All status report

Luis Fernando Muñoz Mejías

Universidad Autónoma de Madrid

6th Quattor Workshop
NIKHEF, 10/2008

Outline

1. News since last workshop

2. The future
   - A solution for DHCP
   - New features

Stabilization

- Lots of feedback from users
    - Thanks!!
- Plenty of bug fixes
- New hooks
    - Anaconda hooks
        - For Kickstart
    - NBP hooks
        - For status changes

User hooks

- Many contributions, you may find something interesting on CVS

Tainted mode

- Nobody complained
- Ill-formed profiles won't force AII to do unexpected things
- Tainted mode doesn't protect against everything
    - We might be vulnerable to symlink attacks
    - We'll switch to use `CAF::FileWriter`.

User complains

- Filesystem creation is slow

    - I'm working on it, there will be news after 1.4 is out.

- aii-dhcp still around

    - Performs DNS requests instead of checking the profile
    - Fetches a profile, anyways
    - Slows down aii-shellfe
    - Doesn't fit with v2's philosophy

Outline

aii-dhcp or ncm-dhcp?

- aii-dhcp configures a daemon
  - That's what NCM components do
- DHCP can be used for assigning IPs to nodes not managed by Quattor
  - Currently, we edit the configuration by hand
- The Quattor server would be managed by itself
  - Chicken-egg problem?

Outline

Dropping privileges

- AII runs user-provided code
    - There may be security flaws in it
- There is no real need for AII running as root
    - We can work out the edition of /etc/dhcpd.conf
- Avoids apache user having to use sudo on aii-installack.cgi
- Makes it easier to develop a SELinux policy for AII
    - Anyone tried to write a SELinux policy that allows sudo?

Dropping privileges
Technical proposal

- aii-shellfe running as user aii, group aii
- /osinstall owned by aii:aii
- apache user member of aii group
- aii group allowed to write only to /osinstall/nbp/pxelinux.cfg
- sudo used at most to restart dhcpd
  - No need for a SELinux policy in this case

Dropping privileges
Additional requirements

- Upgrade must be transparent
  - User should only edit /etc/sudoers
- RPM scripts must set all permissions

Thanks to...

In alphabetical order:

- Stijn De Weirdt
- David Groepp
- Michel Jouvin
- Marco Emilio Poleggi
- Ronald Starink
- Serge Vrijaldenhoven