

トークンベースの構成のUmbrellaルート証明書 の更新

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景](#)

[実行手順](#)

[トラブルシューティング](#)

[検証](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco IOS® XE SD-WANデバイスでトークンベースの登録を使用する場合に、Umbrellaルート証明書を更新するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 公開キーインフラストラクチャ(PKI)の基礎知識。
- Cisco SD-WANテクノロジーの知識

このワークフローは、トークンベースのUmbrella登録を使用している場合にのみ使用されます。APIベースの登録を使用している場合は、Field Notice [FN74166](#)に記載されている手順に従ってルート証明書をインストールする必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.6.6
- vManageバージョン20.6.6

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。

背景

Umbrellaは2024年5月29日からFQDN api.opendns.comの証明書を更新し、証明書は新しいルートca DigiCert Global Root G2によって署名されました。エッジデバイスのPKI証明書リストにこのルートcaが存在せず、トークンベースのUmbrella登録を使用している場合、Umbrella登録は失敗します。このドキュメントのワークフローでは、エッジルータにルートcaをインストールする方法について説明します。

実行手順

エッジデバイスにトークンベースのUmbrella登録があるかどうかを確認してください。設定はこのように表示されます。

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

エッジデバイス登録プロセスを開始し、ルート証明書を取得してインストールするために必要なその他の設定。

```
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
```

エッジデバイスで、ルート証明書trustidrootx3_ca_092024.caが/bootflashに存在するかどうかを確認します。

```
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
```

このルート証明書「DigiCert Global Root G2」をエッジデバイス(/bootflash/sdwan)に

trustidrootx3_ca_092024.caという名前でダウンロードします。

-----BEGIN CERTIFICATE-----

```
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZG1naWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDEEMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBjb210ZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
b20xIDAeBgNVBAMTF0Rpb210ZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZlZDZl
9w0BAQEFAAOCAQ8AMIIBCgKCAQEaUzfnNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sHON03Xss0r0upS/kqbit0tSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZiYa7XzV+hdG82MHauVBjVJ8zUt1uNjbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsUwtP1MvYwnS1cUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vI07CsRnKPzZFBQ9RnbDhxSJITRnrw9FDKZJobq7nMwxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rks7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLsn/pvtsrF9+wX3N3KjIToYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UwTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNu+MeKNhJ7jitra1j41E6Vf8P1wUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiawN0bfVKfj11DiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1Ww6LZZm6zNTf1
MrY=
```

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

/bootflash:trustidrootx3_ca_092024.caの下にある古いルート証明書の名前を trustidrootx3_ca_092024.ca.bkpに変更し、/bootflash/sdwanに移動します。

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


ルート証明書trustidrootx3_ca_092024.caを/bootflashから削除します。

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

/bootflash/sdwanにある新しいルート証明書trustidrootx3_ca_092024.caを/bootflashに移動します。

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

エッジデバイスをリロードします。

 注：トークンベースのUmbrella登録がある場合は、このプロセスに従う必要があります。
APIベースの登録を使用する場合は、このドキュメントで参照されているField Noticeのプロセスに従う必要があります。

トラブルシューティング

これらのデバッグをエッジデバイスで有効にして、新しいルート証明書がインストールされているかどうかを確認できます。

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

ログを確認するには、show loggingを実行するか、/tmp/rp/traceの下のファイルIOSRP_R0をチェックします。次のログが表示されます。

成功

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

失敗

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

検証

エッジデバイスに証明書が正常にインストールされたかどうかを確認するには、次のコマンドを使用します。

```
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.
```

関連情報

- [Cisco Umbrellaの統合](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

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。