Upgrading from EL7 to EL9: Tales from Chicago

Judith Stephen

on behalf of the UChicago MANIAC Lab Team

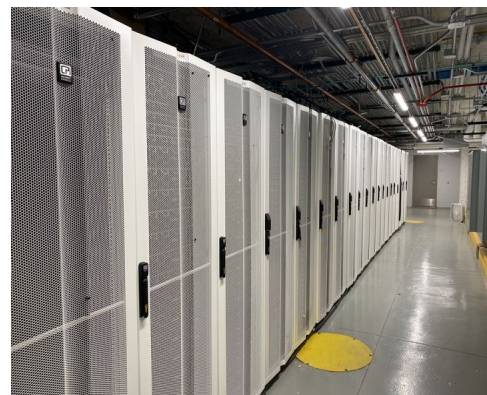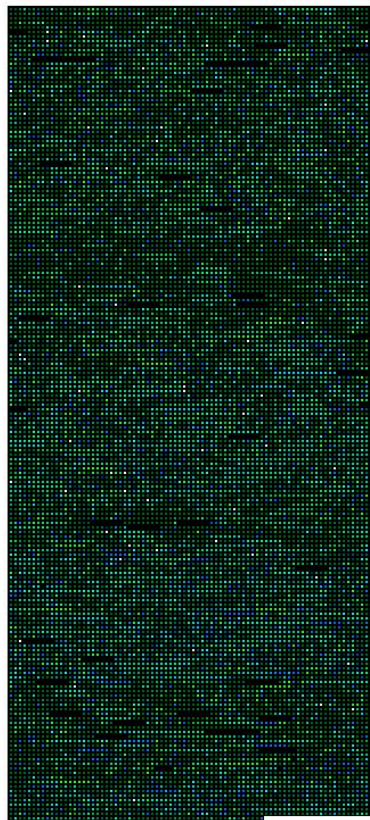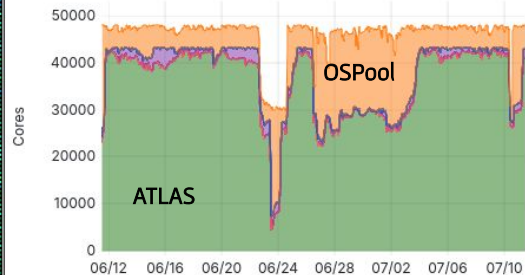# Who are we?

- ## Midwest Tier 2
  - Largest ATLAS Tier2 center
  - ~50,000 (logical) core HTCondor pool spread across UChicago, IU, UIUC
  - Regularly give >10% of our cycles to the OSPool!
- ## ATLAS Analysis Facility at the University of Chicago
  - End-stage analyses, Jupyter, Machine Learning
- ## IRIS-HEP Scalable Systems Laboratory
  - Software R&D for HL-LHC
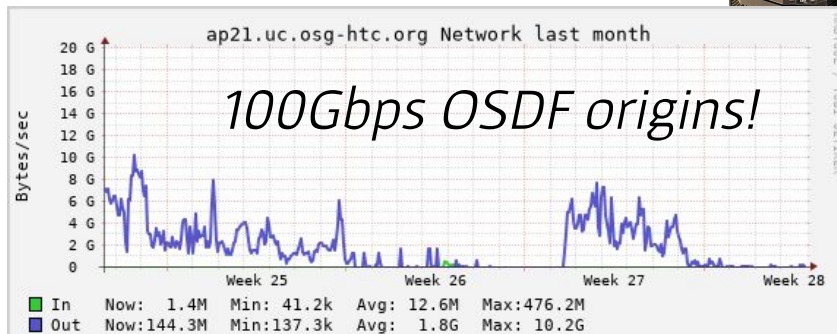

Core Usage by Job Type

Supporting PATh

- We operate several OSPool access points with built-in OSDF origins
  - ap(20-23).uc.osg-htc.org
- We also operate a Kubernetes cluster for PATh infrastructure
  - hub.opensciencegrid.org
  - Hosted Compute Entrypoints for CC* campuses
- Collaboration Support for SPT, XENON, KOTO, Future Colliders


100Gbps OSDF origins!

What are EL7 and EL9 anyway?

- Enterprise Linux (EL) broadly refers to Red Hat Enterprise Linux (RHEL) and its free/open rebuilds (Alma, Rocky, CentOS etc)
- Scientific Linux, a free rebuild from Fermilab, which supported the needs of our community for many years was sadly ended after Enterprise Linux 7
- Red Hat's sudden end-of-support for Enterprise Linux 8 (EL8) and change of direction for CentOS caused a lot of confusion and concern in the community
- We chose to use Alma Linux 9 based on the recommendations of CERN and others

How long did this take?

Running Total of EL8 and EL9 Machines

UC and IU compute

Everything else

Newest production servers
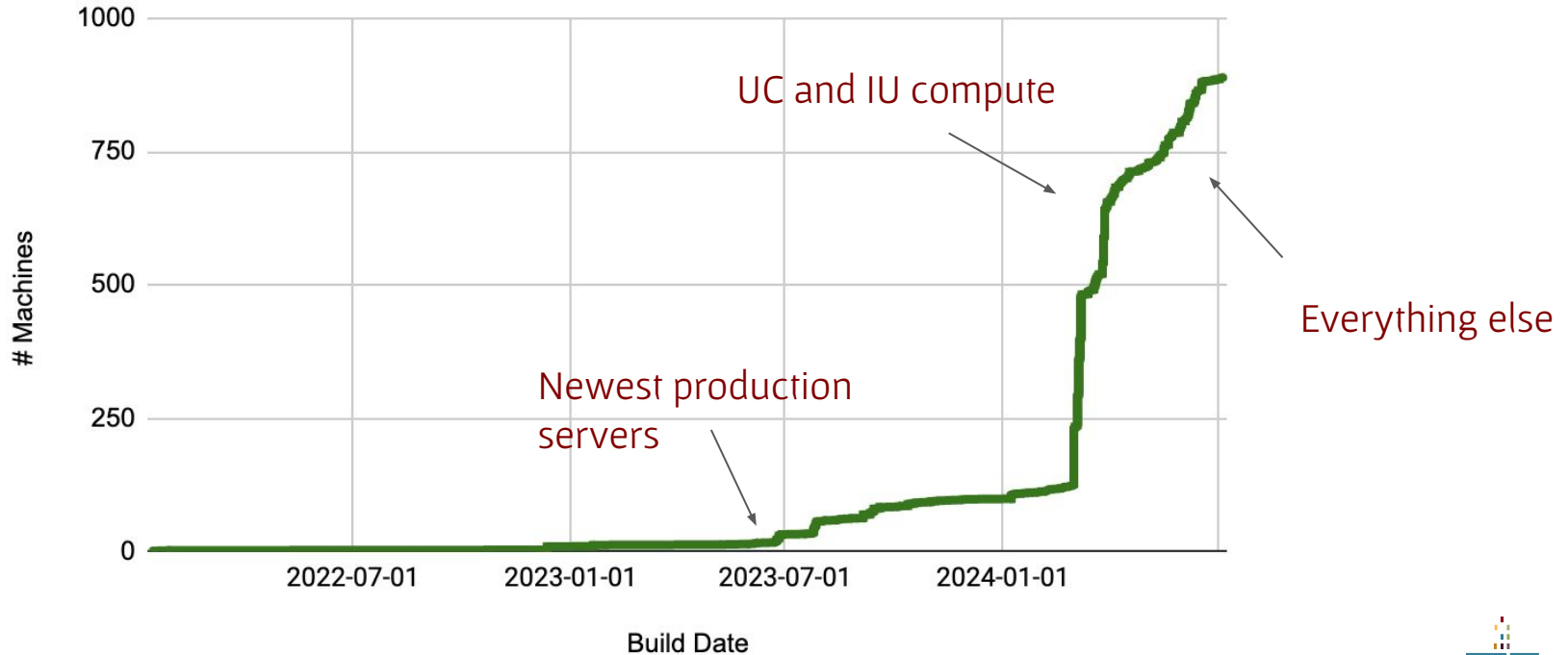
Build infrastructure hurdles

- Cobbler 2.8 needed changes to support EL9

- Cobbler 3.x worked with EL9 but introduced other issues
  - Did not scale anymore for our infrastructure (some relevant github issues)
  - No packages for EL7
  - Still needed manual patches (will be merged in 3.4?)
  - Limited support, slow release cadence

- Migrated our existing provisioning infrastructure to Foreman
  - We were already using Foreman for our Puppet monitoring
  - Re-use underlying build infrastructure (TFTP, DHCP, NAT, etc.)

What about sites not using Cobbler?

- Some traditional build tools are on a little bit of shaky ground
- xCAT's future uncertain, primary maintainers stepped down as of December 1, 2023
- Rocks Cluster – still supported? Last updated 7 years ago
- RedHat Satellite – used to be based on Cobbler, now is based on Foreman

Converting from CentOS-Stream

- AlmaLinux provides conversion scripts and plan to support EL8 with security patches until 2029
  - https://wiki.almalinux.org/documentation/migration-guide
- Many of our newer servers were already CentOS-Stream 8, but the package repositories evaporated on June 1!
- CentOS-Stream 8 repositories archived June 3 coinciding with the EOL of CentOS 8
  - Old repositories still available at vault.centos.org
  - Mirror at mirror.rackspace.com/centos-vault

Initial EL9 Impressions

- [9.0 Release Notes | Red Hat Product Documentation](#)
- Root SSH disallowed by default
- MFA SSH configuration broken
  - /etc/ssh/sshd_config.d/50-redhat.conf turns off keyboard-interactive
- Configuration management needed some updates
  - Package name changes, version strings

Some things don't work anymore...

- SHA–1 deprecated
  - Certificate authorities, ssh keys, etc.
  - `update-crypto-policies --set DEFAULT:SHA1`
- Missing drivers in the base image for older hardware
  - Final goodbye to 11th generation Dell servers
- Python 2 is really gone now

And some things do! (for now)

- Networking
  - NetworkManager is the recommended tool
  - ifcfg format still works
  - Will be removed in the next major release
- Firewall configuration
  - iptables is deprecated, replaced by nftables

Upgrading to OSG 23

- Before we upgraded, we cleaned up our existing HTCondor configuration
  - Use the defaults as much as possible!
  - Updated our pool security settings to use tokens
- Very smooth transition from OSG 3.6 to OSG 23
  - Big thanks to the PATh team

A major RegreSSHion

- We pushed hard to complete as much of the EL9 migration as possible before June 30 to avoid any major security vulnerabilities after the OS went end-of-life
- The predicted vulnerabilities happened… *but only affected EL9!*
  - July 1: CVE-2024-6387
    - *RegreSSHion*, a remote code execution vulnerability in SSH
  - July 8: CVE-2024-6409
    - A different bug with the same behavior
- Please update openssh-server or apply mitigations on your servers if they are on EL9 !!

Summary

- Planning pays off
- It's good to pay down some technical debt
- Be flexible
- Seriously, update openssh!

Questions?

Thank you!