Seminar Betriebssystemdienste und Administration

Einrichtung eines Kerberos V Realms im ASG-Netz

David Tibbe
26.05.2005

Inhaltsübersicht

- Allgemeines
- Installation / Konfiguration
- Administration
- Bedienung und Demonstration

Single Sign-On (SSO)

- Benutzer soll sich einmalig authentifizieren
- weitere Authentifizierungen benutzertransparent
- Anforderungen an SSO:
  - Zentrale Administration
  - Benutzerfreundlich
  - Sicherheit

Kerberos

- Griechische Mythologie: Wächter der Unterwelt
- Authentifizierungsprotokoll
- entstand im Rahmen des „Athena“-Projekts des MIT
- Trusted Third Party Computing
- basiert auf symmetrischen Kryptographieverfahren
- Kerberos V5 in RFC 1510 von 1993 standardisiert

Kerberos Vokabular

Kerberos	gesamtes Netzwerksicherheitspaket
Service	jeder Rechner oder Dienst, auf den zugegriffen werden kann
Ticket	temporärer Ausweis für einen bestimmten Service
KDC	Key Distribution Center, Ticketvergabestelle
Realm	Netzwerk(bereich)
Principal	Kerberos-Benutzer (Dienst oder Person) primary/instance@REALM
TGT	Ticket-Granting Ticket

Ablauf einer Session

- Benutzer meldet sich am System an
- Login-Shell meldet Benutzer am KDC an und erhält TGT
- Sitzung, weitere (transparente) Ticketrequests
- Logout, Shell zerstört Tickets

Installation

- Debian-Packages
  - kdb5-kdc
  - krb5-admin-server
  - krb5-clients
  - krb5-doc
  - libpam-krb5
- Installation mittels apt

Konfiguration

- Alle kerberisierte Rechner benötigen krb5.conf
- Modifizierte Login-Shell
- Daemons eintragen
- KDC hat zusätzliche Konfigurationsdateien:
  - kdc.conf
  - kadm5.acl
  - dictionary

/etc/krb5.conf

```
[libdefaults]
        default_realm = ASG-PLATFORM.ORG
        default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
        default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
        dns_lookup_kdc = false
        dns_lookup_realm = false
[realms]
        ASG-PLATFORM.ORG = {
                kdc = seidel.asg-platform.org:88
                admin_server = seidel.asg-platform.org:749
                default_domain = asg-platform.org
        }
[domain_realm]
        .asg-platform.org = ASG-PLATFORM.ORG
         asg-platform.org = ASG-PLATFORM.ORG
[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log
```

/etc/krb5kdc/kdc.conf

```
[kdcdefaults]
        kdc_ports = 750,88
[realms]
        ASG-PLATFORM.ORG = {
                database_name = /var/lib/krb5kdc/principal
                admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
                acl_file = /etc/krb5kdc/kadm5.acl
                key_stash_file = /etc/krb5kdc/stash
                kdc_ports = 750,88
                max_life = 10h 0m 0s
                max_renewable_life = 7d 0h 0m 0s
                master_key_type = des3-hmac-sha1
                supported_enctypes = des3-hmac-sha1:normal
                                     des-cbc-crc:normal des:normal des:v4
                                     des:norealm des:onlyrealm des:afs3
                default_principal_flags = +preauth
        }
[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log
```

Konfiguration des KDCs

- Anlegen der Datenbank

```
root@seidel: kdb5_util –r ASG-PLATFORM.ORG create –s
kdb5_util: No such file or directory while getting active
    database to ,/var/krb5kdc/principal‘
Initializing Database ,/var/krb5kdc/principal‘ for realm
    ,ASG-PLATFORM.ORG‘
Master key name ,K/M@ASG-PLATFORM.ORG‘
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
root@seidel:
```

Konfiguration des KDCs

- Keytab für administrative Benutzer

```
root@seidel: kadmin.local
kadmin.local: ktadd -k /var/krb5kdc/kadm5.keytab
    kadmin/admin kadmin/changepw
Entry for principal kadmin/admin@ASG-PLATFORM.ORG with
    kvno 3, encryption type DES3-HMAC-SHA1 added to
    keytab
WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw@ASG-PLATFORM.ORG
    with kvno 3, encryption type DES3-HMAC-SHA1 added
    to keytab
WRFILE:/etc/krb5kdc/kadm5.keytab.
kadmin.local: quit
root@seidel:
```

Principals verwalten

- /usr/sbin/kadmin oder kadmin.local
  - listprincs, getprinc, addprinc, delprinc, modprinc
- Policies zur Vergabe von Richtlinien (max. Gültigkeit des Passworts, min. Anforderungen)
  - addpol, modpol, delpol

Beispiel (1/2)

```
dtibbe@grimshaw: /usr/sbin/kadmin
Authenticating as principal dtibbe/admin@ASG-PLATFORM.ORG
    with password.
Password for dtibbe/admin@ASG-PLATFORM.ORG:
kadmin: listprincs
K/M@ASG-PLATFORM.ORG
afs@ASG-PLATFORM.ORG
afsadm@ASG-PLATFORM.ORG
dtibbe/admin@ASG-PLATFORM.ORG
dtibbe@ASG-PLATFORM.ORG
krbtgt/ASG-PLATFORM.ORG@ASG-PLATFORM.ORG
host/grimshaw.asg-platform.org@ASG-PLATFORM.ORG
kadmin: addprinc foo
WARNING: no policy specified for foo@ASG-PLATFORM.ORG;
    defaulting to no policy
Enter password for principal "foo@ASG-PLATFORM.ORG":
Re-enter password for principal foo@ASG-PLATFORM.ORG:
Principal "foo@ASG-PLATFORM.ORG" created.
kadmin:
```

Beispiel (2/2)

```
kadmin: getprinc foo
Principal: foo@ASG-PLATFORM.ORG
Expiration date: [never]
Last password change: Wed May 25 13:17:44 CEST 2005
Password expiration date: [none]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed May 25 13:17:44 CEST 2005 (dtibbe/admin@ASG-
    PLATFORM.ORG)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 6
Key: vno 1, Triple DES cbc mode with HMAC/sha1, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Key: vno 1, DES cbc mode with RSA-MD5, Version 4
Key: vno 1, DES cbc mode with RSA-MD5, Version 5 - No Realm
Key: vno 1, DES cbc mode with RSA-MD5, Version 5 - Realm Only
Key: vno 1, DES cbc mode with RSA-MD5, AFS version 3
Attributes: REQUIRES_PRE_AUTH
Policy: [none]
kadmin: quit
dtibbe@grimshaw:
```

Clientprogramme

- Standardprogramme: rlogin, telnet, ftp…
- Kerberos-Programme
  - **`kinit`** fordert TGT an
  - **`klist`** listet Tickets auf
  - **`kdestroy`** löscht Ticketcache
  - **`kpasswd`** ändert Kerberos-Passwort

Wichtige Ticketarten

- forwardable — können weitergereicht werden
- postdated — Gültigkeitsbeginn in der Zukunft
- renewable — Anforderung neuer Tickets

kinit

- fordert TGT an
- **`kinit foo`** fordert Ticket für foo an
  - -f: forwardable Ticket
  - -l *Zeitausdruck*: Ticket mit beschränkter Gültigkeit
  - -S *service*: Ticket für *service* anfordern
- automatisch beim Login ausgeführt

klist, kdestroy, kpasswd

- klist listet aktuell gespeicherte Tickets auf
  - -e: zeigt Verschlüsselungstyp
  - -f: zeigt Flags
  - -k *filename*: liest Schlüssel aus Keytab aus
- kdestroy löscht alle vorhandenen Tickets
- kpasswd ändert Passwort

Beispiel (1/2)

```
Login: dtibbe
Password for dtibbe@ASG-PLATFORM.ORG:
dtibbe@grimshaw: klist
Ticket cache: FILE:/tmp/krb5cc_1071_wmV0uc
Default principal: dtibbe@ASG-PLATFORM.ORG
Valid starting     Expires            Service principal
05/25/05 15:46:38  05/26/05 01:46:38  krbtgt/ASG-
    PLATFORM.ORG@ASG-PLATFORM.ORG
Kerberos 4 ticket cache: /tmp/tkt1071
klist: You have no tickets cached
dtibbe@grimshaw: kdestroy
dtibbe@grimshaw: klist
klist: No credentials cache found (ticket cache
    FILE:/tmp/krb5cc_1071_wmV0uc)
Kerberos 4 ticket cache: /tmp/tkt1071
klist: You have no tickets cached
dtibbe@grimshaw:
```

Beispiel (2/2)

```
dtibbe@grimshaw: rlogin –x seidel
Trying krb4 rlogin...
krb_sendauth failed: You have no tickets cached
dtibbe@grimshaw: kinit
Password for dtibbe@ASG-PLATFORM.ORG:
dtibbe@grimshaw: klist
Ticket cache: FILE:/tmp/krb5cc_1071_Gu1mpS
Default principal: dtibbe@ASG-PLATFORM.ORG
Valid starting     Expires            Service principal
05/25/05 15:53:09  05/26/05 01:53:07  krbtgt/ASG-
    PLATFORM.ORG@ASG-PLATFORM.ORG
Kerberos 4 ticket cache: /tmp/tkt1071
klist: You have no tickets cached
dtibbe@grimshaw: rlogin –x seidel
dtibbe@seidel:
```

Weitere Features

- Cross-Realm Trusts
  - TGT aus Realm A wird als Authentifizierung für Realm B akzeptiert
- Slave-KDCs
- .k5login
  - gewährt Benutzern Zugriff auf eigenen Account
  - sudo-Ersatz
- .k5users
  - gewährt Benutzern Zugriff auf eigenen Account um ausgewählte Programme auszuführen

Zusammenfassung

- Kerberos ermöglicht umfangreiche Single-Sign-On-Umgebung
- zentrale Administration
- sichere Kommunikation im Netzwerk
- Nur Authentifizierung! Kerberos stellt keine Benutzerinformationen zur Verfügung
- relativ einfache Installation

Probleme und Hinweise

- Zeitsynchronisierung
- physische Sicherheit des KDCs
- Clients ohne Festplatte

- konsequente Umstellung aller Netzwerkdienste
- nicht alle Dienste haben kerberisierte Varianten
- beliebige Ticketanforderungen ohne preauth
- kein Import bestehender Nutzer

Quellen

- **MIT: Kerbero-Dokumentation**, http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/
- **Kerberos 5, Informationsbulletin**, DFN-CERT Zentrum für sichere Netzdienste GmbH http://www.dfn-cert.de/infoserv/dib/dib-2002-02-Kerberos5/Kerberos5-Bulletin.pdf
- **Wikipedia**: http://en.wikipedia.org/wiki/Kerberos_(protocol) http://de.wikipedia.org/wiki/Kerberos_(Informatik)
- **Kerberos-FAQ**: http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html
- **Single-Sign-on am Beispiel TFH Wildau,** Patrick Boettcher, Christian Frömmel: http://www.wi-bw.tfh-wildau.de/_pboettch/home/sso/