Site Report

Plus Book Information

Wolfgang Gehrke
wgehrke@dia.uniroma3.it

Dipartimento di Informatica e Automazione
Università degli Studi Roma Tre

European AFS Workshop 2008

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Outline

1. From Foreign to Own Cell
2. Documented Experience
3. Actual Context
4. Security Considerations
5. Idea for Project
6. Summary

Outsourced Cell

users	260 (faculty, employees, guests)
groups	25 (those reflected in NIS)
volumes	360 (one per user)
AFS	Transarc ⇝ OpenAFS
AUTH	kaserver ⇝ Kerberos V
NSS	NIS remained over the years
OS	Unix ⇝ RedHat Enterprise
HW	Dell rack
GOAL	unite flavors of Unix

Main Requirements

Kerberos	centralized authentication
OpenLDAP	directory service
OpenAFS	file service with self triggered replication
servers	Linux on off-the-shelf servers
clients	Linux (SSO), Mac OS X and Windows (personal use)
one client	IBM 64bit PowerPC with 8 CPUs and 16GB
interest	distributed and parallel computing
use	laboratories with software distribution
also	support for exams

Homegrown Cell

users	220 (students)
groups	12 (those reflected in LDAP)
volumes	920 (4 per user: home, mail, web, profiles)
AFS	OpenAFS
AUTH	Kerberos V
NSS	OpenLDAP
OS	Debian stable (very convenient)
HW	Dell servers
GOAL	full control of the cell

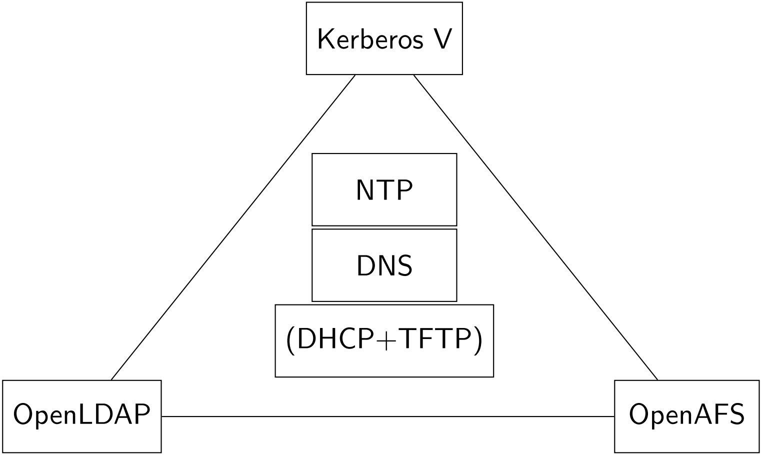
Book with Springer 2007

“Distributed Services with OpenAFS (for Enterprise and Education)” together with Franco Milicchio

(errata at http://www.dia.uniroma3.it/˜wgehrke/docs/errata.html)

- starts with basic services (NTP, DNS)
- explains briefly the theory of all services
- integrates web server, electronic mail, samba
- demonstrates Linux, Mac OS X, Windows clients
- shows application to clusters and laboratories
- extends to databases, DHCP, TFTP
- touches NFS, CVS, Jabber
- fault tolerance by service distribution

Rough Sketch



Rough Sketch continued

	Kerberos V	OpenLDAP	OpenAFS
SMTP relay	keytab sasl-authd	HOME, aliases	MAILDIR
IMAP	keytab courier-authd	HOME	MAILDIR
SAMBA	keytab	HOME user info	Profile
WWW	keytab mod-auth-kerb	HOME	UserDir, DAV

NOT to forget: OpenSSL

involved: symmetric key AND asymmetric key cryptography

Kerberos V

- master/slave
- MIT Kerberos used (better integration with Debian)
- via PAM for RADIUS (INN or wireless clients)
- OpenLDAP via SASL with GSSAPI
- direct integration in Apache and PostgreSQL
- more applications like OpenVPN
- Heimdal alternative
- PKINIT in the context of grid computing
- HX509 with PKCS11 support

LDAP

- sync replication

- OpenLDAP used
- source for name service switch (passwd, shadow, group)
- additionally for mail aliases
- storage for MAC addresses of hosts
- as database for Kerberos
- multi-master and dynamic configuration
- combination with further services like DHCP and DNS
- PKI certificate storage

OpenAFS

- volume replication
- WebDAV, Maildirs, Samba
- CVS, subversion
- @sys expansion
- backup scenarios
- cross-realm trust
- other OS for servers
- recent OS for clients
- debugging commands

Related Technologies

1. DCE/DFS open-sourced by The Open Group
2. NFS version 4 with Kerberos support
3. Microsoft's Dfs
4. Samba 4
5. self-certifying file-system
6. encrypted file-systems
7. Google file-system
8. Hadoop file-system
9. Lustre

Influence of Virtualization

- VMware with freeware versions
- XEN available in Debian, too
- VirtualBox acquired by SUN
- KVM with RedHat support

- XEN works for AFS clients
- possible for database servers
- maybe less suitable for file servers
- interesting in combination with iSCSI

General Aspects

NTP authentication key

DNS forward confirmed reverse DNS but weak point, clients could make use of LDAP

OS hardening

- internal firewall
- mandatory access controls
- intrusion detection and monitoring

Data Related

integrity	possible via ZFS
confidentiality	transmission weak point for the moment
availability	RO volume replication
access control	strong user authentication
full disk encryption	future for ZFS
user level encryption	try for example EncFS

OS Variety

OpenBSD minimalistic secure approach
could be used for database servers
comes with Arla client

OpenSolaris offers ZFS
could be used for file servers
e.g. Nexenta Core Platform close to Debian

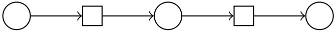
Other commercial alternatives

Distributed “Workflow” Engine

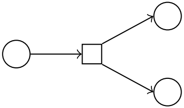
- inspired by workflows
- useful in the web context, too
- at our site: rather document flow
- event-based batch processing
- ideally to be distributed over several AFS Unix clients
- rule processing engine with overseer processes
- mutual exclusion with the help of file locking
- related theory: Petri nets

Workflow Patterns

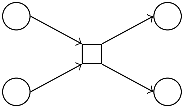
sequence



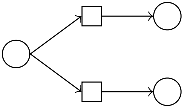
parallel split



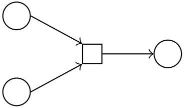
synchronization



exclusive choice



simple merge



Small Annoyances

- rapid Linux kernel development with API changes
- discussion on GPLv3
- `aklog -setpag`
- PAG garbage collection
- normal commands not ACL aware
- delay of propagating ACL change
- file mode bits
- firewall settings

Wish List

- full Kerberos V
- RW replication
- extended attributes and no directory limitations
- more than just one important keytab

- byte-range locks
- Unicode support for Windows
- native driver for Windows
- disconnected operation