Xtremweb-HEP: A best effort virtualization middleware

Oleg Lodygensky
Laboratoire de l’Accélérateur Linéaire

mercredi 24 septembre 14
• Introduction
• Security
• Virtualization
• Internode connection
• Applications
• Platform access
• Discussion
The XtremWeb-HEP Project

Goals
- secured resource broker
- grid interconnection
- virtualization
- p2p communications
  - C/S
  - M/W
  - MapReduce

Main features:
- 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

Contacts
- xtremweb@lal.in2p3.fr
- http://www.xtremweb-hep.org
XtremWeb-HEP: a secured 3 tiers architecture

- **Server certificate**
- **Server public key**
- **Credentials**

- **Task mgt**
- **Data mgt**
- **Local I/O**

**P2P comm**

**XWHEP Services**
- XWHEP scheduler
- XWHEP data repository

**User PC**
- User applications & data

**Volunteer PC**
- Dynamically downloaded user applications and data

**User**
- Worker
- Other data servers

**Citizen**
- Volunteer PC

**Scientist**
- Client

**Administrator**

**Credentials**
- Client
- Worker

**Mercredi 24 septembre 14**
XtremWeb-HEP

• Introduction

• Security
  ✓ authentication
  ✓ authorization
  ✓ access rights
  ✓ confinement

• Virtualization

• Internode 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
- Credentials
- ✗

XWHEP client/worker
- ✗

XWHEP client/worker
- ✗

mercredi 24 septembre 14
Authentication: OpenID

Credentials may be certified by a third party

[Diagram of authentication process]

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>
XtremWeb-HEP

• Introduction
• Security
• Virtualization
  ✓ contextualization
  ✓ security
  ✓ use cases
• Internode connection
• Applications
• Platform access
• Discussion
Virtualization

Real

Virtuel
VM over XWHEP

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

Distributed resource may declare the virtualbox application.

Distributed User
- submit a virtualbox job with a virtual disk

Remote Execution

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

StratusLab proposes distributions with the IaaS paradigms.
VM : Contextualization

Following HEPiX Virtualization Working Group recommendation

“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.”

XWHEP worker

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

/dev/hda
/dev/hdd
/dev/hdb

• 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)

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

mercredi 24 septembre 14
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](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
• Introduction
• Security
• Virtualization
• Internode connection
• Applications
• Platform access
• Discussion
**Internode Communications**

**Interconnect jobs and applications over DG**

Centralized and securized services

- **Submit/monitor**
- **Download job/upload results**

Server certificate
Sever public key
Credentials
Connection
Tunneled connection

**User PC**

- **XWHEP client**
- **SSH tunnel**
- **SSH@localhost**
- **A communicating application untouched code reconfigured only**

**Volunteer PC**

- **SSH reverse tunnel**
- **A communicating application untouched code/reconfigured only**
- **SSH@localhost**
- **XWHEP worker**

**Bypassing FireWalls and NAT**
Interconnect jobs running on volunteer resources

Centralized and securized services

Internode Communications

Submit/monitor

Download job/upload results

XWHEP client

User PC

XWHEP worker

launches

XWHEP smartsockets proxy

(1) Register
(2) Retrieve

XWHEP smartsockets proxy

(1) Register
(2) Retrieve

(3) connect

Volunteer PC

Volunteer PC

(1) Register
(2) Retrieve

(3) connect

Centralized and securized services

Submit/monitor

Download job/upload results
XtremWeb-HEP

• Introduction
• Security
• Virtualization
• Internode 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
• Introduction
• Security
• Virtualization
• Internode connection
• Applications
• Platform access
  ✓ Portal
  ✓ API
• Discussion
BEST EFFORT DEPLOYMENT

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

XWHEP scheduler

XWHEP data repository

Grid5000

Dynamically downloaded user applications and data

WORKER

User task

Sandbox

Qarnot

23
Portail XtremWeb-HEP 9.0.5-head

Logged in as oleg.lodygensky@gmail.com

Applications

Select all | Submit a job

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>moca</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>correlizer</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>dart.jar</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>dsp</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>larbin-crawler</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>guineapig</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>ls</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>guineapig-pp-1.1.1</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>autodock305.sh</td>
<td>DEPLOYABLE</td>
</tr>
<tr>
<td></td>
<td>ubuntu-11-dg-2.iso</td>
<td>VIRTUALBOX</td>
</tr>
</tbody>
</table>

Web interface (v 1.1)
API

XtremWeb-HEP API

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

Go to the client interface

Available interface commands:

- https://xwservpub.lal.in2p3.fr:4326/GETSESSIONS : /GETSESSIONS/anUID : retrieves all sessions
Last month

<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
- Applications
- Platform access
- Discussion
Discussion

Under work

• OpenSAML / Shibboleth
• Map reduce

http://www.xtremweb-hep.org