Cisco Business Dashboard 및 DNS 검증을 사용하여 인증서 암호화 사용

목표

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

소개

*Let's Encrypt*는 자동화된 프로세스를 사용하여 DV(Domain Validation) SSL 인증서를 공개 대상으로 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 .Let's Encrypt*에* 대한 자세한 내용은 Let's Encrypt 웹 사이트를 참조하십시오.

Cisco Business Dashboard*로* 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.

인증서를 자동으로 발급하고 갱신하려면 인터넷에서 대시보드 웹 서버에 연결할 수 있어야 합니다 .그렇지 않은 경우 수동 프로세스를 사용하여 인증서를 쉽게 가져온 다음 명령줄 도구를 사용하여 설치할 수 있습니다.이 문서의 나머지 부분에서는 인증서를 발급하고 대시보드에 설치하는 과정을 단계별로 안내합니다.

표준 포트 TCP/80 및 TCP/443에서 인터넷에서 대시보드 웹 서버에 연결할 수 있으면 인증서 관리 및 설치 프로세스를 자동화할 수 있습니다.자세한 내용은 Cisco Business Dashboard를 위해 암호화를 참조하십시오.

1단계

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

certbot 클라이언트를 가져오려면 대시보드 또는 Unix와 유사한 OS(예: Linux, macOS)를 실행하는 다른 호스트를 사용하고 certbot 클라이언트의 지침을 따라 클라이언트를 설치합니다.이 페이지의 드롭다운 메뉴에서 None *of the Above* for Software*(소프트웨어*에 대한 위의 *없음)* 및 System(시스템에 대한 기본 설정 OS)을 선택합니다.

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.

Cisco Business Dashboard 서버에 certbot 클라이언트를 설치하려면 다음 명령을 사용합니다.

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

2단계

인증서와 연결된 모든 파일을 포함하는 작업 디렉토리를 만듭니다.이러한 파일에는 인증서의 개인 키 및 Let's Encrypt 서비스에 대한 계정 세부 정보*와* 같은 민감한 정보가 포함됩니다.certbot 클라이언트는 적절한 제한 권한이 있는 파일을 생성하지만, 사용 중인 호스트와 계정이 인증된 직원에게만 액세스할 수 있도록 제한되었는지 확인해야 합니다.

대시보드에서 디렉토리를 생성하려면 다음 명령을 입력합니다.

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

3단계

다음 명령을 사용하여 인증서를 요청합니다.

```
:~/certbot$certbot certonly –manual –preferred-challenges 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"
```

이 명령은 나열된 각 이름*에* 대해 DNS TXT 레코드를 생성하라는 프롬프트를 통해 제공된 호스트 이름의 소유권을 검증하도록 Let's Encrypt 서비스에 지시합니다.TXT 레코드가 생성되면 *Let's Encrypt* 서비스에서 레코드가 있는지 확인한 다음 인증서를 발급합니다.마지막으로, cisco-business-dashboard 유틸리티를 사용하여 대시보드에 인증서가 적용됩니다.

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.
—수동	Let's Encrypt 서비스로 자동 *인증을 시도하지* 마십시오.사용자와 대화식으로 작업하여 인증합니다.
—기본 과제 dns	DNS TXT 레코드를 사용하여 인증합니다.
-d dashboard.example.com -d pnpserver.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. pnpserver.<domain> 이름은 DNS 검색을 수행할 때 네트워크 플러그 앤 플레이 기능에서 사용하는 특수 이름입니다.자세한 내용은 Cisco Business Dashboard Administration Guide를 참조하십시오.
—logs-dir . —config-dir . —work-dir .	프로세스 중에 생성된 모든 작업 파일에 현재 디렉터리를 사용합니다.
—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.

—deploy-hook 옵션을 사용하여 인증서를 자동으로 설치할 수 있는 경우는 certbot 클라이언트가 대시보드 서버에서 실행되는 경우에만 가능합니다.certbot 클라이언트가 다른 컴퓨터에서 실행되는 경우 개인 키 및 전체 체인 인증서 파일을 대시보드 서버에 복사하고 다음 명령을 사용하여 설치해

야 합니다.
-cat <전체 체인 인증서 파일> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-dashboard import cert -t pem -k <개인 키 파일> -c /tmp/cbdchain.pem

4단계

certbot 클라이언트에서 생성한 지침에 따라 인증서 생성 프로세스를 진행합니다.

```
:~/certbot$certbot certonly —manual —preferred-challenges 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"
  /home/cisco/certbot/letsencrypt.log
  : ,
```

5단계

이메일 주소 또는 **C**를 입력하여 취소합니다.

```
  (     )( 'c' .):user@example.com
 HTTPS  (1):acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - -
```

6단계

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

7단계

예에 **Y**를 입력하고 아니요에 **N**을 입력합니다.

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

  :
dashboard.example.com  dns-01
pnpserver.example.com  dns-01
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - -
```

8단계

예에 **Y**를 입력하고 아니요에 **N**을 입력합니다.

```
:  IP      .
.Certbot
,  .
IP  ?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 Y   N .
(Y)es/(N)o:Y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 DNS TXT  .
   _acme-challenge.dashboard.example.com:
3AzDTqNGXb8kSkhqXXYWE2ZrFAVCGT2B8oZNGyBwhc
```

9단계

dashboard.example.com 호스트 이름의 소유권을 검증하기 위한 DNS TXT 레코드를 DNS 인프라에 생성해야 합니다.이 작업을 수행하는 데 필요한 단계는 이 문서의 범위를 벗어나며 사용 중인 DNS 공급자에 따라 달라집니다.생성된 후 Dig와 같은 DNS 쿼리 도구를 사용하여 레코드를 사용할 수 있는지 확인합니다.

특정 DNS 제공자에 대해 DNS 챌린지 프로세스를 자동화할 수 있습니다.자세한 내용은 DNS 플러그인을 참조하십시오.

키보드에서 Enter를 누릅니다.

```
    .
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 Enter .
```

10단계

유사한 CLI 출력을 받게 됩니다.인증서에 포함할 각 이름에 대한 추가 TXT 레코드를 만들고 확인합니다.certbot 명령에 지정된 각 이름에 대해 9단계를 반복합니다.

키보드에서 Enter를 누릅니다.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 DNS TXT  .
   _acme-challenge.pnpserver.example.com:
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
    .
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 Enter .
```

11단계

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

```
  ...

 ,      crontab    .
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
  :
- !     .
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
    .
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
 2020-11-11 .
     certbot   .
  .  *all*
"certbot renew"
-    Certbot .
/home/cisco/certbot  .
     .


      .
- Certbot    Cisco  .
ISRG  /:https://letsencrypt.org/donate
EFF :https://eff.org/donate-le
```

12단계

다음 명령을 입력합니다.

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

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

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 Encrypt(암호화 *허용)에서* 발급한 인증서는 수명이 비교적 짧으며 현재 90일입니다.인증서가 유효한지 확인하려면 90일이 끝나기 전에 위에서 설명한 절차를 반복해야 합니다.

certbot 클라이언트 사용에 대한 자세한 내용은 certbot 설명서 페이지를 참조하십시오.