Resolver falhas de validação de certificado do IOS XE devido à incompatibilidade de URL do CDP com URL de download de CRL múltiplo

Contents

Problema

Depois que locais adicionais de URL de download de CRL são adicionados a um dispositivo de hub de VPN Multiponto Dinâmica (DMVPN), alguns túneis spoke não conseguem estabelecer devido à falha de negociação de IKE e o hub registrou este erro:

```
%PKI-3-CERTIFICATE_INVALID: Certificate chain validation has failed
```

Embora a validação da cadeia de certificados seja bem-sucedida e as CRLs sejam baixadas com êxito, a verificação de revogação falha intermitentemente com:

```
No CRL found with matching CDP
revocation status = 2
```

Esse problema ocorre quando o roteador de hub DMVPN usa vários locais de URL de download de CRL (Certificate Revocation List, Lista de revogação de certificados) apontando para o mesmo arquivo de CRL. Os locais de download de CRL incluem URLs baseadas em IP e em FQDN, enquanto o certificado emitido para os roteadores spoke tem apenas a URL baseada em FQDN em seu Ponto de Distribuição de CRL (CDP).

Ambiente

- Dispositivos Cisco que executam o software IOS® XE configurado para IPsec usando autenticação IKE baseada em certificado.

- Vários locais de download de CRL com URLs baseadas em IP e em FQDN hospedando os mesmos arquivos de CRL.
- O certificado emitido para os dispositivos pares tem apenas uma URL em seu CDP.
- Configuração de túnel IPsec usando autenticação baseada em certificado ao impor verificação de revogação de certificado.

Resolução

A resolução envolve a padronização de um único URL CDP canônico em todo o ambiente PKI para garantir a correspondência exata do URL durante a validação da CRL.

Etapas de Implementação Recomendadas

1. Remova os URLs de Download de CRL Baseada em IP da Configuração do Hub, se esses URLs de CRL Baseada em IP não fizerem parte do CDP do Certificado

```
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA1.crl
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA2.crl
```

2. Configure somente URLs de Download de CRL com base em FQDN que Correspondam ao CDP nos Certificados Spoke

```
crypto pki crl download url http://crl.examplecompnay.com/prod/Example%20Company%20Issuing%20CA1.crl
crypto pki crl download url http://crl.examplecompany.com/prod/Example%20Company%20Issuing%20CA2.crl
```

3. Atualizar Modelos de CA Emissora para Usar URLs CDP Consistentes

Certifique-se de que os modelos de autoridade de certificação emissora carimbem somente a URL do CDP baseado em FQDN em certificados recém-emitidos.

4. Registre novamente os certificados de hub e spoke (se for alterado para o novo URL do CDP)

Se estiver implementando um novo URL CDP, altere a CA emissora para publicar o novo URL CDP e reinscreva os certificados hub e spoke para transportar o novo URL.

Implementação de redundância

Para redundância do provedor de CRL, por exemplo, para ter a mesma CRL publicada em diferentes locais de URL para proteger contra falhas nos dispositivos de hospedagem, implemente a redundância de back-end por trás de um único FQDN usando:

- failover de DNS
- Balanceador de carga
- Infraestrutura de CRL redundante

Não use vários CDPs com nomes de host/IPs diferentes, pois o IOS XE os trata como CDPs diferentes, mesmo que façam referência ao mesmo arquivo de CRL.

Verificação

Depois de implementar as alterações, verifique o cache da CRL e o estabelecimento do túnel:

```
show crypto pki crl
```

Confirme se a sessão IKEv2 foi estabelecida com êxito:

```
show crypto session details
```

Causa

O problema é causado pelo comportamento de correspondência exata do URL do CDP do IOS XE durante a validação da CRL. Ao validar um certificado de mesmo nível com a verificação de revogação crl habilitada, o IOS XE executa uma correspondência exata de string entre o URL do CDP incorporado no certificado que está sendo validado e o URL do CDP associado ao CRL armazenado no cache CRL analisado do hub.

Esta sequência de falha ocorre:

1. O hub faz o download com êxito da CRL usando o URL do CDP baseado em IP e faz o cache dela internamente nesse URL.
2. Os certificados spoke fazem referência à URL baseada em FQDN em seu CDP.
3. Durante a validação da revogação, o IOS XE procura uma CRL em cache que corresponda à URL do FQDN.
4. Nenhuma correspondência exata foi encontrada porque o IOS XE trata URLs baseadas em IP e em FQDN como CDPs diferentes.
5. O roteador retorna "Nenhuma CRL encontrada com CDP correspondente" com status de revogação = 2.
6. Falha na validação do certificado com %PKI-3-CERTIFICATE_INVALID.

O IOS XE não normaliza formatos de URL diferentes (IP vs. FQDN) como equivalentes, mesmo quando ambos retornam conteúdo CRL idêntico para o mesmo emissor.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

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.