Mit dem Cisco Business Dashboard sollen Zertifikate verschlüsselt werden.

Ziel

In diesem Dokument wird erläutert, wie Sie ein *Let's Encrypt*-Zertifikat erhalten, es auf dem Cisco Business Dashboard installieren und die automatische Verlängerung über die Befehlszeilenschnittstelle (CLI) einrichten. Wenn Sie allgemeine Informationen zur Verwaltung von Zertifikaten benötigen, lesen Sie den Artikel Zertifikate verwalten im Cisco Business Dashboard.

Der in diesem Dokument beschriebene Prozess wurde in Cisco Business Dashboard Version 2.2.2 und höher automatisiert. Weitere Informationen finden Sie im Abschnitt System > Managing Certificates (System > Zertifikate verwalten) des Administrationsleitfadens.

Einführung

Let's Encrypt ist eine Zertifizierungsstelle, die der Öffentlichkeit kostenlose DV-Secure Sockets Layer (SSL)-Zertifikate mithilfe eines automatisierten Prozesses zur Verfügung stellt. *Let's Encrypt* bietet einen leicht zugänglichen Mechanismus für den Erhalt signierter Zertifikate für Webserver, der dem Endbenutzer das Vertrauen gibt, dass er auf den richtigen Service zugreift. Weitere Informationen finden Sie auf der Website Let's Encrypt.

Die Verwendung von *Let's Encrypt* Zertifikaten mit Cisco Business Dashboard ist relativ einfach. Obwohl das Cisco Business Dashboard einige spezielle Anforderungen für die Zertifikatsinstallation enthält, die über die bloße Bereitstellung des Zertifikats für den Webserver hinausgehen, ist es dennoch möglich, die Ausstellung und Installation des Zertifikats mithilfe der bereitgestellten Befehlszeilentools zu automatisieren. Im verbleibenden Teil dieses Dokuments werden die Ausstellung eines Zertifikats und die Automatisierung der Verlängerung des Zertifikats erläutert.

In diesem Dokument werden HTTP-Herausforderungen verwendet, um die Domäneneigentumsrechte zu überprüfen. Dazu muss der Dashboard-Webserver über die Standard-Ports TCP/80 und TCP/443 vom Internet aus erreichbar sein. Wenn der Webserver nicht über das Internet erreichbar ist, sollten Sie stattdessen DNS-Herausforderungen in Betracht ziehen. Weitere Informationen finden Sie im Benutzerhandbuch "Let's Encrypt for Cisco Business Dashboard with DNS".

Schritt 1

Der erste Schritt besteht darin, Software zu erhalten, die das ACME-Protokollzertifikat verwendet. In diesem Beispiel verwenden wir den Certbot-Client, aber es gibt noch viele andere Optionen.

Schritt 2

Damit die Zertifikatserneuerung automatisiert werden kann, muss der certbot-Client auf dem Dashboard installiert werden. Verwenden Sie die folgenden Befehle, um den certbot-Client auf dem Dashboard-Server zu installieren:

In diesem Artikel ist zu beachten, dass blaue Abschnitte Eingabeaufforderungen und Ausgabe von CLI sind. Im `weißen Text` werden Befehle aufgelistet. Grüne farbige Befehle wie Dashboard.example.com, pnpserver.example.com und user@example.com sollten durch DNS-

Namen ersetzt werden, die für Ihre Umgebung geeignet sind.

```
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
```

Schritt 3

Als Nächstes muss der Dashboard-Webserver so eingerichtet werden, dass er die erforderlichen Challenge-Dateien hostet, um das Eigentum am Hostnamen zu überprüfen. Dazu erstellen wir ein Verzeichnis für diese Dateien und aktualisieren die Konfigurationsdatei des Webservers. Anschließend starten wir die Dashboard-Anwendung neu, damit die Änderungen wirksam werden. Verwenden Sie die folgenden Befehle:

```
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
# Speicherort für Challenge-Dateien erstellt durch certbot location /.well known/acme-question {

root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
EDER
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
```

Schritt 4

Anfordern eines Zertifikats mit dem folgenden Befehl:

```
cbd:~$sudo certbot certonly –webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com –deploy-aken "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
```

Mit diesem Befehl wird der *Let's Encrypt*-Dienst angewiesen, den Besitz der angegebenen Hostnamen zu überprüfen, indem eine Verbindung mit dem auf jedem Namen gehosteten Webdienst hergestellt wird. Das bedeutet, dass der Dashboard-Webdienst vom Internet aus zugänglich sein und auf den Ports 80 und 443 gehostet werden muss. Der Zugriff auf die Dashboard-Anwendung kann über die Zugriffskontrolleinstellungen auf der Seite System > Platform Settings > Web Server (System > Plattformeinstellungen > Webserver) in der Dashboard-Verwaltungs-Benutzeroberfläche (UI) eingeschränkt werden. Weitere Informationen finden Sie im Cisco Business Dashboard Administration Guide.

Die Parameter des Befehls sind aus den folgenden Gründen erforderlich:

zerkleinert	Fordern Sie ein Zertifikat an, und laden Sie die Dateien herunter. Versuchen Sie nicht, sie zu installieren. Im Fall von Cisco Business Dashboard wird das Zertifikat nicht nur vom Webserver, sondern auch vom PnP-Service und anderen Funktionen verwendet. Daher kann der certbot-Client das Zertifikat nicht automatisch installieren.
—webroot -w ...	Installieren Sie die Challenge-Dateien im oben erstellten

	Verzeichnis, damit auf sie über den Dashboard-Webserver zugegriffen werden kann.
-d dashboard.example.com	Die FQDNs, die im Zertifikat enthalten sein sollen. Der aufgelistete Vorname wird in das Feld "Common Name" des Zertifikats aufgenommen, und alle Namen werden im Feld "Subject-Alt-Name" (Betreff-Alt-Name) aufgeführt.
-d pnpserver.example.com	Der pnpserver.<domain>-Name ist ein besonderer Name, der von der Network Plug and Play-Funktion bei der DNS-Erkennung verwendet wird. Weitere Informationen finden Sie im Cisco Business Dashboard Administration Guide.
—deploy-aken ".."	Verwenden Sie das Befehlszeilendienstprogramm cisco-business-Dashboard, um den privaten Schlüssel und die vom *Let's Encrypt*-Dienst empfangene Zertifikatkette zu übernehmen und in die Dashboard-Anwendung zu laden, so als ob die Dateien über die Dashboard User Interface (UI) hochgeladen würden. Das Stammzertifikat, das die Zertifikatkette verankert, wird hier ebenfalls der Zertifikatsdatei hinzugefügt. Dies ist erforderlich, wenn bestimmte Plattformen mithilfe von Network Plug and Play bereitgestellt werden.

Schritt 5

Gehen Sie den Vorgang zum Erstellen des Zertifikats durch, indem Sie die Anweisungen befolgen, die vom certbot-Client generiert wurden:

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —deploy-aken "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
Speichern des Debug-Protokolls unter /var/log/letsencrypt/letsencrypt.log
Ausgewählte Plugins: Authentifizierer webroot, Installer Keine
```

Schritt 6

Geben Sie die E-Mail-Adresse oder **C** auf Abbrechen ein.

```
Geben Sie die E-Mail-Adresse ein (für dringende Verlängerungen und Sicherheitshinweise
verwendet) (geben Sie "c" ein, um
Abbrechen): user@example.com
```

Schritt 7

Geben Sie **A** ein, um der Vereinbarung zuzustimmen, oder **C**, um sie abzubrechen.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Lesen Sie die Nutzungsbedingungen unter
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf Sie müssen
, um sich beim ACME-Server unter
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A
```

Schritt 8

Geben Sie **Y** für Ja oder **N** für Nein ein.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Wären Sie bereit, Ihre E-Mail-Adresse an die elektronische Grenze weiterzugeben?
Foundation, ein Gründungspartner des Let's Encrypt-Projekts und der gemeinnützigen Organisation
Organisation, die Certbot entwickelt? Wir möchten Ihnen gerne eine E-Mail über unsere Arbeit
senden
Verschlüsseln des Internets, EFF-Nachrichten, Kampagnen und Möglichkeiten zur Unterstützung der
digitalen Freiheit.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: J
```

Schritt 9

Das Zertifikat wurde ausgestellt und kann im Unterverzeichnis */etc/letsencrypt/live* im Dateisystem gefunden werden:

```
Erhalt eines neuen Zertifikats
Durchführen der folgenden Herausforderungen:
http-01-Herausforderung für dashboard.example.com
http-01-Herausforderung für pnpserver.example.com
Verwenden des Webroot-Pfads /usr/lib/ciscobusiness/dashboard/www/letsencrypt für alle unerreicht
Domänen.
Zur Überprüfung warten...
Problembehebung
Ausführen des Befehls 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
WICHTIGE HINWEISE:
Herzlichen Glückwunsch! Ihr Zertifikat und Ihre Kette wurden gespeichert unter:
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
Ihre Schlüsseldatei wurde gespeichert unter:
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Ihre Zertifizierung läuft in den Jahren 2020-29 ab. So erhalten Sie eine neue oder angepasste
Version dieses Zertifikats in der Zukunft, führen Sie einfach certbot aus
wieder. Um nicht interaktiv zu verlängern *alle* Ihrer Zertifikate, führen Sie
"Certbot renew"
- Ihre Anmeldeinformationen wurden in Ihrem Certbot gespeichert.
Konfigurationsverzeichnis unter /etc/letsencrypt. Sie sollten
Sichern Sie diesen Ordner jetzt. Dieses Konfigurationsverzeichnis wird
enthält auch Zertifikate und private Schlüssel, die von Certbot erhalten wurden.
regelmäßige Sicherungen dieses Ordners ist ideal.
- Wenn Sie Certbot mögen, erwägen Sie bitte, unsere Arbeit zu unterstützen, indem Sie:
Spenden an ISRG / Let's Encrypt: https://letsencrypt.org/donate
Spende an 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:~$
```

Das Verzeichnis mit den Zertifikaten verfügt über eingeschränkte Berechtigungen, sodass nur der Stammbenutzer die Dateien anzeigen kann. Insbesondere die Datei *privkey.pem* ist sensibel und der Zugriff auf diese Datei sollte nur autorisiertem Personal vorbehalten sein.

Schritt 10

Das Dashboard sollte nun mit dem neuen Zertifikat ausgeführt werden. Wenn Sie die Dashboard-Benutzeroberfläche (UI) in einem Webbrowser öffnen, indem Sie einen der beim Erstellen des Zertifikats angegebenen Namen in die Adressleiste eingeben, sollte der Webbrowser angeben, dass die Verbindung vertrauenswürdig und sicher ist.

Beachten Sie, dass die von *Let's Encrypt* ausgestellten Zertifikate eine relativ kurze Lebensdauer haben - derzeit 90 Tage. Das certbot-Paket für Ubuntu Linux ist so konfiguriert, dass die Gültigkeit des Zertifikats zweimal am Tag überprüft und das Zertifikat erneuert wird, wenn es demnächst abläuft. Daher sollte keine Maßnahme erforderlich sein, um das Zertifikat auf dem neuesten Stand zu halten. Um sicherzustellen, dass die regelmäßigen Überprüfungen ordnungsgemäß durchgeführt werden, warten Sie nach der Erstellung des Zertifikats mindestens zwölf Stunden, und überprüfen Sie dann die certbot-Protokolldatei auf Meldungen, die ähnlich wie folgt sind:

```
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:Argumente: ['-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:Speichern des Debug-Protokolls unter
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.select:
Angeforderter Authentifizierer <certbot.cli.
_Default-Objekt unter 0x7f152969240> und installer <certbot.cli.
_Default object at 0x7f152969240>
2020-07-31 16:50:52,811:INFO:certbot.renewal:Cert noch nicht verlängert
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.select:Angeforderter Authentifizierer
webroot und installer Keine
2020-07-31 16:50:52,812:DEBUG:certbot.renewal:no renewal failure
```

Wenn genügend Zeit für das Ablaufdatum des Zertifikats innerhalb von dreißig Tagen verstrichen ist, verlängert der Certbot-Client das Zertifikat und wendet das aktualisierte Zertifikat automatisch auf die Dashboard-Anwendung an.

Weitere Informationen zur Verwendung des Certbot-Clients finden Sie auf der Seite mit der Dokumentation zum Certbot.