Redpak: Ultra light weight container for embedded systems.

Clément Bénier

6 February 2022
IoT.bzh at a glance

Our position
Bretagne, France

European CyberSecurity Organisation Cyber Valleys mapping

30 years of OS expertise

VxWorks®
WIND RIVER
RTOS n°1 industrial market

TIZEN
OS open source, n°1 TV
Intel Vannes (2011-2015)

AUTOMOTIVE GRADE LINUX
OS open source used by Toyota, Subaru
IoT.bzh: +50% contributions tech. 2016-2020
(incl. Sécurité model)

Our product
redpesk®: OS open source & factory for industrial IoT

Our team
~30 people

Strong recognition in the open source community
Redpak Agenda

I. Motivations in embedded world
II. Illustration
III. Hierarchical model
IV. Rpm management
V. Performance
From hypervisor to light weight containers

- Black box
- Hard to audit
- Update CVEs
- Not adapt to embedded constraints, no resources shared
redpak motivations

• **Provide application isolation**
  - Restricted filesystem visibility
  - Resources access/usage (API, CPU, RAM, Network, …)
  - Built-in security model with MAC (Mandatory Access Control)

• **Maximize resource sharing & minimize system overload**
  - No duplication of root-fs
  - Reuse shared libraries between instances
  - Restrict RAM, Disk, CPU containerization cost
  - Boost container startup time

• **Prevent “diplomatic suitcase” container model**
  - Strict enforcement on installed packages & dependencies
  - Keep the system auditable
  - White box container model
• Control tools
• Shared hierarchical model
• Configuration files
• Rpm management
Redpak Hierarchy

redNodes Hierarchy

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Profiles</th>
<th>Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Shared</td>
<td>- Shared</td>
<td>- Shared</td>
</tr>
<tr>
<td>- Restricted</td>
<td>- Restricted</td>
<td>- Restricted</td>
</tr>
<tr>
<td>- Private</td>
<td>- Private</td>
<td>- Private</td>
</tr>
</tbody>
</table>

Core OS
- Shared
- Restricted
- Private

redPath = coreos / platform / profile / project

Profile
- HTML5 Apps
- Nav Apps
- Project Navigation

Profile
- IVI
- Cluster Apps
- Legacy Apps

Legacy Platform
- Legato, Adaptive, ...

Profile Cluster
- Cluster Apps

Platform
- redpesk Arz
- Vendor BSP (Renesas, Qualcomm, NXP, ...)

Platform
- AGL compatibility

Core OS
- redpesk Arz on Vendor BSP (Renesas, Qualcomm, NXP, ...)

Applications
Nodes

ON DISK

System
Plateforms
Profiles
Projects

RUNTIME

/ Root (tmpfs)

/ usr / lib (RO from system)

/ etc

/ etc/ld.so.conf (volatile)

/ nodes/current_node/usr (RO from current node)

/ nodes/projectX/usr (RO mount from project node)

/ home/app (RW mount from project node)
Yaml config file – config part

- Headers (node info)
- Exports (mounts)
- Environ
- Config (namespaces, cgroups, ...)

```
[rp-owner]$ cat /var/NODES/NODE_A/etc/redpack.yaml
...

config:
  ldpath: /NODES/NODE_A/usr/lib:/NODES/NODE_A/usr/lib64
  inherit: true
  die-with-parent: Unset  # Kills with SIGKILL child process
  share_user: Unset       # Not Create new user namespace
  share_cgroup: Unset     # Not Create new cgroup namespace
  share_net: Unset        # Not Create new network namespace
  share_pid: Unset        # Not Create new pid namespace
  share_ipc: Unset        # Not Create new ipc namespace
  cgroups: # control group
    cpuset:
      cpus: 0-2
      mem:
        max: 512M
  caps: # capabilities
    - cap: net_raw
      mode: unset
  seccomp:
    default: SCMP_ACT_ALLOW
    rules:
    - syscall: kexec_file_load
      action: SCMP_ACT_KILL
    - syscall: breakpoint
      action: SCMP_ACT_KILL
    rulespath: /path/to/bpf1
```
Yaml config file – export part

```
[rp-owner]$ cat /var/NODES/NODE_A/etc/redpack.yaml
...
exports:
- mode: Private  # RW current node and not mounted in childrens
  mount: /nodes/_private
  path: $NODE_PATH/private
- mode: Restricted  # RO
  mount: /nodes/test/usr
  path: $NODE_PATH/usr
- mode: Public  # RO
  mount: /nodes/test/var
  path: $NODE_PATH/var
- mode: Restricted
  mount: /bin
  path: /usr/bin
- mode: Symlink  # create symlink
  mount: /home/$LEAF_ALIAS
  path: /nodes/_private
- mode: Anonymous  # create dir
  mount: /var
- mode: Execfd  # volatile file
  mount: /etc/passwd
  path: getent passwd $UID 65534
```
Rpm databases

- 1 database / 1 node
- installation by node
- Database aggregation
Install a pkg

# install pkg
[rp-owner]$ redwrap-dnf --redpath /var/redpesk/NODES/plateforme1 install mypkg
## Performance

<table>
<thead>
<tr>
<th>Starting Time</th>
<th>X86_64: Qemu (ms)</th>
<th>Aarch64: NXP (ms)</th>
<th>Aarch64: Xilinx (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>redpak</td>
<td>18</td>
<td>150</td>
<td>58</td>
</tr>
<tr>
<td>LXC</td>
<td>59</td>
<td>254</td>
<td>191</td>
</tr>
<tr>
<td>Podman</td>
<td>606</td>
<td>1 706</td>
<td>1 570</td>
</tr>
<tr>
<td>Systemd-nspawn</td>
<td>291</td>
<td>1 516</td>
<td>858</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Container's Engine</th>
<th>X86_64: Qemu (kB)</th>
<th>Aarch64: NXP (kB)</th>
<th>Aarch64: Xilinx (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>redpak</td>
<td>2920</td>
<td>2 308</td>
<td>2 336</td>
</tr>
<tr>
<td>LXC</td>
<td>3 108</td>
<td>2 736</td>
<td>2 732</td>
</tr>
<tr>
<td>Podman</td>
<td>32 108</td>
<td>31 220</td>
<td>31 156</td>
</tr>
<tr>
<td>Systemd-nspawn</td>
<td>14 712</td>
<td>12 632</td>
<td>12 696</td>
</tr>
</tbody>
</table>

- Short startup time adapt to embedded
- Good memory use
Links

- **Redpak**
  - Sources: [https://github.com/redpesk-labs/red-pak](https://github.com/redpesk-labs/red-pak)
  - On redpesk OS: `dnf install red-pak`

- **redpesk®**
  - Website: [https://redpesk.bzh/](https://redpesk.bzh/)
  - Documentation: [https://docs.redpesk.bzh/](https://docs.redpesk.bzh/)
  - Sources: [https://github.com/redpesk/readme](https://github.com/redpesk/readme)

- **IoT.bzh**
  - Website: [https://iot.bzh/](https://iot.bzh/)
  - Vidéos: [https://vimeo.com/search?q=redpesk](https://vimeo.com/search?q=redpesk)

- **Comunnauty Support**
  - Matrix.org: `+redpesk:matrix.org`