Personalizando un Certificado CA en Zeroshell.

Escrito por: Joker

Un poco de Cultura….

¿Qué es un CA x.509?

Un Certificado Digital es el equivalente electrónico a un Documento de Identidad. Permite identificarnos, firmar y cifrar electrónicamente documentos y mensajes.

El Certificado Digital garantiza:

- La integridad de los datos transmitidos
- Su procedencia
- La detección de cualquier manipulación que hayan podido sufrir

En otras palabras el CA es un documento electrónico el cual permite identificarnos ante el servidor zeroshell para entablar comunicación privada y segura a través de la red.

¿Para que usa Zeroshell los CA?

Lo usa para entablar conexiones seguras SSL, para sincronizar datos vía VPN, para expedir un certificado para la configuración de RADIUS SERVER, entre otros muchos usos.

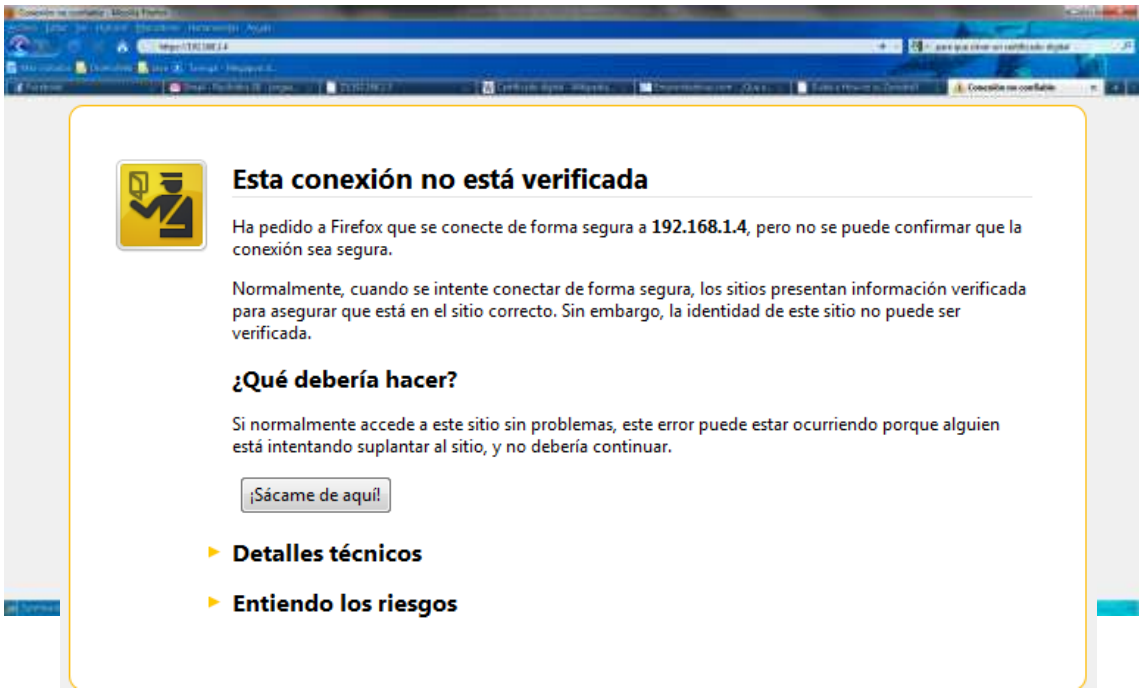
¿Por qué crear mi propio CA y no Usar el Default?

Si solo vamos a usar Zeroshell para probarlo y ver las diferentes funciones que tiene no es necesario crear un CA personalizado ya que bastara con el que por default crea zeroshell, pero si deseamos realizar una implementación de zeroshell en un ambiente productivo o real que mejor que tener nuestros propios certificados que muestren información sobre quienes somos realmente. (Esto no le quita el crédito a zeroshell solo hablo de identificarnos nosotros mismos ante nuestra implementación).

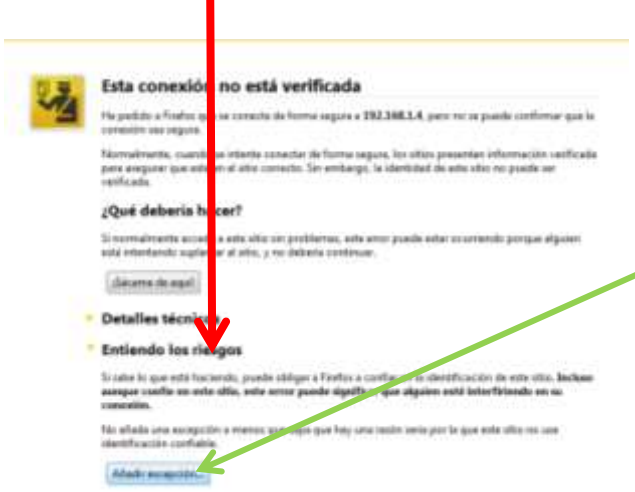
Bueno después de estas 3 preguntas fundamentales para comenzar aquí vamos….

Ingresamos a la interface gráfica de Zeroshell a través de la dirección ip o dominio en el que zeroshell fue previamente configurado:

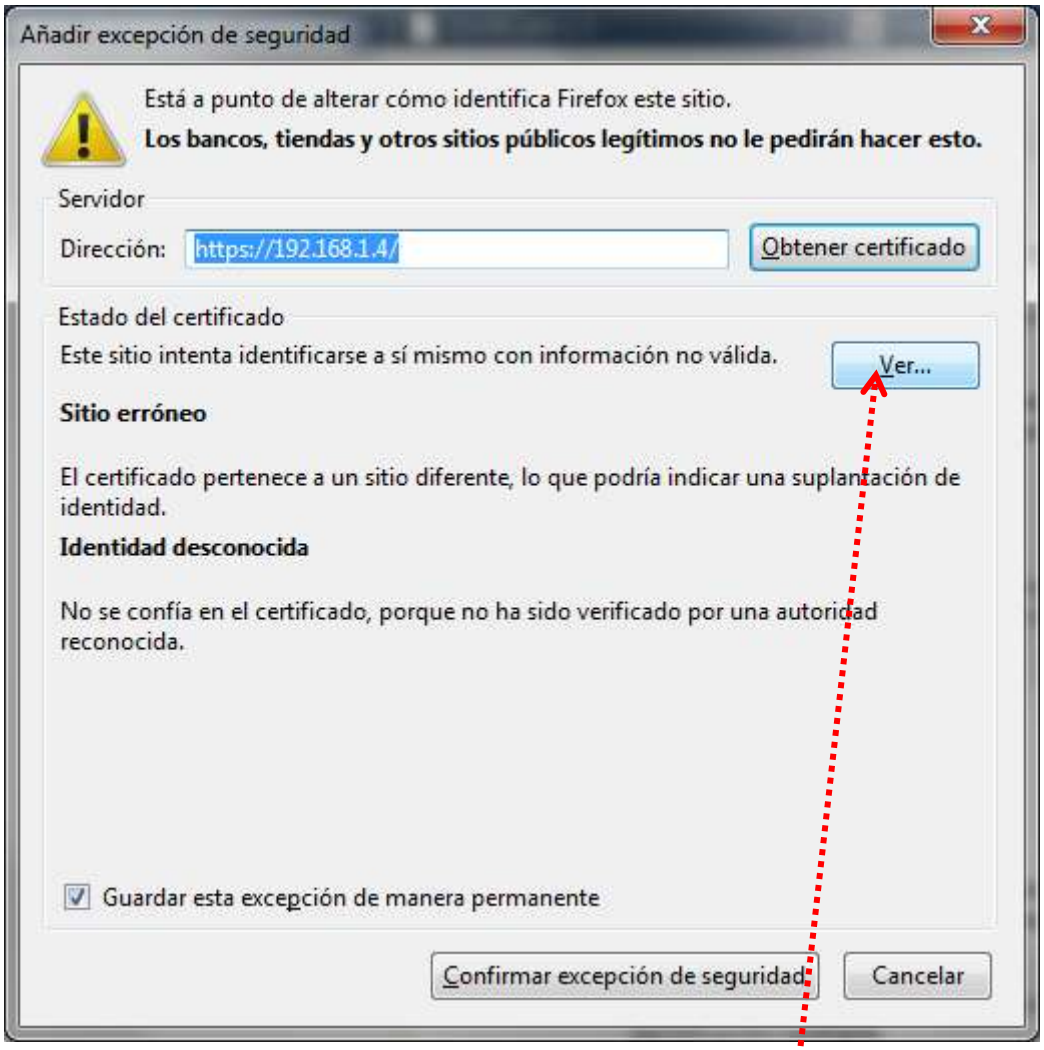
Nota: si estamos trabajando en el profile default de Zeroshell la ip es 192.168.0.75, aunque recomiendo crear nuestro propio perfil.



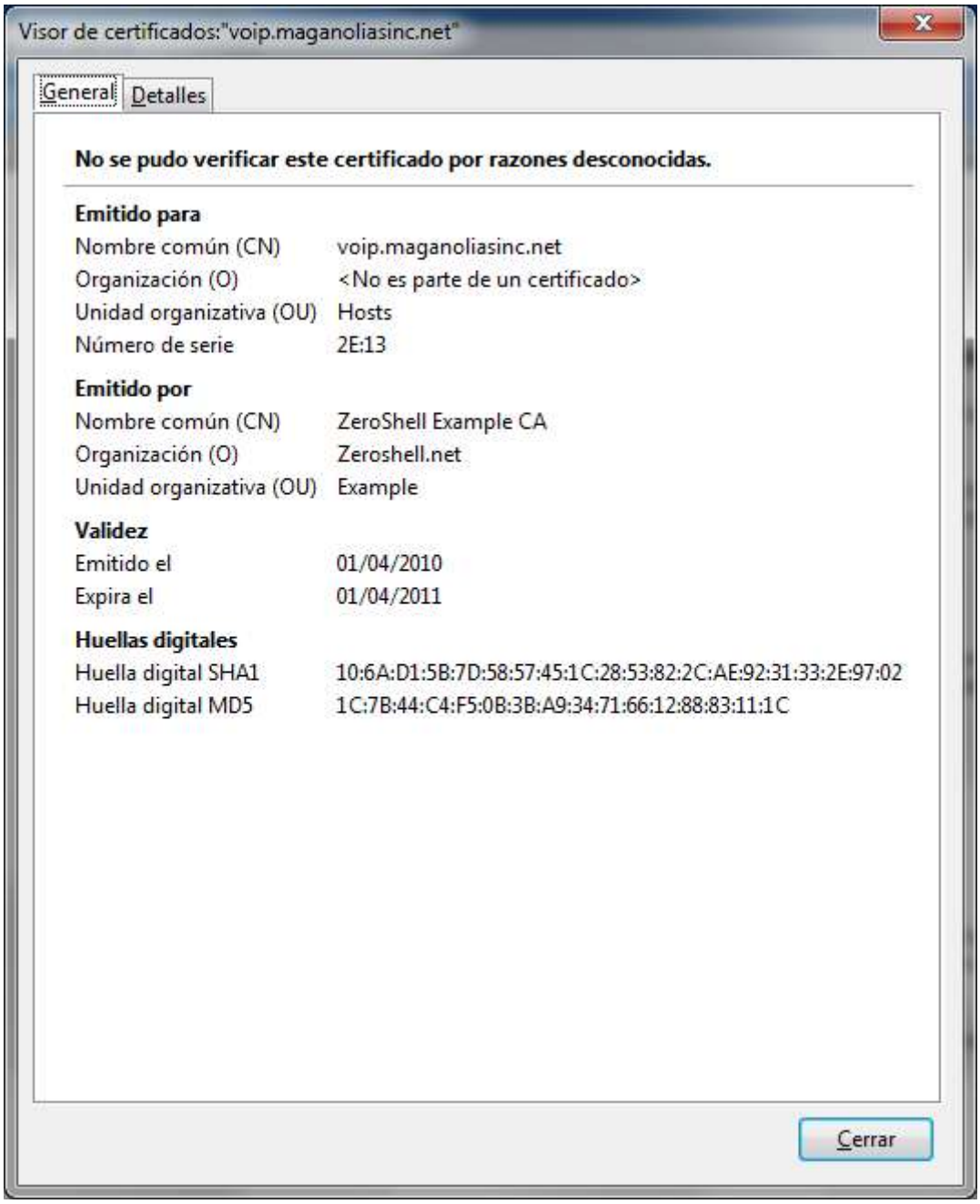
Como podrán ver en el primer inicio nos dira que la conexión no esta verificada en pocas palabras el certificado no es valido para las politicas de nuestro navegador, el movito no es que sea dañino o falso nuestro certificado si no que el validador de mozilla de acuerdo a sus politicas de Certificados ha leido a nuestra identidad Emisora de Certificados como no valida pero eso no significa que estamos en problemas o que no va a funcionar, basta con hacer click en “Entiendo los riesgos”



Y añadir una excepción haciendo clic sobre la leyenda “Añadir Excepción”.



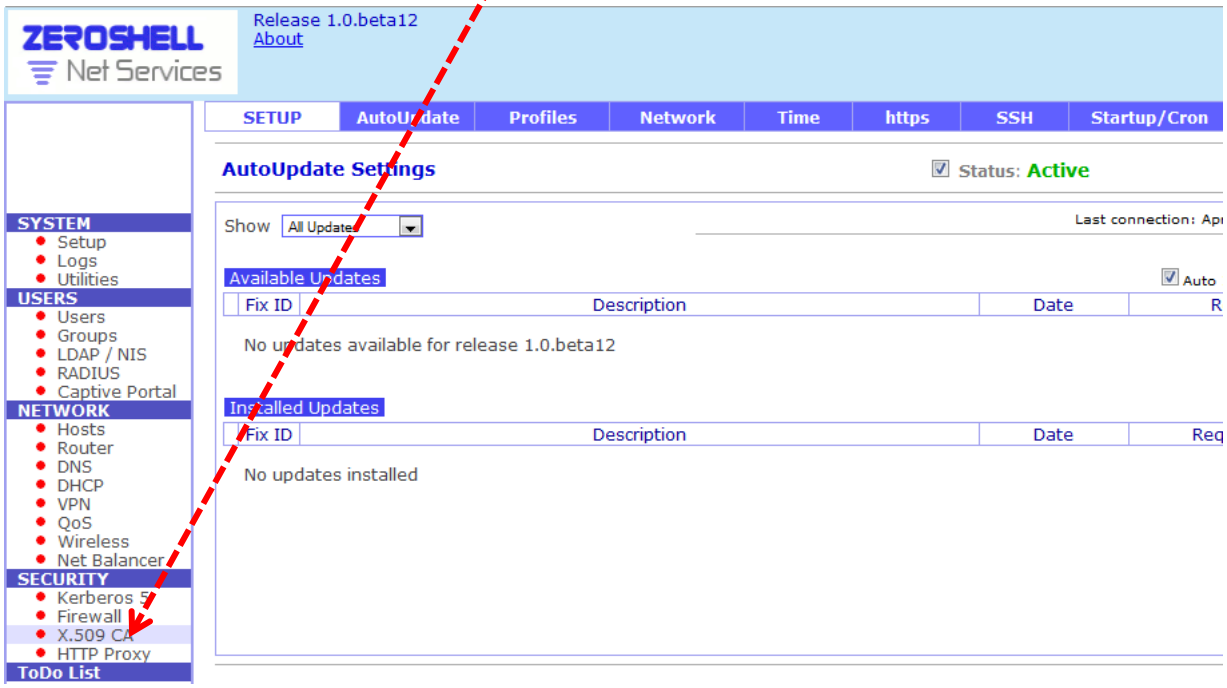
Al hacer clic en “Añadir Excepción” nos aparece una pantalla semejante a esta… vamos a revisar unos cuantos datos haciendo clic sobre el botón “Ver…”



Bien este es nuestro certificado digital el cual fue emitido por zeroshell al entablar una conexión segura SSL , en el podemos apreciar información importante y relevante tal es el caso quien lo emitió, y para quien lo emitió, así como la huella digital o firma del certificado, podrán ver que por default aparece que lo emite zeroshell Example CA, repito si a nosotros solo nos interesa probar zeroshell no tiene ningún caso hacer este tutorial en cambio si vamos a implementar zeroshell para el ambiente en producción o ambiente real y queremos que nuestro Certificado Digital aparezca que fue emitido por nuestra implementación (institución, escuela, hospital), debemos personalizarlo , ¿Cómo hacerlo?, aquí comenzamos….

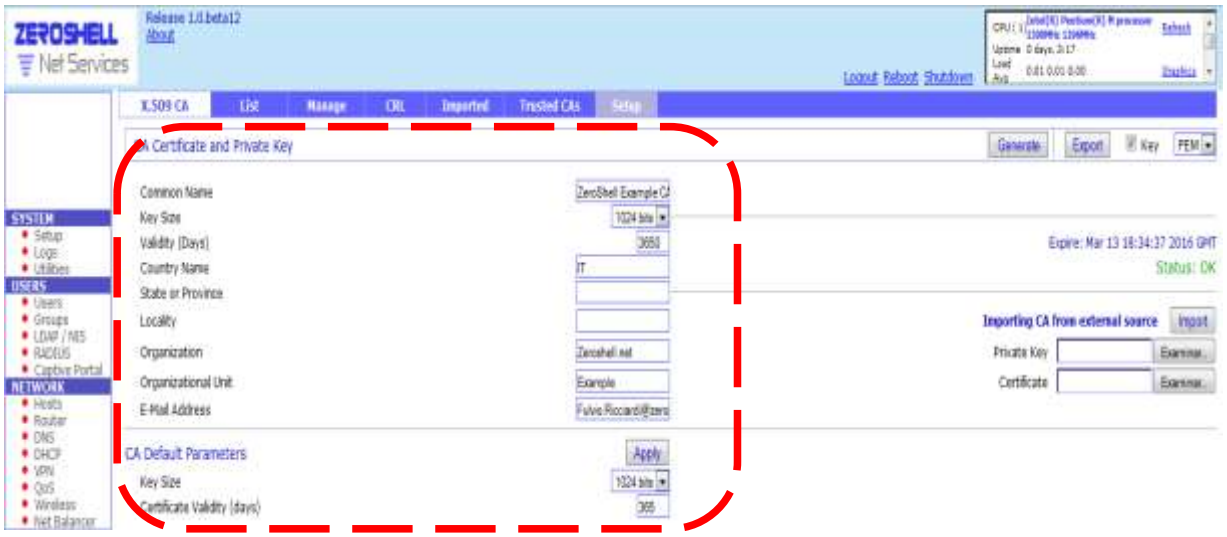
Una vez que hemos agregado la excepción de certificado y hecho login in previamente en la interface web de zeroshell…

Ir al menú Security >> X.509 CA



Acto seguido nos dirigimos a la opción o pestaña con la etiqueta: “Setup”

Una vez que hemos ingresado a “Setup” podremos ver un form de la siguiente manera:



Personalizamos cada uno de los campos del formulario con la información que deseamos:

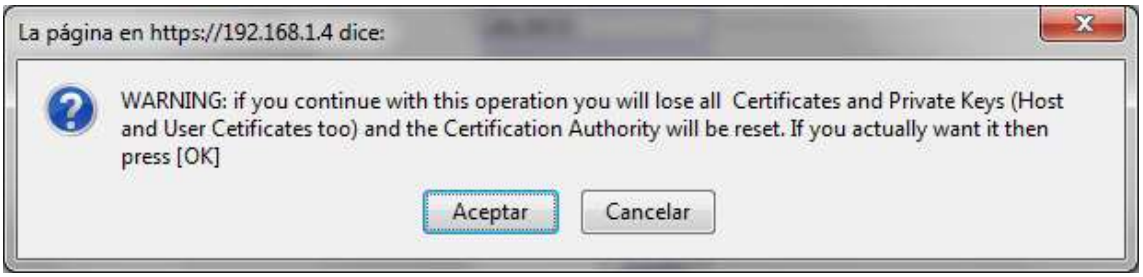
Por ejemplo yo quiero que mi nombre común sea Magnolias Inc. Entonces Borro los datos actuales e introduzco mi dato.

- **El Key Size:** lo dejamos por ahora en default o el valor de 1024 bits.
- **Validity (Days):** se refiere a la cantidad de días en que nuestro Certificado será valido.
- **Country Name:** Para nuestro caso que estamos en México es MX el valor.
- **Satate or Province:** Aquí podemos agregar un dato más sobre en que estado nos encontramos o simplemente dejarlo en blanco.
- **Locality:** La localidad actual.
- **Organization:** Organización a la que pertenecemos o institución.
- **Organization Unit:** Departamento para el cual estamos expidiendo el Certificado
- **Email Address:** Aquí va el mail de contacto o del administrador de la red generalmente.

De acuerdo a nuestro Ejemplo tendriamos algo asi:

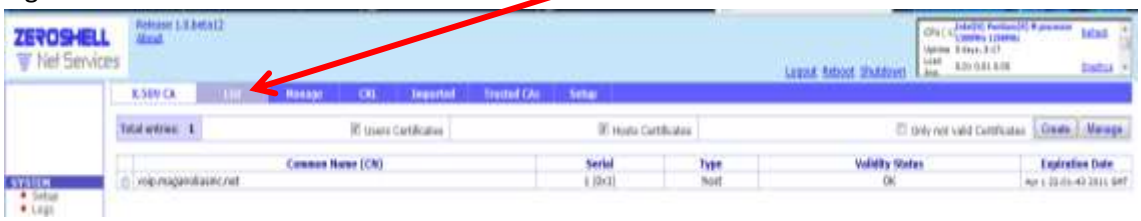
Paso siguinte es hacer clic sobre el botón con la leyenda “Generate”

Nos mostrara una advertencia que nos dice: PRECAUCIÓN: Si continuas con esta operaciones se perderan todos los Certificados y Llaves Privadas ya creadas (Incluyendo HOST y Certificados de Usuarios Tambien), y el certificado de Autoridad sera reiniciado. Aún asi deseas continuar?

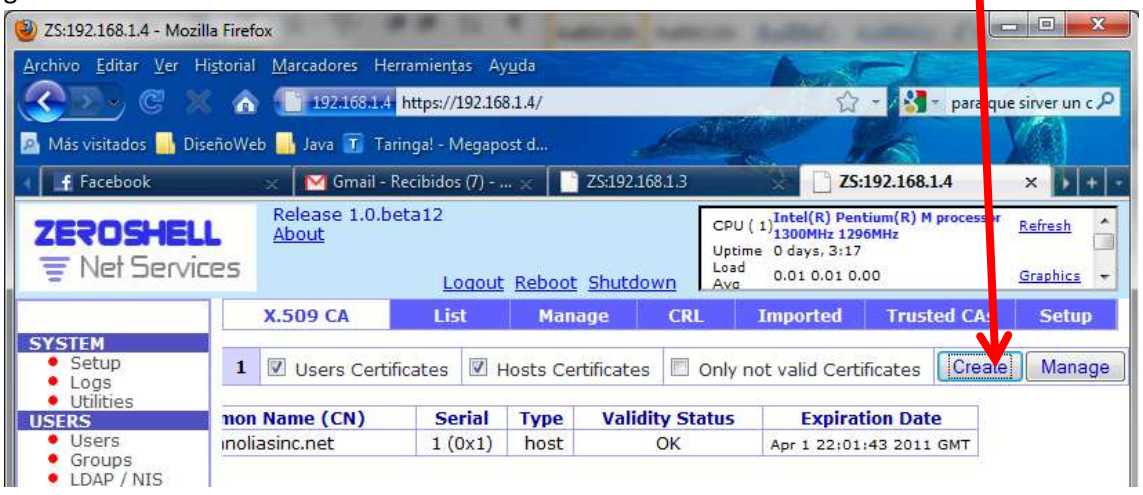


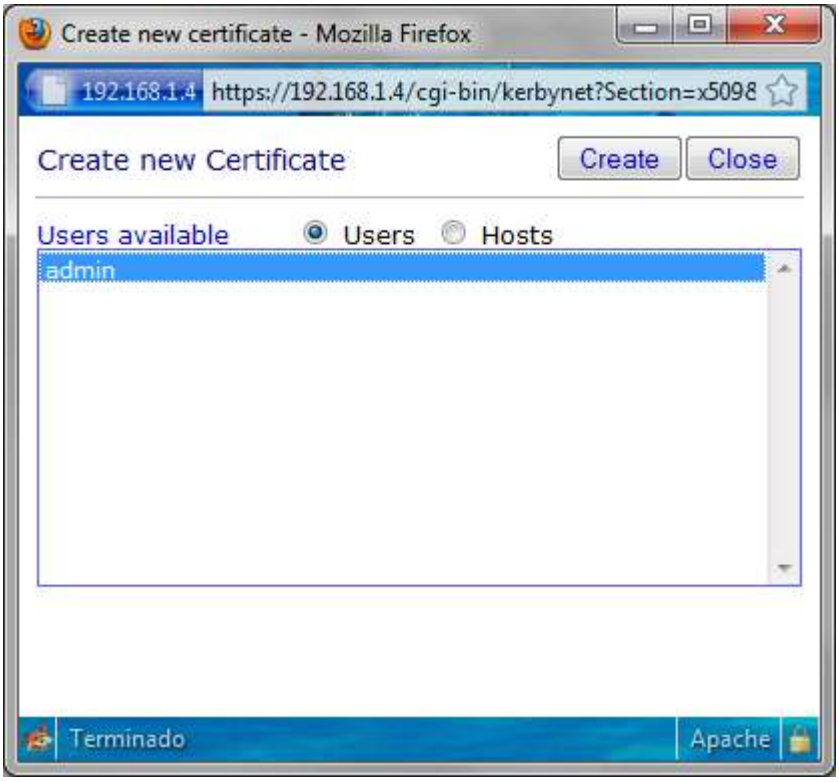
Hacemos clic sobre el botón “Aceptar”

Ahora nos haciendo clic en la pestaña con la leyenda “List” entramos a la lista para regenerar algunos certificados:

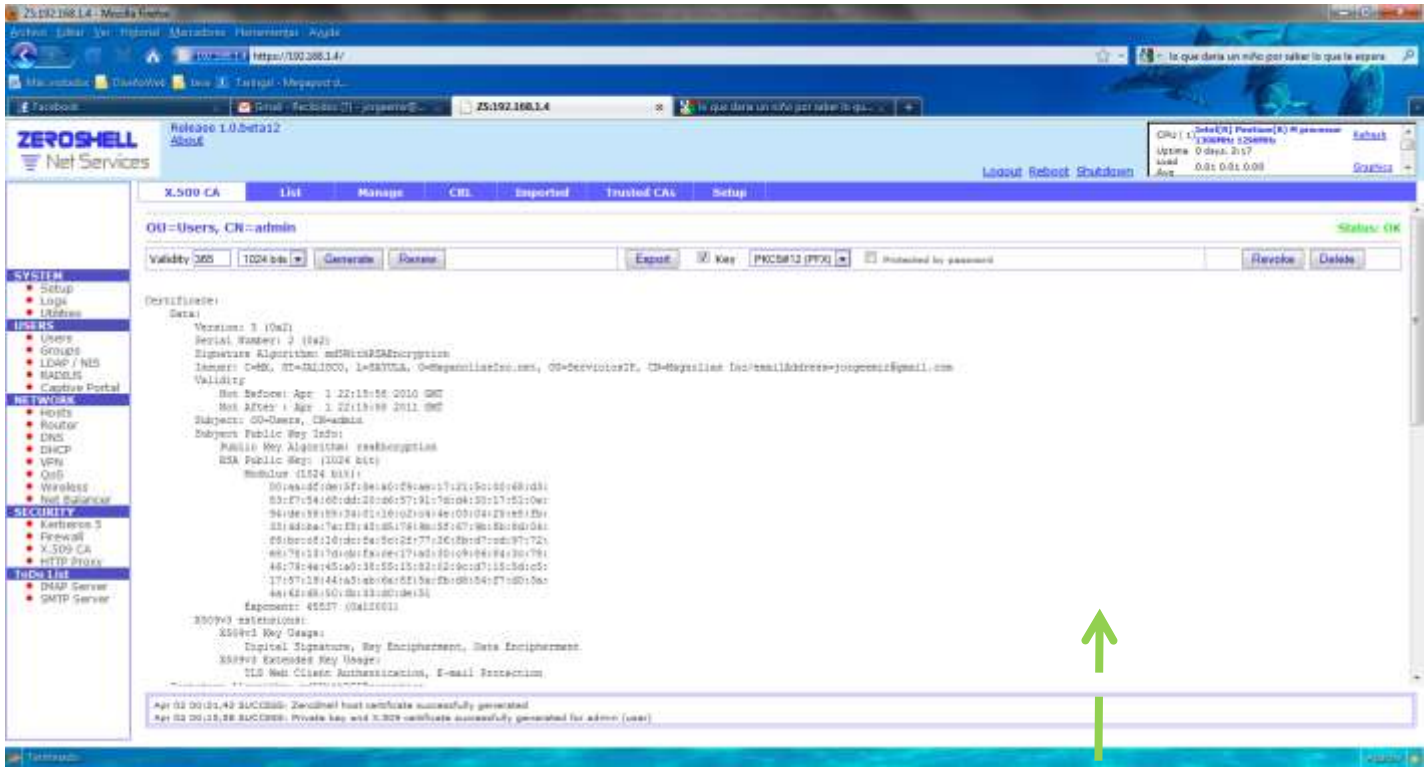


Una vez que estamos en el listado de certificados hacemos clic sobre el botón “Create” para generar el nuevo certificado al usuario “Admin”



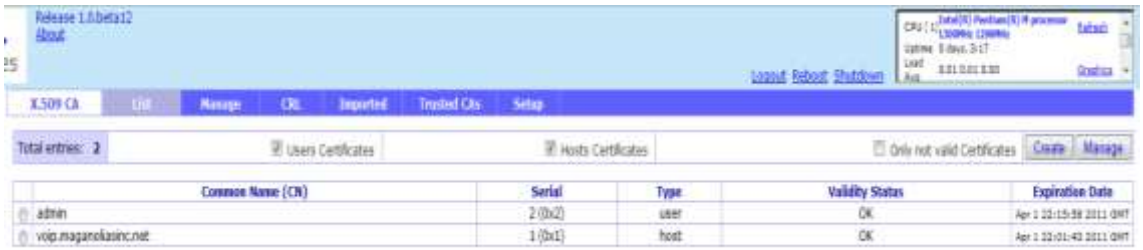


Seleccionamos el usuario al que deseamos crearle su nuevo certificado, que para nuestro caso es “admin”, y hacemos clic sobre el botón “Create”.



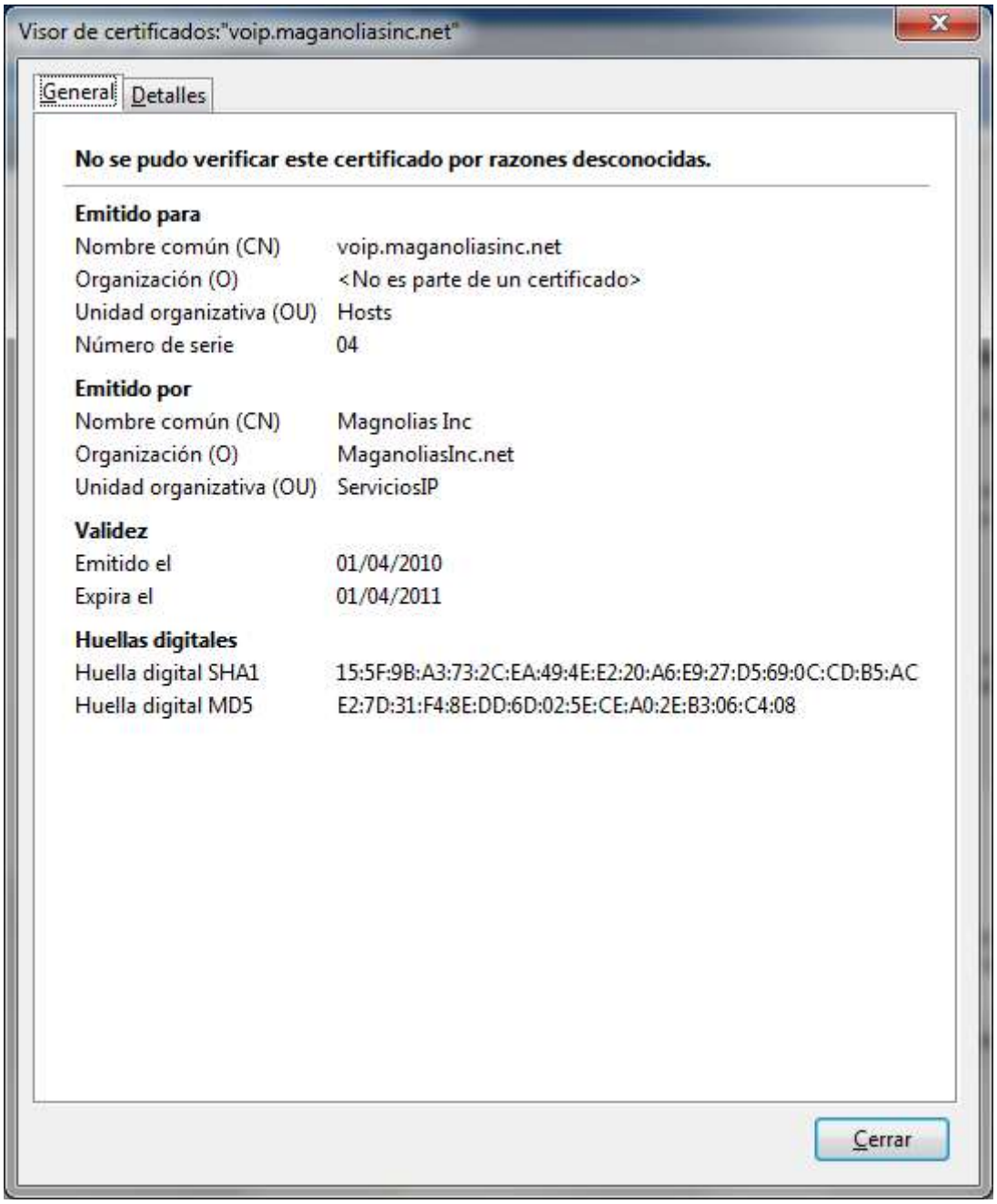
Si todo es correcto debemos de ver una pantalla similar a esta.

Si observamos nuevamente la lista de Certificados podremos ver que ahora ya también aparece el certificado para el usario admin con estatdo OK y valido. Lo que significa que hemos logrado con éxito la personalización de nuestro certificado.



Comprobando que el certificado ahora emite nuestra información:

Para este test puede ingresar desde otra maquina de la lan conectad a zeroshell y observar los datos del certificado:



Ahora si tenemos nuestro certificado personalizado con nuestros propios datos.

¿Cualquier duda o comentario?... jorgeemir@gmail.com

Con Amor y Cariño a mis padres.