

Solución de problemas de integración de Umbrella ISR4k

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Registro e importación de certificados](#)

[Verificación de la importación del certificado y el registro del dispositivo](#)

[Depuración y registro](#)

Introducción

Este documento describe cómo resolver problemas de integración de Umbrella ISR4k

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Este artículo es una continuación de la [guía de implementación de Cisco Umbrella Integration para ISR4k](#) y se proporciona como guía para ayudar a solucionar problemas de registro, así como problemas con la resolución de DNS interno y externo.



Nota: El certificado renovado para `api.opendns.com` del 29 de mayo de 2024 está ahora firmado por una nueva cadena/intermedio/raíz. La nueva raíz es DigiCert Global Root G2 (serial: 03af1e6a711a9a0bb2864b11d09fae5).

Registro e importación de certificados

1. Obtenga su token de API de Umbrella Dashboard: Admin > API Keys > (create) Legacy Network Devices.
2. Importe el certificado de la CA a ISR4k a través de CLI mediante cualquiera de estos métodos:

Importar desde URL:

Ejecute el comando y permita que ISR4k obtenga el certificado:

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

Importar directamente en terminal:

Copie y pegue el certificado de la CA (consulte el anexo) mediante el comando:

(Este certificado es para DigiCert Global Root G2.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCANagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTFORpZ2lDZXJ0IEEdsb2JhbCBSc290IEcyMIIIBjANBgkqhkiG
9w0BAQEFAAOCQAQ8AMIIBCgKCAQEaUzfNnNx7a8myaJCtSnX/RrohCgin9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sHON03Xss0r0upS/kqbit0tSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBjVJ8zUtlunJbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsPwPtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRnrw9FDKZJobq7nMwxM4MphQIDAQABO0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUtiJUIBiV
5uNu5g/6+rkS7QYXjzkWdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLsn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNHj7jitra1j41E6Vf8PlwUHBHQRFxGU7Aj64GxJUTfy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexGRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj1lDiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1
MrY=
-----END CERTIFICATE-----
```

Copie y pegue el certificado intermedio mediante el comando:

(Este certificado es para DigiCert Global G2 TLS RSA SHA256 2020 CA1.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEyDCCA7CgAwIBAgIQDPW9BiTWAvaR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NTlaMFkxCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbmMxMzAxBgNVBAMTKkRlZ2lDZXJ0IEEdsb2Jh
bCBHMiBUTFMgU1NBIFNIQTl1NiAyMDIwIENBMTCASiWdQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMz3EGJPprtjb+2QU1bFbSd7ehJWivH0+dbn4Y+9lavyYEEV
cNsSAPonCrVX0Ft9s1GTcZU0akGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDy
FuqrIvAxIhFhaZamunjZ1x/jfwardUSVc8is/+9dCopZQ+GssjoP80j812s3wwPc
3kbw20X+fSP9k0hRBx5Ro1/tSUZufyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8
osicfebUTVSvQpmowQTCd5zWSOT0EeAqgJnwQ3DPP3Zr0UxJqyRwg2C/Uaoq2yT
zGJSQnW5+Jr6Xl6ysGH1Hx+5fwmY6D36g39HaaECAwEAAaOCAYIwggF+MBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVRO0BBYEFHSFGMBmx9833s+9KTeqAx2+7c0XMB8G
A1UdIwQYMBaAFE4iVCAYlEbjbuYP+vq5Eu0GF485MA4GA1UdDwEB/wQEAwIBhjAd
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYIKwYBBQUHAQEaJBoMCQG
CCsGAQUFBzABhhodHRwOi8vb2Nzc5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
```

```

NGh0dHA6Ly9jYWN1cnRzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDwgM4YxaHR0cDovL2NybdMuZG1naWN1cnQuY29t
LORpZ21DZXJ0R2xvYmFsUm9vdEcyLmNybdA9BgNVHSAENjA0MA5GCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAGewCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAA0CAQEAKPFwyYiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWk0H7U1MV1+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
s1me5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZm0pGrFmCW3R
bpD0ufovARTFXFZkAd19h6g4U5+LXUZtXMYnhIHUfoyMo5tS58aI7Dd8KvvwVVo4
chDYABPPTHPbjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----

```

3. Ingrese el token API a ISR4k CLI mediante el comando:

```

parameter-map type umbrella global
token XXXXXXXXXXXXXXXXXXXXXXXXXXXX

```

4. Esta es la configuración de muestra mínima en ISR4k:

```

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

```

Información adicional:

- Asegúrese de configurar el comando "umbrella out" antes de "umbrella in".
- El registro puede ser exitoso solamente cuando el puerto 443 está en estado abierto y permite que el tráfico pase a través de cualquier firewall existente.
- En la versión anterior de Denali de Cisco IOS XE, se utiliza el comando OpenDNS en lugar de Umbrella.

Verificación de la importación del certificado y el registro del dispositivo

1. Compruebe si el certificado de la CA se ha almacenado correctamente en el dispositivo ISR4k:

- Si la importación del certificado se realizó mediante la URL, ejecute el comando `dir nvram:` para verificar que el certificado `ios.p7b` se almacene correctamente en la NVRAM del dispositivo.

```

[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 -rw- boot system bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin <no date> private-config
32771 -rw- boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin <no date> underlying-config
1 -rw- isr4k.pod3#conf 426 Enter configuration commands, one per line. End with CNTL/Z. <no date> persistent-data
2 -rw- isr4k.pod3(conf) 1182 no boot system <no date> ISR4451-X-4x1GE_0_0_0
4 -rw- isr4k.pod3(conf) 17 boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin <no date> ecfm-ieee-mib
5 -rw- isr4k.pod3(conf) 0 do sh run | inc boot system <no date> ifIndex-table
6 -rw- boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin <no date> QuoVadisRoot#D3ACCA.cer
8 -rw- boot system bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin <no date> CiscoECCRoot#2CA.cer
9 -rw- isr4k.pod3(conf) 793 <no date> CiscoRootCAM#1CA.cer
10 -rw- isr4k.pod3(conf) 791 <no date> QuoVadisRoot#5C6CA.cer
12 -rw- isr4k.pod3#wr 1697 <no date> CiscoRootCA2#CCA.cer
14 -rw- Building configuration... <no date> QuoVadisRoot#509CA.cer
16 -rw- [OK] 1467 <no date> CiscoRXC-R2#1CA.cer
17 -rw- isr4k.pod3#sh bootvar 825 <no date> CiscoECCRoot#1CA.cer
18 -rw- BOOT variable = bootflash:isr4300-universalk9.16.03.03.SPA.bin,12 bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin <no date> DSTRootCA#3#406BCA.cer
19 -rw- CONFIG_FILE variable does not exist <no date> QuoVadisRoot#508BCA.cer
21 -rw- BOOTLDR variable does not exist <no date> CiscoLicensi#1CA.cer
22 -rw- Configuration register is 0x2102 <no date> DigiCertGlob#BC91CA.cer
24 -rw- Standby not ready to show bootvar <no date> cwmp_inventory
27 -rw- isr4k.pod3#rel 1176 <no date> ios.p7b
2945
146259

```

115016968663

- Si la importación del certificado se realizó usando el método copy/paste, ejecute el comando `show cry pki trustpool` y verifique el número de serie y el cn del certificado:

```

#sh umbrella deviceid
Device registration details
Interface Name      Tag      Status      Device-id
GigabitEthernet0/0/1 10.11.11.1/ 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. Para verificar el registro correcto de ISR4k, ejecute el comando `show umbrella device`.

Ejemplo de resultado

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

Salida de panel:

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

Depuración y registro

- Verifique la versión de ISR4k: `show version` o `show platform` (se requiere Cisco IOS XE Denali 16.3 o posterior)
- Habilitar registros de depuración de registro de dispositivos: `"debug umbrella device-registration"` y luego `"show logging"` (para inhabilitar - `no debug umbrella device-registration`)

Estos son registros de ejemplo:

Falta el certificado:

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

Certificado instalado y el dispositivo se ha registrado correctamente:

```
%%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 no se puede resolver:

<#root>

```
%%UMBRELLA-3-DNS_RES_FAILURE:
```

Failed to resolve name api.opendns.com

Retry attempts:0

- Verificar resolución DNS: No hay ningún comando 'dig' o 'nslookup' disponible en ISR4k. Es mejor utilizar "ping hostname source interface #" de la CLI de ISR4k
- ISR con VRF configurado: En la interfaz, asegúrese de tener "ip name-server vrf <vrf_name> <dns_server_ip>" configurado y verifíquelo con "ping vrf <vrf_name> api.opendns.com"
- Asegúrese de que "ip dns server" está configurado: Esto permite que el ISR se consulte directamente.
- Para inhabilitar DNSCrypt, ingrese este comando: parameter-map type umbrella global > no dnscrypt
- Verificación de dominio interno: ejecute el comando show umbrella config y busque el Regex de dominio local, por ejemplo:
 - 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
- No se puede importar el certificado mediante la URL o el certificado importado mediante el terminal se está eliminando después del reinicio:

```
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.
```

Solución: descargue manualmente el paquete de certificados "ios.p7b" mediante curl y cópielo en la memoria flash del router > Borre el certificado existente del grupo > Importe el paquete de certificados "ios.p7b" de la memoria flash:

```
<#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.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).