Using Let’s Encrypt Certificates with Cisco Business Dashboard

Objective

This document explains how to obtain a *Let's Encrypt* certificate, install it on Cisco Business Dashboard, and set up automatic renewal 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.

The process described in this document has been automated in Cisco Business Dashboard version 2.2.2 and higher. Consult the System > Managing Certificates section of the Administration Guide for more information.

Introduction

Let’s Encrypt is a Certificate Authority that provides free, Domain Validation (DV) Secure Sockets Layer (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, 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. The remainder of this document walks through the process of issuing a certificate and automating the renewal of the certificate.

This document uses HTTP challenges to validate domain ownership. This requires the Dashboard web server to be reachable from the Internet on standard ports TCP/80 and TCP/443. If the web server is not reachable from the Internet, then consider using DNS challenges instead. Check out Using Let’s Encrypt for Cisco Business Dashboard with DNS 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.

Step 2

To allow for certificate renewal to be automated, the certbot client must be installed on the Dashboard. To install the certbot client on the Dashboard server, use the following commands:

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.

```
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 3

Next, the Dashboard web server needs to be set up to be host the challenge files required to verify ownership of the hostname. To do this, we create a directory for these files and update the web server configuration file. Then we restart the Dashboard application for the changes to take effect. Use the following commands:

```
cbd:~$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo chmod 755
/usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
# Location for challenge files created by certbot location /.well-known/acme-challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
EOF
cbd:~$ 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
```

Step 4

Request a certificate using the following command:

```
cbd:~$sudo certbot certonly --webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com --deploy-hook "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 importcert -t pem -k /etc/letsencrypt/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 connecting to the web service hosted on each of the names. This means that the dashboard web service must be accessible from the Internet and be hosted on ports 80 and 443. Access to the dashboard application may be restricted using the Access Control settings on the System > Platform Settings > Web Server page in the dashboard administration User Interface (UI). Consult the Cisco Business Dashboard Administration Guide for more information.

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.
--webroot -w …	Install the challenge files in the directory created above so that they may be accessed through the dashboard web server.
-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

--deploy-hook “…”	Administration Guide for more details. 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.

Step 5

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

```
cbd:~$sudo certbot certonly --webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com --deploy-hook "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 importcert -t pem -k /etc/letsencrypt/live/
dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem"
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator webroot, Installer None
```

Step 6

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
```

Step 7

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

Step 8

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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
```

Step 9

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

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for dashboard.example.com
http-01 challenge for pnpserver.example.com
Using the webroot path /usr/lib/ciscobusiness/dashboard/www/letsencrypt for all unmatched
domains.
Waiting for verification...
Cleaning up challenges
Running deploy-hook command: 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
importcert -t pem -k /etc/letsencrypt/live/dashboard.example.com/privkey.pem -c
/tmp/cbdchain.pem
IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Your cert will expire on 2020-10-29. 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 /etc/letsencrypt. 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
cbd:~$ sudo ls /etc/letsencrypt/live/dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
cbd:~$
```

The directory containing the certificates has restricted permissions so only the root 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.

Step 10

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.

Note that certificates issued by *Let's Encrypt* have relatively short lifetimes – currently 90 days. The certbot package for Ubuntu Linux is configured to check the validity of the certificate twice a day and renew the certificate if it is approaching expiry, so no action should be required to keep the certificate up to date. To verify that the periodic checks are occurring correctly, wait for at least twelve hours after initially creating the certificate, and then check the certbot log file for messages similar to the following: `cbd:~$ sudo tail /var/log/letsencrypt/letsencrypt.log`

```
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot version: 0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main:Arguments: ['-q']
2020-07-31 16:50:52,785:DEBUG:certbot.main:Discovered plugins:
(PluginEntryPoint#manual,
PluginEntryPoint#null,PluginEntryPoint#standalone,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log:Root logging level set at 30
2020-07-31 16:50:52,793:INFO:certbot.log:Saving debug log to
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.selection:
Requested authenticator <certbot.cli.
_Default object at 0x7f1152969240> and installer <certbot.cli.
_Default object at 0x7f1152969240>
2020-07-31 16:50:52,811:INFO:certbot.renewal:Cert not yet due for renewal
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection:Requested authenticator
webroot and installer None
2020-07-31 16:50:52,812:DEBUG:certbot.renewal:no renewal failures
```

After enough time has passed for the certificate expiry date to be within thirty days, the certbot client will renew the certificate and apply the updated certificate to the dashboard application automatically.

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