

CERIAS

the center for education and research in information assurance and security

ReAssure: A Publicly Accessible, Safe, Virtualization-based Testbed for Logically Destructive Experiments

Pascal Meunier, Purdue University CERIAS

Advantages

- All ReAssure code is open source
- Uses unmodified operating systems
- Leverages popularity of virtualization
- Large storage allows sharing images with all, specified users, or no sharing
- Multiple users can access PCs in an experiment, each with own account, and control a different virtual machine
- Allows using the same images for testing and production
- Gbit performance
- Experiment independence with VLANs
- Safety –if virtualization is breached, switches and firewall help contain experiments gone amok
- Could use any VM engine in theory
 - if VMware causes jitter, use UML, etc...
- Allows experiments otherwise unsafe

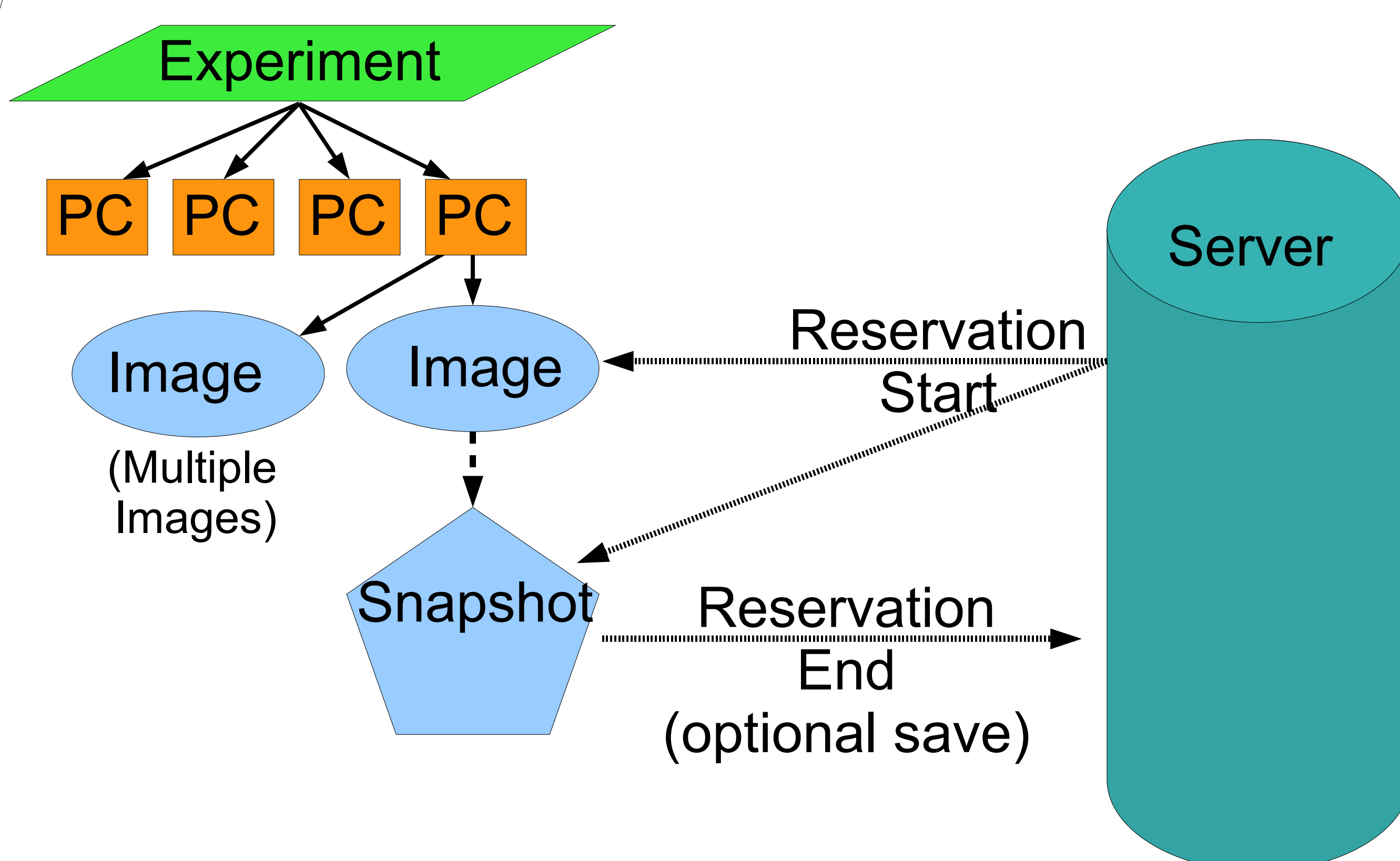
Release 1.0 Features

- Construction of network topologies, both online and with offline GUI
- Support for VMware snapshots (see below)
- Experimental PCs are started and stopped in a specified order
- Images are transferred automatically, registered with VMware and started
- Experimental PCs are reimaged using PXE (Preboot Execution Environment)

Possible Uses

- Labs for courses
- Graduate research
- Remote cooperation
- Testing networks
- Business applications testing
- HoneyClients
- Forensics
- Patch testing
- Exploit testing

Ephemeral Snapshots



- stop and resume your experiments at will, as time allows while saving progress
- decide not to save changes to a snapshot to resume from a previous snapshot

Deployment at Northern Kentucky University

NKU is our new partner in deploying ReAssure, for teaching and research. They will:

- Create images and experiments
- Validate ReAssure in a different environment
- Make any changes they wish (open source)
- Give us feedback

The more people create images and experiments, the more useful it will be.

Contact: Dr. James Walden