Instalar y configurar kerberos en Slackware sin PAM

El KDC

Este procedimiento dará lugar a un nuevo dominio de Kerberos. Si ya tiene acceso a un KDC de Kerberos, puede saltar a las partes del cliente y del servidor de aplicaciones. Además, el siguiente procedimiento es muy breve y no sustituye la lectura de la documentación suministrada en el paquete o en el sitio web de MIT Kerberos.

1. Instale krb (puede descargarlo y compilarlo desde http://slackbuilds.org/repository/14.1/network/krb5/)
2. Configure /etc/krb5.conf, /var/krb5kdc/kdc.conf y /var/krb5kdc/kadm5.acl. Estos archivos son ejemplos que debe ajustar después de leer la documentación de Kerberos.

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. Crear base de datos

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

4.Extraiga las claves del servidor de administración para /var/krb5kdc/kadm5.keytab.

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

5. Crear host y otros principios; extraer a /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.** Crear admin, usuarios principales
kadmin.local: ank krb5adminprinc/admin
kadmin.local: ank krb5userprinc
kadmin.local: quit
```

7. Crear script de inicio/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. Arrancar demonio KDC:

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

9. Recuerde hacer que el script rc.krb5 sea ejecutable si desea que el KDC se inicie automáticamente en el arranque. Verifique la conectividad a KDC con kadmin, kinit:

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

El Cliente

Este procedimiento dará como resultado un cliente capaz de recuperar tickets de Kerberos de un KDC y permitirá a los principales de Kerberos iniciar sesión en la consola. El inicio de sesión exitoso en la consola por parte de un principal generará tickets en el caché del usuario. El inicio de sesión fallido por parte de un principal (debido a que el principal no existe, o se proporcionó una contraseña incorrecta) debe corresponder a las autenticaciones locales (/ etc / shadow). Nota: el principal debe estar asociado con una cuenta en el sistema, ya sea en la base de datos local de passwd o mediante un sistema de red como NIS o LDAP.

1. Instalar krb5 siempre de 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. Verificar kadmin, kinit trabajando

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

4. Agregue el principal del host y extraiga el principal del host a /etc/krb5.keytab usando kadmin y el principal del administrador:

```
# 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
```

Fuentes

- Fuente original:http://arktur.shuttle.de/CD/Testpakete/Kerberos/krb5.html

- Contribuciones por User jamesaxl
- Traducido por: Victor 2019/02/15 19:29 (UTC)

howtos, network services, kerberizing slackware without pam