Elastic Secure Infrastructure

Naved Ansari
Ian Ballou
Design Goals

- Move Hardware securely between different services (tenants)
- Get rid of silos; we should be able to share
- Move hardware rapidly to deal with changes in demand or emergencies
- Should support a large deployment like MGHPCG

SAY “NO” TO BARE-METAL SILOS!!!
Building Blocks

- **HIL: Hardware Isolation Layer**
  - Bare-metal node allocation.
  - Allows dynamic data center re-partitioning.

- **M2: Malleable Metal as a Service**
  - Diskless provisioning system.
  - Enables rapid multiplexing of bare-metal nodes between services.

- **Bolted: Tenant Controlled Bare-Metal Security**
  - Minimize trust in provider.
  - Security-tiering - pay for what you choose.
Status: HIL, M2, and Bolted

- **HIL: Hardware Isolation Layer**
  - Deployed in research production
    - Kaizen and Kumo (since 2+ years)
  - Now compatible with Scalability lab (QUADS) and HPC Clusters (Slurm)

- **M2: Malleable Metal as a Service**
  - Deployed in research production
    - Kaizen and Kumo (since 1 year)

- **Bolted: Tenant Controlled Bare-Metal Security**
  - Prototype complete
Research Production at MOC

- Used by dozens of researchers
- **Kumo leasing system:**
  - 16 Dell nodes available
  - Prevents resource hugging - 6 hour lease
  - Node state resumed using M2
- **Kaizen - New elastic bare metal environment**
  - 140 nodes in total
    - 30 Reserved for OpenStack, 100+ Elastic
  - 100+ Elastic shared between OpenStack deployment and other uses
  - All using HIL and M2.
Building community

- Critical to build a community
  - Productize for broader use cases
- MOC-RedHat round table (Spring 2018)
  - HIL and Ansible Networking
  - Foreman and M2
- Discussion with Project Leads from Ansible, Ironic, Foreman.
HIL and Ansible Networking
HIL and Ansible Networking

- Ansible network automation
  - use ansible playbook to manage network switches.
- HIL will be the multi-tenant RESTful API for Ansible Networking.
- Ansible networking to replaces HIL’s switch drivers.
M2 and Foreman
Bringing a Community to M2

- M2 integrated into Foreman as part of Red Hat Collaboratory
- M2 now usable with a nice interface
- M2 packaged as Foreman plugin for easy use
Who uses Foreman?

- SpaceX
- BBC
- Mozilla
- CERN
- eBay
- Venmo
- … and more!
Integration Specifics
Integration Workflow

Host info → Image → Target → Boot config

Disk image

M2
Concluding Remarks

- Our projects soon serving usable systems at scale
- Open source communities aware and interested
- Our HIL/Ansible Networking and M2/Foreman projects gaining traction
Starting the IAWP/InfiniBand/RDMA stack in the kernel...

Starting the Login Service.

Starting the Dynamic System Tuning Daemon.

Starting the Network Manager...

Starting LSB: Bring up/down networking...

Registered PCI device on em2.

NIC Link is Up 1Gbps. Flow Control: RX-TX.

em2: link is not ready

em2: link becomes ready

em2: link is not ready

Registered transport (user)

Registered named UNIX socket transport module.

Registered udp transport module.

Registered tcp transport module.

Registered tcp MP24.1 backchannel transport module.

Registered rdma transport module.

Starting Initialize the IAWP/InfiniBand/RDMA stack in the kernel.
Thanks!