使用思科业务控制面板加密证书

目标

本文档说明如何获*取加密证*书，将其安装在Cisco Business Dashboard上，以及使用命令行界面(CLI)设置自动续订。 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。

本文档中描述的流程已在Cisco Business Dashboard 2.2.2版及更高版本中自动执行。有关详细信息，请参阅《管理指南》的“系统”>“管理证书”部分。

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)安全套接字层(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。有关详细信息，请访问“让我们加密”网站。

使用*Cisco Business Dashboard加密证*书非常简单。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。本文档的其余部分将介绍颁发证书和自动续订证书的过程。

本文档使用HTTP质询来验证域所有权。这要求从标准端口TCP/80和TCP/443上的Internet可以访问Dashboard Web服务器。如果Web服务器无法从Internet访问，请考虑改用DNS质询。有关详细信息，请参阅使用DNS加密思科业务控制面板。

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。

步骤 2

要允许证书续订自动化，必须在控制面板上安装certbot客户端。要在控制面板服务器上安装certbot客户端，请使用以下命令：

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。

```
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 3

接下来，需要将控制面板Web服务器设置为托管验证主机名所有权所需的质询文件。为此，我们为这些文件创建目录并更新Web服务器配置文件。然后，我们重新启动仪表板应用程序，使更改生效。使用以下命令：

```
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
```

```
#certbot/.well known/acme-challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
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:~$cisco-business-dashboard stop cbd:~$cisco-business-dashboard start
```

步骤 4

使用以下命令请求证书：

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —deploy-hook "cat /etc/letsencrypt/live/
dashboard.example.com/fullchain.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
```

此命令指示*让加密服务*验证通过连接到每个名称上托管的Web服务而提供的主机名的所有权。这意味着仪表板Web服务必须可以从Internet访问，并托管在端口80和443上。使用仪表板管理用户界面(UI)中“系统”>“平台设置”>“Web服务器”页上的“访问控制”设置可以限制对仪表板应用程序的访问。有关详细信息，请参阅《思科业务控制面板管理指南》。

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。
—webroot -w...	将质询文件安装在上面创建的目录中，以便通过控制面板Web服务器访问。
-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
— 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

步骤 5

按照certbot客户端生成的说明完成创建证书的过程：

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/dashboard/www/letsencrypt/ -d
dashboard.example.com -d pnpserver.example.com —deploy-hook "cat /etc/letsencrypt/live/
dashboard.example.com/fullchain.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"
/var/log/letsencrypt/letsencrypt.log
webroot
```

步骤 6

输入电子邮件地址或**C以**取消。

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

步骤 7

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

步骤 8

输入Y表示是，N表示否。

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Foundation“”
Certbot

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o:Y
```

步骤 9

证书已颁发，可在文件系统中的*/etc/letsencrypt/live*子目录中找到：

```
dashboard.example.comhttp-01
pnpserver.example.comhttp-01
webroot/usr/lib/ciscobusiness/dashboard/www/letsencrypt
……

deploy-hookcat /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

- Congratulations!
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem

/etc/letsencrypt/live/dashboard.example.com/privkey.pem
2020-10-29
certbot
**
"certbot renew"
— Certbot
/etc/letsencrypt

Certbot

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

```
cbd:~$ sudo ls /etc/letsencrypt/live/dashboard.example.com
/cert.pem chain.pem fullchain.pem privkey.pem README
cbd:~$
```

包含证书的目录具有受限权限，因此只有根用户才能查看文件。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。

步骤 10

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，“让加密”*颁发的证书的*生存期相对较短 — 当前为90天。Ubuntu Linux的certbot软件包配置为每天两次检查证书的有效性，如果证书即将到期，则续订证书，因此无需执行任何操作使证书保持最新。要验证定期检查是否正确进行，请在最初创建证书后至少等待12小时，然后检查certbot日志文件中是否有类似以下消息： `cbd:~$ sudo tail /var/log/letsencrypt/letsencrypt.log`

```
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main['-q']
2020-07-31 16:50:52,785:DEBUG:certbot.main
(PluginEntryPoint#manual
PluginEntryPoint#nullPluginEntryPoint#standalonePluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log30
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>)(_D)<certbot.cli
(0x7f1152969240>)(_D)
2020-07-31 16:50:52,811:INFO:certbot.renewal
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection
webrootinstaller none
2020-07-31 16:50:52,812:DEBUG:certbot.renewal
```

证书到期日期在30天内经过足够时间后，certbot客户端将更新证书并自动将更新后的证书应用到控制面板应用程序。

有关使用certbot客户端的详细信息，请参阅certbot文档页。