Erneuern des Umbrella-Stammzertifikats für eine tokenbasierte Konfiguration

Inhalt

Einleitung

In diesem Dokument wird der Prozess zur Verlängerung des Umbrella-Root-Zertifikats beschrieben, wenn für Cisco IOS® XE SD-WAN-Geräte eine tokenbasierte Registrierung verwendet wird.

Voraussetzung

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Public Key Infrastructure (PKI).
- Kenntnisse der Cisco SD-WAN-Technologie

Dieser Workflow kann nur verwendet werden, wenn Sie eine tokenbasierte Umbrella-Registrierung verwenden. Wenn Sie eine API-basierte Registrierung verwenden, führen Sie die in Problemhinweis FN74166 genannten Schritte aus, um das Root-Zertifikat zu installieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C8000V Version 17.6.6
- vManage, Version 20.6.6

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.

Hintergrund

Umbrella hat das Zertifikat für FQDN api.opendns.com ab dem 29. Mai 2024 erneuert und das Zertifikat wurde von einem neuen Root-ca DigiCert Global Root G2 signiert. Wenn das Edge-Gerät diesen Root-ca nicht in der PKI-Zertifikatsliste hat und die tokenbasierte Umbrella-Registrierung verwendet wird, schlägt die Umbrella-Registrierung fehl. Der Workflow in diesem Dokument beschreibt die Installation des Root-CA auf dem Edge-Router.

Durchzuführende Schritte

Überprüfen Sie, ob das Edge-Gerät über eine tokenbasierte Umbrella-Registrierung verfügt. So würde die Konfiguration aussehen.

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

Andere Konfiguration, die für den Registrierungsvorgang des Edge-Geräts initiiert werden muss, damit dieses das Root-Zertifikat übernehmen und installieren kann.

```
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
```

Überprüfen Sie auf dem Edge-Gerät, ob das Stammzertifikat trustidrootx3_ca_092024.ca am Speicherort/bootflash vorhanden ist.

```
cedge-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
```

Laden Sie dieses Root-Zertifikat "DigiCert Global Root G2" auf das Edge-Gerät am Standort/bootflash/sdwan mit dem Namen trustidrootx3_ca_092024.ca herunter.

```
-----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-----
```

Verschieben Sie das alte Root-Zertifikat unter /bootflash:trustidrootx3_ca_092024.ca nach /bootflash/sdwan, indem Sie es in trustidrootx3_ca_092024.ca.bkp umbenennen.

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

Löschen Sie das Stammzertifikat trustidrootx3_ca_092024.ca aus /bootflash.

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

Verschieben Sie das neue Stammzertifikat trustidrootx3_ca_092024.ca unter /bootflash/sdwan nach /bootflash.

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

Laden Sie das Edge-Gerät neu.

Hinweis: Dieser Prozess muss ausgeführt werden, wenn Sie eine tokenbasierte Umbrella-Registrierung haben. Bei Verwendung einer API-basierten Registrierung muss der Prozess in der in diesem Dokument erwähnten Problembeschreibung befolgt werden.

Fehlerbehebung

Diese Debug-Funktionen können auf dem Edge-Gerät aktiviert werden, um festzustellen, ob das neue Stammzertifikat installiert wird.

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

Um die Protokolle anzuzeigen, können Sie entweder die Protokollierung anzeigen lassen oder die Datei IOSRP_R0 unter /tmp/rp/trace überprüfen. Diese Protokolle werden angezeigt.

Erfolg

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

Fehler

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

Verifizierung

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob das Zertifikat erfolgreich auf dem Edge-Gerät installiert wurde.

```
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.
```

Zugehörige Informationen

- Cisco Umbrella-Integration
- Technischer Support und Dokumentation für Cisco Systeme

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.