

Problemen oplossen met de overkoepelende ISR4k-integratie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Registratie en invoercertificaat](#)

[Het certificaat importeren en de apparaatregistratie controleren](#)

[Foutopsporing en registratie](#)

Inleiding

In dit document wordt beschreven hoe problemen met de Umbrella ISR4k-integratie kunnen worden opgelost

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

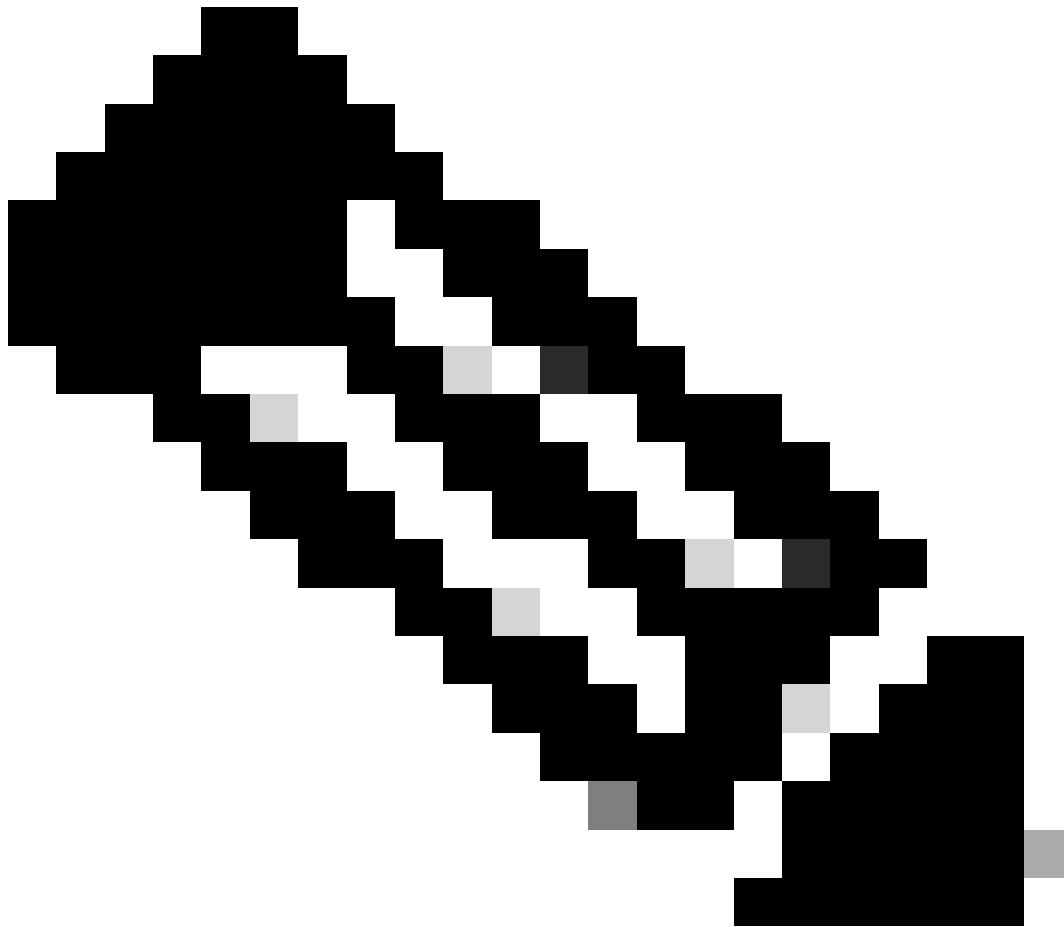
Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Dit artikel is een voortzetting van de [Cisco Umbrella Integration for ISR4k deployment guide](#) en wordt geleverd als een handleiding voor het oplossen van problemen met registratie en problemen met interne en externe DNS-oplossingen.



Opmerking: De hernieuwde cert voor `api.opendns.com` van 29 mei 2024 is nu ondertekend door een nieuwe keten / tussenproduct / root. De nieuwe root is DigiCert Global Root G2 (serieel: 033af1e6a711a9a0bb2864b11d09fae5).

Registratie en invoercertificaat

1. Verkrijg uw API-token van Umbrella Dashboard: Admin > API-sleutels > (maken) Legacy Network Devices.
2. Het CA-certificaat via CLI importeren in de ISR4k met behulp van een van de volgende methoden:

Importeren vanuit URL:

Geef de opdracht en laat ISR4k de cert ophalen:

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

Direct importeren in terminal:

Kopieer en plak het CA-certificaat (zie bijlage) met de opdracht:

(Dit certificaat is voor DigiCert Global Root G2.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCANagAwIBAgIQAzrx5qcRqaC7KGSxHqn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDEwMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RlZ2ZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNnnx7a8myaJCtSnX/RrohCgin9R1UyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sH0N03Xss0r0upS/kqbit0tSZpLY16ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBjVJ8zUtlunJbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsPwUwP1MvYwnS1cUfIKdzX0S0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vI01CsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMwxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkWdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Y19PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitra1j41E6Vf8P1wUHBHQRFXGU7Aj64GxJUTfy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj1lDiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1
MrY=
-----END CERTIFICATE-----
```

Kopieer en plak het tussenliggende certificaat met de opdracht:

(Dit certificaat is voor DigiCert Global G2 TLS RSA SHA256 2020 CA1.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEYDCCA7CgAwIBAgIQDPW9Bi tWAvR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NT1aMFkxCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbmMxMzAxXBgNVBAMTKkRlZ2ZlZDZlZDZlZDZl
bCBHMiBUTFMgU1NlIFNlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
ggEPADCCAQoCggEBAMz3EGJPprtjb+2QU1bFbSd7ehJWivH0+dbn4Y+9lavyYEEV
cNsSAPonCrVX0ft9s1GTcZU0akGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDy
FuqrIvAxIhFhaZamunjZ1x/jfWardUSVc8is/+9dCopZQ+GssjoP80j812s3wwPc
3kbW20X+fSP9k0hRBx5Ro1/tSUZufyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8
osi cfebUTVSvQpmowQTCd5zWS0TOEeAqgJnwQ3DPP3Zr0UxJqyRewg2C/Uaoq2yT
zGJSQnW5+Jr6X16ysGH1Hx+5fwmY6D36g39HaaECAwEAAaOCAYIwggF+MBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVRO0BBYEFHSFgMBmx9833s+9KTeqAx2+7c0XMB8G
A1UdIwQYMBaAFE4iVCAY1ebjbuYP+vq5Eu0GF485MA4GA1UdDwEB/wQEAwIBhjAd
```

```
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwdgYIKwYBBQUHAQEEajBoMCQG
CCsGAQUFBzABhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
NGh0dHA6Ly9jYWN1cnRzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDwgM4YxaHR0cDovL2NybdMuZG1naWN1cnQuY29t
LORpZ21DZXJ0R2xvYmFsUm9vdEcyLmNybdDA9BgNVHSAENjA0MA5GCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAGewCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAA0CAQEAKPFwyYiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWk0H7U1MVl+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
s1me5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZm0pGrFmCW3R
bpd0UfovARTFXFZkAd19h6g4U5+LXUZtXMYnhIHUfoym05tS58aI7Dd8KvvwVVo4
chDYABPPTHPbjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3. Voer de API-token in ISR4k CLI in met de opdracht:

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

4. Dit is de minimale monsterconfiguratie op 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
```

Aanvullende informatie:

- Zorg ervoor dat u de opdracht "Paraplu uit" vóór "Paraplu in" configureert.
- Registratie kan alleen succesvol zijn als poort 443 zich in een open toestand bevindt en het verkeer door een bestaande firewall kan passeren.
- In de oudere Cisco IOS XE Denali-versie wordt de opdracht OpenDNS gebruikt in plaats van Umbrella.

Het certificaat importeren en de apparaatregistratie controleren

1. Controleer of het CA-certificaat met succes is opgeslagen op het ISR4k-apparaat:

- Als het importeren van het certificaat is gedaan met behulp van de URL, geeft u de opdracht `dir nvram:`

om te controleren of het ios.p7b-certificaat met succes is opgeslagen in het NVRAM-apparaat.

```
[ISR4k02-CWSSDMLAB#dir nvram:ter is 0x2102
Directory of nvram:/
 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 <no date> private-config
 32771  -rw-   boot system bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin <no date> underlying-config
 1      ----   isr4k.pod3#conf 3086   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-universalk9.03.16.04b.S.155-3.S4b-ext.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-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin <no date> QuoVadisRoot#D3ACCA.cer
 8      -rw-   isr4k.pod3(conf 793   <no date> CiscoECCRoot#2CA.cer
 9      -rw-   isr4k.pod3(conf 791   <no date> CiscoRootCAM#1CA.cer
10     -rw-   isr4k.pod3#wr 1697   <no date> QuoVadisRoot#5C6CA.cer
12     -rw-   Building configuration... <no date> CiscoRootCA2#CCA.cer
14     -rw-   [OK] 1467   <no date> QuoVadisRoot#509CA.cer
16     -rw-   isr4k.pod3#sh 825   <no date> CiscoRXC-R2#1CA.cer
17     -rw-   BOOT variable = bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin,12:bootflash:isr4300-universalk9.03.16.04b.S.155-3.S4b-ext.SPA.bin <no date> CiscoECCRoot#1CA.cer
18     -rw-   CONFIG_FILE variable does not exist <no date> DSTRootCAX3#406BCA.cer
19     -rw-   BOOTLDR variable does not exist <no date> QuoVadisRoot#508BCA.cer
21     -rw-   Configuration register is 0x2102 <no date> CiscoLicensi#1CA.cer
22     -rw-   Standby not ready to show bootvar. <no date> DigiCertGlob#BC91CA.cer
24     -rw-   isr4k.pod3#rel 2945   <no date> cwmp_inventory
27     -rw-   146259   <no date> ios.p7b
```

115016968663

- Als het importeren van het certificaat is uitgevoerd met de methode copy/paste, voert u de opdracht show cry pki trustpool uit en controleert u het serienummer en cn van het certificaat:

```
FW011FW011#sh umbrella deviceid
Device registration details
Interface Name      Tag      Status      Device-id
GigabitEthernet0/0/1 11.11.11.11/ 200 SUCCESS 010a9e60fe3b4689

FW011FW011#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. Voer de opdracht `paraplu-apparaat tonen` uit om de succesvolle registratie van ISR4k te verifiëren.

Steekproefuitvoer:

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

Dashboarduitvoer:

 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

Foutopsporing en registratie

- Controleer de ISR4k-versie: toon de versie of toon het platform (vereist Cisco IOS XE Denali 16.3 of nieuwer)
- Debuglogboeken voor apparaatregistratie inschakelen: `"debug umbrella device-registration"` en vervolgens `"show logging"` (uitschakelen - geen debugumbrella apparaatregistratie)

Dit zijn voorbeeldlogs:

Certificaat ontbreekt:

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

Certificaat geïnstalleerd en apparaat is geregistreerd:

```
*%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 kan niet worden opgelost:

<#root>

**%UMBRELLA-3-DNS_RES_FAILURE:*

Failed to resolve name api.opendns.com

Retry attempts:0

- DNS-resolutie controleren: er is geen opdracht 'dig' of 'nslookup' beschikbaar op ISR4k. U kunt het beste "ping hostname source interface #" van de ISR4k CLI gebruiken
- ISR met VRF geconfigureerd: Zorg ervoor dat op de interface "ip name-server vrf <vrf_name> <dns_server_ip>" is geconfigureerd en controleer met "ping vrf <vrf_name> api.opendns.com"
- Zorg ervoor dat "ip dns server" is geconfigureerd: hierdoor kan de ISR rechtstreeks worden opgevraagd.
- Als u DNSCrypt wilt uitschakelen, voert u deze opdracht in: parametermaptype umbrella global > no dnscrypt
- Interne domeinverificatie: Voer de opdracht paraplū-configuratie tonen en kijk voor de Local Domain Regex, bijvoorbeeld:
 - umbrella config weergeven > Local Domain Regex parameter-map: dns bypass
 - Uitvoeren weergeven | beDNS_Bypass
 - Platform hardware weergeven QFP Active Feature DNS-Snoop-Agent Client HW-Pattern-List
- Certificaat kan niet worden geïmporteerd via URL of certificaat geïmporteerd met terminal wordt verwijderd na opnieuw opstarten:

```
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.
```

Oplossing: handmatig downloaden "ios.p7b" cert bundel via curl en kopiëren naar de router flash > Wis bestaand certificaat uit pool > Importeren "ios.p7b" cert bundel van 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.
```


Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.