Security in TB management

Louis Poncet
System Engineer SA3 - OSCT

Information Society

Summary

- Introduction
- Current map (CESGA and INFN in reinstallation)
- Os installation
- Staying Up-to-date
- Firewalls
  - Host
  - Network
- Security test
- Log files
- Tools
- Conclusion

Introduction

- Distributed testbed sites are not protect on our GRID (the testing and certification one)
- We are running uncertified middleware our risk of security hole is higher than in PPS or PROD
- We are owner of dteam access the “biggest” VO
- All security policies of your computing centre need to be apply also on the testbed

The current testbed

In Reinstallation

INFN (LSF)

CESGA

CY-02-CYGRID-CERT

bdii201.grid.ucy.ac.cy:2170/bdii-site
httpg://se201.grid.ucy.ac.cy:8443/srm/managerv1
ce201.grid.ucy.ac.cy
wmslb201.grid.ucy.ac.cy:7772
se201.grid.ucy.ac.cy
httpg://se201.grid.ucy.ac.cy:8446/srm/managerv2

CERN TB 1A

lxb2018.cern.ch
http://lxb1941.cern.ch:8085/
lxb1941.cern.ch
lxb2020.cern.ch:7512
lxb2016.cern.ch:7772
httpg://lxb1921.cern.ch:8443/srm/managerv1
httpg://lxb1921.cern.ch:8446/srm/managerv2

DESYCERTTP

httpg://cork.desy.de:8443/srm/managerv2
httpg://swords.desy.de:8443/srm/managerv1
httpg://dublin.desy.de:8443/srm/managerv1
httpg://dublin.desy.de:8443/srm/managerv2
httpg://cork.desy.de:8443/srm/managerv1

CERN TB 1B

https://lxb2054.cern.ch:7443/glite_wms...
httpg://lxb1917.cern.ch:8443/srm/managerv1
http://lxb1401.cern.ch:8085/
https://lxb2054.cern.ch:9003/lb
httpg://lxb1917.cern.ch:8446/srm/managerv2
lxb2034.cern.ch
lxb2034.cern.ch:2170/bdii-site

PIC-SA3

vce02.pic.es
vce01.pic.es
gsissh://voboxsa3.pic.es:1975
site-bdii-sa3.pic.es:2170/bdii-site

Os installation

- **Kickstart installation; default network install for SLX**
  - Minimal set of packages depending of the node type
  - Minimal for core services hosts (apt/yum will install what is really require)
- **Partitioning on the HD(s)**
- **Network settings configuration of network devices**
- **A “keep certificate and server ssh keys” process in the kickstart can be implemented using a RAM disk**
- **Removing all unused services and tools**
- **Setting of SSH and extra repositories for internal tools**
  - Periodic reinstallation is a good idea
- **Installation of tools for security and testing (for internal repository)**

Our Kickstart

```
<...>
#Root password
rootpw --iscrypted *NP*
authconfig --enableshadow --enablemd5
<...>
#Firewall configuration
firewall --enabled --ssh
<...>
#Package install information
%packages --resolvedeps
@ base
#@ Administration Tools
@ System Tools
#@ development-tools
#@ text-internet
#emacs
#XFree86-xauth
ntp
<...>
%pre
mkdir -p /tmp/preserve
mkdir -p /tmp/fs
for I in 1 2 3
do
   L=`e2label /dev/sda$I`
   if [ ""$L = "/" ]
   then
      mount /dev/sda$I /tmp/fs
   fi
done

if [ -f /tmp/fs/etc/grid-security/hostcert.pem ]; then
    cp /tmp/fs/etc/grid-security/host*.pem /tmp/preserve
fi


if [ -f /tmp/fs/etc/ssh/ssh_host_key ]; then
    cp /tmp/fs/etc/ssh/ssh_host_* /tmp/preserve
fi

cd /
umount /tmp/fs
<...>
```

```
<...>
# Removing unwanted packages from Base install
chroot /mnt/sysimage /usr/bin/yum -y remove acpid apmd
aspell aspell-en bind-libs bind-utils bluez-bluefw bluez-
hcidump bluez-libs bluez-utils cr
yptsetup cups cups-libs curl cyrus-sasl-plain desktop-
file-utils fontconfig freetype ftp htmlview indexhtml
ipsec-tools ipw2100-firmware ipw2200-
firmware irda-utils isdn4k-utils jpackage-utils jwhois
lftp lha libgcrypt libgpg-error libidn libjpeg libpcap
libpng libtiff libwvstreams libxslt
 lrzsz minicom mtr mt-st NetworkManager nfs-utils nfs-
utils-lib nss_ldap numactl parted pcmcia-cs pdksh perl-
AppConfig-caf pinfo portmap ppp redh
at-lsb redhat-menus rp-pppoe rsync stunnel system-config-
network-tui system-config-securitylevel-tui tcpdump
unix2dos wireless-tools words wvdial
 xinetd xmlsec1 xmlsec1-openssl xorg-x11-libs xorg-x11-
Mesa-libGL ypbind yp-tools perl-CAF
<...>
#Security repository
echo "[GD Security]" >> /mnt/sysimage/etc/yum.repos.d/gd-
security.repo
echo "name=GD Security" >> /mnt/sysimage/etc/yum.repos.d/
gd-security.repo
echo "baseurl=http://grid-deployment.web.cern.ch/grid-
deployment/gis/apt/security/sl3/en/i386" >> /mnt/
sysimage/etc/yum.repos.d/gd-security.repo
echo "enabled=1" >> /mnt/sysimage/etc/yum.repos.d/gd-
security.repo
echo "" >> /mnt/sysimage/etc/yum.repos.d/gd-security.repo
<...>
# SSH
echo "PermitRootLogin without-password" >> /mnt/sysimage/
etc/ssh/sshd_config
echo "Protocol 2" >> /mnt/sysimage/etc/ssh/sshd_config
```

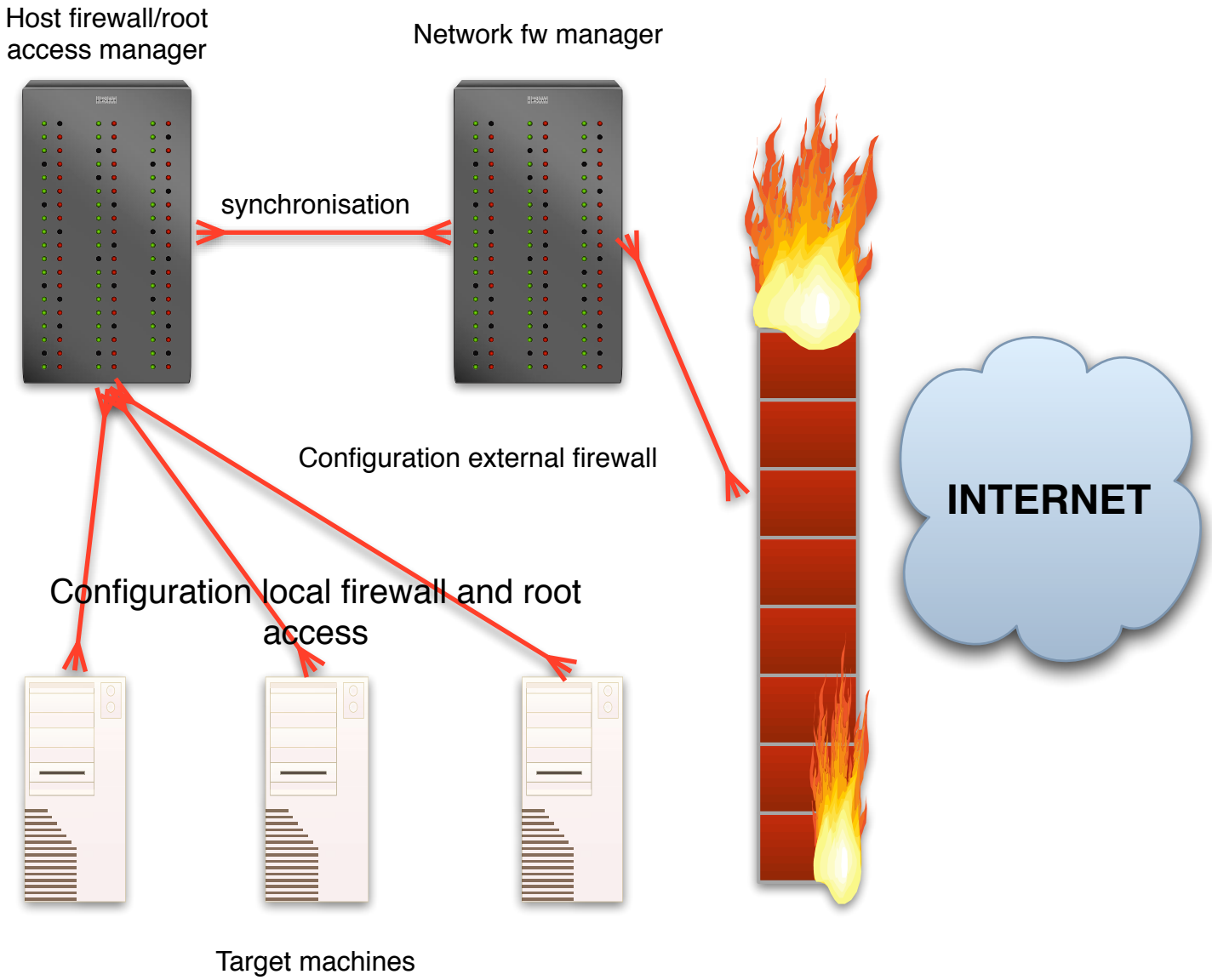
Staying Up-to-date

- **In our case USE auto update.**
  - We are doing the certification of the middleware but the Os can break the TB
- **Usage of a advance package manager**
- **The principle is to maintain a repository accessible by all hosts of the computing centre**
  - Depending of the bandwidth it is possible to use a Web proxy
    - All downloads are made one time
  - The repositories commonly contain few categories
    - An OS, updates and externals that contain security fixes for installed applications
    - Signatures should checked for the packages (ex : yum & apt configuration)
    - Running periodically a package verifier can be really useful
- **The problem is the kernel & kernel modules updates which need a reboot**

Firewalls

- **Why a local firewall when my site has a network one ?**
  - Prevent attacks from the LAN
- **One firewall profile per type of services**
- **Block what you want as you want**
  - You can block port access for all host or just a set of host
  - That decrease the load of a service (misconfiguration)
- **The logging of firewall activities can show you problems on your testbed**
  - Why there is connections attempt on this port ??
- **The site network firewall should apply the same rules as the system one**

Our case


Host firewall/root access manager
Network fw manager
synchronisation
Configuration external firewall
INTERNET
Configuration local firewall and root access
Target machines

- **SAM is running on production services every 4 hours**
- **Today, 2 security tests are running on WNs with SAM**
  - For Checking the validity of timestamps :
    - The “CRL Timestamps”
    - http://grid.cyfronet.pl/sam-doc/CE/CE-wn-sec-crl.html
  - For checking the ACL of sensible places on Wns
    - Searching files writable for other CE-wn-sec-fp
    - https://lxn1181.cern.ch:8443/sam-val/docs/CE-wn-sec-fp.html

Log files

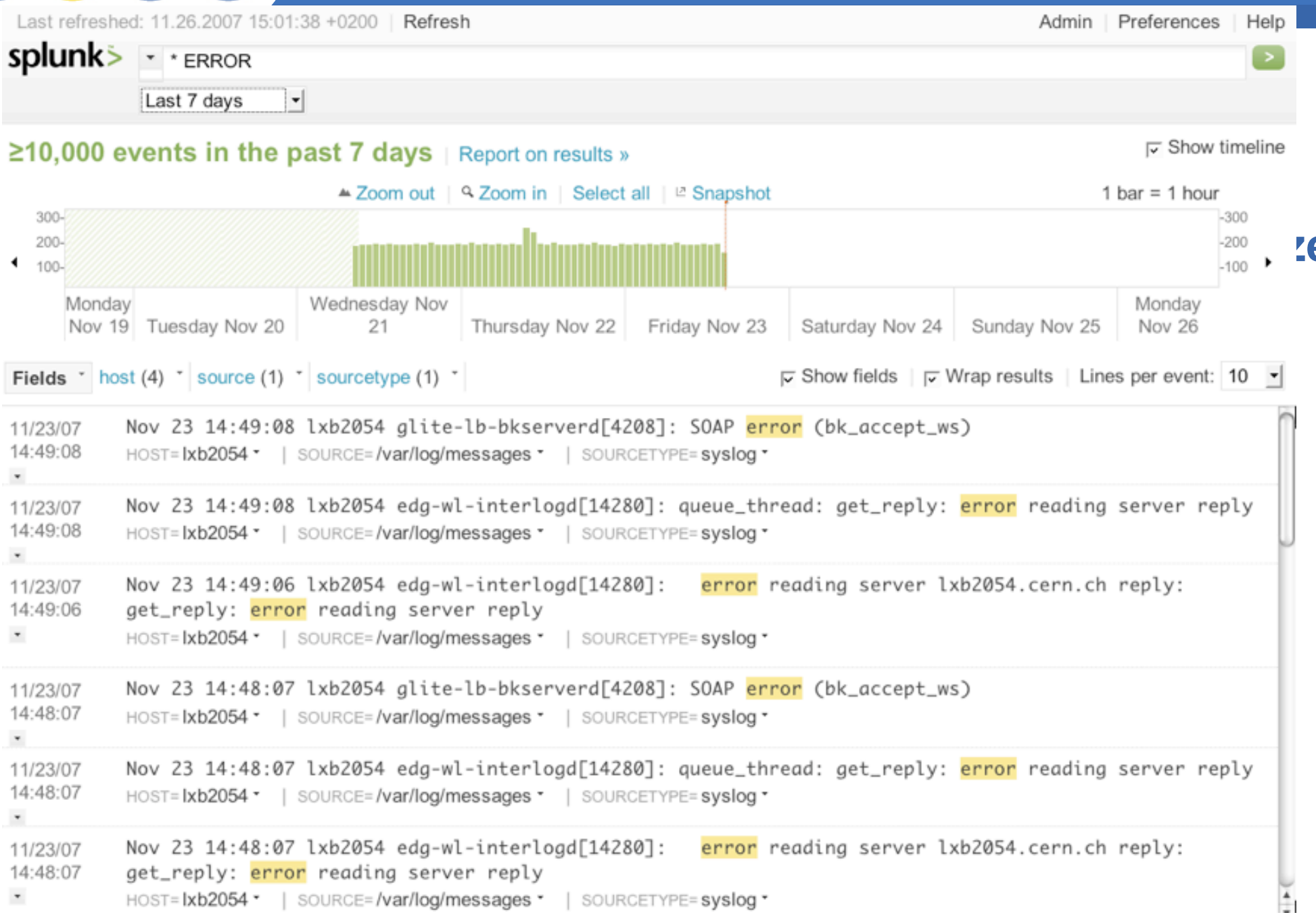
- Logs are mandatory to keep a trace of what happened
- An attacks second or third step is to stop and erase logging of actions on the machine
- The usage of a sys log server to centralize the logs of all services reduces the risk of loosing all the traces of the alarm
- How to use them? There is so much data that i can’t find the needle in haystack
- Tools can help you! I am using Splunk which gives you everything you need to debug

Tools

- **Installation / Maintenance**
  - APT
  - YUM
  - Squid (web proxy)
  - Fabric management tools
  - chkconfig
  - rpmverify
- **Project providing external tools repositories :**
  - jpackage - http://www.jpackage.org/
  - Dag - http://dag.wieers.com
  - Fresh Rpms - http://freshrpms.net
- **For monitoring the status of your settings :**
  - Pakiti - http://pakiti.sourceforge.net/
  - SAM
  - Nagios
  - Local made patch monitor
- **Logs**
  - Splunk

Splunk

- **Splunk ?**
  - Data mining of log in a “perfect” way.
  - commercial product able to handle 100 Mb of log per day for free
- **Exploring the logs is pretty complex a tool that centralize this work is very efficient**
- **You can find the way to configure it for free in my wiki page about it**


Last refreshed: 11.26.2007 15:01:38 +0200 | Refresh
Admin | Preferences | Help
splunk>
* ERROR
Last 7 days
≥10,000 events in the past 7 days | Report on results »
Show timeline
Zoom out | Zoom in | Select all | Snapshot
1 bar = 1 hour
300
200
100
Monday Nov 19
Tuesday Nov 20
Wednesday Nov 21
Thursday Nov 22
Friday Nov 23
Saturday Nov 24
Sunday Nov 25
Monday Nov 26
Fields
host (4)
source (1)
sourcetype (1)
Show fields
Wrap results
Lines per event: 10
11/23/07 14:49:08
Nov 23 14:49:08 lxb2054 glite-lb-bkserverd[4208]: SOAP error (bk_accept_ws)
HOST=lxb2054 | SOURCE=/var/log/messages | SOURCETYPE=syslog
11/23/07 14:49:08
Nov 23 14:49:08 lxb2054 edg-wl-interlogd[14280]: queue_thread: get_reply: error reading server reply
HOST=lxb2054 | SOURCE=/var/log/messages | SOURCETYPE=syslog
11/23/07 14:49:06
Nov 23 14:49:06 lxb2054 edg-wl-interlogd[14280]: error reading server lxb2054.cern.ch reply: get_reply: error reading server reply
HOST=lxb2054 | SOURCE=/var/log/messages | SOURCETYPE=syslog
11/23/07 14:48:07
Nov 23 14:48:07 lxb2054 glite-lb-bkserverd[4208]: SOAP error (bk_accept_ws)
HOST=lxb2054 | SOURCE=/var/log/messages | SOURCETYPE=syslog
11/23/07 14:48:07
Nov 23 14:48:07 lxb2054 edg-wl-interlogd[14280]: queue_thread: get_reply: error reading server reply
HOST=lxb2054 | SOURCE=/var/log/messages | SOURCETYPE=syslog
11/23/07 14:48:07
Nov 23 14:48:07 lxb2054 edg-wl-interlogd[14280]: error reading server lxb2054.cern.ch reply: get_reply: error reading server reply
HOST=lxb2054 | SOURCE=/var/log/messages | SOURCETYPE=syslog

patch_monitor

- **DB with :**
  - 1/ date_check, hostname, patch_installed
  - 2/ date_check, hostname, type_of_node, Os
  - 3/ date_check, hostname, patch_to_remove
- **1 : comparison of what is installed and configuration of the repositories**
- **2 : list the rpm meta pkg (SL3) or group installed (SL4)**
- **3 : look for errors with update simulation, check content of repositories if error, list the configuration to remove in your package manager configuration**

- **Simple Web interface listing the DB content for the last, day, week, month**

Conclusion

- Tune your kickstart and or your native tools for network install
- Double your firewall (hosts & network)
- Try to monitor your services
- Maintain stable apt/yum repositories ping us as soon as you find conflicts
- Give your tricks to all the team