使用思科业务控制面板和DNS验证加密证书

目标

本文档说明如何获取*加密证书*，并使用命令行界面(CLI)将其安装到Cisco Business Dashboard上。如果要获得有关管理证书的一般信息，请参阅“Manage Certificates on the Cisco Business Dashboard(在思科业务控制面板上管理证书)”一文。

简介

让我们使用加密(Encrypt)是一个证书颁发机构，它使用自动化流程向公众提供免费的域验证(DV)SSL证书。*让我们使用加密*提供一种易于访问的机制来获取Web服务器的签名证书，使最终用户确信他们正在访问正确的服务。有关“我们加*密”的详细信息*，请访问“我们加密”网站。

使用*Cisco Business Dashboard加密证*书是相当简单的。虽然Cisco Business Dashboard对证书安装有一些特殊要求，不仅使证书可用于Web服务器，但使用所提供的命令行工具自动执行证书的颁发和安装仍然可行。

要自动颁发和续订证书，必须可从Internet访问控制面板Web服务器。如果情况并非如此，则可以使用手动过程轻松获取证书，然后使用命令行工具安装。本文档的其余部分将介绍颁发证书并将其安装到控制面板的过程。

如果从Internet可通过标准端口TCP/80和TCP/443访问控制面板Web服务器，则可以自动执行证书管理和安装过程。有关详细信息，请参阅Let ws Encrypt for Cisco Business Dashboard。

第 1 步

第一步是获取使用ACME协议证书的软件。在本示例中，我们使用certbot客户端，但有许多其他选项可用。

要获取certbot客户端，请使用控制面板或运行类似Unix的OS（例如Linux、macOS）的其他主机，并按照certbot客户端上的说明安装客户端。在此页面的下拉菜单中，选择*None of the Above for Software和您*的首选OS for System。

请注意，在本文中，蓝色部分是CLI提示和输出，这一点很重要。白文出命令。包括dashboard.example.com、pnpserver.example.com和user@example.com等绿色命令应替换为适合您环境的DNS名称。

要在Cisco Business Dashboard服务器上安装certbot客户端，请使用以下命令：

```
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
```

步骤 2

创建工作目录以包含与证书关联的所有文件。请注意，这些文件包括敏感信息，例如证书的私钥和加密服务的*帐户详细*信息。当certbot客户端将创建具有适当限制权限的文件时，您应确保主机和正在使用的帐户仅限于授权员工访问。

要在控制面板上创建目录，请输入以下命令：

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

步骤 3

使用以下命令请求证书：

```
cbd:~/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"
```

此命令指示*让加密服务*验证所提供主机名的所有权，方法是提示您为列出的每个名称创建DNS TXT记录。创建TXT记录后，“让我*们加密”服*务确认记录存在，然后颁发证书。最后，使用cisco-business-dashboard实用程序将证书应用到控制面板。

命令上的参数是必需的，原因如下：

ceronly	请求证书并下载文件。请勿尝试安装它们。在Cisco Business Dashboard中，证 因此，certbot客户端无法自动安装证书。
— 手动	请勿尝试使用“我们加密*”服务自动进行身*份验证。以交互方式与用户一起进行身份
— 首选挑战dns	使用DNS TXT记录进行身份验证。
-d dashboard.example.com	应包含在证书中的FQDN。列出的名字将包含在证书的“公用名”字段中，所有名字
-d pnpserver.example.com	pnpserver.<domain>名称是网络即插即用功能在执行DNS发现时使用的特殊名称
—logs-dir 。	
—config-dir 。	使用当前目录获取在流程中创建的所有工作文件。
—work-dir。	
— 部署挂接“……”	使用cisco-business-dashboard命令行实用程序获取从*Let's Encrypt*服务收到的私 同的方式将其加载到控制面板应用中。 锚定证书链的根证书也会添加到此处的证书文件中。使用网络即插即用部署的某些

只有在仪表板服务器上运行certbot客户端时，才可使用 — deploy-hook选项自动安装证书。如果certbot客户端正在其他计算机上运行，则应将私钥和全链证书文件复制到控制面板服务器，并使用以下命令进行安装：

-cat <fullchain certificate file>/etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-dashboard importcert -t pem -k <私钥文件> -c /tmp/cbdchain.pem

步骤 4

按照certbot客户端生成的说明完成创建证书的过程：

```
cbd:~/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
```

步骤 5

输入电子邮件地址或C以取消。

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

步骤 6

输入A同意或C取消。

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

步骤 7

输入Y表示是，N表示否。

```
Foundation“〃
Certbot

YN
(Y)es/(N)o:Y


dns-01 dashboard.example.com
pnpserver.example.comdns-01
– – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – -
```

步骤 8

输入Y表示是，N表示否。

```
NOTE:IP
.certbot

IP
– – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – -
YN
(Y)es/(N)o:Y
– – – – – – – – – – – – – – – – – – – – – – – – – – – – – – – -
DNS TXT
_acme-challenge.dashboard.example.com
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

步骤 9

必须在DNS基础设施中创建DNS TXT记录，以验证dashboard.example.com主机名的所有权。执行此操作所需的步骤不在本文档的讨论范围之内，具体取决于所使用的DNS提供商。创建后，使用DNS查询工具（如“挖掘”）验证记录是否可用。

对于某些DNS提供商，DNS质询过程可能会自动进行。有关详细信息，请参阅DNS插件。

按键盘上的Enter。

```
– – – – – – – – – – – – – – – – – – – – – – – – – – – – – -
Enter
```

步骤 10

您将收到类似的CLI输出。为要包含在证书中的每个名称创建并验证其他TXT记录。对certbot命令中指定的每个名称重复步骤9。

按键盘上的Enter。

```
– – – – – – – – – – – – – – – – – – – – – – – – – – – – – -
DNS TXT
_acme-challenge.pnpserver.example.com
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc

– – – – – – – – – – – – – – – – – – – – – – – – – – – – – -
Enter
```

步骤 11

证书已颁发，可以在文件系统的*live* 子目录中找到：

```
……

crontab
deploy-hookcat ~/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

- Congratulations!
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem

/home/cisco/certbot/live/dashboard.example.com/privkey.pem
2020-11-11
certbot
**
"certbot renew"
– Certbot


Certbot

– Certbot
ISRG/https://letsencrypt.org/donate
EFFhttps://eff.org/donate-le
```

步骤 12

输入以下命令：

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

包含证书的目录具有受限权限，因此只有思科用户可以查看文件。特别是*privkey.pem*文件是敏感文件，对此文件的访问应仅限授权人员访问。

控制面板现在应使用新证书运行。如果在地址栏中输入创建证书时指定的任何名称，在Web浏览器中打开控制面板用户界面(UI)，则Web浏览器应指示连接受信任且安全。

请注意，“让我们加密”*颁发的证书*的生存期相对较短 — 当前为90天。为确保证书保持有效，您需要在90天运行之前重复上述过程。

有关使用certbot客户端的详细信息，请参阅certbot文档页。