

Solução de problemas da integração do Umbrella ISR4k

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Registro e Importação de Certificado](#)

[Verificação da Importação de Certificado e Registro de Dispositivo](#)

[Depuração e registro](#)

Introdução

Este documento descreve como resolver problemas da integração do Umbrella ISR4k

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Este artigo é uma continuação do [guia de implantação do Cisco Umbrella Integration para ISR4k](#) e é fornecido como um guia para ajudar a solucionar problemas de registro, bem como problemas com resolução de DNS interno e externo.



Note: O certificado renovado para api.opendns.com de 29 de maio de 2024 foi assinado por uma nova cadeia/intermediário/raiz. A nova raiz é DigiCert Global Root G2 (serial: 033af1e6a711a9a0bb2864b11d09fae5)

Registro e Importação de Certificado

1. Obtenha seu token de API no Umbrella Dashboard: Admin > Chaves de API > (criar) Dispositivos de Rede Herdados.

2. Importe o certificado CA para o ISR4k via CLI usando um destes métodos:

Importar da URL:

Emita o comando e permita que o ISR4k busque o certificado:

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

Importar diretamente no terminal:

Copie e cole o certificado CA (consulte o anexo) usando o comando:

(Este certificado é para a raiz global G2 do DigiCert.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDEwMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2l0eSb2JhbCB290IEcyMIIIBjANBgkqhkiG9w0BAQEF
AAQCAQ8AMIIBCgKCAQEaUzfNnN7a8myaJCtSnX/RrohCgin9RlUyfuI2/Ou8jqJkTx
65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx1x7e/dfgy5SDN
67sH0N03Xss0r0upS/kqbit0tSZpLY16ZtrAGCSYP9PIUkY92eQq2EGnI/yuum06Z
Iya7XzV+hdG82MHauVBjVJ8zUtlunJbd134/tJS7SsVQepj5WztC07TG1F8PapsP
UwtP1MvYwnSlcUfIKdzX0S0xZKBgyMUNGPHgm+F6HmIcr9g+UQvIO1CsRnKPZzFBQ
9RnbDhxSJITRnrw9FDKZJobq7nMwxM4MphQIDAQABo0IwQDAPBgNVHRMBAf8EBTADAQ
H/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUtiJUIBiV5uNu5g/6+rkS7QYXjzk
wDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY1Y19PMWLSn/pvtsrF9+wX
3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4NeF22d+mQrvHRAiGfzZ0JF
rabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NGFdtom/DzMNU+MeKNhJ7jitra1j
41E6Vf8P1wUHBHQRFXGU7Aj64GxJUTfy8bJZ918rG0maFvE7FBcf6IKshPECBV1/
MURexGRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTePLiaWN0bfVKfjl1DiIGknibVb63d
DcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1MrY=
-----END CERTIFICATE-----
```

Copie e cole o certificado intermediário usando o comando:

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

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEyDCCA7CgAwIBAgIQDPW9BiTWA vR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NTlaMFkxMzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbmMxMzAxBgNVBAMTKkRpZ2l0eSb2JhbCBHMi
BUTFMgU1NBIFNIQTl1NiAyMDIwIENBMTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQo
CggEBAMz3EGJPprtjb+2QU1bFbSd7ehJwivH0+dbn4Y+9lavyYEEVcNsSAPonCrVX0F
t9s1GTcZU0akGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDyFuqrIvAxIhFhaZa
munjZ1x/jfwardUSVc8is/+9dCopZQ+GssjoP80j812s3wwPc3kbw20X+fSP9k0hRB
x5Ro1/tSUZufyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8osicfebUTVSvQpmowQTC
d5zWS0TOEaAggJnwQ3DPP3Zr0UxJqyRewg2C/Uaoq2yTzGJSQnWS+Jr6X16ysGH1H
x+5fwmY6D36g39HaaECAwEAAaOCAYIwggF+MBIGA1UdEwEB/wQIMAYBAf8CAQAwHQYD
VRO0BBYEFHSFGMBmx9833s+9KTeqAx2+7c0XMB8GA1UdIwQYMBaAFAFE4iVCAY1ebj
buYP+vq5Eu0GF485MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQ
YIKwYBBQUHAWIwdgYIKwYBBQUHAQEaAjBoMCQCcCsGAQUFBzABhhodHRwOi8vb2Nz
cC5kaWdpY2VydC5jb20wYAYIKwYBBQUHMAKG
```

```
NGh0dHA6Ly9jYWN1cnRzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVROfBDsw0TA3oDWgM4YxaHR0cDovL2NybdMuZG1naWN1cnQuY29t
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. Insira o token de API para a CLI do ISR4k usando o comando:

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

4. Esta é a configuração mínima básica de exemplo no 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
```

Informações adicionais:

- Certifique-se de configurar o comando "umbrella out" antes do comando "umbrella in".
- O registro pode ser bem-sucedido apenas quando a porta 443 está em um estado aberto e permite que o tráfego passe por qualquer firewall existente.
- Na versão mais antiga do Cisco IOS XE Denali, o comando OpenDNS é usado no lugar do Umbrella.

Verificação da Importação de Certificado e Registro de Dispositivo

1. Verifique se o certificado CA foi armazenado com êxito no dispositivo ISR4k:

- Se a importação do certificado foi feita usando o URL, emita o comando `dir nvram:` para verificar se o certificado `ios.p7b` foi armazenado com êxito na NVRAM do 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 ---- 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 <no date> private-config
32771 -rw- isr4k.pod3#conf 3086 <no date> underlying-config
1 ---- Enter configuration commands, one per line. End with CNTL/Z. <no date> persistent-data
2 -rw- isr4k.pod3(conf) 426 <no date> ISR4451-X-4x1GE_0_0_0
4 -rw- isr4k.pod3(conf) 1182 no boot system <no date> ecfm-ieee-mib
5 -rw- boot system bootflash:isr4300-universalk9.16.03.03.SPA.bin <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 <no date> DSTRootCA#3406BCA.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- 146259 <no date> ios.p7b

```

115016968663

- Se a importação do certificado foi feita usando o método copy/paste, execute o comando `show cry pki trustpool` e verifique o número de série e o cn do certificado:

```

#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. Para verificar o registro bem-sucedido do ISR4k, execute o comando `show umbrella deviceid`.

Saída de exemplo:

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

Saída do painel:

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

Depuração e registro

- Verificar a versão do ISR4k: `show version` OU `show platform` (necessário Cisco IOS XE Denali 16.3 ou mais recente)
- Habilitar logs de depuração de registro de dispositivo: `"debug umbrella device-registration"` e depois `"show logging"` (para desabilitar - `no debug umbrella device-registration`)

Estes são logs de exemplo:

Certificado ausente:

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

Certificado instalado e dispositivo registrado com êxito:

```
*%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 não pode ser resolvido:

<#root>

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

Failed to resolve name api.opendns.com

Retry attempts:0

- Verifique a resolução DNS: Não há nenhum comando 'dig' ou 'nslookup' disponível no ISR4k. É melhor usar "ping hostname source interface #" da CLI do ISR4k
- ISR com VRF configurado: Na interface, verifique se você tem "ip name-server vrf <vrf_name> <dns_server_ip>" configurado e verifique com "ping vrf <vrf_name> api.opendns.com"
- Verifique se o "servidor ip dns" está configurado: Isso permite que o ISR seja consultado diretamente.
- Para desativar o DNSCrypt, digite este comando: parameter-map type umbrella global > no dnscrypt
- Verificação de domínio interno: execute o comando show umbrella config e procure o Local Domain Regex, por exemplo:
 - show umbrella config > Local Domain Regex parameter-map: desvio de DNS
 - show run | be dns_bypass
 - show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list
- Não é possível importar certificado usando URL ou o certificado importado usando terminal está sendo excluído após a reinicialização:

```
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.
```

Solução alternativa: baixe manualmente o pacote de certificados "ios.p7b" via curl e copie para a flash do Roteador > Limpar certificado existente do pool > Importar pacote de certificados "ios.p7b" da 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.

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.