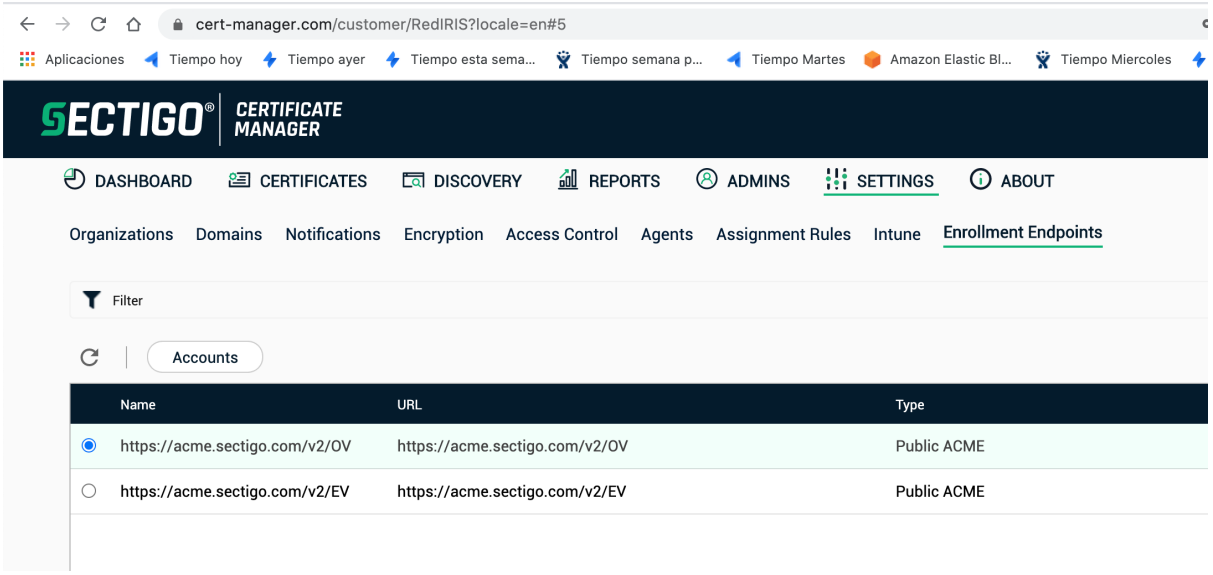
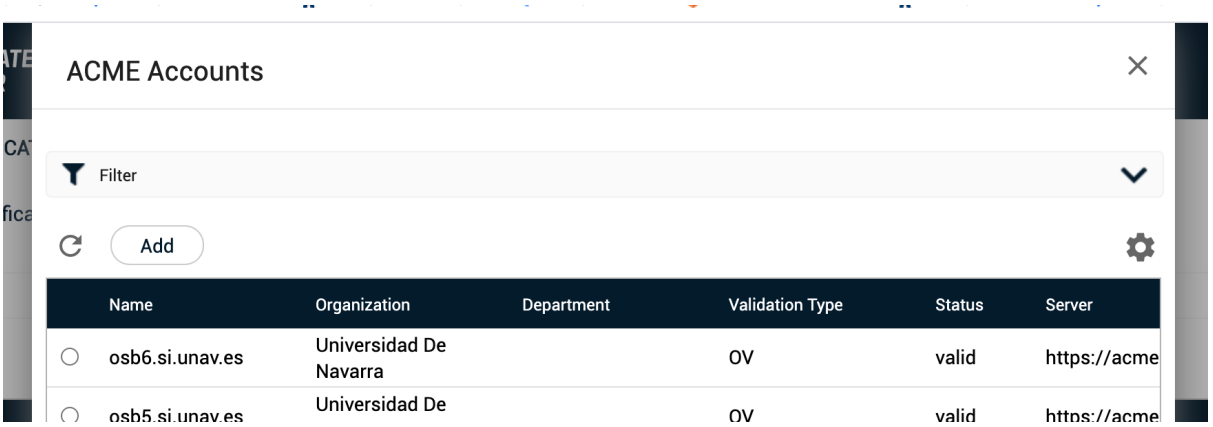
Crear una nueva cuenta ACME en el proveedor de certificados:

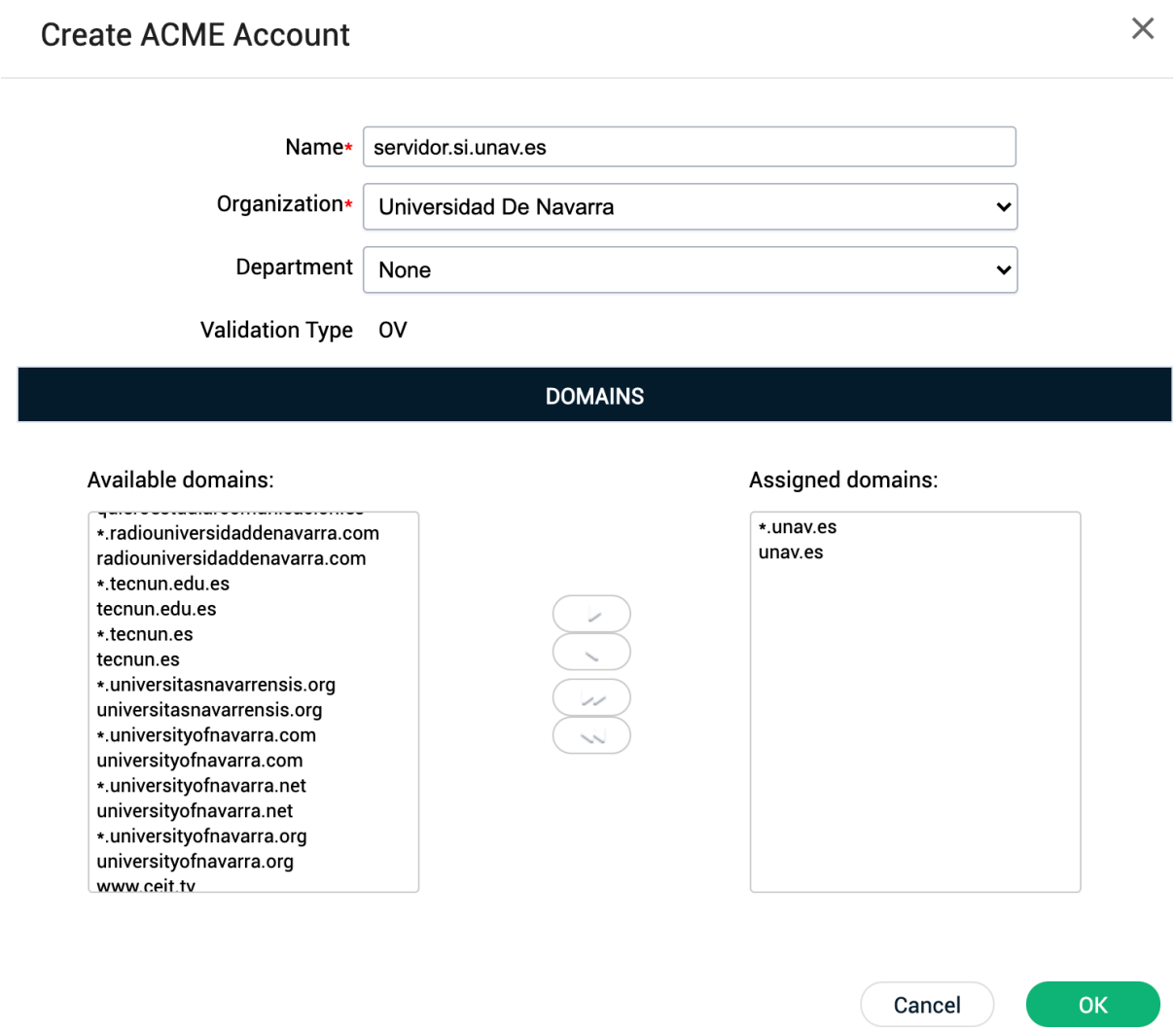
En el https://cert-manager.com/customer/RedIRIS acceder a settings, enrollment endpoints y elegir el OV: https://acme.sectigo.com/v2/OV, y pulsar en accounts:



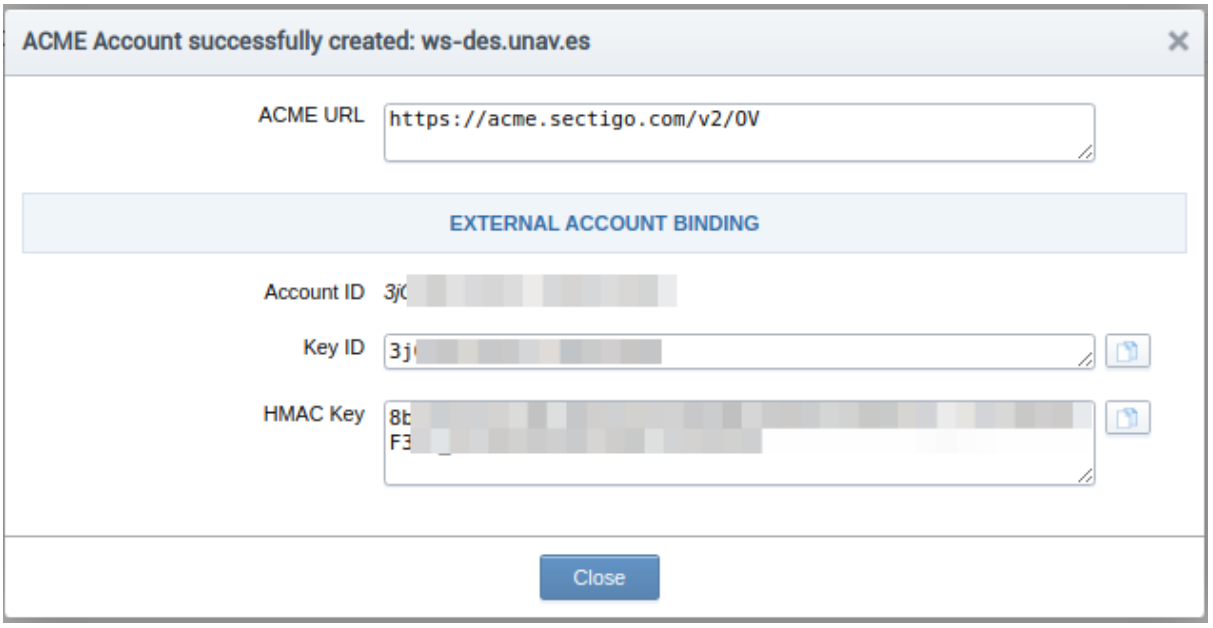
Añadir una nueva cuenta ACME:



En el nombre de la cuenta, poner el nombre del servidor que va a acceder, en ACME server elegir el de OV, y en los dominios elegir aquellos para los que se quiera que el servidor pida certificados;



Esto creará una cuenta externa, con un Key ID y un HMAC Key, que usaremos para configurar certbot en el cliente. Anotar estos valores, no se mostrarán más:



Lo correcto sería guardarlo en el gestor de contraseñas, creando dos entradas nuevas en el servidor, que se llamarán:

certbot eab-kid para el 'usuario'

certbot eab-hmac-key para la 'contraseña'

Configurar certbot en el servidor cliente:

La instalación dependerá del sistema operativo. Aquí pondremos los más habituales:

a. CentOS Linux release 7.7.1908 (Core)

Instalar el cliente

```
yum install certbot
```

Asegurarse de que hay conectividad directa (preferible) con acme.sectigo.com:443 y ocsp.sectigo.com puertos 80 y 443. Si es el segundo caso, hay que configurar el proxy temporalmente en el servidor con:

```
export https_proxy=http://proxy.unav.es:8080
export HTTPS_PROXY=http://proxy.unav.es:8080
export http_proxy=http://proxy.unav.es:8080
export HTTP_PROXY=http://proxy.unav.es:8080
```

Esta configuración de proxy se perderá al salir de la sesión, por lo que es muy recomendable ***solicitar que se abra la conexión directa***.

Registrar la cuenta que hemos creado anteriormente:

```
certbot register --email correodelcertmaster@institucion.es --server
https://acme.sectigo.com/v2/OV --eab-kid 3jXXXXXXXXXXXX --eab-hmac-key
8bXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

y seguir las instrucciones en pantalla:

```
certbot register --email correodelcertmaster@institucion.es --server
https://acme.sectigo.com/v2/OV --eab-kid SECRETO --eab-hmac-key SECRETO

Saving debug log to /var/log/letsencrypt/letsencrypt.log
Starting new HTTPS connection (1): acme.sectigo.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Please read the Terms of Service at
https://secure.trust-provider.com/repository/docs/Legacy/20181101_CertificatSubscriberAgreement_v_2_1_click.html.
You must agree in order to register with the ACME server at
https://acme.sectigo.com/v2/OV
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
(A)gree/(C)ancel: A
Resetting dropped connection: acme.sectigo.com
Starting new HTTPS connection (2): acme.sectigo.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the
```

```
web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
(Y)es/(N)o: N
IMPORTANT NOTES:
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
```

NOTA!! Problemas si el eab-kid y el eab-hmac-key comienzan por -

Hay workaround? NO PARECE SENCILLO. Si se ha generado una cuenta ACME que comience por -, intentar eliminarla y crear una nueva.

NOTA!! Error de python

Si al ejecutar el comando da el error pkg_resources.DistributionNotFound: acme>=1.8.0, hay que instalar

yum install python-acme

Solicitar un certificado sin instalación automática

Ahora ya podemos solicitar el certificado para el servidor, en nuestro ejemplo dominio.institucion.es:

```
certbot  certonly --standalone --non-interactive --agree-tos --email
correodelcertmaster@institucion.es --server https://acme.sectigo.com/v2/OV
--domain dominio.institucion.es

Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Starting new HTTPS connection (1): acme.sectigo.com
Obtaining a new certificate
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/dominio.institucion.es/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/ws-des.unav.es/privkey.pem
   Your cert will expire on 2021-09-23. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - If you like Certbot, please consider supporting our work by:
   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

En la solicitud ya no parece que sea necesario incluir el identificador y la password, de modo que se puede simplemente pedir así:

```
certbot  certonly --standalone --non-interactive --agree-tos --email
correodelcertmaster@institucion.es --server https://acme.sectigo.com/v2/OV
--domain dominio.institucion.es
```

Esto nos habrá dejado en la ruta indicada todos los certificados que necesitamos para configurar en nuestro servicio:

```
[root@servidors ~]# cd /etc/letsencrypt/live/dominio.institucion.es/
[root@servidor dominio.institucion.es]# ll
total 4
lrwxrwxrwx 1 root root  38 sep 23 11:54 cert.pem ->
../../archive/dominio.institucion.es/cert1.pem
lrwxrwxrwx 1 root root  39 sep 23 11:54 chain.pem ->
../../archive/dominio.institucion.es/chain1.pem
lrwxrwxrwx 1 root root  43 sep 23 11:54 fullchain.pem ->
../../archive/dominio.institucion.es/fullchain1.pem
lrwxrwxrwx 1 root root  41 sep 23 11:54 privkey.pem ->
../../archive/dominio.institucion.es/privkey1.pem
-rw-r--r-- 1 root root 692 sep 23 11:54 README
```

Estos ficheros contienen:

	cert.pem	chain.pem	fullchain.pem	privkey.pem
Certificado del servidor solicitado Firmado por Sectigo RSA Organization Validation Secure Server CA	✔️		✔️	
Certificado de Sectigo RSA Organization Validation Secure Server CA Firmado por USERTrust RSA Certification Authority		✔️	✔️	
Certificado de USERTrust RSA Certification Authority		✔️	✔️	

Firmado por AAA Certificate Services				
Clave privada				✔

Con estos ficheros ahora podremos hacer las tareas que necesitemos para que nuestro servicio recoja este nuevo certificado y lo utilice: Como por ejemplo convertirlo de pem a pkcs12, importarlo en un jdk, y hacer que un weblogic utilice ese JDK.

Para renovar este certificado, habrá que hacer un script que haga las tareas anteriores, y además reinicie el servicio (apache instalado por nosotros, tomcat, weblogic, etc...)

```
certbot renew --deploy-hook /path/to/deploy-hook-script
```

Por ejemplo, en el caso de un servidor, donde el certificado debe usarse para un apache y un weblogic, se ha configurado el apache para que use los certificados que deja certbot directamente en la carpeta /etc/letsencrypt/live/SERVIDOR, se ha configurado el weblogic para que use el KEYSTORE indicado, con el alias y la password indicadas, y para rehacer ese keystore y reinicar el weblogic y el apache se ha usado el siguiente script:

```
#/bin/bash
KEYSTORE="/u01/app/oracle/osb/osbdomain/osbdomain/keystore.jks"
KEYTOOL="/u01/app/oracle/osb/software/jdk/latest/bin/keytool"
CERTNAME="dominio.institucion.es"
cd /etc/letsencrypt/live/$CERTNAME/
cat cert.pem chain.pem > certchain.pem
ALIAS=`pwd | sed 's/^.*\///'`
/usr/bin/openssl pkcs12 -export -inkey privkey.pem  -in certchain.pem -out
certchain.p12 -name $ALIAS -password pass:password
FECHA=`date +%y%m%d-%H%M%S`
mv $KEYSTORE $KEYSTORE-$FECHA
$KEYTOOL -importkeystore -deststorepass password -destkeypass password
-destkeystore $KEYSTORE -srckeystore certchain.p12 -srcstoretype PKCS12
-srcstorepass password -alias $ALIAS
$KEYTOOL -import -trustcacerts -keystore $KEYSTORE -file root.pem -alias
sectigoroot -deststorepass password
$KEYTOOL -import -trustcacerts -keystore $KEYSTORE -file int.pem -alias
sectigoint -deststorepass password
/usr/sbin/service osb stop
/usr/sbin/service osb start
/usr/sbin/service httpd stop
/usr/sbin/service httpd start
```

Solicitar un certificado con instalación automática

Apache

Si tenemos un apache instalado ‘de caja’ (con yum install httpd), podemos correr los siguientes comandos para que certbot genere el certificado y autoconfigure y recargue el apache para usar los nuevos certificados:

```
yum install python2-certbot-apache
```

```
certbot --apache --agree-tos --email correodelcertmaster@institucion.es
--server https://acme.sectigo.com/v2/OV --eab-kid SECRETO --eab-hmac-key
SECRETO --domain dominio.institucion.es
```

Configurar la autorenovación del certificado.

Si queremos que el certificado se renueve todos los días, introducir la siguiente linea en el crontab. Esto sólo lo haremos para comprobar que el proceso funciona correctamente, y apache muestra el certificado correcto:

```
0 7 * * 1-5 certbot renew --force-renewal -q
```

Ojo: Cuando se lanza desde crontab, certbot introduce un retardo aleatorio antes de procesar el comando, de modo que al hacer la prueba es probable que se piense que 'se ha colgado', o 'no funciona'. En /var/log/letsencrypt/letsencrypt.log se ve el timeout que ha metido:

2020-09-24 09:08:02,737:INFO:certbot._internal.renewal:Non-interactive renewal: random delay of 463.468800978 seconds

Si queremos que el certificado se renueve cuando vaya a caducar (comportamiento deseado)

```
0 7 * * 1-5 certbot renew -q
```

(Visto en https://certbot.eff.org/docs/using.html#renewing-certificates: This command attempts to renew any previously-obtained certificates that expire in less than **30** days)

Configurar backup

Asegurarse de que se hace backup de la carpeta /etc/letsencrypt.

Cambiar monitorización

Para saber qué certificados han sido generados con certbot y por tanto están automatizados, deberíamos cambiar el nombre del checkeo en nagios para que incluya ‘certbot’ en su descripción para permitir una rápida idenficación de todos los servidores automatizados.