

Dipartimento di Matematica *"U.Dini"* Università degli Studi di Firenze

Alberto Mancini
mancini@math.unifi.it

June 3th 2009
AFS and Kerberos Best Practices Workshop 2009
Stanford University

The Dept.

“U.Dini”

Alberto Mancini

The Dept. “U.Dini” is the department of Math of the University of Firenze, Italy

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs



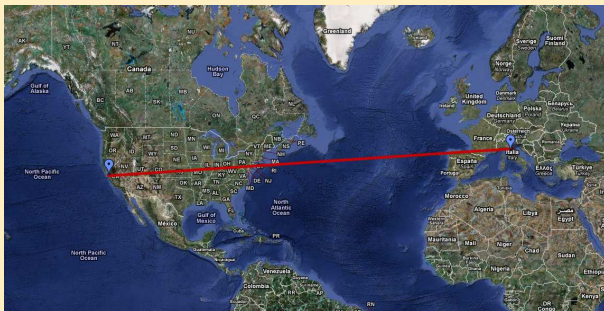
The Dept.

“U.Dini”

Alberto Mancini

The Dept. “U.Dini” is the department of Math of the University of Firenze, Italy

6k miles far from here



The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

a small Dept.

- \approx 50 faculty
- \approx 500 students (math and IT)
- \approx 500 former students
- a few (< 100) managed workstations
- 3 (tech) staff + some coworkers (students)
- provide "IT infrastructure" to 3 mathematical institutions and to part of the administration of the University.

around 2002

We switched to AFS/Kerberos (actually *AFS/Kerberos/LDAP*) a few years ago, moving from a setup essentially based on SaMBa, nis and nfs, looking for

- improved security
- access to resources from outside
- better manageability



xen dom0's

afs fileserver
afs dbserver
kdc + ldap

iSCSI
shared storage
afs
(internal)
cell
AliEn
grid node

private cell for "offices"

- 1 KDC (MIT)
- 2 OpenAFS filesystems
- 1 OpenAFS dbserver

- hosting administration's data;
- groups mimic administrative structure

masi@math.unifi.it

cell for our AliEn grid's node

- 1 KDC (MIT)
- 1 OpenAFS filesystems
- 1 OpenAFS dbserver

- testbed for KCA/pkinit
- currently **NOT USED** in production (issues with locking)

{gorini,masi,zaza}@math.unifi.it

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

Kerberos (in our experience)

"U.Dini"

Alberto Mancini

the Good

- integrates (quite) well
 - with our "captive portal" (through radius)
 - with our CMS (through apache's mod-auth-kerberos)
 - with linux's login (through pam)
 - with our cyrus (through saslauthd)
 - with (through)
- "slave" KDC works as expected

the Bad

- "trough"
sometime is a mess to handle authentication (mainly in webapps)
- a bit ... complicated
Kerberos/GSSAPI/SASL documentation sometime "helps"
- lack of expertise
it's hard to find commercial support at least, at our "budget level"

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

Shibboleth

We are currently testing the adoption of a *Shibboleth identity provider* to better integrate Kerberos auth. with webapps (and authorization through attributes).

- Seems the emerging standard
- Many (some) webapp ready
- Attributes from our LDAP directory

- addressing the problem of delegation of credentials (?)

... criticism is welcome !!

mancini@math.unifi.it, masi@math.unifi.it, zaza@math.unifi.it

OpenAFS (in our experience)

“U.Dini”

Alberto Mancini

the Good

- flexibility (volumes etc...)
- ACL's vs UNIX permissions
- volume replicas
- “CopyOnWrite” online backups
- ...

the Bad

- “users”
users find too complex the use of fs and vos
- granularity of permissions
e.g. volume's release
- (offline)backup
full dump of volumes once a week
- relation between mount points and volumes
our external db (ldap) rarely is coherent with the filesystem

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

OpenAFS (current investigation)

"U.Dini"

Alberto Mancini

We definitely need a web interface to storage.

- access without a client
- manipulation ACL's
- informations about backups and mountpoints
- managing volume's releases (eventually).

- filedrawers
- new application

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

OpenAFS (current investigation)

"U.Dini"

Alberto Mancini

We definitely need a web interface to storage.

- access without a client
- manipulation ACL's
- informations about backups and mountpoints
- managing volume's releases (eventually).

- filedrawers
 - available
 - many of the req. features

 - really complex
- new application

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

OpenAFS (current investigation)

"U.Dini"

Alberto Mancini

We definitely need a web interface to storage.

- access without a client
- manipulation ACL's
- informations about backups and mountpoints
- managing volume's releases (eventually).

- filedrawers
- new application
 - still using waklog
 - a few webservice (easy to maintain)
 - the whole app in javascript (tests done using extjs)

As a side effect of our tests we developed a tiny **php extension** to provide the functionality of fs (**pioctl**) and, we started to, providing some of the functionality of vos.

mancini@math.unifi.it, zaza@math.unifi.it

The Dept.

Briefly, Today

Kerberos

OpenAFS

nix/afs

nix repository over afs (plannig/preliminary tests)

- nix (<http://nixos.org>)

Nix is a purely functional package manager. It allows multiple versions of a package to be installed side-by-side, ensures that dependency specifications are complete, supports atomic upgrades and rollbacks, allows non-root users to install software

- openAFS

... common filespace ... replicated volumes ...

`maggese@math.unifi.it, mancini@math.unifi.it`

Thank you

Alberto Mancini (mancini@math.unifi.it)