Kerberos und Single Sign-On für Linux

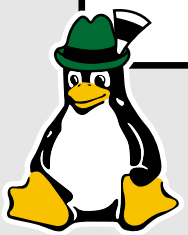
One account to rule them all

Sebastian 'tokkee' Harl
<sh@teamix.net>

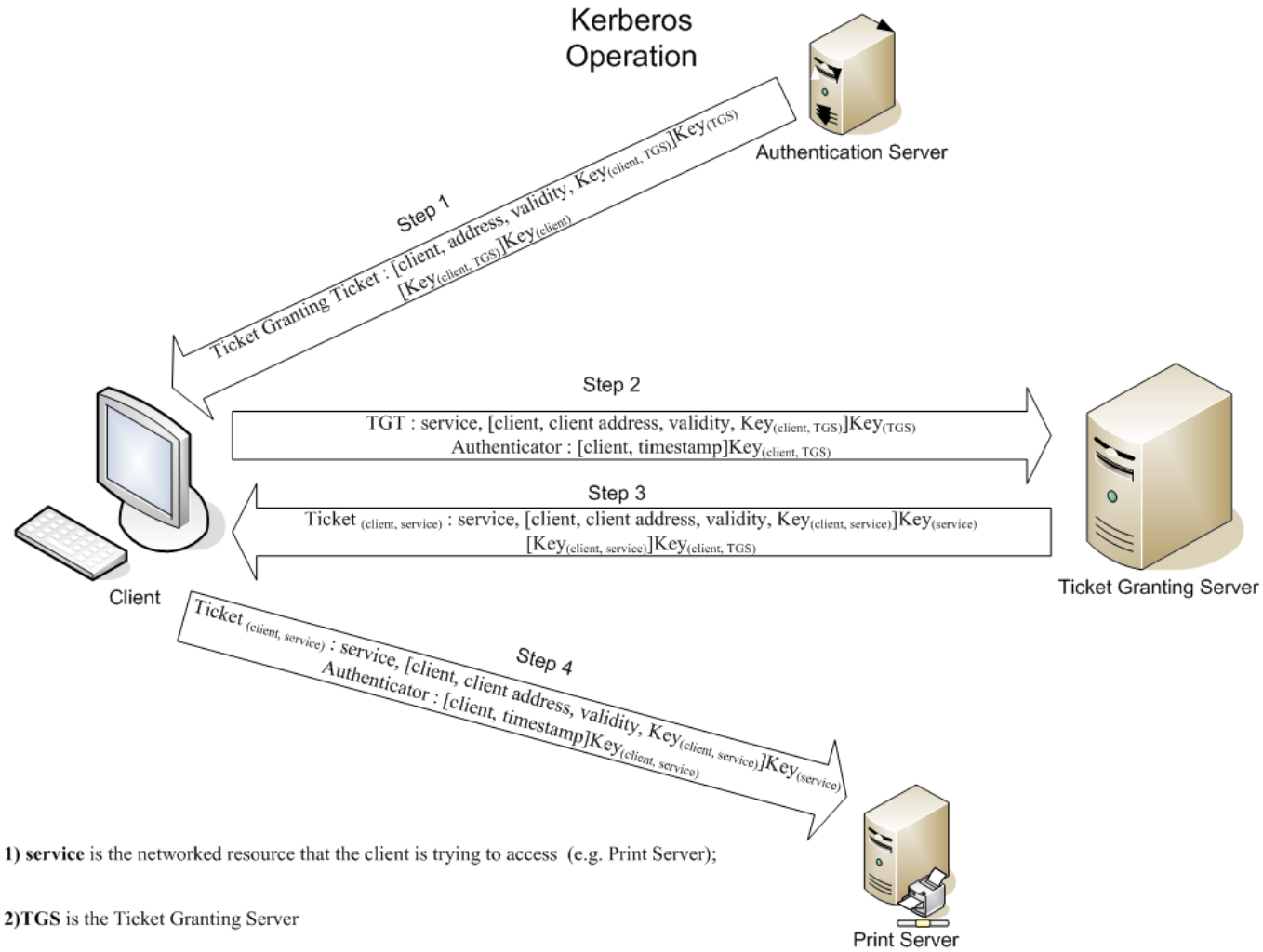
28. April 2012
Grazer Linuxtage

Kerberos: Überblick

- Sichere Authentifizierung über (unsichere) Netzwerke
- Zwei Varianten: MIT (Standard) und Heimdal
- Version 4 veraltet und sollte nicht mehr verwendet werden
- Zweiseitige Überprüfung der Authentizität
  (Client- und Server-seitig)
- Symmetrische Kryptographie mit "trusted third-party" (KDC)
- Auch zur Verschlüsselung und Verifizierung nutzbar
- Single-Sign-On
- Mittels GSS-API in beliebige Programme integrierbar
- `http://web.mit.edu/kerberos/`

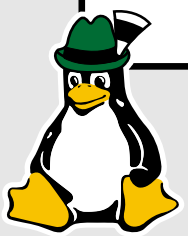


Kerberos: Funktionsweise



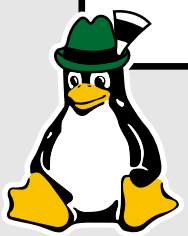
1) service is the networked resource that the client is trying to access (e.g. Print Server);

2)TGS is the Ticket Granting Server



Kerberos: Installation

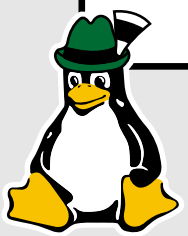
- In jeder Linux-Distribution enthalten
- Debian:
  `krb5-kdc`, `krb5-admin-server`, `krb5-user`, `libpam-krb5`
- SLES:
  `krb5`, `krb5-server`, `krb-client`, `pam_krb5`



Kerberos: KDC aufsetzen

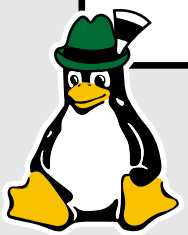
/etc/krb5kdc/kdc.conf (Debian)
/var/lib/kerberos/krb5kdc/kdc.conf (SUSE)

```
[kdcdefaults]
kdc_ports = 88

[realms]
TEAMIX.NET = {
    database_name = /var/lib/krb5kdc/principal
    admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
    acl_file = /etc/krb5kdc/kadm5.acl
    max_life = 10h 0m 0s
    max_renewable_life = 7d 0h 0m 0s
}

[logging]
kdc = FILE:/var/log/krb5/krb5kdc.log
admin_server = FILE:/var/log/krb5/kadmind.log
```



Kerberos: KDC aufsetzen (2)

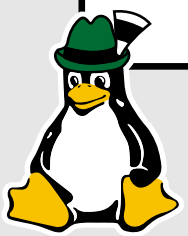
```
/etc/krb5kdc/kadm5.acl

*/admin@TEAMIX.NET
```



Kerberos konfigurieren

/etc/krb5.conf (Server und Client)

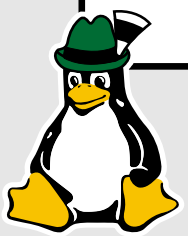
```
[libdefaults]
default_realm = TEAMIX.NET
ticket_lifetime = 24h
forwardable = true # SSH
allow_weak_crypto = true # NFS (Kernel < 2.6.35)

[realms]
TEAMIX.NET = {
    kdc = <IP>
    admin_server = <IP>
    default_domain = teamix.net
}

[domain_realm]
.site = TEAMIX.NET
site = TEAMIX.NET
```



Kerberos: PAM Client Konfiguration

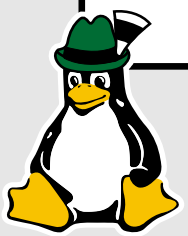
/etc/krb5.conf

```
[appdefaults]
pam = {
    ticket_lifetime = 1d
    renew_lifetime = 1d
    forwardable = true
    proxiable = true
    minimum_uid = 1
    external = sshd
    use_shmem = sshd
    clockskew = 300
}
```



Kerberos: KDC administrieren

- `# kdb5_util create -s`
- `# kadmin.local`
  `kadmin.local:  addprinc root/admin`
- `# service krb5-kdc start # krb5kdc auf SUSE`
  `# service krb5-admin-server start # kadmind auf SUSE`

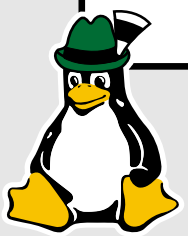


Kerberos: Wichtige Befehle

- `kadmin.local`, `kadmin`: Administration der Principal-DB
- `kinit`: TGT anfragen
  - `kinit -f`: weiterleitbares Ticket (z.B. SSH)
  - `kinit -R`: TGT erneuern
- `klist`: Liste aller Tickets des aktuellen Benutzers anzeigen
- `kdestroy`: Alle Tickets aus dem Cache löschen
- `kprop`: KDC-Replikation

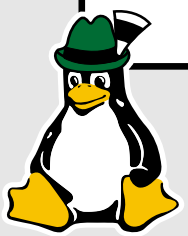
Troubleshooting:

- Meist DNS-Probleme
- ... oder Zeit-Synchronisation



Kerberos: PAM

- `/etc/pam.d/common-account`
  ```
  account sufficient pam_krb5.so use_first_pass
  ```
- `/etc/pam.d/common-auth`
  ```
  auth sufficient pam_krb5.so use_first_pass
  ```
- `/etc/pam.d/common-password`
  ```
  password sufficient pam_krb5.so
  ```
- `/etc/pam.d/common-session`
  ```
  session optional pam_krb5.so
  ```

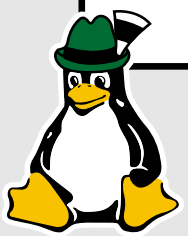


Kerberos: NFSv4

- Für NFS-Server und -Client:
  `kadmin: addprinc -randkey nfs/<FQDN>`
  `kadmin: ktadd -e des-cbc-crc:normal nfs/<FQDN>`
  (ab Linux 2.6.35 auch andere möglich)

- `/etc/default/nfs-common`
  `NEED_IDMAPD=yes`
  `NEED_GSSD=yes`
- `/etc/default/nfs-kernel-server`
  `NEED_SVCGSSD=yes`

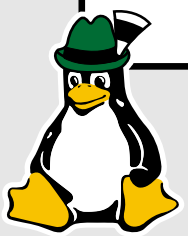
- `service nfs-common start`
  `service nfs-kernel-server start`



Kerberos: NFS sec Flavors

- `mount -t nfs4 -o sec=krb5p \`
  `$NFS_SERVER:/$PFAD $MNT_PT`

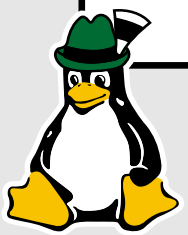
- `sys`: Zugriffsbeschränkung nur an Hand Client-IP (wie NFS3)
- `krb5`: Authentifizierung über Kerberos
- `krb5i`: Wie `krb5` mit Integritätscheck der Daten
- `krb5p`: Wie `krb5i` mit Verschlüsselung der übertragenen Daten



Kerberos: Benutzer-Zugriff auf NFS+KRB

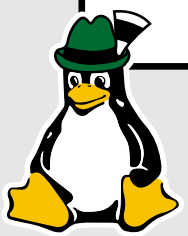
Jeder Benutzer, der auf einen kerberisierten NFS-Mount zugreifen möchte, muss ebenfalls am Kerberos authentifiziert sein.

- pam_krb5: TGT bei Anmeldung erhalten; quasi via SSO
- `kadmin: addprinc <USERNAME>`
- Client-seitig: `kinit` als entsprechender Benutzer
- **Wichtig:** das betrifft auch Webserver-Benutzer o.ä.
  - → Apache hat leider keine (mir bekannte) Möglichkeit, das zu automatisieren (→ Cron, o.ä.)



Kerberos: OpenSSH

- OpenSSH unterstützt GSSAPI seit Version 4.0
- `kadmin: addprinc -randkey host/<SSHD_HOST>`
  `kadmin: ktadd host/<SSHD_HOST>`
- `/etc/ssh/sshd_config`
  `GSSAPIAuthentication yes`
  `GSSAPICleanupCredentials yes`
- `# service ssh restart`
- `/etc/ssh/ssh_config`
  `GSSAPIAuthentication yes`
  `GSSAPIDelegateCredentials yes`

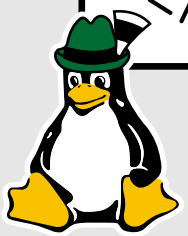


Kerberos: Apache

- Apache: mod-auth-kerb

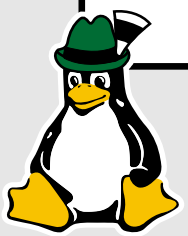
  → kadmin: addprinc -randkey HTTP/<FQDN>
  kadmin: ktadd -k /etc/apache2/krb5.keytab HTTP/<FQDN>

```
<Location ...>
    AuthType Kerberos
    AuthName "teamix SSO"
    KrbMethodNegotiate On
    KrbMethodK5Passwd On
    KrbAuthRealms TEAMIX.NET
    Krb5Keytab /etc/apache2/krb5.keytab
    KrbSaveCredentials On # -> CGI Scripts
    require user tokkee@TEAMIX.NET
</Location>
```



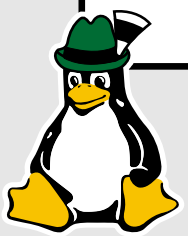
Kerberos: Apache und CGI

- Mit KrbSaveCredentials On werden die Auth-Credentials CGI-Skripten zur verfügung gestellt
- Zugriff:
  - $REMOTE_USER – Benutzername
  - $KRB5CCNAME – Credential-Cache



Kerberos: Firefox / Iceweasel

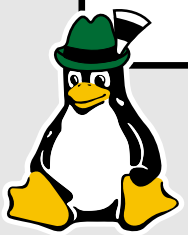
- Firefox: `about:config`
  `network.negotiate-auth.trusted-uris https://`
  `network.negotiate-auth.delegation-uris https://`



Kerberos: Subversion

- Subversion (HTTPS OOTB):
  `/.subversion/servers`

```
[global]
http-auth-types = Negotiate
```

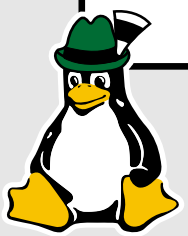


Kerberos & SSO

Vielen Dank für die Aufmerksamkeit!

Gibt es Fragen?

Kontakt:
Sebastian 'tokkee' Harl
<sh@teamix.net>

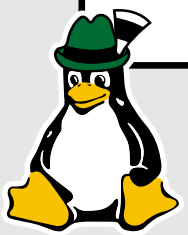


NetApp™: LDAP konfigurieren

Für NFS4 empfiehlt sich die Verwendung von LDAP (o.ä.), um eine zentrale Benutzerdatenbank auf allen beteiligten Systemen zu verwenden.

Konfiguration:

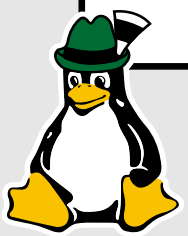
```
filer> options ldap
ldap.base               dc=teamix,dc=net
ldap.enable             on
ldap.name               cn=admin,dc=teamix,dc=net
ldap.passwd             ******
ldap.port               389
ldap.servers            172.21.254.1
```



NetApp™: LDAP verwenden

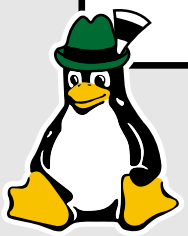
Kontrolle der Name Service Switch Konfiguration

```
filer> rdfile /etc/nsswitch.conf
passwd:    files    nis      ldap
netgroup:  files    nis      ldap
group:     files    nis      ldap
shadow:    files    nis
```



NetApp™: NFSv4 aktivieren

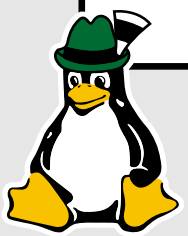
```
filer> options nfs.v4.enable on
filer> options nfs.v4.id.domain of.teamix.net
```



NetApp™: Kerberos aktivieren

KDC:

```
kadmin.local:  addprinc -randkey nfs/<FILER-FQDN>
kadmin.local:  ktadd -k krb5.keytab.filer
    -e des-cbc-crc:normal nfs/<FILER-FQDN>
# cp krb5.keytab.filer
/mnt/filer/etc/UNIX_krb5.keytab
# cp /etc/krb5.conf /mnt/filer/etc/krb5.conf
```



NetApp™: Kerberos aktivieren (2)

Filer:

```
filer> options nfs.kerberos.enable on
filer> nfs setup
Enable Kerberos for NFS? y
The filer supports these types of Kerberos Key Distribution Centers
(KDCs):
    1 - UNIX KDC
    2 - Microsoft Active Directory KDC
Enter the type of your KDC (1-2):  1
Enter the Kerberos realm name:  TEAMIX.NET
Enter the host instance of the NFS server principal name:  <FILER-FQDN>

NFS setup complete.
```