Configuración de bind para el acceso a los servicios de la Red SARA

Este documento pretende ser una fuente de ejemplos de cómo configurar un servidor DNS bind para el acceso a los servicios de la Red SARA a través de IRIS-SARA. En ningún caso, este documento contendrá todos los dominios necesarios para el acceso a un servicio concreto; esta información está disponible en el wiki del servicio IRIS-SARA (http://wiki.rediris.es/iris-sara).

Antes de los ejemplos de configuración, se explica la necesidad de realizar estas modificaciones. Para cualquier duda, está disponible el buzón de atención de incidencias de IRIS-SARA (incidencias.redsara@rediris.es) y el correo de los autores de este documento.

1.- Sobre IRIS-SARA

El servicio IRIS-SARA (http://www.rediris.es/iris-sara/) ofrece acceso a la Red SARA, y a los servicios disponibles en ella, para las Universidades españolas. El caso típico es el de una Universidad que desea validar certificados electrónicos con @firma; que su servicio de Administración quiera acceder al Portal del Funcionario, o que el personal de la Universidad quiera acceder al PAE (Portal de Administración Electrónica, antiguo CTT).

Para que este caso típico se implemente, una Universidad seguirá los siguientes pasos:

- Darse de alta en IRIS-SARA una única vez, firmando las Condiciones de Uso y asumiendo las responsabilidades derivadas de su firma
- El solicitante del servicio deberá asegurarse de que, en sus accesos vía SIR (http://www.rediris.es/sir), su identificación incluye el atributo 'ePE' con el valor 'urn:mace:rediris.es:entitlement:sara:req';
- Por cada servicio al que quiera acceder (@firma, Portal del Funcionario, PAE, …) deberá rellenar el formulario de alta de servicios de la Red SARA (http://www.rediris.es/iris-sara/priv/SIR/alta_sara.php), donde incluirá:
  - El nombre del servicio al que quiere solicitar acceso
  - En caso de ser necesario, un documento justificativo de que el prestador del servicio final habilita el acceso de la Universidad
  - Las direcciones IP públicas de la Universidad desde las que se accederá al servicio
  - Las direcciones IP públicas de los servidores DNS que resolverán los hosts donde se presta el servicio solicitado
  - Una vez que RedIRIS habilite estas IPs la Universidad deberá incluir, en los servidores DNS declarados en este formulario, los hosts asociados al servicio solicitado

La necesidad de modificar los servidores DNS responde a los siguientes condicionantes:

- Gran parte de los hosts asociados a los servicios de la Red SARA no existen en los DNS públicos; por lo tanto, deben definirse explícitamente para que resuelvan frente a un servidor DNS que sí conoce estos hosts. Por ejemplo, el host afirma.redsara.es

no existe en la zona pública de redsara.es; sin embargo, si la consulta se realiza frente al DNS 130.206.180.9, resuelve con la IP 130.206.180.11

- No hay un dominio específico que incluya todos los hosts de servicios de la Red SARA. Algunos se prestan bajo el dominio map.es, otros bajo redsara.es, etc.
- En algunos casos, la Universidad querrá resolver algunos hosts a través del DNS para IRIS-SARA y otros a través del DNS público. Por ejemplo, el host informes.map.es resuelve en el DNS de IRIS-SARA con la IP 130.206.180.16, pero no resuelve el host www.map.es; en cambio, el DNS público resuelve www.map.es con las IP 82.150.0.13 y 213.9.211.13, pero el DNS de IRIS-SARA no conoce este host. Esto se ha resuelto, como se verá más adelante, definiendo zonas de un único host.
- Finalmente, hay servicios disponibles a través de IRIS-SARA que también permiten el acceso público, por ejemplo http://administracionelectronica.gob.es. Este host resuelve, en un DNS público, a la IP 213.27.145.16; y en el de IRIS-SARA, a la IP 130.206.180.20. El acceso vía Red SARA ofrece más información que el acceso público, por lo que una institución podría querer que una parte de sus usuarios accedan vía Internet y otra parte vía Red SARA.

Para dar solución a estos condicionantes, se ofrece a las universidades un DNS primario con IP 130.206.180.9, donde se definirán todos (y únicamente) los hosts de servicios de la Red SARA con direccionamiento público de RedIRIS (dentro del rango 130.206.180.0/23).

2.- Configuración básica.

Con las siguientes líneas, que incluimos en *named.conf* nuestro DNS podrá resolver las preguntas que se le hagan para esas zonas en cuestión.

Nota 1: Estas configuraciones son un ejemplo de cómo se pueden implementar las zonas para los servicios de la Red SARA en bind; no son un desglose completo de todos las zonas necesarias. Esta información está disponible en http://wiki.rediris.es/iris-sara.

Nota 2: Las zonas se pueden definir como slave o forward indistintamente; la decisión de usar un tipo u otro corresponde a la Universidad según sus preferencias.Los ejemplos siguientes son una muestra de cómo se podría configurar de una u otra forma

```
// Red Sara-RedIris
zone "redinteradministrativa.es" {
      type forward;
      forwarders {130.206.180.9; };
};
zone "informes.map.es" {
       type slave;
       file "db.informes.map.es";
       masters {
            130.206.180.9;
      };
};
zone "funciona.es" {
      type forward;
      forwarders {130.206.180.9; };
};
zone "administracionelectronica.gob.es" {
      type forward;
      forwarders {130.206.180.9; };
};
```

3.- Información complementaria.

Existen un par de características, que pueden resultar útiles a la hora de sincronizar con el servidor de nombres primario:

1. Si nuestro DNS se encuentra en una máquina con múltiples IP y queremos forzar que la sincronización con esas zonas sea por una IP en concreto, podremos incluir en la configuración de cada zona esta línea (dentro de *options* o de *view*): *transfer-source mi.ip port 53;* Esta opción normalmente no se usará dado que ya estamos comunicando a RedIris cuál será la IP de nuestro DNS, a parte, se recomienda no usarla si no se conoce realmente a qué afecta en nuestro DNS en producción.

2. Dichas zonas únicamente deberían ser visibles desde la red interna de cada universidad, para ello podemos crear una vista dentro de la configuración de nuestro DNS, a fin de indicarle que cuando las *querys* vengan desde nuestra red, resuelva las zonas de la Red SARA, y si las *querys* vienen desde fuera, no resuelva dichas zonas.

   Aquí vemos un ejemplo de configuración para la red de la Universitat Jaume I (*150.128.0.0/16*):

```
view "ujinet" {
      match-clients { 127.0.0.1; 150.128.0.0/16; };

      zone "." {
            type hint;
            file "db.cache";
      };

      zone "localhost" {
            type master;
            file "db.localhost";
      }; iep

      zone "0.0.127.IN-ADDR.ARPA" {
            type master;
            file "db.127.0.0";
      };

      zone "uji.es" {
            type master;
            file "db.uji";
      };

      // Red Sara-RedIris
      zone "redinteradministrativa.es" {
            type forward;
            forwarders {130.206.180.9; };
      };

      zone "informes.map.es" {
            type forward;
            forwarders {130.206.180.9; };
      };

      zone "funciona.es" {
            type forward;
            forwarders {130.206.180.9; };
     };

      zone "administracionelectronica.gob.es" {
            type forward;
            forwarders {130.206.180.9; };
     };

};
```