OpenNebula

PROWLER

FOSDEM

Arming Cloud Computing Continuum: Hunting vulnerabilities in open source hybrid clouds

Jordi Guijarro
Principal Technologist Cloud-Edge Innovation @ OpenNebula Systems

OpenNebula.io

Hello, FOSDEM!

OpenNebula

Jordi Guijarro | **Principal Technologist Cloud-Edge Innovation** at OpenNebula Systems

➔ **Jordi Guijarro Olivares is the Principal Technologist for Cloud-Edge Innovation at OpenNebula Systems. With over 20 years of experience, he is an expert cloud-oriented and cybersecurity architectures applied Innovation.**

➔ **He currently manages the EU IPCEI-CIS ONEnextgen project ecosystem, coordinates the Virt8ra.eu Cluster, and actively participates in various national and European projects.**

➔ **Course instructor at UOC and UPC Cybersecurity Masters (Cloud Security and Digital Identity)**

Table of Contents

OpenNebula

1 **What is OpenNebula?**
Open... What?

2 **Open Source CSPMs**
Born for help

3 **Prowler and OpenNebula**
The perfect couple ❤️

4 **Live Demo 🎬: Let's see it in action!**
A CSPM in the Far Edge

5 **Key Takeaways**
MCPs, Automatic remediation,...

Edge Computing Observatory

What is edge?

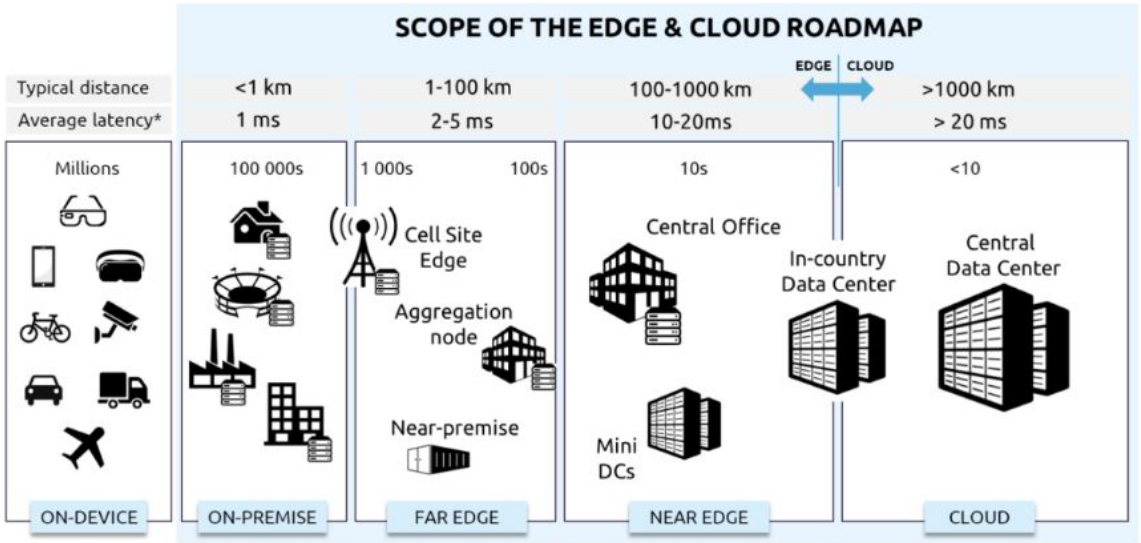
European Commission

English Search

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > Policies > Edge Observatory for the Digital Decade – Monitoring the Deployment of Edge Nodes



https://digital-strategy.ec.europa.eu/en/policies/edge-observatory

Edge Computing Observatory

What is edge?

Edge nodes measured as the number of compute nodes providing **latencies below 20 milliseconds**, such as an individual server or other set of connected computing resources, operated as part of an edge computing infrastructure, typically residing within an edge data centre operating at the infrastructure edge, and therefore physically closer to its intended users than a cloud node in a centralised data centre, designed and operated:

- **in an energy-efficient manner** to minimize its carbon footprint and environmental impact, with a specific focus on reducing greenhouse gas emissions, to achieve a net-zero carbon impact
- **at the edge of a network** to provide secure access to data and services. It must provide both **physical and cyber security** to ensure uninterrupted operation and data safety.

https://digital-strategy.ec.europa.eu/en/policies/edge-observatory

Advancing Europe's Federated Cloud-Edge Infrastructure

Second Version of the IPCEI-CIS Reference Architecture Released

With the release of Version 2.0 of the IPCEI-CIS Reference Architecture (ICRA), the 8ra Initiative continues to support building a sovereign, interoperable digital infrastructure for Europe. The ICRA offers a structured framework to guide the development of a federated Multi-Provider Cloud-Edge Continuum capable of supporting the next generation of data-driven applications across sectors such as manufacturing, mobility, energy as well as the integration of AI.

https://www.8ra.com/wp-content/uploads/IPCEI-CIS_Reference-Architecture_2-0.pdf

Far-Edge & IoT: The O-CEI Model

OpenNebula

O-CEI is an EU-funded Horizon Europe project to orchestrate the **Cloud-Edge-IoT continuum**. It uses a **Blueprint-Driven Methodology** to translate high-level requirements into repeatable **technical deployments** across **8 different pilots,** such as electricity grids, agrifood or logistics, with **high technical maturity** (**TRL 7**).

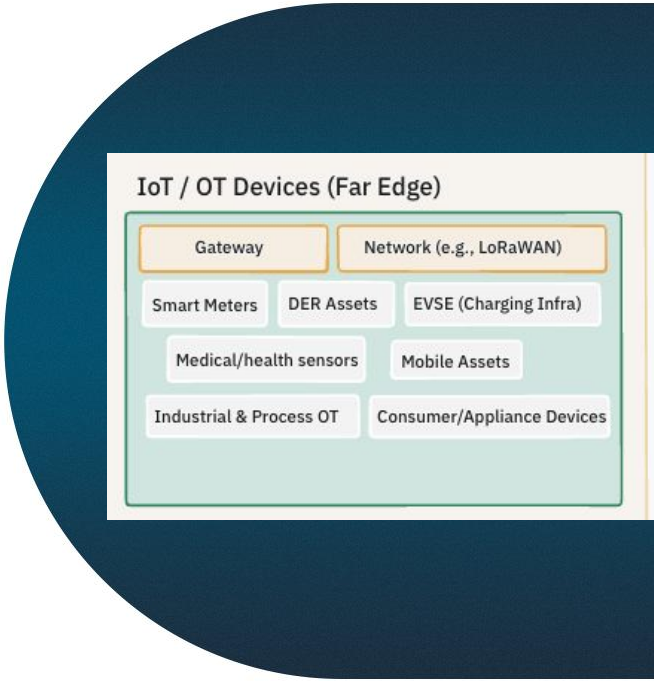
O-CEI

- **Practical Extension**

In O-CEI, we have successfully extended the framework by adding a **Far-Edge / IoT** layer specifically to manage small, low-power devices and sensors at the industrial ground level.

- **Our Proposal for IPCEI v3.0**

We propose exploring the addition of this same layer to the **next ICRA version** to finally **connect** everything from the **Data Center** down to the **individual IoT device or sensor**.



1 What is OpenNebula?

Who is OpenNebula Systems?

The **Open-Source Company** behind the OpenNebula **Cloud & Edge Computing Platform**

- First open source **IaaS** solution, created **17 years ago.**
- **Enterprise infrastructure software** company with **15 years of experience**.
- HQs in **Madrid** (Spain, EU) and **Burlington** (MA, US), and offices in Brussels (BE, EU) and Brno (CZ, EU).
- Scaling-up from 2024 thanks to the **IPCEI-CIS** EU funding program.

OpenNebula: Open-Source Cloud Platform

OpenNebula

The **open source platform** for the cloud-edge continuum

OpenNebula is an **open-source cloud management platform** that unifies **VMs, containers, and Kubernetes** under a **single pane of glass**. From data centers to edge nodes, it orchestrates workloads across the entire cloud-edge continuum.

Multi-Hypervisor

KVM & LXC containers

Hybrid & Multi-Cloud

Integration with AWS, **Scaleway**, **OVH cloud**, and more!

ARM64 Native

Full support since v7.0

Kubernetes Ready

Cluster API, OneKE, **RKE2**

AI-ready platform

OneDRS + **MCP** integration

Enterprise Features

Multi-tenancy, **federation**, HA

Why OpenNebula for Edge Computing?

OpenNebula

Feature / Platform	OpenNebula 7.0	Proxmox	VMware / CloudStack
ARM Support	✓ **Yes** (Native)	✗ Unofficial / Experimental	✗ No (x86 only)
Marketplace **ARM** Images	✓ **Yes** (Native)	✗ No official ARM templates	✗ No
Installation Simplicity	✓ **Simple** (MiniONE/OneDeploy)	Complex / Unsupported	✗ Unsupported on ARM
Resource Efficiency	✓ **Very High**	High (x86 only)	Low (x86 only)
Edge / IoT Use Cases	✓ **Native Support**	Limited	✗ Not designed for Edge

OpenNebula leads in ARM and edge deployments — the clear choice for edge computing and IoT.

2

Open Source CSPMs and the Cloud Continuum

Defining the Computing Continuum

The transition from **Device Edge** to **Public Cloud** is no longer a binary choice but a fluid reality.

IoT Edge:
Sensors and actuators generating raw data.

Fog Nodes:
Open-source orchestration (For Example OpenNebula).

Private Core:
Open-source orchestration (For Example OpenNebula).

The "Hunting" Ground: Vulnerabilities

Orchestration Gaps

Security drifts between public cloud APIs and private KVM/LXC clusters.

Credential Leakage

Plaintext secrets in VM templates and CI/CD pipelines at the edge.

Breakout Risks

Container escapes targeting underlying hybrid infrastructure hosts.

The Challenge of Hybrid Clouds and CSPMs Gap

OpenNebula

Centralized Clouds

- **Far** from data sources
- **High** latency
- **Expensive** Bandwidth

Edge Computing Needs

- Process data **locally**
- **Sub-millisecond response** times
- Work **offline** or with limited connectivity

The CSPMs Gap

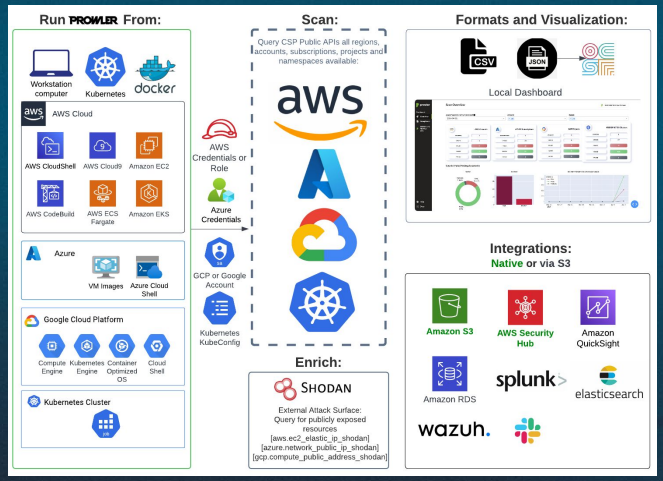
- Enterprise platforms too heavy
- **DIY** solutions are manual and slow
- **Distributed control planes** scenario

What if you could run security posture checks where is needed?

With Prowler for OpenNebula under native ARM64 support, now you can.

3

Prowler and OpenNebula



New Prowler Provider: OpenNebula

We present a new extension to **Prowler**, **the leading FOSS cloud security tool**, adding native support for OpenNebula.

The contribution delivers a modular, non-intrusive framework that allows operators to audit sovereign hybrid clouds with the same way as hyperscale providers.

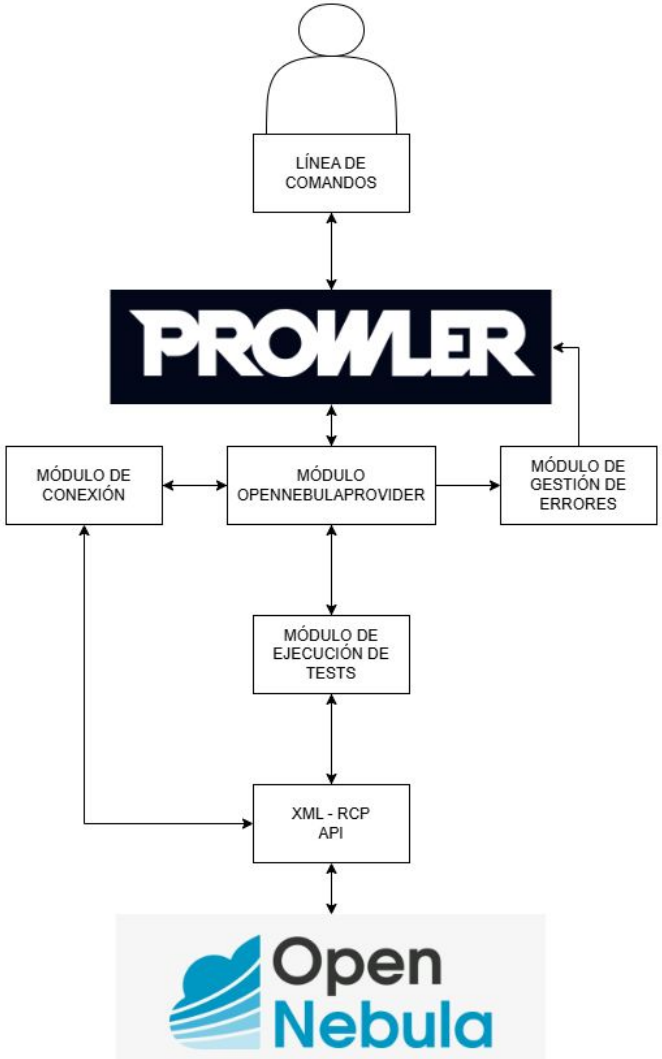
Provider	Service	Status	Critical	High	Medium	Low	Muted
aws	accessanalyzer	FAIL (1)	0	0	0	1	0
aws	account	FAIL (1)	0	0	1	0	0
aws	lambda	FAIL (1)	0	0	0	1	5
aws	backup	FAIL (1)	0	0	0	1	0
aws	cloudformation	FAIL (5)	0	0	5	0	3
aws	cloudtrail	FAIL (4)	0	0	1	3	9
aws	cloudwatch	FAIL (19)	0	0	19	0	6
aws	config	PASS (1)	0	0	0	0	0

THANKS to Daniel Rontomé (@rontomano) and Toni de la Fuente (@toniblyx)

https://github.com/rontomano/TFM_prowler/

Design & Implementation Logic

- **XML-RPC API Integration:** Mapping of OpenNebula resources to Prowler providers.
- **Resource Mapping:** Auditing VMs, VNETs, Images, and IAM roles across zones.
- **Check Engine:** Extensible Python-based checks aligned with CIS Benchmarks.
- **Zero-Trust Auditing:** Verifying host registration and template sanitization.



Security Services and Controls

Audit Category	Specific Security Controls	Standard Alignment
Identity (IAM)	MFA, Overly permissive roles, Admin password policies	CIS 1.0 / NIST
Networking	VLAN Isolation, Exposed XML-RPC, Firewall status	SOC 2
VM Infrastructure	Unencrypted storage images, Template sanitization	GDPR / CIS
Compliance	Evidence collection for NIS2 and DORA directives	EU Directives

4

Live Demo 🎬: Let’s see it in action!

Raspberry Pi + OpenNebula: It's a match!

OpenNebula

Raspberry Pi meets OpenNebula

Hardware

Device:	Raspberry Pi 5 (BCM2712)
RAM:	**4GB / 8GB Recommended**
Storage:	NVMe SSD (PCIe) preferred
Network:	Gigabit Ethernet / PoE+
Cost:	**50€ - 100€** (8GB)

Software Stack

OS:	**Ubuntu** Server 24.04 LTS
Hypervisor:	KVM with ARM
Platform:	OpenNebula 7.0 "Phoenix"
Web UI:	FireEdge Sunstone
Marketplace:	**Pre-built ARM64 Appliances**

Two deployment paths:

MiniONE — Quick single-command setup for testing & development

OneDeploy — Ansible-based IaC for production deployments

MiniONE

From zero to cloud in less than **2 minutes**

OpenNebula

MiniONE is a **single-script installer** designed to deploy a full OpenNebula stack on a single machine. Optimized for Edge nodes, labs, and PoC environments.

1 Flash Ubuntu

Flash Ubuntu Server 24.04 LTS (**ARM64**) to your microSD or SSD.

2 Update System

Ensure the **local package** is updated.

3 Execute the MiniONE script

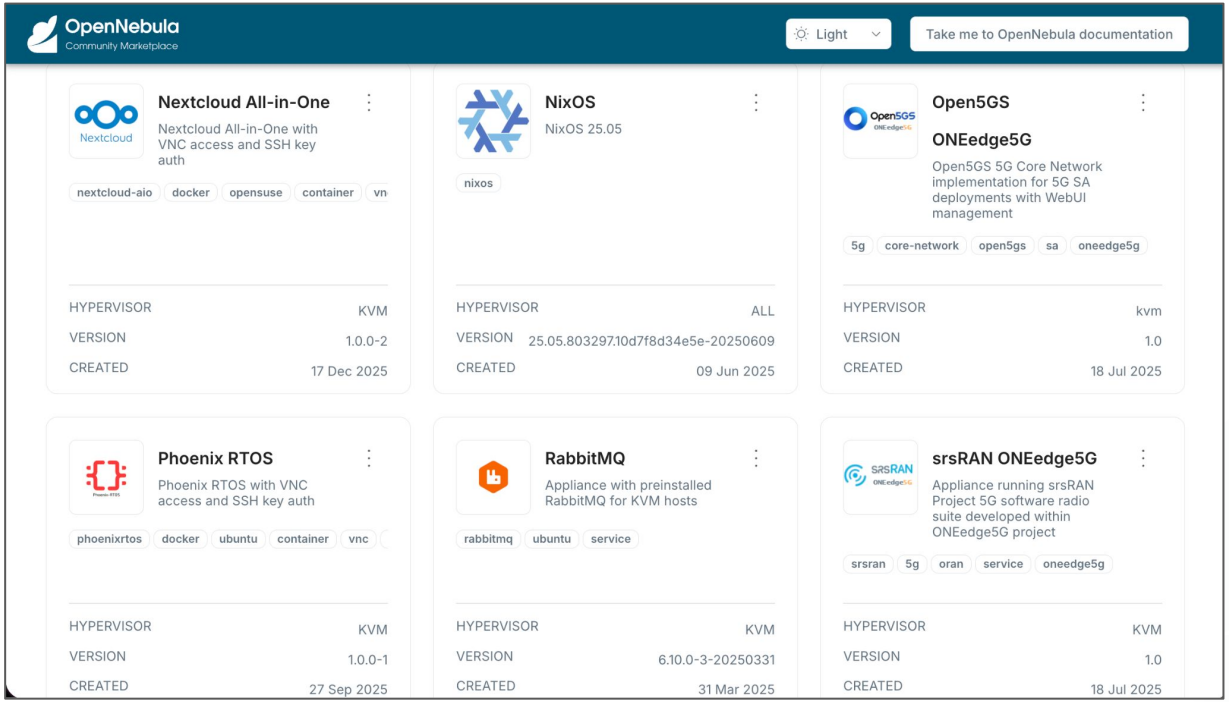
Download and run the MiniONE script with default or custom parameters.

BASH — DEPLOY-CLOUD.SH

```
$ sudo apt update && sudo apt upgrade -y
$ wget \
    'https://github.com/OpenNebula/minione/
     releases/latest/download/minione'
$ chmod +x minione
$ sudo ./minione
# Initializing OpenNebula "Phoenix" 7.0 ...
```

✓ **After ~90 seconds: Full OpenNebula cloud with Sunstone UI, Alpine VM template, and KVM hypervisor!**

Community Marketplace: x86 and ARM64



Scan Me


92%
AWS

4 Key Takeaways

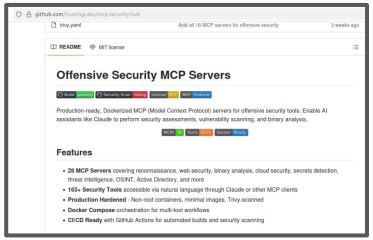
Best Practices for Sovereign Hybrid Clouds

Establish Baselines: Define hardened configurations for every VM image and host.

Automate Compliance: Replace manual audits with continuous, code-driven scanning.

RBAC Hardening: Minimum viable permissions..

[Experimental] Smart Remediation: AI + MCP Power




```
(prowler-py3.12) root@localhost:~/TFM_prowler# prowler opennebula --credentials-file one_cred
                                _
 _ __  _ __ _____      _| | ___ _ __
| '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
| |_) | | | (_) \ V  V /| |  __/ |
| .__/|_|  \___/ \_/\_/ |_|\___|_|v5.5.0
|_| the handy multi-cloud security tool

Date: 2026-01-26 13:23:23

-> Opennebula Credentials
  · user_id: 0
  · user_name: oneadmin
  · group_id: 0
  · group_name: oneadmin

-> Using the following configuration:
  · Config File: /root/TFM_prowler/prowler/config/config.yaml

Executing 10 checks, please wait...
-> Scan completed! |████████████████████████████████████| 10/10 [10

Overview Results:
```

12.5% (2) Failed	87.5% (14) Passed	0.0% (0) Muted

OpenNebula Cluster Scan Results (severity columns are for fails only):

Provider	Service	Status	Critical	High	Medium	Low	Muted
opennebula	Authentication and Access Control	FAIL (1)	0	0	1	0	0
opennebula	Host	PASS (2)	0	0	0	0	0
opennebula	Network and Secure Communications	PASS (1)	0	0	0	0	0
opennebula	Template	FAIL (1)	0	1	0	0	0
opennebula	Virtual Machine	PASS (2)	0	0	0	0	0

```
* You only see here those services that contains resources.

Detailed results are in:
 - JSON-OCSF: /root/TFM_prowler/output/prowler-output-oneadmin-20260126132323.ocsf.json
 - CSV: /root/TFM_prowler/output/prowler-output-oneadmin-20260126132323.csv
 - HTML: /root/TFM_prowler/output/prowler-output-oneadmin-20260126132323.html
```

"Visibility is the first line of defense in the cloud computing continuum."

OpenNebula @ FOSDEM 2026

OpenNebula

AI Plumbers :

OneAI: An Open-Source Framework for Managing AI Models at Scale.

Network :

Building an Open Source Private 5G Network: A Practical Blueprint.

Virtualization & Cloud Infrastructure :

How I Turned a Raspberry Pi into an Open-Source Edge Cloud with OpenNebula.

Arming Cloud Computing Continuum: Hunting vulnerabilities in open source hybrid clouds.

Find our Booth in LEVEL 1 of BUILDING K

OpenNebula

Thank You!

OpenNebula.io

ONEnextgen

> OpenNebula.io/IPCEI-CIS

IPCEI-CIS

Next-Generation European Platform for the Datacenter-Cloud-Edge Continuum

Initiative supported by the Spanish Ministry for Digital Transformation and Civil Service through the **ONEnextgen Project: Next-Generation European Platform for the Datacenter-Cloud-Edge Continuum** (UNICO IPCEI-2023-003) and co-funded by the European Union's NextGenerationEU instrument through the Recovery and Resilience Facility (RRF).

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

UNICO IPCEI