Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Autentificación de un cliente linux a través de LDAP (57773 lectures)

Per **Jesús Roncero Franco**, ***golan*** (http://www.roncero.org)

Creado el 13/06/2002 02:17 modificado el 13/06/2002 02:17

Con este artículo veremos cómo configurar un cliente linux para que se autentifique a partir de un directorio LDAP en vez de usar los ficheros locales. Esto nos puede permitir tener un número de ordenadores que se autentifiquen contra una base de usuarios centralizada.

Tal como vimos en el artículo sobre la creación de un directorio LDAP[1], en este veremos cómo hacer que un cliente linux se autentifique usando el LDAP, es decir, no usará /etc/passwd para validar a los usuarios.

Configuración Básica

Supondremos en este paso que tenemos un servidor LDAP que está funcionando y que tiene los datos de los usuarios, logins, claves, etc. Este servidor puede estar funcionando en modo seguro SSL, pero, para esta parte, no nos hace falta.

La configuración en este caso es sencilla, tendremos que modificar dos ficheros del sistema.
El primero de ellos es el fichero **/etc/ldap.conf**. Este fichero sirve para indicar los parámetros globales del sistema para utilizar el servidor LDAP como cliente.
En él indicaremos el servidor ldap y sobre qué parte del directorio nos vamos a autentificar. básicamente debemos añadir esto:

```
host bulma.net
base dc=bulmalug,dc=net
```

siendo **host** la dirección de la máquina, y **base** el nombre distinguido que usaremos para la localizar la base de datos de los usuarios.
En el fichero **/etc/nsswitch.conf** vamos a indicar cómo queremos que se autentifique el linux. Para ello lo editamos y y colocamos estos tres parámetros así:

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
```

De esta forma le estamos indicando el orden que debe utilizar linux para hacer la autentificación. Primero que mire en los ficheros locales, segundo en el directorio ldap. La manera recomendable es hacerlo así. Se tiene en los ficheros locales el usuario root exclusivamente, y el resto en el directorio, de manera que el usuario root tiene siempre acceso y el resto, serán autentificados a través del LDAP. No es recomendable tener el usuario root en el servidor LDAP o invertir el orden de la autentificación, ya que, en el caso de un fallo del servidor ldap, nos podemos quedar sin poder acceder a la máquina.

NOTA Es conveniente probar la autentificación teniendo varias consolas de root abiertas para que en caso de fallo no haya problemas para entrar en la máquina y poder modificar estos ficheros. Ten en cuenta que, al estar modificando el proceso de autentificación, cualquier fallo en la configuración te puede dejar sin acceso a la máquina, teniendo que arrancar desde disquetes. ¡Quedas advertido! ;-)

Básicamente es esto lo único que se necesita hacer para que la autentificación se lleve a cabo a través del LDAP, en modo no seguro.
Conviene indicar también que los usuarios de redhat tienen disponible una herramienta llamada *authconfig* que hace todo esto, es decir, modificar estos ficheros.

Y, por supuesto, haced man nsswitch.conf y man ldap.conf para ver todas las opciones.

Configuración en modo seguro SSL

Una vez que ya tenemos configurado el sistema, añadir el modo seguro es relativamente fácil, partiendo de que tenemos soporte OpenSSL.

En el fichero **/etc/ldap.conf** añadiremos estas entradas:

```
port 636
ssl yes
sslpath /usr/local/ssl/certs
```

Indicandole que queremos usar ssl, el puerto del ssl y el directorio dónde se encuentran los certificados.
Para instalar los certificados usaremos un pequeño truco ;-)

Utilizaremos Netscape 4.5, e intentaremos acceder a la dirección dónde tengamos el servidor pero a través de su puerto seguro, es decir, https://bulma.net:636/ . Ojo con el **https**. De esta forma, el netscape creerá que se está conectado a un servidor web seguro e iniciará el proceso de aceptación del certificado. Deberemos decirle que confiamos en el certificado y que queremos aceptarlo para esta y sucesivas sesiones. Una vez hecho esto, al darle a terminar, el netscape nos informará de que se ha producido un error ya que, al no ser un servidor web en ese puerto, no se recibirán datos. Pero por otro lado, habremos aceptado el certificado en un fichero dentro del directorio de netscape, que es lo que queremos usar.
Bien, este fichero es **cert7.db** que se encuentra en **$HOME/.netscape** y hay que colocarlo en **/usr/local/ssl/certs**

Una vez hecho este paso, ya está preparado el sistema para usar los certificados y autentificarse a través del OpenLDAP en modo seguro.

Para terminar

Por último, señalar que esto sólo realiza la autentificación. Otra cosa de la que debereis aseguraros, según la configuración que tengais, es realizar el montaje de los directorios de los usuarios, dónde teneis varias opciones, como NFS o samba. Pero eso ya os lo dejo como ejercicio ;-).

Un agradecimiento especial a José Moguer Maestre, mi compañero en las prácticas en empresa dónde investigamos a fondo sobre OpenLDAP.

Jesús Roncero.

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=1343

E-mail del autor: jesus _ARROBA_ roncero.org
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1371