Umbrella ISR4k 통합 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[등록 및 인증서 가져오기](#)

[인증서 가져오기 및 디바이스 등록 확인](#)

[디버깅 및 로깅](#)

소개

이 문서에서는 Umbrella ISR4k 통합 문제를 해결하는 방법에 대해 설명합니다

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

이 문서는 [Cisco Umbrella Integration for ISR4k 배포 가이드](#)를 이어온 문서이며 등록 문제 및 내부 및 외부 DNS 확인 문제를 해결하는 데 도움이 되는 가이드로 제공됩니다.

참고: 2024년 5월 29일부터 api.opendns.com에 대해 갱신된 인증서가 새로운 체인/중간/루트에 의해 서명됩니다. 새 루트는 DigiCert 전역 루트 G2(일련 번호: 033af1e6a711a9a0bb2864b11d09fae5).

등록 및 인증서 가져오기

1. Umbrella 대시보드에서 API 토큰을 가져옵니다. Admin(관리) > API Keys(API 키) > (create) Legacy Network Devices(레거시 네트워크 디바이스).
2. 다음 방법 중 하나를 사용하여 CLI를 통해 CA 인증서를 ISR4k로 가져옵니다.

URL에서 가져오기:

명령을 실행하고 ISR4k에서 인증서를 가져오도록 허용합니다.

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

터미널에서 직접 가져오기:
다음 명령을 사용하여 CA 인증서를 복사하여 붙여넣습니다(첨부 참조).

(이 인증서는 DigiCert 전역 루트 G2에 대한 것입니다.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwUm9vdCBH
MjAeFw0xMzA4MDEwMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYWwvZG90aW50LWVudC5j
b20xIDAeBgNVBAMTF0R2Z1DZXJ0IEEdsb2JhbCBSb290IEcyMIIIBIjANBgkqhkiG
9w0BAQEFAAQCAQ8AMIIBCgKCAQEaUzfNnNx7a8myaJCtSnX/RrohCgiN9R1UyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sH0N03Xss0r0upS/kqbit0tSZpLY16ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZiYa7XzV+hdG82MHauVBjVJ8zUt1uNjbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsPwtP1MvYwnS1cUfIKdzX0S0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vI01CsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMwxM4MphQIDAQABO0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rKs7QYXjzkWdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Y19PMWLsn/pvtsrF9+wX3N3KjIT0YFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNu+MeKNhJ7jitra1j41E6Vf8P1wUHBHQRFxGU7Aj64GxJUTfy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexGRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj11DiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1
MrY=
-----END CERTIFICATE-----
```

다음 명령을 사용하여 중간 인증서를 복사하여 붙여넣습니다.

(이 인증서는 DigiCert Global G2 TLS RSA SHA256 2020 CA1에 사용됩니다.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEyDCCA7CgAwIBAgIQDPW9Bi tWAvR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NT1aMFkxMzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYWwvZG90aW50LWVudC5j
b20xIDAeBgNVBAMTF0R2Z1DZXJ0IEEdsb2JhbCBSb290IEcyMIIIBIjANBgkqhkiG
9w0BAQEFAAQCAQ8AMIIBCgKCAQEaUzfNnNx7a8myaJCtSnX/RrohCgiN9R1UyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sH0N03Xss0r0upS/kqbit0tSZpLY16ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZiYa7XzV+hdG82MHauVBjVJ8zUt1uNjbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsPwtP1MvYwnS1cUfIKdzX0S0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vI01CsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMwxM4MphQIDAQABO0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rKs7QYXjzkWdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Y19PMWLsn/pvtsrF9+wX3N3KjIT0YFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNu+MeKNhJ7jitra1j41E6Vf8P1wUHBHQRFxGU7Aj64GxJUTfy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexGRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj11DiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1
MrY=
-----END CERTIFICATE-----
```

```
NGh0dHA6Ly9jYWN1cnRzLmRpZ21jZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDwgM4YxaHR0cDovL2NybdMuZG1naWN1cnQuY29t
LORpZ21DZXJ0R2xvYmFsUm9vdEcyLmNybdA9BgNVHSAENjA0MA5GCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAGewCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAA0CAQEAKPFwyyiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWkOH7U1MV1+t
wcW1BSAuWdH/SvWgKtiw1a3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
s1me5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZm0pGrFmCW3R
bpD0ufovARTFXFZkAd19h6g4U5+LXUZtXMYnhIHUfoyMo5tS58aI7Dd8KvVwVVo4
chDYABPPTHPbjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3. 다음 명령을 사용하여 ISR4k CLI에 대한 API 토큰을 입력합니다.

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

4. ISR4k의 최소 샘플 컨피그레이션입니다.

```
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
```

추가 정보:

- "umbrella in" 명령 전에 "umbrella out"을 구성해야 합니다.
- 포트 443이 열린 상태이고 트래픽이 기존 방화벽을 통과할 수 있는 경우에만 등록이 성공할 수 있습니다.
- 이전 Cisco IOS XE Denali 버전에서는 Umbrella 대신 OpenDNS 명령이 사용됩니다.

인증서 가져오기 및 디바이스 등록 확인

1. CA 인증서가 ISR4k 디바이스에 성공적으로 저장되었는지 확인합니다.

- URL을 사용하여 인증서 가져오기를 수행한 경우 `dir nvram` 명령을 실행합니다. ios.p7b 인증서가 디바이스 NVRAM에 성공적으로 저장되었는지 확인합니다.

```

[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-universalk9.03.16.04b3-15-3.54b-ext.SPA.bin
32771 -rw-   boot system bootflash:isr4300-universalk9.16.03.03-15-3.54b-ext.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(conf) 426     <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-universalk9.03.16.04b3-15-3.54b-ext.SPA.bin
5 -rw-   boot system bootflash:isr4300-universalk9.16.03.03-15-3.54b-ext.SPA.bin
5 -rw-   isr4k.pod3(conf) 0     no sh run | inc boot system <no date>  ifIndex-table
6 -rw-   boot system bootflash:isr4300-universalk9.16.03.03-15-3.54b-ext.SPA.bin
8 -rw-   boot system bootflash:isr4300-universalk9.03.16.04b3-15-3.54b-ext.SPA.bin
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(conf) 1697   <no date>  QuoVadisRoot#D3ACCA.cer
12 -rw-   Building configuration... <no date>  CiscoRootCA2#CCA.cer
14 -rw-   [OK] 1467   <no date>  QuoVadisRoot#509CA.cer
16 -rw-   isr4k.pod3#sh bootvar 825     <no date>  CiscoXC-R2#1CA.cer
17 -rw-   BOOT variable = bootflash:isr4300-universalk9.16.03.03-15-3.54b-ext.SPA.bin 464     <no date>  CiscoECCRoot#1CA.cer
18 -rw-   CONFIG_FILE variable does not exist
18 -rw-   BOOTLDR variable does not exist <no date>  DSTRootCAX3#406BCA.cer
19 -rw-   Configuration register is 0x2102 1492   <no date>  QuoVadisRoot#508BCA.cer
21 -rw-   Standby not ready to show bootvar 805     <no date>  CiscoLicensi#1CA.cer
22 -rw-   isr4k.pod3#rel 1176   <no date>  DigiCertGlob#BC91CA.cer
24 -rw-   2945   <no date>  cwmp_inventory
27 -rw-   146259 <no date>  ios.p7b

```

115016968663

- 인증서 가져오기가 복사/붙여넣기 방법을 사용하여 수행된 경우 show cry pki trustpool 명령을 실행하고 인증서의 일련 번호 및 cn을 확인합니다.

```

[ISR4k02-CWSSDMLAB#sh umbrella deviceid
Device registration details
Interface Name      Tag          Status      Device-id
GigabitEthernet0/0/1  111.111.111.111/ 200 SUCCESS  010a9e60fe3b4689

[ISR4k02-CWSSDMLAB#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
[ISR4k02-CWSSDMLAB#

```

28552066223252

2. ISR4k의 성공적인 등록을 확인하려면 show umbrella deviceid 명령을 실행합니다.

샘플 출력:

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

대시보드 출력:

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

디버깅 및 로깅

- ISR4k 버전 확인: show version 또는 show platform(필수 Cisco IOS XE Denali 16.3 이상)
- 디바이스 등록 디버그 로그를 활성화합니다. "debug umbrella device-registration" 다음 "show logging" (비활성화하려면 - debug umbrella device-registration을 실행하지 않음)

다음은 샘플 로그입니다.

인증서 누락:

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

인증서가 설치되고 디바이스가 성공적으로 등록되었습니다.

```
%%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.com은 확인할 수 없습니다.

<#root>

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

```
Failed to resolve name api.opendns.com
```

Retry attempts:0

- DNS 확인: ISR4k에서 사용할 수 있는 'dig' 또는 'nslookup' 명령이 없습니다. ISR4k CLI에서 "ping hostname source interface #"를 사용하는 것이 좋습니다
- VRF가 구성된 ISR: 인터페이스에서 "ip name-server vrf <vrf_name> <dns_server_ip>"가 구성되어 있는지 확인하고 "ping vrf <vrf_name> api.opendns.com"으로 확인합니다.
- "IP DNS 서버"가 구성되었는지 확인합니다. 이렇게 하면 ISR을 직접 쿼리할 수 있습니다.
- DNSCrypt를 비활성화하려면 다음 명령을 입력합니다. parameter-map type umbrella global > no dnscrypt
- 내부 도메인 확인: show umbrella config 명령을 실행하고 로컬 도메인 Regex를 찾습니다. 예를 들면 다음과 같습니다.
 - show umbrella config > Local Domain Regex parameter-map: dns 우회
 - 쇼런 | be dns_bypass
 - 플랫폼 하드웨어 qfp 활성 기능 dns-snoop-agent 클라이언트 hw-pattern-list 표시
- URL을 사용하여 인증서를 가져올 수 없거나 터미널을 사용하여 가져온 인증서가 재부팅 후 삭제됩니다.

```
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.
```

해결 방법: curl을 통해 수동으로 "ios.p7b" 인증서 번들을 다운로드하고 라우터의 플래시에 복사 > 폴에서 기존 인증서 지우기 > 플래시에서 "ios.p7b" 인증서 번들 가져오기:

```
<#root>
```

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

```
crypto pki certificate pool
```

```
cabundle nvram:Trustpool115.cer
```

```
crypto pki trustpool clean
```

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

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

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.