EUROPEAN WEATHER CLOUD

EWC Secrets Manager

9th EWC User Workshop (hybrid), 22th September 2026

Kamil Rajtar (EUMETSAT)

Agenda

- EWC Secrets Manager
  - Why now: the gap we are closing
  - Pilot foundation
    - Namespaces and secret engines
    - AppRole and EWC IAM
  - Automation use cases
    - Kubernetes / ESO
    - Ansible
    - GitLab and GitHub runners
    - CLI and programming languages
  - Pilot
  - Questions and feedback

Why now: the gap we are closing

Service	Current	New
Authentication	One login per application	EWC IAM – Single Sign On
Cloud management UI	MORPHEUS	openstack.
Workflows / Instance types	Morpheus Workflows/Instances	EWC Community Hub + EWCCLI
Secret Manager	Morpheus Cypher	EWC Secret Manager PILOT
Logging and Monitoring	Morpheus agent on each VM	TBD – analysing solutions

Identity is unifying — secrets must catch up

THE GAP WE ARE CLOSING

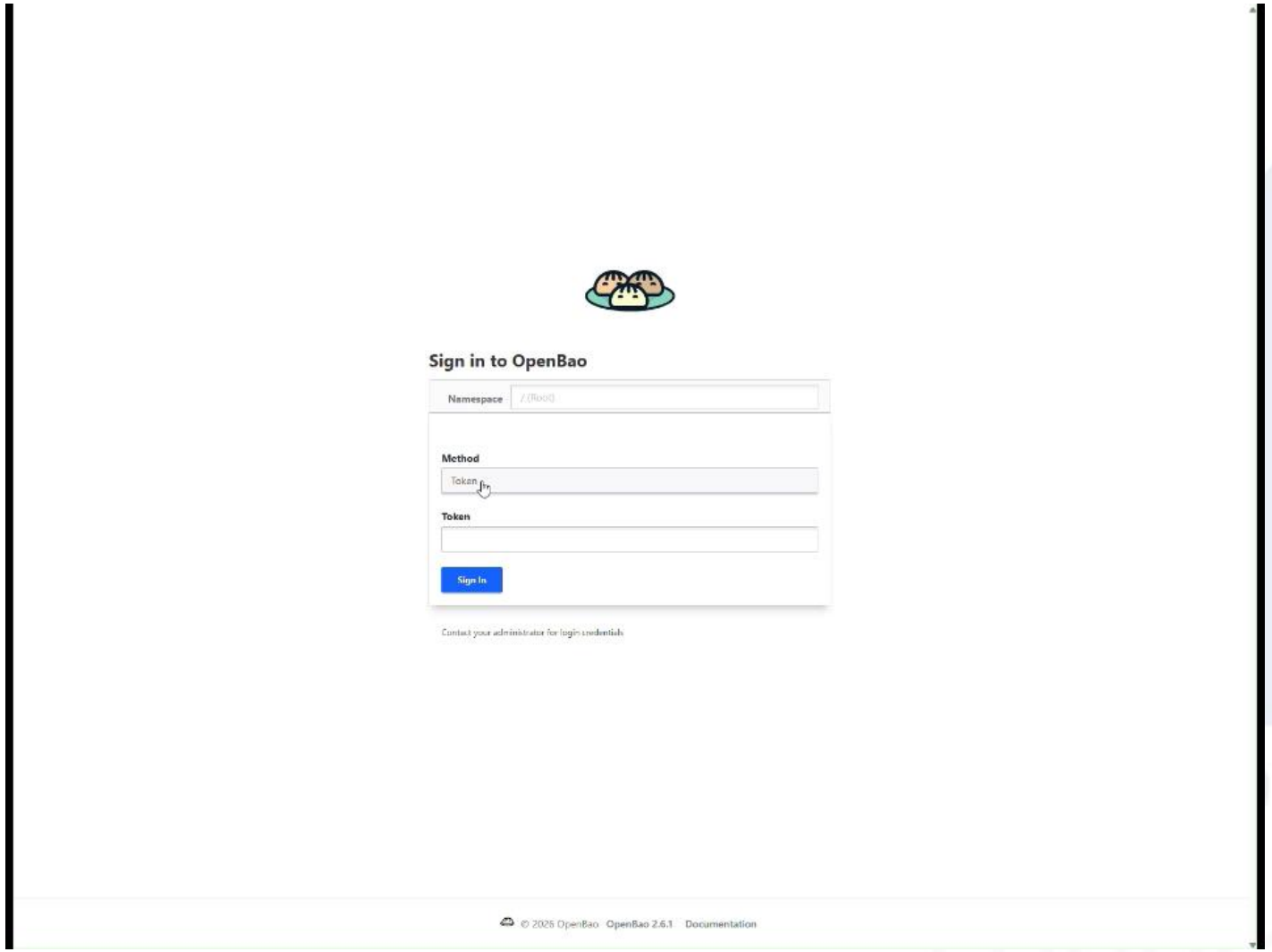
Today		With EWC Secrets Manager
Fragmented human access One login per application	›	**Unified entry point** Human sign-in through EWC IAM
Service-bound secret store Morpheus Cypher retires with Morpheus	›	**Shared cloud capability** Managed Vault as a shared cloud service
Tenant governance Isolation and delegated admin vary by service	›	**Namespace boundaries** Tenant-scoped secrets, policies and identities
Machine & workload access No common path for Kubernetes, Ansible and CI	›	**Policy-scoped automation** AppRole plus runtime delivery patterns
Morpheus-only integration No external tools; Morpheus automation only CLI limited to Morpheus VMs	›	**Tool-independent access** Works with Kubernetes, Ansible,CI/CD, CLI or programming languages

Make secrets a shared cloud service — not a feature embedded in each application.

Sources: EWC IAM onboarding & workshop deck; OpenBao Namespaces and AppRole documentation.

Demo: OpenBao in action

Authenticate → retrieve a secret → use it without exposing credentials



Built for tenants, users and machines

PILOT FOUNDATION

01

NAMESPACES

Isolated tenant environments for secrets, policies and identities.

Delegated administration stays inside the namespace.

02

SECRET ENGINES

Pilot: versioned KV v2 for arbitrary key/value secrets.

Other engines can generate credentials, certificates or encryption services when enabled.

03

APPROLE

Machine-oriented login using RoleID + SecretID.

Policies and constraints issue a scoped token with a bounded lifetime.

04

EWC IAM

Human login through EWC IAM using Keycloak/OIDC.

Tenant identity is directed to the corresponding namespace and role.

Default-deny access, then grant only the paths and operations each role needs.

Sources: OpenBao Namespaces, Secrets Engines, KV v2 and AppRole; EWC IAM service documentation.

EUROPEAN WEATHER CLOUD

Automate secret delivery — don’t embed credentials

After onboarding: authenticate → authorize by policy → fetch at runtime → use or reconcile

K	**KUBERNETES / ESO**	ExternalSecret declares the required path	›	ESO uses AppRole to read KV v2	› **Kubernetes Secret is created and reconciled**
A	**ANSIBLE**	Playbook starts without an embedded secret	›	Ansible client retrieves the secret at runtime	› **Task consumes the value; repo and inventory stay clean**
CI	**GITLAB & GITHUB RUNNERS**	A pipeline job starts	›	AppRole today; OIDC/JWT when trusted	› **Job uses the secret; pipeline configuration stays clean**
SDK	**CLI & PROGRAMMING LANGUAGES**	A CLI command or application starts	›	CLI or language client authenticates and reads	› **Application uses the secret; source code stays clean**

Configure authentication, policies and paths once — then reuse the pattern across tools.

Sources: EWC ESO/AppRole pattern; External Secrets Operator; Ansible; GitLab and GitHub security docs.

Demo: ESO secret delivery

ExternalSecret → OpenBao AppRole → reconciled Kubernetes Secret

Pilot is open!

Pilot launch, automated tenant onboarding, then go-live

01

PILOT START

NOW

Contact us to be the first one to try it.

02

AUTOMATED ONBOARDING

PER TENANCY

Provision namespace, access and policies automatically for each tenancy.

03

GO-LIVE

Q1 2027

Target go-live for the service.

ENABLEMENT • NOVEMBER

User webinar

Hands-on sessions will help users prepare, configure access and integrate their tools.

Questions & Feedback

We’d love to hear your thoughts and questions.

Feedback on the Secrets Manager

THANKS!