# 1 Instalación do servidor kerberos en Ubuntu Server

Neste apartado abordaremos os pasos necesarios para instalar o servidor kerberos e configuralo para que use como base de datos de usuarios o servidor LDAP. Pero en primeiro lugar, teremos que engadir no LDAP o esquema de kerberos, que define unha serie de atributos que o servidor kerberos precisará almacenar para os *principals*, e que deberán ter aqueles usuarios que vaian usar kerberos para autenticarse contra outros servizos.

## 1.1 Sumario

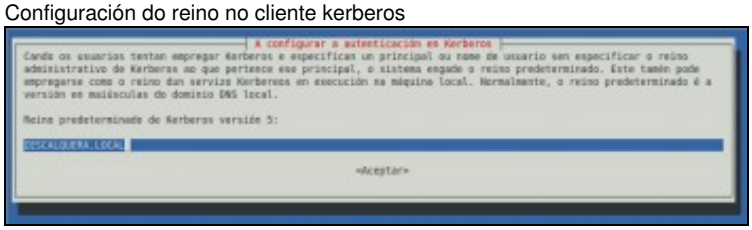


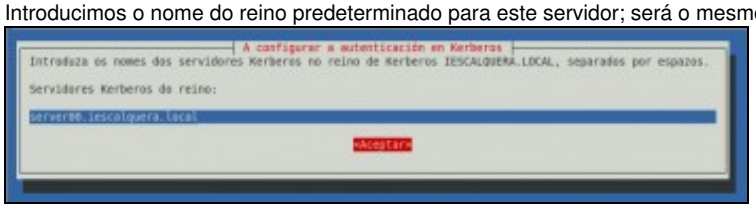
## 1.2 Instalar e configurar o servidor kerberos

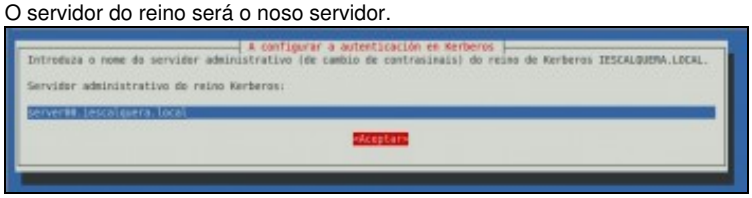
- Teremos que configurar o servidor de kerberos para que actúe como Centro de Distribución de Chaves (*KDC*). Instalamos no servidor os paquetes necesarios:

```
sudo apt-get install krb5-kdc krb5-admin-server
```

Na instalación dos paquetes, pediránsenos algúns datos de configuración básicos para o novo servidor kerberos:

- Configuración do reino no cliente kerberos
- 

Introducimos o nome do reino predeterminado para este servidor; será o mesmo que o nome de DNS do noso dominio en maiúsculas.
- 

O servidor do reino será o noso servidor.
- 

Poñemos o mesmo como servidor administrativo.

- 

Información sobre a instalación do paquete e comando que podemos usar para crear o reino kerberos. Nós non usaremos ese comando, xa que usaremos un específico para o uso do LDAP como base de datos.

## 1.3 Configurar o servidor LDAP para servir de base de datos de kerberos

### 1.3.1 Incluír o esquema de kerberos no servidor LDAP

- Instalaremos o paquete **krb5-kdc-ldap** que contén o esquema de kerberos para LDAP:

```
sudo apt-get install krb5-kdc-ldap
```

- O paquete inclúe o esquema en formato *schema* e comprimido, así que o descomprimiremos e transformarémolo a formato LDIF para poder engadilo no LDAP:

```
sudo gzip -d /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz
sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema /etc/ldap/schema/
```

- Creamos o ficheiro *schema_convert.conf* co seguinte contido:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/kerberos.schema
```

- Creamos un directorio temporal para almacenar o ficheiros LDIF:

```
mkdir /tmp/ldif_output
```

- Usamos o comando *slapcat* para converter o ficheiro de esquema a LDIF:

```
slapcat -f schema_convert.conf -F /tmp/ldif_output -n0 -s "cn={12}kerberos,cn=schema,cn=config" > /tmp/cn=kerberos.ldif
```

- Editamos o ficheiro creado por este último comando: */tmp/cn\=kerberos.ldif*, cambiando estes dous atributos:

```
dn: cn=kerberos,cn=schema,cn=config
...
cn: kerberos
```

- e borrando as seguintes liñas que se atopan ao final do ficheiro:

```
structuralObjectClass: olcSchemaConfig
entryUUID: 18ccd010-746b-102d-9fbe-3760cca765dc
creatorsName: cn=config
createTimestamp: 20090111203515Z
entryCSN: 20090111203515.326445Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20090111203515Z
```

- Cargamos o esquema en formato LDIF (contrasinal *1234*):

```
ldapadd -x -D cn=admin,cn=config -W -f /tmp/cn\=kerberos.ldif
Enter LDAP Password:
adding new entry "cn=kerberos,cn=schema,cn=config"
```

### 1.3.2 Engadir os índices necesarios para as buscas de kerberos

- Engadimos un índice para o atributo *krbPrincipalName*, que almacena o nome do usuario ou principal, que será o dato polo que kerberos buscará aos usuarios (Premer despois da última liña Control+D):

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
add: olcDbIndex
olcDbIndex: krbPrincipalName eq,pres,sub
```

### 1.3.3 Actualizar a listas de control de acceso do LDAP

- Utilizamos de novo o comando *ldapmodify* (De novo prememos Control+D para introducir as liñas en formato LDIF):

```
ldapmodify -x -D cn=admin,cn=config -W
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
replace: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange,krbPrincipalKey by self write by anonymous auth by dn.base="cn=admin,dc=iescalq
-
add: olcAccess
olcAccess: to dn.base="" by * read
-
add: olcAccess
olcAccess: to * by dn="cn=admin,dc=iescalquera,dc=local" write by * read
```

## 1.4 Configurar o reino kerberos e autenticación contra o LDAP

### 1.4.1 Configurar kerberos para usar o LDAP como base de datos

- Imos editar o ficheiro de configuración de kerberos */etc/krb5.conf* incluíndo as liñas que aparecen en negriña. O que facemos con esta configuración é configurar o servidor kerberos para que use como base de datos de usuario o servidor LDAP. Tamén de paso imos activar os logs do servidor kerberos para poder analizar posibles erros:

```
[realms]
        IESCALQUERA.LOCAL = {
                kdc = server00.iescalquera.local
                admin_server = server00.iescalquera.local
                default_domain = iescalquera.local
```

```
                database_module = openldap_ldapconf
        }

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

[dbdefaults]
        ldap_kerberos_container_dn = dc=iescalquera,dc=local

[dbmodules]
        openldap_ldapconf = {
                db_library = kldap
                ldap_kdc_dn = "cn=admin,dc=iescalquera,dc=local"

                # este obxecto precisa ter permisos de lectura no contedor
                # do reino, contedor de usuario e subarbores do reino
                ldap_kadmind_dn = "cn=admin,dc=iescalquera,dc=local"

                ldap_service_password_file = /etc/krb5kdc/service.keyfile
                ldap_servers = ldapi:///
                ldap_conns_per_server = 5
        }

[logging]
     kdc = SYSLOG:INFO:DAEMON
     admin_server = SYSLOG:INFO:DAEMON
     default = SYSLOG:INFO:DAEMON
```

### 1.4.2 Crear e configurar o reino kerberos

- Usamos o comando *kdb5_ldap_util utility* para crear o reino de kerberos. O comando solicitaranos o contrasinal do usuario administrador do LDAP (*admin*) e despois establecer un contrasinal para a base de datos mestra do LDAP (poremos **abc123.**):

```
sudo kdb5_ldap_util -D  cn=admin,dc=iescalquera,dc=local create -subtrees dc=iescalquera,dc=local -r IESCALQUERA.LOCAL -s -H ldap://
Password for "cn=admin,dc=iescalquera,dc=local":
Initializing database for realm 'IESCALQUERA.LOCAL'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

- Creamos un ficheiro no que se almacena o contrasinal que terá que usar kerberos para conectarse ao servidor LDAP:

```
sudo kdb5_ldap_util -D  cn=admin,dc=iescalquera,dc=local stashsrvpw -f /etc/krb5kdc/service.keyfile cn=admin,dc=iescalquera,dc=local
```

- Lanzamos os servizos de kerberos, para comprobar que os datos introducidos son correctos:

```
sudo /etc/init.d/krb5-admin-server restart
sudo /etc/init.d/krb5-kdc restart
```

## 1.5 Sincronizar a hora do sistema

- Como vimos na introdución a kerberos, neste protocolo é moi importante a sincronización da hora entre o cliente e o servidor, xa que o ticket emitido polo servidor kerberos ten unha validez entre unha data/hora inicio e data/hora fin, e o cliente crea o paquete *autenticador* introducindo a súa hora do sistema, que logo e comprobado polo Servidor do Servizo. É por iso que se a hora do sistema cliente e servidor teñen un desfase superior a 5 minutos, o protocolo kerberos pode comezar a fallar.

- Para evitalo, imos sincronizar a hora do cliente e do servidor con un servidor de tempos, usando o protocolo NTP. En Ubuntu podemos usar o comando **ntpdate** para sincronizar a hora con un servidor de tempos. Por exemplo:

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

- Con isto xa temos sincronizada a hora do servidor con este servidor. Para maior seguridade, sería interesante definir unha tarefa programada que cada certas horas execute este comando, pero isto o veremos máis adiante.

- En http://www.pool.ntp.org podemos buscar direccións de servidor NTP distribuídos por todo o mundo.

## 1.6 Engadir usuario administrador de kerberos

- En kerberos, os usuarios reciben o nome de *pincipals*. Imos crear un *principal* con privilexios de administración en kerberos, para poder manipular no futuro a información de kerberos (e lle teremos que asociar un contrasinal). Usaremos os comandos *kadmin.local* e *kadmin*, que permiten xestionar a información de kerberos (usaremos *kadmin.local* cando nos imos conectar a kerberos dende o propio servidor):

```
sudo kadmin.local -q "addprinc admin/admin"
Authenticating as principal root/admin@IESCALQUERA.LOCAL with password.
WARNING: no policy specified for admin/admin@IESCALQUERA.LOCAL; defaulting to no policy
Enter password for principal "admin/admin@IESCALQUERA.LOCAL":
Re-enter password for principal "admin/admin@IESCALQUERA.LOCAL":
Principal "admin/admin@IESCALQUERA.LOCAL" created.
```

- Darémoslle privilexios a este usuario, creando o ficheiro */etc/krb5kdc/kadm5.acl* co contido:

```
*/admin@IESCALQUERA.LOCAL       *
```

E reiniciamos de novo os servizos de kerberos para cargar a nova acl:

```
sudo /etc/init.d/krb5-admin-server restart
sudo /etc/init.d/krb5-kdc restart
```

## 1.7 Engadir un principal

Agora xa podemos engadir un principal que se corresponda con un usuario do dominio, como por exemplo o usuario *xan*. Asignarémoslle como contrasinal **abc123.** xa que é o mesmo contrasinal que o usuario **xan** ten no LDAP:

```
sudo kadmin.local
Authenticating as principal root/admin@IESCALQUERA.LOCAL with password.
kadmin.local:   addprinc -x dn="uid=xan,ou=usuarios,dc=iescalquera,dc=local" xan
WARNING: no policy specified for xan@IESCALQUERA.LOCAL; defaulting to no policy
Enter password for principal "xan@IESCALQUERA.LOCAL":
Re-enter password for principal "xan@IESCALQUERA.LOCAL":
Principal "xan@IESCALQUERA.LOCAL" created.
kadmin.local:  exit
```

-- Antonio de Andrés Lema e Carlos Carrión Álvarez