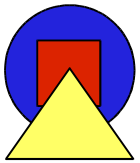
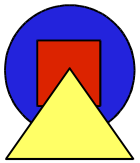


5 Things to make Cluster Security the least of your worries

Alf Wachsmann

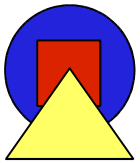
Stanford Linear Accelerator Center

alfw@slac.stanford.edu



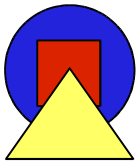
5 Things

1) Automated System Installation and Administration
2) Emergency Script
3) Patch System
4) Batch Queue for System Administration
5) Structural Design



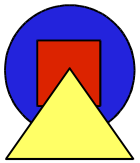
Introduction

- recommendations are not much different for clusters than for desktops or servers
- only 4) Batch Queue is cluster specific



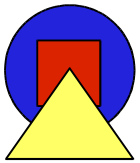
Automation

- have a consistent and automated way for
  - installing the OS on your machines
  - performing the post-installation on your newly installed machines
  - doing your daily system administration tasks on your machines
- do NOT build on cluster specific tools like OSCAR
- extend what you do on desktops/servers to your cluster or
- start with your cluster and extend tools to desktops/servers
- possible tool: cfengine (http://www.cfengine.org)



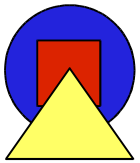
Emergency Script

- set up a light weight system that runs at least once an hour on all your machines to perform tasks in an emergency situation
- under normal conditions, this does nothing at all
- can call your automation or patch tool if necessary
- at SLAC: empty shell script in heavily cloned AFS volume called by cron



Patch System

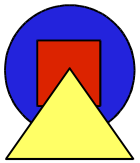
- have a tool that allows for easy patching of all your machines
- be consistent (i.e., don't miss a machine!)
- reboot after glibc or kernel patches (see next slide)
- possible tool for Linux: autorpm (http://www.autorpm.org)



Batch Queue

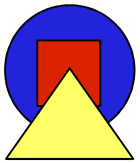
- set up a
  - highest priority
  - non-preemtable
  - non-preemptive

  queue in your batch queueing system to patch and reboot your cluster machines **without** interfering with other batch jobs
- user of that queue needs to execute jobs as `root` (at SLAC: user `lsf` with password-less `sudo` privs)
- this is biggest difference to desktops/servers!
- Sun GridEngine (http://www.sun.com/software/gridware), PBS, Condor, LSF, ...



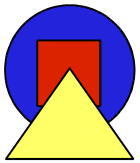
Structural Design

- put your cluster in the "Internet Free Zone" (IFZ) or in a private (non-routable) subnet.
  GRID is wrong here!
- don't allow users to logon to your cluster machines – use batch instead
- install as little software as possible on your cluster nodes
- run as little services/daemons as possible



References

- Book with general ideas how to run a datacenter:
  The Practice of System and Network Administration
  by Thomas A. Limoncelli and Christine Hogan
- Book about why computers need administration:
  Principles of Network and System Administration
  by Mark Burgess
- Book with ideas how to automate things:
  Automating Unix and Linux Administration
  by Kirk Bauer



5 Things

1) Automated System Installation and Administration
2) Emergency Script
3) Patch System
4) Batch Queue for System Administration
5) Structural Design