

# Configuración do cliente kerberos

## 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

## 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:

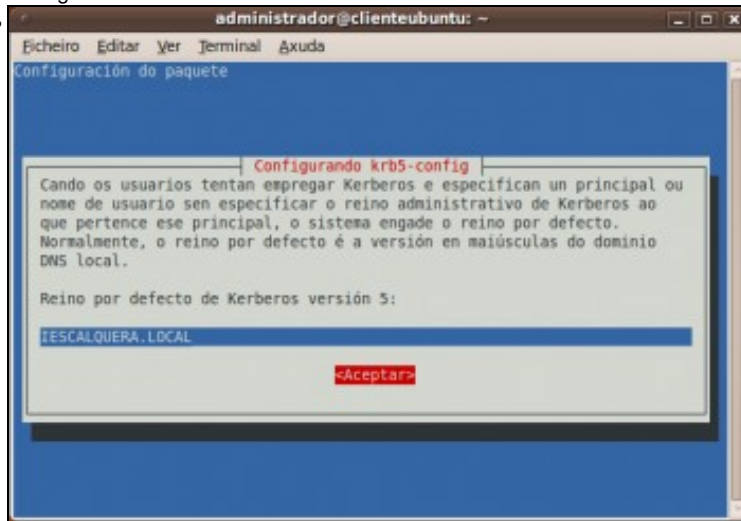
```
sudo ntpdate es.pool.ntp.org
```

## Instalación e configuración do cliente kerberos

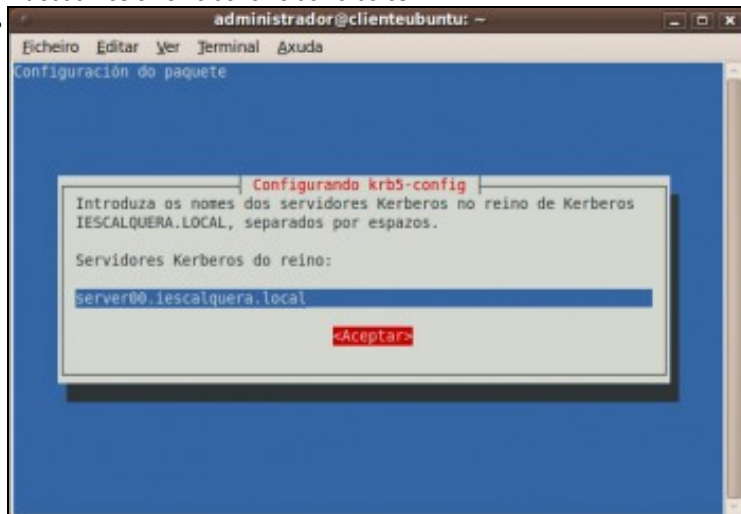
- Instalaremos os paquetes necesarios para o cliente kerberos:

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

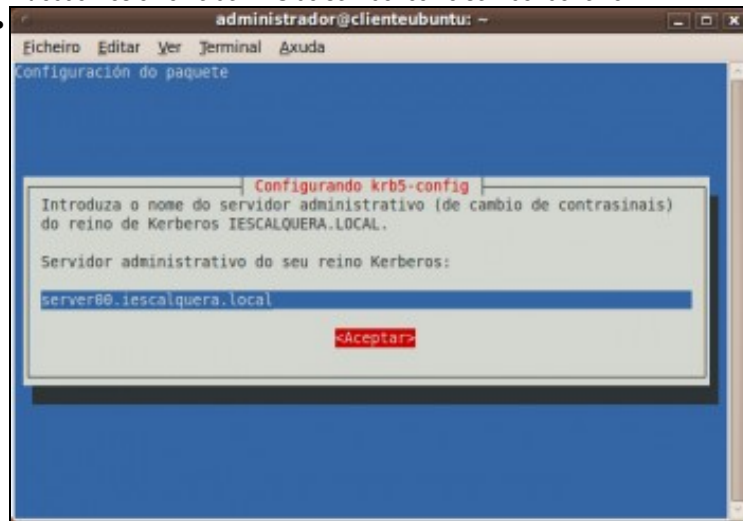
- Configuración do reino no cliente kerberos



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
```

## 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.

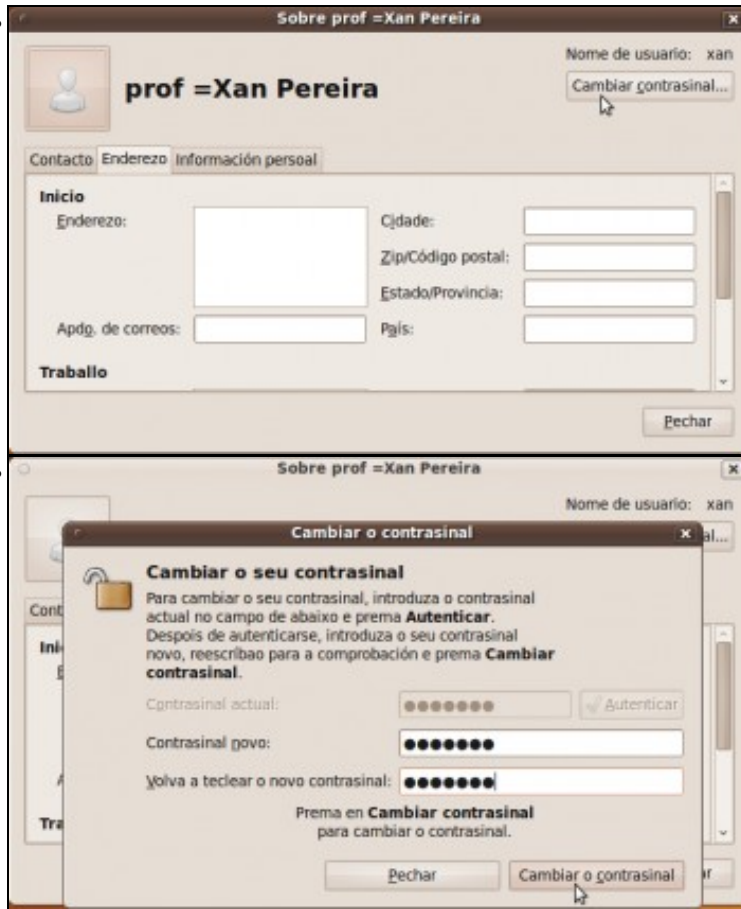
Os ficheiros de configuración de PAM almacénanse na carpeta */etc/pam.d*, e aí atoparemos un ficheiro por cada servizo que se pode requirir e nel especificanse as tarefas a realizar para ese servizo. Os servizos máis importante son *common-account*, *common-auth*, *common-session* e *common-password*,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



- 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 contrasinal de usuario LDAP



-- Antonio de Andrés Lema e Carlos Carrión Álvarez