在Cisco Business Dashboard上使用Let's Encrypt Certificates

目標

本檔案將說明如何取得*Let's Encrypt*憑證、將其安裝在Cisco Business Dashboard上，以及使用指令行介面(CLI)設定自動續訂。 如果您想瞭解有關管理證書的一般資訊，請檢視Cisco Business Dashboard上的文章Manage Certificates。

本文檔中描述的流程已在Cisco Business Dashboard 2.2.2版及更高版本中自動執行。有關詳細資訊，請參閱《管理指南》的 System > Managing Certificates部分。

簡介

*Let's Encrypt是一個證書頒發機*構，它使用自動過程向公眾提供免費的域驗證(DV)安全套接字層(SSL)證書。*Let's Encrypt提供*一種易於訪問的機制來獲取Web伺服器的簽名證書，使終端使用者確信他們訪問的是正確的服務。如需詳細資訊，請參閱讓我們加密網站。

在Cisco Business Dashboard上使用*Let's Encrypt* certificates相當簡單。儘管Cisco Business Dashboard對證書安裝有一些特殊要求，除了僅向Web伺服器提供證書外，使用提供的命令列工具自動頒發和安裝證書仍是可行的。本文檔的其餘部分將介紹頒發證書和自動續訂證書的過程。

本文檔使用HTTP挑戰來驗證域所有權。這要求儀表板的Web伺服器可以通過標準埠TCP/80和TCP/443從Internet訪問。如果無法從Internet訪問Web伺服器，請考慮改用DNS挑戰。如需詳細資訊，請檢視使用Let's Encrypt for Cisco Business Dashboard with DNS。

步驟1

第一步是獲取使用ACME協定證書的軟體。在本例中，我們使用certbot client，但還有許多其他選項可用。

步驟2

要自動續訂證書，必須在控制面板上安裝certbot客戶端。要在儀表板伺服器上安裝certbot客戶端，請使用以下命令：

必須注意的是，本文中藍色部分是來自CLI的提示和輸出。命令。綠色命令(包括dashboard.example.com、pnpserver.example.com和user@example.com)應替換為適合您的環境的DNS名稱。

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

步驟3

接下來，需要將Dashboard Web伺服器設定為託管驗證主機名所有權所需的質詢檔案。為此，我們將為這些檔案建立一個目錄並更新Web伺服器配置檔案。然後我們重新啟動儀表板應用程式，以使更改生效。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:~$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
#certbot location/.known/acme-challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
EOF
cbd:~$ 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
```

步驟4

使用以下命令請求證書：

```
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 /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
```

此命令指示*Let's Encrypt*服務驗證通過連線到每個名稱上承載的Web服務提供的主機名的所有權。這意味著儀表板Web服務必須可以從Internet訪問，並且託管在埠80和443上。可以使用儀表板管理使用者介面(UI)中「系統」>「平台設定」>「Web伺服器」頁上的「訪問控制」設定來限制對儀表板應用程式的訪問。 有關詳細資訊，請參閱《Cisco Business Dashboard管理指南》。

需要命令上的引數的原因如下：

certonly	請求證書並下載檔案。請勿嘗試安裝。對於Cisco Business Dashboard，證書不 此，certbot客戶端無法自動安裝證書。
—webroot -w ...	將質詢檔案安裝在上面建立的目錄中，以便通過儀表板Web伺服器訪問它們。
-d dashboard.example.com	應包括在證書中的FQDN。列出的第一個名稱將包含在證書的「公用名」欄位中
-d pnpserver.example.com	pnpserver.<domain>名稱是執行DNS發現時網路即插即用功能使用的特殊名稱。
—deploy-hook "。."	使用cisco-business-dashboard命令列實用程式提取從*Let's Encrypt服務接收的私* *相同的方式將其載入到儀表板應用程式。* 將錨定憑證鏈結的根憑證也新增到此處的憑證檔案中。使用網路即插即用部署的

步驟5

請按照certbot客戶端生成的說明完成建立證書的過程：

```
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 /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"
/var/log/letsencrypt/letsencrypt.log
Webroot
```

步驟6

輸入要取消的電子郵件地址或C。

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

第7步

輸入**A**同意，或輸入**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
```

步驟8

輸入**Y**表示「是」，輸入**N**表示「否」。

```
– – – – – – – – – – – – – – – – – – –
Electronic Frontier
FoundationLet's Encrypt
Certbot
EFF
– – – – – – – – – – – – – – – – – – –
(Y)es/(N)o:Y
```

步驟9

證書已頒發，並且可以在檔案系統中*/etc/letsencrypt/live*子目錄中找到：

```
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

–
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem

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


Certbot

– Certbot
```

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

包含證書的目錄具有受限許可權，因此只有根使用者才能檢視檔案。尤其是*privkey.pem*檔案是敏感的，對此檔案的訪問應僅限於授權人員。

步驟10

儀表板現在應使用新證書運行。如果您通過在Web瀏覽器中輸入在位址列中建立證書時指定的任何名稱來開啟儀表板使用者介面(UI)，則Web瀏覽器應指示連線是受信任和安全的。

請注意，*Let's Encrypt簽發的憑*證有效期相對較短 — 目前為90天。適用於Ubuntu Linux的certbot套件設定為每天檢查兩次憑證的有效性，並在接近到期時續訂憑證，因此無需採取任何行動將憑證保持最新。要驗證定期檢查是否正確執行，請在最初建立證書後等待至少12小時，然後檢查certbot日誌檔案是否有類似以下消息： `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><certbot.cli(_D)
0x7f(_D1152969240>
2020-07-31 16:50:52,811:INFO:certbot.renewal
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection
webroot
2020-07-31 16:50:52,812:DEBUG:certbot.renewal:no renewal failures
```

在證書到期日期經過三十天內的足夠時間後，certbot客戶端將自動更新證書並將更新的證書應用到儀表板應用程式。

有關使用certbot使用者端的詳細資訊，請參閱certbot檔案頁面。