Uso de Cifrar certificados con Cisco Business Dashboard y validación de DNS

Objetivo

Este documento explica cómo obtener un certificado *Encriptemos* e instalarlo en Cisco Business Dashboard mediante la interfaz de línea de comandos (CLI). Si desea obtener información general sobre la administración de certificados, consulte el artículo Administrar certificados en el panel de Cisco Business.

Introducción

Let's Encrypt es una autoridad certificadora que proporciona al público certificados SSL gratuitos de validación de dominio (DV) mediante un proceso automatizado. *Cifrar* proporciona un mecanismo de fácil acceso para obtener certificados firmados para servidores web, lo que confiere al usuario final la confianza de que está accediendo al servicio correcto. Para obtener más información sobre *Cifremos*, visite el sitio web Cifremos.

Usar *Cifremos* certificados con Cisco Business Dashboard es razonablemente sencillo. Aunque Cisco Business Dashboard tiene algunos requisitos especiales para la instalación de certificados, además de poner el certificado a disposición del servidor web, sigue siendo factible automatizar la emisión e instalación del certificado mediante las herramientas de línea de comandos proporcionadas.

Para emitir y renovar certificados automáticamente, el servidor web del panel debe estar accesible desde Internet. Si no es así, se puede obtener fácilmente un certificado mediante un proceso manual y, a continuación, instalarlo mediante las herramientas de la línea de comandos. El resto de este documento recorre el proceso de emitir un certificado e instalarlo en el Panel.

Si el servidor web del panel es accesible desde Internet en los puertos estándar TCP/80 y TCP/443, es posible automatizar el proceso de instalación y administración de certificados. Consulte Cifremos para Cisco Business Dashboard para obtener más detalles.

Paso 1

El primer paso es obtener el software que utiliza el certificado de protocolo ACME. En este ejemplo, estamos utilizando el cliente certbot, pero hay muchas otras opciones disponibles.

Para obtener el cliente certbot, utilice el Panel u otro host que ejecute un sistema operativo similar a Unix (por ejemplo, Linux, macOS) y siga las instrucciones en el cliente certbot para instalar el cliente. En los menús desplegables de esta página, seleccione *Ninguno de los anteriores* para Software y su sistema operativo preferido para System.

Es importante tener en cuenta que en este artículo, las secciones azules son avisos y resultados de CLI. El `texto blanco` enumera los comandos. Los comandos de color verde, incluidos panel.ejemplo.com, pnpserver.ejemplo.com y user@example.com, deben reemplazarse por nombres DNS adecuados para su entorno.

Para instalar el cliente certbot en el servidor de Cisco Business Dashboard, utilice los siguientes comandos:

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

Paso 2

Cree un directorio de trabajo para que contenga todos los archivos asociados al certificado. Tenga en cuenta que estos archivos incluyen información confidencial como la clave privada del certificado y los detalles de la cuenta para el servicio *Cifremos*. Si bien el cliente de certificados creará archivos con los permisos adecuados y restrictivos, debe asegurarse de que el host y la cuenta que se está utilizando estén restringidos para el acceso sólo al personal autorizado.

Para crear el directorio en el Panel, introduzca los siguientes comandos:

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

Paso 3

Solicite un certificado mediante el siguiente comando:

```
cbd:~/certbot$certbot certonly —manual —preferido-desafía dns -d panel.ejemplo.com -d pnpserver.ejemplo.com
—logs-dir . —config-dir . —work-dir . —implementar "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"
```

Este comando instruye al servicio *Encriptemos* para validar la propiedad de los nombres de host proporcionados pidiéndole que cree registros DNS TXT para cada uno de los nombres enumerados. Una vez que se han creado los registros TXT, el servicio *Encriptemos* confirma que los registros existen y luego emite el certificado. Por último, el certificado se aplica al panel mediante la utilidad cisco-business-panel.

Los parámetros del comando son necesarios por los siguientes motivos:

certonly	Solicite un certificado y descargue los archivos. No intente instalarlos. En el caso de Cisco Business Dashboard, el certificado no sólo lo utiliza el servidor web, sino también el servicio PnP y otras funciones. Como resultado, el cliente de certificados no puede instalar el certificado automáticamente.
--manual	No intente autenticarse automáticamente con el servicio *Cifrar*. Trabaje de forma interactiva con el usuario para autenticarse.
—preferido-Challenge dns	Autentique mediante registros DNS TXT.
-d panel.ejemplo.com -d pnpserver.example.com	Los FQDN que se deben incluir en el certificado. El nombre mostrado se incluirá en el campo Nombre común del certificado y todos los nombres se enumerarán en el campo Asunto-Alt-Nombre. El nombre pnpserver.<domain> es un nombre especial que utiliza la función Network Plug and Play al realizar la detección de DNS. Consulte la guía de administración de Cisco Business Dashboard para obtener más información.
—logs-dir . —config-dir . —work-dir .	Utilice el directorio actual para todos los archivos de trabajo creados durante el proceso.
—Deploy-hook "..."	Utilice la utilidad de línea de comandos cisco-business-panel

para tomar la clave privada y la cadena de certificados recibida del servicio *Cifrar* y cargarlos en la aplicación de panel de la misma forma que si los archivos se cargaran a través de la interfaz de usuario del panel (IU).

El certificado raíz que ancla la cadena de certificados también se agrega al archivo de certificado aquí. Esto es necesario para ciertas plataformas que se implementan mediante Network Plug and Play.

La instalación automática del certificado mediante la opción —Deploy-hook sólo es posible cuando el cliente de certbot se está ejecutando en el servidor de tablero. Si el cliente certbot se está ejecutando en un equipo diferente, los archivos de clave privada y de certificado de cadena completa se deben copiar en el servidor de tablero e instalar mediante los comandos:

-cat <archivo de certificado completo> /etc/ssl/certs/DST_Root_CA_X3.pem >/tmp/cbdchain.pem

cisco-business-Dashboard importcert -t pem -k <private key file> -c /tmp/cbdchain.pem

Paso 4

Siga el proceso de creación del certificado siguiendo las instrucciones generadas por el cliente de certificados:

```
cbd:~/certbot$certbot certonly —manual —preferido-desafía dns -d panel.ejemplo.com -d
pnpserver.ejemplo.com
—logs-dir . —config-dir . —work-dir . —implementar "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"
Guardando registro de depuración en /home/cisco/certbot/letsencrypt.log
Complementos seleccionados: Manual del autenticador, Instalador Ninguno
```

Paso 5

Introduzca la dirección de correo electrónico o **C** para cancelar.

```
Introduzca la dirección de correo electrónico (utilizada para los avisos de seguridad y
renovación urgentes) (introduzca "c" para cancelar): user@example.com
Inicio de nueva conexión HTTPS (1): acme-v02.api.letsencrypt.org
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -
```

Paso 6

Introduzca **A** para aceptar o **C** para cancelar.

```
Lea las condiciones del servicio en
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. Debe
aceptar para registrarse en el servidor ACME en
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

- -
- -
- - - - - - - - - -
Introduzca **A** para aceptar o **C** para cancelar.
(A)gree/(C)ancel: R
- -
- -
- -
- -
- -
- - - - - - - - - -

Paso 7

Introduzca **Y** para Sí o **N** para No.

¿Estaría dispuesto a compartir su dirección de correo electrónico con Electronic Frontier?
Foundation, socio fundador del proyecto *Cifremos* y la organización sin ánimo de lucro
organización que desarrolla Certbot? Nos gustaría enviarle un correo electrónico sobre nuestro
trabajo
encriptación de la web, noticias de EFF, campañas y formas de apoyar la libertad digital.
Introduzca **Y** para Sí o **N** para No.
(Y)es/(N)o: S
Obtención de un nuevo certificado
Realización de los siguientes retos:
desafío dns-01 para panel.ejemplo.com
desafío dns-01 para pnpserver.example.com
- -
- -
- -
- -
- -
- - - - - - - - - -

Paso 8

Introduzca **Y** para Sí o **N** para No.

NOTE: La dirección IP de esta máquina se registrará públicamente como si lo hubiera solicitado
certificado. Si está ejecutando certbot en modo manual en una máquina que no lo está
su servidor, por favor asegúrese de que está de acuerdo con eso.
¿Está de acuerdo con que se registre su IP?
- -
- -
- -
- -
- -
- - - - - - - - - -
Introduzca **Y** para Sí o **N** para No.
(Y)es/(N)o: S
- -
- -
- -
- -
- -
- - - - - - - - - -
Implemente un registro TXT DNS con el nombre
_acme-desafío.panel.ejemplo.com con el siguiente valor:
3AzDTqNGXb8kSkhqXXYWE2iZrFAVCGT2B8oZNGyBwhc

Paso 9

Se debe crear un registro TXT DNS para validar la propiedad del nombre de host de panel.ejemplo.com en la infraestructura DNS. Los pasos necesarios para hacer esto están fuera del alcance de este documento y dependerán del proveedor DNS que se utilice. Una vez creado, valide que el registro esté disponible mediante una herramienta de consulta DNS como Dig.

El proceso de desafío de DNS puede automatizarse para ciertos proveedores de DNS. Consulte Complementos DNS para obtener más detalles.

Pulse **Intro** en el teclado.

```
Antes de continuar, verifique que se haya implementado el registro.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - -
Presione Ingresar para continuar
```

Paso 10

Recibirá un resultado CLI similar. Cree y verifique registros TXT adicionales para cada nombre que se incluirá en el certificado. Repita el paso 9 para cada nombre especificado en el comando certbot.

Pulse **Intro** en el teclado.

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - -
Implemente un registro TXT DNS con el nombre
_acme-desafío.pnpserver.example.com con el siguiente valor:
Txruc89x8dVaHmLHJII0oA2ILmIY83XYl13yYakjNuc
Antes de continuar, verifique que se haya implementado el registro.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - -
Presione Ingresar para continuar
```

Paso 11

El certificado ha sido emitido y puede encontrarse en el subdirectorio *activo* en el sistema de archivos:

```
Esperando verificación...
Eliminación de los retos
Trayectorias no estándar, es posible que no funcionen con crontab instalado por el administrador
de paquetes del sistema operativo
```

```
Ejecución del comando de implementación-gancho: 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
NOTAS IMPORTANTES:
- ¡Enhorabuena! Su certificado y cadena se han guardado en:
/home/cisco/certbot/live/dashboard.example.com/fullchain.pem
El archivo de clave se ha guardado en:
/home/cisco/certbot/live/dashboard.example.com/privkey.pem
Su certificado caducará el 2020-11-11. Para obtener una nueva o una nueva
versión de este certificado en el futuro, simplemente ejecute certbot
de nuevo. Para renovar *todos* los certificados de forma no interactiva, ejecute
"renovación de certbot"
- Las credenciales de su cuenta se han guardado en su robot de certificación
directorio de configuración en /home/cisco/certbot. Debería hacer un
copia de seguridad segura de esta carpeta ahora. Este directorio de configuración
también contiene certificados y claves privadas obtenidas por Certbot así
realizar copias de seguridad regulares de esta carpeta es ideal.
- Si le gusta Certbot, considere apoyar nuestro trabajo:
Donación a ISRG / Cifremos: https://letsencrypt.org/donate
Donación a EFF: https://eff.org/donate-le
```

Paso 12

Ingrese los siguientes comandos:

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

El directorio que contiene los certificados tiene permisos restringidos, por lo que sólo el usuario de cisco puede ver los archivos. El archivo *privkey.pem*, en particular, es sensible y el acceso a este archivo debe limitarse únicamente al personal autorizado.

El panel debe estar ejecutándose con el nuevo certificado. Si abre la interfaz de usuario del panel en un explorador web introduciendo cualquiera de los nombres especificados al crear el certificado en la barra de direcciones, el explorador web debe indicar que la conexión es segura y de confianza.

Tenga en cuenta que los certificados emitidos por *Let's Encrypt* tienen una vida útil relativamente corta, actualmente de 90 días. Para asegurarse de que el certificado sigue siendo válido, deberá repetir el proceso descrito anteriormente antes de que hayan transcurrido 90 días.

Para obtener más información sobre el uso del cliente de certbot, consulte la página de documentación de certbot.