Verschlüsseln Sie Zertifikate mit dem Cisco Business Dashboard und der DNS-Validierung

Ziel

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

Einführung

Let's Encrypt ist eine Zertifizierungsstelle, die mithilfe eines automatisierten Prozesses der Öffentlichkeit kostenlose DV-SSL-Zertifikate bereitstellt. *Let's Encrypt* bietet einen leicht zugänglichen Mechanismus für den Erhalt signierter Zertifikate für Webserver, sodass der Endbenutzer darauf vertrauen kann, dass er auf den richtigen Service zugreift. Weitere Informationen zu *Let's Encrypt* finden Sie auf der Website Let's Encrypt.

Die *Verwendung von* Zertifikaten mithilfe des Cisco Business Dashboards *soll* ganz einfach erfolgen. 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.

Um Zertifikate automatisch auszustellen und zu erneuern, muss der Dashboard-Webserver über das Internet erreichbar sein. Ist dies nicht der Fall, kann ein Zertifikat problemlos mithilfe eines manuellen Prozesses abgerufen und dann mithilfe der Befehlszeilentools installiert werden. Im verbleibenden Teil dieses Dokuments werden die Ausstellung und Installation eines Zertifikats im Dashboard erläutert.

Wenn der Dashboard-Webserver über die Standardports TCP/80 und TCP/443 aus dem Internet erreichbar ist, können die Zertifikatsverwaltung und der Installationsprozess automatisiert werden. Weitere Informationen finden Sie im Leitfaden "Let's Encrypt for Cisco Business Dashboard".

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.

Um den certbot-Client zu erhalten, verwenden Sie das Dashboard oder einen anderen Host, auf dem ein Unix-ähnliches Betriebssystem (z. B. Linux, MacOS) ausgeführt wird, und befolgen Sie die Anweisungen auf dem certbot-Client zur Installation des Clients. Wählen Sie in den Dropdown-Menüs auf dieser Seite *Keine der oben genannten Optionen* für Software und Ihr bevorzugtes Betriebssystem für System aus.

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.

Verwenden Sie die folgenden Befehle, um den certbot-Client auf dem Cisco Business Dashboard-

Server zu installieren:

```
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 2

Erstellen Sie ein Arbeitsverzeichnis, das alle Dateien enthält, die dem Zertifikat zugeordnet sind. Beachten Sie, dass diese Dateien vertrauliche Informationen enthalten, z. B. den privaten Schlüssel für das Zertifikat und Kontodetails für den *Let's Encrypt*-Dienst. Während der certbot-Client Dateien mit entsprechend beschränkenden Berechtigungen erstellt, sollten Sie sicherstellen, dass der Host und das verwendete Konto für den Zugriff auf autorisierte Mitarbeiter beschränkt sind.

Geben Sie die folgenden Befehle ein, um das Verzeichnis im Dashboard zu erstellen:

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

Schritt 3

Anfordern eines Zertifikats mit dem folgenden Befehl:

```
cbd:~/certbot$certbot certonly –Manual –preferred-problems 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
```

Mit diesem Befehl wird der *Let's Encrypt*-Dienst angewiesen, den Besitz der angegebenen Hostnamen zu überprüfen, indem Sie dazu aufgefordert werden, für jeden der aufgeführten Namen DNS-TXT-Datensätze zu erstellen. Nach dem Erstellen der TXT-Datensätze bestätigt der Dienst *"Let's Encrypt"* die vorhandenen Datensätze und gibt das Zertifikat aus. Schließlich wird das Zertifikat mithilfe des Dienstprogramms cisco-business-Dashboard auf das Dashboard angewendet.

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.
—Manuell	Versuchen Sie nicht, sich automatisch mit dem Dienst *Let's Encrypt* zu authentifizieren. Arbeiten Sie zur Authentifizierung interaktiv mit dem Benutzer zusammen.
—Trends mit bevorzugten Herausforderungen	Authentifizierung mithilfe von DNS-TXT-Datensätzen.
-d dashboard.example.com -d pnpserver.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. 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.
—logs-dir: —config-dir . —work-dir .	Verwenden Sie das aktuelle Verzeichnis für alle Arbeitsdateien, die während des Vorgangs erstellt wurden.
—deploy-aken ".."	Verwenden Sie das Befehlszeilendienstprogramm cisco-business-Dashboard, um den privaten Schlüssel und die Zertifikatkette, die vom *Let's Encrypt*-Dienst empfangen wurden, 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.

Die automatische Installation des Zertifikats mithilfe der Option —deploy-aken ist nur möglich, wenn der certbot-Client auf dem Dashboard-Server ausgeführt wird. Wenn der certbot-Client auf einem anderen Computer ausgeführt wird, sollten die Dateien für den privaten Schlüssel und das vollständige Zertifikat auf den Dashboard-Server kopiert und mithilfe der folgenden Befehle installiert werden:

-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

Schritt 4

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

```
cbd:~/certbot$certbot certonly –Manual –preferred-problems 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
Speichern des Debug-Protokolls unter /home/cisco/certbot/letsencrypt.log
Ausgewählte Plugins: Authentifizierungshandbuch, Installer None
```

Schritt 5

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 abzubrechen): user@example.com
Neue HTTPS-Verbindung starten (1): acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Schritt 6

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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Geben Sie A ein, um der Vereinbarung zuzustimmen, oder C, um sie abzubrechen.
(A)gree/(C)ancel: A
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Schritt 7

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.
Geben Sie Y für Ja oder N für Nein ein.
(Y)es/(N)o: J
Erhalt eines neuen Zertifikats
Durchführen der folgenden Herausforderungen:
dns-01-Herausforderung für dashboard.example.com
dns-01-Herausforderung für pnpserver.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Schritt 8

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

```
HINWEIS: Die IP-Adresse dieses Computers wird öffentlich protokolliert, sobald sie dies
angefordert hat.
Zertifikat. Wenn Sie Certbot im manuellen Modus auf einem Computer ausführen, der nicht
Stellen Sie sicher, dass Sie damit einverstanden sind.
Sind Sie damit einverstanden, dass Ihre IP-Adresse protokolliert wird?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Geben Sie Y für Ja oder N für Nein ein.
(Y)es/(N)o: J
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Geben Sie einen DNS-TXT-Datensatz unter dem Namen ein.
_acme-question.dashboard.example.com mit folgendem Wert:
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

Schritt 9

In der DNS-Infrastruktur muss ein DNS-TXT-Datensatz erstellt werden, um den Besitz des Hostnamens "dashboard.example.com" zu überprüfen. Die hierfür erforderlichen Schritte sind nicht im Rahmen dieses Dokuments enthalten und hängen vom verwendeten DNS-Provider ab. Überprüfen Sie nach dem Erstellen mithilfe eines DNS-Abfragetools wie Dig, ob der Datensatz verfügbar ist.

Der DNS-Challenge-Prozess kann für bestimmte DNS-Provider automatisiert werden. Weitere Informationen finden Sie unter DNS-Plugins.

Betätigen Sie die **Eingabetaste** auf Ihrer Tastatur.

```
Bevor Sie fortfahren, überprüfen Sie, ob der Datensatz bereitgestellt wurde.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Drücken Sie die Eingabetaste, um fortzufahren
```

Schritt 10

Sie erhalten eine ähnliche CLI-Ausgabe. Erstellen und überprüfen Sie für jeden im Zertifikat enthaltenen Namen zusätzliche TXT-Datensätze. Wiederholen Sie Schritt 9 für jeden im Befehl certbot angegebenen Namen.

Betätigen Sie die **Eingabetaste** auf Ihrer Tastatur.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Geben Sie einen DNS-TXT-Datensatz unter dem Namen ein.
_acme-Challenge.pnpserver.example.com mit folgendem Wert:
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
Bevor Sie fortfahren, überprüfen Sie, ob der Datensatz bereitgestellt wurde.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Drücken Sie die Eingabetaste, um fortzufahren
```

Schritt 11

Das Zertifikat wurde ausgestellt und kann im *Live*-Unterverzeichnis im Dateisystem gefunden werden:

```
Zur Überprüfung warten...
Problembehebung
Nicht standardmäßige Pfad(e), funktionieren möglicherweise nicht mit Crontab, die von Ihrem
Paketmanager des Betriebssystems installiert wurde.
Ausführen des Befehls 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
WICHTIGE HINWEISE:
Herzlichen Glückwunsch! Ihr Zertifikat und Ihre Kette wurden gespeichert unter:
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
Ihre Schlüsseldatei wurde gespeichert unter:
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Ihre Zertifizierung läuft in den Jahren 2010-2011 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.
Verzeichnis configuration unter /home/cisco/certbot. 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
```

Schritt 12

Geben Sie die folgenden Befehle ein:

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

Das Verzeichnis mit den Zertifikaten verfügt über eingeschränkte Berechtigungen, sodass nur der

Cisco Benutzer die Dateien anzeigen kann. Insbesondere die Datei *privkey.pem* ist sensibel und der Zugriff auf diese Datei sollte nur autorisiertem Personal vorbehalten sein.

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.

Bitte beachten Sie, dass Zertifikate von *Let's Encrypt* eine relativ kurze Lebensdauer haben - derzeit 90 Tage. Um sicherzustellen, dass das Zertifikat gültig bleibt, müssen Sie den oben beschriebenen Vorgang wiederholen, bevor die 90 Tage gültig sind.

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