

为基于令牌的配置续订Umbrella根证书

目录

[简介](#)

[前提条件](#)

[要求](#)

[使用的组件](#)

[背景](#)

[执行的步骤](#)

[故障排除](#)

[确认](#)

[相关信息](#)

简介

本文档介绍将基于令牌的注册用于Cisco IOS® XE SD-WAN设备时更新Umbrella根证书的过程。

前提条件

要求

Cisco 建议您了解以下主题：

- 公钥基础设施(PKI)基础知识。
- Cisco SD-WAN技术知识

仅当您使用基于令牌的Umbrella注册时，才会使用此工作流程。如果您使用基于API的注册，请执行Field Notice [FN74166](#)中提到的步骤，以获取安装的根证书。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- C8000V版本17.6.6
- vManage版本20.6.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

Umbrella从2024年5月29日起续订FQDN api.opendns.com的证书，并且证书由新的根ca DigiCert全局根G2签署。如果边缘设备在PKI证书列表中不存在此根ca，并且如果它使用基于令牌的

Umbrella注册，则Umbrella注册将失败。本文档的工作流程介绍如何在边缘路由器上安装root-ca。

执行的步骤

请检查边缘设备是否具有基于令牌的Umbrella注册。这是配置的外观。

```
parameter-map type umbrella global
 token 83F1YHF457592596A3D8CF52YHDFSDRD
```

边缘设备注册过程启动、获取根证书并安装所需的其他配置。

```
parameter-map type umbrella global
 vrf 10
 dns-resolver umbrella >>>>required

ip nat inside source list nat-acl interface GigabitEthernet0/0/0 overload

interface GigabitEthernet0/0/0
 ip dhcp client client-id ascii FGL233913F6
 ip address 10.122.164.132 255.255.255.128
 ip nat outside >>>>>
 negotiation auto
end
```

在边缘设备上，检查位置/bootflash中是否存在根证书trustidrootx3_ca_092024.ca。

```
edge-ISR1100-4G#dir bootflash: | in .ca
30 -rw- 237 Aug 13 2024 08:47:55 +00:00 pki_certificates
25 -rw- 1294 Aug 13 2024 08:46:54 +00:00 trustidrootx3_ca_092024.ca
```

在位于位置/bootflash/sdwan的边缘设备上下载此根证书“DigiCert全局根G2”，名称为trustidrootx3_ca_092024.ca。

```
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUN1cnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWN1cnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDEwMjAwMDAaMTUxMjAwMDAeFw0xMzA4MDEwMjAwMDAaMTUxMjAw
MRUwEwYDVQQKEwEaWdpQ2VydCBHbG9iYWwgYVBAcTEhIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAuzfNnN7a8myaJCtSnX/RrohCgiN9R1UyfuI2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsuLecYxpsMNzaHxmx
1x7e/dfgy5SDN67sHON03Xss0r0upS/kqbit0tSZpLY16ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUt1uNJbd134/tJS7SsVQepj5Wz
```

```
tC07TG1F8PapsUwtP1MVYwnS1cUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vI01CsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJJobq7nMwxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rks7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Y19PMWLsn/pvtsrF9+wX3N3KjIT0YFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitra1j41E6Vf8P1wUHBHQRFxGU7Aj64GxJUTFy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexGRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj11DiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1
MrY=
```

-----END CERTIFICATE-----

通过将旧的根证书重命名为trustidrootx3_ca_092024.ca.bkp，将其在
/bootflash : trustidrootx3_ca_092024.ca下移到/bootflash/sdwan。

```
copy bootflash:trustidrootx3_ca_092024.ca bootflash:sdwan/trustidrootx3_ca_092024.ca.bkp
```


从/bootflash中删除根证书trustidrootx3_ca_092024.ca。

```
cedge-ISR1100-4G#delete bootflash:trustidrootx3_ca_092024.ca
```

将/bootflash/sdwan下的新根证书trustidrootx3_ca_092024.ca移到/bootflash。

```
copy bootflash:sdwan/trustidrootx3_ca_092024.ca bootflash:
```

重新加载边缘设备。

 注意：如果您具有基于令牌的Umbrella注册，则需要遵循此流程。如果使用了基于API的注册，则本文档中引用的现场通知中的流程需要遵守。

故障排除

可以在边缘设备上启用这些调试，以查看是否安装了新的根证书。

```
cedge-ISR1100-4G#debug umbrella device-registration
```

要查看日志，您可以执行show logging或检查/tmp/rp/trace下的IOSRP_R0文件。您会看到这些日志

。

成功

```
2024/08/13 08:36:18.289855465 {IOSRP_R0-0}{1}: [iosrp] [24596]: UUID: 0, ra: 0, (info): *Aug 13 08:36:
```

失败

```
2024/08/13 08:36:20.838420795 {IOSRP_R0-0}{1}: [iosrp] [24596]: UUID: 0, ra: 0, (warn): *Aug 13 08:36:
```

确认

要验证是否已在边缘设备上成功安装证书，可以使用以下命令。

```
cedge-ISR1100-4G#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 033AF1E6A711A9A0BB2864B11D09FAE5
  Certificate Usage: Signature
  Issuer:
    cn=DigiCert Global Root G2
    ou=www.digicert.com
    o=DigiCert Inc
    c=US
  Subject:
    cn=DigiCert Global Root G2
    ou=www.digicert.com
    o=DigiCert Inc
    c=US
  Validity Date:
    start date: 12:00:00 UTC Aug 1 2013
    end date: 12:00:00 UTC Jan 15 2038
  Associated Trustpoints: trustidrootx3_ca_092024
  Storage: nvram:DigiCertGlob#FAE5CA.cer
```

```
cedge-ISR1100-4G#show crypto pki trustpoints
Trustpoint SLA-TrustPoint:
  Subject Name:
    cn=Cisco Licensing Root CA
    o=Cisco
    Serial Number (hex): 01
  Certificate configured.
```

```
Trustpoint trustidrootx3_ca_092024:
  Subject Name:
```

cn=DigiCert Global Root G2
ou=www.digicert.com
o=DigiCert Inc
c=US

Serial Number (hex): 033AF1E6A711A9A0BB2864B11D09FAE5
Certificate configured.

相关信息

- [Cisco Umbrella集成](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。