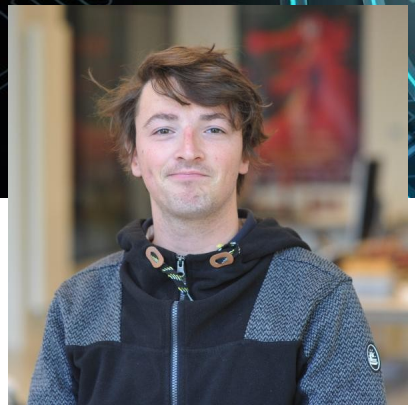


Redpak: Ultra light weight container for embedded systems.

Clément Bénier

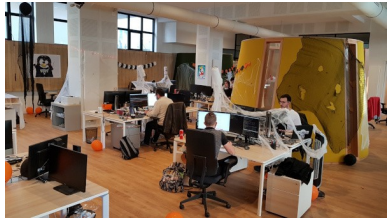
6 February 2022

IoT.bzh at a glance

Our position

Bretagne, France

European **C**yber**S**ecurity **O**rganisation Cyber Valleys mapping



30 years of OS expertise

Wind River (1990) - Intel (2009) - IoT.bzh (2015)

VxWorks®
WIND RIVER

RTOS n°1 industrial market

TIZEN
SAMSUNG

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

redpesk®

Our team

~30 people

Strong recognition in the open source community

FOSDEM

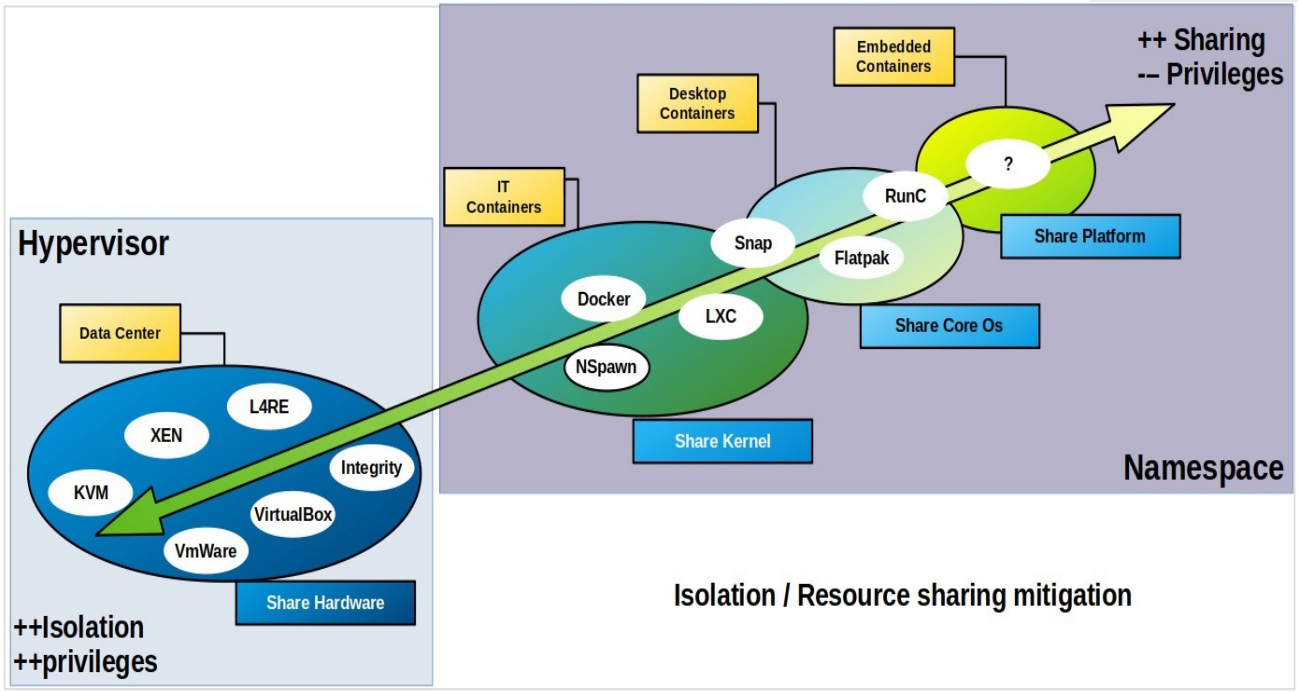
IOT BZH

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

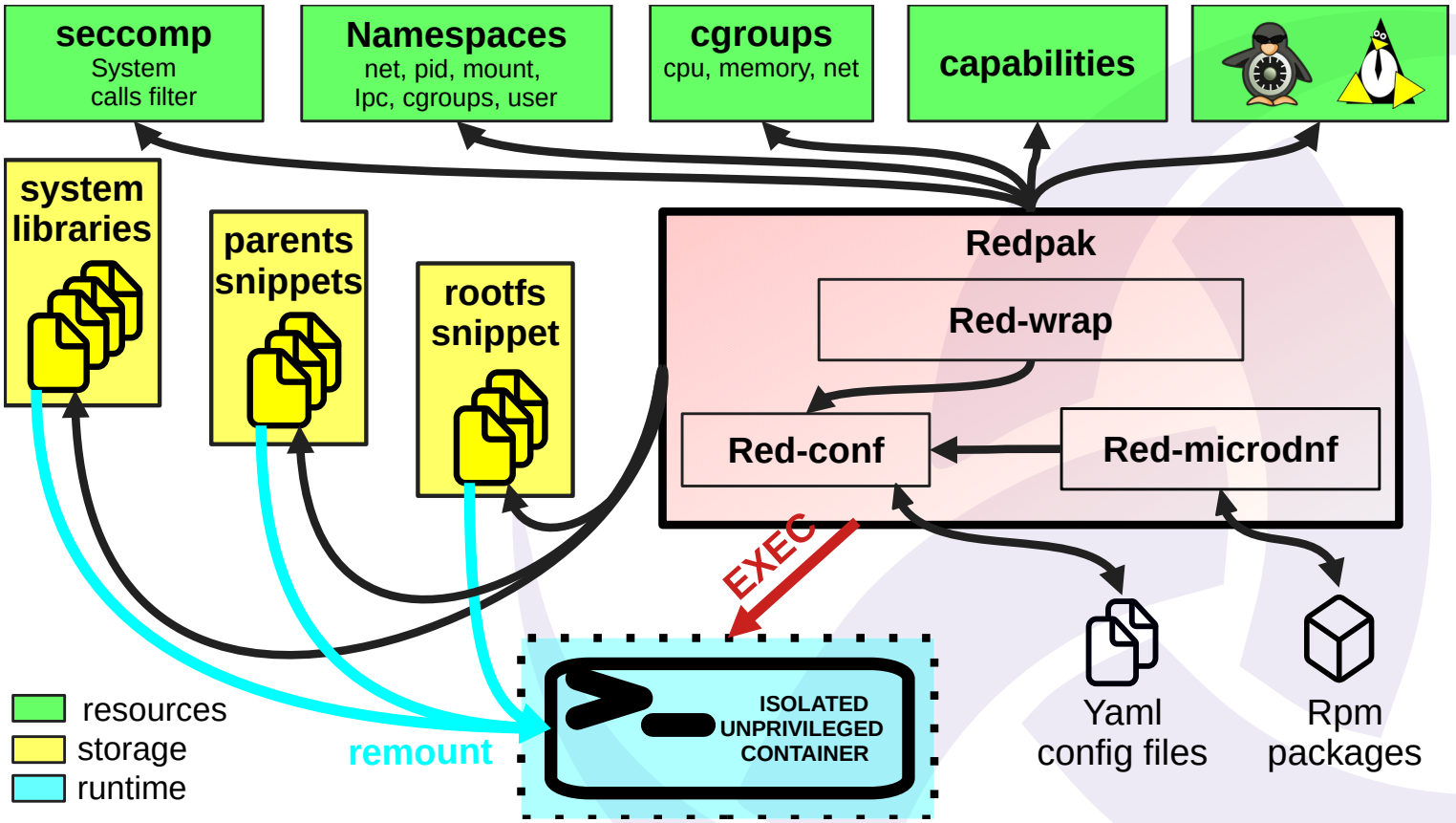


redpak motivations

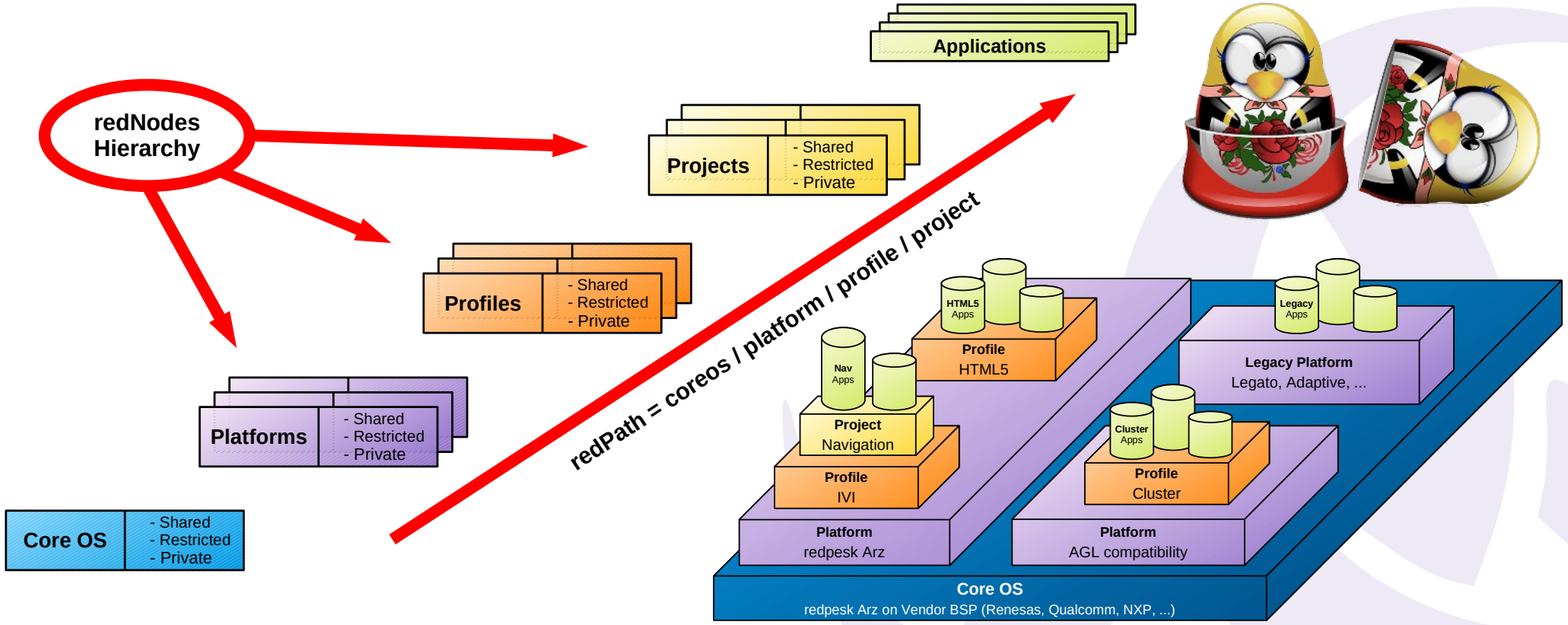
- **Provide application isolation**
  - Restricted filesystem visibility
  - Resources access/usage (API, CPU, RAM, Network, …)
  - Built-in security model with MAC (Mandatory Access Control)
- **Maximize resource sharing & minimize system overload**
  - No duplication of root-fs
  - Reuse shared libraries 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

Concept illustration

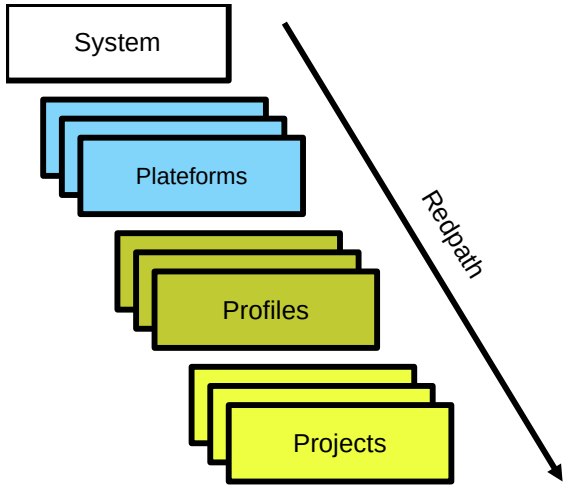
- Control tools
- Shared hierarchical model
- Configuration files
- Rpm management



Redpak Hierarchy

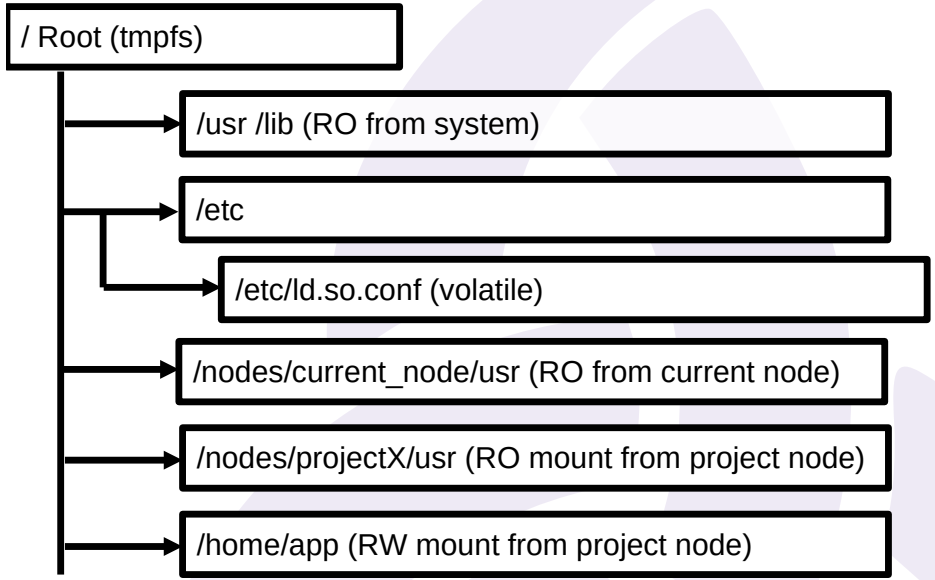


Nodes




```
/var/nodes/
├── plateform1
│   ├── etc
│   ├── usr/lib64/…
│   ├── profile1
│   │   ├── etc
│   │   ├── usr/lib64/...
│   │   ├── var/lib/rpm/…
│   │   ├── project1
│   │   │   ├── etc
│   │   │   ├── usr
│   │   │   └── bin
│   │   └── project2...
│   ├── profile2
│   └── profile3
└── plateform2...
```

RUNTIME



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
```

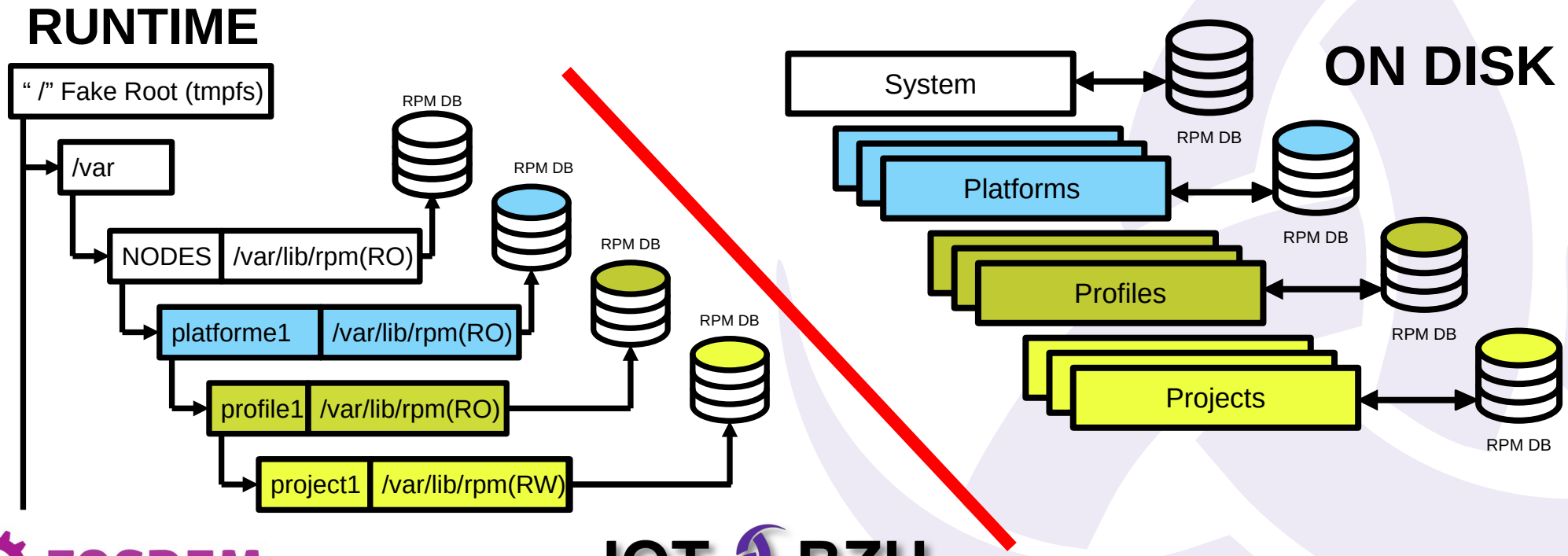
IOT BZH

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
```

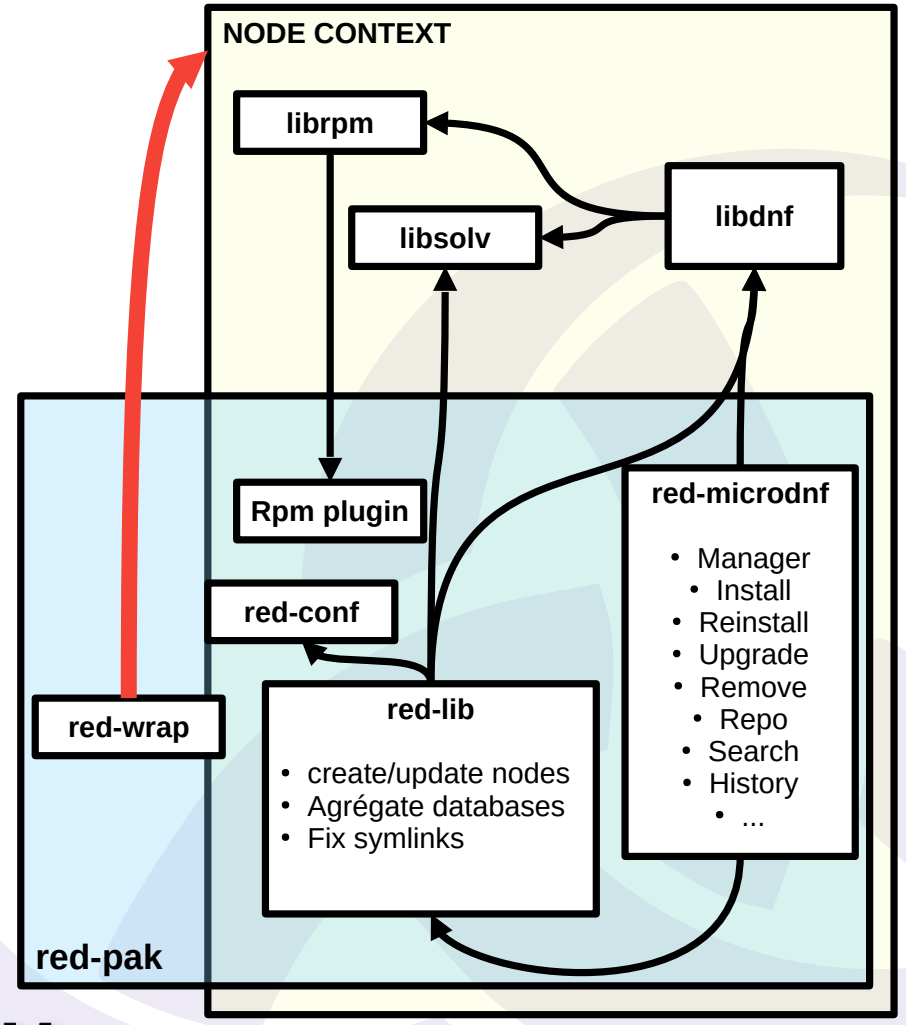
Rpm databases

- 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

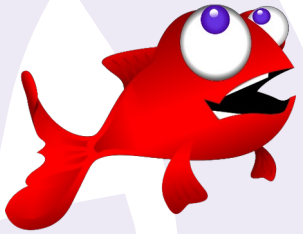
Starting Time	X86_64: Qemu (ms)	Aarch64: NXP (ms)	Aarch64: Xilinx (ms)
redpak	18	150	58
LXC	59	254	191
Podman	606	1 706	1 570
Systemd-nspawn	291	1 516	858

Container's Engine Resident Set Size	X86_64: Qemu (kB)	Aarch64: NXP (kB)	Aarch64: Xilinx (kB)
redpak	2920	2 308	2 336
LXC	3 108	2 736	2 732
Podman	32 108	31 220	31 156
Systemd-nspawn	14 712	12 632	12 696

- Short startup time adapt to embedded
- Good memory use

Links

- **Redpak**
  - Sources: https://github.com/redpesk-labs/red-pak
  - On redpesk OS: *dnf install red-pak*
- **red**pesk®
  - Website: https://redpesk.bzh/
  - Documentation: https://docs.redpesk.bzh/
  - Sources: https://github.com/redpesk/readme
- **IoT.bzh**
  - Website: https://iot.bzh/
  - Publications: https://iot.bzh/en/publications
  - Vidéos: https://vimeo.com/search?q=redpesk
- **Comunnautary Support**
  - Matrix.org: +redpesk:matrix.org



redpesk®