包括ISR4k統合のトラブルシューティング

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

概要

登録と証明書のインポート

証明書インポートとデバイス登録の確認

デバッグと口ギング

はじめに

このドキュメントでは、Umbrella ISR4k統合のトラブルシューティング方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

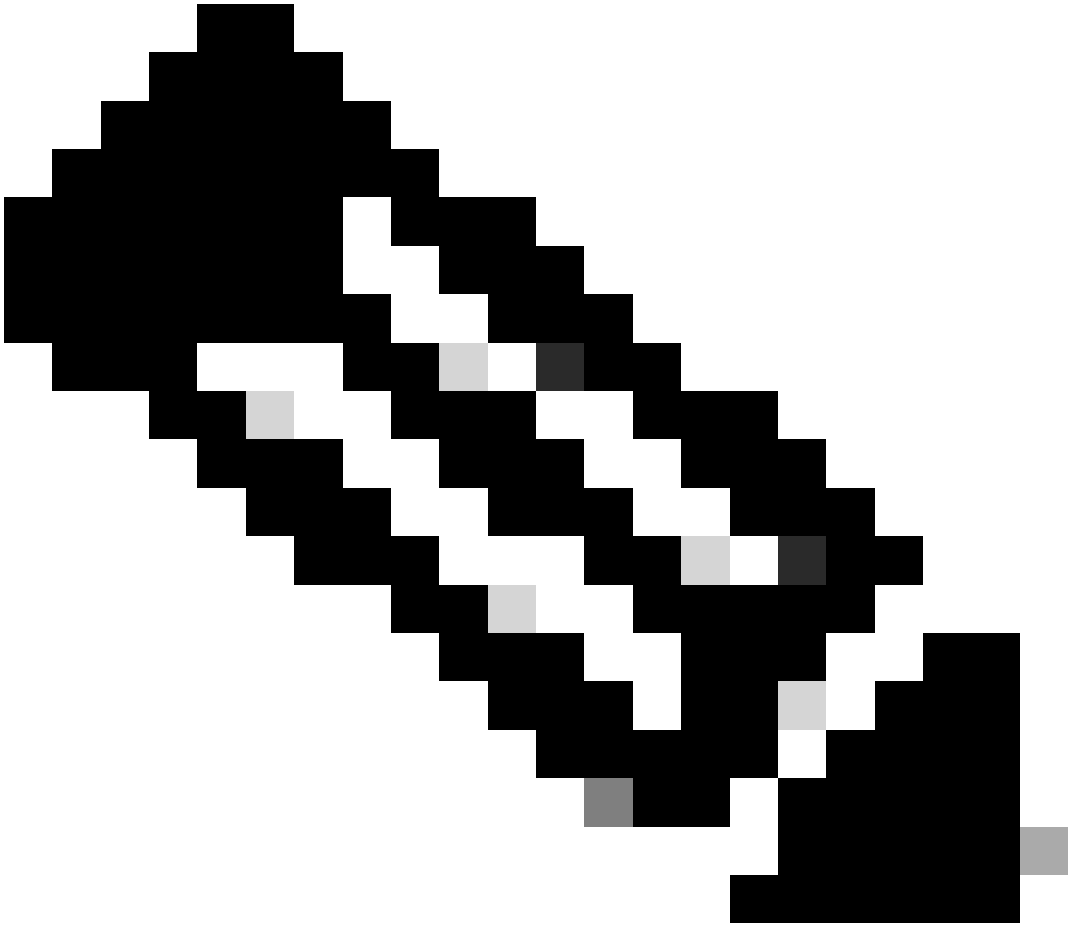
使用するコンポーネント

このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

この記事は『Cisco Umbrella Integration for ISR4k導入ガイド』の続きであり、登録に関する問題や内部および外部のDNS解決に関する問題のトラブルシューティングに役立つガイドとして提供されています。



注:2024年5月29日以降に更新されたapi.opendns.comの証明書には、新しいchain/intermediate/rootが署名されています。新しいルートはDigiCert Global Root G2（シリアル：033af1e6a711a9a0bb2864b11d09fae5）です。

登録と証明書のインポート

1. UmbrellaダッシュボードからAPIトークンを取得します： Admin > API Keys > (create) Legacy Network Devices。

2. 次のいずれかの方法を使用して、CLI経由でISR4kにCA証明書をインポートします。

URLからインポート：
次のコマンドを発行し、ISR4kで証明書を取得できるようにします。

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

端子に直接インポート：
次のコマンドを使用して、CA証明書（添付ファイルを参照）をコピーアンドペーストします。

(この証明書はDigiCert Global Root G2用です)。

```
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-----
```

次のコマンドを使用して、中間証明書をコピーアンドペーストします。

(この証明書はDigiCert Global G2 TLS RSA SHA256 2020 CA1用です)。

```
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+vq5EuOGF485MA4GA1UdDwEB/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. 次のコマンドを使用して、ISR4k CLIにAPIトークンを入力します。

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

4. ISR4kの最低限の設定例を次に示します。

```
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
```

Additional Information:

- 「umbrella in」コマンドを実行する前に、「umbrella out」を設定してください。
- 登録が成功するのは、ポート443がオープン状態で、トラフィックが既存のファイアウォールを通過できる場合だけです。
- 古いバージョンのCisco IOS XE Denaliでは、Umbrellaの代わりにOpenDNSコマンドが使用されていました。

証明書インポートとデバイス登録の確認

1. CA証明書がISR4kデバイスに正常に保存されたかどうかを確認します。

- 証明書のインポートがURLを使用して行われた場合、コマンド`dir nvram:`を発行して、ios.p7b証明書がデバイスのNVRAMに正常に保存されていることを確認します。

```
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

- 証明書のインポートがコピー/ペースト方式を使用して行われた場合は、`show cry pki trustpool`コマンドを実行して、証明書のシリアル番号とcnを確認します。

```
#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. ISR4kが正常に登録されたことを確認するには、`show umbrella deviceid`コマンドを実行します

。

出力例：

```
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
```

ダッシュボード出力：

115016791766

デバッグとロギング

- ISR4kバージョンの確認：`show version`または`show platform`（Cisco IOS XE Denali 16.3以降で必要）
- デバイス登録のデバッグログを有効にします：「`debug umbrella device-registration`」から「`show logging`」(無効にするには、`no debug umbrella device-registration`)

サンプルログを次に示します。

証明書がありません：

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

証明書がインストールされ、デバイスが正常に登録されました：

```
*%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は解決できません：

```
<#root>
```

*%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- DNS解決を確認します。ISR4kには「dig」または「nslookup」コマンドがありません。ISR4k CLIから「ping hostname source interface #」を実行することを推奨します
- VRFが設定されたISR：インターフェイスで、「ip name-server vrf <vrf_name> <dns_server_ip>」が設定されていることを確認し、「ping vrf <vrf_name> api.opendns.com」で確認します。
- 「ip dns server」が設定されていることを確認します。これにより、ISRに対して直接クエリーを実行できます。
- DNSCryptを無効にするには、次のコマンドを入力します。parameter-map type umbrella global > no dnscrypt
- 内部ドメインの検証：コマンドshow umbrella configを実行して、ローカルドメインの正規表現を検索します。次に例を示します。
  - show umbrella config > Local Domain Regexパラメータマップ：dnsバイパス
  - show run | be dns_bypass（この例ではDNSバイパスを使用します）
  - show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list
- URLを使用して証明書をインポートできない、またはターミナルを使用してインポートされた証明書が再起動後に削除される：

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.

回避策：curl経由で「ios.p7b」証明書バンドルを手動でダウンロードし、ルータのフラッシュにコピー>プールから既存の証明書を消去>フラッシュから「ios.p7b」証明書バンドルをインポート：

<#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.
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。