

# 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. Im Verzeichnis **/var/lib/krb5kdc/** sollten jetzt folgende Dateien liegen:

```
-rw----- 1 root root 68 17. Nov 18:01 .k5.OSIT.CC
```

```
-rw-r--r-- 1 root root 0 9. Nov 17:37 .keep_app-crypt_mit-krb5-0
-rw-r--r-- 1 root root 46 10. Nov 00:04 kadm5.acl
-rw-r--r-- 1 root root 6310 9. Nov 22:53 kadm5.acl.example
-rw-r--r-- 1 root root 686 17. Nov 17:56 kdc.conf
-rw-r--r-- 1 root root 304 9. Nov 17:37 kdc.conf.example
-rw----- 1 root root 16384 17. Nov 18:41 principal
-rw----- 1 root root 8192 17. Nov 18:01 principal.kadm5
-rw----- 1 root root 0 17. Nov 18:01 principal.kadm5.lock
```

## Kerberos-Tools

Nun geht es zu erstellen der Principals. Dazu verwenden wir zunächst das Admin-Tool **kadmin.local**. Die Tools **kadmin** und **kadmin.local** sind von der Funktionalität identisch; allerdings greift **kadmin.local** direkt auf die KDC-Datenbank zu und benötigt selbst keine Kerberos-Authentifizierung (die zu diesem Zeitpunkt ja auch noch gar nicht in Funktion ist). Zur späteren, netzwerkweiten Verwaltung sollte **kadmin** verwendet werden.

```
kadmin.local
Authenticating as principal root/admin@OSIT.CC with password.
kadmin.local:
kadmin.local: ?
kadmin.local: addprinc root/admin
```

Hier haben wir nun den admin Principal angelegt, zur Verwaltung unserer Kerberos-Datenbank. Mit **getprincs** sieht man alle bestehenden. Da Kerberos alleine ja keinen Sinn macht, gehen wir gleich zur Verbindung mit LDAP weiter.

## Kerberos und LDAP

Um unseren LDAP in Verbindung mit SASLMech GSSAPI nutzen zu können, müssen wir Principals für die Hosts und die Services anlegen:

```
kadmin.local: addprinc -randkey itmgmt.osit.cc
```

Hier erfolgt keine Passwortabfrage, stattdessen wird ein Zufallsschlüssel generiert. Analog zum Host-Principal für Ldapmaster generieren wir einen weiteren für Ldapslave. Um min einen Service-Principal anzulegen (hier natürlich **ldap**), müssen wir auch den Host angeben, auf dem er läuft, also:

```
kadmin.local: addprinc -randkey ldap/itmgmt.osit.cc
```

In der gleichen Weise gehen wir vor für **ldap/ldapslave**, bevor wir **kadmin.local** per **exit**-Kommando verlassen.

From:

<https://www.deepdoc.at/dokuwiki/> - **DEEPDOC.AT - enjoy your brain**

Permanent link:

[https://www.deepdoc.at/dokuwiki/doku.php?id=kerberos\\_mit&rev=1417982398](https://www.deepdoc.at/dokuwiki/doku.php?id=kerberos_mit&rev=1417982398)

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

