Argonne NATIONAL LABORATORY

Experiences with Eucalyptus: Deploying an Open Source Cloud

Rick Bradshaw - bradshaw@mcs.anl.gov
Piotr T Zbiegiel - pzbiegiel@anl.gov
Argonne National Laboratory

U.S. DEPARTMENT OF ENERGY

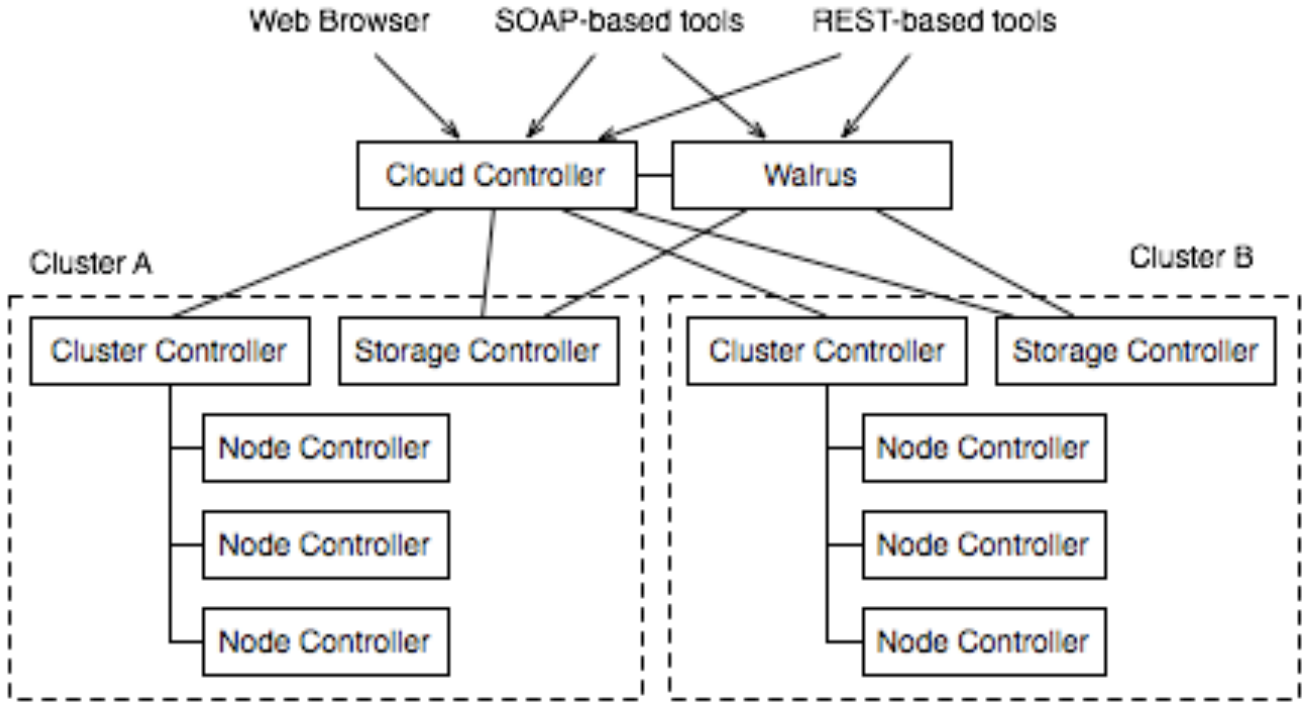
Overview

- Introduction and Background
- Eucalyptus experiences and observations
  - Scalability
  - Security
  - Support
- Our chosen support model
- Conclusions and future work

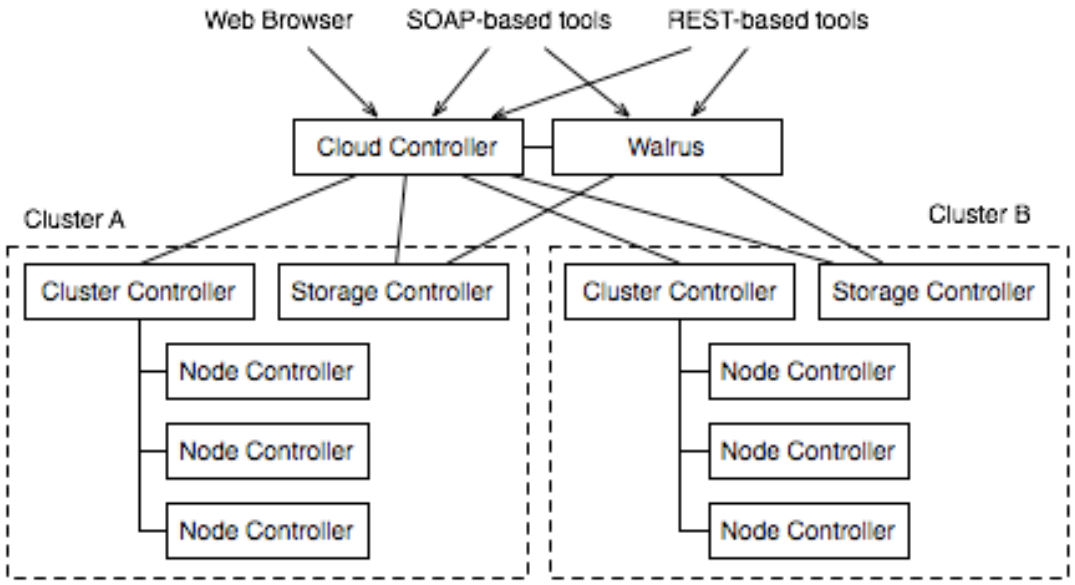
Introduction

- Clouds for scientific computing?
  - Magellan Project
    - buy or build
- What cloud software is available?
  - Different Cloud APIs
    - EC2 (http://aws.amazon.com/ec2/)
    - Rackspace (http://www.rackspacecloud.com/?CMP=Google_rackspace+cloud_exact)
    - Nimbus (http://www.nimbusproject.org/)
    - many more out there
- Why did we choose Eucalyptus?
  - EC2 compatibility
  - Open Source / Free
  - UEC from Ubuntu

Eucalyptus 1.6.2



Eucalyptus Scalability: Cluster sizes



- Tested Eucalyptus with various sized clusters (40, 80, 160, 240 nodes behind one cluster controller)
- All-around performance best with smaller clusters
- Performance deteriorated as clusters size grew due to iterative operations
- Eucalyptus instance termination operation is serial
  - Instances that don't terminate in a timely manner are communicated to all nodes
  - The process delays other activities while it works on terminating instances
  - Naturally, larger clusters result in longer execution times for such operations
  - Instance requests which never left the cluster controller due to errors are still "terminated" on the node controllers!

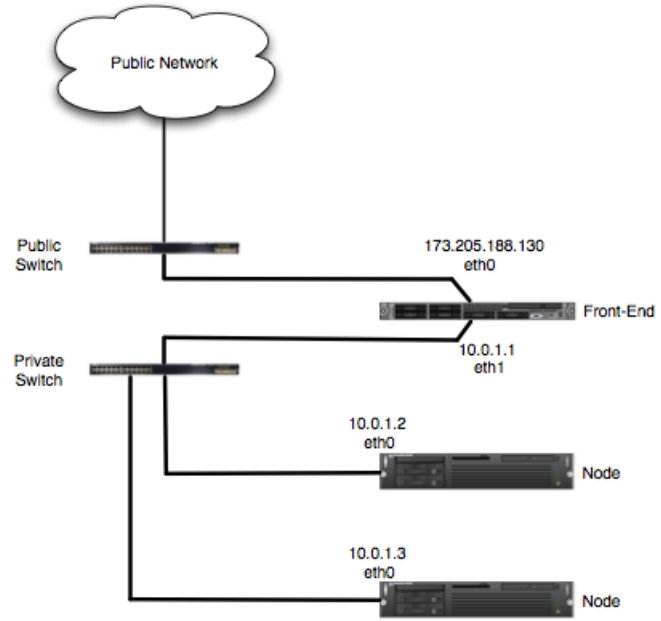
Eucalyptus

Eucalyptus Scalability: Load Testing

- Load tests were done to stress the software.
- Eucalyptus performed acceptably given enough time to complete requests
- Rapid churning (starting and stopping instances) gives Eucalyptus heartburn.
- Ran into hard limit on a single cluster controller
  - Somewhere between 750 and 800 running VMs
  - Caused by message size limitation in cloud and cluster controller communication protocol

Security: Network Security

- Eucalyptus network mode: MANAGED-NOVLAN
- VM network traffic masquerades as Cluster Controller
- By default, VMs can communicate with Node Controllers and other internal systems. (BAD)
- iptables rules on node controllers
  - prevents VMs from making unwanted connections
  - No impact to cloud operation



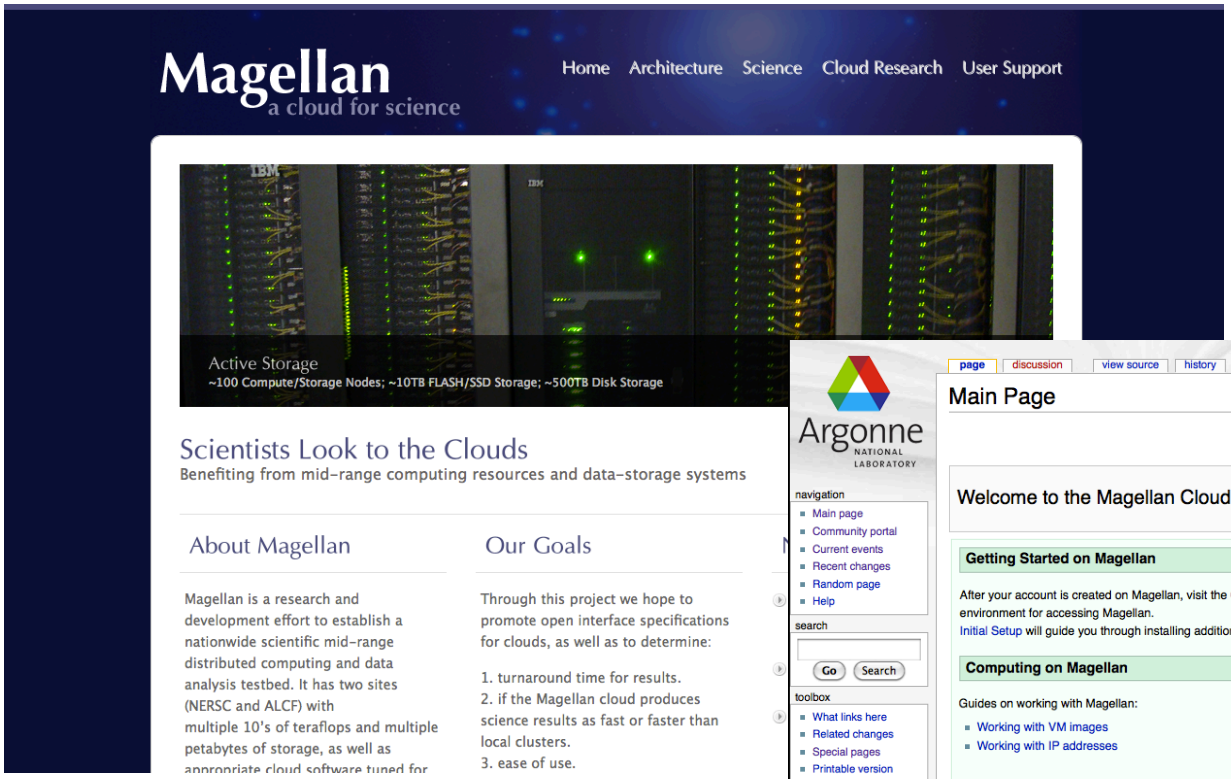
Security: IDS

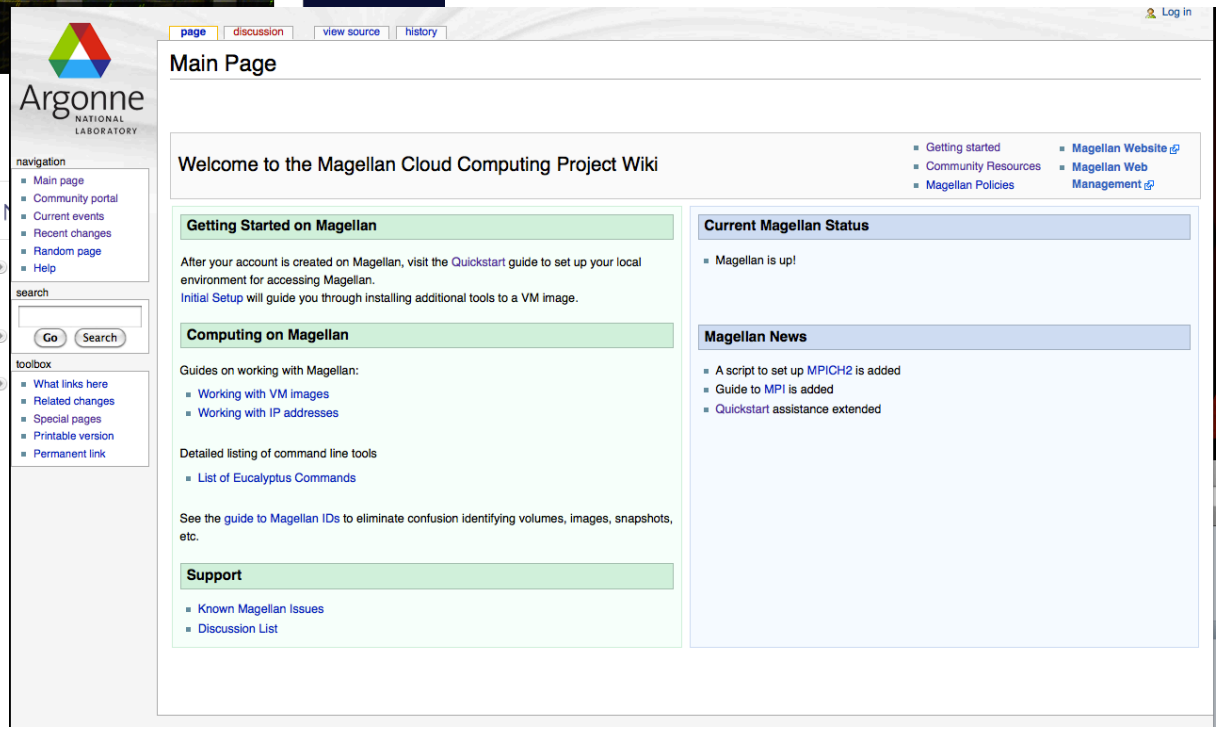
- Risk areas identified for the VMs
  - Outside IPs scanning/attacking VMs
  - VMs scanning/attacking outside IPs
  - VMs running suspect services
- Eucalyptus MANAGED-NOVLAN network model provides suitable IDS access
- IDS watches internal Cluster Controller interface
- Monitors all inbound and outbound traffic to the VMs
- Also monitors communication between security groups
- Can not see VMs communicating within a security group.

Security: Image Security Concerns

- Users can upload and register customized disk images
- Sys Admins must register kernel and ramdisk images
- Uploaded images automatically made public
  - Users must choose to change permissions
  - Contents of image can be inadvertently leaked
- Users can upload compromised images
  - A myriad of ways to backdoor
  - Bucket naming is fairly open
  - This even happened accidentally
- Users can upload images with exploitable vulnerabilities
  - Every user is a sys admin
  - We can recommend but not require best practices

User Support





User Support

- We chose a community based support model
  - forums(still haven't found one everyone agrees on)
  - wikis
  - mailing lists
  - best effort documentation
- The difference between Job support and OS/VM support
  - the complexity is greatly increased
  - learning curve for users is steep
  - pre-built images do not always work without effort
    - Kernels
    - KVM vs. Xen
    - startup environment

Conclusions

- Works but still evaluating other solutions
  - Nimbus
  - OpenStack
- Don't believe the hype
  - every cloud stack has its qualities and faults
  - usage/API should help make the choice