Het gebruik van Let's Encrypt Certificaten met Cisco Business Dashboard en DNS-validatie

Doel

Dit document legt uit hoe u een *Let's Encrypt*-certificaat kunt verkrijgen en installeert het op Cisco Business Dashboard met behulp van de Opdracht Line Interface (CLI). Als u algemene informatie wilt over het beheer van certificaten, controleer dan het artikel Certificaten beheren op het Cisco Business Dashboard.

Inleiding

Let's Encrypt is een certificaatinstantie die gratis, Domain Validation (DV) SSL-certificaten aan het publiek verstrekt door middel van een geautomatiseerd proces. *Laten we Encrypt* een makkelijk toegankelijk mechanisme bieden voor het verkrijgen van ondertekende certificaten voor webservers, wat het eindgebruiker vertrouwen geeft dat hij toegang heeft tot de juiste service. Ga voor meer informatie over *Let's Encrypt* op de website van Let's Encrypt.

Het gebruik van *Let's Encrypt* certificaten met Cisco Business Dashboard is redelijk eenvoudig. Hoewel Cisco Business Dashboard enige speciale vereisten heeft voor de installatie van certificaten naast het beschikbaar maken van het certificaat aan de webserver, is het nog steeds mogelijk de afgifte en installatie van het certificaat te automatiseren met behulp van de meegeleverde gereedschappen voor opdrachtregel.

Als u automatisch certificaten wilt uitgeven en verlengen, moet de Dashboard webserver vanaf het internet bereikbaar zijn. Als dit niet het geval is, kan een certificaat eenvoudig worden verkregen met behulp van een handmatig proces en kan het worden geïnstalleerd met behulp van de gereedschappen voor de opdrachtregel. De rest van dit document loopt via de procedure voor de afgifte van een certificaat en de installatie ervan op het Dashboard.

Als de Dashboard webserver bereikbaar is vanaf het internet op de standaardpoorten TCP/80 en TCP/443, is het mogelijk om het certificaatbeheer te automatiseren en het installatieproces te installeren. Controleer Let op Let's Encrypt voor Cisco Business Dashboard voor meer informatie.

Stap 1

De eerste stap is het verkrijgen van software die het ACME protocol certificaat gebruikt. In dit voorbeeld gebruiken we de tartbot client, maar er zijn veel andere opties beschikbaar.

Om de tartbotclient te verkrijgen, gebruikt u het Dashboard of een andere host die een Unix-achtige OS runt (bijv. Linux, macOS) en volgt u de instructies op de tartbot client om de client te installeren. Selecteer in de vervolgkeuzemenu's op deze pagina *de optie Geen van de bovenstaande opties* voor software en uw favoriete besturingssysteem voor het systeem.

Het is belangrijk op te merken dat in dit artikel blauwe delen worden gevraagd en geproduceerd vanuit CLI. De opdrachten `voor de` witte `tekst` staan in de lijst. Groene gekleurde opdrachten, waaronder dashboard.voorbeeldv.com, pnpserver.voorbeeldcom en user@example.com moeten worden vervangen door DNS-namen die geschikt zijn voor uw omgeving.

U kunt de volgende opdrachten gebruiken om de tartbotclient op de Cisco Business Dashboard-server te installeren:

```
cbd : $sudo apt update cbd:~$sudo installeert software-eigenschappen-alledaags cbd:~$sudo add-apt-opslagplaats ppa:certbot/certbot cbd : $sudo apt update cbd :~$sudo apt installeert tartbot
```

Stap 2

Maak een werkmap met alle bestanden die aan het certificaat gekoppeld zijn. Let op dat deze bestanden gevoelige informatie bevatten, zoals de privé-sleutel voor het certificaat en de accountgegevens voor de *Let's Encrypt* service. Terwijl de certbot client bestanden maakt met voldoende beperkingen, dient u er voor te zorgen dat de host en de account die gebruikt wordt, beperkt zijn voor toegang tot alleen geautoriseerd personeel.

Als u de map op het Dashboard wilt maken, voert u de volgende opdrachten in:

```
cbd :~$ mkdir certbot cbd:~/certbot $cd-tartbot
```

Stap 3

Aanvragen van een certificaat met de volgende opdracht:

```
cbd:~/certbot$certbot certonly —Manual —preferred-challenge dns -d dashboard.voorbeelds.com -d pnpserver.voorbeeldcom
—logs-dir. —configuratie-dir. —werkdir. —stel de haak "cat ~/certbot/live/dashboard.voorbeeld.com/fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-dashboard invoer -t pem -k ~/certbot/live/dashboard.voorbeeld.com /privkey.pem -c /tmp/cbdchain.pem"
```

Deze opdracht geeft de service *Encrypt* op *om* de eigendom van de hostnamen te valideren door u te vragen DNS TXT-records voor elk van de vermelde namen te maken. Zodra de TXT-bestanden zijn gemaakt, bevestigt de *dienst Encrypt* dat de bestanden bestaan en geeft u het certificaat af. Tot slot wordt het certificaat toegepast op het dashboard met behulp van het cisco-business-dashboard hulpprogramma.

De parameters in de opdracht zijn om de volgende redenen vereist:

certalleen	Offerte aanvragen en de bestanden downloaden. Probeer ze niet te installeren. In het geval van Cisco Business Dashboard wordt het certificaat niet alleen gebruikt door de webserver, maar ook door de VPN-service en andere functies. Als gevolg daarvan kan de tartbotclient het certificaat niet automatisch installeren.
—handleiding	Probeer niet automatisch te authenticeren met de *Let's Encrypt* service. Werk interactief met de gebruiker om authenticatie te bewerkstelligen.
—dns voor favoriete uitdagingen	Verifieer het gebruik van DNS TXT-records.
-d dashboard.voorbeeld.com -d pnpserver.voorbeeld.com	De FQDN's die in het certificaat moeten worden opgenomen. De voornaam wordt in het veld Naam van het certificaat opgenomen en alle namen worden in het veld Naam van het onderwerp vermeld. De VPN-server.<domeinnaam> is een speciale naam die door de functie Netwerk plug and Play wordt gebruikt bij het uitvoeren van DNS-ontdekking. Raadpleeg de Cisco Business Dashboard Management Guide voor meer informatie.
—logs-dir.	Gebruik de huidige map voor alle werkbestanden die tijdens

—configuratie-dir. —werkdir.	het proces zijn gemaakt.
—pudhaak "..."	Gebruik het commando line hulpprogramma van cisco-business-dashboard om de privésleutel en de certificaatketen te nemen die van de dienst *Let's Encrypt* worden ontvangen en ze op dezelfde manier in de dashboard toepassing te laden als als wanneer de bestanden via de Dashboard User Interface (UI) zijn geüpload. Het basiscertificaat dat de certificeringsketen verankert wordt hier ook aan het certificaatbestand toegevoegd. Dit wordt vereist door bepaalde platforms die worden ingezet met Network Plug en Play.

Automatische installatie van het certificaat met de optie —implementeren-haak is alleen mogelijk wanneer de tartbotclient op de dashboard server wordt uitgevoerd. Als de client op een andere computer wordt uitgevoerd, worden de certificeringsbestanden van de privé-toets en de volledige ketting gekopieerd naar de dashboard server en geïnstalleerd met de opdrachten:
-cat <fullchain certificate file> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-dashboard importplatform -t pem-k <private key file> -c /tmp/cbdchain.pem

Stap 4

Volg de procedure voor het maken van het certificaat door de instructies te volgen die door de tartbotclient zijn gegenereerd:

```
cbd:~/certbot$certbot certonly —Manual —preferred-challenge dns -d dashboard.voorbeelds.com -d
pnpserver.voorbeeldcom
—logs-dir. —configuratie-dir. —werkdir. —stel de haak "cat ~/certbot/live/
dashboard.voorbeeld.com/fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem;
/usr/bin/cisco-business-dashboard invoer -t pem -k ~/certbot/live/dashboard.voorbeeld.com
/privkey.pem -c tmp/cbdchain.pem"
Debug loggen opslaan op /home/cisco/certbot/letsencrypt.log
Geselecteerde stekkers: Verificatiehandleiding, installatieprogramma, geen
```

Stap 5

Voer het e-mailadres in of **C** om te annuleren.

```
Voer een e-mailadres in (gebruikt voor spoedeisende vernieuwing en veiligheidsmededelingen) (Typ
'c' om te annuleren): user@example.com
Nieuwe HTTPS-verbinding starten (1): acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Stap 6

Typ **A** om **het** goed te keuren of **C** om te annuleren.

```
Lees de servicevoorwaarden door op
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. U moet
stemmen in met als doel zich te registreren op de ACME-server op
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
Typ A om het goed te keuren of C om te annuleren.
A)groe/(C)ancel: A
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Stap 7

Voer **Y in** voor Ja of **N** voor Nee.

```
Wilt u uw e-mailadres met de elektronische grens delen?
Foundation, oprichter van het Let's Encrypt project en non-profit
organisatie die Certbot ontwikkelt? We sturen je graag e-mail over ons werk
Het EFF-nieuws, -campagnes en -manieren om digitale vrijheid te ondersteunen versleutelen.
Voer Y in voor Ja of N voor Nee.
(Y)es/(N)o: Y
Een nieuw certificaat verkrijgen
De volgende uitdagingen uitvoeren:
dns-01-uitdaging voor dashboard.voorbeeld.com
dns-01-uitdaging voor pnpserver.voorbeeldcom
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Stap 8

Voer **Y in** voor Ja of **N** voor Nee.

```
OPMERKING: Het IP van deze machine wordt gepubliceerd als zijnde vereist
certificaat. Als u de machine handmatig in de modus zet op een machine die niet actief is
Uw server, zorg er alstublieft voor dat u het daarmee eens bent.
Ben je oké dat je IP wordt ingelogd?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Voer Y in voor Ja of N voor Nee.
(Y)es/(N)o: Y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Installeer een DNS TXT-record onder de naam
_acme-challenge.dashboard.voorbeeld.com met de volgende waarde:
3AzDTqNGXb8kSHQXXYWE2iZRFAVCGT2B8NhBWK
```

Stap 9

Een DNS TXT-record om de eigendom van de hostname van dashboard.voorbeeld.com te valideren, moet in de DNS-infrastructuur worden aangemaakt. De daartoe vereiste stappen vallen buiten het toepassingsgebied van dit document en zullen afhangen van het gebruik van de DNS-provider. Bevestig dat de record beschikbaar is op basis van een DNS-query-tool zoals Dig.

Het DNS-uitdagingsproces kan voor bepaalde DNS-aanbieders worden geautomatiseerd. Zie DNS-plug-in voor meer informatie.

Druk op **ENTER** op uw toetsenbord.

```
Controleer, voordat u doorgaat, of de gegevens worden gebruikt.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Druk op ENTER om verder te gaan
```

Stap 10

U ontvangt een soortgelijke CLI-uitvoer. Maak en controleer aanvullende TXT-bestanden voor elke naam die in het certificaat moet worden opgenomen. Herhaal stap 9 voor elke naam die in de tartbot-opdracht is gespecificeerd.

Druk op **ENTER** op uw toetsenbord.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Installeer een DNS TXT-record onder de naam
_acme-challenge.pserver.voorbeeldcom met de volgende waarde:
Txruc89x8dVaHmLHJII0oA2ILmIY83XY13yYakjNuc
Controleer, voordat u doorgaat, of de gegevens worden gebruikt.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Druk op ENTER om verder te gaan
```

Stap 11

Het certificaat is afgegeven en kan worden gevonden in het subdirectoraat *live* in het bestandssysteem:

```
Wachten op verificatie...
Opruimen van problemen
Niet-standaard pad(en) werken mogelijk niet met een tab geïnstalleerd door de systeembeheerder
Plaatsing-shaak opdracht uitvoeren: cat ~/certbot/live/dashboard.example.com/fullchain.pem
/etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-dashboard invoer
-t pem-k ~/certbot/live/dashboard.example.com/privkey.pem-c /tmp/cbdchain.pem
BELANGRIJKE OPMERKINGEN:
- Gefeliciteerd! Uw certificaat en keten zijn opgeslagen op:
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
Uw sleutelbestand is opgeslagen op:
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Uw cert vervalt op 2020-11-11. Voor een nieuwe of getweeklekte applicatie
versie van dit certificaat in de toekomst, gebruik gewoon de tartbot
nogmaals. Om *all* van uw certificaten niet interactief te vernieuwen, loop
"tartbot vernieuwt "
- Uw account is ongeldig gemaakt in uw Certbot
configuratiemap in de startpagina/cisco/tartbot. U moet een
veilige back-up van deze map nu. Deze configuratiemap zal
bevat ook certificaten en privésleutels die door Certbot zijn verkregen.
het maken van regelmatige back-ups van deze map is ideaal .
- Als u Certbot leuk vindt, overweegt u dan om ons werk te ondersteunen door:
Doneren aan ISRG / Laten we versleutelen: https://letsencrypt.org/donate
Doneren aan EFF: https://eff.org/donate-le
```

Stap 12

Geef de volgende opdrachten op:

```
cbd:~/certbot$cd live/dashboard.voorbeeld.com/dashboard cbd
:~/certbot/live/dashboard.example.com$ls
cert.pem chain.pem fullchain.pem privé.pem README
```

De map met de certificaten heeft beperkte toegang zodat alleen de cisco-gebruiker de bestanden kan bekijken. Het bestand *particuliere.pem* is met name gevoelig en de toegang tot dit bestand dient beperkt te blijven tot geautoriseerd personeel.

Het Dashboard moet nu worden gebruikt met het nieuwe certificaat. Als u de Dashboard User Interface (UI) in een webbrowser opent door een van de namen in te voeren die zijn opgegeven bij het maken van het certificaat in de adresbalk, dan geeft de webbrowser aan dat de verbinding

betrouwbaar en veilig is.

Merk op dat certificaten die zijn afgegeven door *Let's Encrypt* relatief korte levensduur hebben - momenteel 90 dagen. Om er zeker van te zijn dat het certificaat geldig blijft, moet u de hierboven beschreven procedure herhalen voordat de 90 dagen zijn verstreken.

Zie de documentpagina van de tartbotclient voor meer informatie over het gebruik van de tartbot client.