Utilizzo di Let's Encrypt Certificates con Cisco Business Dashboard

Obiettivo

Questo documento spiega come ottenere un certificato *Let's Encrypt*, installarlo in Cisco Business Dashboard e configurare il rinnovo automatico 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.

Il processo descritto in questo documento è stato automatizzato in Cisco Business Dashboard versione 2.2.2 e successive. Per ulteriori informazioni, consultare la sezione Sistema > Gestione dei certificati della Guida all'amministrazione.

Introduzione

Let's Encrypt è un'autorità di certificazione che fornisce gratuitamente certificati DV (Domain Validation) Secure Sockets Layer (SSL) al pubblico tramite 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, visitare il sito Web Let's Encrypt.

L'utilizzo dei certificati *Let's Encrypt* 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. La parte restante di questo documento descrive il processo di rilascio di un certificato e di automazione del rinnovo del certificato.

In questo documento vengono utilizzate le sfide HTTP per convalidare la proprietà del dominio. È quindi necessario che il server Web del dashboard sia raggiungibile da Internet tramite le porte standard TCP/80 e TCP/443. Se il server Web non è raggiungibile da Internet, è consigliabile utilizzare le sfide DNS. Per ulteriori informazioni, vedere Utilizzo di Let's Encrypt per Cisco Business Dashboard con DNS.

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.

Passaggio 2

Per consentire l'automazione del rinnovo del certificato, è necessario installare il client certbot nel dashboard. Per installare il client certbot nel server dashboard, utilizzare i comandi seguenti:

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.

```
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 3

Successivamente, il server Web del dashboard deve essere configurato per ospitare i file di richiesta necessari per verificare la proprietà del nome host. A tale scopo, viene creata una directory per questi file e viene aggiornato il file di configurazione del server Web. Quindi si riavvia l'applicazione Dashboard per rendere effettive le modifiche. Utilizzare i seguenti comandi:

```
cbd:~$sudo mkdir /usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo chmod 755
/usr/lib/ciscobusiness/dashboard/www/letsencrypt cbd:~$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
# Percorso per i file di verifica creati dalla posizione certbot /.well-known/acme-challenge {
root/usr/lib/ciscobusiness/dashboard/www/letsencrypt;
}
EOF
cbd:~$ 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
```

Passaggio 4

Richiedere un certificato utilizzando il comando seguente:

```
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 import -t pem -k /etc/letsencrypt/live/dashboard.example.com
/privkey.pem -c /tmp/cbdchain.pem
```

Questo comando indica al servizio *Let's Encrypt di* convalidare la proprietà dei nomi host forniti connettendosi al servizio Web ospitato su ciascuno dei nomi. Ciò significa che il servizio Web del dashboard deve essere accessibile da Internet e deve essere ospitato sulle porte 80 e 443. L'accesso all'applicazione del dashboard può essere limitato utilizzando le impostazioni del controllo di accesso nella pagina Sistema > Impostazioni piattaforma > Server Web nell'interfaccia utente di amministrazione del dashboard. Per ulteriori informazioni, consultare la Cisco Business Dashboard Administration Guide.

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.
—webroot -w ...	Installare i file di verifica nella directory creata in precedenza in modo che sia possibile accedervi tramite il server Web del dashboard.
-d dashboard.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.
-d pnpserver.example.com	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

—deploy-hook "..."	Cisco Business Dashboard Administration Guide. 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 nello stesso modo in cui i file sono stati caricati tramite l'interfaccia utente (UI) 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.

Passaggio 5

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

```
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 import -t pem -k /etc/letsencrypt/live/dashboard.example.com
/privkey.pem -c /tmp/cbdchain.pem"
Salvataggio del log di debug in /var/log/letsencrypt/letsencrypt.log
Plugin selezionati: Autenticatore webroot, Installatore Nessuno
```

Passaggio 6

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

```
Immetti l'indirizzo email (utilizzato per gli avvisi urgenti di rinnovo e sicurezza) (Immetti
'c' per
annulla): user@example.com
```

Passaggio 7

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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
A)acconsente/C)annulla: A
```

Passaggio 8

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 l'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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y
```

Passaggio 9

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

```
Come ottenere un nuovo certificato
Sfide:
http-01 sfida per dashboard.example.com
http-01 sfida per pnpserver.example.com
Utilizzando il percorso webroot /usr/lib/ciscobusiness/dashboard/www/letsencrypt per tutti i
domini non corrispondenti.
In attesa di verifica...
Problemi di pulizia
Esecuzione del comando deploy-hook: visitare il sito Web all'indirizzo
/etc/letsencrypt/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
/etc/letsencrypt/live/dashboard.example.com/privkey.pem -c /tmp/cbdchain.pem
NOTE IMPORTANTI:
Congratulazioni! Il certificato e la catena sono stati salvati in:
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
Il file di chiave è stato salvato in:
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Il certificato scadrà il 2020-10-29. 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 /etc/letsencrypt. 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
cbd:~$ sudo ls /etc/letsencrypt/live/dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
cbd:~$
```

La directory contenente i certificati dispone di autorizzazioni limitate, pertanto solo l'utente root 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.

Passaggio 10

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.

Notare che i certificati rilasciati da *Let's Encrypt* hanno una durata relativamente breve, attualmente 90 giorni. Il pacchetto certbot per Ubuntu Linux è configurato per controllare la validità del certificato due volte al giorno e rinnovare il certificato se sta per scadere, quindi non è necessario eseguire alcuna azione per mantenere il certificato aggiornato. Per verificare che i controlli periodici vengano eseguiti correttamente, attendere almeno dodici ore dalla creazione iniziale del certificato e quindi cercare nel file di log certbot messaggi simili ai seguenti: `cbd:~$ coda sudo /var/log/letsencrypt/letsencrypt.log`

```
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot versione: 0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main:Argomenti: ['-q']
2020-07-31 16:50:52,785:DEBUG:certbot.main:Plugin individuati:
(PluginEntryPoint#manuale,
PluginEntryPoint#null,PluginEntryPoint#standalone,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log:Livello di registrazione radice impostato su 30
2020-07-31 16:50:52,793:INFO:certbot.log:Salvataggio del log di debug su
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.selection:
Autenticatore richiesto <certbot.cli.
_Oggetto predefinito in 0x7f1152969240> e programma di installazione <certbot.cli.
_Oggetto predefinito in 0x7f1152969240>
2020-07-31 16:50:52,811:INFO:certbot.RENEW:Cert non ancora dovuto per il rinnovo
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.selection:Autenticatore richiesto
webroot e installatore Nessuno
2020-07-31 16:50:52,812:DEBUG:certbot.rinnovo:nessun errore di rinnovo
```

Trascorso il tempo necessario affinché la data di scadenza del certificato sia compresa entro trenta giorni, il client certbot rinnoverà il certificato e applicherà automaticamente il certificato aggiornato all'applicazione dashboard.

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