

OpenStack / FreeIPA

The Magic Box of Toys and The AD of Linux
Presented by Oliver Smith
30th June 2016

OpenStack

- It's a magical stack of open-ness
 - Authentication/Service Catalog (Keystone)
 - Compute/Vms (Nova)
 - Networking (Neutron)
 - OS Images/Snapshots (Glance)
 - Block Storage (Cinder)
 - Object Storage (Swift)
 - Dashboard (Horizon)
 - Telemetry (Ceilometer), DNS(Designate), Containers (Magnum)...
- It's a huge unstable mess
 - OS updates not recommended
 - Point releases break








• But it's still fantastic

Durham
University

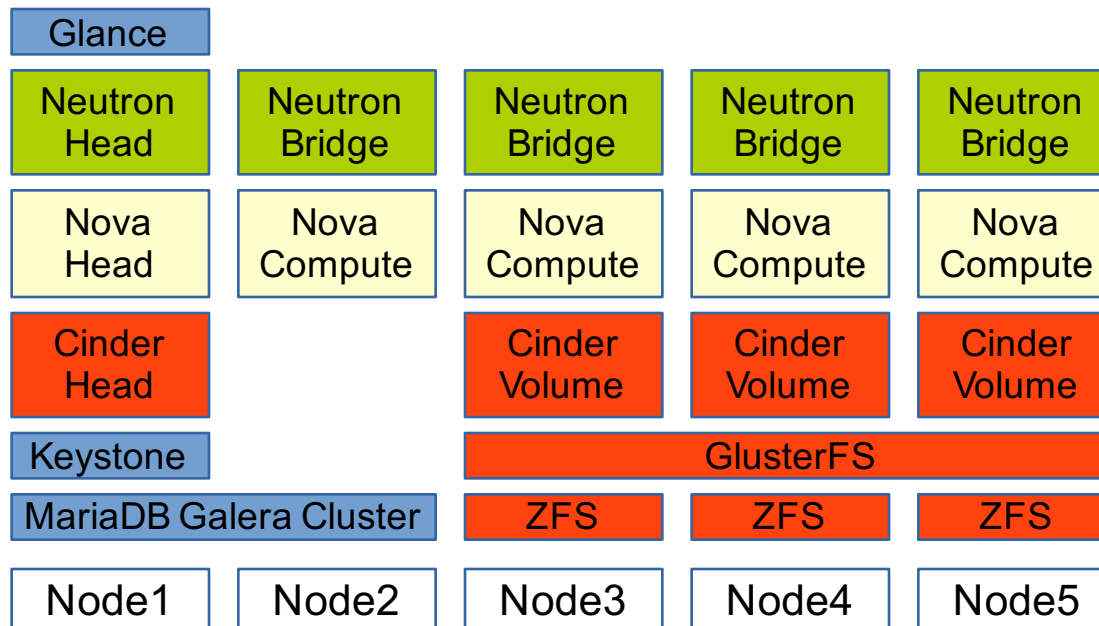
DurhamStack™

What are we trying to build?

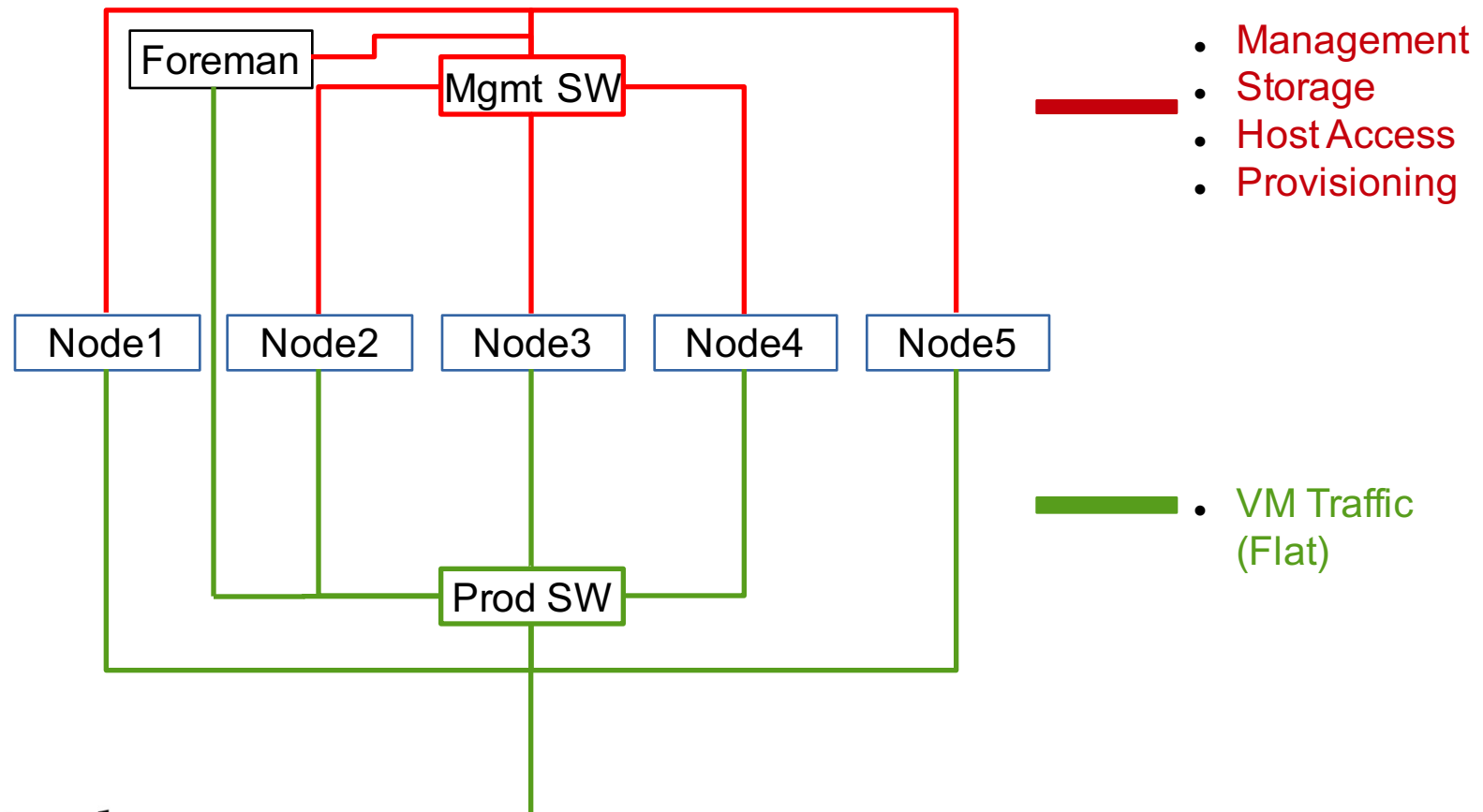
- Reliable HA VM hosting platform 
- Hyper-converged! Storage and compute in the same boxes 
- Multiple physical and logical zones
- Multiple groups of users 
- Automated installation and expansion 
- Integration with our existing systems
 - Foreman/Puppet 
 - FreeIPA
 - DNS/DHCP

DurhamStack – Proof of Concept

- Proof of concept build – 28 CPUs, 120GB memory, 3.6TB HA storage
- Deployed using Foreman/Puppet with small standalone modules
- Running one production-ish VM, a Perfsonar, and many test VMs



DurhamStack – Network Layout

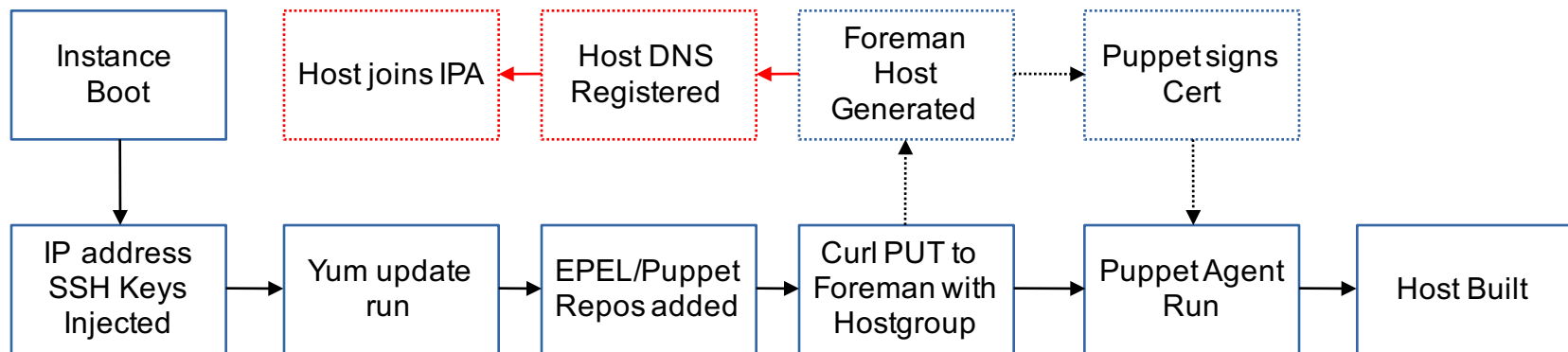


DurhamStack – Storage Layout

- Each node has 6x1TB in ZFS raidz2
- GlusterFS Replication volume with 3 replicas
 - Works but slow due to replication over slow network links
 - Change to distributed disperse volume for actual build with much faster networking
 - The storage will be spread across all nodes when similar hardware is used for the actual build
- Cinder presents the same volume three times to Nova for redundancy
- Glance also using the Cinder volume for image storage

Integration – Cloud-init

- Very customisable configuration tool that runs on boot of instances
- Standard run configures networking and SSH keys using Nova Metadata service
- Can modify cloud-init either by injecting new config files to images or by providing 'userdata' at instance creation
- Modules available to add functionality but they need to be maintained



FreeIPA

- Free...Identity/Policy/Authentication
- Highly configurable LDAP based identity system
- The Active Directory for Linux, community version of Red Hat IdM
- Kerberos used heavily for authentication and access control
- Comes with a built in CA with certificates being generated as hosts are joined
- Can manage DNS and NTP
- Supports both Master/Master and Master/Slave replication topologies

Identity

Does all the standard bits:

- Handles both users and hosts
- User groups and host groups
- Standard attributes available in UI, but more available using Idapmodify

More interesting bits:

- Stores host SSH hostkeys which can be used for known hosts
- Self service web interface for users
 - Add own SSH public keys
 - Configure own two factor authentication
- Supports migration of users/groups into IPA from OpenLDAP/AD
- Management of DNS records if integrated DNS is in use

Policy

- Fine grained Host Based Access Control
 - Who?
 - What?
 - How?
 - Example: Deny Col. Mustard on the GridUI with the SSH
- Central management of sudoers
- Central management for automounter
- Multiple password policies based on usergroup

Client Side - SSSD

- System Security Services Daemon – Not specific to IPA but used by the client-tools
- SSSD is configured during ipa-client-install which joins the host
- Host join can be done using either
 - Admin username/password
 - One time password for automation (Cloud-init/Foreman)
- SSSD handles all the client side interaction with IPA
 - PAM for authentication
 - Sudo
 - AutoFS
- Can have some issues with software expecting traditional access to users/groups

FreeIPA on Grid

- Used for both GridUI users and Pool Accounts
- SLURM working with configuration change
 - Enumerate = True
- ARC not working at present
 - Can't find users in LDAP
- DPM working fine
- ARGUS working fine

Questions?