排除Umbrella ISR4k集成故障

目录

简介

本文档介绍如何对Umbrella ISR4k集成进行故障排除

先决条件

要求

本文档没有任何特定的要求。

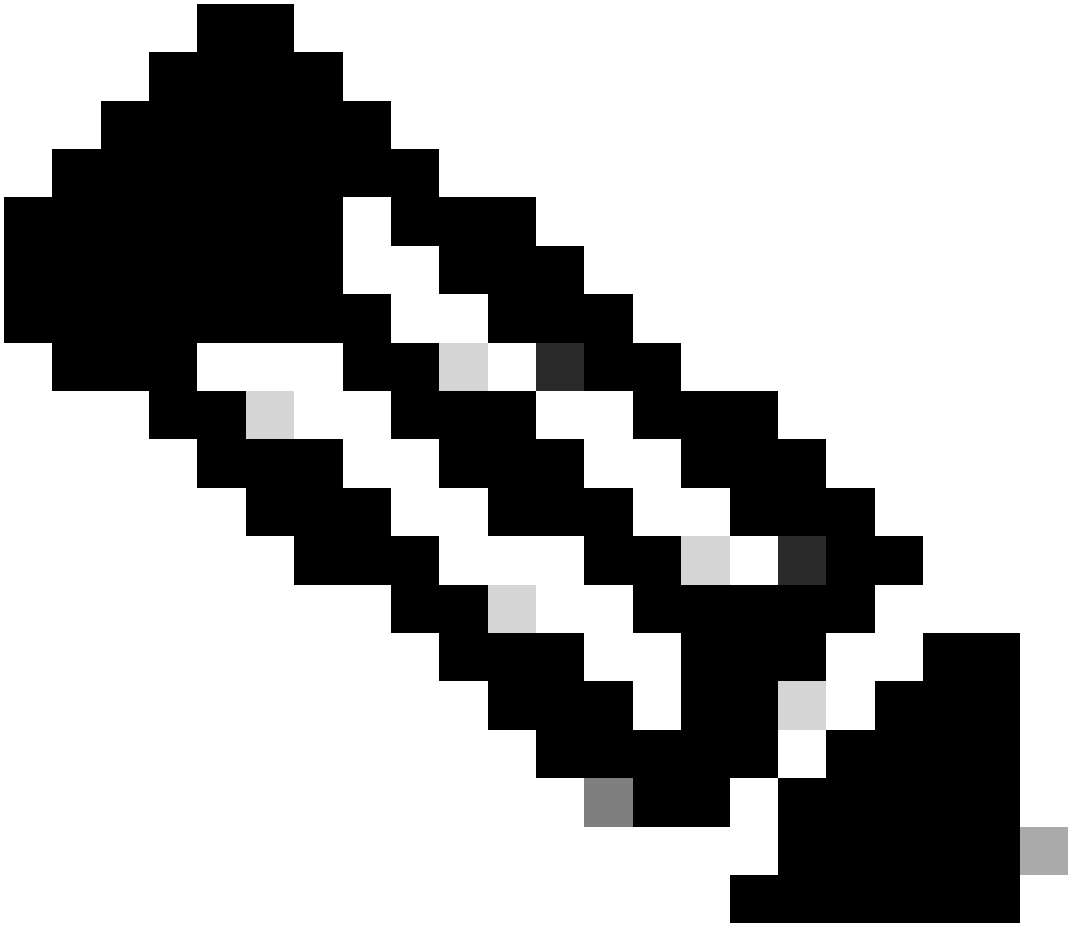
使用的组件

本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

本文是适用于ISR4k的Cisco Umbrella Integration部署指南的延续，可作为帮助解决注册问题以及内部和外部DNS解析问题的指南。



注意：2024年5月29日为api.opendns.com续订的证书现在由新的链/中间体/根证书签署。新的根是DigiCert全局根G2(串行：033af1e6a711a9a0bb2864b11d09fae5)。

注册和证书导入

1.从Umbrella控制面板获取您的API令牌：Admin > API Keys >（创建）Legacy Network Devices。

2.使用以下任一方法，通过CLI将CA证书导入ISR4k:

从URL导入：
发出命令并允许ISR4k获取证书：

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

直接在终端中导入：
使用命令复制并粘贴CA证书（请参阅附件）：

(此证书用于DigiCert Global Root G2。)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuumO6ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
-----END CERTIFICATE-----
```

使用命令复制并粘贴中间证书：

(此证书适用于DigiCert Global G2 TLS RSA SHA256 2020 CA1。)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEyDCCA7CgAwIBAgIQDPW9BitWAvR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NTlaMFkxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxMzAxBgNVBAMTKkRpZ2lDZXJ0IEdsb2Jh
bCBHMiBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMz3EGJPprtjb+2QUlbFbSd7ehJWivH0+dbn4Y+9lavyYEEV
cNsSAPonCrVXOFt9slGTcZUOakGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDy
FuqrIvAxIhFhaZAmunjZlx/jfWardUSVc8is/+9dCopZQ+GssjoP8Oj812s3wWPc
3kbW2OX+fSP9kOhRBx5Ro1/tSUZUfyyIxfQTnJcVPAPooTncaQwywa8WV0yUROJ8
osicfebUTVSvQpmowQTCd5zWSOTOEeAqgJnwQ3DPP3ZrOUxJqyRewg2C/Uaoq2yT
zGJSQnWS+Jr6Xl6ysGHlHx+5fwmY6D36g39HaaECAwEAAaOCAYIwggF+MBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFHSFgMBmx9833s+9KTeqAx2+7c0XMB8G
A1UdIwQYMBaAFE4iVCAYlebjbuYP+vq5EuOGF485MA4GA1UdDwEB/wQEAwIBhjAd
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYIKwYBBQUHAQEEajBoMCQG
CCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
NGh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuZGlnaWNlcnQuY29t
```

```
L0RpZ2lDZXJ0R2xvYmFsUm9vdEcyLmNybDA9BgNVHSAENjA0MAsGCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAgEwCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAAOCAQEAkPFwyyiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWkOH7U1MVl+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
slme5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZmOpGrFmCW3R
bpDOufovARTFXFZkAdl9h6g4U5+LXUZtXMYnhIHUfoyMo5tS58aI7Dd8KvvwVVo4
chDYABPPTHPbqjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3.使用命令输入ISR4k CLI的API令牌：

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

4.这是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
```

其它信息：

- 确保在“umbrella in”命令之前配置“umbrella out”。
- 只有当端口443处于打开状态并允许流量通过任何现有防火墙时，才能成功注册。
- 在旧版Cisco IOS XE Denali中，使用OpenDNS命令而不是Umbrella。

验证证书导入和设备注册

1.验证CA证书是否已成功存储在ISR4k设备上：

- 如果使用URL完成了证书导入，请发出命令`dir nvram:`验证ios.p7b证书是否成功存储在设备NVRAM中。

```
ISR4k02-CWSSDMLAB#dir nvram:
Directory of nvram:/

32769  -rw-        3086                    <no date>  startup-config
32770  ----        3582                    <no date>  private-config
32771  -rw-        3086                    <no date>  underlying-config
    1  ----         426                    <no date>  persistent-data
    2  -rw-        1182                    <no date>  ISR4451-X-4x1GE_0_0_0
    4  -rw-          17                    <no date>  ecfm_ieee_mib
    5  -rw-           0                    <no date>  ifIndex-table
    6  -rw-        1736                    <no date>  QuoVadisRoot#D3ACCA.cer
    8  -rw-         793                    <no date>  CiscoECCRoot#2CA.cer
    9  -rw-         791                    <no date>  CiscoRootCAM#1CA.cer
   10  -rw-        1697                    <no date>  QuoVadisRoot#5C6CA.cer
   12  -rw-        1088                    <no date>  CiscoRootCA2#CCA.cer
   14  -rw-        1467                    <no date>  QuoVadisRoot#509CA.cer
   16  -rw-         825                    <no date>  CiscoRXC-R2#1CA.cer
   17  -rw-         464                    <no date>  CiscoECCRoot#1CA.cer
   18  -rw-         846                    <no date>  DSTRootCAX3#406BCA.cer
   19  -rw-        1492                    <no date>  QuoVadisRoot#508BCA.cer
   21  -rw-         805                    <no date>  CiscoLicensi#1CA.cer
   22  -rw-        1176                    <no date>  DigiCertGlob#BC91CA.cer
   24  -rw-        2945                    <no date>  cwmp_inventory
   27  -rw-      146259                    <no date>  ios.p7b
```

115016968663

- 如果使用copy/paste方法完成了证书导入，请运行命令`show cry pki trustpool`，并验证证书的序列号和cn:

```
#sh umbrella deviceid
Device registration details
Interface Name          Tag                 Status          Device-id
GigabitEthernet0/0/1    [redacted]          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.要验证ISR4k是否成功注册，请运行`show umbrella deviceid`命令。

示例输出：

```
Device registration details

Interface Name                          Tag            Status       Device Id

interface GigabitEthernet0/0/1.10     odns_v10_5     200 SUCCES    010a04efd4e4bc14

interface GigabitEthernet0/0/1.11     odns_v11       200 SUCCES    010a04efd4e4xy15
```

控制面板输出：

115016791766

调试和日志记录

- 验证ISR4k版本：`show version`或`show platform`（所需的Cisco IOS XE Denali 16.3或更高版本）
- 启用设备注册调试日志："`debug umbrella device-registration`"然后"`show logging`"(要禁用 — `no debug umbrella device-registration`)

以下是示例日志：

证书丢失：

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

证书已安装，设备已成功注册：

```
*%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无法解析：

<#root>

*%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- 验证DNS解析：ISR4k上没有“dig”或“nslookup”命令可用。 最好从ISR4k CLI使用“ping hostname source interface #”
- 配置了VRF的ISR:在接口上，确保配置了“ip name-server vrf <vrf_name> <dns_server_ip>”，并使用“ping vrf <vrf_name> api.opendns.com”进行验证
- 确保配置了“ip dns server”：这允许直接查询ISR。
- 要禁用DNSCrypt，请输入以下命令：parameter-map type umbrella global > no dnscrypt
- 内部域验证：运行命令show umbrella config并查找本地域正则表达式，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
- 无法使用URL导入证书，或者使用终端导入的证书在重新启动后被删除：

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.

解决方法：通过curl手动下载“ios.p7b”证书捆绑包并将其复制到路由器的闪存>从池中清除现有证书>从闪存导入“ios.p7b”证书捆绑包：

<#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.

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。