Risoluzione dei problemi relativi all'integrazione di Umbrella ISR4k

Sommario

Introduzione

Questo documento descrive come risolvere i problemi relativi all'integrazione con Umbrella ISR4k

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

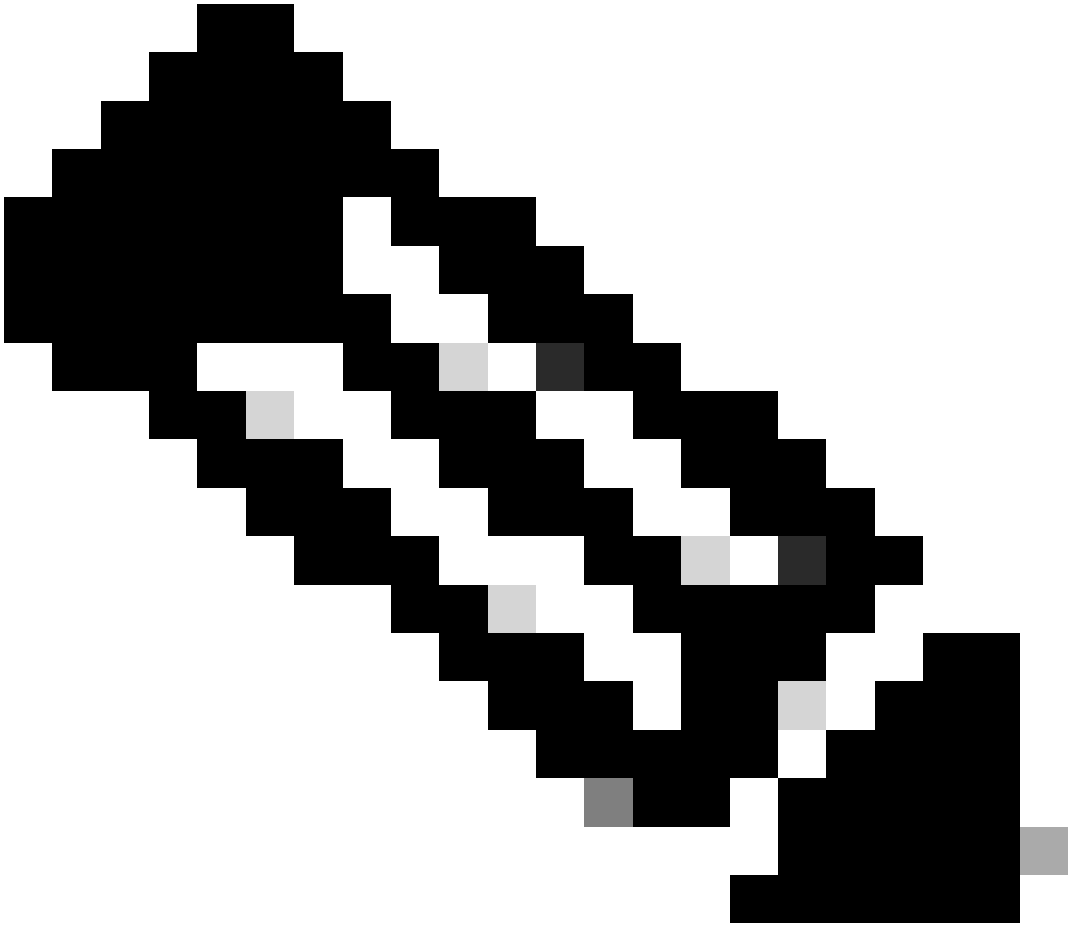
Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Questo articolo è la continuazione della guida alla distribuzione di Cisco Umbrella Integration for ISR4k e viene fornito come guida per la risoluzione dei problemi di registrazione e della risoluzione DNS interna ed esterna.



Nota: Il certificato rinnovato per api.opendns.com dal 29 maggio 2024 è ora firmato da una nuova catena/intermedio/radice. La nuova radice è DigiCert Global Root G2 (seriale: 033af1e6a711a9a0bb2864b11d09fae5).

Registrazione e importazione certificati

1. Ottenere il token API da Umbrella Dashboard: Admin > Chiavi API > (crea) Dispositivi di rete legacy.

2. Importare il certificato CA nell'ISR4k tramite CLI utilizzando uno dei metodi seguenti:

Importa da URL:
Eseguire il comando e consentire a ISR4k di recuperare il certificato:

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

Importare direttamente nel terminale:
Copiare e incollare il certificato CA (vedere l'allegato) utilizzando il comando:

Questo certificato è per 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-----
```

Copiare e incollare il certificato intermedio utilizzando il comando:

(Questo certificato è per 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/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. Immettere il token API nella CLI ISR4k utilizzando il comando:

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

4. Questa è la configurazione di esempio minima per 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
```

Ulteriori informazioni:

- Assicurarsi di configurare "umbrella out" prima del comando "umbrella in".
- La registrazione può avere esito positivo solo quando la porta 443 è in uno stato aperto e consente al traffico di passare attraverso un firewall esistente.
- Nella versione precedente di Cisco IOS XE Denali, viene usato il comando OpenDNS al posto di Umbrella.

Verifica dell'importazione dei certificati e della registrazione dei dispositivi

1. Verificare che il certificato CA sia stato memorizzato correttamente sul dispositivo ISR4k:

- Se il certificato è stato importato utilizzando l'URL, usare il comando `dir nvram:` per verificare che il certificato ios.p7b sia stato archiviato correttamente nella NVRAM del dispositivo.

```
[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

- Se l'importazione del certificato è stata eseguita utilizzando il metodo di copia/incolla, eseguire il comando `show cry pki trustpool` e verificare il numero di serie e il numero di serie del certificato:

```
#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. Per verificare che la registrazione dell'ISR4k sia stata completata correttamente, eseguire il comando `show umbrella deviceid`.

Output di esempio:

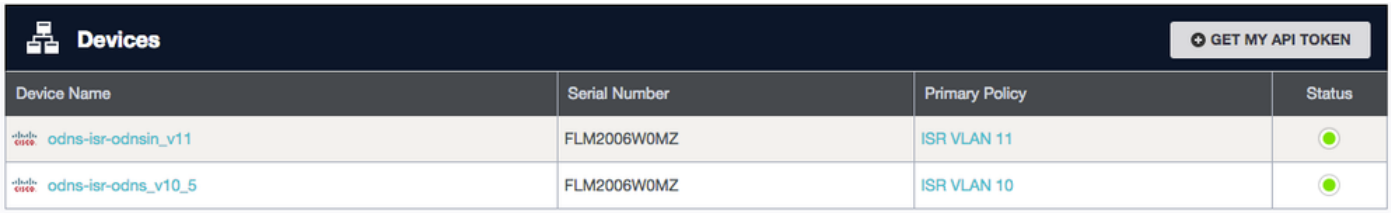
```
Device registration details

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
```

Output dashboard:



115016791766

Debug e registrazione

- Verificare la versione ISR4k: `show version` o `show platform` (richiesto Cisco IOS XE Denali 16.3 o successivo)
- Abilita registri di debug registrazione dispositivo: "`debug umbrella device-registration`", quindi "`show logging`" (per disabilitare, `non eseguire il debug umbrella device-registration`)

Di seguito sono riportati alcuni log di esempio:

Certificato mancante:

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

Il certificato è stato installato e il dispositivo è stato registrato:

```
*%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 non è risolvibile:

<#root>

*%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- Verifica risoluzione DNS: Nessun comando 'dig' o 'nslookup' disponibile su ISR4k. Si consiglia di usare "`ping hostname source interface #`" dalla CLI di ISR4k
- ISR con VRF configurato: Sull'interfaccia, verificare che "`ip name-server vrf <vrf_name> <dns_server_ip>`" sia configurato e verificare con "`ping vrf <vrf_name> api.opendns.com`"
- Verificare che "ip dns server" sia configurato: In questo modo è possibile eseguire direttamente una query sull'RCI.
- Per disabilitare DNSCrypt, immettere questo comando: `parameter-map type umbrella global > no dnscrypt`
- Verifica del dominio interno: eseguire il comando `show umbrella config` e cercare il file Regex del dominio locale, ad esempio:
  - `show umbrella config` > Mapping parametri Regex dominio locale: bypass dns
  - `show run | be dns_bypass`
  - `show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list`
- Impossibile importare il certificato utilizzando l'URL oppure il certificato importato utilizzando il terminale viene eliminato dopo il riavvio:

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.

Soluzione. Scaricare manualmente il pacchetto di certificati "ios.p7b" tramite curl e copiarlo nella memoria flash del router > Cancella il certificato esistente dal pool > Importa il pacchetto di certificati "ios.p7b" dalla memoria 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.
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).