Lisa2001 San Diego 2/12 - 7/12 2001

Alain van Hoof

Henry Jonkers

Raimond Kollman

Robert Jan Oosterloo

Rudi Engelbertink

Snow B.V.

Welcome

- Alain
  Large Installation System Administration
  Cfengine (workshop)

Welcome

- Alain
  Large Installation System Administration
  Cfengine (workshop)
- Henri

Welcome

- Alain
  Large Installation System Administration
  Cfengine (workshop)
- Henri
- Raimond
  (verhinderd)

Welcome

- Alain
  Large Installation System Administration
  Cfengine (workshop)
- Henri
- Raimond
  (verhinderd)
- Robert Jan
  Using Cryptography and Authentication for Mail Transport and Sendmail

Welcome

- Alain
  Large Installation System Administration
  Cfengine (workshop)
- Henri
- Raimond
  (verhinderd)
- Robert Jan
  Using Cryptography and Authentication for Mail Transport and Sendmail
- Rudi
  Advanced topics in DNS Administration

Alain van Hoof

- PAM (part of Linux System Administration tutorial)
- Cfengine (workshop)

Pluggable Authentication Modules

Is for example login program using PAM?

```
$ ldd /bin/login
....
libpam.so.0 => /lib/libpam.so.0 (0x40050000)
libpam\_misc.so.0 => /lib/libpam\_misc.so.0 (0x4005c000)
....
```

PAM modules are shared libs

/lib/security (Linux - RedHat)
/usr/lib/security (Solaris)
/etc/pam.conf (Solaris)
/etc/pam.d/<service> (Linux - RedHat)
example:
/etc/pam.d/login

```
auth  required /lib/security/pam_unix_auth.so
account  required /lib/security/pam_unix_account.so
password required /lib/security/pam_unix_passwd.so
session  required /lib/security/pam_unix_session.so

= Normal unix-like login
```

Extra Modules example 1

/etc/pam.d/login

```
auth        required    /lib/security/pam_unix_auth.so
auth        required    /lib/security/pam_nologin.so
account     required    /lib/security/pam_unix_account.so
password    required    /lib/security/pam_unix_passwd.so
session     required    /lib/security/pam_unix_session.so
```

If /etc/nologin exists only root is allowed to login, all users and root are shown the contents of /etc/nologin.

Extra Modules example 2

/etc/pam.d/passwd

```
auth     required /lib/security/pam_unix_auth.so likeauth nullok
account  required /lib/security/pam_unix_account.so
password required /lib/security/pam_cracklib.so retry=3
password required /lib/security/pam_unix_passwd.so nullok use_auth
session  required /lib/security/pam_unix_session.so
```

Only when cracklib can’t crack the new user-password the user password is changed.
Other ’interesting’ possibility: ldap-module

Cfengine

What is cfengine:

- Agent based configuration and maintenance
- Minimal user intervention
- Predictable, convergent behavior
- Keep things simple

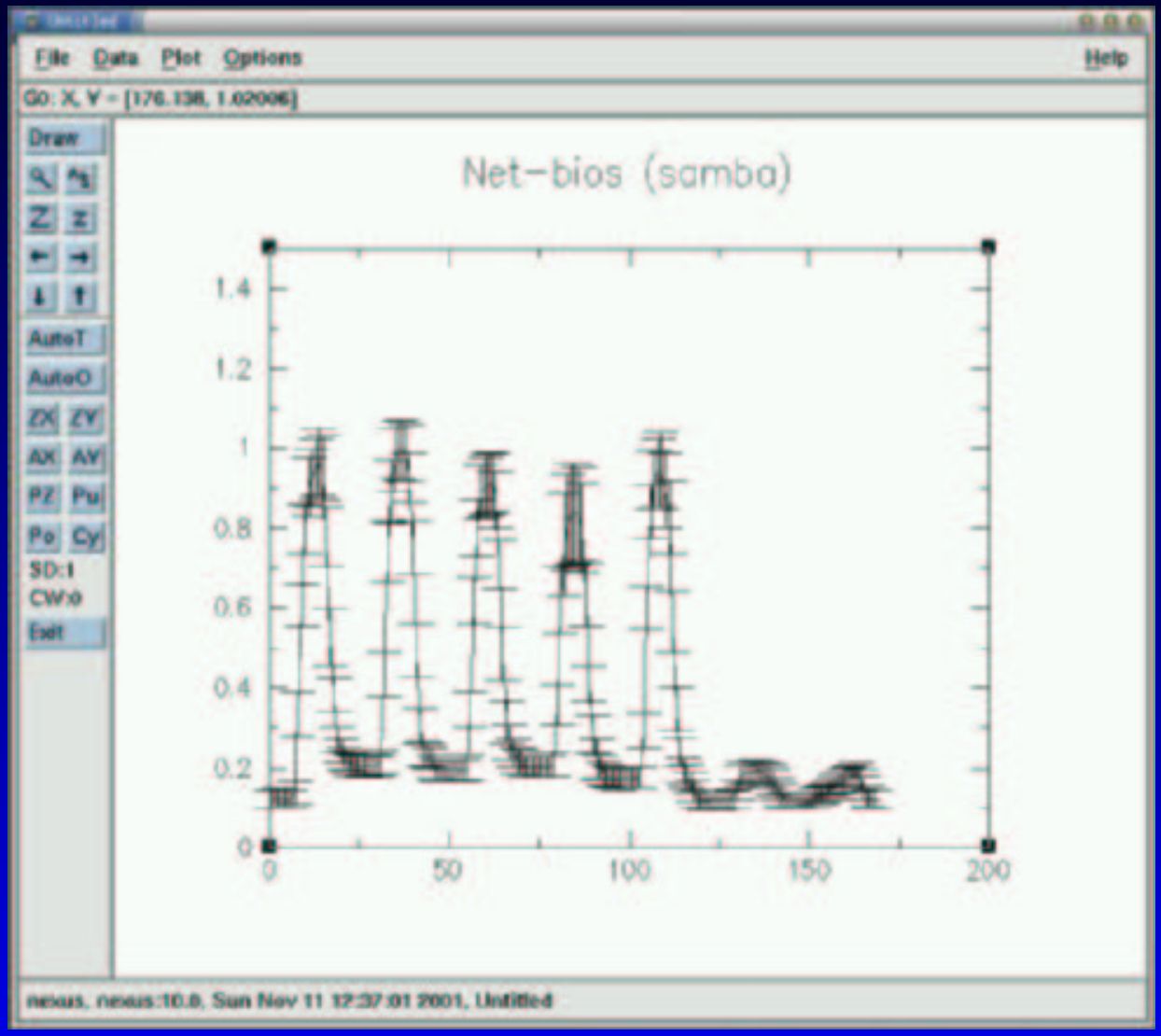
Cfengine

- New version 2.0 " almost there"(cfengine-2.0a16)
- Name changes of program and daemons
- New: Environment Daemon
- Gaming engine

Environment daemon 1

- Collects compressed statistics over months
- Just a few MB of data!
- Average and std-dev
- Sets classes and variables

Environment daemon 2



Environment daemon 3

- Paper and Lecture:
  - Simulation of User-Driven Computer Behavior
- Simulation of users using 8 different kind of user parameters.
- Output is number of processes running
- Use Real-life data to get correct parameter values (from environment daemon cfengine)
- Change parameter values of simulation to see "what happens if..."

Gaming engine 1

- Strategies (random)
- Probabilistic classes

```
strategies:
    OnTheHour::
            { spread_load
            percent_10: "1"    #  1/10
            percent_30: "3"    #  3/10
            percent_60: "6"    #  6/10
            }
```

Gaming engine 2

- Paper and Lecture:
  - Scheduling Partially Ordered Events in a Randomized Framework
- Conclusions:
  - Randomized schedules are more efficient
  - Difficult to identify the model = difficult to make predictions
- (security?)

Questions

- Questions?

Questions

- Questions?

- See also:

  PAM:
  http://www.us.kernel.org/pub/linux/libs/pam/
  http://www.sun.com/solaris/pam/

  Cfengine:
  http://www.cfengine.org

Robert Jan Oosterloo

Using Cryptography and Authentication for Mail Transport and Sendmail

Waarom authenticatie

- Waarom authenticatie voor versturen van mail?
- Misbruik van de mailserver als spamrelay
- MUA’s (Mail User Agents) en MTA’s (Mail Transfer Agents) moeten zich authenticeren bij de MTA voor doorsturen van mail.

Authentication

- Voor sendmail bestaat er vanaf versie 8.10 de AUTH extensie. (RFC 2554 "SMTP Service Extension for Authentication")
- Om dit te bereiken gebruikt Sendmail de SASL library. ("Simple Authentication and Security Layer").

SASL terminologie

- userid (authorization-id). Definieert permissies.
- authid (authenticatie-id). Definieert credentials.
- realm. Een groep users of systemen die binnen een zelfde authenticatie omgeving vallen.
- mechanism. Het authenticatie mechanisme wat gebruikt wordt.

SASL authenticatie

- KERBEROS_V4, Kerberos 5 (GSSAPI)
- PLAIN
- Shared secret (CRAM-MD5 en DIGEST-MD5)
  Opgeslagen in /etc/sasldb.db

Installatie Sendmail + SASL

- FreeBSD: sendmail-sasl, cyrus-sasl
- Debian/GNU Linux: sendmail, libsasl7, sasl-bin, libsasl-digestmd5

Configuratie SASL

- Via /usr/lib/sasl/appname.conf (bv. Sendmail.conf)
- Beschikbare opties:
- pwcheck_method (passwd, shadow, kerberos_v4, pam, sasldb, pwcheck, mysql, ldap) (Voor PLAIN authenticatie)
- auto_transition. Als een client met PLAIN inlogt, voeg toe aan sasldb.
- srvtab. Kerberos 4 keys.
- Aanmaken /etc/sasldb.db. Via saslpasswd commando.

Overzicht users

Overzicht users in /etc/sasldb.db

```
# sasldblistusers
user: jan   realm: mta-server mech: PLAIN
user: piet  realm: mta-server mech: DIGEST-MD5
user: klaas realm: mta-server mech: DIGEST-MD5
user: piet  realm: mta-server mech: PLAIN
user: piet  realm: mta-server mech: CRAM-MD5
user: klaas realm: mta-server mech: PLAIN
user: klaas realm: mta-server mech: CRAM-MD5
user: jan   realm: mta-server mech: CRAM-MD5
user: jan   realm: mta-server mech: DIGEST-MD5
```

Aanzetten AUTH in Sendmail

define(‘confAUTH_MECHANISMS’, ‘DIGEST-MD5 CRAM-MD5’)

TRUST_AUTH_MECH(‘DIGEST-MD5’)

Controleren AUTH

Telnet naar poort 25 van de mailserver.
Geef ’ehlo’ (Extended Hello) commando:

220 mta-server.mail.nl ESMTP Sendmail 8.12.1/8.12.1; Tue, 5 Feb 2002 21:08:42 +0100 (CET)
ehlo client
250-mta-server.mail.nl Hello klaas@client.mail.nl [192.168.0.2], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5 PLAIN
250-DELIVERBY

250 HELP

AUTH activeren (client)

Via de access map.
FEATURE(access_db, ‘hash -T<TMPF> /etc/mail/access’)
AuthInfo:mta-server.mail.nl "U:klaasP:password R:mta-server" "M:DIGEST-MD5"
Opletten, juiste realm gebruiken.

Voor de access map: makemap hash access < access

Client ondersteuning

Veel mail clients gebruiken een lege realm (Netscape/Eudora)

Henry Jonkers

Topics in UNIX and Linux System Administration

Policy and Politics

Types of Policies and Procedures

- User Policies
- SysAdmin Policies
- Emergencies
- Security Policies
- Hiring and Firing

User Policies

- Logins
- Acceptable
- Software
- Email
- Hacking

User Policy – Logins 1

- Who gets a login
  - Who decides
  - What happens when they leave
- Password Policy
  - Password Ageing
  - Teach your users to use good passwords
- Remote access
  - ssh only
  - telnet/ftp allowed ?
  - imap/pop without security allowed?

User Policy – Logins 2

- Sharing Accounts
  - No accountability, no way to actually know who is logged in
- Group Accounts
  - Also no accountability

User Policy – Logins 2

- Sharing Accounts
  - No accountability, no way to actually know who is logged in
- Group Accounts
  - Also no accountability
  - "root" is a groups account

User Policy – Acceptable Use

- Personal email OK?
- Web OK
  - Browsing for fun
  - Work use only
- Hacking
  - Cracking passwords
  - Breaking into other machines
  - Disrupting Service
- What are the conqequences of violating the acceptable use policy

User Policy – Software

- Supported vs. Unsupported
- Very hard to police
  - Especially on desktop systems
  - Requires a software audit to see what's there: Hmm, we paid for 3 copies of Reflection but we seem to have it installed on 300 machines

User Policies – Email

- SPAM
  - Incoming; Filter at mail gateway, let users filter for themselves
  - Outgoing; A problem for ISP's
- Attachment and viruses
  - Instructions to users not to open attachments from strangers (Just doesn't work)
  - Filter attachments and refuse them at mail gateway. Types .vba .dot .exe .com .reg are suspect Return mail with message saying why you rejected it

System Administrator Policies 1

- Sysadmin policy – root access
- Need "su" to do their job
- Allows access to all data
  - Allows access to log files and accounting data that might record inappropriate use
- sudo, super, run as alternatives to "su" or logging in as root

System Administrator Policies 2

- Limited "su" via sudo program from University of Colorado
  - ftp from ftp.cs.colorado.edu in pub/sysadmin/utilities
  - Allows fine grain conrol of root privileges:
    1 per user
    2 per host
    3 per command and its arguments
  - Logs all uses via syslog

System Administrator Policies 3

- Backups
  - Often data IS the company's assets where are backup tapes stored safe from physical harm, flood, earthquake, fire etc safe from malicious harm, disgruntled employee, competitor, terrorists
- Purchasing Policies
  - Are sysadmins invlolved in the purchasing process
  - They need to be with a veto power
  - List of supported hardware/software
  - End of life policy
- Maintenance Policy
  - Vendor contracts or third party maintenance

Emergencies 1

- Catastrophe vs. attack vs. sysadmin on vacation
- Offline Documentation
  - Telephone numbers: Staff Hardware support Software support CERT – Computer Emergency Response Team
  - Machine Configurations Disk partitions Boot procedures Locations
  - Backups Location of backup tapes Dump sequence, dump dates

Emergencies 2

- Backup/failover machines, data centers
  - WTC disaster tested everyones Y2K preparations
  - Mostly worked fine
  - Example: Morgan Stanley's data center was in WTC. Backup 10 miles away Failed over fine, a bit of trouble keeping up with volume once market opened
- In real emergency sysadmins must have dictorial powers
  - to shut down machines
  - To disconnect from networks
  - To kill running programms

Emergencies 3

- Who is in charge
  - Need chain of command, known and agreed to before emergency occurs
  - Dealing with media; Don’t especially if emergency is occurring in real time Good job for a boss type person
- What is an emergency
  - Definition depends on your site
  - Usually includes:
    - 1 Threat to data stored at site
    - 2 Unauthorized use of computing resources at site
    - 3 Impersonating your site
  - Natural disasters

Security Policy/Procedures

- Everyday hygiene
  - All accounts with passwords
  - Run security monitoring tools (cops, tripwire, snort)
  - Actually read reports they generate
  - Monitor machines that have network packet filters installed very carefully
- Don’t assume that a firewall at your router will protect you
  - Make each hosts secure, shutdown services
  - Use good password programm
  - Remove inactive accounts
  - Don’t allow guest accounts with no password or password "guest"

Hiring, Firing, Training

- Who to hire
  - Experienced sysadmins
  - Beginners and grow them
- Evaluation schemes
  - Self evaluation, scale 1 (never heard of it) to scale 5 (could teach it)
  - technical evaluation
  - Include bogus questions
- Listen very carefully to former employers and other references
- Fire early, during initial trial period if possible – it’s easy then