Fehlerbehebung bei der Umbrella ISR4k-Integration

Inhalt

Einleitung

Dieses Dokument beschreibt die Fehlerbehebung bei der Umbrella ISR4k-Integration

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

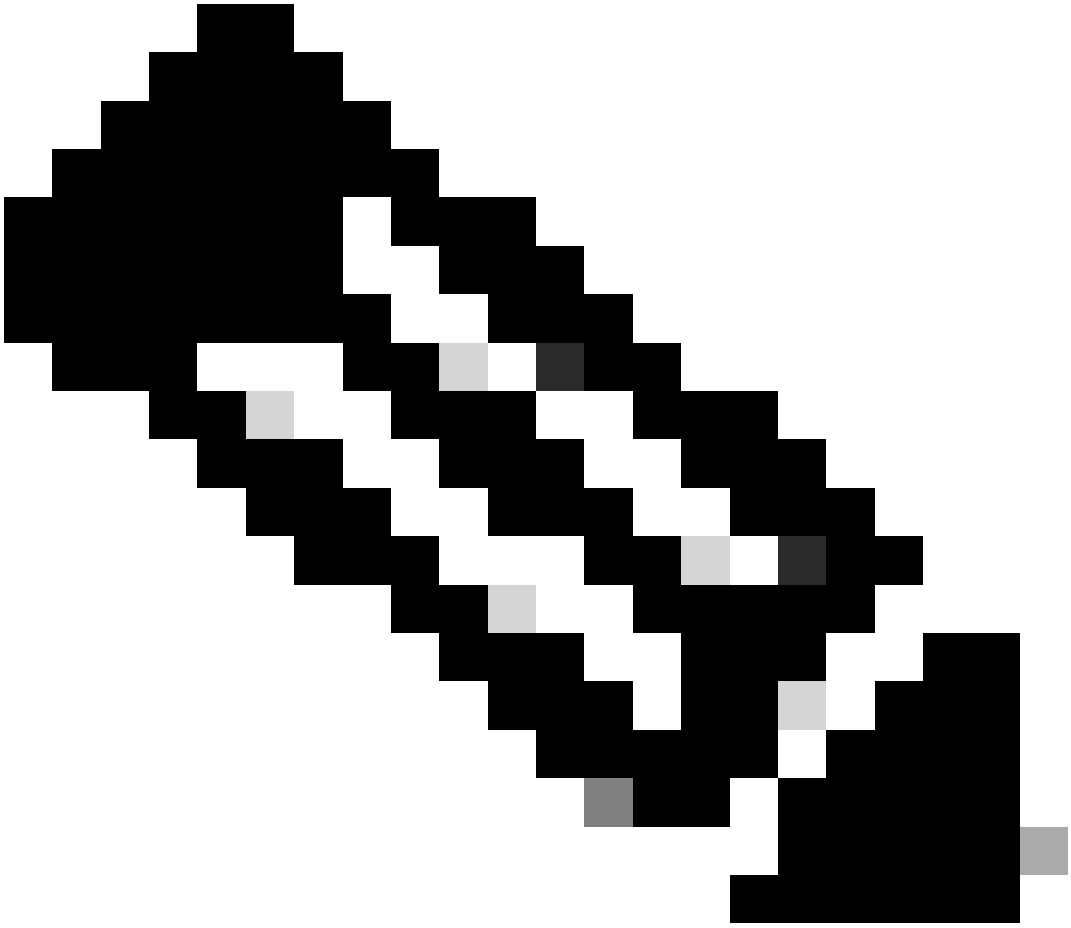
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Dieser Artikel stellt eine Fortsetzung des Cisco Umbrella Integration für ISR4k-Bereitstellungsleitfadens dar und dient als Leitfaden zur Behebung von Registrierungsproblemen sowie von Problemen mit der internen und externen DNS-Auflösung.



Anmerkung: Das erneuerte Zertifikat für api.opendns.com vom 29. Mai 2024 wurde nun von einer neuen Kette/Zwischenprodukt/Wurzel unterzeichnet. Der neue Root ist DigiCert Global Root G2 (seriell: 033af1e6a711a9a0bb2864b11d09fae5).

Registrierung und Zertifikatimport

1. Rufen Sie Ihr API-Token vom Umbrella Dashboard ab: Admin > API Keys > Legacy Network Devices (erstellen).

2. Importieren Sie das Zertifizierungsstellenzertifikat mithilfe einer der folgenden Methoden über die CLI in den ISR4k:

Von URL importieren:
Geben Sie den Befehl ein, und lassen Sie ISR4k das Zertifikat abrufen:

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

Direkter Import im Terminal:
Kopieren Sie das CA-Zertifikat (siehe Anhang), und fügen Sie es mithilfe des folgenden Befehls ein:

(Dieses Zertifikat gilt für 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/yuum06ZIya7XzV+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-----
```

Kopieren Sie das Zwischenzertifikat, und fügen Sie es mithilfe des folgenden Befehls ein:

(Dieses Zertifikat gilt für 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+vq5Eu0GF485MA4GA1UdDwEB/wQEAwIBhjAd
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYIKwYBBQUHAQEEajBoMCQG
CCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
NGh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuZGlnaWNlcnQuY29t
L0RpZ2lDZXJ0R2xvYmFsUm9vdEcyLmNybDA9BgNVHSAENjA0MAsGCWCGSAGG/WwC
ATAHBgVngQwBATAIBgZngQwBAgEwCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAAOCAQEAkPFwyyiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWkOH7U1MVl+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
slme5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZm0pGrFmCW3R
bpD0ufovARTFXFZkAdl9h6g4U5+LXUZtXMYnhIHUfoyMo5tS58aI7Dd8KvvwVVo4
chDYABPPTHPbqjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3. Geben Sie das API-Token für die ISR4k-CLI über den folgenden Befehl ein:

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

4. Dies ist die absolute minimale Beispielkonfiguration auf 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
```

Zusätzliche Informationen:

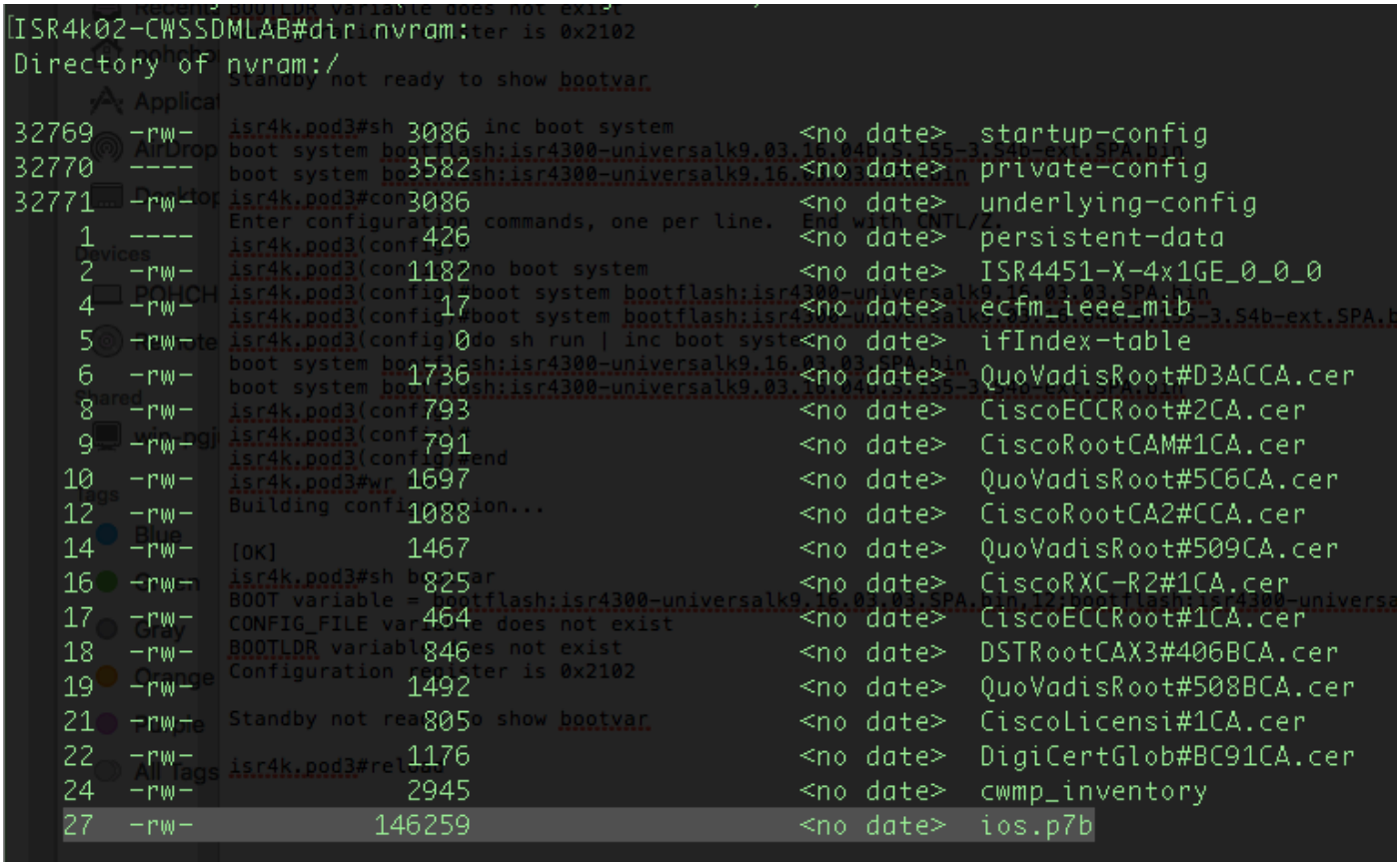
- Stellen Sie sicher, dass Sie den Befehl "umbrella out" (Regenschirm aus) vor "umbrella in" (Regenschirm ein) konfigurieren.
- Die Registrierung kann nur erfolgreich sein, wenn sich Port 443 im offenen Zustand befindet und den Datenverkehr durch eine vorhandene Firewall leiten lässt.
- In älteren Cisco IOS XE Denali-Versionen wird der OpenDNS-Befehl anstelle von Umbrella verwendet.

Überprüfen des Zertifikatimports und der Geräteregistrierung

1. Überprüfen Sie, ob das Zertifizierungsstellenzertifikat erfolgreich auf dem ISR4k-Gerät

gespeichert wurde:

- Wenn der Zertifikatimport über die URL durchgeführt wurde, geben Sie den Befehl `dir nvram:` um zu überprüfen, ob das ios.p7b-Zertifikat erfolgreich im Geräte-NVRAM gespeichert wurde.



115016968663

- Wenn der Zertifikatimport mit der Copy/Paste-Methode durchgeführt wurde, führen Sie den Befehl `show cry pki trustpool aus`, und überprüfen Sie die Seriennummer und cn des Zertifikats:

```
#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
[redacted]#
```

28552066223252

2. Führen Sie den Befehl `show umbrella device` aus, um zu überprüfen, ob die ISR4k-Registrierung erfolgreich war.

Beispiel für das Ergebnis:

```
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
```

Dashboard-Ausgabe:

115016791766

Debuggen und Protokollieren

- ISR4k-Version überprüfen: `show version` oder `show platform` (Cisco IOS XE Denali 16.3 oder höher erforderlich)

- Geräteregistrierungs-Debug-Protokolle aktivieren: "`debug umbrella device-registration`", dann "`show logging`" (deaktivieren - `keine debug umbrella device-registration`)

Dies sind Beispielprotokolle:

Zertifikat fehlt:

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

Das Zertifikat wurde installiert, und das Gerät wurde erfolgreich registriert:

```
*%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 lässt sich nicht auflösen:

<#root>

*%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- DNS-Auflösung überprüfen: Auf ISR4k ist kein "dig"- oder "nslookup"-Befehl verfügbar. Verwenden Sie am besten "`ping hostname source interface #`" von der ISR4k CLI.
- ISR mit konfiguriertem VRF: Vergewissern Sie sich, dass Sie auf der Schnittstelle "`ip name-server vrf <vrf_name> <dns_server_ip>`" konfiguriert haben, und verifizieren Sie dies mit "`ping vrf <vrf_name> api.opendns.com`".
- Stellen Sie sicher, dass "ip dns server" konfiguriert ist: Dadurch kann der ISR direkt abgefragt werden.
- Um DNSCrypt zu deaktivieren, geben Sie den folgenden Befehl ein: `parameter-map type umbrella global > no dnscrypt`
- Interne Domänenüberprüfung: Führen Sie den Befehl `show umbrella config` aus, und suchen Sie nach dem lokalen Domänenregulär, z. B.:
  - `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`
- Zertifikat kann nicht mit URL importiert werden oder Zertifikat, das mit Terminal importiert wurde, wird nach dem Neustart gelöscht:

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.

Problemumgehung: Manuelles Herunterladen des Zertifikatsbündels "ios.p7b" über curl und Kopieren in den Flash-Speicher des Routers > Vorhandenes Zertifikat aus Pool löschen > Zertifikatsbündel "ios.p7b" aus Flash importieren:

<#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.
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.