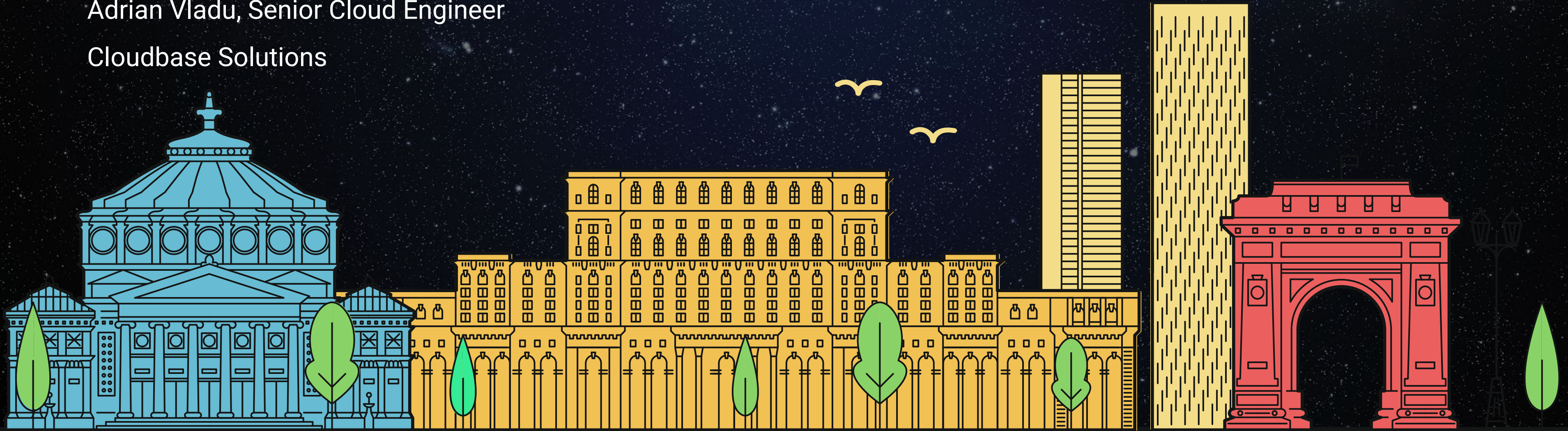
6th of May 2025

The first CNCF OS
Flatcar Container Linux

Alessandro Pilotti, CEO

Adrian Vladu, Senior Cloud Engineer

Cloudbase Solutions



solutions
cloudbase

www.cloudbase.it

About us

Adrian Vladu - Senior Cloud engineer / Flatcar Container Linux maintainer

Github: @ader1990

Email: avladu@cloudbasesolutions.com

Alessandro Pilotti - CEO

Github: @alexpilotti

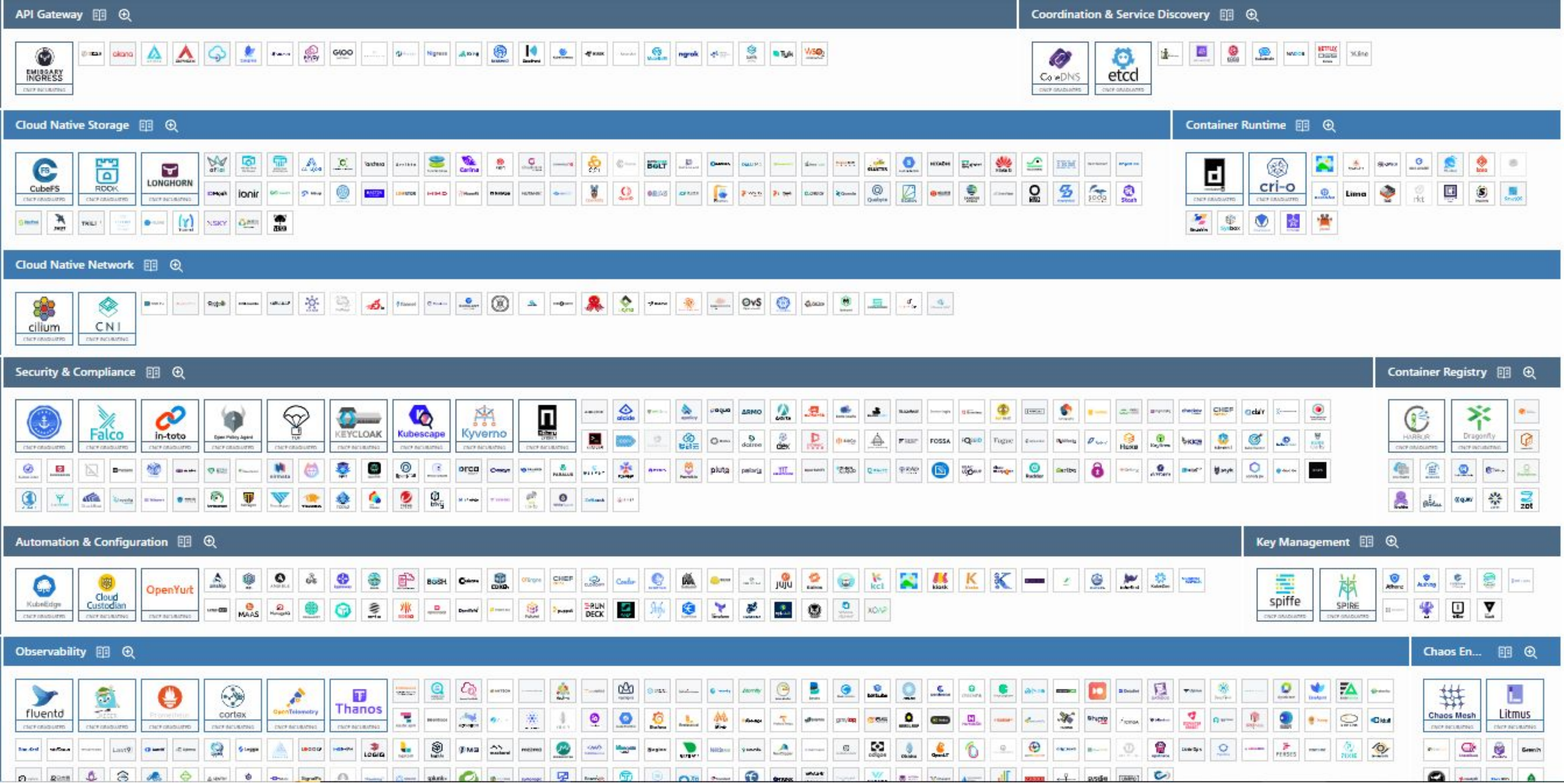
Email: apilotti@cloudbasesolutions.com

Outline

- About Flatcar Container Linux
- The Basics - demo time
- AI deployments with Flatcar
- The AI - demo time
- Hyperlight with Flatcar
- Hyperlight - demo time

Flatcar Container Linux

- **Compact, easy** to run OS
- **Image** based
- **Secure and reliable** by design
- Tailored for containerization, kubernetization: **cloud-native** world



API Gateway

Coordination & Service Discovery

Cloud Native Storage

Container Runtime

Cloud Native Network

Security & Compliance

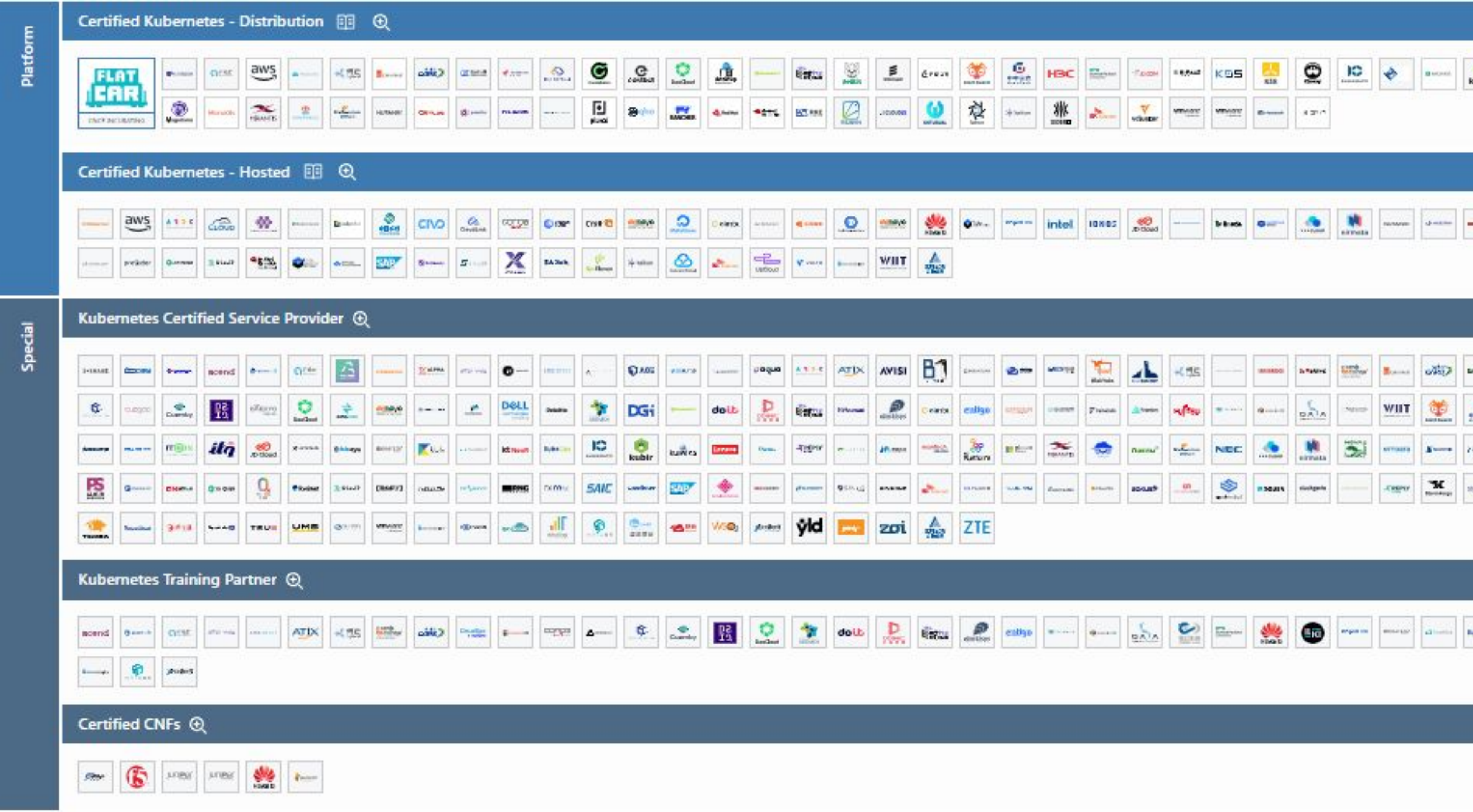
Container Registry

Automation & Configuration

Key Management

Observability

Chaos En...



Platform

Certified Kubernetes - Distribution

Certified Kubernetes - Hosted

Special

Kubernetes Certified Service Provider

Kubernetes Training Partner

Certified CNFs

CNCF and Flatcar Container Linux

- **Flatcar Container Linux** was accepted to **CNCF** on 2nd of August 2024
- **Incubating** maturity level - going for Graduation
- The only **OS** in the CNCF `matrix`
- https://www.cncf.io/projects/flatcar-container-linux/

Flatcar Ancestry

- Drop-in replacement for **CoreOS**
- Downstream fork of **Gentoo**

Flatcar Pedigree

- **Immutable** OS
- **Image** based OS
- Similar but not the same to:
  - Fedora COREOS
  - openSuse Leap Micro
  - ParticleOS
  - Talos
  - Kairos

Flatcar Images

- Small image footprint ~ **500MB**
- Only **300** source packages
- /usr partition uses btrfs **compression**
- /boot partition uses native **compression**
- Initrd and grub binaries are already **compressed**

Flatcar Images

- Supported **architectures**
  - AMD64
  - ARM64
  - RISC-V (work in progress - PoC presented at **FOSDEM** 2025**)**

Flatcar Images - Supported OEMs

- AWS
- Azure
- Google Cloud
- DigitalOcean
- Scaleway
- Packet/Equinix
- Hetzner
- Akamai
- OpenStack
- QEMU
- Hyper-V
- VMware
- Proxmox
- KubeVirt

Flatcar Images - Built-in Security

- **Immutable /usr** partition
- **A/B** partitioning scheme for updates
- **dm-verity** (against live attacks)
- Supports **Secure Boot**
- Systemd-sysexts are also **immutable**
- **LUKS2** encryption (TPM and HSM/SYSTEMD, CLEVIS/TANG)
- https://www.flatcar.org/docs/latest/reference/supply-chain/

Flatcar Images - Updates

- **Rolling** release channels - released **every month**
  - Alpha
  - Beta
  - Stable
- LTS - **18 months** support with yearly cadence, updated each month
- https://www.flatcar.org/releases

Flatcar Images - Updates

- **Nebraska** project to control the updates lifecycle (similar to **Landscape**/**Foreman**)
  - https://github.com/flatcar/nebraska
- Updates are **atomic** with **rollback on failure**
- https://www.flatcar.org/docs/latest/setup/releases/update-strategies/

Flatcar Images - Bootstrapping

- **ignition** vs **cloud-init**
- **initrd** based (early boot, before switch_root pivot)
- Capabilities:
  - Storage
  - Systemd
  - Networking
  - Users
- OpenStack OEM (coreos-metadata)
- https://github.com/coreos/ignition
- https://github.com/coreos/ignition/blob/main/docs/configuration-v3_0.md

Flatcar Container Linux - Purpose

- To run **containers**

Flatcar Container Linux - Composability

- How do you extend an **immutable** system?
- **systemd-sysext**

Flatcar Container Linux - Composability

- **Docker** systemd-sysext
- **Containerd** systemd-sysext

Flatcar Container Linux - Basic Demo

- Basic **Hyper-V** or **QEMU** based demo
- https://www.flatcar.org/docs/latest/installing/vms/hyper-v/
- https://www.flatcar.org/docs/latest/installing/vms/qemu/

Flatcar Container Linux - Composability

- https://flatcar.github.io/sysext-bakery/
- https://travier.github.io/fedora-sysexts/
- Other Container runtime:
  - crio
- K8S
  - Kubernetes (vanilla)
  - K3S
  - RKE2
- Applications
  - Falco, Tailscale
  - Nvidia drivers
- Wasm
  - Wasmtime
  - Wasmcloud
  - Wasmedge

Flatcar Container Linux - Composability Demo

- Demo time
- **K3S** Hyper-V based demo
  - `curl -sfL https://get.k3s.io > k3s-install.sh`
  - `INSTALL_K3S_SKIP_DOWNLOAD="true" bash -x k3s-install.sh`
- https://www.flatcar.org/docs/latest/installing/vms/hyper-v/

Flatcar Container Linux - Advanced Composability

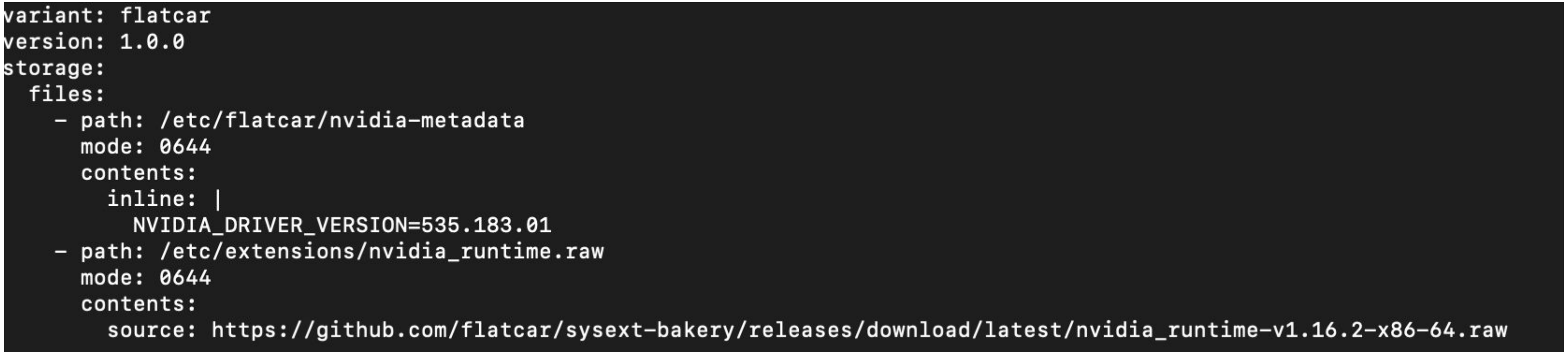
- Cluster API managed Kubernetes
- https://cluster-api.sigs.k8s.io/
- https://github.com/cloudbase/bmk
- Use K8s to manage the lifecycle of K8S clusters

Flatcar Container Linux - Decoupling K8S

- https://github.com/flatcar/flatcar-demos/tree/main/FOSDEM2025/kubernetes-plumbing
- The lifecycle of **K8S** is decoupled from the lifecycle of the **Flatcar Container Linux**
- Download the new sysext, refresh the sysext, restart kubelet

Flatcar Container Linux - NVIDIA Drivers

- Dealing with NVIDIA drivers can be challenging
  - Linus Torvalds: “*NVIDIA has been the single worst company we've ever dealt with. So, NVIDIA, (omissis).*”
- Need to match driver version and CUDA version with GPU
- For Docker, the Nvidia runtime is needed
- Flatcar makes all this very easy to deploy with a Butane config file
- **Demo time**



```
variant: flatcar
version: 1.0.0
storage:
  files:
    - path: /etc/flatcar/nvidia-metadata
      mode: 0644
      contents:
        inline: |
          NVIDIA_DRIVER_VERSION=535.183.01
    - path: /etc/extensions/nvidia_runtime.raw
      mode: 0644
      contents:
        source: https://github.com/flatcar/sysext-bakery/releases/download/latest/nvidia_runtime-v1.16.2-x86-64.raw
```

Flatcar Container Linux - Hyperlight

- Beyond containers
  - **Bare Metal -> VMs -> Containers -> Serverless**
- The challenge:
  - **Speed** - spawning workloads within **milliseconds**
  - **Security**
    - Sandboxing workloads with VM primitives without VMs (**Micro VMs**)
    - Limiting attack surface -> eliminate unnecessary host and guest features
- The lineage:
  - Google crosvm
  - Amazon Firecracker
  - Rust-VMM
  - Insula (Cloudbase + CrowdStrike project) - Predates Firecracker
  - Hyperlight
- **Demo time**

Flatcar Container Linux - Takeaways

- **Simple**, slim and easy to use
- **Composability** is powerful
- More and more use-cases at the **edge**
- **AI / Bleeding edge software ready**

Flatcar Container Linux - Questions

Questions, questions, questions

Flatcar Container Linux - Resources

- https://www.flatcar.org
- https://www.flatcar.org/releases
- https://github.com/flatcar/sysext-bakery