FermiCloud: A private cloud to support Fermilab Scientific Users

S. Tom, K. Chadwick, D. Youum, G. Garzoglio, H. Kim, P. Mhashilkar, T. Levshina

FermiCloud Architecture Diagrams

What is FermiCloud?

- Infrastructure-as-a-service private cloud for Fermilab Scientific Program.
- Integrated into Fermilab site security structure.
- Virtual machines have full access to existing Fermilab network and mass storage devices.
- Scientific stakeholders get on-demand access to virtual machines without system administrator intervention.
- Virtual machines created by users and destroyed or suspended when no longer needed.
- Tested for developers and integrators to evaluate new grid and storage applications on behalf of scientific stakeholders.
- Ongoing project to build and expand the facility:
  - Technology, scalability, monitoring, performance improvement.
  - High availability and reliability

FermiCloud Operations

- Stock virtual machine images are provided for new users.
- Active virtual machines get security patches from site patching services.
- Dormant virtual machines get woken up periodically to get their patches.
- New virtual machines scanned by site anti-virus and vulnerability scanners, don’t get network access until they pass.
- Three levels of service:
  - 24 by 7 high availability, can have fixed IP number,
  - 9 by 5 development/integration, use one of a pool of fixed IPs.
  - Opportunistic — Can be pre-empted if idle or if higher-priority users need cloud.

X.509 Authentication

- Use OpenNebula Pluggable authentication feature.
- Wrote X.509 authentication plugin and contributed back to OpenNebula, included in OpenNebula 3.
- X.509 Authentication is integrated into command line tools, EC2 Query API, OCCI API, SunStone management GUI.
- Contributing to standards bodies to make authorization callout to external services, similar to Grid authentication.

Virtualization and MPI

- Bare-Metal virtualization
- Bare-Metal with pinning (Notes: 2)
- Open vSwitch (Note: 2)

Monitoring and Metrics

- Note - Available Production services are operational 100% to 100% "onsubscription"

 Accounting

- Machines in two different buildings
- Mirrored SAN between buildings
- Global shared file system between all nodes
- Copies of all VM’s available in both buildings
- Network routable from each building
- Pre-emptive live migration for scheduled outage
- Restart of VM’s after unscheduled building failure

Work supported by the U.S. Department of Energy under contract No. DE-AC02-07CH11359