Utilizzo di Let's Encrypt Certificates con Cisco Business Dashboard e la convalida DNS

Obiettivo

In questo documento viene illustrato come ottenere un certificato *Let's Encrypt* e installarlo in Cisco Business Dashboard utilizzando l'interfaccia della riga di comando (CLI). Per informazioni generali sulla gestione dei certificati, vedere l'articolo Gestione dei certificati in Cisco Business Dashboard.

Introduzione

Let's Encrypt è un'autorità di certificazione che fornisce gratuitamente certificati SSL di convalida del dominio (DV) al pubblico utilizzando un processo automatizzato. *Let's Encrypt* fornisce un meccanismo facilmente accessibile per ottenere certificati firmati per i server Web, dando all'utente finale la certezza di accedere al servizio corretto. Per ulteriori informazioni su *Let's Encrypt*, visitare il sito Web di Let's Encrypt.

L'utilizzo dei certificati *Crittografia* con Cisco Business Dashboard è abbastanza semplice. Sebbene Cisco Business Dashboard preveda alcuni requisiti speciali per l'installazione dei certificati, oltre a rendere il certificato disponibile per il server Web, è comunque possibile automatizzare il rilascio e l'installazione del certificato utilizzando gli strumenti della riga di comando forniti.

Per rilasciare e rinnovare automaticamente i certificati, è necessario che il server Web del dashboard sia raggiungibile da Internet. In caso contrario, è possibile ottenere facilmente un certificato utilizzando un processo manuale e installarlo utilizzando gli strumenti della riga di comando. La parte restante di questo documento descrive il processo di rilascio di un certificato e di installazione nel dashboard.

Se il server Web del dashboard è raggiungibile da Internet tramite le porte standard TCP/80 e TCP/443, è possibile automatizzare la gestione dei certificati e il processo di installazione. Per ulteriori informazioni, vedere Crittografia per Cisco Business Dashboard.

Passaggio 1

Il primo passaggio consiste nell'ottenere un software che utilizzi il certificato del protocollo ACME. In questo esempio viene utilizzato il client certbot, ma sono disponibili molte altre opzioni.

Per ottenere il client certbot, utilizzare il dashboard o un altro host che esegue un sistema operativo simile a Unix (ad esempio Linux, macOS) e seguire le istruzioni sul client certbot per installare il client. Nei menu a discesa di questa pagina, selezionare *Nessuna delle opzioni precedenti* per Software e SO preferito per Sistema.

Èimportante notare che in questo articolo, le sezioni blu sono prompt e output dalla CLI. Il `testo bianco` elenca i comandi. I comandi di colore verde, inclusi dashboard.example.com, pnpserver.example.com e user@example.com, devono essere sostituiti con nomi DNS appropriati per l'ambiente in uso.

Per installare il client certbot sul server Cisco Business Dashboard, utilizzare i comandi seguenti:

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

Passaggio 2

Creare una directory di lavoro contenente tutti i file associati al certificato. Si noti che questi file includono informazioni riservate, ad esempio la chiave privata per il certificato e i dettagli dell'account per il servizio *Let's Encrypt*. Mentre il client certbot creerà file con autorizzazioni adeguatamente restrittive, è necessario assicurarsi che l'host e l'account utilizzato siano limitati per l'accesso solo al personale autorizzato.

Per creare la directory sul quadro comandi, immettere i seguenti comandi:

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

Passaggio 3

Richiedere un certificato utilizzando il comando seguente:

```
cbd:~/certbot$certbot certonly –manual –preferred-CHALLENGes dns -d dashboard.example.com -d pnpserver.example.com
–dir-log . dir-config. –dir-lavoro . –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 import -t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem"
```

Questo comando indica al servizio *Crittografia* di convalidare la proprietà dei nomi host forniti richiedendo di creare record TXT DNS per ognuno dei nomi elencati. Una volta creati i record TXT, il servizio *Let's Encrypt* conferma che i record esistono e quindi emette il certificato. Infine, il certificato viene applicato al dashboard utilizzando l'utilità cisco-business-dashboard.

I parametri del comando sono necessari per i motivi seguenti:

certonly	Richiedere un certificato e scaricare i file. Non tentare di installarli. Nel caso di Cisco Business Dashboard, il certificato viene utilizzato non solo dal server Web, ma anche dal servizio PnP e da altre funzioni. Di conseguenza, il client certbot non è in grado di installare il certificato automaticamente.
- manuale	Non tentare di eseguire automaticamente l'autenticazione con il servizio *Crittografia*. Utilizzo interattivo dell'utente per l'autenticazione.
dns con problematiche preferite	Eseguire l'autenticazione utilizzando i record TXT DNS.
-d dashboard.example.com -d pnpserver.example.com	FQDN da includere nel certificato. Il nome indicato verrà incluso nel campo Nome comune del certificato e tutti i nomi verranno elencati nel campo Nome-Alt-Soggetto. Il nome pnpserver.<dominio> è un nome speciale utilizzato dalla funzionalità Plug and Play di rete quando si esegue l'individuazione DNS. Per ulteriori informazioni, consultare la Cisco Business Dashboard Administration Guide.
—dir-log . dir-config. —dir-lavoro .	Utilizzate la directory corrente per tutti i file di lavoro creati durante il processo.
—deploy-hook "..."	Utilizzare l'utilità da riga di comando cisco-business-

dashboard per acquisire la chiave privata e la catena di certificati ricevuti dal servizio *Let's Encrypt* e caricarli nell'applicazione dashboard come se i file fossero stati caricati tramite l'interfaccia utente del dashboard.

Anche il certificato radice che ancora la catena di certificati viene aggiunto al file del certificato. Questa operazione è richiesta da alcune piattaforme distribuite mediante Network Plug and Play.

L'installazione automatica del certificato tramite l'opzione —deploy-hook è possibile solo quando il client certbot viene eseguito sul server del dashboard. Se il client certbot viene eseguito su un computer diverso, i file della chiave privata e del certificato fullchain devono essere copiati nel server dashboard e installati utilizzando i comandi seguenti:

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

cisco-business-dashboard import -t pem -k <file chiave privata> -c /tmp/cbdchain.pem

Passaggio 4

Eseguire il processo di creazione del certificato seguendo le istruzioni generate dal client certbot:

```
cbd:~/certbot$certbot certonly —manual —preferred-CHALLENGes dns -d dashboard.example.com -d
pnpserver.example.com
—dir-log . dir-config. —dir-lavoro . —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 import -t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c tmp/cbdchain.pem"
Salvataggio del log di debug in /home/cisco/certbot/letsencrypt.log
Plugin selezionati: Manuale dell'autenticatore, Installatore Nessuno
```

Passaggio 5

Immettere l'indirizzo e-mail o **C** per annullare.

```
Immetti l'indirizzo e-mail (utilizzato per gli avvisi urgenti di rinnovo e di sicurezza)
(immetti 'c' per annullare): user@example.com
Avvio nuova connessione HTTPS (1): acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Passaggio 6

Immettere **A** per accettare o **C** per annullare.

```
Leggere le condizioni per l'utilizzo del servizio all'indirizzo
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. Devi
acconsentire a effettuare la registrazione presso il server ACME all'indirizzo
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Immettere A per accettare o C per annullare.
A)acconsente/C)annulla: A
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Passaggio 7

Immettere **Y** per Sì o **N** per No.

```
Sareste disposti a condividere il vostro indirizzo email con la Frontiera Elettronica?
```

```
Foundation, un partner fondatore del progetto Let's Encrypt e dell'organizzazione no profit
organizzazione che sviluppa Certbot? Vorremmo inviarti un'e-mail sul nostro lavoro
Crittografia del Web, notizie EFF, campagne e metodi per supportare la libertà digitale.
Immettere Y per Sì o N per No.
(Y)es/(N)o: Y
Come ottenere un nuovo certificato
Sfide:
dns-01 challenge per dashboard.example.com
dns-01 challenge per pnpserver.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Passaggio 8

Immettere **Y** per Sì o **N** per No.

```
NOTA: L'indirizzo IP di questo computer verrà registrato pubblicamente come utente che ha
richiesto questo
certificato. Se certbot è in esecuzione in modalità manuale su un computer che non è
il server, assicurarsi che non vi siano problemi.
La registrazione dell'indirizzo IP è corretta?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Immettere Y per Sì o N per No.
(Y)es/(N)o: Y
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Distribuire un record DNS TXT con il nome
_acme-challenge.dashboard.example.com con il valore seguente:
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc
```

Passaggio 9

Ènecessario creare un record DNS TXT per convalidare la proprietà del nome host dashboard.example.com nell'infrastruttura DNS. I passaggi necessari a tale scopo non rientrano nell'ambito di questo documento e dipendono dal provider DNS utilizzato. Una volta creato, verificare che il record sia disponibile utilizzando uno strumento di query DNS come Dig.

Il processo di verifica DNS può essere automatizzato per alcuni provider DNS. Per ulteriori informazioni, vedere Plugin DNS.

Premere **Invio** sulla tastiera.

```
Prima di continuare, verificare che il record sia distribuito.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Premere Invio per continuare
```

Passaggio 10

si riceverà un output CLI simile. Creare e verificare ulteriori record TXT per ogni nome da includere nel certificato. Ripetere il passaggio 9 per ogni nome specificato nel comando certbot.

Premere **Invio** sulla tastiera.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Distribuire un record DNS TXT con il nome
_acme-challenge.pnpserver.example.com con il valore seguente:
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
Prima di continuare, verificare che il record sia distribuito.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Premere Invio per continuare
```

Passaggio 11

Il certificato è stato emesso e si trova nella sottodirectory *live* nel file system:

```
In attesa di verifica...
Problemi di pulizia
I percorsi non standard potrebbero non funzionare con crontab installato da Gestione pacchetti
del sistema operativo
Esecuzione del comando 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 import
-t pem -k ~/certbot/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem
NOTE IMPORTANTI:
Congratulazioni! Il certificato e la catena sono stati salvati in:
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
Il file di chiave è stato salvato in:
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Il certificato scadrà il 2020-11-11. Per ottenere un certificato
versione del certificato in futuro, eseguire certbot
di nuovo. Per rinnovare *tutti* i certificati in modo non interattivo, eseguire
"certbot renew"
- Le credenziali dell'account sono state salvate nel Certbot
directory di configurazione in /home/cisco/certbot. Dovresti fare una
backup protetto della cartella. Questa directory di configurazione
contiene anche certificati e chiavi private ottenuti da Certbot so
èconsigliabile eseguire backup regolari di questa cartella.
- Se ti piace Certbot, ti preghiamo di sostenere il nostro lavoro:
Donazione a ISRG / Let's Encrypt: https://letsencrypt.org/donate
Donazione al FEP: https://eff.org/donate-le
```

Passaggio 12

Immettere i seguenti comandi:

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

La directory contenente i certificati dispone di autorizzazioni limitate, pertanto solo l'utente cisco può visualizzare i file. Il file *privkey.pem*, in particolare, è sensibile e l'accesso a questo file deve essere limitato al solo personale autorizzato.

Il dashboard dovrebbe essere in esecuzione con il nuovo certificato. Se si apre l'interfaccia utente del dashboard in un browser Web immettendo uno dei nomi specificati durante la creazione del certificato nella barra degli indirizzi, il browser Web dovrebbe indicare che la connessione è attendibile e sicura.

I certificati rilasciati da *Let's Encrypt* hanno una durata relativamente breve, attualmente 90 giorni. Per garantire la validità del certificato, è necessario ripetere la procedura descritta in precedenza prima che siano trascorsi 90 giorni.

Per ulteriori informazioni sull'utilizzo del client certbot, consultare la pagina della documentazione di certbot.