



# Lxadm – secure admin cluster

---

Miroslav Siket  
CERN IT-FIO/FS  
(Working proposal)



# Outline

---

- Motivation
- Securing the Lxadm cluster
- Moving towards secure fabric management
- Interoperability
- Deployment outline



# Motivation

---

- Need for a secure working environment
- Restricted access
- Limit impact of breakings
- Centralized and isolated availability of the fabric administration tools
- Software audit



# Securing the lxadm cluster

---

- Running only sshd, restrict other network daemons
- No afs (avoid unwanted software dist...)
- No kerberos login (avoid stealing admin's ticket)
- Only secure connection from registered networks
- Firewall – protection from outside and inside
- Fast security updates, extensive monitoring
- Local passwords?
- Secure applications only (no suid,...)
- Restricted root access – only FIO security people?
- No general users



# Secure fabric management

---

- All SMS and FIO admin tools to be moved to lxadm cluster:
  - PrepareInstall, aims registration,...
  - Sms/leaf tools
  - Fio tools like cluster\_update,...
- Cdbop and configuration manipulation
- Centralize fabric software
- Root access only from this cluster to other clusters
- Wssh, ...



# Interoperability

---

- To have secure administration we have to secure connected servers as well and connection to them – f.e.:
  - Lxconf
  - Linuxsoft
  - Aims
  - Lxservb\*
  - Lsf masters
  - Access to cdbsql write access
  - Root passwords and sensitive information handling



# Deployment

---

- Currently we have 2 machines – lxadm01 and lxadm02 – ssh access only, will create local users that need access and remove afs connection
- Iptables for firewall in place
- Start deploying all rpm based tools now - request for rpms for other tools...
- Secure communication between the lxadm and other servers – separate sshd instance for root only access – firewalled
- Secure communication between the lxadm and administration clusters
- Remove tools from publicly available clusters (like lxplus)
- Secure notification mechanism (notd) – firewall



# Conclusion

---

- Advantages:
  - Easier to secure one cluster than multiple of machines
  - Centralized administration – software/access
  - Limiting the impact of the possible breakings
  - Secure environment/control
  - Fast action possible – f.e. in kernel upgrades
  
- Disadvantages:
  - Machines will become critical – we need 2 at all times
  - More exposed to attacks – more attractive for attackers
  - One more cluster to manage...