Xtremweb-HEP
A best effort virtualization middleware

Oleg Lodygensky
Laboratoire de l’Accélérateur Linéaire
High Energy Physics

9 km

© CERN Geneva
XtremWeb-HEP

• Introduction
• Security
• Virtualization
• Internode connection
• Intergrid connection
• Applications
• Platform access
• Discussion
XWHEP: a secured best effort virtual cluster

Main features
- multi applications
- multi users
- certified server
- TSL communications
- authentication
  - ✓ X509 cert
  - ✓ OpenId
- authorisations
- access rights
- confinement
- virtualization
- p2p communications

Informations
- since 2006
- 600K€ E.U. funded
- 300K€ ANR funded

Goals
- virtualized cluster
- secured ressource broker
- grid interconnection
- virtualization
- p2p communications
  - C/S
  - M/W
### Volunteer Computing

<table>
<thead>
<tr>
<th>Volunteer cluster</th>
<th>Condor</th>
<th>Boinc</th>
<th>OurGrid</th>
<th>XtremWeb</th>
<th>XWHEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>volunteer ressources</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>multi OSes</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>type</td>
<td>cluster</td>
<td></td>
<td>desktop grid</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>deployment</td>
<td>per domain</td>
<td></td>
<td>global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>firewall bypassing</td>
<td>✗</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>shared FS</td>
<td>✓</td>
<td></td>
<td></td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td>delegated</td>
<td></td>
<td>included</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization</td>
<td>delegated</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Open ID</td>
<td>✗</td>
<td></td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>X509</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sandbox</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Heartbeat signal</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>multi users</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>multi applications</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>volunteer experience</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>large deployment</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>X</td>
</tr>
</tbody>
</table>

---

O. Lodygensky -  |  XtremWeb-HEP 9.0.5  |  CERN GDB - Nov
XtremWeb-HEP: a 3 tiers architecture

Administrator

User task

Dynamically downloaded user applications and data

Volunteer PC

Citizen

Other data servers

XWHEP Services

XWHEP scheduler

XWHEP data repository

CLIENT

User applications & data

User PC

Scientist

WORKER

Sandbox

Dynamically
downloaded
user applications
and data

Other data
servers

Server certificate

Server public key

Credentials

P2P comm

Task mgt

Data mgt

Local I/O
Introduction

Security
- authentication
- authorization
- access rights
- confinement

Virtualization

Internode connection

Intergrid connection

Applications

Platform access

Discussion
**AUTHENTICATION: CERTIFICATES**

Distributed parts connect using services public key and must present valid credentials.

- **Server certificate**
- **Serveur public key**
- **Credentials**
- **Job Mgt**
- **Data Mgt**

---

XWHEP Services

- XWHEP scheduler
- XWHEP data repository

---

XWHEP client/worker

---

Distributed parts connect using services public key and must present valid credentials.
Authentication: OpenID

Credentials may be certified by a third party

https://developers.google.com/accounts/docs/OpenID
Authorization

Credential is associated to a usage level.

Administrator

• manage public applications
• manage jobs, datas etc.
• manage users and usergroups
• manage workers

Standard user

• manage private applications
• manage its own jobs and datas

Group Administrator

• manage its group
  ▶ applications
  ▶ users
  ▶ jobs
  ▶ datas

Worker user

This is used to deploy workers
• no action allowed
• user rights delegation
  ▶ can compute user job
  ▶ can update user job
  ▶ can upload user job results
Access rights

Request completions depend on access rights.

All objects (applications, datas, users, jobs, usergroups etc) are associated to access rights (AR) that allow/deny accesses (read, write, execute).

Access rights define access types

<table>
<thead>
<tr>
<th>Access Types</th>
<th>Default Access Rights</th>
<th>Min Authz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>700</td>
<td>Std user</td>
</tr>
<tr>
<td>Group</td>
<td>750</td>
<td>Group admin</td>
</tr>
<tr>
<td>Public</td>
<td>755</td>
<td>Admin</td>
</tr>
</tbody>
</table>
Confidentiality

Authorisations and access rights define confinement levels

Public workers can execute public jobs of all users (and public jobs only)

Group worker can execute any public jobs and group jobs of any user of its group (and its group only)

Group worker may also be strictly restricted to its own group only (refusing public jobs not belonging to its group)

Private workers can execute all jobs of its owner (and its owner only)
XtremWeb-HEP

• Introduction
• Security
• Virtualization
  ✓ contextualization
  ✓ security
  ✓ use cases
• Internode connection
• Intergrid connection
• Applications
• Platform access
• Discussion
Virtualization
**VM over XWHEP**

Centralized and securized services store applications and data
- scheduler
- repository
- etc.

Distributed resource (volunteer PC)
- download the virtual disk
- create and run a new VM inside its local VirtualBox

Distributed resource may declare the virtualbox application.

StratusLab proposes distributions with the IaaS paradigms.

Distributed User
- submit a virtualbox job with a virtual disk

Remote Execution
“Contextualization is defined as the process by which a Virtual Machine instance is configured based on a master Virtual Machine Image. In general, contextualization consists in passing arbitrary data to the Virtual Machine at boot time.”

- **bootable VD**
- **typically a live CD (350Mb)**

- **created on the fly by the worker**
  - (=> not downloaded)
  - mounted on /scratch
  - typically 8Gb
  - this is a variable size file
  - => upload size then depends on result size (max: 8Gb - hopefully less)

**XWHEP worker**

- contextualization VD
- if exists, mounted on /context
- if exists, /context/context.sh executed at the end of boot process

User may require some ports (ssh, http...)

Following HEPiX Virtualization Working Group recommendation
VM : Security

All XWHEP security paradigms apply
- authentication
- authorization
- access rights

Virtual machines :
- recent OS including last known bugs and security corrections
- root access denied
- “sudo” usage disabled
- no access to LAN
- connection only using electronic keys
VM : Use Case

- HEP applications are linked to ROOT (http://root.cern.ch)
- DG resources don’t have ROOT
  ➡ submitted jobs will not run

✓ Deploy a VM with ROOT and XWHEP worker
✓ Submit such VM on the fly
  ➡ the native worker shares VirtualBox
  ➡ the native worker launches the VM
    ➡ the virtualized worker shares ROOT
    ➡ the virtualized worker run HEP jobs
XtremWeb-HEP

- Introduction
- Security
- Virtualization
- Internode connection
- Intergrid connection
- Applications
- Platform access
- Discussion
Interconnect jobs and applications over DG

Centralized and securized services

Submit/monitor

Download job/upload results

Bypassing FireWalls and NAT

O. Lodygensky - 3 - Nov
Interconnect jobs running on volunteer resources

Centralized and securized services

User PC

(1) Register
(2) Retrieve

Submit/monitor

Download job/upload results

Internode Communications

Volunteer PC

XWHEP client

XWHEP worker

XWHEP smartsockets proxy

(1) Register
(2) Retrieve

(3) connect

XWHEP smartsockets proxy

launched

XWHEP worker

launched

Volunteer PC

SmartSockets Hub

Internet Communications

Submit/monitor

Download job/upload results

Internode Communications

Volunteer PC

XWHEP client

XWHEP worker

XWHEP smartsockets proxy

(1) Register
(2) Retrieve

(3) connect

XWHEP smartsockets proxy

launched

XWHEP worker

launched

Volunteer PC

SmartSockets Hub
XtremWeb-HEP

• Introduction
• Security
• Virtualization
• Internode connection
• Intergrid connection
• Applications
• Platform access
• Discussion
EDGeS & EDGI FP7 projects

- Integrate Service Grids and Desktop Grids
- Enable very large number of computing resources (100K-1M processors)
- Attract new scientific communities
- Provide a Grid application development environment
- Provide application repository and bridges for the execution in the SG-DG system
XtremWeb-HEP

• Introduction
• Security
• Virtualization
• Internode connection
• Intergrid connection
• Applications
• Platform access
• Discussion
Applications

Porting Multiparametric MATLAB Application for Image and Video Processing to Desktop Grid for High-Performance Distributed Computing
Yuri Gordienko, Institut de Physique du Metal - Kiev - Ukraine

DART: A Framework for Distributed Audio Analysis and Music Information Retrieval
Eddie Al-Shakarchi, Cardiff University - UK

DNA Correlation Applications
A. Abuseiris, Erasmus - NL

High Energy Cosmic Rays
A. Cordier LAL - France
XtremWeb-HEP

• Introduction
• Security
• Virtualization
• Internode connection
• Intergrid connection
• Applications
• Platform access
  ✓ Portal
  ✓ API
• Discussion
Our Platform

https://xwservpub.lal.in2p3.fr:4326

XWHEP scheduler

XWHEP data repository

WORKER

Dynamically downloaded user applications and data

User task

Sandbox

Grid5000

Qarnot Computing
Portal
XtremWeb-HEP API

You are logged as "oleg.lodygensky@gmail.com"

Go to the client interface

Available interface commands:

Last month - Best Effort

<table>
<thead>
<tr>
<th>Site</th>
<th>#hosts</th>
<th>#CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid5000</td>
<td>170</td>
<td>1148</td>
</tr>
<tr>
<td>Qarnot</td>
<td>73</td>
<td>584</td>
</tr>
</tbody>
</table>
XtremWeb-HEP

- Introduction
- Security
- Virtualization
- Internode connection
- Intergrid connection
- Applications
- Platform access
- Discussion
Discussion

Under work
- OpenSAML / Shibboleth
- Map reduce

http://www.xtremweb-hep.org