# 使用Let's Encrypt Certificates with Cisco Business Dashboard and DNS Validation

## 目標

本檔案將說明如何取得*Let's Encrypt*憑證，並使用指令行介面(CLI)將其安裝在Cisco Business Dashboard上。 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。

### 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域驗證(DV)SSL證書。*Let's Encrypt提供*一種易於訪問的機制，用於獲取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。有關*Let's Encrypt*的更多資訊，請訪問Let's Encrypt網站。

在Cisco *Business Dashboard上使用*Let*讓我們加*密證書非常簡單。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。

要自動頒發和續訂證書，必須能夠從Internet訪問儀表板Web伺服器。如果情況並非如此，則可以使用手動過程輕鬆獲取證書，然後使用命令列工具進行安裝。本文檔的其餘部分將介紹頒發證書並將其安裝在控制面板中的過程。

如果通過標準埠TCP/80和TCP/443從網際網路訪問控制面板Web伺服器，則可以自動執行證書管理和安裝過程。請檢視讓我們加密思科業務控制面板以瞭解詳細資訊。

#### 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。

要獲取certbot客戶端，請使用儀表板或運行類Unix作業系統（如Linux、macOS）的其他主機，並按照certbot客戶端上的說明安裝客戶端。在此頁面上的下拉選單中，選擇*以上任一軟體選項*和您的系統首選作業系統。

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。

要在Cisco Business Dashboard伺服器上安裝certbot客戶端，請使用以下命令：

```
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2

建立一個工作目錄以包含與證書關聯的所有檔案。請注意，這些檔案包括敏感資訊，例如憑證的私密金鑰和*Let's Encrypt服務的帳戶詳細*資訊。雖然certbot客戶端將建立具有適當限制許可權的檔案，但您應確保主機和正在使用的帳戶被限製為只能訪問經過授權的員工。

要在儀表板上建立目錄，請輸入以下命令：

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

**步驟3**

使用以下命令請求證書：

```
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*Let's Encrypt*服務驗證通過提示您為列出的每個名稱建立DNS TXT記錄而提供的主機名的所有權。建立TXT記錄後，*Let's Encrypt*服務會確認記錄存在，然後發出證書。最後，使用cisco-business-dashboard實用程式將證書應用到控制面板。

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<br>此，certbot客戶端無法自動安裝證書。 |
| — 手動 | 請勿嘗試使用*Let's Encrypt服務自動進行身份*驗證。以互動方式與使用者進行身 |
| —preferred-challenges dns | 使用DNS TXT記錄進行身份驗證。 |
| -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。 |
| —logs-dir。<br>—config-dir。<br>—work-dir。 | 將當前目錄用於進程期間建立的所有工作檔案。 |
| —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<br>相同的方式將其載入到儀表板應用程式。*<br><br>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 |

僅當儀表板伺服器上運行certbot客戶端時，才能使用 — deploy-hook選項自動安裝證書。如果certbot客戶端正在另一台電腦上運行，則應將私鑰和全鏈證書檔案複製到儀表板伺服器並使用以下命令進行安裝：

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

cisco-business-dashboard importcert -t pem -k <私鑰檔案> -c /tmp/cbdchain.pem

**步驟4**

請按照certbot客戶端生成的說明完成建立證書的過程：

```
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
```

### 步驟5

輸入要取消的電子郵件地址或C。

```
cuser@example.com
HTTPS(1):acme-v02.api.letsencrypt.org
– – – – – – – – – – – – – – – – – – –
```

### 步驟6

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
– – – – – – – – – – – – – – – – – – –
AC
(A)gree/(C)ancel:A
– – – – – – – – – – – – – – – – – – –
```

### 第7步

輸入Y表示「是」，輸入N表示「否」。

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


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

### 步驟8

輸入Y表示「是」，輸入N表示「否」。

```
IP
certbot


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

### 步驟9

必須在DNS基礎設施中建立用於驗證dashboard.example.com主機名所有權的DNS TXT記錄。執行此操作所需的步驟超出本文檔的範圍，具體取決於使用的DNS提供程式。建立後，使用Dig等DNS查詢工具驗證記錄是否可用。

對於某些DNS提供者，可以自動執行DNS詢問過程。如需詳細資訊，請參閱DNS外掛。

按鍵盤上的**Enter**鍵。

```
– – – – – – – – – – – – – – – – – – – –
Enter
```

### 步驟10

您將收到類似的CLI輸出。為要包括在證書中的每個名稱建立和驗證其他TXT記錄。對certbot命令中指定的每個名稱重複步驟9。

按鍵盤上的**Enter**鍵。

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

– – – – – – – – – – – – – – – – – – – –
Enter
```

### 步驟11

證書已經頒發，可以在檔案系統的*live*子目錄中找到：

```
……

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

–
/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


Certbot

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

### 步驟12

輸入以下命令：

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

包含證書的目錄具有受限許可權，因此只有思科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。

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，由*Let's Encrypt簽發的憑*證有效期相對較短 — 目前為90天。為了確保證書保持有效，您需要在90天運行之前重複上述過程。

有關使用certbot使用者端的詳細資訊，請參閱certbot檔案頁面。