Scientific Linux Status Update

Speaker: Pat Riehecky

Authors: Glenn Cooper, Rennie Scott, Bonnie King, Pat Riehecky

HEPiX May 2018

14 May 2018

Major Updates

- Connie Sieh has retired
  - We wish her well!
- Red Hat bought CoreOS
- Scientific Linux
  - Official Docker containers
  - 7.5 released
  - 6.9 released
- CVE-2018-1000156
  - patch: Malicious patch files cause ed to execute arbitrary commands

Official Docker Containers

Scientific Linux now has official Docker containers.

docker run -it sl:6 /bin/bash
docker run -it sl:7 /bin/bash
docker run -it sl:latest /bin/bash

They are updated monthly with latest security errata.
See the official readme for more information.

As a reminder, containers will let you run things long past their end of life date.

SL5 – It is removed from your site right?

SL5 went end of life March 31 2017

The SL distribution servers show over 2700 individual IP addresses still requesting nightly updates in April 2018.

SL6 – Production Phase 3

SL6 end of life November 30 2020

- RHEL 6.10 BETA
  - April 27 2018
- Current status is Production Phase 3

During the Production 3 Phase, Critical Impact Security Advisories and selected Urgent Priority Bug Fix Advisories may be released as they become available.

Other errata advisories may be delivered as appropriate.

SL7 – Production Phase 2

SL7 end of life June 30 2024

- SL 7.5
  - May 10 2018
- Current status is Production Phase 2

During the Production 2 Phase, Critical impact Security Advisories and selected Urgent Priority Bug Fix Advisories may be released as they become available. Other errata advisories may be delivered as appropriate.

New functionality and new hardware enablement are not planned.

Production Phase 1?

With nothing in Production Phase 1, we wonder about RHEL8.

Also, the RHEL8-alpha Anaconda branch exists:
https://github.com/rhinstaller/anaconda/tree/rhel8-alpha-branch

RHEL8 Public BETA expected in 2018

It may resemble Fedora 28 or 29

No commitments at Red Hat Summit

May 8 - 10 2018

Preparing for RHEL8 - python

RHEL8 will be python3 by default

The expectation is that python 2.7 will be provided as a software collection by upstream.

Folks who depend on python 2 should really begin the migration to python3.

Python3 is currently available as a software collection for SL6 and SL7

Python 2.7 End of Life is January 1, 2020

Preparing for RHEL8 - customization

The SL Team has been working with Fedora to get a number of packages to automatically de-brand themselves:

- abrt
- https://github.com/abrt/abrt/issues/1194
- libreport
- https://github.com/abrt/libreport/pull/469
- dhcp
- https://bugzilla.redhat.com/show_bug.cgi?id=1399351
- oscap-anaconda-addon
- https://github.com/OpenSCAP/oscap-anaconda-addon/pull/3
- ntp
- https://bugzilla.redhat.com/show_bug.cgi?id=1443596
- chrony
- https://bugzilla.redhat.com/show_bug.cgi?id=1443599

And many more

Preparing for RHEL8 - Anaconda

The SL Team has gotten a new hook added to Anaconda in Fedora 29 – postConfigureInstallClass

This permits adding repos or changing the anaconda runtime based on the ProductID

- Backport to RHEL8 anaconda request

  - https://github.com/rhinstaller/anaconda/pull/1459

SL Plans to use this to simplify adding things like EPEL and ElRepo for users to select. CentOS can add any SIGs they like as well.

CERN Locmap folks, this can simplify your codebase.

Preparing for RHEL8 - Anaconda

The SL Team is talking with the Anaconda team about a UI change to make locating additional repos (provided by the last slide) easier to find.

Follow the discussion at:

https://www.redhat.com/archives/anaconda-devel-list/2018-April/msg00010.html

https://www.redhat.com/archives/anaconda-devel-list/2018-May/msg00000.html

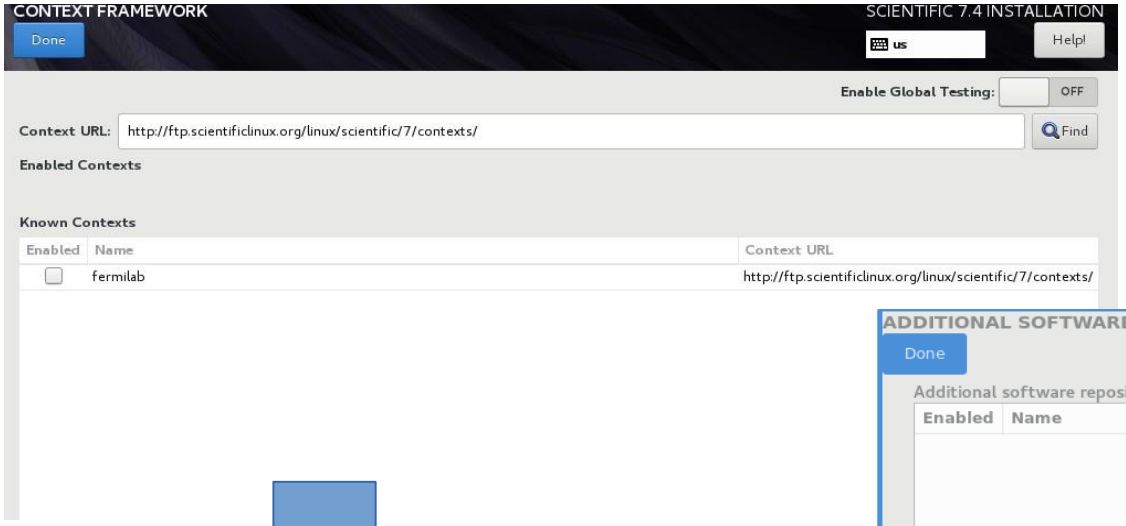
Or Join in!

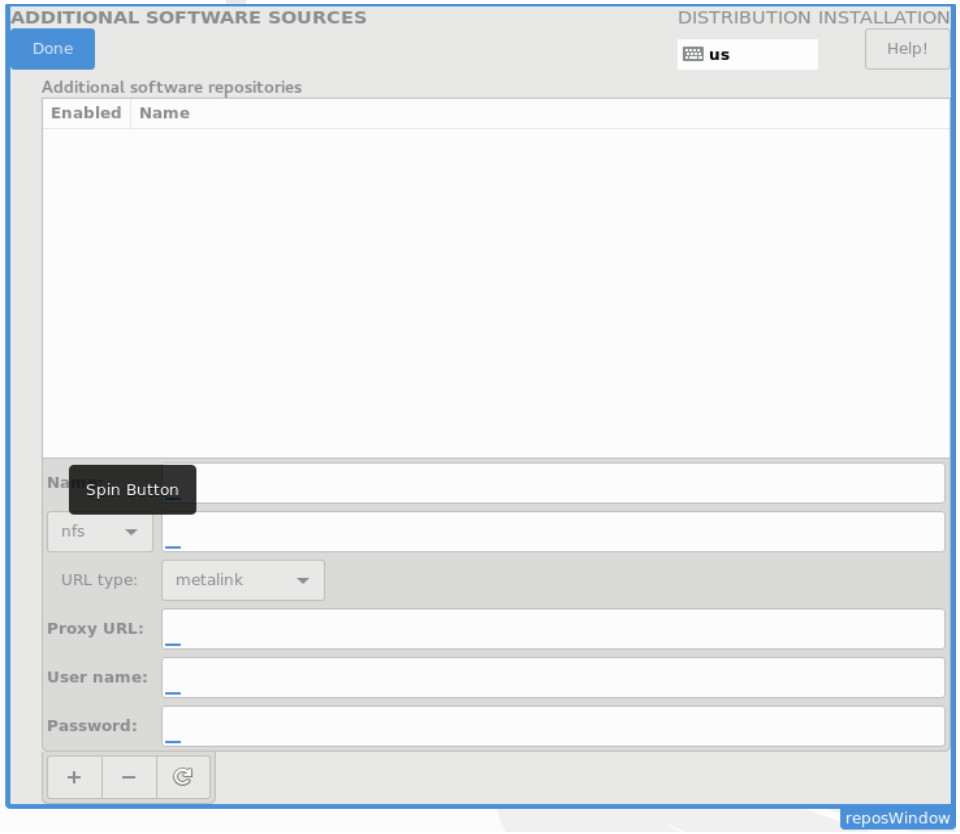
This is going to be a bigger change.

- Add some bits to the UI
- Alter the UX

CERN Locmap folks, this is for you too.

Preparing for RHEL8 - Anaconda





Preparing for the future

Firmware updates

- Spectre/Meltdown are really only fixed with a firmware update
  - Too many physical systems to manually flash them
  - Where there is one bug...
    - there are 8 more CVEs reserved for Spectre-NG
- RHEL7.4 added fwupd to help with this
  - Permits root to stage an EFI firmware update from a terminal
  - Talk to your vendor about this - firmware is generally not GPL
    - They must provide the firmware to LVFS.org
      - Linux Vendor Firmware Service

Preparing for the future

systemctl --user is coming

- Users can start/stop user level services defined in their home area
  - Currently requires valid login session
  - For long running services, what if their home area requires Kerberos auth?
    - Fermilab uses kcron for non-interactive Kerberos
      - Source available under MIT license
    - MIT Kerberos has /var/kerberos/krb5/user/${EUID}/client.keytab
    - Heimdal does not (to my knowledge)

Preparing for the future

Systemd stateless/immutable systems

- Newer versions of systemd (RHEL8+) support generating /etc and /var dynamically
- So long as /usr is available, the local system specifics can be generated at boot
  - /usr can be published via NFS
    - or perhaps casync/CVMFS
- A system can reset it self to a ‘known good’ configuration via reboot rather than reinstall

http://0pointer.net/blog/projects/stateless.html

Future Curiosity

Custodia – a tool for managing secrets

- Shipped in RHEL 7.4
- Custodia is a project that aims to define an API for modern cloud applications that allows to easily store and share passwords, tokens, certificates and any other secret in a way that keeps data secure, manageable and auditable.
  - How do you get secrets into transient cloud images?

Future Curiosity

Casync – content addressable data synchronizer

- A combination of the rsync algorithm and content-addressable storage
- An efficient way to store and retrieve multiple related versions of large file systems or directory trees
- An efficient way to deliver and update OS, VM, IoT and container images over the Internet in an HTTP and CDN friendly way

Future Curiosity

OSTree

- An upgrade system for Linux-based operating systems that performs atomic upgrades of complete filesystem trees.
- It is not a package system; rather, it is intended to complement them.
- The underlying architecture might be summarized as "git for operating system binaries".
- Via systemd’s stateless mode, perfect rollback is possible.
- A primary model is composing packages on a server, and then replicating them to clients.

Thanks to:

Ongoing Collaborators:

- Stephan Wiesand / DESY – OpenAFS
- Chris Brown and Dave Kraus / GE Medical / HELiOS – ZFS
- Urs Beyerle / ETHZ – Live Images
- Akemi Yagi – Functional testing and community contributions

Questions?