Jeff Hamm
hammjd@yahoo.com
jeff.hamm@mandiant.com

Senior
Consultant

Virtual Lab Environment

Introduction Slide

- Virtual Lab Environment
- Network Topography
- Virtual Forensic Workstations

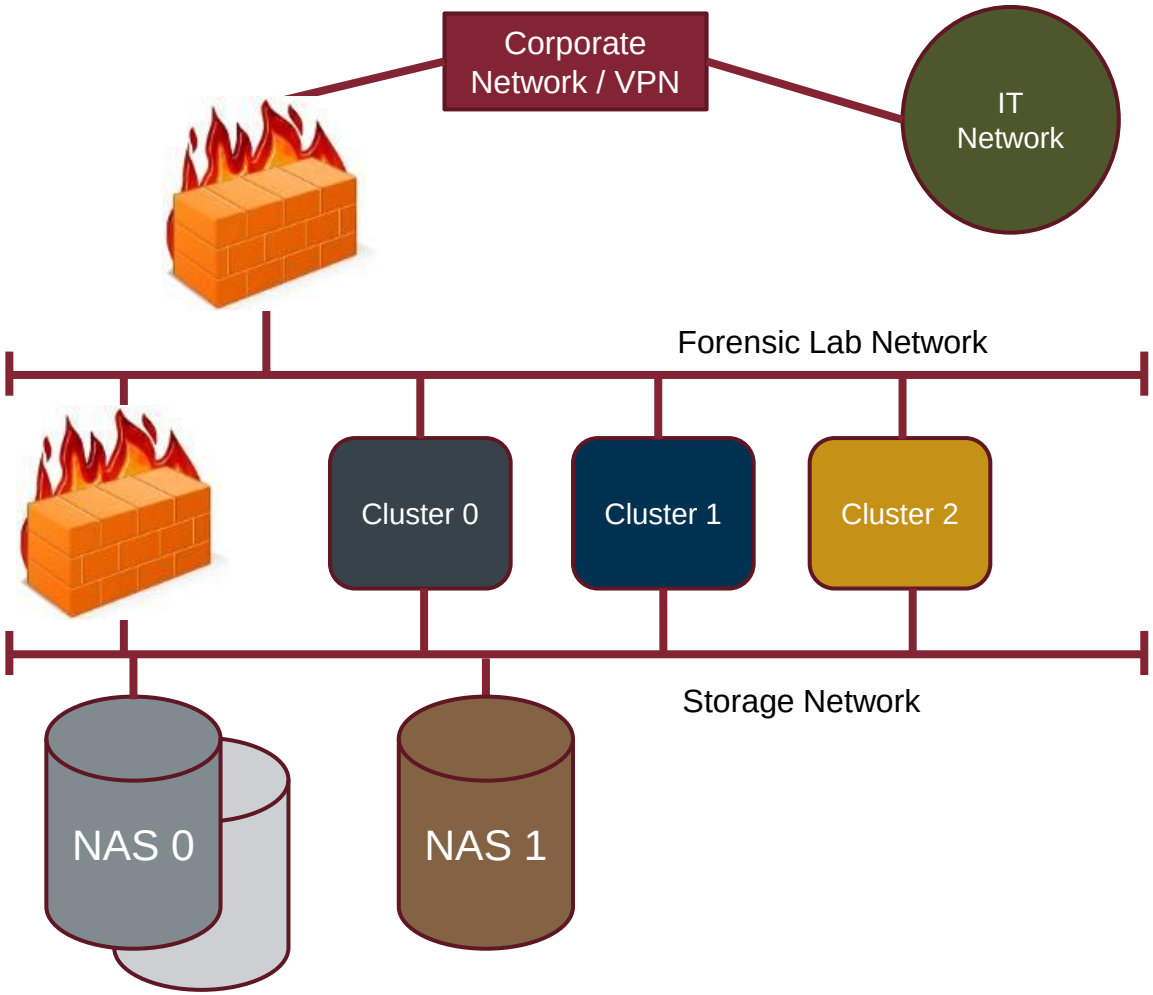
Virtual Lab Environment

- Advantages:
  - Templates for New Cases
  - Archiving of VMs
  - Replacement Costs of Physical Machines
  - Remote Logins
    - Two-Factor Authentication
- Disadvantages:
  - Lack of “hands on feel”
  - Initial Overhead Costs
  - Requires Dedicated Personel

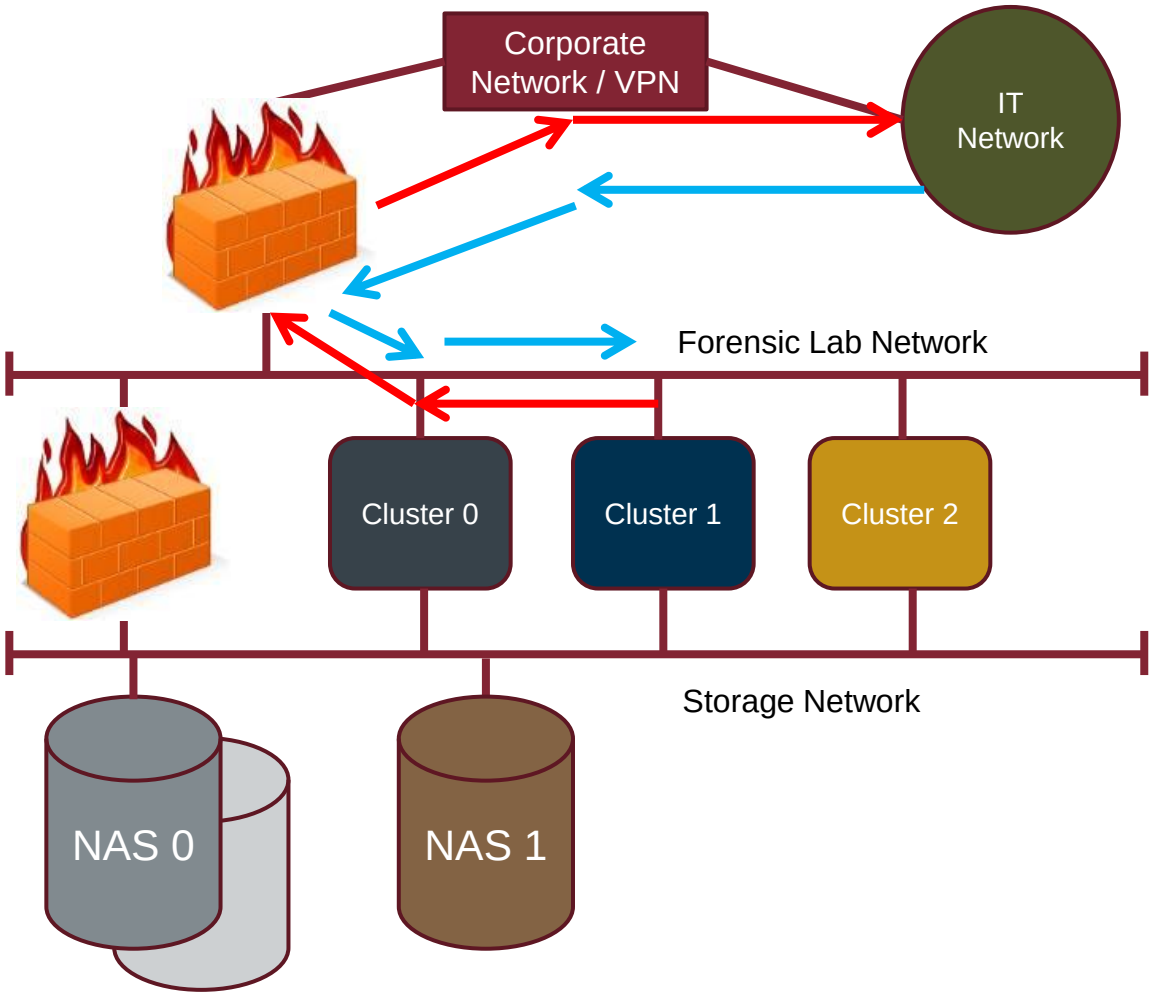
Network Topography

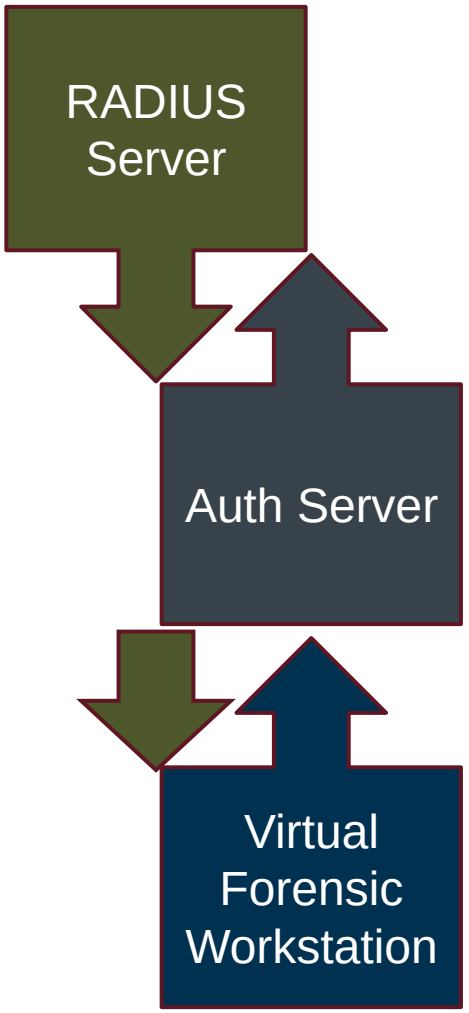
- Corporate Network / VPN Layer
- Forensic Lab Layer
- Storage Layer

Network Topography

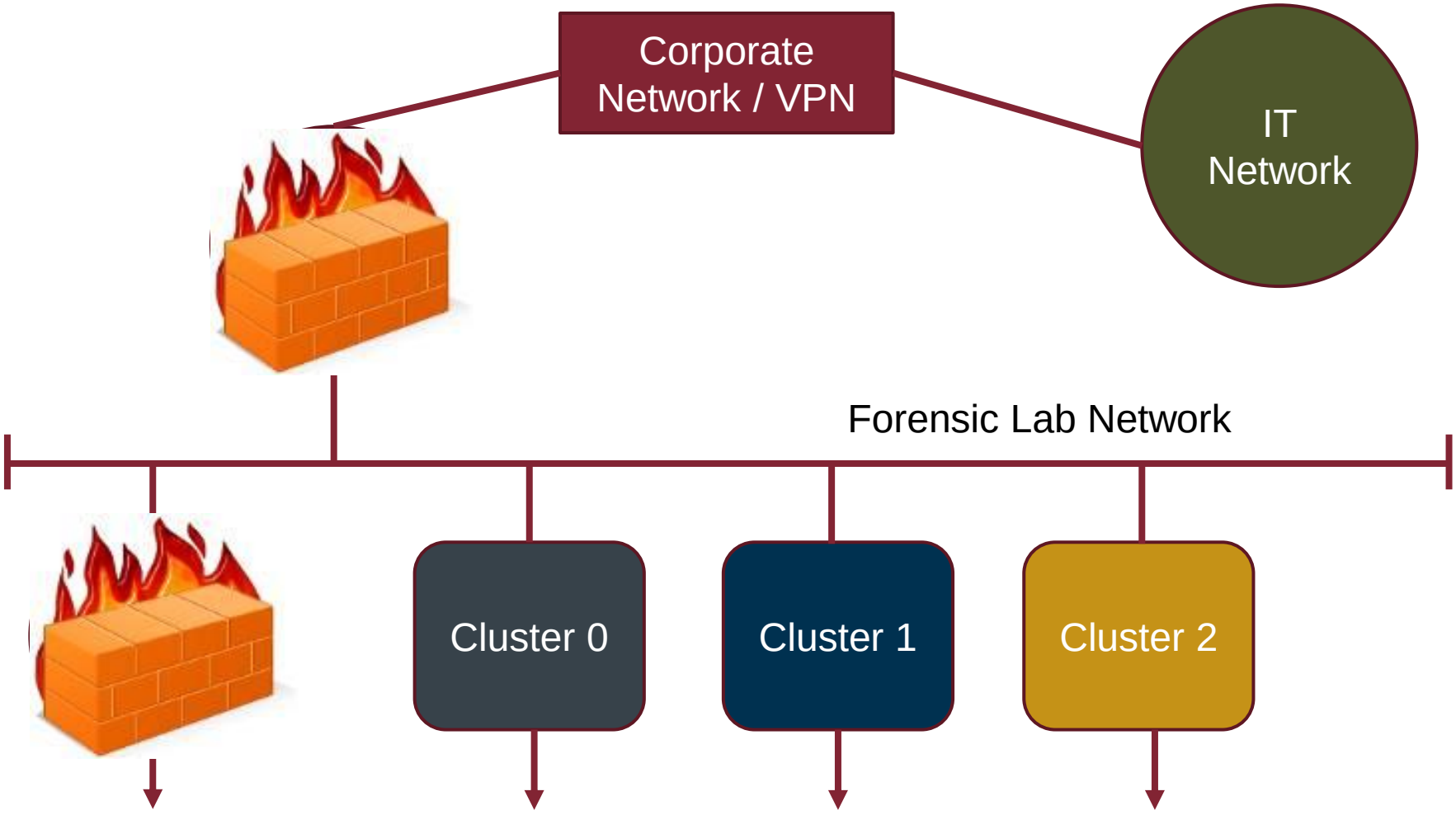


Two Factor Authentication





Network Topography



Network Topography

CLUSTER 0

- Authentication Server
  - OpenLDAP
  - RADIUS
- Admin Server
  - AV Updater
  - Web Portal
- Admin Workstation
  - XenConsole
- License Server
  - FTK
  - EnCase
- Storage Firewall

SPECIFICIATIONS

- VMWare ESX
  - For USB Pass Through
- 1 Physical Machine

Network Topography

CLUSTER 1

- Xen License Server
- Web Provisioning
- Analysis VMs

SPECIFICATIONS

- XenServer Enterprise
  - Scalability
- 2 Physical Machines
  - Server Apps
    - 24 GB RAM
    - 1x Xeon
  - Analysis VMs
    - 512 GB RAM
    - Quad Xeon (40 CPU)

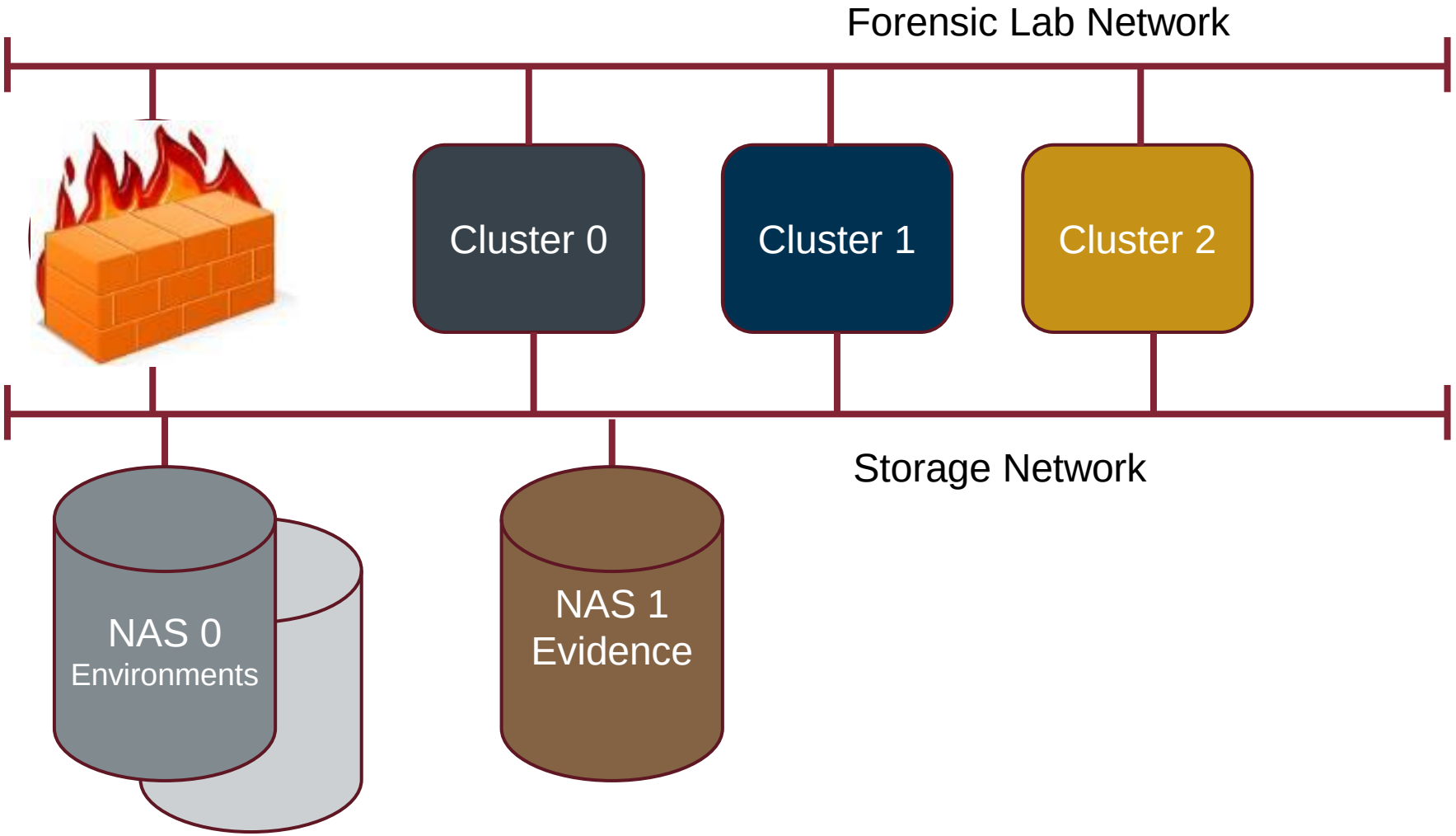
CLUSTER 2

- FTK Infrastructure
  - PostgreSQL Database
  - Worker0
  - Worker1
  - Worker2
  - Worker3

SPECIFICATIONS

- XenServer
- 2 Physical Machines

Network Topography

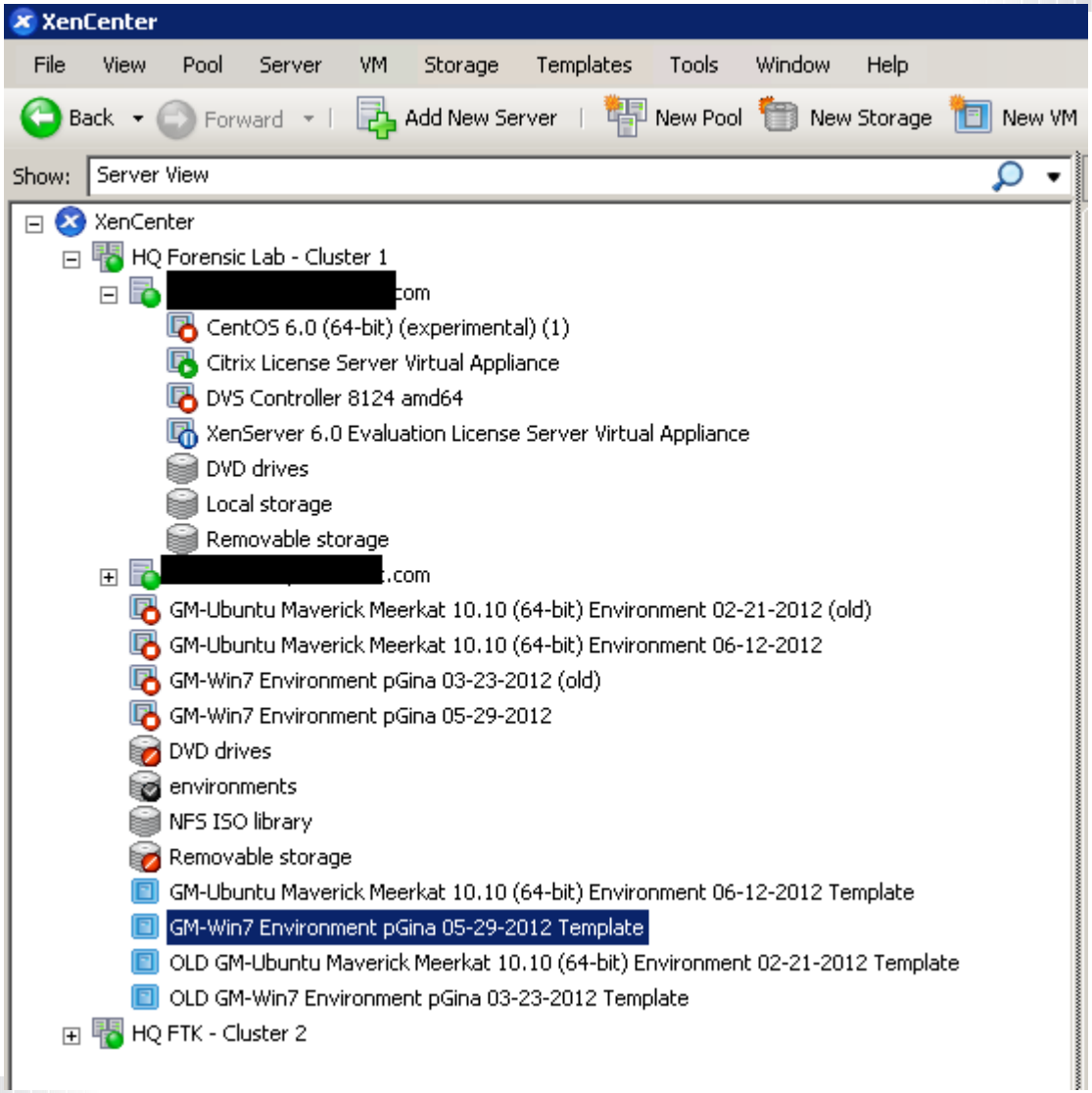


Virtual Forensic Workstations

MANDIANT

- XenCenter
  - Windows 7 Workstations
    - Template
    - Updates in SVN
    - Access via RDP
  - Ubuntu 10 Workstations
    - Template
    - CLI
    - Access via SSH

Virtual Forensic Workstations



Jeff Hamm
hammjd@yahoo.com
jeff.hamm@mandiant.com

Senior
Consultant

Virtual Lab Environment