Running CentOS Stream in Production

A Case Study in Boring Tech
Who are we??

Robby Callicotte
- DevOps Team Supervisor
- Fedora Package Maintainer
- CentOS Alt Images SIG

Salman Butt
- SysOps Team Supervisor
- Fedora Package Maintainer
- Linux Enthusiast
How did we get here?

Brief history of CentOS

- Started in 2004[1]
- RedHat sponsored in 2014

The change to Stream

- Announced in 2019 by Chris Wright[2]
- The Future is Stream by Rich Bowen[3]
How did we get here?

The changing ecosystem

- Alma Linux
- Rocky Linux
- Suse
- Oracle
- OpenELA
CentOS relationship to RHEL and Fedora

Red Hat

Fedora

CentOS

CentOS Stream relationship to RHEL and Fedora

Fedora

CentOS Stream

Red Hat
Contributions flow among all elements of the ecosystem; however, there is a stronger connection between CentOS Stream and Red Hat Enterprise Linux. They each contribute to the other while also ensuring that new code is submitted as far upstream as possible, and, ideally, directly into the relevant open source community projects.

1. Open source community projects
   A collection of projects, each working toward their own goals

2. Fedora Linux
   Brings together the best ideas from the huge number of available open source community projects

3. CentOS Stream
   Provides a streamlined contribution path to the next minor release of Red Hat Enterprise Linux

4. Red Hat Enterprise Linux
   A production-grade operating system that provides a more secure, supported, and flexible foundation for critical workloads and applications
Super scientific usage survey

Do you run CentOS Stream in production?
61 responses

72.1% Yes
27.9% No

Survey conducted via Google forms in July 2023
Our philosophy

- Use internal mirroring as much as possible to pin release versions
- Internal versions only updated after passing tests
- Security team handles critical updates (CVEs)
- Swap-in updates where possible
- Package internal (company) tools as RPMs
- Battle-tested config management

These precepts were in place BEFORE CentOS Stream existed
Scope of environment

- Varies in size from 2000 to 4000 vms
- Over 1000 physical machines
- Tens of thousands of container deployments
- Three datacenters in US
- Multi-cloud presence
- Assist in thousands of OT-realtime deployments
Patching

Quarterly Updates:

● Package repos updated from last good nightly build
● Production VMs patched via “in-swap” method*
  ○ Physical systems patched “in-place”
● Rancher images rebuilt via Koji
● Lorax isos rebuilt via Jenkins job

Nightly Builds:

● Mirrors updated @ 1:30am
● CICD testing - rebuild environment using Kitchen-CI
● “Sandbox VMs” updated/rebooted in place every 15 days
Vendor support

- **Security tools**
  - Crowdstrike
  - Rapid7
  - Big Fix

- **GeoScience**
  - PreStack Pro
  - AASPI

- **Open Source (It just works)**
  - RabbitMQ
  - Victoria Metrics/Prometheus
  - MemSQL/SingleStore
  - And many, many, many more

- **Faux-pen Source**
  - Elastic Search
  - Hashicorp Suite
RPM Packaging

- Use upstream tools as much as possible.
- Wrote custom integrations for
  - Koji
  - Distgit[7]
  - Cobbler
  - Fedpkg/Fedora-review
Technologies used

Source Control
- Github
- Dist-git
- Consul

Deployment
- SaltStack
- Docker
- Portainer
- Rancher
- Nspawn
- VMWare
- Cloud

CICD
- Jenkins
- Github Actions
- Kitchen CI
- Cobbler
- Koji
- Lorax
- Harbor
- Harbor

Monitoring/Observability
- Zabbix
- Victoria Metrics
- Grafana

Deployment
- SaltStack
- Docker
- Portainer
- Rancher
- Nspawn
- VMWare
- Cloud
### CentOS Stream Jobs

#### Jenkins Dashboard

<table>
<thead>
<tr>
<th>Name</th>
<th>Last Success</th>
<th>Last Failure</th>
<th>Last Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>imgbuilder</td>
<td>2 days 8 hr - #32</td>
<td>9 mo 6 days - #28</td>
<td>16 min</td>
</tr>
<tr>
<td>imgcanary</td>
<td>11 hr - #564</td>
<td>8 days 11 hr - #555</td>
<td>17 min</td>
</tr>
<tr>
<td>isobuilder</td>
<td>2 days 8 hr - #37</td>
<td>6 mo 5 days - #33</td>
<td>13 min</td>
</tr>
<tr>
<td>isobuilder-iplc</td>
<td>2 days 8 hr - #28</td>
<td>1 yr 1 mo - #22</td>
<td>18 min</td>
</tr>
<tr>
<td>nightly-converge-tests</td>
<td>11 hr - #564</td>
<td>11 hr - #564</td>
<td>N/A</td>
</tr>
<tr>
<td>nightly-repo-updates</td>
<td>11 hr - #165</td>
<td>N/A</td>
<td>1 min 24 sec</td>
</tr>
<tr>
<td>repo-updates</td>
<td>2 days 8 hr - #11</td>
<td>6 mo 7 days - #8</td>
<td>11 min</td>
</tr>
<tr>
<td>rprnancanary</td>
<td>12 hr - #743</td>
<td>11 days - #732</td>
<td>7 min 12 sec</td>
</tr>
<tr>
<td>rprninspector</td>
<td>11 hr - test-0-833 fc41</td>
<td>1 mo 6 days - test-0-796 fc41</td>
<td>27 sec</td>
</tr>
</tbody>
</table>
### CentOS Stream Jobs - Nightly Repo Updates

#### Pipeline nightly-repo-updates
Updates the internal Cobbler CentOS Stream repos for nightly builds

#### Stage View

<table>
<thead>
<tr>
<th>Build</th>
<th>Apr 03</th>
<th>01:29</th>
<th>No Changes</th>
<th>482ms</th>
<th>1s</th>
<th>1min 20s</th>
<th>175ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>165</td>
<td>Apr 02</td>
<td>01:29</td>
<td>No Changes</td>
<td>333ms</td>
<td>919ms</td>
<td>1min 17s</td>
<td>132ms</td>
</tr>
<tr>
<td>164</td>
<td>Apr 01</td>
<td>01:29</td>
<td>No Changes</td>
<td>452ms</td>
<td>1s</td>
<td>30s</td>
<td>162ms</td>
</tr>
<tr>
<td>163</td>
<td>Mar 31</td>
<td>01:29</td>
<td>No Changes</td>
<td>431ms</td>
<td>1s</td>
<td>35s</td>
<td>173ms</td>
</tr>
</tbody>
</table>

Average stage times:
(Average full run time: 1min 15s)
## CentOS Stream Jobs - Cobbler Repos

### Index of /cblr/repo_mirror

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>adminer7-stable/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>adminer8-stable/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>appstream8-latest/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>automotive9-latest/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>base7/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>base8-latest/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>base8/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>base9-latest/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>base9/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aarch64/</td>
<td>2024-04-06 02:12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Index of /cblr/...-base9

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMPOSE_ID</td>
<td>2024-03-25 11:13</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>E02/</td>
<td>2024-03-24 22:57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EULA</td>
<td>2024-03-31 22:50</td>
<td>299</td>
<td></td>
</tr>
<tr>
<td>LICENSE</td>
<td>2024-03-31 22:50</td>
<td>18K</td>
<td></td>
</tr>
<tr>
<td>Packages/</td>
<td>2024-04-03 16:57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.repo</td>
<td>2024-04-01 04:25</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>base9.repo</td>
<td>2024-04-10 02:13</td>
<td>135</td>
<td></td>
</tr>
<tr>
<td>extra_files.json</td>
<td>2024-03-31 22:50</td>
<td>745</td>
<td></td>
</tr>
<tr>
<td>images/</td>
<td>2024-03-25 20:16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>isolinux/</td>
<td>2024-04-03 16:56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>repodata/</td>
<td>2024-04-03 16:56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timestamps.txt</td>
<td>2024-04-01 04:25</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>
### Pipeline imgcanary

Runs canary tests against the RPM build/deployment infrastructure.

### Stage View

<table>
<thead>
<tr>
<th>Stage</th>
<th>Pipeline Status</th>
<th>Build Time</th>
<th>Test Time</th>
<th>Build Time with Waiting</th>
<th>Test Time with Waiting</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Complete</td>
<td>2h 26m 22s</td>
<td>45m 12s</td>
<td>2h 31m 34s</td>
<td>46m 12s</td>
</tr>
<tr>
<td>B</td>
<td>Complete</td>
<td>2h 26m 22s</td>
<td>45m 12s</td>
<td>2h 31m 34s</td>
<td>46m 12s</td>
</tr>
<tr>
<td>C</td>
<td>Complete</td>
<td>2h 26m 22s</td>
<td>45m 12s</td>
<td>2h 31m 34s</td>
<td>46m 12s</td>
</tr>
<tr>
<td>D</td>
<td>Complete</td>
<td>2h 26m 22s</td>
<td>45m 12s</td>
<td>2h 31m 34s</td>
<td>46m 12s</td>
</tr>
</tbody>
</table>

**Recent Changes**

- [View previous changes](#)

### Recent Builds

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Owner</th>
<th>Arch</th>
<th>Finished</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1902</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1901</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1900</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1899</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1898</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1897</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1896</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1895</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1894</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
<tr>
<td>1893</td>
<td>imgcanary</td>
<td>kojadmin</td>
<td>march 2024-03-01</td>
<td>06:42:46</td>
<td></td>
</tr>
</tbody>
</table>
SaltStack - Config Management

- Local Testing
- Github Runner Testing
- Nightly Jobs
  - Alerts via Teams
  - Email Notification
- Uses Kitchen-CI [8]
  - COPR repos available [9][10][11]
### Pipeline isobuilder

 Builds for production iso images.

### Stage View

<table>
<thead>
<tr>
<th>Stage</th>
<th>Declarative: Checkout SCM</th>
<th>HW Info</th>
<th>SetupDirs</th>
<th>Build ISO</th>
<th>Deploy ISO files</th>
<th>CleanupDirs</th>
<th>Declarative: Post Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>952ms</td>
<td>1s</td>
<td>421ms</td>
<td>8min 45s</td>
<td>41s</td>
<td>428ms</td>
<td>203ms</td>
</tr>
<tr>
<td>#47</td>
<td>549ms</td>
<td>1s</td>
<td>484ms</td>
<td>12min 20s</td>
<td>1min 3s</td>
<td>754ms</td>
<td>164ms</td>
</tr>
<tr>
<td>#45</td>
<td>439ms</td>
<td>966ms</td>
<td>356ms</td>
<td>10min 13s</td>
<td>57s</td>
<td>726ms</td>
<td>115ms</td>
</tr>
</tbody>
</table>
CentOS Stream Jobs - ISO Builds

# Command prompt text
menu color cmdmark 0 #84b8ffff #00000000 none
menu color cmdline 0 #ffffff #00000000 none

# Do not display the actual menu unless the user presses a key. All that is displayed is a timeout message.

menu tabmsg Press Tab for full configuration options on menu items.

menu separator # insert an empty line
menu separator # insert an empty line

label linux
  menu label ^Install @PRODUCT@ @VERSION@
  menu default
  kernel vmlinux
  append initrd=initrd.img @ROOT@ quiet inst.ks=http://123.456.789.com/cblr/svc/op/ks/profile/---c9s-vmware-x86_64
How it all comes together
Future Improvements

- Better way to test cluster install automation
- Possible use of OpenQA to test images
- Upgrade from dist-git to Pagure
Questions?

End of Presentation

ANY QUESTIONS?
References

8. https://kitchen.ci/