أستكشاف أخطاء تكامل Umbrella ISR4k وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف أخطاء تكامل Umbrella ISR4k وإصلاحها

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

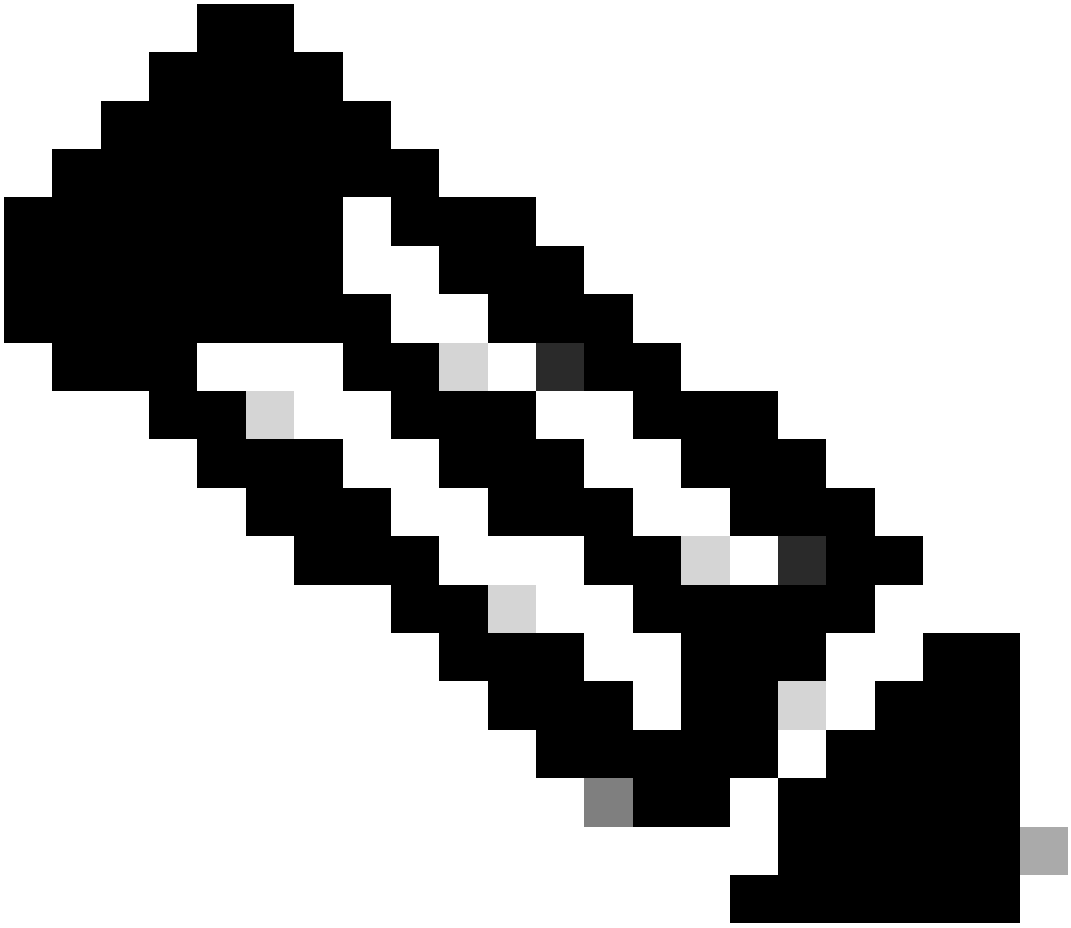
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Umbrella.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

نظرة عامة

تعد هذه المقالة إستمرارا لدليل نشر ISR4k من Cisco Umbrella Integration، كما يتم تقديمها كدليل للمساعدة في أستكشاف أخطاء التسجيل وإصلاحها، بالإضافة إلى المشاكل المتعلقة بحل DNS الداخلي والخارجي.



ملاحظة: وتم الآن التوقيع على الوثيقة المجددة api.opendns.com من 29 إلى 20 أيار/مايو 2024 من قبل سلسلة جديدة/سلسلة متوسطة/جذر جديد. الجذر الجديد هو DigiCert Global Root G2 (serial: 033af1e6a711a9a0bb2864b11d09fae5).

التسجيل واستيراد الشهادة

1. الحصول على رمز API المميز من لوحة معلومات Umbrella: Admin > مفاتيح API > (إنشاء) أجهزة الشبكة القديمة.

2. إستيراد شهادة CA إلى ISR4k عبر CLI باستخدام أي من الطريقتين التاليتين:

إستيراد من URL:
أصدرت الأمر وسمحت ISR4k أحضرت ال cert:

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

الاستيراد مباشرة في الوحدة الطرفية:
نسخ ولصق شهادة CA (راجع المرفق) باستخدام الأمر:

(هذه الشهادة خاصة ب 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-----
```

نسخ ولصق الشهادة الوسيطة باستخدام الأمر:

(هذه الشهادة تخص DigiCert Global G2 TLS RSA256 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/tSUZUfyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8
osicfebUTVSvQpmowQTCd5zWSOTOEeAqgJnwQ3DPP3Zr0UxJqyRewg2C/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. أدخل رمز API المميز إلى ISR4k CLI باستخدام الأمر:

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

4. هذا هو الحد الأدنى لتكوين العينة على 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
```

معلومات إضافية:

- تأكد من تكوين الأمر "umbrella out" قبل الأمر "umbrella in".
- يمكن أن يكون التسجيل ناجحا فقط عندما يكون المنفذ 443 في حالة فتح ويسمح بحركة المرور بالمرور من خلال أي جدار حماية موجود.
- في إصدار Denali الأقدم من Cisco IOS XE، يتم إستخدام الأمر OpenDNS بدلا من Umbrella.

التحقق من إستيراد الشهادة وتسجيل الأجهزة

1. تحقق مما إذا تم تخزين شهادة CA بنجاح على جهاز ISR4k:

- إذا تم إستيراد الشهادة باستخدام عنوان URL، قم بإصدار الأمر `dir nvram:` للتحقق من تخزين شهادة IOS.p7b بنجاح في ذاكرة NVRAM الخاصة بالجهاز.

```
ISR4k02-CWSSDMLAB#dir nvram:
Directory of nvram:/

32769  -rw-        3086                    <no date>  startup-config
32770  ----        3582                    <no date>  private-config
32771  -rw-        3086                    <no date>  underlying-config
    1  ----         426                    <no date>  persistent-data
    2  -rw-        1182                    <no date>  ISR4451-X-4x1GE_0_0_0
    4  -rw-          17                    <no date>  ecfm_ieee_mib
    5  -rw-           0                    <no date>  ifIndex-table
    6  -rw-        1736                    <no date>  QuoVadisRoot#D3ACCA.cer
    8  -rw-         793                    <no date>  CiscoECCRoot#2CA.cer
    9  -rw-         791                    <no date>  CiscoRootCAM#1CA.cer
   10  -rw-        1697                    <no date>  QuoVadisRoot#5C6CA.cer
   12  -rw-        1088                    <no date>  CiscoRootCA2#CCA.cer
   14  -rw-        1467                    <no date>  QuoVadisRoot#509CA.cer
   16  -rw-         825                    <no date>  CiscoRXC-R2#1CA.cer
   17  -rw-         464                    <no date>  CiscoECCRoot#1CA.cer
   18  -rw-         846                    <no date>  DSTRootCAX3#406BCA.cer
   19  -rw-        1492                    <no date>  QuoVadisRoot#508BCA.cer
   21  -rw-         805                    <no date>  CiscoLicensi#1CA.cer
   22  -rw-        1176                    <no date>  DigiCertGlob#BC91CA.cer
   24  -rw-        2945                    <no date>  cwmp_inventory
   27  -rw-      146259                    <no date>  ios.p7b
```

115016968663

- إذا تم إستيراد الشهادة باستخدام طريقة النسخ/اللصق، قم بتشغيل الأمر `show cry pki trustpool` وقم بالتحقق من الرقم التسلسلي وcn للشهادة:

```
#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
```

28552066223252

2. للتحقق من التسجيل الناجح لـ ISR4k، قم بتشغيل الأمر `show umbrella device`.

نموذج الإخراج:

```
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
```

إخراج لوحة المعلومات:

115016791766

تصحيح الأخطاء والتسجيل

- التحقق من إصدار ISR4k: `show version` أو `show platform` (يتطلب الأمر Cisco IOS XE Denali 16.3 أو أحدث)
- تمكين سجلات تصحيح أخطاء تسجيل الأجهزة: "`debug umbrella device-register`" ثم "`show logging`" (لتعطيل - `no debug umbrella device-register`)

هذه نماذج من السجلات:

الشهادة مفقودة:

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

تم تثبيت الشهادة وتسجيل الجهاز بنجاح:

```
*%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 غير قابل للحل:

<#root>

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

Failed to resolve name api.opendns.com

Retry attempts:0

- التحقق من دقة DNS: الأمر 'dig' أو 'nslookup' متوفر على ISR4k. إنه أفضل إستخدام ISR4k الأوامر سطر واجهة من "# فيضيل امس اردصم ةهجاول
- ISR مع VRF يشكل: على الواجهة، تأكد من أن لديك ip name-server vrf <vrf_name> <dns_server_ip>" التي تم تكوينها والتحقق منها باستخدام ping vrf <vrf_name> api.opendns.com
- تأكد من تكوين "خادم IP DNS": وهذا يسمح بالاستعلام عن ISR مباشرة.
- لتعطيل تشفير DNSCrypt، أدخل هذا الأمر: no dnscrypt < ةمعلمعا ةطيرخ عون ةلظم
- التحقق من صحة المجال الداخلي: قم بتشغيل الأمر show umbrella config والبحث عن مرجع المجال المحلي، على سبيل المثال:
  - show umbrella config > Local domain regex parameter-map: تجاوز DNS
  - تشغيل العرض | DNS_BYPASS
  - show platform hardware qfp طشن ةمس DNS-snoop-agent client hw-pattern-list
- يتعذر إستيراد الشهادة باستخدام URL أو الشهادة التي تم إستيرادها باستخدام الوحدة الطرفية التي يتم حذفها بعد إعادة التشغيل:

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.

الحل البديل: قم بتنزيل حزمة الشهادة "ios.p7b" يدويا عبر التفاف ونسخ إلى ذاكرة الفلاش الخاصة بالموجه > مسح الشهادة الموجودة من التجمع > إستيراد حزمة الشهادة "ios.p7b" من الذاكرة المؤقتة:

<#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.
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).