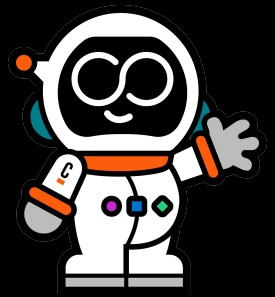
CAMUNDA

Supercharge your Camunda 8 Self-Managed instance with managed AWS services

CamundaCon Amsterdam 2025

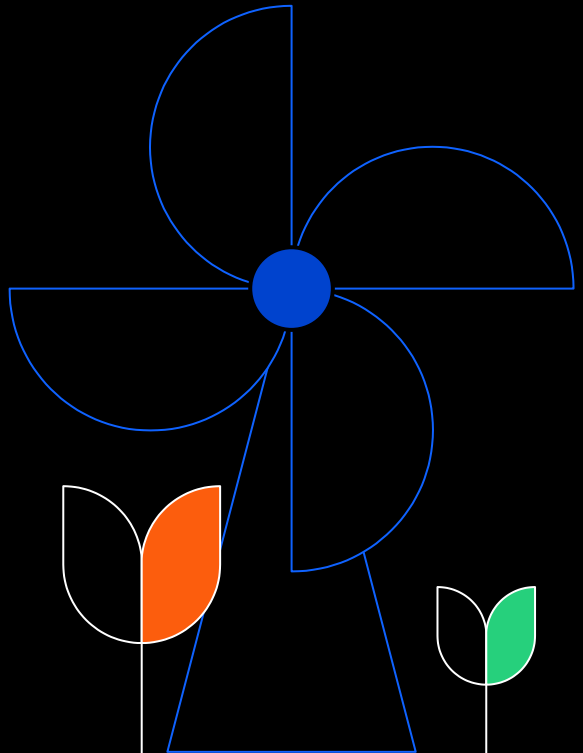
Technical Use Cases

That’s me



Norman Lüring
Senior Consultant
@Camunda

Goals



- Understand the value of managed services
- Introduce common managed services utilized for a Camunda 8 architecture on AWS
- Highlight recommendations from the *field*
- Show-case an IaC deployment
- Have fun presenting, Norman

Managed Services

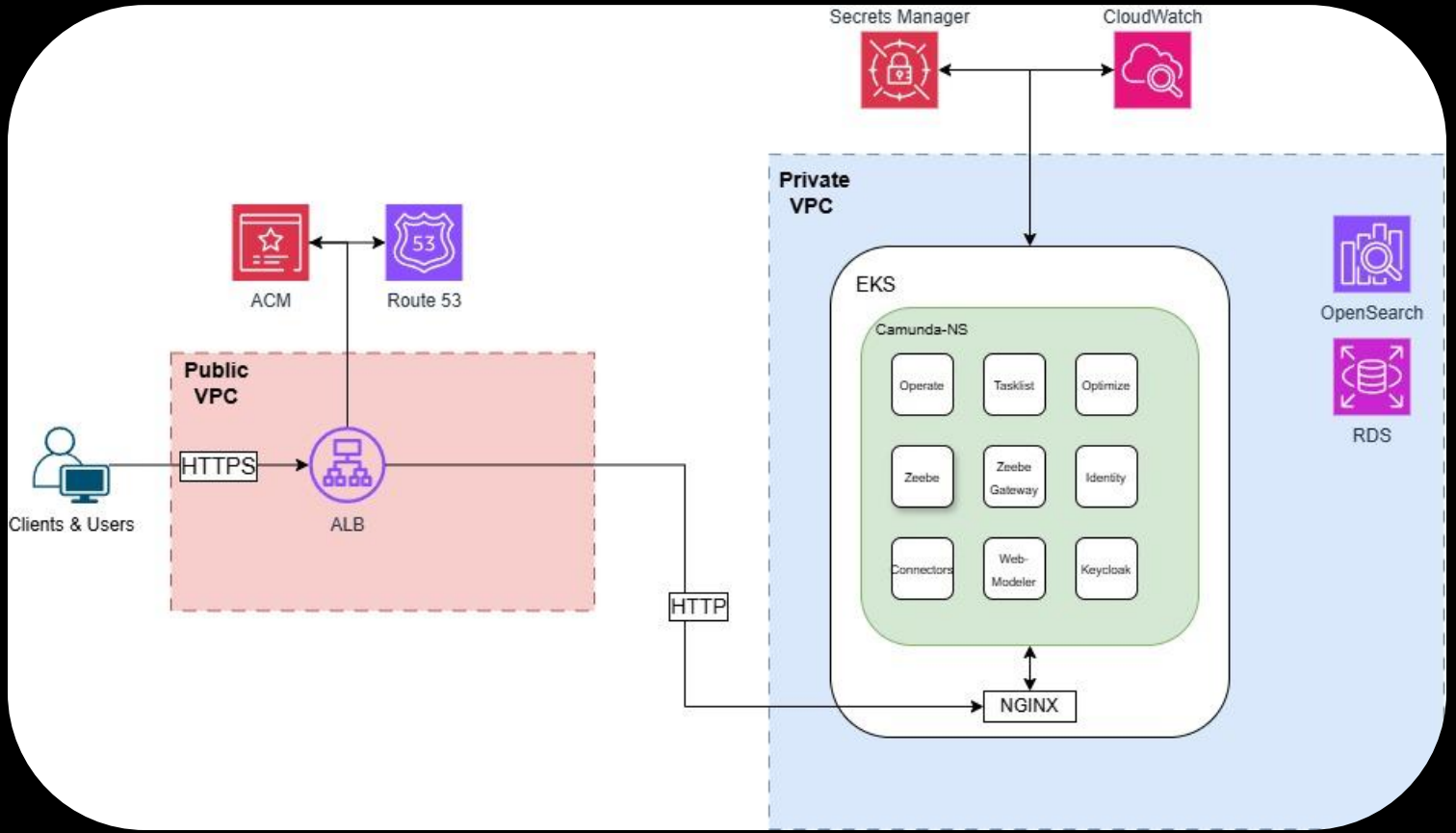
AMS (AWS Managed Services) provides full-lifecycle services to provision, run, and support your infrastructure, and automates common activities such as change requests, monitoring, patch management, security, and backup services.

Key Characteristics

- Less Ops (patching, *scaling*, *backups*)
- Higher reliability by built-in HA and SLAs
- Security best-practices and automation
- Often alignment with enterprise strategy
- Budgetable pricing

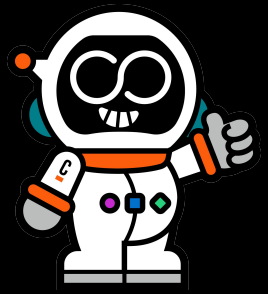

BUT MANAGED SERVICES
ARE EXPENSIVE

Sample Architecture Diagram



AMS Recommendations

AWS EKS



- Heart of the Camunda deployment ❤️
- Utilizes EC2 Nodes/Nodegroups with multi-zone capabilities
- Integratable with several AWS services like CloudWatch
- Extensible by addons with agents, controllers and CRDs:
  - EBS-CSI-Driver, ALB-Controller, CloudWatch-Agent, [...]
- From the field:
  - **Enable RBAC for K8s!**
  - **Follow node & storage recommendations from our docs**

AWS VPC

- Provides isolated networking for EKS
- Design public/private subnets to isolate services
- Uses VPC endpoints to keep traffic to RDS/OS/S3 off the internet
- Enforce least-privilege with Security Group per namespace
- From the field:
  - **Make sure Security Groups restrict access to ALB**
  - **Private Networks to rule them all**
  - **Peering > Transit Gateways in Dual-Region setups**

AWS IAM

- Manages users, groups and roles for humans and service accounts
- Integrates SSO & MFA for corporate identity providers
- IAM Access Analyzer to detect overly broad policies
- From the field:
  - **Enforce IRSA for every pod-to-AMS interaction**
  - **Apply least-privilege permissions**
  - **Disable node-level credentials**
  - **Apply environment based permission boundaries**

AWS OpenSearch

- Backend for Camunda history data
- Deployed in private subnets with encryption in transit & at rest
- Leverages ISM (Index State Management) for easy retention
- Multi-zone by nature
- (Limitation) Camunda 8 Optimize <= 8.8
- From the field:
  - **Enforce IRSA exclusively for OpenSearch and limit access**
  - **Use sidecar containers for dashboard/API connectivity**
  - **Sizing depends on load**

AWS RDS

- Utilized by Web-Modeler and Camunda Identity Components
- Multi-Zone and automated backups by nature
- From the field:
  - **Reuse RDS instance for Camunda applications**
  - **Solely IRSA principals are not possible**
  - **Master username/password is only used at creation/rotation time and can be managed by AWS ASM**

AWS Route53

- Highly scalable and available Domain Name System
- Manages public & private hosted zones per environment
- In theory: Failover routing for dual-region deployments
- Creates alias records to point to ALBs
- From the field:
  - **Automate change propagation via IaC**

AWS ACM

- Certificates are not easy and a common struggle in deploying C8
- Certificate rotations are automatically managed by AWS⭐
- No-cost certificates for integrated services
- From the field:
  - **Use certificate managers like ACM, cert-manager [...]**
  - **mTLS requires RISK-assessment**

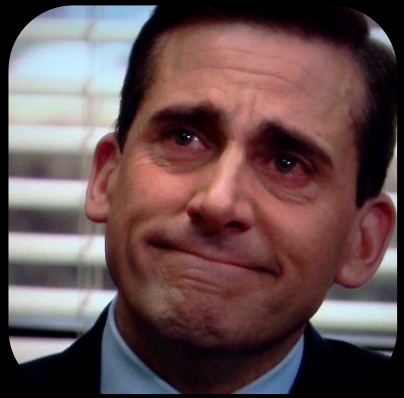
AWS Secrets Manager

- Centralized and secure store for credentials and sensitive information
- Built-in rotation for AWS services
- Synchronization to AWS EKS via Secrets Operator or CSI Driver
- OOTB secret access auditing on CloudTrail and possible alert mechanism
- From the field:
  - **Keep per environment secret namespacing and rotate during maintenance windows**
  - **Sidecars will mount rotated secrets without downtime**

AWS CloudWatch

- One-stop hub for metrics, logs and alerts
- Good log aggregation for many services OOTB
- CloudWatch Agent for EKS ease installation
- From the field:
  - **No replacement for Camunda Grafana**
  - **Configure retention policies for logs**
  - **Complex pricing model based on API queries/storage[...]**

And furthermore



- S3 for Backups and Configuration management
- Camunda process integration with Connectors (SQS,SNS, Lambda Bedrock, [...])
- Camunda SaaS available on AWS

Example Project

https://tinyurl.com/awsccon

Thank you!

Connect with me:

Norman Lüring
https://www.linkedin.com/in/norman-luering/