Heimdal-Integration in eine OpenAFS-Umgebung

Andreas Haupt
<andreas.haupt@desy.de>

Agenda

- Kerberosimplementation in OpenAFS
- Warum Kerberos5
- MIT vs. Heimdal
- Software / Konfiguration
- Migration

Kerberosimplementation in OpenAFS

- Basiert auf Kerberos4
- Implementation vor der Standardisierung
- Modifikationen:
  - String2Key Methode
  - Keine Adressverifikation von Tickets
  - TGT wird normalerweise verworfen

Kerberosimplementation in OpenAFS

- Weitere Besonderheiten:
  - Dynamisches Master- / Slavekonzept der Datenbankserver
  - Mehrere Principals im Ticket-Cache möglich
  - Automatisches Principallocking
  - Sperren von Principals für Administrator unmöglich

Warum Kerberos5

- Höhere Sicherheit:
  - Längere Schlüssel möglich
  - Preauthentication
  - String2Key-Methode
  - Replay Cache (nur MIT)

Warum Kerberos5

- Mehr Software Kerberos5-fähig (GSSAPI)
- Zusätzliche Features in Tickets:
  - Erneuerbare, weiterleitbare, vordatierbar
  - Längere Lebenszeiten

MIT vs. Heimdal

- Vorteile MIT:
  - Gute Dokumentation
  - Viele Features, die in Heimdal noch fehlen
  - Softwareunterstützung
- Nachteile MIT:
  - AFS Integration nur über Zusatzkit
  - Keine völlig freie Distribution

MIT vs. Heimdal

- Vorteile Heimdal:
  - Perfekt für die Integration in OpenAFS geeignet
  - Datenbankpropagierung in Echtzeit
- Nachteile Heimdal:
  - Spärliche Dokumentation
  - Fehlende Features

Migration

- Kompilation der nötigen Software
- Start Testserver / Initialisierung der Realm
- Funktionalitätschecks
- Konvertierung der AFS KA-Datenbank
- Konfiguration der Realm
- Paralleler Probebetrieb
- Abschaltung KA-Server

Software

- Kerberos4 Unterstützung in Heimdal / MIT
  - Abwärtskompatibilität
  - Für Heimdal KTH-Krb4 Bibliotheken nötig
- Heimdal gegen OpenSSL 0.9.6 binden

Software

- Administration durch Perlskripte
  - AFS Module von Norbert Grüner:
    - http://www.mpa-garching.mpg.de/~nog/perl/AFS-2.03.tar.gz
  - Heimdal::Kadm5:
    - ftp://ftp.su.se/pub/users/leifj/Heimdal-Kadm5-0.2.tar.gz
    - Viele Dinge funktionieren (noch) nicht

Software

- ARC:
  - Altes arc (CERN) benutzt Kerberos4
  - K5-arc von Alf Wachsmann funktioniert, aber Verschlüsselungsprobleme
  - Neuer Perl-SASL Server in Arbeit

Konfiguration der Realm

```
[libdefaults]
    default_realm = IFH.DE
    ticket_lifetime = 90000
    renew_lifetime = 2592000
    krb4_get_tickets = true
    forwardable = true
[realms]
    IFH.DE = {
        kdc = kdc1.ifh.de kdc2.ifh.de kdc3.ifh.de
        admin_server = kdc1.ifh.de
        kpasswd_server = kdc1.ifh.de
        default_domain = ifh.de
        v4_name_convert = {
            host = {
                rcmd = host
            }
        }
    }
[domain_realm]
    .ifh.de = IFH.DE
[kadmin]
    default_keys = v4 v5 afs3-salt:ifh.de
[kdc]
    enable-kerberos4 = true
    enable-kaserver = true
    enable-524 = true
    v4-realm = IFH.DE
```

Initialisierung der Realm

- Initialisierung:

  # kadmin -l init <REALM>

  # kadmin -l add testuser

- Testen des Principals

  # kinit testuser

  # klist

  Credentials cache: FILE:/tmp/krb5cc_0

  ....

Initialisierung der Realm

- Setzen eines Master Keys:

  # kstash

- Heimdalsync konvertiert AFS-Datenbank
  - Von Wolfgang Friebel (FTP Server)
  - Konvertierung mittels hprop
  - Vergleich mit kadmin -l dump
  - Änderungen in merge-Datei
  - kadmin -l merge <merge-Datei>

Konfiguration der Realm

- PAM:
  - pam_krb5afs (Version 1.3rc7) von Balazs Gal
  - kdm, ssh, Bildschirmschoner, ...
  - Auf Solaris teilweise mit Problemen
  - Probleme beim Binden mit statischen Bibliotheken (libtool)

Konfiguration der Realm

- OpenSSH:
  - Version 3.6.1p1 mit Patches (FTP Server)
    - Kerberos5/4, AFS über Protokoll 1
  - Version 3.7.1p2 ohne direkte AFS/Krb4 Unterstützung
    - GSSAPI über Protokoll 2
  - Automatisches Verteilen der host/<name> Principals

Konfiguration der Realm

- Ticket-/Tokenforwarding in OpenSSH bis Version 3.6.1p2:
  - /etc/ssh/sshd_config:

    KerberosAuthentication yes

    KerberosTgtPassing yes

    AFSTokenPassing yes
  - /etc/ssh/ssh_config

    KerberosAuthentication yes

    KerberosTgtPassing yes

    AFSTokenPassing yes

Konfiguration der Realm

- Ticketforwarding in OpenSSH ab 3.7:
  - /etc/ssh/sshd_config:

    GSSAPIAuthentication yes
  - /etc/ssh/ssh_config

    GSSAPIAuthentication yes

    GSSAPIDelegateCredentials yes
  - AFS-Token erneut aus TGT generieren (PAM?)

Konfiguration der Realm

- DNS:
  - Alias für KDC empfehlenswert
  - _kerberos.udp.IFH.DE. IN SRV 0 0 88 kdc1.ifh.de.
  - _kerberos.tcp.IFH.DE. IN SRV 0 0 88 kdc1.ifh.de.
- Router:
  - Port 88, 750, 4444 für die Welt öffnen

Migration

- Probebetrieb auf Nicht-AFS-Server (kdc, kadmind)
- Regelmäßiger Dump der KA-Datenbank
  - Problem: TGS-Key
- Umstellung Einzelner Hosts
  - krb5.conf, SSH, PAM

Migration

- Abschaltung KA-Server
  - kdc auf Testserver läuft weiter
- kdc, kadmind, ... unter bos-Aufsicht stellen
- Aliasnamen umhängen
- kdc auf Testserver abschalten

Zusammenfassung

- Kerberos5-fähige Dienste in IFH.DE
  - OpenSSH
  - IMAP (über SASL – GSSAPI)
  - VAMOS (Konfigurationstool)

Links

- Dieser Vortrag:
  - /afs/ifh.de/project/AFS/AFS-Workshop-2003/Talks/
- Meine Diplomarbeit:
  - http://www-zeuthen.desy.de/~ahaupt/OpenAFS-Heimdal-Integration.pdf
- Patches, etc.:
  - ftp://ftp.ifh.de/pub/unix/kerberos/

Abschluß

Vielen Dank für Ihre Aufmerksamkeit!