

# 1 Configuración do cliente kerberos

## 1.1 Sumario

- 1 Sincronización da hora no equipo cliente
- 2 Instalación e configuración do cliente kerberos
- 3 Configuración do sistema de autenticación para que utilice kerberos
- 4 Cambiar o contrasinal dun usuario

## 1.2 Sincronización da hora no equipo cliente

Como xa comentamos no apartado anterior, cando usamos kerberos é moi importante que as horas do equipo cliente e a do equipo servidor estean sincronizadas, polo que imos sincronizar a hora do cliente por NTP igual que o fixemos no servidor, usando o comando **ntpdate**. Por exemplo:

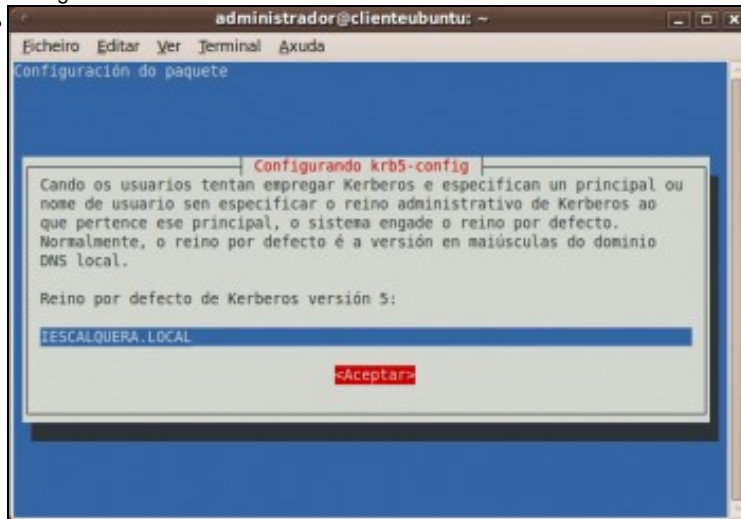
```
sudo ntpdate es.pool.ntp.org
```

## 1.3 Instalación e configuración do cliente kerberos

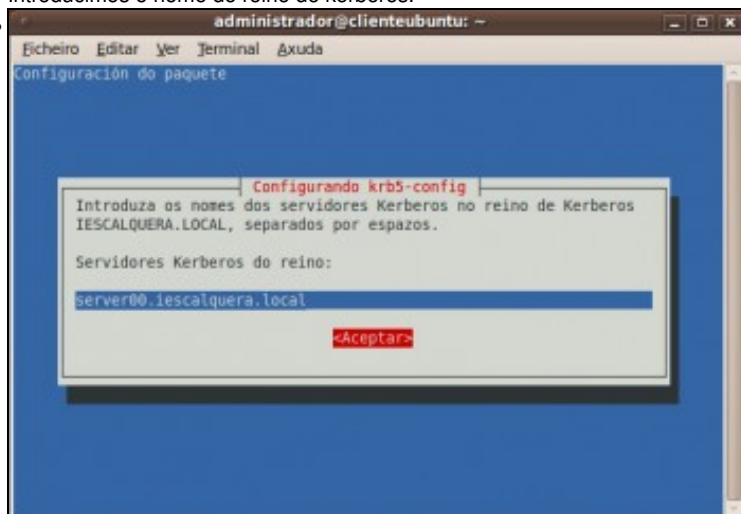
- Instalaremos os paquetes necesarios para o cliente kerberos:

```
sudo apt-get install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

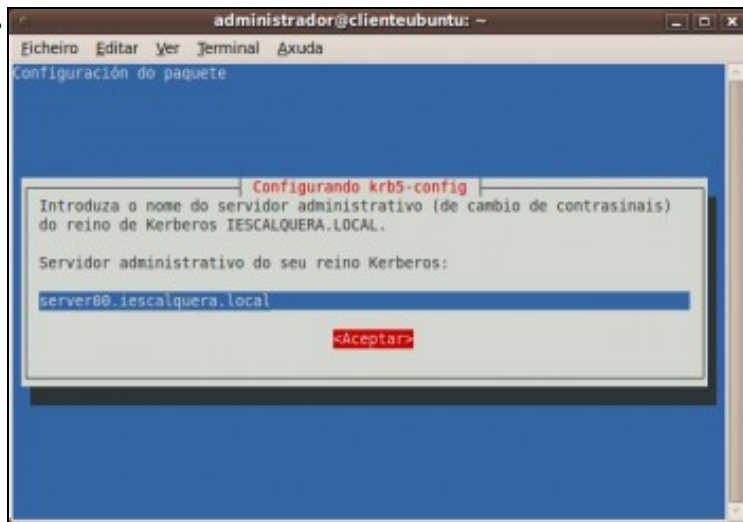
- Configuración do reino no cliente kerberos



Introducimos o nome do reino de kerberos.



Introducimos o nome de DNS do servidor como servidor do reino.



Poñemos o mesmo como servidor administrativo.

- Se se comete algún erro na información introducida nestas pantallas, pódese introducir de novo co comando:

```
sudo dpkg-reconfigure krb5-config
```

- Podemos usar o comando *kinit* para un ticket de kerberos para o usuario *xan* (Teremos que introducir o seu contrasinal de kerberos, que é **abc123**):

```
kinit xan@IESCALQUERA.LOCAL
Password for xan@IESCALQUERA.LOCAL:
```

- Comprobamos co comando *klist* que o servidor kerberos enviou o ticket solicitado:

```
klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: xan@IESCALQUERA.LOCAL
Valid starting    Expires          Service principal
03/15/10 11:15:51  03/16/10 11:15:51  krbtgt/IESCALQUERA.LOCAL@IESCALQUERA.LOCAL
    renew until 03/15/10 11:15:51
```

## 1.4 Configuración do sistema de autenticación para que utilice kerberos

Para configurar os métodos autenticación nun sistema Linux, hai dous aspectos importantes que debemos configurar correctamente:

- O ficheiro */etc/nsswitch.conf*: Este ficheiro permítenos configurar que servizos utilizará o sistema para obter os usuarios, grupos, contrasinais, nomes de outros equipos, etc.
- O sistema **PAM** (*Pluggable Authentication Modules*): Mediante as librerías de PAM, podemos establecer tamén as accións que se realizarán en distintas situacións: cando o usuario se autentica, cando abre sesión, cando abre unha sesión non interactiva, cando cambia o contrasinal, etc.

Os ficheiros de configuración de PAM almacénanse na carpeta */etc/pam.d*, e aí atoparemos un ficheiro por cada servizo que se pode requirir e nel especificanse as tarefas a realizar para ese servizo. Os servizos máis importante son *common-account*, *common-auth*, *common-session* e *common-password*, xa que son os que habitualmente teremos que modificar para a autenticación por LDAP, para usar kerberos, etc.

O problema é que a configuración destes ficheiros é bastante delicada (téñase en conta que unha configuración incorrecta pode facer que os usuarios xa non se poidan autenticar e será difícil de recuperar), e por iso cada vez é máis frecuente que as distribucións ofrezan programas que automatizan a actualización destes ficheiros cos parámetros correctos segundo a situación (autenticar contra un servidor LDAP, uso de kerberos, etc.)

No caso de Ubuntu, dispoñemos da ferramenta **auth-client-config** que nos permite configurar facilmente tanto NSS (o ficheiro *nsswitch.conf*) como PAM. Esta ferramenta recibe como parámetro un ficheiro de perfil, no que están almacenados todos os cambios que debe facer para configurar correctamente NSS e PAM. Para o uso de LDAP e kerberos non trae por defecto ningún perfil, así que teremos que crear nós este ficheiro de perfil.

Creemos o ficheiro `/etc/auth-client-config/profile.d/krb-auth-config` co seguinte contido:

```
[krb5ldap]
nss_passwd=passwd: files ldap
nss_group=group: files ldap
nss_shadow=shadow: files ldap
nss_netgroup=netgroup: files ldap
pam_auth=auth          sufficient pam_krb5.so
                auth          required pam_unix.so nullok_secure use_first_pass
pam_account=account    sufficient pam_krb5.so
                account        required pam_unix.so
pam_password=password  requisite pam_krb5.so minimum_uid=10000
                password      [success=2 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512
                password      [success=1 user_unknown=ignore default=die] pam_ldap.so use_authtok try_first_pass
                password      requisite pam_deny.so
pam_session=session    required pam_unix.so
                session        optional pam_mkhomedir.so skel=/etc/skel/
                session        optional pam_krb5.so
                session        optional pam_foreground.so

[krb5ldap.cached]
nss_passwd=passwd: files ldap [NOTFOUND=return] db
nss_group=group: files ldap [NOTFOUND=return] db
nss_shadow=shadow: files ldap
nss_netgroup=netgroup: files ldap
pam_auth=auth          required pam_env.so
                auth          sufficient pam_unix.so likeauth nullok
                auth          [default=ignore success=1 service_err=reset] pam_krb5.so use_first_pass
                auth          [default=die success=done] pam_ccreds.so action=validate use_first_pass
                auth          sufficient pam_ccreds.so action=store use_first_pass
                auth          required pam_deny.so
pam_account=account    sufficient pam_krb5.so
                account        required pam_unix.so
pam_password=password  requisite pam_krb5.so minimum_uid=10000
                password      [success=2 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512
                password      [success=1 user_unknown=ignore default=die] pam_ldap.so use_authtok try_first_pass
                password      requisite pam_deny.so
pam_session=session    required pam_unix.so
                session        optional pam_mkhomedir.so skel=/etc/skel/
                session        optional pam_krb5.so
                session        optional pam_foreground.so
```

Executamos o comando *auth-client-config* indicándolle que cargue o perfil de kerberos e LDAP:

```
sudo auth-client-config -a -p krb5ldap
```

Feito!! Podemos probar a iniciar sesión con un usuario do dominio que tamén sexa un *principal* en kerberos e comprobar co comando *klist* que o ticket de kerberos foi solicitado automaticamente.

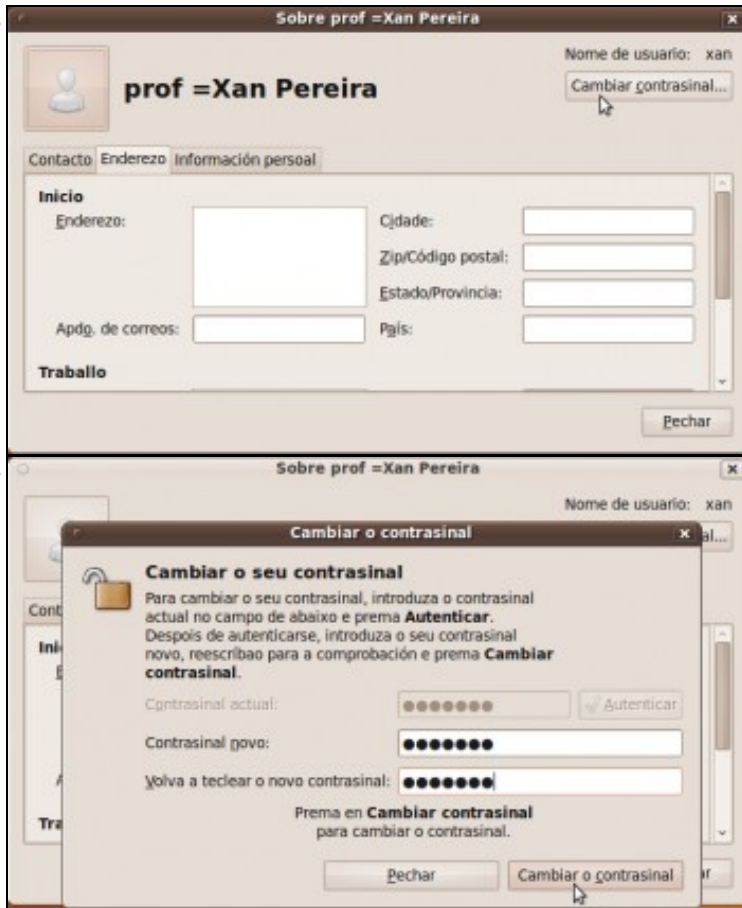
## 1.5 Cambiar o contrasinal dun usuario

Outro efecto da configuración que acabamos de cargar para a autenticación por kerberos é que se un usuario cambia o seu contrasinal cambiarase automaticamente o seu contrasinal de LDAP e de kerberos. Hai que ter en conta que, aínda que kerberos usa o LDAP para obter os contrasinais dos usuarios, non se usa o mesmo atributo para almacenar o contrasinal de kerberos (atributo *krbPrincipalName*) que o contrasinal do usuario Linux (*UserPassword*), así que no noso dominio será importante ter estes dous contrasinais sempre sincronizados, para que a autenticación de kerberos non falle.

O usuario ten varias alternativas para cambiar o seu contrasinal:

- Usando o comando **passwd**: Este comando cambia o contrasinal do usuario en LDAP e kerberos.
- Usando a aplicación gráfica de Ubuntu (No menú **Sistema->Preferencias->Sobre min**): Se o usuario cambia o contrasinal con esta ferramenta, tamén serán actualizados os dous contrasinais:

- Cambio de contraseña de usuario LDAP



-- Antonio de Andrés Lema e Carlos Carrión Álvarez