Utilisation de Chiffrons les certificats avec le tableau de bord Cisco Business

Objectif

Ce document explique comment obtenir un certificat *Cryptons*, l'installer sur le tableau de bord Cisco Business et configurer le renouvellement automatique 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.

Le processus décrit dans ce document a été automatisé dans Cisco Business Dashboard version 2.2.2 et ultérieure. Consultez la section Système > Gestion des certificats du Guide d'administration pour plus d'informations.

Introduction

Let's Encrypt est une autorité de certification qui fournit gratuitement des certificats SSL (Secure Sockets Layer) de validation de domaine (DV) au public à l'aide d'un processus automatisé. *Encrypt* 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, visitez le site Web Let's Encrypt.

L'utilisation *des* certificats *Encrypt* 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. Le reste de ce document passe en revue le processus de délivrance d'un certificat et d'automatisation du renouvellement du certificat.

Ce document utilise les défis HTTP pour valider la propriété de domaine. Cela nécessite que le serveur Web du tableau de bord soit accessible depuis Internet sur les ports standard TCP/80 et TCP/443. Si le serveur Web n'est pas accessible depuis Internet, envisagez plutôt d'utiliser les défis DNS. Pour plus d'informations, reportez-vous à la rubrique Encrypt for Cisco Business Dashboard with DNS.

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.

Étape 2

Pour permettre l'automatisation du renouvellement de certificat, le client certbot doit être installé sur le tableau de bord. Pour installer le client certbot sur le serveur de tableau de bord, utilisez les commandes suivantes :

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.

```
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 3

Ensuite, le serveur Web Dashboard doit être configuré pour héberger les fichiers de vérification requis pour vérifier la propriété du nom d'hôte. Pour ce faire, nous créons un répertoire pour ces fichiers et mettons à jour le fichier de configuration du serveur Web. Ensuite, nous redémarrons l'application Tableau de bord pour que les modifications prennent effet. Utilisez les commandes suivantes :

```
cbd :~$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd :~$ sudo chmod 755 /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd :~$sudo bash -c 'cat > /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' « EOF
# Emplacement des fichiers de confirmation créés par l'emplacement certbot /.well-known/acme-challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencryption ;
}
EOF
cbd :~$ 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 :~$ démarrage de cisco-business-dashboard
```

Étape 4

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

```
cbd :~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d dashboard.example.com -d pnpserver.example.com —Deployment-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
```

Cette commande indique au service *Chiffrer* de valider la propriété des noms d'hôte fournis en se connectant au service Web hébergé sur chacun des noms. Cela signifie que le service Web du tableau de bord doit être accessible depuis Internet et hébergé sur les ports 80 et 443. L'accès à l'application de tableau de bord peut être restreint à l'aide des paramètres de contrôle d'accès de la page System > Platform Settings > Web Server de l'interface utilisateur de l'administration du tableau de bord. Pour plus d'informations, reportez-vous au Guide d'administration du tableau de bord 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.
—webroot -w ...	Installez les fichiers de confirmation dans le répertoire créé ci-dessus afin qu'ils puissent être accessibles via le serveur Web du tableau de bord.

-d tableau de bord.exemple.com -d pnpserver.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. 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.
—“ 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.

Étape 5

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

```
cbd :~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —Deployment-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"
Enregistrement du journal de débogage sur /var/log/letsencrypt/letsencrypt.log
Plugins sélectionnés : Webroot de l'authentificateur, aucune installation
```

Étape 6

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
```

Étape 7

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

Étape 8

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'organisation à but non lucratif
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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o : O
```

Étape 9

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

```
Obtention d'un nouveau certificat
Relever les défis suivants :
défi http-01 pour dashboard.example.com
défi http-01 pour pnpserver.example.com
Utilisation du chemin webroot /usr/lib/ciscobusiness/dashboard/www/letsencrypt pour tous les
domaines sans correspondance.
En attente de vérification...
Relever les défis
Exécution de la commande déploiement-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
REMARQUES IMPORTANTES:
- Félicitations ! Votre certificat et votre chaîne ont été enregistrés sur :
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
Votre fichier de clé a été enregistré sur :
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Votre certificat expirera le 20/10/29. 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 /etc/letsencrypt. 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
cbd :~$ sudo ls /etc/letsencrypt/live/dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
cbd :~$
```

Le répertoire contenant les certificats a des autorisations restreintes, de sorte que seul l'utilisateur racine 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.

Étape 10

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.

Notez que les certificats émis par *Let's Encrypt* ont des durées de vie relativement courtes - actuellement 90 jours. Le paquet certbot pour Ubuntu Linux est configuré pour vérifier la validité du certificat deux fois par jour et renouveler le certificat s'il arrive à expiration, donc aucune action ne devrait être requise pour maintenir le certificat à jour. Pour vérifier que les vérifications périodiques se produisent correctement, attendez au moins douze heures après avoir créé le certificat initialement, puis vérifiez dans le fichier journal de certbot les messages similaires aux suivants : `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:Plugins découverts :
(PluginEntryPoint#Manual,
PluginEntryPoint#null,PluginEntryPoint#standalone,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log:Niveau de journalisation racine défini à 30
2020-07-31 16:50:52,793:INFO:certbot.log:enregistrement du journal de débogage dans
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.selection :
Authentificateur demandé <certbot.cli.
_Objet par défaut à 0x7f1152969240> et programme d'installation <certbot.cli.
_Objet par défaut à 0x7f1152969240>
2020-07-31 16:50:52,811:INFO:certbot.renew:Le certificat n'est pas encore en cours de
renouvellement
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection:Authentificateur demandé
webroot et installateur Aucun
2020-07-31 16:50:52,812:DEBUG:certbot.renew:aucun échec de renouvellement
```

Une fois que le délai d'expiration du certificat est suffisant pour être dans les trente jours, le client certbot renouvelle le certificat et applique automatiquement le certificat mis à jour à l'application de tableau de bord.

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