atualização deve permanecer na sua versão principal atual. Não atualize para uma versão principal superior sem orientação explícita do TAC.

Atualize os controladores SD-WAN com o uso da GUI ou CLI do vManage

Note: Se você encontrar algum problema durante a atualização, abra um caso no TAC para obter suporte à atualização.

Passo 3: Abra um caso no TAC e carregue os arquivos do Admin-Tech para verificação

Após a atualização na Etapa 2, abra um caso de suporte do Cisco TAC e carregue os arquivos admin-tech coletados na Etapa 1. O TAC verifica os admin-techs em busca de indicadores de comprometimento.

Ações necessárias:

1. Abra um caso TAC de Gravidade 3 com "CVE-2026-20182" e o ID PSIRT relevante no título para iniciar o processo de digitalização.
2. Carregue TODOS os pacotes de registro admin-tech coletados na Etapa 1 (Controladores, Gerentes e Validadores)
3. Aguarde o TAC concluir a verificação e comunicar os resultados

Note: O TAC analisa os arquivos admin-tech e comunica os resultados da verificação. Se nenhum indicador de comprometimento for encontrado, nenhuma ação além da atualização será necessária.

Passo 4: Se o comprometimento for identificado — siga as orientações do TAC

Se o TAC identificar indicadores de comprometimento em seu ambiente, o TAC entrará em contato com você com orientações específicas de correção. Complete todas as instruções fornecidas pelo TAC.

Se nenhum indicador de comprometimento for identificado, a atualização concluída na Etapa 2 será suficiente e nenhuma outra correção será necessária.

Versões de software fixo

Estas versões de software contêm correções para as vulnerabilidades identificadas:

Aplica-se às versões atuais	Versão Fixa	Software disponível
20.3, 20.6, 20.9	20.9.9.1	20.9.9.1 imagens de atualização para vManage, vSmart e vBond
20.10, 20.11, 20.12.5 e	20.12.5.4	20.12.5.4 imagens de atualização para

Aplica-se às versões atuais	Versão Fixa	Software disponível
anteriores em 20.12		vManage, vSmart e vBond
20.12.6.x	20.12.6.2	20.12.6.2 imagens de atualização para vManage, vSmart e vBond
20.12.7	20.12.7.1	20.12.7.1 imagens de atualização para vManage, vSmart e vBond
20.13, 20.14, 20.15.4.3 e anteriores em 20.15	20.15.4.4	20.15.4.4 imagens de atualização para vManage, vSmart e vBond
20.15.5.x	20.15.5.2	Imagens de atualização 20.15.5.2 para vManage, vSmart e vBond
20.16, 20.17, 20.18.x	20.18.2.2	20.18.2.2 imagens de atualização para vManage, vSmart e vBond

Observação: para clientes na nuvem SD-WAN (anteriormente conhecida como Cloud Delivered Cisco Catalyst SD-WAN [CDCS]), 20.15.506 também é uma versão fixa. Isso se aplica especificamente à implantação de cluster hospedado pela Cisco e é tratado separadamente do caminho de atualização padrão. Todos esses clientes já foram atualizados para a versão fixa 20.15.506.

Referências importantes:

- Matriz de atualização
- Matriz de compatibilidade do controlador

Anexo: Etapas de verificação manual (somente se a coleta de Admin-Tech não for possível)

Note: A coleta de tecnologia administrativa é o método preferido e recomendado. Use a verificação manual apenas se você absolutamente não puder coletar e compartilhar arquivos admin-tech. Se você não conseguir coletar arquivos de tecnologia administrativa, use estas etapas manuais para coletar indicadores preliminares para o TAC.

Note:

- Estas etapas fornecem apenas dados preliminares
- A coleta de tecnologia administrativa é altamente preferível para uma avaliação precisa
- Documente suas descobertas e compartilhe-as com o TAC em seu caso de suporte
- O TAC determina a avaliação oficial

Requisitos: Estas etapas devem ser executadas em todos os componentes do controle.

Verificação 1: Verificar Logons SSH Não Autorizados em Logs Auth

Passo 1: Identificar IPs válidos do sistema vManage

Acesse cada controlador vSmart e execute:

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

Saída de exemplo:

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                    PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                          PORT    PUBLIC I
-------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                          12346   10.1.10.1
```

Passo 2: Criar sequência de expressão regular (somente vBond e vSmart)

Combine todos os IPs do sistema da Etapa 1 em um padrão regex OR:

```
system-ip1|system-ip2|...|system-ipn
```

Passo 2b: Etapa adicional para sistemas vManage

Se você estiver executando esses comandos no próprio vManage, anexe o IP do localhost (127.0.0.1), o IP do sistema local, todos os IPs de cluster e o IP da interface de transporte da VPN 0 ao regex:

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

Para localizar o IP do sistema vManage local, use:

```
show control local-properties
```

Para localizar o IP da interface de transporte da VPN 0 e o IP do cluster, use:

```
show interface | tab
```

Passo 3: Executar Comando de Verificação

Execute este comando, substituindo `REGEX` pela sua string regex da Etapa 2:

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

Note: Este comando filtra logs de autenticação para mostrar apenas logons vmanage-admin de fontes inesperadas. Logons legítimos devem ser originados apenas de IPs relacionados ao vManage.

Passo 4: Interpretar resultados e documentos do TAC

Se NENHUMA saída for exibida:

- Nenhum indicador de comprometimento detectado neste dispositivo
- Documente este resultado para seu caso de TAC
- Continuar a avaliação dos controladores restantes

Se as linhas de log forem impressas:

- Examine cuidadosamente cada endereço IP mostrado
- Verifique se o IP não está relacionado à infraestrutura do vManage (IP do cluster, IP antigo do sistema ou similar)

- Se não for possível identificar o IP de origem como legítimo, isso poderá indicar possíveis indicadores de comprometimento
- A entrada de registro mostra um carimbo de data/hora e um endereço IP de origem
- Documentar todas as descobertas e abrir um caso de TAC imediatamente
- Inclua as entradas de registro, carimbos de data/hora e IPs de origem no seu caso
- O TAC executa a determinação de avaliação oficial

Verificação 2: Verificar Conexões de Peer Não Autorizadas em Syslogs de Controlador

Esse comando extrai todos os pares peer-type e peer-system-ip dos arquivos syslog do controlador e os exibe como uma lista para você revisar. Ele não sinaliza automaticamente entradas suspeitas — você deve inspecionar a saída e determinar se cada IP de sistema de peer é uma parte legítima e conhecida de sua infraestrutura de SD-WAN. Execute isso em todos os componentes de controle (Controladores, Gerenciadores e Validadores).

Passo 1: Execute o comando em cada componente de controle:

Primeiro, acesse vshell e navegue até o diretório de log:

```
vs
cd /var/log
```

Em seguida, execute este comando para pesquisar o glob de arquivo vsyslog*:

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

Repita isso para o glob de arquivos messages* e também para o glob de arquivos vdebug*.

Passo 2: Interpretar resultados e documentos do TAC

Se a saída mostrar apenas IPs de sistema vManage/vSmart/vBond conhecidos:

- Nenhum indicador de comprometimento detectado nesta verificação
- Documente este resultado para seu caso de TAC
- Continuar a avaliação dos componentes de controle restantes

Se a saída contiver IPs de sistemas pares não reconhecidos:

- Examine cuidadosamente cada endereço IP e tipo de peer mostrado
- Verifique se o IP não está relacionado à sua infraestrutura conhecida do plano de controle

da SD-WAN
- Se não for possível identificar o IP de origem como legítimo, isso poderá indicar possíveis indicadores de comprometimento
- Documentar todas as descobertas e abrir um caso de TAC imediatamente
- Inclua a saída completa do comando com pares peer-type e peer-system-ip no seu caso
- O TAC executa a determinação de avaliação oficial

Verificação 3: Verificar se há Challenge-Back Ausente em Conexões de Controle Ativas

Esta verificação inspeciona a saída de detalhes de conexões de controle para sessões pares que são relatadas como ativas (ou recentemente desativadas), mas que não têm a troca `challenge-ack` esperada. Uma sessão que troca pacotes de `hello` em ambas as direções ao mostrar `challenge-ack 0` nas estatísticas de Tx ou Rx indica que o peer nunca concluiu o handshake de desafio esperado — uma anomalia que justifica investigação. Execute isso em todos os componentes de controle (Controladores, Gerenciadores e Validadores).

Passo 1: Coletar a saída dos detalhes das conexões de controle

Na CLI do dispositivo, execute:

```
show control connections detail
show control connections-history detail
```

Salve a saída em um arquivo (por exemplo, `vdaemon.txt`) para inspeção.

Passo 2: O que procurar

Para cada registro de peer (delimitado por cabeçalhos `REMOTE-COLOR-` / `SYSTEM-IP-`), sinalize o registro se `todas` essas condições forem verdadeiras:

- O estado da sessão é UP ou TEAR_DOWN
- O contador hello das estatísticas de transmissão e o contador hello das estatísticas de recepção são diferentes de zero (os hellos estão fluindo em ambas as direções)
- challenge-ack é 0 no bloco Tx Statistics ou Rx Statistics (ou ambos)

Exemplo de registro correspondente (observe as setas `<<<` que destacam o `desafio-ack` ausente)

```
----------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
----------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
```

```
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
    ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

No exemplo acima, os contadores de `hello` de Tx e Rx são diferentes de zero (conexão ativa), mas `challenge-ack` é `0` em ambas as direções.

Passo 3: Comando de pesquisa manual

Para exibir rapidamente os registros de candidato de um `vdaemon.txt` salvo (ou qualquer arquivo que contenha a saída `show control connections detail`), execute:

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

Cada bloco retornado representa uma sessão de peer em que challenge-ack é relatado como 0. Revise cada bloco na íntegra para confirmar se o estado é up ou tear_down e que os contadores hello em Tx e Rx são diferentes de zero antes de tratá-lo como um acerto.

Passo 4: Interpretar resultados e documentos do TAC

Se nenhum registro atender às três condições:

- Nenhum indicador de comprometimento detectado nesta verificação
- Documente este resultado para seu caso de TAC
- Continuar a avaliação dos componentes de controle restantes

Se um ou mais registros atenderem às três condições:

- Examine cuidadosamente os valores de `SYSTEM-IP-`, `private-ip` e `public-ip` para cada registro sinalizado
- Verifique se o peer não é uma parte legítima conhecida do plano de controle da SD-WAN (membro do cluster, local DR, endereço IP atribuído anteriormente a um componente)

- Se você não puder identificar o peer como legítimo, isso pode indicar possíveis indicadores de comprometimento
- Documentar todas as descobertas e abrir um caso de TAC imediatamente
- Inclua o(s) registro(s) correspondente(s) completo(s) e a saída do comando source no seu caso
- O TAC executa a determinação de avaliação oficial

Perguntas mais freqüentes

P: Qual é a primeira etapa para lidar com esse consultivo de segurança?

R: Colete arquivos admin-tech de todos os componentes de controle e atualize todos os componentes de controle para uma versão de software fixa. Após a atualização, abra um caso de TAC e carregue os técnicos de administração para que o TAC possa verificar seu ambiente em busca de indicadores de comprometimento.

P. Para qual versão preciso fazer upgrade?

R. Atualize para a versão fixa mais próxima o mais cedo possível.

P: Preciso coletar técnicos de administração de todos os componentes do controle?

R: Sim, o TAC exige arquivos técnicos de administração de todos os controladores (vSmart, coletados um de cada vez), todos os gerentes (vManage) e todos os validadores (vBond) para avaliar corretamente seu ambiente.

P: Como o TAC determina se meu sistema foi comprometido?

R: O TAC analisa os arquivos administrativos e técnicos usando ferramentas especializadas para avaliar seu ambiente em busca de indicadores de comprometimento.

P: Há uma maneira de executar minha própria verificação automática usando as ferramentas do TAC?

R: Os clientes também podem usar a ferramenta self-service "Check Bug Applicability" que está incorporada na página da ferramenta de pesquisa de bugs para a identificação de bug Cisco CSCwt50498 para verificar novamente os admin-techs dos componentes de controle.

P: O que acontece se forem identificados indicadores de comprometimento?

R: O TAC entra em contato com você para discutir as próximas etapas e orientações específicas ao seu ambiente. A Cisco não executa a correção em seu nome — O TAC fornece as orientações necessárias para que você prossiga.

P: Como posso saber qual versão de software fixa usar?

R: Consulte a tabela Versões Fixas de Software neste documento. O TAC confirma a versão apropriada para seu ambiente específico.

P: Posso iniciar a atualização antes que o TAC analise meus técnicos de administração?

R: Yes. Colete os técnicos administrativos, atualize para uma versão fixa e abra um caso no TAC para que o TAC possa verificar os técnicos administrativos em busca de indicadores de comprometimento.

P: O tempo de inatividade é esperado durante a correção?

R: O impacto depende da sua arquitetura de implantação e do caminho de correção. O TAC fornece orientação sobre como minimizar o impacto do serviço durante o processo.

P: Todos os controladores precisam ser atualizados caso nenhum indicador de comprometimento seja encontrado?

R: Sim, todos os componentes de controle da SD-WAN (vManage, vSmart e vBond) devem ser atualizados para uma versão de software fixa. A atualização de apenas um subconjunto de controladores não é suficiente.

P: Tenho uma sobreposição de SD-WAN hospedada na nuvem. Quais são minhas opções de atualização?

R: Para sobreposições hospedadas na nuvem, os clientes têm duas opções:

1. Verifique se o ambiente está agendado para uma atualização automática navegando até SSP > Detalhes de Sobreposição > Alterar Janelas.
2. Se você não quiser esperar pela atualização agendada, terá duas opções:
    - Atualize você mesmo usando os guias de atualização disponíveis neste documento.
    - Abra um caso TAC de espera para a janela de manutenção de sua preferência. O TAC está disponível para ajudá-lo se você encontrar dificuldades com a atualização.

P: Precisamos atualizar os roteadores de borda também?

R: Não, os dispositivos Cisco IOS XE não são afetados por este aviso.

P: Somos uma sobreposição hospedada pela Cisco. Precisamos corrigir alguma ACL ou executar uma ação no SSP?

R: Todos os clientes hospedados pela Cisco são aconselhados a revisar suas próprias regras de entrada permitidas vistas no SSP e garantir que somente os prefixos necessários do seu lado sejam permitidos. Essas regras são apenas para acesso de gerenciamento e não se aplicam a roteadores de borda. Revise-os em SSP > Detalhes de sobreposição > Permitir regras de entrada. Observe que a porta 22, 830 sempre foi bloqueada por padrão no provisionamento do dia 0 pela Cisco de fora para os controladores hospedados na nuvem.

P: Estamos na nuvem SD-WAN (anteriormente conhecida como nuvem distribuída Cisco Catalyst SD-WAN [CDCS]). Para qual versão nós vamos ser atualizados?

R: Com base na versão atual, os clusters de nuvem SD-WAN estão atualmente no cronograma para serem atualizados OU já foram atualizados para as versões fixas. Estas são as versões fixas

da SD-WAN Cloud (anteriormente CDCS):

1. Clusters Early Adoter = 20.18.2.2 (isso é realmente o mesmo que a versão padrão)

2. Clusters de versão recomendados = 20.15.506 (versão específica dos CDCS com correções PSIRT)

Os clientes de nuvem de SD-WAN não precisam tomar nenhuma ação de forma eficaz para lidar com essa PSIRT.

P: Estamos no espaço Compartilhado. Para qual versão nós vamos ser atualizados?

R: Com base na versão atual, os Locatários Compartilhados estão atualmente no cronograma para serem atualizados OU já foram atualizados para as versões fixas. Estas são as versões fixas do espaço compartilhado:

1. Clusters de versão recomendados = 20.15.5.2

P: O Cisco TAC oferece análise forense ou serviços de investigação para essas vulnerabilidades?

R: O Cisco TAC pode ajudar os clientes verificando os Indicadores de comprometimento (IoCs) relacionados a essas vulnerabilidades. No entanto, o TAC não realiza análises forenses detalhadas ou investigações de incidentes. Para um trabalho de computação forense abrangente ou investigações de segurança detalhadas, recomendamos que os clientes envolvam a empresa de terceiros de resposta a incidentes (IR) de sua preferência.

P: Quais são as melhores práticas gerais ou maneiras de reduzir as vulnerabilidades da minha sobreposição de SD-WAN?

R: Consulte o Guia de Proteção de SD-WAN do Cisco Catalyst para obter as melhores práticas e recomendações para reduzir as vulnerabilidades na sobreposição de SD-WAN.

P: Vemos logs de um usuário "raiz" em nosso sistema. Isso é preocupante?

R: Verifique o que mais está acontecendo no sistema no momento. Esses registros podem ser completamente esperados. Por exemplo, os logs de alteração de login do sistema de um usuário "raiz" são vistos quando os técnicos de administração são gerados. Os logs também podem ser vistos de um usuário "root" durante uma reinicialização.

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

       user-name:"root" user-id:245  generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

        user-name:"root" user-id:248  generated-at:2-28-2026T23:3:47
```

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.