Het gebruik van Let's Encrypt Certificaten met Cisco Business Dashboard

Doel

Dit document legt uit hoe u een *Let's Encrypt*-certificaat kunt verkrijgen, het op Cisco Business Dashboard installeert en automatisch vernieuwing installeert 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.

Het in dit document beschreven proces is geautomatiseerd in Cisco Business Dashboard versie 2.2.2 en hoger. Raadpleeg het gedeelte Systeem > Certificaten beheren van de beheerdershandleiding voor meer informatie.

Inleiding

Let's Encrypt is een certificaatinstantie die het publiek met behulp van een geautomatiseerd proces gratis, Domeinvalidatie (DV) Secure Socket Layer (SSL)-certificaten verstrekt. *Versleutelen* biedt een gemakkelijk toegankelijk mechanisme voor het verkrijgen van ondertekende certificaten voor webservers, waardoor de eindgebruiker erop kan vertrouwen dat hij toegang heeft tot de juiste dienst. Ga voor meer informatie naar de website 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. De rest van dit document loopt door het proces van afgifte van een certificaat en automatisering van de vernieuwing van het certificaat.

Dit document gebruikt HTTP-uitdagingen om domeineigendom te valideren. Dit vereist dat de Dashboard webserver bereikbaar is vanaf het internet op standaardpoorten TCP/80 en TCP/443. Als de webserver niet bereikbaar is vanaf het internet, dan kunt u overwegen DNS-uitdagingen in plaats daarvan te gebruiken. Controleer of Let op het gebruik van Let's Encrypt voor Cisco Business Dashboard met DNS 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.

Stap 2

Om de vernieuwing van het certificaat te kunnen automatiseren, moet de tartbotclient op het Dashboard zijn geïnstalleerd. U kunt de volgende opdrachten gebruiken om de tartbotclient op de Dashboard-server te installeren:

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.

```
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 3

Daarna moet de Dashboard webserver worden ingesteld om de challenge files te ontvangen die vereist zijn om de eigendom van de hostname te controleren. Om dit te doen, maken we een folder voor deze bestanden en werken we het configuratiebestand van de webserver bij. Vervolgens herstarten we de Dashboard-toepassing zodat de wijzigingen van kracht worden. Gebruik de volgende opdrachten:

```
cbd:~$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo chmod
755/usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo bash-c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' < EOF
# Plaats voor provoceringsbestanden gemaakt door locatie van de tartbot /.welbekende/acme-
challenge {
wortel/gebruiker/lib/ciscobusiness/dashboard/www/letsencrypt;
>
waarvan
cbd:~$ cbd :~$sudo chown cbd:cbd /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-
letsencrypt.conf cbd :~$sudo chmod 640 /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-
letsencrypt.conf cbd:$cisco-business-dashboard-stop cbd:~$cisco-business-dashboard start
```

Stap 4

Aanvragen van een certificaat met de volgende opdracht:

```
cbd:~$sudo certbot certonly –webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.voorbeeld.com-d pnpserver.voorbeeld.com –ingericht-haak "cat/etc/letsencrypt/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/etc/letsencrypt/live/dashboard.voorbeelds.com
/privkey.pem-c /tmp/cbdchain.pem
```

Deze opdracht geeft de *Let's Encrypt* service opdracht om de eigendom van de hostnamen te valideren door verbinding te maken met de webservice die op elk van de namen wordt gehost. Dit betekent dat de dashboard webservice via het internet toegankelijk moet zijn en op poorten 80 en 443 moet worden gehost. De toegang tot de dashboard-toepassing kan worden beperkt met behulp van de Access Control-instellingen op het systeem > Platform-instellingen > Webpagina in het dashboard-beheergebruikersinterface (UI). Raadpleeg de Cisco Business Dashboard Management Guide voor meer informatie.

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.
—webroot -w ...	Installeer de uitdagingsbestanden in de bovengenoemde map zodat ze toegankelijk zijn via de dashboard webserver.
-d dashboard.voorbeeld.com	De FQDN's die in het certificaat moeten worden opgenomen. De voornaam wordt in het veld Naam van het certificaat

-d pnpserver.voorbeeld.com	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.
—pudhaak "..."	Gebruik het commando line hulpprogramma van cisco-business-dashboard om de privésleutel en de certificeringsketen 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.

Stap 5

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

```
cbd:~$sudo certbot certonly –webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.voorbeeld.com-d pnpserver.voorbeeld.com –ingericht-haak "cat/etc/letsencrypt/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/etc/letsencrypt/live/dashboard.voorbeeldd.com
/privkey.pem-c /tmp/cbdchain.pem"
Debug loggen opslaan op /var/log/letsencrypt/letsencrypt.log
Geselecteerde stekkers: Verificatiebron, installatieprogramma, geen
```

Stap 6

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

```
Voer een e-mailadres in (gebruikt voor spoedeisende vernieuwing en veiligheidsmededelingen)
(Voer 'c' in om
annuleren): user@example.com
```

Stap 7

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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
A)groe/(C)ancel: A
```

Stap 8

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

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Wilt u uw e-mailadres met de elektronische grens delen?
Foundation, een oprichter van het Let's Encrypt-project en de non-profitorganisatie
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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
```

Stap 9

Het certificaat is afgegeven en kan worden gevonden in de submap *etc/letsencrypt/live* in het bestandssysteem:

```
Een nieuw certificaat verkrijgen
De volgende uitdagingen uitvoeren:
http-01 challenge voor dashboard.voorbeeld.com
http-01 challenge voor pserver.voorbeeldcom
Gebruik van het snijpad /usr/lib/ciscobusiness/dashboard/www/letsencrypt voor alle niet
afgesloten domeinen.
Wachten op verificatie...
Opruimen van problemen
Plaatsing-shaak opdracht uitvoeren: cat
/etc/letsencrypt/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
/etc/letsencrypt/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem
BELANGRIJKE OPMERKINGEN:
- Gefeliciteerd! Uw certificaat en keten zijn opgeslagen op:
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
Uw sleutelbestand is opgeslagen op:
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Uw cert vervalt op 2020-10-29. 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 op /etc/letsencrypt. 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
cbd:~$ sudo ls/etc/letsencrypt/live/dashboard.voorbeeld.com
/ cert.pem chain.pem fullchain.pem privé.pem README
cbd:~$
```

De map met de certificaten heeft beperkte rechten zodat alleen de root 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.

Stap 10

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 door *Let's Encrypt* afgegeven certificaten relatief korte levensduur hebben - momenteel 90 dagen. Het tartbot-pakket voor Ubuntu Linux is ingesteld om de geldigheid van het certificaat twee keer per dag te controleren en het certificaat te verlengen indien het nadert, zodat er geen actie vereist is om het certificaat up-to-date te houden. Om na te gaan of de periodieke controles correct verlopen, moet u ten minste twaalf uur wachten na de eerste invoering van het certificaat en vervolgens het logbestand van de tartbot controleren op berichten die vergelijkbaar zijn met de volgende: `cbd :~$ sudo - staart /var/log/letsencrypt/letsencrypt.log`

```
2020-07-31 16:50:52.783:DEBUG:certbot.main:tartbot versie: 0.31.0
2020-07-31 16:50:52.784:DEBUG:certbot.main:Argumenten: ['-q']
2020-07-31 16:50:52.785:DEBUG:certbot.main:ontdekte stekkers:
(PluginEntryPoint#handmatig,
PluginEntryPoint#ongeldige, PluginEntryPoint#standalone, PluginEntryPoint#webroot)
2020-07-31 16:50:52.793:DEBUG:certbot.log:Root logging level ingesteld op 30
2020-07-31 16:50:52.793:INFO:tartbot.log:opslaan van debug
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52:802:DEBUG:certbot.plug-ins.selectie:
Vereiste authenticator <certbot.cli.
_Standaardobject bij 0x7f152969240> en installateur <certbot.cli.
_Standaardobject op 0x7f152969240>
2020-07-31 16:50:52,811:INFO:tartbot.vernieuwing:Kert nog niet te verlengen
2020-07-31 16:50:52.812:DEBUG:certbot.plug-ins.Selectie:Verzocht authentiek
product en installateur Geen
2020-07-31 16:50:52.812:DEBUG:certbot.vernieuwing:geen vernieuwingsfouten
```

Na voldoende tijd om de vervaldatum van het certificaat binnen dertig dagen te laten vallen, zal de opdrachtgever het certificaat verlengen en het bijgewerkte certificaat automatisch op de dashboard-toepassing toepassen.

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