

排除Umbrella ISR4k整合故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[註冊和證書匯入](#)

[驗證證書匯入和裝置註冊](#)

[偵錯和記錄](#)

簡介

本文檔介紹如何對Umbrella ISR4k整合進行故障排除

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

本文是[Cisco Umbrella Integration for ISR4k部署指南](#)的繼續，旨在幫助您解決註冊問題，以及解決內部和外部DNS解析問題。



附註：2024年5月29日為api.opendns.com續簽的證書現在由新的鏈/中介軟體/根簽署。新的根是DigiCert全域性根G2(串列：033af1e6a711a9a0bb2864b11d09fae5)。

註冊和證書匯入

- 1.從Umbrella儀表板獲取API令牌：Admin > API Keys >(create)Legacy Network Devices。
- 2.使用以下方法之一，通過CLI將CA證書匯入ISR4k:

從URL匯入：

發出命令並允許ISR4k提取證書：

```
crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

直接在終端中匯入：

使用以下命令複製並貼上CA憑證（請參閱附件）：

(此證書用於DigiCert全域性根G2。)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHqn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDEuMjA4MDEuMjA4MDEuMjA4MDEuMjA4MDEuMjA4MDEuMjA4MDEu
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYWwgY290IEcyMIIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNnN7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmVPrC3oXgkRRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sHON03Xss0r0upS/kqbit0tSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNjbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsPuwTf1MvYwnSlcuFIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPzZFBQ9RnbDhxSJITRnrw9FDKZJobq7nMwxM4MphQIDAQABO0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkWdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNu+MeKNh7jitra1j41E6Vf8P1wUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj1ldiGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTf1
MrY=
-----END CERTIFICATE-----
```

使用命令複製並貼上中間證書：

(此證書適用於DigiCert Global G2 TLS RSA SHA256 2020 CA1。)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEYDCCA7CgAwIBAgIQDPW9BiTWAuR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NTlaMFkxCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYWwgY290IEcyMIIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNnN7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmVPrC3oXgkRRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sHON03Xss0r0upS/kqbit0tSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNjbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsPuwTf1MvYwnSlcuFIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPzZFBQ9RnbDhxSJITRnrw9FDKZJobq7nMwxM4MphQIDAQABO0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkWdQYJKoZIhvcNAQELBQADggEPADCCAQoCggEBAMz3EGJPr
tjb+2QU1bFbSd7ehJWivH0+dbn4Y+9lavyYEEVcNsSAPonCrVX0Ft9s1GTcZUoakGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDy
FuqrIvAxIhFhaZamunjZlx/jfWardUSVc8is/+9dCopZQ+GssjoP80j812s3wWPc
3kbw20X+fSP9k0hRBx5Ro1/tSUZufyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8
osicfebUTVsVqpmowQTCd5zWS0TOEeAggJnwQ3DPP3Zr0UxJqyRwg2C/Uaoq2yT
zGJSQnWS+Jr6X16ysGH1Hx+5fwmY6D36g39HaaECAwEAAOCAYIwggF+MBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVRO0BBYEFHSFgMBmx9833s+9KTeqAx2+7c0XMB8G
A1UdIwQYMBaAFE4iVCAY1ebjbuYP+Vq5Eu0GF485MA4GA1UdDwEB/wQEAwIBhjAd
BgNVHUSUEFjAUBGgrBgEFBQCDAQYIKwYBBQUHAWIwdgYIKwYBBQUHAQEaJBoMCQG
CCsGAQUFBzABhhodHRwOi8vb2Nzc5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
NGh0dHA6Ly9jYWNlcnRzLmRwZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RHM
i5jcnQwQgYDVRO0BFDswOTA3oDwgM4YxaHR0cDovL2NybdMuZGlnaWNlcnQuY29t
```

```
LORpZ21DZXJ0R2xvYmFsUm9vdEcyLmNybdA9BgNVHSAENjA0MA5GCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAGewCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAA0CAQEAKPFwyyiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWkOH7U1MV1+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
s1me5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZm0pGrFmCW3R
bpD0ufovARTFXfZkAd19h6g4U5+LXUZtXMYnhIHUfoym05tS58aI7Dd8KvvwVVo4
chDYABPPTHPbjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3.使用命令輸入ISR4k CLI的API令牌：

```
parameter-map type umbrella global
token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

4.這是ISR4k上的最低配置示例：

```
interface GigabitEthernet0/0/0
ip address 192.168.50.249 255.255.255.252
ip nat outside
umbrella out

interface GigabitEthernet0/0/1.10
encapsulation dot1Q 10
ip address 192.168.8.254 255.255.255.0
ip nat inside
umbrella in odns_v10_5
```

Additional Information:

- 確保在「umbrella in」指令之前設定「umbrella out」。
- 僅當埠443處於開啟狀態並允許流量通過任何現有防火牆時，才能成功註冊。
- 在舊版Cisco IOS XE Denali中，使用OpenDNS命令而不是Umbrella。

驗證證書匯入和裝置註冊

1.驗證CA證書是否已成功儲存在ISR4k裝置上：

- 如果使用URL完成了憑證匯入，請發出命令dir nvram:驗證ios.p7b證書是否成功儲存在裝置NVRAM中。

```

[ISR4k02-CWSSDMLAB#dir nvram:ter is 0x2102
Directory of nvram:/
Standby not ready to show bootvar

32769 -rw- isr4k.pod3#sh 3086 inc boot system <no date> startup-config
32770 ---- boot system bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin
32771 -rw- boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin
32771 -rw- isr4k.pod3#conf 3086 <no date> underlying-config
1 ---- Enter configuration commands, one per line. End with CNTL/Z.
1 ---- isr4k.pod3(config) 426 <no date> persistent-data
2 -rw- isr4k.pod3(config) 1182 no boot system <no date> ISR4451-X-4x1GE_0_0_0
4 -rw- isr4k.pod3(config) 17 boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin
5 -rw- boot system bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.t
5 -rw- isr4k.pod3(config) 0 do sh run | inc boot system <no date> ifIndex-table
6 -rw- boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin
8 -rw- boot system bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.t
8 -rw- isr4k.pod3(config) 793 <no date> QuoVadisRoot#D3ACCA.cer
9 -rw- isr4k.pod3(config) 791 <no date> CiscoECCRoot#2CA.cer
10 -rw- isr4k.pod3(config) 1697 <no date> CiscoRootCAM#1CA.cer
12 -rw- Building configuration... <no date> QuoVadisRoot#5C6CA.cer
14 -rw- [OK] 1467 <no date> CiscoRootCA2#CCA.cer
16 -rw- isr4k.pod3#sh bootvar 825 <no date> QuoVadisRoot#509CA.cer
17 -rw- BOOT variable = bootflash:isr4300-universalk9.16.03.03.SPA.bin,12 bootflash:isr4300-universa
18 -rw- CONFIG_FILE variable does not exist <no date> CiscoRXC-R2#1CA.cer
18 -rw- BOOTLDR variable does not exist <no date> CiscoECCRoot#1CA.cer
19 -rw- Configuration register is 0x2102 <no date> DSTRootCA#3406BCA.cer
21 -rw- Standby not ready to show bootvar <no date> QuoVadisRoot#508BCA.cer
22 -rw- isr4k.pod3#rel 1176 <no date> CiscoLicensi#1CA.cer
24 -rw- 2945 <no date> DigiCertGlob#BC91CA.cer
27 -rw- 146259 <no date> cwmp_inventory
ios.p7b

```

115016968663

- 如果使用copy/paste方法完成了證書匯入，請運行命令show cry pki trustpool並驗證證書的序列號和cn:

```

#sh umbrella deviceid
Device registration details
Interface Name      Tag      Status      Device-id
GigabitEthernet0/0/1 111.111.111.111/ 200 SUCCESS  010a9e60fe3b4689

#sh crypto pki trustpool | inc Digi
cn=DigiCert Global Root G2
o=DigiCert Inc
cn=DigiCert Global Root G2
o=DigiCert Inc
cn=DigiCert Global Root CA
o=DigiCert Inc
cn=DigiCert Global Root CA
o=DigiCert Inc
cn=DigiCert Global Root CA
o=DigiCert Inc
cn=DigiCert TLS RSA SHA256 2020 CA1
o=DigiCert Inc
http://crl3.digicert.com/DigiCertGlobalRootCA.crl
http://crl4.digicert.com/DigiCertGlobalRootCA.crl

```

28552066223252

2.要驗證ISR4k註冊是否成功，請運行命令show umbrella deviceid。

輸出示例：

Device registration details

Interface Name	Tag	Status	Device Id
interface GigabitEthernet0/0/1.10	odns_v10_5	200 SUCCE	010a04efd4e4bc14
interface GigabitEthernet0/0/1.11	odns_v11	200 SUCCE	010a04efd4e4xy15

儀表板輸出：

Devices GET MY API TOKEN			
Device Name	Serial Number	Primary Policy	Status
 odns-isr-odnsin_v11	FLM2006W0MZ	ISR VLAN 11	
 odns-isr-odns_v10_5	FLM2006W0MZ	ISR VLAN 10	

115016791766

偵錯和記錄

- 驗證ISR4k版本：show version或show platform (所需的Cisco IOS XE Denali 16.3或更高版本)
- 啟用裝置註冊調試日誌："debug umbrella device-registration" , 然後"show logging"(禁用 — no debug umbrella device-registration)

以下是示例日誌：

缺少證書：

Jun 13 04:05:32.639: %OPENDNS-3-SSL_HANDSHAKE_FAILURE: SSL handshake failed

已安裝證書並且裝置已成功註冊：

%%PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS: Trustpool Download is successful
%%OPENDNS-6-DEV_REG_SUCCESS: Device id for interface/tag GigabitEthernet0/0/1/odns_v10_5 is 010a0e4bc14

Api.opendns.com無法解析：

<#root>

%%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- 驗證DNS解析：ISR4k上沒有「dig」或「nslookup」命令可用。最好從ISR4k CLI使用「ping hostname source interface #」
- 配置了VRF的ISR:在介面上，確保已設定「ip name-server vrf <vrf_name> <dns_server_ip>」，並使用「ping vrf <vrf_name> api.opendns.com」進行驗證
- 確保配置了「ip dns server」：這允許直接查詢ISR。
- 要禁用DNSEncrypt，請輸入以下命令：parameter-map type umbrella global > no dnscrypt
- 內部域驗證：運行show umbrella config命令並查詢本地域正規表示式，例如：
 - show umbrella config > Local Domain Regex parameter-map:dns bypass
 - show run | be dns_bypass
 - show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list
- 無法使用URL匯入證書，或者使用終端匯入的證書在重新啟動後被刪除：

```
crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

```
% Error: failed to open file.
```

```
% No certificates imported from http://www.cisco.com/security/pki/trs/ios.p7b.
```

解決方法：通過curl手動下載「ios.p7b」證書捆綁包，並將其複製到路由器的快閃記憶體>從池中清除現有證書>從快閃記憶體匯入「ios.p7b」證書捆綁包：

```
<#root>
```

```
Show run | sec crypto pki
```

```
crypto pki certificate pool
```

```
cabundle nvram:Trustpool15.cer
```

```
crypto pki trustpool clean
```

```
crypto pki trustpool import url flash:ios.p7b
```

```
Reading file from bootflash:ios.p7b
```

```
% PEM files import succeeded.
```

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）。