Configuración do servidor Samba4 como controlador de dominio

Neste momento xa temos o servizo de Samba4 instalado no noso servidor Debian, pero aínda está configurado para actuar como un controlador dun dominio, que é o que nos pretendemos. Neste apartado imos ver os pasos que temos que seguir para acadalo.

Sumario

- 1 Configurar como servidor de DNS o equipo local
- 2 Promocionar a controlador de dominio
    - 2.1 Utilizando o servidor de DNS interno de Samba4
    - 2.2 Utilizando o servidor de DNS externo (Bind)
- 3 Arranque e comprobación do servizo samba
- 4 Comprobación do servidor Kerberos

Configurar como servidor de DNS o equipo local

No momento en que o servizo de Samba se configura para actuar como controlador de dominio, iniciará tamén o servizo de DNS (ou ben co servizo interno de Samba ou ben usando o servidor bind). É moi importante que o sistema Debian estea configurado para usarse a si mesmo como servidor de DNS, para poder resolver os nomes das máquinas do dominio.

Nós xa deberíamos ter esta configuración feita, pero non ven de máis revisala. Comprobamos o contido do ficheiro /**etc/resolv.conf**, que debería ser como o que segue:

```
domain iescalquera.local
search iescalquera.local
nameserver 172.16.5.10
```

Promocionar a controlador de dominio

Xa estamos listos para executar o comando que promoverá o servizo de Samba4 a controlador de dominio , inicializando as estruturas de LDAP, DNS e kerberos necesarias.

Temos aquí dúas opcións fundamentais, que son configurar como servizo de DNS o servizo de DNS incluído dentro de Samba4 ou utilizar o servizo bind que xa temos configurado na máquina. A decisión de utilizar un ou outro dependerá fundamentalmente da complexidade da configuración de DNS que requiramos na nosa rede (xa que bind é unha implementación máis completa do servizo DNS), e da facilidade que busquemos na instalación (no noso caso xa temos o servizo de bind instalado, pero se non teríamos que instalalo e configuralo mentres que o servizo de DNS interno de Samba configúrase de forma automática).

Por iso aquí imos mostrar as dúas alternativas, e o lector pode escoller a que prefira.

Utilizando o servidor de DNS interno de Samba4

Se nos decantamos por utilizar o servizo de DNS interno de Samba4, non podemos ter ao mesmo tempo iniciado o servizo de bind xa que darían conflitos entre eles. Por iso para evitar problemas en caso de reinicios do sistema nos que o bind se iniciaría de forma automática, imos quitar o paquete de bind, co comando *apt-get*:

```
apt-get remove bind9
```

E agora usaremos o comando **samba-tool** para promocionar o servizo Samba4 a controlador de dominio. Introducimos o comando:

```
samba-tool domain provision --use-rfc2307 --interactive
```

O parámetro *--use-rfc2307* permite que na estrutura do LDAP se almacenen os atributos POSIX dos usuarios e grupos (UIDs, GIDs, etc.), así que ímolo usar sempre que no dominio teñamos clientes Windows e Linux.

O comando vai solicitar de forma interactiva (grazas ao uso do parámetro *--interactive*) os seguintes valores, como vemos na imaxe:

```
root@dserver00:~# samba-tool domain provision --use-rfc2307 --interactive
Realm: IESCALQUERA.LOCAL
 Domain [IESCALQUERA]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
 DNS forwarder IP address (write 'none' to disable forwarding) [172.16.5.10]: 8.8.8.8
Administrator password:
Retype password:
```

Execución do comando *samba-tool domain provision*
Os parámetros que temos que configurar son:

- **Nome do reino de kerberos**: Será o mesmo que o nome do dominio pero en maiúsculas: **IESCALQUERA.LOCAL**. Se xa se nos suxire ese valor simplemente prememos *Intro*, e se non introducímolo e prememos *Intro*.
- **Nome do dominio**: Temos que introducir o nome de NetBIOS do dominio, sen o sufixo de DNS. Tamén xa ven por defecto o correcto, así que só prememos *Intro*.
- **Rol do servidor**: Indicamos se o servizo de samba vai actuar como controlador de dominio, membro dun dominio ou como unha máquina independente. Premendo *Intro* xa escollemos a opción *dc* (*domain controller*) para que o equipo sexa un controlador de dominio, que é a que ven por defecto.
- **Backend de DNS**: Neste caso, seleccionamos o valor por defecto *SAMBA_INTERNAL* que establece que se faga uso do servidor de DNS integrado de Samba4.
- **Dirección IP de reenvío de DNS**: Introducimos a dirección IP do servidor de DNS ao que queremos que o servidor de DNS integrado de Samba4 reenvíe as consultas de DNS que non poida resolver el mesmo, que serán todas aquelas de equipos en Internet, que non están na rede local. Na imaxe introduciuse o servidor DNS público de Google, coa dirección IP 8.8.8.8.
- **Contrasinal do Administrador**: Vaise crear un usuario co nome de *Administrator* que permite administrar inicialmente o dominio, aínd que logo nos poderemos crear os usuarios que queiramos con privilexios de administrador. Aquí introducimos o contrasinal que vai ter este usuario (introducimos *abc123.*). Teremos que introducilo dúas veces para evitar erros na súa escritura.

Na imaxe podemos ver a finalización da execución do comando, onde se indican os datos do servizo samba:

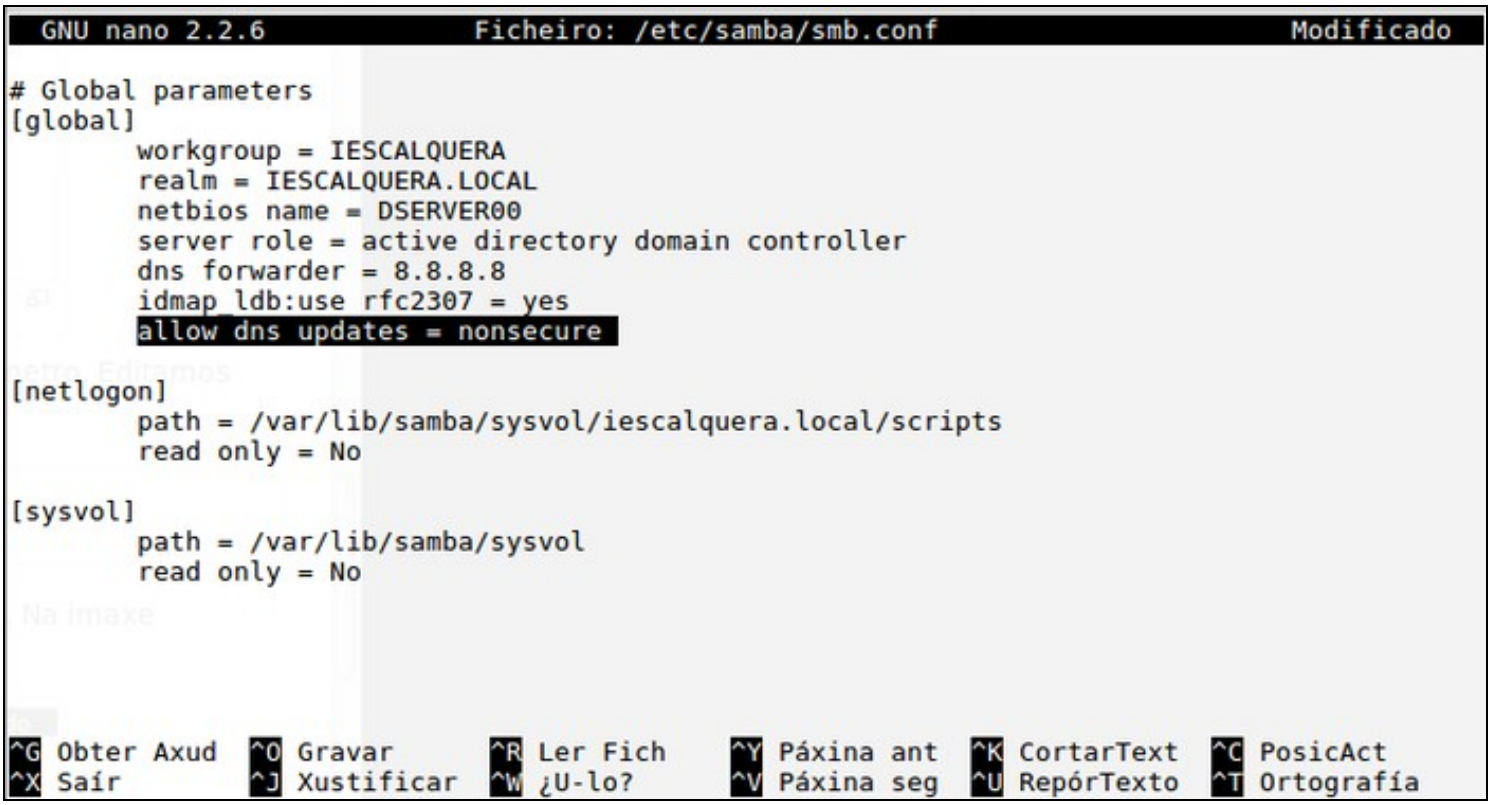
```
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              dserver00
NetBIOS Domain:        IESCALQUERA
DNS Domain:            iescalquera.local
DOMAIN SID:            S-1-5-21-177752966-1236432468-2211788286

root@dserver00:~#
```

Execución do comando *samba-tool domain provision*
Para rematar, imos editar o ficheiro de configuración de samba (**/etc/samba/smb.conf**) para engadir un parámetro. Editamos con *nano* este ficheiro e dentro da sección *[global]* engadimos a liña:

```
        allow dns updates = nonsecure
```

para que os equipos cliente se poidan rexistrar automaticamente no DNS cando se integran dentro do dominio. Na imaxe podemos ver o contido do ficheiro de configuración:



Edición do ficheiro de configuración para permitir actualizacións do DNS

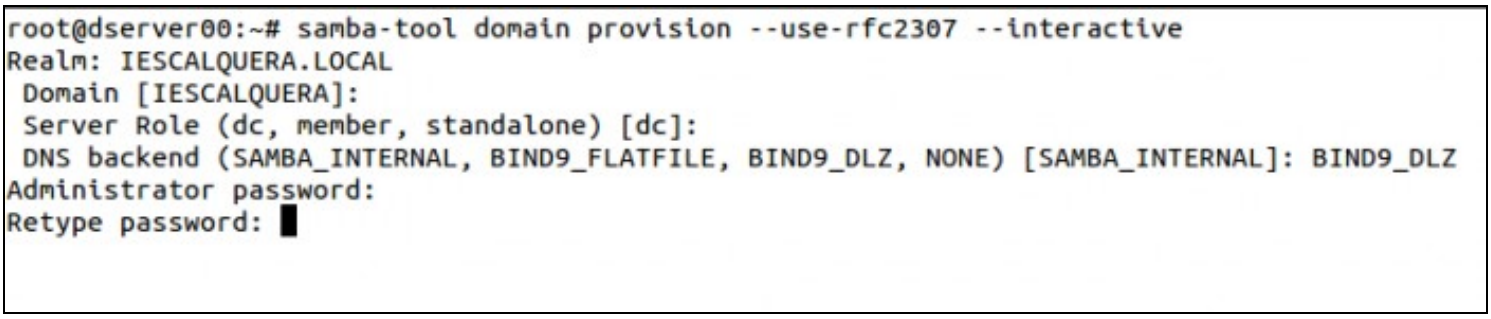
Utilizando o servidor de DNS externo (Bind)

Se decidimos utilizar o servidor de DNS Bind, dado que no noso caso xa o temos instalado non temos nada que facer; usaremos o comando **samba-tool** para promocionar o servizo Samba4 a controlador de dominio. Introducimos o comando:

```
samba-tool domain provision --use-rfc2307 --interactive
```

O parámetro *--use-rfc2307* permite que na estrutura do LDAP se almacenen os atributos POSIX dos usuarios e grupos (UIDs, GIDs, etc.), así que ímolo usar sempre que no dominio teñamos clientes Windows e Linux.

O comando vai solicitar de forma interactiva (grazas ao uso do parámetro *--interactive*) os seguintes valores, como vemos na imaxe:



Execución do comando *samba-tool domain provision*

Os parámetros que temos que configurar son:

- **Nome do reino de kerberos**: Será o mesmo que o nome do dominio pero en maiúsculas: **IESCALQUERA.LOCAL**. Se xa se nos suxire ese valor simplemente prememos *Intro*, e se non introducímolo e prememos *Intro*.
- **Nome do dominio**: Temos que introducir o nome de NetBIOS do dominio, sen o sufixo de DNS. Tamén xa ven por defecto o correcto, así que só prememos *Intro*.
- **Rol do servidor**: Indicamos se o servizo de samba vai actuar como controlador de dominio, membro dun dominio ou como unha máquina independente. Premendo *Intro* xa escollemos a opción *dc* (*domain controller*) para que o equipo sexa un controlador de dominio, que é a que ven por defecto.
- **Backend de DNS**: Neste caso, seleccionamos o valor por defecto *BIND9_DLZ* que establece que se faga uso do servidor de DNS Bind.

- **Contrasinal do Administrador**: Vaise crear un usuario co nome de *Administrator* que permite administrar inicialmente o dominio, aínd que logo nos poderemos crear os usuarios que queiramos con privilexios de administrador. Aquí introducimos o contrasinal que vai ter este usuario (introducimos *abc123.*). Teremos que introducilo dúas veces para evitar erros na súa escritura.

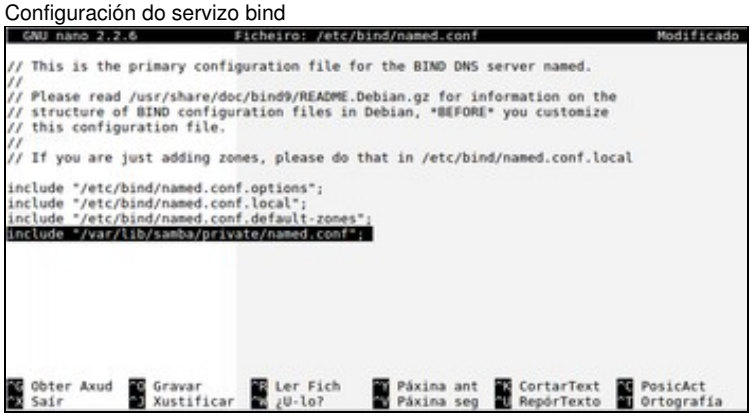
Na imaxe podemos ver a finalización da execución do comando, onde se indican os datos do servizo samba:

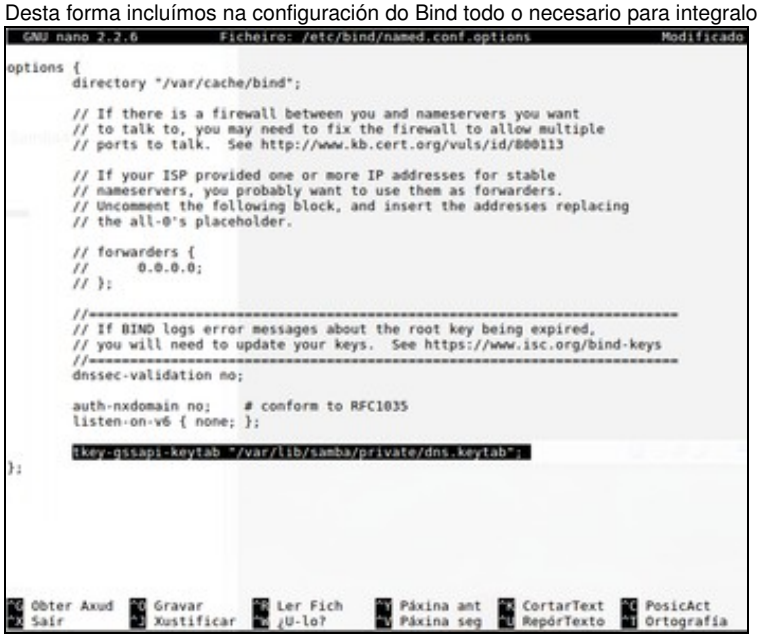
```
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              dserver00
NetBIOS Domain:        IESCALQUERA
DNS Domain:            iescalquera.local
DOMAIN SID:            S-1-5-21-1410788611-2910874867-472673252

root@dserver00:~#
```

Execución do comando *samba-tool domain provision*

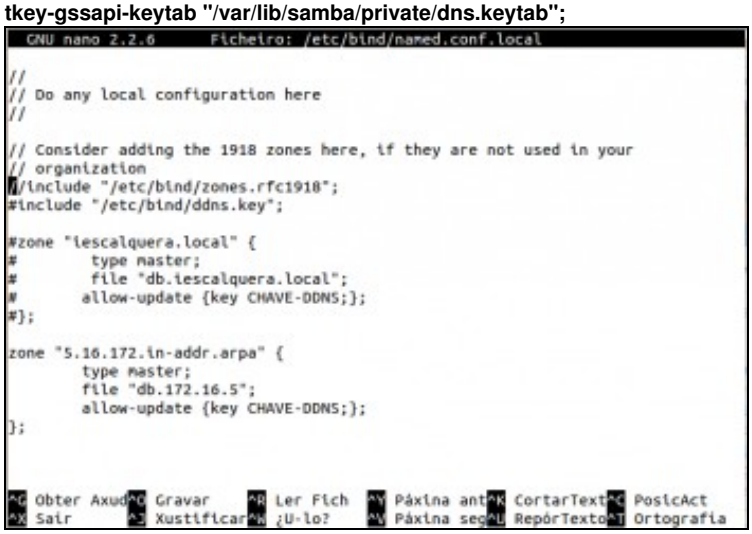
Como último paso, temos que facer algúns axustes na configuración de Bind para a súa integración con Samba4.

- Configuración do servizo bind
- 

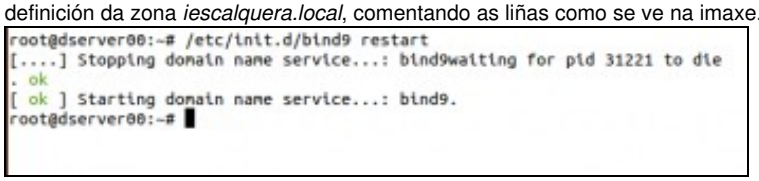
  Engadimos ao final do ficheiro */etc/bind/named.conf* a liña:
  include "/var/lib/samba/private/named.conf";
  Desta forma incluímos na configuración do Bind todo o necesario para integralo co servizo samba
- 

Para que o servizo samba poida facer actualizacións automáticas no servidor DNS bind cando engadimos equipos no dominio, imos engadir a seguinte liña dentro da sección *options* no ficheiro */etc/bind/named.conf.options*:

tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";

- 

A configuración de samba xa inclúe unha zona co nome do dominio, así que temos que retirar do ficheiro */etc/bind/named.conf.local* a definición da zona *iescalquera.local*, comentando as liñas como se ve na imaxe.

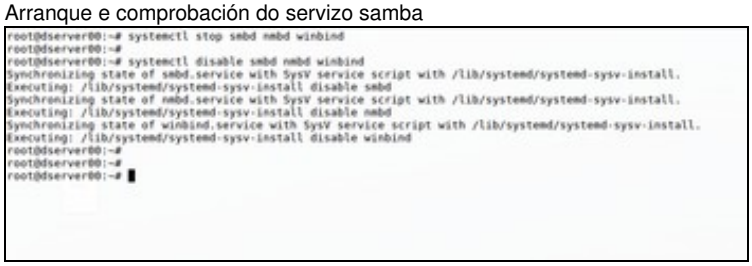
- 

Reiniciamos o servizo Bind para aplicar os cambios:

/etc/init.d/bind9 restart

Arranque e comprobación do servizo samba

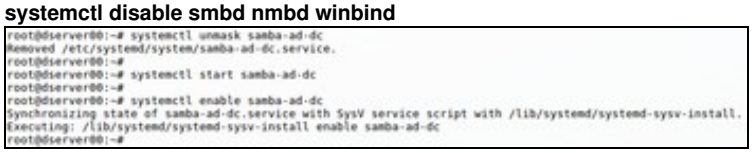
Xa estamos en disposición de arrancar o servizo de samba, e comprobar tanto o funcionamento do servizo *smbd* como do DNS:

- Arranque e comprobación do servizo samba
- 

En Debian 9, o servizo que debemos usar para iniciar o servidor Samba varia dependendo de se o equipo vai tomar ou non o rol de controlador do dominio. Neste caso, en lugar e usar directamente os servizos *smbd*, *nmbd* e *winbind*, usaremos o servizo **samba-ad-dc**. Así que primeiro detemos e desactivamos estes servizos cos comandos:

systemctl stop smbd nmbd winbind

systemctl disable smbd nmbd winbind

- 

E a continuación, activamos e iniciamos o servizo **samba-ad-dc** (*Samba Active Directory Domain Controller*):

systemctl unmask samba-ad-dc

systemctl start samba-ad-dc

systemctl enable samba-ad-dc

- ```
  root@dserver00:~# smbclient -L localhost -U%
  Domain=[IESCALQUERA] OS=[Windows 6.1] Server=[Samba 4.5.12-Debian]

          Sharename       Type      Comment
          ---------       ----      -------
          netlogon        Disk
          sysvol          Disk
          IPC$            IPC       IPC Service (Samba 4.5.12-Debian)
  Domain=[IESCALQUERA] OS=[Windows 6.1] Server=[Samba 4.5.12-Debian]

          Server               Comment
          ---------            -------

          Workgroup            Master
          ---------            -------
          WORKGROUP            DSERVER00
  root@dserver00:~#
  ```

Imos utilizar o cliente de samba *smbclient* sobre a nosa propia máquina (*localhost*) para comprobar que o servizo responde:
smbclient -L localhost -U%

- ```
  root@dserver00:~# host -t SRV _ldap._tcp.iescalquera.local
  _ldap._tcp.iescalquera.local has SRV record 0 100 389 dserver00.iescalquera.local.
  root@dserver00:~#
  root@dserver00:~# host -t SRV _kerberos._udp.iescalquera.local
  _kerberos._udp.iescalquera.local has SRV record 0 100 88 dserver00.iescalquera.local.
  root@dserver00:~#
  root@dserver00:~# host -t A dserver00.iescalquera.local
  dserver00.iescalquera.local has address 172.16.5.10
  root@dserver00:~#
  root@dserver00:~#
  ```

Comprobamos co comando *host* que o servizo de DNS resolve os nomes dos obxectos creados na inicialización do dominio:
host -t SRV _ldap._tcp.iescalquera.local: Devolverá que máquina executa o servizo de LDAP do dominio, e en que porto
host -t SRV _kerberos._udp.iescalquera.local: Devolverá que máquina executa o servizo de kerberos, e en que porto
host -t A dserver00.iescalquera.local: Devolverá a dirección IP do noso servidor

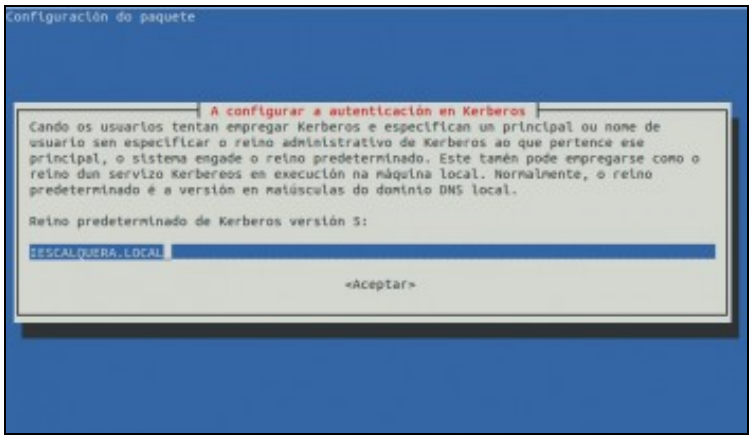
Comprobación do servidor Kerberos

Este paso en realidade non é necesario para a configuración do servidor, xa que o único que imos facer é comprobar que o servizo de Kerberos funciona correctamente instalando o cliente de Kerberos e autenticándonos contra el con un usuario do dominio (polo momento con *Administrator*, que é o único usuario que temos). Porén, coidamos que é moi interesante facelo, porque así podemos verificar que esta peza tan importante do dominio funciona correctamente, así como entender un pouco mellor o funcionamento de Kerberos.

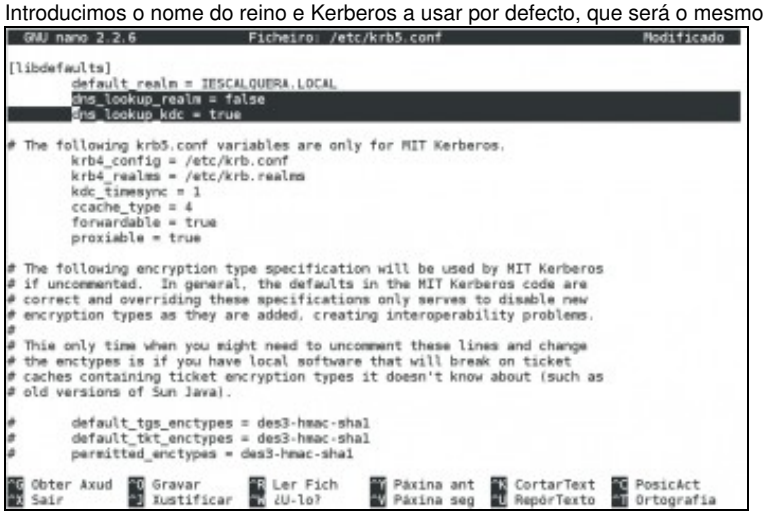
- Comprobación do servidor Kerberos

- ```
  root@dserver00:~# apt-get install krb5-user
  Lendo as listas de paquetes... Feito
  Construíndo a árbore de dependencias
  Lendo a información do estado... Feito
  Instalaranse os seguintes paquetes extra:
    krb5-config
  Os seguintes paquetes NOVOS hanse instalar:
    krb5-config krb5-user
  0 anovados, 2 instalados, Vanse retirar 0 e deixar 18 sen anovar.
  Ten que recibir 178 kB de arquivos.
  Despois desta operación ocuparanse 440 kB de disco adicionais.
  Quere continuar [S/n]? S
  ```

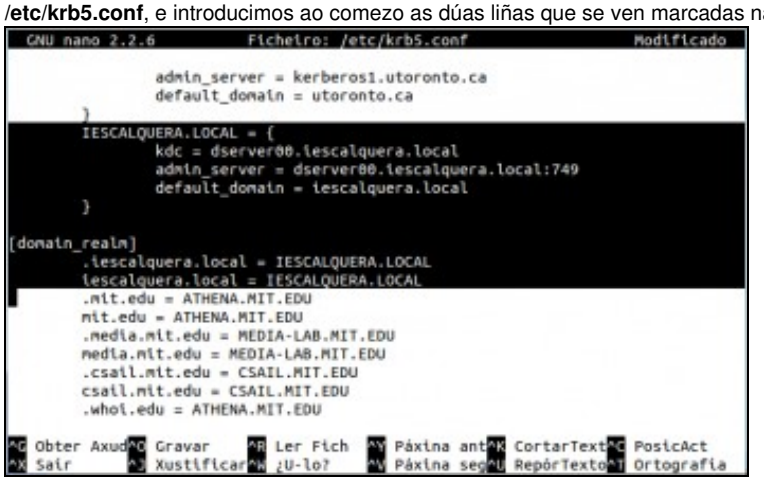
Instalamos o paquete do cliente Kerberos:
apt-get install krb5-user
  ```

- 

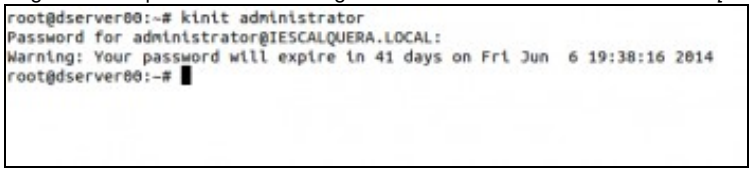
Introducimos o nome do reino e Kerberos a usar por defecto, que será o mesmo que o nome do dominio pero en maiúsculas.

- 

Agora temos que configurar no cliente de Kerberos o noso *reino* de Kerberos. Abrimos o ficheiro de configuración do cliente Kerberos, **/etc/krb5.conf**, e introducimos ao comezo as dúas liñas que se ven marcadas na imaxe.

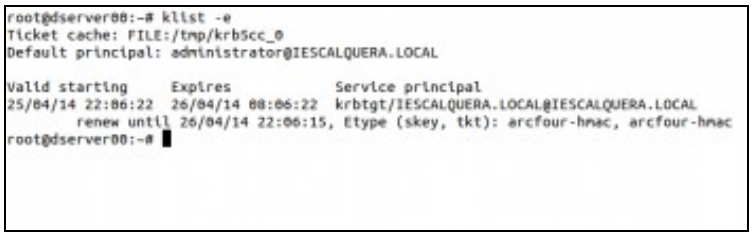
- 

Engadimos os parámetros de configuración do reino ao final da sección de *[realms]*, e tamén dentro da sección de *[domain_realm]*.

- 

Co comando *kinit* podemos iniciar unha sesión de Kerberos para obter un ticket que nos permitirá autenticarnos. Ao ter configurado o reino *IESCALQUERA.LOCAL* como reino por defecto, basta con poñer:

kinit administrator

- 

  Agora comprobamos o ticket que se nos enviou e a súa validez, co comando: **klist -e**

- Contido engadido ao ficheiro /**etc/krb5.conf**:

```
        dns_lookup_realm = false
        dns_lookup_kdc = true

        .....

        IESCALQUERA.LOCAL = {
                kdc = dserver00.iescalquera.local
                admin_server = dserver00.iescalquera.local:749
                default_domain = iescalquera.local
        }

[domain_realm]
        .iescalquera.local = IESCALQUERA.LOCAL
        iescalquera.local = IESCALQUERA.LOCAL
```

-- Antonio de Andrés Lema e Carlos Carrión Álvarez