Alf Wachsmann
DESY Zeuthen
(alf@ifh.de)

Einführung von AFS-Home-Verzeichnissen im DESY Zeuthen – Konsequenzen für Nutzer

Inhalt

1. Motivation
   - Was AFS ist und wozu es gebraucht wird
   - Warum wir AFS-Home-Verzeichnisse einführen
2. Kerberos4
   - Warum ein zweites Paßwort benötigt wird
   - Handhabung von Tickets und Tokens
3. AFS
   - Zugriffskontrolle für AFS-Verzeichnisse
   - AFS-Home-Verzeichnisse
4. Wie es mit AFS im DESY Zeuthen weitergeht
5. Appendix
   - „Literatur“, Computer, Kommandos

Wozu AFS?

AFS (**A**ndrew **F**ile **S**ystem) ist ein weltweites File-System

Authentisierung mit

```
paris> klog alf@cern.ch
```

oder

```
paris> klog alf -cell cern.ch
```

Zugriffe:

```
paris> /afs/cern.ch/user/a/alf/bin/tstprogramm
paris> cp /afs/cern.ch/user/a/alf/private/src/hello.c ~/.
```

Organisationseinheit: **AFS-Zelle**; unsere heißt: `ifh.de`

Warum AFS-Home-Verzeichnisse?

- DFS ist noch nicht brauchbar
- die gesamte HEP-Geminschaft macht auf absehbare Zeit AFS
- weltweit eindeutiger Namensraum
- bessere Unterstützung der weltweit kooperierenden Physikergemeinde
- AFS+Kerberos4 ist performanter, zuverlässiger und viel sicherer als NFS+NIS
- wegen Linux haben wir sie sowieso schon
- u.a. im CERN und in DESY HH gibt es mittlerweile gute Erfahrungen
- Administration vereinfacht sich (z.B. Verlagern ist transparent)

Ein zweites Paßwort?!

Paßworte für UNIX (NIS) **und** für AFS (Kerberos4), aber wir haben eine **integrierte AFS-Umgebung**!

`kpasswd`, `passwd`, `yppasswd` ändern **beide** Paßworte
(`check_pass` zur Qualitätsüberprüfung)

Authentisierung erfolgt nun durch NIS **und** Kerberos4.

Deswegen wurden/werden alle Authentisierungsprogramme ausgetauscht:
`login`, `rsh`, `ssh`, `telnet`, `ftp`, `xdm`, `xlock`, ...

Tickets und Tokens I

Authentisierung gegenüber Kerberos erzeugt ein **Ticket Granting Ticket (TGT)** oder kurz **Ticket**.

Befehl: `kinit`.

Ein `klist` danach ergibt:

```
Ticket file:    /tmp/tkt2171
Principal:      alf@IFH.DE

  Issued           Expires          Principal
Sep 22 09:42:48  Sep 22 19:42:48  krbtgt.IFH.DE@IFH.DE
```

Ein Ticket alleine gibt noch keine AFS-Zugriffsberechtigung!

Tickets und Tokens II

Authorisierung für AFS erzeugt ein **Token**:
`afslog` erzeugt aus einem Ticket ein Token.
Ein `klist` danach ergibt:

```
Ticket file:    /tmp/tkt2171
Principal:      alf@IFH.DE

  Issued           Expires          Principal
Sep 22 09:42:48  Sep 22 19:42:48  krbtgt.IFH.DE@IFH.DE
Sep 22 09:47:05  Sep 22 19:47:05  afs@IFH.DE
```

Anzeigen von Tickets und Tokens geht auch mit `tokens`:

```
Tokens held by the Cache Manager:
User's (AFS ID 2171) tokens for afs@ifh.de [Expires Sep 22 19:47]
User alf's tokens for krbtgt.IFH.DE@ifh.de [Expires Sep 22 19:42]
   -End of list-
```

Tickets und Tokens III

- Mit einem Token kann auf AFS zugegriffen werden!
- Unsere integrierte AFS-Umgebung erzeugt Ticket **und** Token!
- Der Befehl `klog` erzeugt auch beides (anders als `kinit`)!
- Tickets und Tokens haben eine maximale **Lebensdauer** von 25 Stunden. Weil Tokens aus Tickets erzeugt werden, haben diese **höchstens** deren noch verbleibende Lebensdauer (erneuern mit `klog`).
- **Vernichten** von Tokens mit `unlog`,
  von Tickets und Tokens mit `kdestroy`.
- `ssh`-Tools geben Tickets und Tokens auf andere Rechner weiter (Ticket/Token-Forwarding).
- Abgelaufene Tickets oder Token verhindern das Funktionieren z.B. der `ssh`-Tools!

AFS-Zugriffsrechte: ACLs

ACL: **A**ccess **C**ontrol **L**ist

ACLs werden für ganze Verzeichnisse vergeben, nicht für einzelne Dateien.

Es gibt ACLs für Gruppen und für Nutzer.

Es gibt folgende Rechte:

r:	read	Dateien dürfen gelesen werden
l:	lookup	Inhalt des Verzeichnisses darf angesehen werden
i:	insert	neue Dateien dürfen angelegt werden
d:	delete	Dateien dürfen gelöscht werden
w:	write	Dateien dürfen verändert werden
k:	lock	Programm darf „flock“ auf Dateien machen
a:	administer	ACLs dürfen verändert werden

AFS-Zugriffsrechte: Gruppen I

Es gibt fest definierte System-Gruppen:

`system:anyuser`	jeder, auch ohne AFS-Account oder Token (weltweit!!)
`system:authuser`	jeder der eigenen Zelle mit Token
`system:administrators`	Systemadministratoren

Es gibt Gruppen von Computer-Nutzern:
Bei uns: `ifh-hosts` für alle Nutzer DESY Zn'er Rechner und
`desy-hosts` für alle Nutzer DESY HHer Rechner.
⇒ Alle Nutzer auf einem solchen Rechner, auch ohne Token, dürfen zugreifen.

Es gibt die bekannten (UNIX-)Gruppen:
`sysprog`, `theorie`, `l3`, `amanda`, ...
⇒ Authentisierte Mitglieder der Gruppe dürfen zugreifen.

AFS-Zugriffsrechte: Gruppen II

Ansehen der eigenen Gruppenzugehörigkeiten mit `pts membership <Account>`

Funktioniert nur für Nutzer mit Token und den eigenen Account!

`pts membership alf` ergibt:

```
Groups alf (id: 2171) is a member of:
  registry:registry
  tex
  system:administrators
  sysprog:sysprog
  www
  ftpadm
```

`pts membership pipke` ergibt:

```
Groups pipke (id: 1594) is a member of:
  rz
```

AFS-Zugriffsrechte: Ansehen

Ansehen der ACLs mit `fs la <Pfad>` (`la`: listacl)

`fs la /afs/ifh.de/user/a/alf` ergibt

```
Access list for /afs/ifh.de/user/a/alf is
Normal rights:
  ifh-hosts rl                          <- Nutzer auf DESY Zn'er Rechnern
  system:administrators rlidwka         <- Systemadmins
  sysprog:sysprog rl                    <- Gruppe des Nutzers
  system:anyuser l                      <- weltweit jeder
  alf rlidwka                           <- der Nutzer
```

`fs la /afs/ifh.de/user/a/alf/private` ergibt

```
Access list for /afs/ifh.de/user/a/alf/private is
Normal rights:
  alf rlidwka
```

AFS-Zugriffsrechte: Verändern

Ändern der ACLs mit `fs sa <Pfad> <ACLs>` (`sa`: setacl)

`fs sa . alf rl rz none`
erlaubt dem Nutzer `alf` das Lesen von Dateien und das Ansehen des Verzeichnisinhalts
und entzieht der Gruppe `rz` alle Rechte

Plattformabhängigkeiten

`@sys` wird abhängig vom Betriebssystem des Rechners aufgelöst (nur **im** AFS!!).
Der Wert von `@sys` ist abfragbar mit dem Befehl `sys`.

Bei uns gibt es zur Zeit: `hp700_ux90`, `hp_ux102`, `sgi_62`, `rs_aix41`, `sun4c_411`, `sun4m_412`, `sun4x_55`, `sun4x_56`, `i386_linux2`

Anwendung z.B.: Links der Form `bin -> @sys/bin`

AFS-Home-Verzeichnisse: Struktur

Für Nutzer `foobar` ist der Pfad: `/afs/ifh.de/user/f/foobar/`

Es gibt **Unterverzeichnisse** mit entpsrechenden ACLs:

`/afs/ifh.de/user/f/foobar/public/`

`/afs/ifh.de/user/f/foobar/<GROUP>/`

`/afs/ifh.de/user/f/foobar/private/`

`/afs/ifh.de/user/f/foobar/public/www/` WEB Home-Page des Nutzers

`/afs/ifh.de/user/f/foobar/.OldFiles/` „Backup“, nur Lesen möglich

`/afs/ifh.de/user/f/foobar/scripts/` system**un**abhängige Programme

Links

`/afs/ifh.de/user/f/foobar/bin -> .@sys/bin` system**ab**hängige Programme

`/afs/ifh.de/user/f/foobar/www ->`
`/afs/ifh.de/user/f/foobar/public/www`

AFS-Home-Verzeichnisse: Quota

AFS-Home-Verzeichnisse haben eine Quota von 50MB.

Anzeigen der Quota mit dem Befehl `fs lq <Pfad>` (`lq`: listquota)

`fs lq /afs/ifh.de/user/p/pipke` ergibt:

```
Volume Name          Quota    Used    % Used   Partition
user.pipke           50000    3775        8%         45%
```

Noch zu tun

- Politik und Werkzeuge zur Administration von AFS-Bereichen für die Experimente: Lösung vom CERN (10/98)
- volles Backup:
  - Variante 1: Lösung aus DESY HH wird angepaßt (11/98)
  - Variante 2: Legato Networker ist angesprochen worden
- Batchsysteme:
  - Codine: Genias wird eine Lösung liefern.
  - LoadLeveler: Lösung vom CERN (12/98?)
- WinNT-Nutzer:
  AFS-Integration wie in DESY HH oder CERN (12/98)
- Mac-Nutzer:
  Untersuchungen sind im Gange, evtl. Lösung vom CERN

Perspektiven

- AFS-Bereiche für die Experimente werden eingerichtet (11/98)
- erst wenn das Backup-Problem gelöst ist, wird für „normale“ Nutzer die Migration ins AFS begonnen (1/99?)
- vollständige Migration der Home-Verzeichnisse ins AFS ist angestrebt
- dezentrale AFS-Server (CERNer Erfahrungen abwarten, Lizenzproblem?!)

„Literatur“

- AFS at DESY Zn:
  `http://www.ifh.de/computing/services/AFS/AFS.html`
- AFS at DESY HH:
  `http://www.desy.de/~unix_adm/afs.html`
- AFS at CERN:
  `http://wsspinfo.cern.ch/file/afssp.html`
- CERN AFS User’s Guide:
  `http://wsspinfo.cern.ch/file/doc/afsug.html`
- AFS FAQs:
  `http://www.angelfire.com/hi/plutonic/afs-faq.html`
- AFS Beginner’s Guide:
  `http://www.alw.nih.gov/Docs/AFS/AFS_toc.html`

Computer

Computer am DESY Zeuthen **ohne** AFS: `sgi`, `orion`, `fdgsun`, alle nicht zentral administrierten LINUX-PCs