解決由於多個CRL下載URL的CDP URL不匹配而導致的IOS XE證書驗證失敗

目錄

問題

將附加CRL下載URL位置新增到動態多點VPN(DMVPN)中心裝置後，由於IKE協商失敗，某些分支隧道無法建立，並且中心記錄以下錯誤：

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

雖然證書鏈驗證成功且成功下載CRL，但吊銷檢查間歇性失敗，原因如下：

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

當DMVPN中心路由器使用指向同一CRL檔案的多個證書撤銷清單(CRL)下載URL位置時，會出現此問題。CRL下載位置包括基於IP和基於FQDN的URL，而向分支路由器頒發的證書在其CRL分發點(CDP)中僅具有基於FQDN的URL。

環境

- 運行IOS® XE軟件的Cisco裝置，使用基於證書的IKE身份驗證為IPsec配置。
- 多個CRL下載位置，具有託管相同CRL檔案的基於IP和基於FQDN的URL。
- 向對等裝置頒發的證書在其CDP中只有一個URL。
- 實施證書撤銷檢查時使用基於證書的身份驗證的IPsec隧道配置。

解析

解決方法涉及在PKI環境中對單個規範CDP URL進行標準化，以確保在CRL驗證期間進行準確的URL匹配。

建議實施步驟

1.如果基於IP的CRL URL不是證書CDP的一部分，請從集線器配置中刪除基於IP的CRL下載URL

```
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.僅配置與分支證書中的CDP匹配的基於FQDN的CRL下載URL

```
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.更新發佈CA模板以使用一致的CDP URL

確保頒發的CA模板僅將基於FQDN的CDP URL戳記到新頒發的證書中。

4.重新註冊中心輻射型證書（如果更改為新的CDP URL）

如果實施新的CDP URL，請更改發佈CA以發佈新的CDP URL，並重新註冊中心及分支證書以攜帶新的URL。

冗餘實施

例如，要使CRL提供程式冗餘在不同的URL位置發佈相同的CRL以防止託管裝置發生故障，請使用以下方式在單個FQDN後面實施後端冗餘：

- DNS故障轉移
- 負載均衡器
- 冗餘CRL基礎架構

請勿使用具有不同主機名/IP的多個CDP，因為IOS XE會將其視為不同的CDP，即使它們引用相同的CRL檔案也是如此。

驗證

實施更改後，驗證CRL快取和隧道建立：

```
show crypto pki crl
```

確認IKEv2會話建立成功：

```
show crypto session details
```

原因

此問題是由於CRL驗證期間IOS XE精確CDP URL匹配行為引起的。當驗證啟用了撤銷檢查crl的對等證書時，IOS XE會在被驗證證書中嵌入的CDP URL與儲存在集線器的已分析CRL快取中的CRL相關聯的CDP URL之間執行完全字串匹配。

出現以下故障序列：

1. 集線器使用基於IP的CDP URL成功下載CRL，並在該URL下將其內部快取。
2. 分支證書在其CDP中引用基於FQDN的URL。
3. 在吊銷驗證期間，IOS XE會搜尋與FQDN URL匹配的快取CRL。
4. 找不到完全匹配項，因為IOS XE將基於IP和基於FQDN的URL視為不同的CDP。
5. 路由器返回「未找到與匹配CDP的CRL」，撤銷狀態= 2。
6. 證書驗證失敗，出現%PKI-3-CERTIFICATE_INVALID。

IOS XE不會將不同的URL格式（IP與FQDN）規範化為等效格式，即使兩個格式都返回同一頒發者的相同CRL內容時也是如此。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。