

Installing and Configuring Kerberos Clients on Red Hat 8.0

v3.0

Note that the following instructions pertain to Red Hat version 8.0. Installations on other Red Hat versions may differ.

1. Install the `krb5-libs`, `krb5-workstation` and `pam_krb5` packages. On Red Hat 8.0, the `krb5-libs` and `pam_krb5` packages install along with the operating system. The `krb5-workstation` package can be found on CD number 3.
2. Configure Kerberos for command line login and login via telnet and rlogin using PAM as follows:
 - a. Login on the console of your Red Hat machine as root and execute `startx` to bring up the GUI.
 - b. Choose menu options **System Settings...Authentication**.
 - c. Select the **Authentication** tab and check the **Enable Kerberos Support** box.
 - d. Click on the **Configure Kerberos...** button.
 - e. Enter data in the **Realm**, **KDCs** and **Admin Servers** boxes. If your Active Directory domain is "mycompany.com", your realm would be "MYCOMPANY.COM" (not including the quotes). The KDCs and Admin Servers boxes should both contain the fully qualified domain name of your Active Directory domain controller (e.g. bigcheese.mycompany.com). The data entered here is placed in the `/etc/krb5.conf` file.
 - f. Click OK and you should be set to go.

Please note that with your system configured in this way, logins via telnet and rlogin will send your users' passwords across the network in the clear.

3. If you need to make changes to the ticket attributes (lifetime, renew lifetime, forwardable option, etc.) that will be used during login, modify the `krb5.conf` file in `/etc`. This file will look something like the following and the section you are most likely to modify is the one called "[appdefaults]":

```
[logging]
  default = FILE:/var/log/krb5libs.log

[libdefaults]
  ticket_lifetime = 24000
  default_realm = MYCOMPANY.COM
  dns_lookup_realm = false
  dns_lookup_kdc = false

[realms]
  MYCOMPANY.COM = {
    kdc = bigcheese.mycompany.com:88
    admin_server = bigcheese.mycompany.com:749
```

```
default_domain = mycompany.com
}
```

```
[domain_realm]
.mycompany.com = MYCOMPANY.COM
*.mycompany.com = MYCOMPANY.COM
mycompany.com = MYCOMPANY.COM
```

```
[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```

4. For additional security using telnet, rlogin, rsh, rcp and ftp, configure the Kerberized services provided in the Red Hat package as shown below. Making use of the Kerberized services enables your users to login via telnet or rlogin, or use the rcp, rsh and ftp tools, without sending their passwords across the network in the clear. Note that these instructions pertain to setting up the server side of a Kerberized services environment. In order to make use of Kerberized services, you will also need to provide Kerberized client tools on the machines from which your users will be working. These client tools are installed on Red Hat with the krb5-workstation package and are configured with the krb5.conf file.

5. Configure the Kerberized telnet server as follows:

- a. Modify the /etc/xinetd.d/krb5.telnet file to include “disable = no” as shown in this sample file:

```
service telnet
{
    flags            = REUSE
    socket_type      = stream
    wait             = no
    user             = root
    server           = /usr/kerberos/sbin/telnetd
    log_on_failure  += USERID
    disable          = no
}
```

- b. Modify the /etc/xinetd.d/telnet file to include “disable = yes” as shown in this sample file:

```
service telnet
{
    flags            = REUSE
    socket_type      = stream
    wait             = no
```

```
user          = root
server        = /usr/sbin/in.telnetd
log_on_failure += USERID
disable       = yes
}
```

- c. Re-HUP the xinetd daemon as follows:
 - i. Obtain the process ID of the xinetd process using this command:

```
ps -aux | grep xinetd
```
 - ii. The output of this command should be something like:

```
root 648 1 0 May20 ? 00:00:01 xinetd -stayalive -reuse -pidfil
root 24465 22557 0 16:26 pts/1 00:00:00 grep xinetd
```
 - iii. The process ID is the first number shown on the left for the line that does not include the “grep” statement. In this case, the process ID is 648.
 - iv. Restart the xinetd daemon with this command (substituting the process ID you obtained above):

```
kill -HUP 648
```
6. Configure the Kerberized rlogin server similarly to the telnet server, setting “disable” to yes in the /etc/xinetd.d/rlogin file and setting “disable” to no in the /etc/xinetd.d/klogin file. Re-HUP the xinetd daemon as above. To provide for encrypted rlogin, the eklogin file in /etc/xinetd.d must also be modified to set “disable” to no.
7. Configure the Kerberized rsh and rcp server similarly to the telnet server, setting “disable” to yes in the /etc/xinetd.d/rsh file and setting “disable” to no in the /etc/xinetd.d/kshell file. Re-HUP the xinetd daemon as above.
8. The steps for configuration of the Kerberized ftp server differ from the above and can be provided if desired.
9. In order for the Kerberized services to work correctly, you must create a key table file. This can either be done using the ktpass tool on Active Directory or with the css_akdamin tool. Using css_akdadmin, create a service principal for the client machine (e.g. host/client.mycompany.com@MYCOMPANY.COM) and write its key to a key table file using the following command (where Administrator is a username in Active Directory with sufficient permissions to add a user to the database):

```
css_akdadmin.sh -p Administrator -w -q "ank -k host/client.mycompany.com"
```

By default the key table will be placed in /etc and called krb5.keytab.