Using Let’s Encrypt Certificates with Cisco Business Dashboard and DNS Validation

Objective

This document explains how to obtain a *Let's Encrypt* certificate and install it on Cisco Business Dashboard using the Command Line Interface (CLI). If you want general information on managing certificates, check out the article Manage Certificates on the Cisco Business Dashboard.

Introduction

Let’s Encrypt is a Certificate Authority that provides free, Domain Validation (DV) SSL certificates to the public using an automated process. *Let's Encrypt* provides an easily accessible mechanism for obtaining signed certificates for web servers, giving the end-user confidence that they are accessing the correct service. For more information on *Let's Encrypt*, visit the Let’s Encrypt website.

Using *Let's Encrypt* certificates with Cisco Business Dashboard is reasonably straightforward. Although Cisco Business Dashboard has some special requirements for certificate installation beyond just making the certificate available to the webserver, it is still feasible to automate the issuing and installation of the certificate using the command line tools provided.

To issue and renew certificates automatically, the Dashboard web server must be reachable from the Internet. If this is not the case, a certificate can be easily obtained using a manual process and then installed using the command line tools. The remainder of this document walks through the process of issuing a certificate and installing it in the Dashboard.

If the Dashboard web server is reachable from the Internet on standard ports TCP/80 and TCP/443, it is possible to automate the certificate management and install process. Check out Let’s Encrypt for Cisco Business Dashboard for details.

Step 1

The first step is to obtain software that uses the ACME protocol certificate. In this example, we are using the certbot client, but there are many other options available.

To obtain the certbot client, use the Dashboard or another host running a Unix-like OS (e.g. Linux, macOS) and follow the instructions on certbot client to install the client. In the dropdown menus on this page, select *None of the Above* for Software and your preferred OS for System.

It is important to note that in this article, blue sections are prompts and output from CLI. The `white text` lists commands. Green colored commands, including dashboard.example.com, pnpserver.example.com, and user@example.com should be replaced with DNS names that are appropriate for your environment.

To install the certbot client on the Cisco Business Dashboard server, use the following commands:

```
cbd:~$sudo apt update cbd:~$sudo apt install software-properties-common cbd:~$sudo add-apt-repository ppa:certbot/certbot cbd:~$sudo apt update cbd:~$sudo apt install certbot
```

Step 2

Create a working directory to contain all the files associated with the certificate. Note that these files include sensitive information such as the private key for the certificate and account details for the *Let's Encrypt* service. While the certbot client will create files with appropriately restrictive permissions, you should ensure that the host and the account being used are restricted for access to only authorized staff.

To create the directory on the Dashboard, Enter the following commands:

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

Step 3

Request a certificate using the following command:

```
cbd:~/certbot$certbot certonly --manual --preferred-challenges dns -d dashboard.example.com -d
pnpserver.example.com
--logs-dir . --config-dir . --work-dir . --deploy-hook "cat ~/certbot/live/dashboard.example.com
/fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-
dashboard importcert -t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c
/tmp/cbdchain.pem"
```

This command instructs the *Let's Encrypt* service to validate ownership of the hostnames provided by prompting you to create DNS TXT records for each of the names listed. Once the TXT records have been created, the *Let's Encrypt* service confirms the records exist and then issues the certificate. Finally, the certificate is applied to the dashboard using the cisco-business-dashboard utility.

The parameters on the command are required for the following reasons:

certonly	Request a certificate and download the files. Do not attempt to install them. In the case of Cisco Business Dashboard, the certificate is not only used by the web server, but also by the PnP service and other functions. As a result, the certbot client is not able to install the certificate automatically.
--manual	Do not attempt to automatically authenticate with the *Let's Encrypt* service. Work interactively with the user to authenticate.
--preferred-challenges dns	Authenticate using DNS TXT records.
-d dashboard.example.com	The FQDNs that should be included in the certificate. The first name listed will be included in the Common Name field of the certificate, and all names will be listed in the Subject-Alt-Name field.
-d pnpserver.example.com	The pnpserver.<domain> name is a special name used by the Network Plug and Play feature when performing DNS discovery. Consult the Cisco Business Dashboard Administration Guide for more details.
--logs-dir . --config-dir . --work-dir .	Use the current directory for all the working files created during the process.
--deploy-hook "…"	Use the cisco-business-dashboard command line utility to take the private key and the certificate chain received from the *Let's Encrypt* service and load them into the dashboard application in the same way as if the files were uploaded through the Dashboard User Interface (UI).

The root certificate that anchors the certificate chain is also added to the certificate file here. This is required by certain platforms being deployed using Network Plug and Play.

Automatic installation of the certificate using the --deploy-hook option is only possible when the certbot client is being run on the dashboard server. If the certbot client is being run on a different computer, then the private key and fullchain certificate files should be copied to the dashboard server and installed using the commands:

-cat <fullchain certificate file> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

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

Step 4

Go through the process of creating the certificate by following the instructions generated by the certbot client:

```
cbd:~/certbot$certbot certonly --manual --preferred-challenges dns -d dashboard.example.com -d
pnpserver.example.com
--logs-dir . --config-dir . --work-dir . --deploy-hook "cat ~/certbot/live/dashboard.example.com
/fullchain.pem /etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-
dashboard importcert -t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c
tmp/cbdchain.pem"
Saving debug log to /home/cisco/certbot/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
```

Step 5

Enter the email address or **C** to Cancel.

```
Enter email address (used for urgent renewal and security notices) (Enter 'c' to cancel):
user@example.com
Starting new HTTPS connection (1): acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Step 6

Enter **A** to agree or **C** to cancel.

```
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Enter A to agree or C to cancel.
(A)gree/(C)ancel: A
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Step 7

Enter **Y** for Yes or **N** for No.

```
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
```

```
Enter Y for Yes or N for No.
(Y)es/(N)o: Y
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for dashboard.example.com
dns-01 challenge for pnpserver.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Step 8

Enter **Y** for Yes or **N** for No.

```
NOTE: The IP of this machine will be publicly logged as having requested this
certificate. If you're running certbot in manual mode on a machine that is not
your server, please ensure you're okay with that.
Are you OK with your IP being logged?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Enter Y for Yes or N for No.
(Y)es/(N)o: Y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.dashboard.example.com with the following value:
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

Step 9

A DNS TXT record to validate the ownership of the dashboard.example.com hostname must be created in the DNS infrastructure. The steps required to do this are outside the scope of this document and will depend on the DNS provider being used. Once created, validate that the record is available using a DNS query tool such as Dig.

The DNS challenge process may be automated for certain DNS providers. See DNS Plugins for more details.

Press **Enter** on your keyboard.

```
Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

Step 10

You will receive a similar CLI output. Create and verify additional TXT records for each name to be included in the certificate. Repeat Step 9 for each name specified in the certbot command.

Press **Enter** on your keyboard.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.pnpserver.example.com with the following value:
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
Before continuing, verify the record is deployed.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Press Enter to Continue
```

Step 11

The certificate has been issued and may be found in the *live* subdirectory in the filesystem:

```
Waiting for verification...
Cleaning up challenges
Non-standard path(s), might not work with crontab installed by your operating system package
manager
Running deploy-hook command: cat ~/certbot/live/dashboard.example.com/fullchain.pem
/etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem; /usr/bin/cisco-business-dashboard
importcert -t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem
IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
Your key file has been saved at:
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Your cert will expire on 2020-11-11. To obtain a new or tweaked
version of this certificate in the future, simply run certbot
again. To non-interactively renew *all* of your certificates, run
"certbot renew"
- Your account credentials have been saved in your Certbot
configuration directory at /home/cisco/certbot. You should make a
secure backup of this folder now. This configuration directory will
also contain certificates and private keys obtained by Certbot so
making regular backups of this folder is ideal.
- If you like Certbot, please consider supporting our work by:
Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
Donating to EFF: https://eff.org/donate-le
```

Step 12

Enter the following commands:

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

The directory containing the certificates has restricted permissions so only the cisco user can view the files. The *privkey.pem* file, in particular, is sensitive and access to this file should be restricted to authorized personnel only.

The Dashboard should now be running with the new certificate. If you open the Dashboard User Interface (UI) in a web browser by entering any of the names specified when creating the certificate in the address bar, the web browser should indicate that the connection is trusted and secure.

Please note that certificates issued by *Let's Encrypt* have relatively short lifetimes – currently 90 days. To ensure the certificate remains valid, you will need to repeat the process described above before the 90 days are up.

For more information about the use of the certbot client, consult the certbot documentation page.