Administración dos usuarios do dominio con LDAP e kerberos

Implicacións do uso de kerberos no mantemento dos usuarios do dominio

Implantar o servidor de kerberos no dominio implica unha maior complexidade na administración dos usuarios do dominio, xa que cada usuario que deamos de alta no dominio, teremos que dalo de alta tamén como un *principal* en kerberos. Cando damos de alta o usuario como *principal*, engádenselle ao usuario no LDAP unha serie de valores para os atributos propios do esquema de kerberos, entre os que se atopan o nome do *principal* no atributo *krbPrincipalName* (*usuario@reino*, por exemplo *xan@IESCALQUERA.LOCAL*) e o contrasinal do usuario de kerberos *krbPrincipalKey*.

Desta forma, cada vez que engadimos, editamos (sobre todo se cambiamos o contrasinal) ou borramos un usuario deberíamos lembrarnos de facer a operación correspondente no *principal* de kerberos, usando o comando *kadmin* ou *kadmin.local*.

Para non ter que facer estes procesos de forma manual, imos ver como configurar a ferramenta de *Usuarios e grupos LDAP* do webmin para que realice estas funcións de forma automática.

Configuración do webmin para a administración dos usuarios do LDAP con kerberos

O módulo de *Usuarios e grupos LDAP* do webmin permite introducir scripts para sexan executados antes ou despois da creación, modificación ou borrado de usuarios ou de grupos. Estes scripts teñen acceso a través dunhas variables de contorno ao tipo de acción que desencadeou o script e aos datos do usuario ou grupo modificado (Máis información en http://doxfer.com/Webmin/UsersAndGroups#Configuring_the_Users_and_Groups).

No noso caso precisamos un script que cando se cree un novo usuario cree o correspondente principal de kerberos, se se modifica un usuario actualice o seu contrasinal e se se elimina un usuario elimine o principal de kerberos.

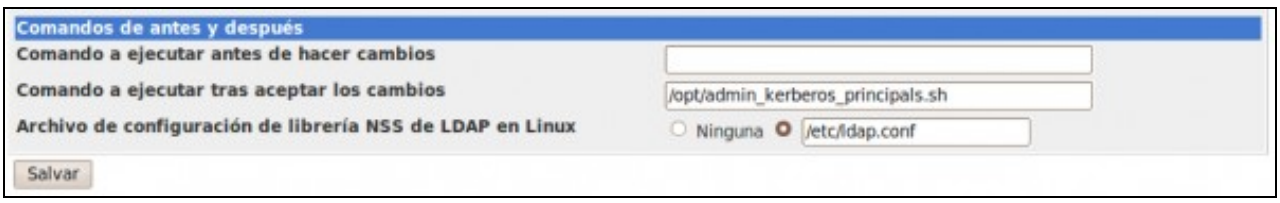
Pois ben, tendo en conta os parámetros que recibe o script podería ter o seguinte contido:

```
#!/bin/bash
case "$USERADMIN_ACTION" in
"CREATE_USER") kadmin.local -q "addprinc -x dn=uid=$USERADMIN_USER,ou=usuarios,dc=iescalquera,dc=local -pw $USERADMIN_PASS $USERADMI
"MODIFY_USER") kadmin.local -q "cpw -pw $USERADMIN_PASS $USERADMIN_USER";;
"DELETE_USER") kadmin.local -q "delprinc -force $USERADMIN_USER";;
esac
```

Almacenamos o script no ficheiro */opt/admin_kerberos_principals.sh* e lle damos permisos de execución co comando:

```
sudo chmod 755 /opt/admin_kerberos_principals.sh
```

Picamos no enlace de **Configuración de módulo** na páxina principal do módulo de *Usuarios e grupos LDAP* e introducimos a ruta ao script no parámetro de **Comando a ejecutar tras aceptar los cambios** que atopamos na sección de **Comandos de antes y despues** na parte inferior da páxina. Picamos no botón de **Salvar** para almacenar este parámetro:



-- Antonio de Andrés Lema e Carlos Carrión Álvarez