A fundamental step to Telco Cloud & Edge homogenization and sustainability

Every cloud has a SYLVA lining
Content

1. Why Sylva?

2. Our approach

3. What we deliver
CSPs began their journey in Telco Cloud and edge almost a decade ago. However, some challenges remain to solve.

**Market analysis**

- **Siloed approach**
  - Historical Model doesn’t fit with multivendor approach
  - #Shift to a common Cloud Layer

- **Security threats**
  - Operators are increasingly threatened by hackers*
  - #Invest in Security

- **New network functions**
  - New Network Functions require Cloud native infra and distributed Cloud (O-RAN, 5G core, CDN)
  - #Shift from VNF to CNF

- **Lack of automation**
  - Continuous Innovation & Service Automation to shorten the TTM and reduce OpEx
  - # Telco cloud and edge automation

*GSMA 2022 Security Report*
Why Sylva?

Mission statement

The main carriers in Europe, together with network function providers, initiated the Sylva project to address Telco and Edge use cases.

The project objectives are:

- To release a cloud software framework tailored for telco and edge requirements that address the technical challenges of the industry layer of this ecosystem.

- To develop a reference implementation of the cloud software framework and create a validation program for such implementations.
## Why Sylva?

### Opportunities we want to unblock

<table>
<thead>
<tr>
<th>Technology</th>
<th>Business</th>
<th>Ecosystem</th>
<th>Regulation / Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological backwardness</td>
<td>Proprietary solutions <strong>Lock In</strong></td>
<td>Fragmentation of solutions</td>
<td><strong>Strong regulation</strong></td>
</tr>
<tr>
<td>Slow innovation</td>
<td>High <strong>prices</strong></td>
<td><strong>Hyperscallers entry</strong></td>
<td><strong>High cyber risk</strong></td>
</tr>
<tr>
<td><strong>Open-source</strong> instead of proprietary solutions</td>
<td><strong>Reduce cost</strong> (open source, mutualization)</td>
<td><strong>Common Telco Cloud technology</strong></td>
<td><strong>Compliance with European regulation</strong></td>
</tr>
<tr>
<td>Simplify &amp; automate the operational model</td>
<td><strong>Interoperability</strong> (validation program, large adoption)</td>
<td><strong>Convergence</strong> of the telco cloud layer</td>
<td><strong>High security standards</strong></td>
</tr>
</tbody>
</table>

### Current Threats for Telcos

- Technological backwardness
- Proprietary solutions **Lock In**
- Fragmentation of solutions
- **Strong regulation**
- Slow innovation
- High **prices**
- **Hyperscallers entry**
- **High cyber risk**

### Opportunities Through Sylva

- **Open-source** instead of proprietary solutions
- **Reduce cost** (open source, mutualization)
- **Common Telco Cloud technology**
- **Compliance with European regulation**
- Simplify & automate the operational model
- **Interoperability** (validation program, large adoption)
- **Convergence** of the telco cloud layer
- **High security standards**
Our approach

The five technical pillars

Network performance

Distributed cloud

Security

Open Source

Energy efficiency

Network Performance to answer to CNF requirements and performance
Telco features: SR-IOV, DPDK, Low latency, Specific CNI CaaS on BareMetal

Distributed cloud

BM Automation: Declarative approach & Gitops to manage thousands of heterogenous nodes
MultiK8S: Optimized lifecycle Management of many K8S Clusters in DC

Best in Class Security Design

Answer Telco grade requirements

Open source and standardized API

Support multi-Vendor CNF & boost market adoption

Energy efficiency

Measure & Optimize to limit Energy Consumption

New version
Our approach

Summary of workgroups under Sylva TSC

#01 Telco Cloud Stack
Mathieu Rohon
Orange

#02 Validation Center
Luis Velarde
Telefónica

#03 EUCS Security
Théophile Debauche
Orange

#04 Energy Efficiency
S Kannan
Nokia

NEW

#05 Communication & Adoption
Andre Antunes
Celfocus

NEW

#06 Evolution of Governance
Théophile Debauche
Orange

Technical Steering Committee
with Orange, DT, TIM, TEF, Vodafone, Nokia & Ericsson at the board

Sylva Co-Chairman: Giuseppe Ferraris (TIM) & Guillaume Nevicato (Orange)
Content

1. Why Sylva?
2. Our approach
3. What we deliver
## Sylva adoption benefits

### Current State

**Telecom Operators**
- Siloed approach that leads to higher costs
- High TTM for new services
- Different reference architectures among Telcos that delays the innovation

**Network Function Providers**
- Heterogeneous cloud layer that increases the complexity of delivering the network functions SW releases to different Telecom Operators

**System Integrators**
- High risk projects due to difficult integration and support
- Lack of compliance with regulation & high security standards

**HW/infra providers**
- Lack of Telco-grade capabilities visibility
- Custom development

### Future State

**Telecom Operators**
- **Common cloud layer** and reference architecture for CaaS among Telcos that will reduce costs
- **Create a cloud continuum** and guarantees compatibility among operators in the MEC Federation initiative (Operator Platform)
- Create a Sylva reference NF validation process that decreases the TTM of new services, market prospect of NF, and the certification cost/time of NF.

**Network Function Providers**
- Homogenous cloud layer that enables the build once deploy many, in different Telecom Operators
- **Reduce cost and time** in certification in Operators’ infra by leveraging the validation process on Sylva as a reference
- Provide an environment to test the Telco-grade capabilities required by the NF

**System Integrators**
- **Systems interoperability** and compliance with regulation & high-security standards
- **New business opportunity** to:
  - Create a distribution out of Sylva;
  - Provide support for deployments of Sylva in Operators
  - Provide a validation service to NFs

**HW/infra providers**
- Obtain information on the Telco-grade capabilities expected by Operators from a CaaS and on NFs that must be certified in their own CaaS solution
- **Reduce cost** in testing by incorporating capabilities integrated as OpenSource in Sylva
- Showing the HW can enable the capabilities required for a horizontal platform
- **Standardize developments** using Sylva

---

Orange Restricted
What we deliver

Open-Source ecosystem

Project Synergies

- Anuket (RA2/RC2) covers the specifying, integrating and verifying Telco-specific stacks and the validation of Telco applications
  - Sylva will leverage RA2 and cover requirements specifics to European Telcos
  - Sylva will contribute back specific extensions to Anuket
  - Note: Anuket is requirements driven, while Sylva is implementation driven. Also, Sylva is intended to be an implementation of Anuket as RC2 compliant.
- CNCF provides necessary components such as OSS projects (K8S) and validation programs (CNF)
  - Leverage K8S as part of the software framework
  - Contribute extensions that address Telco needs
  - Build on top of CNF Validation program
- The O-RAN Software community develops many of the workloads that will use the telco CaaS
  - Address requirements of O-RAN workloads (e.g. synchronization cards)
  - Provide feedback to the O-RAN-SC and O-RAN workgroups
- Sylva is based on open-source components such as GitOps, Service Mesh and will integrate with the software coming from the LF Networking and Edge umbrella projects
- Sylva will align with the specifications and recommendations of organizations like Gaia-X (Secure and sovereign data management), MITRE and ENISA (Security). It will provide feedback, as necessary, to these organization for further improvements of the specifications.
To address such use case as 5GCore Distributed UPF, CDN or Open RAN, Sylva will provide an architecture able to manage from Central to far edge site.

*this is an example on how SYLVA could be deployed in a multi cluster environment
**What we deliver**

HLD

Gitops Tool: **Flux**

K8s cluster manager: **CAPI**

Coordinate with Rancher engineering teams:
- For ClusterAPI rke2 bootstrap provider: [https://github.com/rancher-sandbox/cluster-api-provider-rke2](https://github.com/rancher-sandbox/cluster-api-provider-rke2)
- For BareMetal management with Metal3: [https://github.com/rancher-sandbox/baremetal](https://github.com/rancher-sandbox/baremetal)
The **sylva-core** ([https://gitlab.com/sylva-projects/sylva-core](https://gitlab.com/sylva-projects/sylva-core)) project provides tools to let you choose what will compose your Sylva stack. It is hosting:
- scripts to operate the stack
- a **sylva-unit helm chart** used to deploy flux objects
- some value examples used to build the sylva stack that fits your need
What we deliver

Validation centre: Scope

Validation program has two parts **CNF validation** & Derivative stack validation

---

**CNF validation (Ongoing)**

- Demonstrate CNFs can work on top of SYLVA stack
- First official validations against Sylva release v1
- Run over a validation platform (reference implementation of a Sylva stack release)
- Not a complete certification (onboarding + basic functional test)
- Leverage Anuket assets (CNCF test suit, functest)

**Derivative stack (distribution) validation (To be started)**

- Demonstrating distributions include the capabilities required
- Will leverage the tests defined for each Sylva release
- Will make use of “dummy CNFs” or “validated CNFs” to test the capabilities
- Leverage Anuket assets (k8s_conformance testing, xtest)
- Distributions must exist in order to validate them, only after Sylva v1 is released

---

Sylva aims to release an Open Source cloud software framework integrating the capabilities required for telco and edge workloads.

Sylva uses as a reference the requirements from existing organizations (e.g.: Anuket, O-Ran, Enisa, ...)

---

**Main Benefits**

- Interoperability, no lock-in;
- NF portfolio validated in the validation program;
- Compliance with regulation and high security standards.

---

*Sylva*

Sylva aims to release an Open Source cloud software framework integrating the capabilities required for telco and edge workloads.

Sylva uses as a reference the requirements from existing organizations (e.g.: Anuket, O-Ran, Enisa, ...)

---

**Main Benefits**

- Interoperability, no lock-in;
- NF portfolio validated in the validation program;
- Compliance with regulation and high security standards.
Validation center: CNF validation process

What we deliver

1 - Identify platform capabilities required by CNF
   CNF provider support

2 - Install & configure reference platform with required capabilities

3 - Onboard CNF under test in reference platform
   CNF provider support

4 - Confirm CNF onboarding

Run minimum functional verification scripts and generate report

Operators may run any additional functional testing before deciding and/or deploying the CNF in production

5 - Identify minimum CNF functional test
   CNF provider support

6 - Define steps/commands to provision CNF and run minimum CNF functional verification
   CNF provider support

7 - Create script to run Steps for functional verification
Validation center: Time plan summary

**What we deliver**

- **M1:** Successful execution of platform smoke tests and additional CNF's vendor platform performance tests/commands
- **M2:** Successful installation of "dummy" Helm chart to check platform capabilities
- **M3:** Confirm that CNF's images and charts are accessible from the cluster
- **M4:** Confirm that the CNF is correctly deployed in the cluster
- **M5:** Successful CNF's functional testing

**Timeline:**

- **WEEKS 1-2:** Configure validation platform
- **WEEKS 3-4:** CNF on-boarding and instantiation
- **WEEKS 5-6:** CNF functional testing
Sylva Partner adoption
A huge reach in a few months since the public launch

Contribution under evaluation

Mobile NF
Fix NF
IT editor

Integrators

NDA eGate
MOU eGate
Sylva Creation
Press Release
First public code release

Orange Restricted
# What we have done in 2022

## Use cases integration

<table>
<thead>
<tr>
<th>Use cases integration</th>
<th>June-2022 Alpha</th>
<th>7th Nov-2022 Beta</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>O-RAN CNF</strong></td>
<td>5GCore CNF</td>
<td>UDM</td>
</tr>
<tr>
<td><strong>Other CNF</strong></td>
<td>AMF</td>
<td>Speed Server</td>
</tr>
<tr>
<td><strong>5GC IT Tooling</strong></td>
<td>5GC IT</td>
<td></td>
</tr>
</tbody>
</table>

## Cloud Features

### Security
- Central authentication & Secret
  - **K8S distro**: RKE, RKE2

### Automation
- Script to deploy MultiCluster K8S Management (Rancher) & Workload Cluster
- **Deployment Model**
  - CaaS on libvirt

### Reference Architecture & Objectives
- in LF Architecture / Sylva
  - **Security**: PKI integration
  - **BM**: BM automation exploration
  - **Storage**: Ceph
  - **Operational** monitoring tooling
  - **Testing** CI with K8S Anuket Xtesting
  - **Deployment Model**
    - Pilot CaaS on Vsphere (limited)/Openstack
    - Exploration CaaS on BM (without full BM Automation)
What we deliver

What will be done in 2023

1st public release

April V0.1

- K8S distro: K8S Vanilia & RKE2
- OS: Ubuntu
- BM automation (CAPI, Metal3)
- Storage: Cinder (Openstack)
- Deployment Model
  - Pilot Caas on BM
  - CAPV (Capi on Vsphere) / Vsphere CSI
  - CAPO (Capi on Openstack)
- Security -WG03
  - First EUCS conformity evaluation (sovereign cloud)

June V0.2

- K8S distro: additional distro /which use cases
- OS Management
  - RealTime Module, explore Immutable OS
- Acceleration & Perf
  - SRIOV, DPDK, NUMA, Kubevirt with DPDK Pilot
- Deployment Model
  - Workload Cluster Management
  - Caas on BM (enhanced LCM on BM)
  - CAPD Workload Cluster (new Dev&CI)
- Storage: Longhorn
- LAN Automation
  - Exploration Netw Modelisation and L2 VLAN automation (SONIC ? ENO ?, etc …)
- Monitoring: per Cluster then federated Solution
  - RBAC implementation
- Security -WG03
  - EUCS requirements: IAM, SOC, Hardening

Nov V0.3

- K8S Distro: additional distro /which use cases
- OS Management
  - RealTime Module, explore Immutable OS
- Acceleration & Perf
  - SRIOV, DPDK, NUMA, Kubevirt with DPDK Pilot
- Deployment Model
  - Workload Cluster Management
  - Caas on BM (enhanced LCM on BM)
  - CAPD Workload Cluster (new Dev&CI)
- Storage: Longhorn
- LAN Automation
  - Exploration Netw Modelisation and L2 VLAN automation (SONIC ? ENO ?, etc …)
- Monitoring: per Cluster then federated Solution
  - RBAC implementation
- Security -WG03
  - EUCS requirements: IAM, SOC, Hardening

RAN

- CU-ORAN

Core

- SIG
- free5GC

Fix & Edge

- CDN

Cloud Features

- CI: Auto test to enhance
- OS: Suse OS
- Acceleration & Perf
  - SRIOV, DPDK, NUMA, Kubevirt with DPDK Pilot
- Deployment Model
  - Workload Cluster Management
  - Caas on BM (enhanced LCM on BM)
  - CAPD Workload Cluster (new Dev&CI)
- Storage: Longhorn
- LAN Automation
  - Exploration Netw Modelisation and L2 VLAN automation (SONIC ? ENO ?, etc …)
- Monitoring: per Cluster then federated Solution
  - RBAC implementation
- Security -WG03
  - EUCS requirements: IAM, SOC, Hardening

Edge

- Edge automation
- Edge App
- Federation CAMARA
- Edge WG

Network

- CDN
- FW
- SDWAN
- VNF via Kubevirt

Last TSC Update 05/04/2023
Thank you