Cómo crear un certificado SSL en IIS con Let's Encrypt

por Diego Bonavida

Para obtener un certificado SSL, a través de Let's Encrypt, para un host que esté corriendo en una máquina de Windows hay tres opciones:

1) Usar la herramienta LetsEncrypt-Win-Simple. Es la forma más fácil de obtener el certificado, se ejecuta a través de la línea de comandos.
2) Usar la librería ACMESharp, una librería de Windows PowerShell que usa la API de ACME para obtener el certificado a través de una gran variedad de comandos. Esta opción es la que te permite tener más control.
3) Usar Certify, un cliente de Let's Encrypt que te ayuda a obtener el certificado de manera rápida. Aún está en su versión alfa, por lo que no se recomienda.

A continuación se presentan los pasos para crear un certificado SSL a través de la segunda opción, usando la librería ACMESharp en Windows PowerShell.

1	Asegurarse de tener el host para el que quieres obtener el certificado corriendo en IIS, en la propia máquina en la que se va a usar la herramienta.
2	Asegurarse de que el host es accesible desde internet (puerto 80 para http y puerto 443 para https). En Azure es de la siguiente forma: *Máquinas virtuales* > *Grupo de recursos* > *Grupo de seguridad de red* > *Reglas de seguridad de entrada.*
3	Asegurarse de que el Firewall de Windows no esté bloqueando los puertos 80 y 443 (por defecto no deberían).
4	Abrir Windows PowerShell. Si no lo tienes, instálalo.
5	Descargar e instalar la librería ACMESharp como un módulo de Windows PowerShell. Ya que, dependiendo de si tienes una versión u otra, el método y comandos son distintos, se presenta una solución para instalarlo manualmente que sirve para cualquier versión. 1. Descargar el archivo *ACME-posh.zip* de la última release. 2. Click derecho al archivo e ir a Propiedades. Marcar la casilla "Desbloquear", ya que todos los archivos se encuentran bloqueados. 3. Extraer la carpeta ACMESharp en el directorio de los módulos de PS: C:\Windows\System32\WindowsPowerShell\v1.0\Modules

6	Importar el módulo e inicializar *Vault*. Para ello, ejecutar en PowerShell los siguientes comandos:
	`Import-Module ACMESharp`
	`Import-Module ACMESharp\ACMESHARP-IIS`
	`Initialize-ACMEVault`

7 Crear un nuevo *Registration* usando el siguiente comando:

```
New-ACMERegistration -Contacts mailto:somebody@example.org -AcceptTos
```

8 Crear un identificador para el dominio usando el siguiente comando, poniendo los nombres que desees en los parámetros tras -Dns y -Alias. Esos nombres se usarán en los siguientes pasos:

```
New-ACMEIdentifier -Dns myserver.example.com -Alias dns1
```

9 Probar que el dominio es propiedad del usuario. Hay dos formas de probarlo, a través del HTTP Challenge o del DNS Challenge. Para este caso, se va a usar la primera opción. Ejecuta el siguiente comando usando los nombres que se utilizaron en el paso anterior, además de sustituir YOUR_SITE_NAME por el nombre del sitio existente en el IIS Manager correspondiente al dominio:

```
Complete-ACMEChallenge dns1 -ChallengeType http-01 -Handler iis
-HandlerParameters @{ WebSiteRef = 'YOUR_SITE_NAME' }
```

10 Una vez realizado el HTTP Challenge (***Nota:*** *Asegurarse que, en la página web, los ficheros estáticos pueden ser accesibles desde el navegador, o la prueba puede fallar*), toca enviar la respuesta con el siguiente comando:

```
Submit-ACMEChallenge dns1 -ChallengeType http-01
```

11 Como el servidor de Let's Encrypt valida las respuestas de forma asíncrona, es posible que no se obtenga una respuesta inmediata. Ejecutar el siguiente comando para ver el estado de la validación:

```
(Update-ACMEIdentifier dns1 -ChallengeType http-01).Challenges |
Where-Object {$_.Type -eq "http-01"}
```

En la respuesta, es posible que se vea el campo *Status* con el valor de "pending". Ejecutar el comando anterior las veces necesarias hasta que *Status* tome el valor de "valid".

```
...
Status         : valid
...
```

12 Generar el certificado y enviarlo con los siguientes comandos:

```
New-ACMECertificate dns1 -Generate -Alias cert1
Submit-ACMECertificate cert1
```

13 Si el certificado no se ha generado de forma inmediata, actualizar con el siguiente comando las veces necesarias hasta ver que el campo *IssuerSerialNumber* tiene como valor una cadena alfanumérica:

```
Update-ACMECertificate cert1
```

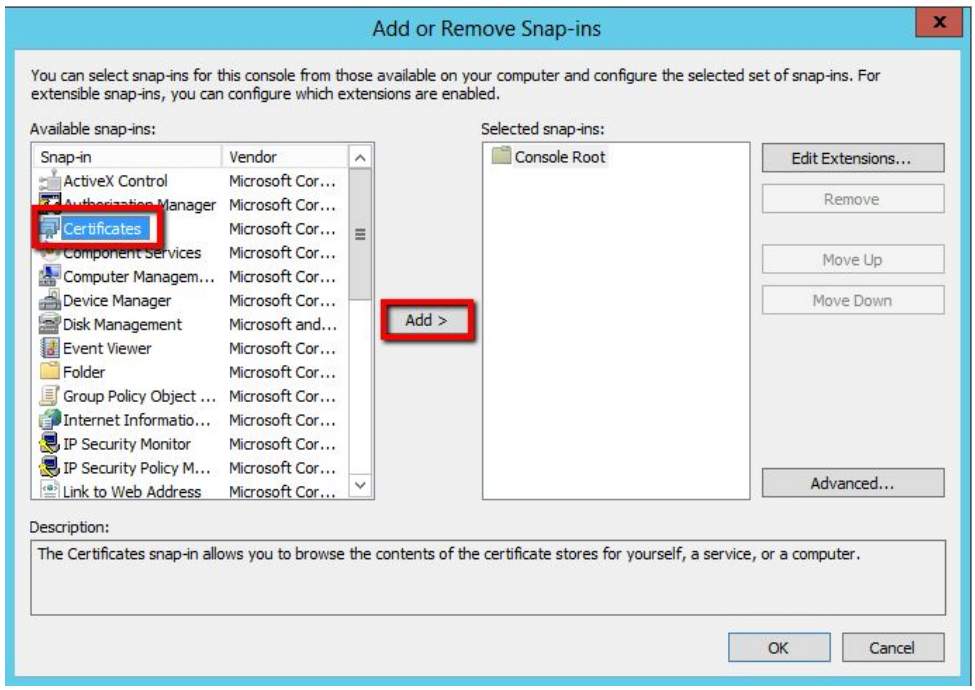
14 Exportar el certificado en un archivo PFX para instalarlo en el IIS con el siguiente comando:

```
Get-ACMECertificate cert1 -ExportPkcs12 "path\to\cert1.pfx"
```

15 Para importar el certificado en el IIS a través de un archivo PFX se han de realizar los siguientes pasos:

1. Click derecho al botón de Inicio en Windows y seleccionar “Ejecutar”. En la ventana emergente, escribir *mmc* y Aceptar.

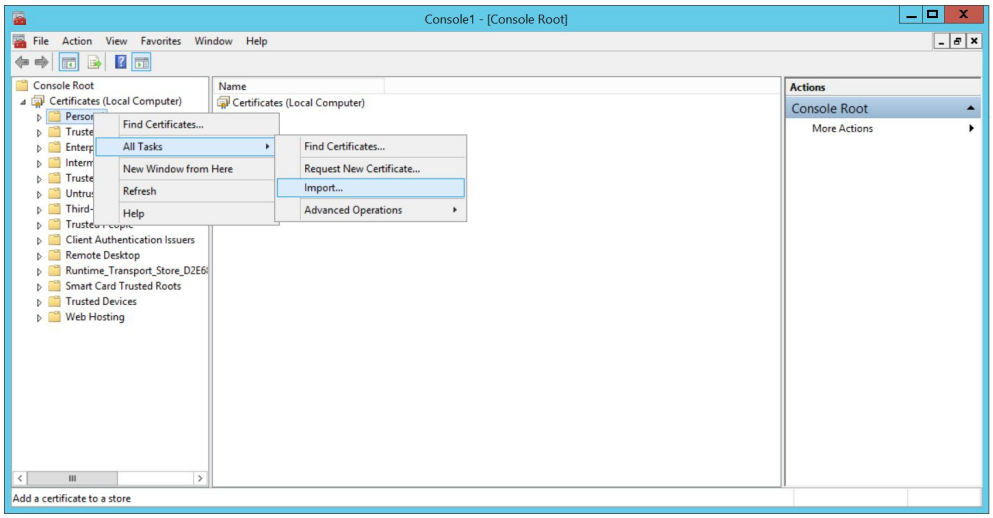
2. Se abrirá una ventana *Console*. Ir a *File* > *Add/Remove Snap-in*, y en la nueva ventana, seleccionar “Certificates” y añadirlo al panel de la derecha, tal y como se muestra en la imagen.



3. A continuación, en la ventana *Certificates snap-in*, seleccionar la opción “Computer Account”. Darle a Next.

4. En la ventana *Select Computer*, seleccionar la opción “Local Computer: (the computer this console is running on)”. Darle a Finish.

5. De vuelta a la ventana *Console*, en la sección de Console Root, expandir la carpeta “Certificates (Local Computer)”, hacer click derecho en la carpeta “Personal” y seleccionar *All tasks* > *Import*, tal y como se muestra en la imagen.



6. Se abrirá una nueva ventana para importar el certificado. En la primera página, seleccionar el archivo PFX correspondiente al certificado SSL que se quiera importar. Darle a Next.

7. En la página siguiente, si no se puso una contraseña al certificado cuando se exportó desde el Windows PowerShell, dejar el campo vacío y darle a Next.

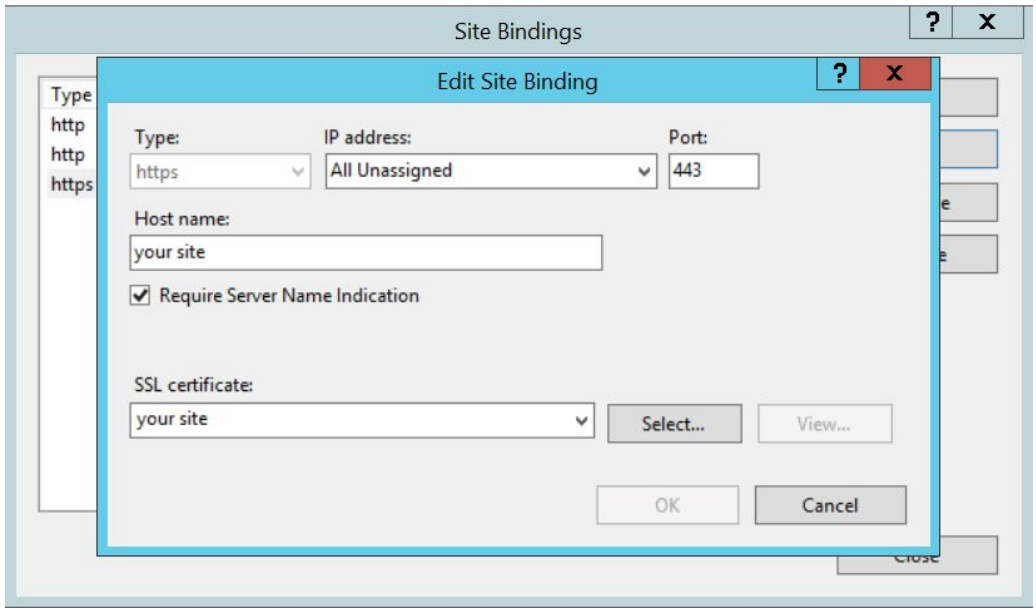
8. En la página *Certificate Store*, seleccionar la opción “Automatically select the certificate store based on the type of certificate”. Darle a Next.

9. Verificar la información y darle a Finish. Una vez mostrado el mensaje “The import was successful” sólo falta activar el certificado en el IIS.

16 Para activar el certificado importado en el paso anterior, hay que dirigirse al IIS Manager y en la sección *Sites*, seleccionar el sitio en el que se quiere activar el certificado.

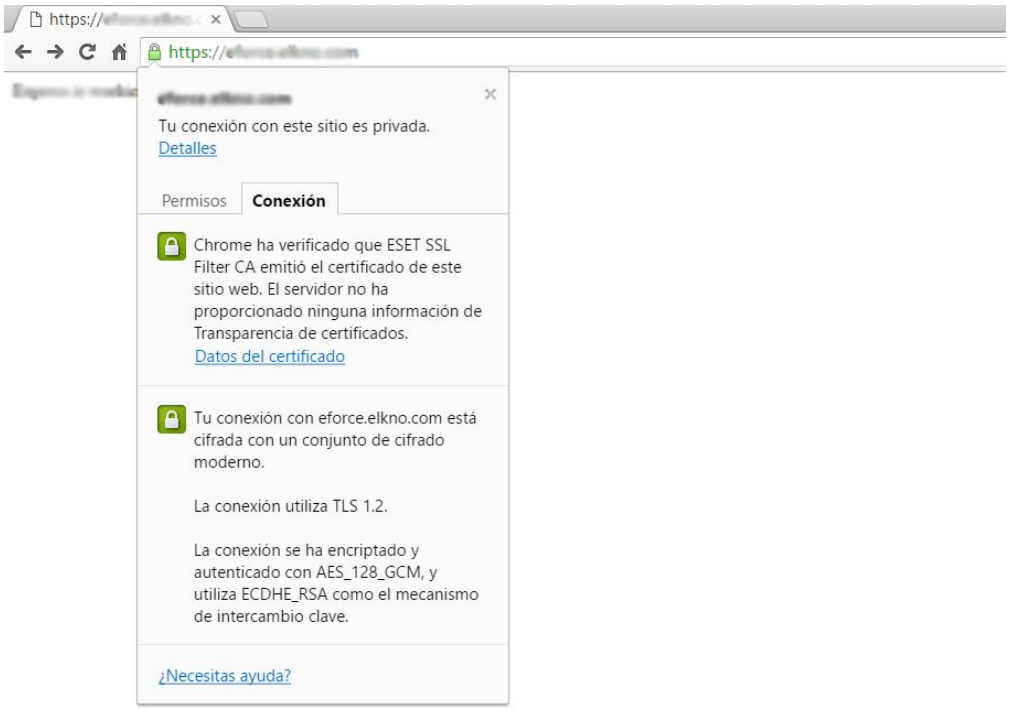
17 A continuación, en el menú *Actions*, seleccionar *Bindings*.

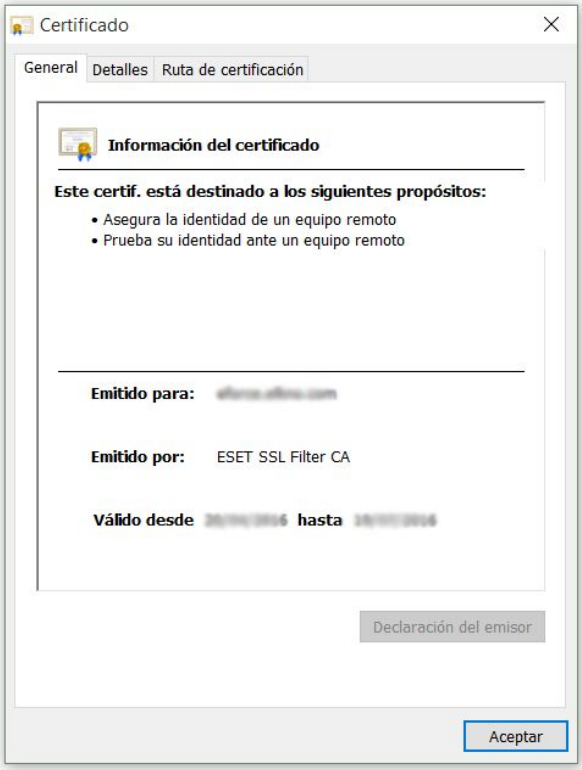
18 Se abrirá una nueva ventana *Site Bindings*. Darle al botón Añadir y rellenar los campos tal y como se muestra en la imagen, cambiando “your site” por el dominio que se quiere asegurar, además de seleccionar el certificado con el mismo nombre que el dominio (establecido por defecto).



19 Una vez instalado el certificado, toca reiniciar IIS o el sitio para que se reconozca.

20 Abre el navegador y accede a tu dominio a través de https. Verás cómo, a partir de ahora, tu sitio estará protegido con un certificado SSL tal y como se ve en las imágenes.





Una vez realizados estos pasos, tendremos un certificado SSL emitido por Let's Encrypt para los próximos tres meses.

Para poder extender el certificado una vez haya expirado ese periodo de tiempo, no hay implementada aún una opción de renovación (al menos no en la versión de ACMESharp con la que se hizo este documento, correspondiente a la v0.8.1.0), por lo que la única opción es volver a abrir el Windows PowerShell, importar la librería de ACMESharp con el comando "Import-Module ACMESharp" y repetir los pasos del 12 al 19, asignando un nombre diferente al alias del certificado.