# 一 RedHat/CentOS安装和配置kerberos

需要在kerberos server和客户端都先安装ntp (Internet时间协议，保证服务器和客户机时间同步 )

## 1  kerberos 服务器端

* 1. install /start ntp

|  |
| --- |
| #sudo yum install ntp  #sudo service ntpd start |

* 1. install kerberos server:

|  |
| --- |
| #yum install krb5-server krb5-libs krb5-auth-dialog |

  可选： install kerberos client:

|  |
| --- |
| # yum install krb5-workstation |

1.3 edit /etc/krb5.conf and /var/kerberos/krb5kdc/kdc.conf

|  |
| --- |
| # sudo vi /etc/krb5.conf |

Replacing EXAMPLE.COM with your domain name.

Replace the kerberos.example.com with your kdc server.

|  |
| --- |
| # sudo vi /var/kerberos/krb5kdc/kdc.conf |

Replacing EXAMPLE.COM with your domain name.

* 1. create the databse using kdb5\_util utility.

|  |
| --- |
| # sudo /usr/sbin/kdb5\_util create -s |

### 1.5 edit  /var/kerberos/krb5kdc/kadm5.acl file

|  |
| --- |
| # sudo vi  /var/kerberos/krb5kdc/kadm5.acl file |

such as:将 \*/admin@EXAMPLE.COM  \*  [改为\*/admin@MYCOMPANY.COM](mailto:改为*/admin@MYCOMPANY.COM)

### 1.6. use kadmin.local to add  admin user:

|  |
| --- |
| #kadmin.local  #addprinc steve/admin  #addprinc tony/admin |

### 1.7. start kerberos:

|  |
| --- |
| # /sbin/service krb5kdc start   # /sbin/service kadmin start |

1.8. now you can use kadmin to manage principal:

|  |
| --- |
| #kadmin -q "addprinc  user1/admin" |

This way you actaully use client mode to connect to kdc and do admin level task  
1.9. verify KDC ok.

|  |
| --- |
| #kinit tony/admin  #klist |

## 2 各个客户机端

### 2.1. install kerberos client

|  |
| --- |
| #yum install krb5-workstation |

### 2.2. edit /etc/krb5.conf

|  |
| --- |
| #sudo vi /etc/krb5.conf |

Replace the EXAMPLE.com with your domain name

replace the kerberos.example.com with your  kdc server

### 2.3. authenticate the admin user with Kerberos

|  |
| --- |
| #kinit steve/admin |

view the principls from client machine:

|  |
| --- |
| #sudo kadmin  #list\_principals |

## 3 用kerberos进行OS 级本地认证和远程登录

-----------------enable kerbose local authentication----------  
1. install pAM

|  |
| --- |
| sudo apt-get install libpam-krb5 |

### 2.view conf file:

|  |
| --- |
| sudo cat /etc/pam.d/common-auth |

------------configure the client can remote login using kerborse-----------  
1. create another principal such as:

|  |
| --- |
| service/clienthost@realm |

2.  add the keytab for such principal

|  |
| --- |
| kadmin : ktadd -k /etc/service.keytab  service/clienthost@realm |

save the keytab to /etc/krb5.keytab  
二 Ubuntu安装和配置kerberos

## 1.kdc server side

### 1.install the krb5-kdc and krb5-admin-server packages. From a terminal enter:

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

### 2.Create new realm

|  |
| --- |
| sudo krb5\_newrealm |

### 3.reconfigure realm

|  |
| --- |
| sudo dpkg-reconfigure krb5-kdc |

### 4.View config files

|  |
| --- |
| /etc/krb5kdc/kdc.conf  /etc/krb5.conf |

### 5. create admin user:

1)in kdc server type in:

|  |
| --- |
| sudo kadmin.local  addprinc steve/admin  quit/exit |

2) edit ACL file /etc/krb5kdc/kadm5.acl  like:

[steve/admin@EXAMPLE.COM](mailto:steve/admin@EXAMPLE.COM) \*

restart krb5-admin-server for ACL take affect:

|  |
| --- |
| sudo  /etc/init.d/krb5-admin-server  restart |

3) check the user and ticket:

|  |
| --- |
| kinit steve/admin  klist |

 ---the above 2 command canalso be performed on client machines that installed krb5  client package

After creating admin user (steve/admin), the admin user later can aslo login in to KDC  do management stuff from client machine

## 2.client side

### 1. install client software

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

### 2.configure client:

|  |
| --- |
| sudo dpkg-reconfigure krb5-config |

### 3.view client configuration

|  |
| --- |
| /etc/krb5.conf |

### 4.check user/ticket:

for admin user principal:

|  |
| --- |
| kinit steve/admin (steve/admin@EXAMPLE.com) Password for steve/admin@EXAMPLE.COM: |

for common user principal:

|  |
| --- |
| kinit  xxx (xxx@EXAMPLE.com) |

for service principal:

|  |
| --- |
| kinit service/host@realm |

## 3.Enable kerbose local authentication

1. install pAM、

|  |
| --- |
| sudo apt-get install libpam-krb5 |

2.view conf file:

|  |
| --- |
| sudo cat /etc/pam.d/common-auth |

## 4.configure serice to use kerborse

suppose service principal is  service/host@realm

1. create service principal

|  |
| --- |
| kadmin : addprinc  -randkey  service/host@realm |

1. add keytab for service

|  |
| --- |
| kadmin: ktadd  -k /etc/service.keytab  service/host@realm |

### 3.save the keytab to correct location for service

## 5. Configure the client can remote login using kerborse

1. create another principal such as:

|  |
| --- |
| service/clienthost@realm |

1. add the keytab for such principal

|  |
| --- |
| kadmin : ktadd -k /etc/service.keytab  service/clienthost@realm |

save the keytab to /etc/krb5.keytab

# 三 管理kerberos principal

初始化管理用户比如steve/admin后，  运行kadmin即进入管理程序（可在安装了kerberos krb5-workstation软件包的kdc或客户端）

|  |
| --- |
| # kinit steve/admin  # kadmin |

## 1.创建/改变principal

### 1.1 创建service principal

|  |
| --- |
| addprinc  -pw $passwd  $principalname/$servicehost@realm ---add service principal with password  addprinc  -randkey  $principalname/$servicehost@realm ---add service principal with random key |

### 1.2 创建普通principal

|  |
| --- |
| addprinc  -pw $passwd  $principalname ---add principal with passwd |

### 1.3 改变principal

|  |
| --- |
| modprinc  -pw $passwd  $principalname ---change principal |

改密码：

|  |
| --- |
| cpw -pw $passwd  $principalname ---change principal password |

## 2 查看principal

 listprincs

# 四 管理keytab

服务principal的credential需要保存在keytab文件中。

1.获取keytab

进入kadmin

1.1 用ktadd :

ktadd -k  $<keytab\_file\_name>   service/servicehost@realm  或者 #ktadd -k $<keytab\_file\_name>  service/servicehost

比如：

# ktadd -k /etc/myservice.keytab  myservice/servicehost

1.2 用xst

xst -k $<keytab\_file\_name> $service/servicehost

 2. 查看keytab

klist -k -t $<keytab\_file\_name>