Install and configuring kerberos On Slackware without PAM

The KDC

This procedure will result in a new Kerberos realm. If you already have access to a Kerberos KDC, you can skip to the client and application server parts. Also, the below procedure is very abbreviated and is not a substitute for reading the documentation supplied in the package or on the MIT Kerberos website.

1. Install krb (you can download and build it from http://slackbuilds.org/repository/14.1/network/krb5/)
2. Configure /etc/krb5.conf, /var/krb5kdc/kdc.conf and /var/krb5kdc/kadm5.acl . These files are examples which you should adjust after reading the Kerberos documentation.

krb5.conf

```
 [domain_realm]
        example.com = EXAMPLE.COM
        .example.com = EXAMPLE.COM

[libdefaults]
        default_realm = EXAMPLE.COM
        dns_kdc_lookup = true
        dns_realm_lookup = true
        forwardable = true
        renewable = true
        [realms]

EXAMPLE.COM = {
    kdc = kerberos-1.example.com:88
    kdc = kerberos-2.example.com:88
        admin_server = kerberos-1.example.com:749
        }
```

kdc.conf

```
[kdcdefaults]
        kdc_ports = 749,88

[realms]
        EXAMPLE.COM = {
                database_name = /var/krb5kdc/principal
                admin_keytab = FILE:/var/krb5kdc/kadm5.keytab
                acl_file = /var/krb5kdc/kadm5.acl
                key_stash_file = /var/krb5kdc/.k5.EXAMPLE.COM
                kdc_ports = 749,88
                max_life = 10h 0m 0s
```

```
                max_renewable_life = 7d 0h 0m 0s
                supported_keytypes = aes256-cts des-cbc-crc des-cbc-md5
        }
```

kadm5.acl

```
krb5adminprinc/admin   *
```

3. Create DataBase

```
/usr/kerberos/sbin/kdb5_util create -r EXAMPLE.COM -s
```

4. Extract the admin server keys to /var/krb5kdc/kadm5.keytab.

```
/usr/kerberos/sbin/kadmin.local
kadmin.local: xst -k /var/krb5kdc/kadm5.keytab kadmin/admin kadmin/changepw
```

5. Create host and other principals; extract to /etc/krb5.keytab

```
kadmin.local: ank -randkey host/fully.qualified.domain.name
kadmin.local: xst -k /etc/krb5.keytab host/fully.qualified.domain.name
```

```
**6.** Create admin, user principals
kadmin.local: ank krb5adminprinc/admin
kadmin.local: ank krb5userprinc
kadmin.local: quit
```

7. Create startup script /etc/rc.d/rc.krb5

rc.krb5 - shamelessly ripped off from rc.samba from Slackware 13.0

```
#!/bin/sh
#
# /etc/rc.d/rc.krb5
#
# Start/stop/restart the MIT Kerberos V KDC
#
# To make Kerberos start automatically at boot, make this
# file executable:  chmod 755 /etc/rc.d/rc.krb5
#

krb5_start() {
  if [ -x /usr/kerberos/sbin/krb5kdc -a -x /usr/kerberos/sbin/kadmind -a -r
/etc/krb5.conf -a -r /var/krb5kdc/kdc.conf ]; then
    echo "Starting Kerberos:  /usr/kerberos/sbin/krb5kdc"
    /usr/kerberos/sbin/krb5kdc
```

```
    echo "                  /usr/kerberos/sbin/kadmind"
    /usr/kerberos/sbin/kadmind
  fi
}

krb5_stop() {
  killall krb5kdc kadmind
}

krb5_restart() {
  krb5_stop
  sleep 2
  krb5_start
}

case "$1" in
'start')
  krb5_start
  ;;
'stop')
  krb5_stop
  ;;
'restart')
  krb5_restart
  ;;
*)
  # Default is "start", for backwards compatibility with previous
  # Slackware versions.  This may change to a 'usage' error someday.
  krb5_start
esac
```

8. Start KDC daemons:

```
# chmod +x /etc/rc.d/rc.krb5
# /etc/rc.d/rc.krb5 start
```

9. Remember to make the rc.krb5 script executable if you want the KDC to start automatically at boot. Verify connectivity to KDC with kadmin, kinit:

```
$ kinit krb5userprinc
$ klist
$ kadmin -p krb5adminprinc/admin
```

The Client

This procedure will result in a client capable of retrievving Kerberos tickets from a KDC and allow Kerberos principals to login at the console. Successful console login by a principal will generate tickets in the user's cache. Failed login by a principal (because the principal doesn't exist, or the wrong password was supplied) should fall through to local authentications (/etc/shadow). Note: the principal

must be associated with an account on the system, either in the local passwd database or via a network system such as NIS or LDAP.

1. Install krb5 always http://slackbuilds.org/repository/14.1/network/krb5/  . **2.** Setup /etc/krb5.conf: **krb5.conf**

```
[domain_realm]
        example.com = EXAMPLE.COM
        .example.com = EXAMPLE.COM

[libdefaults]
        default_realm = EXAMPLE.COM
        dns_kdc_lookup = true
        dns_realm_lookup = true
        forwardable = true
        renewable = true

[realms]

EXAMPLE.COM = {
            kdc = kerberos-1.example.com:88
            kdc = kerberos-2.example.com:88
            admin_server = kerberos-1.example.com:749
        }
```

3. Verify kadmin, kinit working

```
$ kinit krb5userprinc
$ klist
$ kadmin -p krb5adminprinc/admin
```

4. Add host principal, and extract host principal to /etc/krb5.keytab using kadmin and admin principal:

```
# kadmin -p krb5adminprinc/admin
kadmin: ank -randkey host/fully.qualified.domain.name
kadmin: xst -k /etc/krb5.keytab host/fully.qualified.domain.name
kadmin: quit
```

Sources

* Original source: https://www.canich.net/slackware/krb5.html * Contributions by User jamesaxl

howtos, network services, kerberizing slackware without pam