

Konfiguration des Servers unter Gentoo

Installation des Servers mit den richtigen Useflags:

```
emerge -va app-crypt/mit-krb5 # keyutils openldap pkinit threads
```

In LDAP die Schematas nicht vergessen zu aktivieren. Es gibt zwei Konfigurationsverzeichnisse:

```
/etc/krb5.*  
/var/lib/krb5kdc
```

Konfigdateien

krb5.conf

```
nano /etc/krb5.conf
```

```
[libdefaults]  
    default_realm = OSIT.CC  
  
[realms]  
# use "kdc = ..." if realm admins haven't put SRV records into DNS  
    OSIT.CC = {  
        kdc = itmgmt.osit.cc  
        admin_server = itmgmt.osit.cc  
    }  
  
#[domain_realm]  
#    mit.edu = ATHENA.MIT.EDU  
#    csail.mit.edu = CSAIL.MIT.EDU  
#    .ucsc.edu = CATS.UCSC.EDU  
  
[logging]  
#    kdc = CONSOLE
```

kdc.conf

```
nano /var/lib/krb5kdc/kdc.conf
```

```
[kdcdefaults]  
    kdc_ports = 750,88  
  
[realms]  
    OSIT.CC = {
```

```

        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/var/lib/krb5kdc/kadm5.keytab
        dict_file = /var/lib/krb5kdc/kadm5.dict
        acl_file = /var/lib/krb5kdc/kadm5.acl
#       key_stash_file = /var/lib/krb5kdc/.k5.OSIT.CC
#       master_key_name = /var/lib/krb5kdc/m-key
        kdc_ports = 750,88
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
    }

[logging]
    kdc = FILE:/var/log/krb5/kdc.log
    admin_server = FILE:/var/log/krb5/kadmin.log

[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        retain_after_close = false
        minimum_uid = 0
        try_first_pass = true
    }

```

kadm5.acl

```

*/admin@OSIT.CC *
*@OSIT.CC cil
*/*@OSIT.CC i

```

Um exklusivere ACLs zu gestalten kann man sich die Datei **kadm5.acl.example** zu Gemüte führen. Die Reihenfolge der Einträge ist wichtig. Genau wie bei den LDAP-ACLs wird die Suche nach dem ersten passenden Eintrag abgebrochen. Die erste Spalte gibt das Muster vor; die Berechtigungen ergeben sich aus den in der zweiten Spalte angegebenen Parametern; ***** bedeutet Vollzugriff, **cil** erlaubt z.B. Passwortänderungen (**c=change**), Auslesen der Principals und (**l=list**) und Datenbankabfragen (**i=info**). Die Admin-Principals haben in unserer Konfiguration Vollzugriff, User haben **cil**, und Services bzw. Hosts nur **i**.

Anlegen der Datenbank

```
kdb5_util create -r OSIT.CC -s
```

Das ganze dauert gut 5-8 Minuten, danach wird das Passwort festgelegt. Um das ganze nicht zu sehr zu verkomplizieren sollten wir hier das Passwort des LDAPadmins verwenden.

From:

<http://www.osit.cc/dokuwiki/> - **DEEPDOC.AT - enjoy your brain**

Permanent link:

http://www.osit.cc/dokuwiki/doku.php?id=kerberos_mit&rev=1417981046

Last update: **2025/11/29 22:06**

