Utilisation du chiffrement des certificats avec le tableau de bord Cisco Business et la validation DNS

Objectif

Ce document explique comment obtenir un certificat *Cryptons* et l'installer sur Cisco Business Dashboard à l'aide de l'interface de ligne de commande (CLI). Pour obtenir des informations générales sur la gestion des certificats, consultez l'article Gérer les certificats sur le tableau de bord Cisco Business.

Introduction

Let's Encrypt est une autorité de certification qui fournit gratuitement des certificats SSL de validation de domaine (DV) au public à l'aide d'un processus automatisé. *Le chiffrement* fournit un mécanisme facilement accessible pour obtenir des certificats signés pour les serveurs Web, donnant à l'utilisateur final la certitude qu'il accède au service approprié. Pour plus d'informations sur *Let's Encrypt*, visitez le site Web Let's Encrypt.

L'utilisation *de* certificats *Chiffrons* avec Cisco Business Dashboard est relativement simple. Bien que le tableau de bord Cisco Business présente certaines exigences spécifiques pour l'installation des certificats, au-delà de la simple mise à disposition du certificat au serveur Web, il est toujours possible d'automatiser l'émission et l'installation du certificat à l'aide des outils de ligne de commande fournis.

Pour émettre et renouveler automatiquement des certificats, le serveur Web du tableau de bord doit être accessible depuis Internet. Si ce n'est pas le cas, un certificat peut être facilement obtenu à l'aide d'un processus manuel, puis installé à l'aide des outils de ligne de commande. Le reste de ce document passe en revue le processus d'émission d'un certificat et de son installation dans le tableau de bord.

Si le serveur Web du tableau de bord est accessible depuis Internet sur les ports standard TCP/80 et TCP/443, il est possible d'automatiser la gestion des certificats et le processus d'installation. Pour plus d'informations, découvrez Encrypt for Cisco Business Dashboard.

Étape 1

La première étape consiste à obtenir un logiciel qui utilise le certificat de protocole ACME. Dans cet exemple, nous utilisons le client certbot, mais il existe de nombreuses autres options disponibles.

Pour obtenir le client certbot, utilisez le tableau de bord ou un autre hôte exécutant un système d'exploitation de type Unix (par exemple Linux, macOS) et suivez les instructions du client certbot pour installer le client. Dans les menus déroulants de cette page, sélectionnez *Aucun des éléments ci-dessus* pour le logiciel et votre système d'exploitation préféré pour le système.

Il est important de noter que dans cet article, les sections bleues sont des invites et des sorties de CLI. Le `texte blanc` répertorie les commandes. Les commandes de couleur verte, notamment dashboard.example.com, pnpserver.example.com et user@example.com doivent être remplacées par des noms DNS appropriés à votre environnement.

Pour installer le client certbot sur le serveur Cisco Business Dashboard, utilisez les commandes suivantes :

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

Étape 2

Créez un répertoire de travail contenant tous les fichiers associés au certificat. Notez que ces fichiers incluent des informations sensibles telles que la clé privée du certificat et les détails du compte pour le service *Chiffrement*. Bien que le client certbot crée des fichiers avec des autorisations suffisamment restrictives, vous devez vous assurer que l'hôte et le compte utilisés sont restreints pour l'accès uniquement au personnel autorisé.

Pour créer le répertoire dans le tableau de bord, saisissez les commandes suivantes :

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

Étape 3

Demandez un certificat à l'aide de la commande suivante :

```
cbd :~/certbot$certbot certonly —Manual —preference-challenge dns -d dashboard.example.com -d pnpserver.example.com
—log-dir . —config-dir . —rép_travail . —Deployment-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"
```

Cette commande demande au service *Chiffrer* de valider la propriété des noms d'hôte fournis en vous invitant à créer des enregistrements DNS TXT pour chacun des noms répertoriés. Une fois les enregistrements TXT créés, le service *Let's Encrypt* confirme l'existence des enregistrements, puis émet le certificat. Enfin, le certificat est appliqué au tableau de bord à l'aide de l'utilitaire cisco-business-dashboard.

Les paramètres de la commande sont requis pour les raisons suivantes :

certonly	Demandez un certificat et téléchargez les fichiers. N'essayez pas de les installer. Dans le cas de Cisco Business Dashboard, le certificat n'est pas seulement utilisé par le serveur Web, mais également par le service PnP et d'autres fonctions. Par conséquent, le client certbot ne peut pas installer le certificat automatiquement.
—manuel	N'essayez pas de vous authentifier automatiquement avec le service *Chiffrer*. Travailler de manière interactive avec l'utilisateur pour s'authentifier.
—best-challenge dns	Authentifier à l'aide des enregistrements DNS TXT.
-d tableau de bord.exemple.com	Les noms de domaine complet qui doivent être inclus dans le certificat. Le prénom répertorié sera inclus dans le champ Common Name du certificat et tous les noms seront répertoriés dans le champ Subject-Alt-Name.
-d pnpserver.exemple.com	Le nom pnpserver.<domaine> est un nom spécial utilisé par la fonctionnalité Plug-and-Play réseau lors de la détection DNS. Pour plus d'informations, reportez-vous au Guide d'administration du tableau de bord Cisco Business

	Dashboard.
—log-dir . —config-dir . —rép_travail .	Utilisez le répertoire actuel pour tous les fichiers de travail créés au cours du processus.
—“ de combiné de déploiement... ”	Utilisez l'utilitaire de ligne de commande cisco-business-dashboard pour prendre la clé privée et la chaîne de certificats reçus du service *Chiffrer* et les charger dans l'application de tableau de bord de la même manière que si les fichiers étaient téléchargés via l'interface utilisateur du tableau de bord. Le certificat racine qui ancre la chaîne de certificats est également ajouté au fichier de certificat ici. Cela est nécessaire pour certaines plates-formes déployées à l'aide de Network Plug and Play.

L'installation automatique du certificat à l'aide de l'option —Deployment-hook n'est possible que lorsque le client certbot est exécuté sur le serveur de tableau de bord. Si le client certbot est exécuté sur un autre ordinateur, alors la clé privée et les fichiers de certificat en chaîne complète doivent être copiés sur le serveur du tableau de bord et installés à l'aide des commandes suivantes :

-cat <fichier de certificat complet> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-dashboard importcert -t pem -k <fichier de clé privée> -c /tmp/cbdchain.pem

Étape 4

Passez en revue le processus de création du certificat en suivant les instructions générées par le client certbot :

```
cbd :~/certbot$certbot certonly —Manual —preference-challenge dns -d dashboard.example.com -d
pnpserver.example.com
—log-dir . —config-dir . —rép_travail . —Deployment-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"
Enregistrement du journal de débogage sur /home/cisco/certbot/letsencrypt.log
Plugins sélectionnés : Manuel de l'authentificateur, aucune installation
```

Étape 5

Entrez l'adresse e-mail ou **C** pour annuler.

```
Saisissez l'adresse e-mail (utilisée pour les avis de renouvellement et de sécurité urgents)
(saisissez 'c' pour annuler) : user@example.com
Démarrage de la nouvelle connexion HTTPS (1) : acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Étape 6

Entrez **A** pour accepter ou **C** pour annuler.

```
Veuillez lire les conditions d'utilisation à l'adresse
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. Vous devez
convenir pour s'enregistrer auprès du serveur ACME à
https://acme-v02.api.letsencrypt.org/directory
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Entrez A pour accepter ou C pour annuler.
(A)gree/(C)ancel : A
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Étape 7

Entrez **Y** pour Oui ou **N** pour Non.

```
Seriez-vous prêt à partager votre adresse e-mail avec Electronic Frontier ?
Fondation, partenaire fondateur du projet Let's Encrypt et de l'association
organisation qui développe Certbot ? Nous aimerions vous envoyer un e-mail sur notre travail
crypter le web, les informations EFF, les campagnes et les moyens de soutenir la liberté
numérique.
Entrez Y pour Oui ou N pour Non.
(Y)es/(N)o : O
Obtention d'un nouveau certificat
Relever les défis suivants :
défi dns-01 pour dashboard.example.com
défi dns-01 pour pnpserver.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Étape 8

Entrez **Y** pour Oui ou **N** pour Non.

```
NOTE: L'adresse IP de cet ordinateur sera enregistrée publiquement comme ayant demandé cette
certificat. Si vous exécutez certbot en mode manuel sur une machine qui n'est pas
votre serveur, assurez-vous que vous êtes d'accord avec cela.
Êtes-vous d'accord avec la consignation de votre adresse IP ?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Entrez Y pour Oui ou N pour Non.
(Y)es/(N)o : O
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Déployez un enregistrement DNS TXT sous le nom
_acme-challenge.dashboard.example.com avec la valeur suivante :
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

Étape 9

Un enregistrement DNS TXT pour valider la propriété du nom d'hôte dashboard.example.com doit être créé dans l'infrastructure DNS. Les étapes requises pour ce faire ne sont pas couvertes par ce document et dépendront du fournisseur DNS utilisé. Une fois créé, vérifiez que l'enregistrement est disponible à l'aide d'un outil de requête DNS tel que Dig.

Le processus de contestation DNS peut être automatisé pour certains fournisseurs DNS. Voir Plugins DNS pour plus de détails.

Appuyez sur **Entrée** sur votre clavier.

```
Avant de continuer, vérifiez que l'enregistrement est déployé.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Appuyez sur Entrée pour continuer
```

Étape 10

Vous recevrez une sortie CLI similaire. Créer et vérifier des enregistrements TXT supplémentaires pour chaque nom à inclure dans le certificat. Répétez l'étape 9 pour chaque nom spécifié dans la

commande certbot.

Appuyez sur **Entrée** sur votre clavier.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Déployez un enregistrement DNS TXT sous le nom
_acme-challenge.pnpserver.example.com avec la valeur suivante :
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
Avant de continuer, vérifiez que l'enregistrement est déployé.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Appuyez sur Entrée pour continuer
```

Étape 11

Le certificat a été émis et se trouve dans le sous-répertoire *live* du système de fichiers :

```
En attente de vérification...
Relever les défis
Chemin(s) non standard, peut ne pas fonctionner avec crontab installé par votre gestionnaire de
packages du système d'exploitation
Exécution de la commande déploiement-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
REMARQUES IMPORTANTES:
- Félicitations ! Votre certificat et votre chaîne ont été enregistrés sur :
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
Votre fichier de clé a été enregistré sur :
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Votre certificat expirera le 2020-11-11. Pour obtenir un nouveau
version de ce certificat dans le futur, exécutez simplement certbot
encore une fois. Pour renouveler *tous* de vos certificats de manière non interactive, exécutez
«renouvellement certbot »
- Vos informations d'identification de compte ont été enregistrées dans votre Certbot
répertoire de configuration dans /home/cisco/certbot. Tu devrais faire
sauvegarde sécurisée de ce dossier maintenant. Ce répertoire de configuration
contiennent également des certificats et des clés privées obtenus par Certbot.
faire des sauvegardes régulières de ce dossier est idéal.
- Si vous aimez Certbot, pensez à soutenir notre travail en :
Don à ISRG / Chiffrement : https://letsencrypt.org/donate
Don au FEP : https://eff.org/donate-le
```

Étape 12

Entrez les commandes suivantes :

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

Le répertoire contenant les certificats a des autorisations restreintes, de sorte que seul l'utilisateur cisco peut afficher les fichiers. Le fichier *privkey.pem*, en particulier, est sensible et l'accès à ce fichier doit être limité au personnel autorisé uniquement.

Le tableau de bord doit maintenant être exécuté avec le nouveau certificat. Si vous ouvrez

l'interface utilisateur du tableau de bord dans un navigateur Web en entrant l'un des noms spécifiés lors de la création du certificat dans la barre d'adresses, le navigateur Web doit indiquer que la connexion est sécurisée et fiable.

Veuillez noter que les certificats délivrés par *Let's Encrypt* ont une durée de vie relativement courte - actuellement 90 jours. Pour vous assurer que le certificat reste valide, vous devez répéter le processus décrit ci-dessus avant que les 90 jours ne soient écoulés.

Pour plus d'informations sur l'utilisation du client certbot, consultez la page de documentation certbot.