# Openstack patching at scale

An Admins worst nightmare.

Warren Jeffs March 2019

# Virtual machines

We are mainly worried about VMs with a long lifecycle.VMs with short life cycles usually are gone before patches are required.

Users are put in charge of managing patching

- VMs have automatic updates enabled by default.
- No reboots are enforced for kernel patches, this is down to users
- We have rundeck job that lists all available updates for machines from Pakiti. Will be used as automated contacting of projects/users that own machines not complying to patching T+C.

Hopefully this is mainly self managed by users, and automation should reduce the amount of operational staff effort.

# Openstack Services

## Managed via Aquilon

- Machines are locked to snapshots of package repos.
  - A new snapshot is selected in Aquilon, machines are recompiled and auto update.
    - After packages may trigger automatic service reboots, but we do them manually.
    - As all services are 3+ nodes, rolling reboots are done to bring them upto patching level.

## This work takes some operational effort for patches.

- Kernel updates can make this process take a lot longer as they require machine restarts not just services.

# Hypervisors

Aquilon handles patching same as services.

Kernel updates are extremely time consuming.

- VMs are spread out over HVs.
- A HV needs draining before it can be restarted – we have scripts for helping with this.
  - Some VMs fail, and may require manual/non live migration.
- GPU Sessions can't be migrated
  - have to wait for lifecycle of VM to happen. So nodes can be drained 1 at a time for patching.

Extremely time consuming, can take weeks to get all HVs patched.

# Future plans

Rundeck job to defragment HVs.

- Make sure the HVs are filled at all times, so we have maximum amount of empty HVs. This should give a quick selection of HVs to get patched quickly, these can then be used for migrating off the other ones.
  - This will not help with GPU nodes.

Education of users to get them to build there services to withstand VM restarts.

- Being able to reboot VMs when required for updates also allows manual migrations which will allow migration across HV generations.