Uso de Cifrar certificados con Cisco Business Dashboard

Objetivo

Este documento explica cómo obtener un certificado *Encriptemos*, instalarlo en Cisco Business Dashboard y configurar la renovación automática 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.

El proceso descrito en este documento se ha automatizado en Cisco Business Dashboard versión 2.2.2 y posteriores. Consulte la sección Sistema > Administración de certificados de la Guía de administración para obtener más información.

Introducción

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

Usar certificados *Cifremos* 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. El resto de este documento recorre el proceso de emitir un certificado y automatizar la renovación del certificado.

Este documento utiliza los desafíos HTTP para validar la propiedad del dominio. Esto requiere que el servidor web del panel sea accesible desde Internet en los puertos estándar TCP/80 y TCP/443. Si el servidor web no es accesible desde Internet, considere la posibilidad de utilizar los retos de DNS en su lugar. Consulte Uso de Cifrar para Cisco Business Dashboard con DNS 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.

Paso 2

Para permitir que la renovación de certificados se automatice, el cliente de certificados se debe instalar en el Panel. Para instalar el cliente certbot en el servidor Panel, utilice los siguientes comandos:

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.

```
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 3

A continuación, el servidor web del panel debe configurarse para alojar los archivos de desafío necesarios para verificar la propiedad del nombre de host. Para ello, creamos un directorio para estos archivos y actualizamos el archivo de configuración del servidor web. A continuación, reiniciamos la aplicación Panel para que los cambios surtan efecto. Utilice los siguientes comandos:

```
cbd:~$sudo mkdir /usr/lib/ciscobusiness/panel/www/letsencrypt cbd:~$sudo chmod 755
/usr/lib/ciscobusiness/panel/www/letsencrypt cbd:~$sudo bash -c 'cat >
/var/lib/ciscobusiness/dashboard/nginx/nginx-loc-letsencrypt.conf' << EOF
# Ubicación de los archivos de desafío creados por ubicación de certbot /.well-known/acme-
Challenge {
root/usr/lib/ciscobusiness/panel/www/letsencrypt;
}
EOF
cbd:~$ 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-panel start
```

Paso 4

Solicite un certificado mediante el siguiente comando:

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/panel/www/letsencrypt/ -d
panel.ejemplo.com -d pnpserver.example.com —despliegue-hook "cat /etc/letsencrypt/live/
panel.ejemplo.com/fullchain.pem ; /usr/bin/cisco-business-Dashboard importcert -t pem -k
/etc/letsencrypt/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 mediante la conexión al servicio web alojado en cada uno de los nombres. Esto significa que el servicio web del panel debe ser accesible desde Internet y estar alojado en los puertos 80 y 443. El acceso a la aplicación del panel puede restringirse mediante la opción de control de acceso en la página System > Platform Settings > Web Server de la interfaz de usuario de administración del panel. Consulte la guía de administración de Cisco Business Dashboard para obtener más información.

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.
—webroot -w...	Instale los archivos de desafío en el directorio creado anteriormente para que se pueda acceder a ellos a través del servidor web del panel.
-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

—Deploy-hook "..."	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. 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.

Paso 5

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

```
cbd:~$sudo certbot certonly —webroot -w /usr/lib/ciscobusiness/panel/www/letsencrypt/ -d
panel.ejemplo.com -d pnpserver.example.com —despliegue-hook "cat /etc/letsencrypt/live/
panel.ejemplo.com/fullchain.pem ; /usr/bin/cisco-business-Dashboard importcert -t pem -k
/etc/letsencrypt/live/Dashboard.example.com /privkey.pem -c /tmp/cbdchain.pem"
Guardando registro de depuración en /var/log/letsencrypt/letsencrypt.log
Complementos seleccionados: Authenticator webroot, Installer None
```

Paso 6

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
```

Paso 7

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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -
(A)gree/(C)ancel: R
```

Paso 8

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

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -
¿Estaría dispuesto a compartir su dirección de correo electrónico con Electronic Frontier?
Foundation, un socio fundador del proyecto Let's Encrypt 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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - -
(Y)es/(N)o: S
```

Paso 9

El certificado ha sido emitido y puede encontrarse en el subdirectorio */etc/letsencrypt/live* en el sistema de archivos:

```
Obtención de un nuevo certificado
Realización de los siguientes retos:
http-01 Challenge para Dashboard.example.com
http-01 Challenge para pnpserver.example.com
Utilizando la ruta de acceso de webroot /usr/lib/ciscobusiness/panel/www/letsencrypt para todos
los dominios sin coincidencia.
Esperando verificación...
Eliminación de los retos
Ejecución del comando de implementación-gancho: 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
NOTAS IMPORTANTES:
- ¡Enhorabuena! Su certificado y cadena se han guardado en:
/etc/letsencrypt/live/dashboard.example.com/fullchain.pem
El archivo de clave se ha guardado en:
/etc/letsencrypt/live/dashboard.example.com/privkey.pem
Su certificado caducará el 2020-10-29. 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 /etc/letsencrypt. 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
cbd:~$ sudo ls /etc/letsencrypt/live/Dashboard.example.com
/ cert.pem chain.pem fullchain.pem privkey.pem README
cbd:~$
```

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

Paso 10

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 *Cifrar* tienen una duración relativamente corta, actualmente de 90 días. El paquete de certificado para Ubuntu Linux está configurado para verificar la validez del certificado dos veces al día y renovar el certificado si se acerca a la fecha de vencimiento, por lo que no se requiere ninguna acción para mantener actualizado el certificado. Para verificar que las comprobaciones periódicas se están produciendo correctamente, espere al menos doce horas después de crear inicialmente el certificado y, a continuación, verifique el archivo de registro de certificados para ver mensajes similares a los siguientes: `cbd:~$ sudo tail /var/log/letsencrypt/letsencrypt.log`

```
2020-07-31 16:50:52,783:DEBUG:certbot.main:certbot versión: 0.31.0
2020-07-31 16:50:52,784:DEBUG:certbot.main:Argumentos: ['-q']
2020-07-31 16:50:52,785:DEBUG:certbot.main:Complementos descubiertos:
(PluginEntryPoint#manual,
PluginEntryPoint#null,PluginEntryPoint#autónomo,PluginEntryPoint#webroot)
2020-07-31 16:50:52,793:DEBUG:certbot.log:Nivel de registro raíz establecido en 30
2020-07-31 16:50:52,793:INFO:certbot.log:Almacenamiento del registro de depuración en
/var/log/letsencrypt/letsencrypt.log
2020-07-31 16:50:52,802:DEBUG:certbot.plugins.select:
autenticador solicitado <certbot.cli.
_Objeto predeterminado en 0x7f1152969240> e instalador <certbot.cli.
_Objeto predeterminado a 0x7f1152969240>
2020-07-31 16:50:52,811:INFO:certbot.renovación:Certificado aún no renovado
2020-07-31 16:50:52,812:DEBUG:certbot.plugins.select:Requested authenticator
webroot e installer None
2020-07-31 16:50:52,812:DEBUG:certbot.renovación:sin fallos de renovación
```

Una vez transcurrido el tiempo suficiente para que la fecha de vencimiento del certificado se encuentre dentro de los treinta días, el cliente de certificados renovará el certificado y aplicará el certificado actualizado a la aplicación de panel automáticamente.

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