Cisco Business Dashboard로 인증서 암호화 사용

목표

이 문서에서는 *Let's Encrypt* 인증서를 가져와서 Cisco Business Dashboard에 설치하고 CLI(Command Line Interface)를 사용하여 자동 갱신을 설정하는 방법에 대해 설명합니다. 인증서 관리에 대한 일반적인 정보를 확인하려면 Cisco Business Dashboard(Cisco 비즈니스 대시보드)에서 Manage Certificates(인증서 관리)를 참조하십시오.

이 문서에 설명된 프로세스는 Cisco Business Dashboard 버전 2.2.2 이상에서 자동화되었습니다 .자세한 내용은 Administration Guide의 System > Managing Certificates 섹션을 참조하십시오.

소개

*Let's Encrypt*는 자동화된 프로세스를 사용하여 DV(Domain Validation) SSL(Secure Sockets Layer) 인증서를 일반 사용자에게 제공하는 인증 기관입니다.*Let's Encrypt*는 웹 서버용 서명된 인증서를 얻기 위한 쉽게 액세스할 수 있는 메커니즘을 제공하여 최종 사용자가 올바른 서비스에 액세스할 수 있다는 확신을 줍니다.자세한 내용은 Let's Encrypt 웹 사이트를 참조하십시오.

Cisco Business Dashboard로 인증서 *암호화*를 사용하는 것은 상당히 간단합니다.Cisco Business Dashboard는 인증서를 웹 서버에서 사용할 수 있게 하는 것 이상의 인증서 설치에 대한 몇 가지 특별한 요구 사항을 가지고 있지만, 제공된 명령줄 도구를 사용하여 인증서의 발급 및 설치를 자동화하는 것은 여전히 가능합니다.이 문서의 나머지 부분에서는 인증서를 발급하고 인증서 갱신을 자동화하는 과정을 단계별로 안내합니다.

이 문서에서는 HTTP 과제를 사용하여 도메인 소유권을 검증합니다.이렇게 하려면 표준 포트 TCP/80 및 TCP/443의 인터넷에서 대시보드 웹 서버에 연결할 수 있어야 합니다. 인터넷에서 웹 서버에 연결할 수 없는 경우 대신 DNS 문제를 사용하십시오.자세한 내용은 Cisco Business Dashboard with DNS를 사용하여 Let's Encrypt for Cisco Business Dashboard를 참조하십시오.

1단계

첫 번째 단계는 ACME 프로토콜 인증서를 사용하는 소프트웨어를 가져오는 것입니다.이 예에서는 certbot 클라이언트를 사용하지만 사용 가능한 다른 옵션이 많습니다.

2단계

인증서 갱신을 자동화하려면 Dashboard(대시보드)에 certbot 클라이언트를 설치해야 합니다.대시보드 서버에 certbot 클라이언트를 설치하려면 다음 명령을 사용합니다.

이 문서에서 파란색 섹션은 CLI의 프롬프트와 출력입니다. 에 명령이 나열됩니다 .dashboard.example.com, pnpserver.example.com 및 user@example.com를 비롯한 녹색의 명령은 환경에 적합한 DNS 이름으로 교체해야 합니다.

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

3단계

다음으로, 호스트 이름의 소유권을 확인하는 데 필요한 챌린지 파일을 호스팅하도록 대시보드 웹

서버를 설정해야 합니다.이렇게 하려면 이러한 파일에 대한 디렉토리를 만들고 웹 서버 구성 파일을 업데이트합니다.그런 다음 Dashboard 애플리케이션을 다시 시작하여 변경 사항을 적용합니다.다음 명령을 사용합니다.

```
:~$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letencrypt cbd:~$sudo chmod 755
/usr/lib/ciscobusiness/dashboard/www/letterencrypt :~$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
# certbot location /.well-known/acme-challenge     {
/usr/lib/ciscobusiness/dashboard/www/letsencrypt
}
EOF
:~$ :~$sudo chow cbd:cbd /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf :~$
sudo chmod 640 /var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf cbd:~$cisco-
business-dashboard stop cbd:~$cisco-business-dashboard start
```

4단계

다음 명령을 사용하여 인증서를 요청합니다.

```
CBD:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letecrypt/ -d
dashboard.example.com -d pnpserver.example.com —deploy-hook "cat /etc/letsencrypt/live/
dashboard.example.com./etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem;/usr/bin/cisco-
business-dashboard importcert -t pem -k /etc/letencrypt/live/dashboard.example.com /privkey.pem
-c /tmp/cbdchain.pem
```

이 명령은 *Let's Encrypt* 서비스에 각 이름에 호스팅된 웹 서비스에 연결하여 제공된 호스트 이름의 소유권을 검증하도록 지시합니다.즉, 대시보드 웹 서비스에 인터넷에서 액세스할 수 있어야 하며 포트 80 및 443에서 호스팅되어야 합니다. 대시보드 관리 UI(사용자 인터페이스)의 시스템 > 플랫폼 설정 > 웹 서버 페이지에서 액세스 제어 설정을 사용하여 대시보드 응용 프로그램에 대한 액세스를 제한할 수 있습니다. 자세한 내용은 Cisco Business Dashboard Administration Guide를 참조하십시오.

다음과 같은 이유로 명령에 대한 매개변수가 필요합니다.

인증서 전용	인증서를 요청하고 파일을 다운로드합니다.설치를 시도하지 마십시오.Cisco Business Dashboard의 경우 인증서는 웹 서버뿐 아니라 PnP 서비스 및 기타 기능에서도 사용됩니다.따라서 certbot 클라이언트는 인증서를 자동으로 설치할 수 없습니다.
—webroot -w...	대시보드 웹 서버를 통해 액세스할 수 있도록 위에서 생성한 디렉토리에 챌린지 파일을 설치합니다.
-d dashboard.example.com	인증서에 포함해야 하는 FQDN입니다.나열된 이름은 인증서의 Common Name(공통 이름) 필드에 포함되며 모든 이름이 Subject-Alt-Name(주체-대체 이름) 필드에 나열됩니다.
-d pnpserver.example.com	pnpserver.<domain> 이름은 DNS 검색을 수행할 때 네트워크 플러그 앤 플레이 기능에서 사용하는 특수 이름입니다.자세한 내용은 Cisco Business Dashboard Administration Guide를 참조하십시오.
—배포 후크 ".."	cisco-business-dashboard 명령줄 유틸리티를 사용하여 Let's Encrypt 서비스에서 수신한 개인 키 및 인증서 체인을 대시보드 사용자 인터페이스(UI)를 통해 파일이 업로드된 것과 동일한 방식으로 대시보드 애플리케이션에 로드하십시오. 인증서 체인을 고정하는 루트 인증서는 여기에서 인증서 파일에도 추가됩니다.이는 Network Plug and Play를 사용하여 구축하는 특정 플랫폼에 필요합니다.

5단계

certbot 클라이언트에서 생성한 지침에 따라 인증서 생성 프로세스를 진행합니다.

```
CBD:~$sudo certbot certonly –webroot -w /usr/lib/ciscobusiness/dashboard/www/letecrypt/ -d
dashboard.example.com -d pnpserver.example.com –deploy-hook "cat /etc/letsencrypt/live/
dashboard.example.com./etc/ssl/certs/DST_Root_CA_X3.pem > /tmp/cbdchain.pem;/usr/bin/cisco-
business-dashboard importcert -t pem -k /etc/letencrypt/live/dashboard.example.com/privkey.pem -
c /tmp/cbdchain.pem"
  /var/log/letsencrypt/letsencrypt.log
  : webroot,
```

6단계

이메일 주소 또는 **C**를 입력하여 취소합니다.

```
  (     )(  'c' .
):user@example.com
```

7단계

동의하려면 **A**를 입력하고 **C**를 취소하려면 클릭합니다.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -
   .
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf
ACME
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -
(A)/(C):A
```

8단계

예에 **Y**를 입력하고 아니요에 **N**을 입력합니다.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -
  Electronic Frontier ?
Foundation, Let's Encrypt
Certbot  Cisco    .
, EFF , ,
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - -
(Y)es/(N)o:Y
```

9단계

인증서가 발급되었으며 파일 시스템의 */etc/letsencrypt/live* 하위 디렉토리에서 찾을 수 있습니다.

```
  :
dashboard.example.com  http-01
pnpserver.example.com  http-01
     webroot  /usr/lib/ciscobusiness/dashboard/www/letsencrypt .
```

```
  ...

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
  :
- !     .
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
    .
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
 2020-10-29 .
     certbot   .
  .  *all*
"certbot renew"
-    Certbot .
/etc/letencrypt  .
     .


      .
- Certbot    Cisco  .
ISRG  /:https://letsencrypt.org/donate
EFF :https://eff.org/donate-le
:~$ sudo ls /etc/leteencrypt/live/dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
:~$
```

인증서가 포함된 디렉터리에 제한된 권한이 있으므로 루트 사용자만 파일을 볼 수 있습니다 .privkey.*pem* 파일은 특히 민감한 파일이며 이 파일에 대한 액세스는 승인된 담당자로만 제한되어야 합니다.

10단계

이제 대시보드가 새 인증서로 실행되고 있어야 합니다.주소 표시줄에 인증서를 만들 때 지정된 이름을 입력하여 웹 브라우저에서 대시보드 UI(사용자 인터페이스)를 열 경우, 웹 브라우저는 연결이 신뢰할 수 있고 안전함을 나타내야 합니다.

Let's Encrypt에서 발급한 인증서는 수명이 비교적 짧으며 현재 90일입니다.Ubuntu Linux용 certbot 패키지는 인증서의 유효성을 하루에 두 번 확인하고 만료 시기가 다가오는 경우 인증서를 갱신하도록 구성되어 있으므로 인증서를 최신 상태로 유지하기 위해 어떤 조치도 필요하지 않습니다.정기적인 검사가 올바르게 수행되는지 확인하려면 인증서를 처음 생성한 후 최소 12시간 동안 기다린 다음 certbot 로그 파일에서 다음과 유사한 메시지를 확인합니다. `:~$ sudo tail`

```
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot :0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main::['-q']
2020-07-31 16:50:52,785:DEBUG:certbot.main:  :
(PluginEntryPoint#,
PluginEntryPoint#null,PluginEntryPoint#standalone,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log:30
2020-07-31 16:50:52,793:INFO:certbot.log:
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.selection:
  <certbot.cli.
```

```
0x7f1152969240>    <certbot.cli  (_D)
 (0x7f1152969240)(_D)
2020-07-31 16:50:52,811:INFO:certbot.renewal:
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection:
webroot  installer
2020-07-31 16:50:52,812:DEBUG:certbot.renewal:
```

인증서 만료 날짜가 30일 이내인 데 충분한 시간이 지나면 certbot 클라이언트는 인증서를 갱신하고 업데이트된 인증서를 대시보드 애플리케이션에 자동으로 적용합니다.

certbot 클라이언트 사용에 대한 자세한 내용은 certbot 설명서 페이지를 참조하십시오.