BUOYANT
SERVICE MESH
ACADEMY

# Running Linkerd on Amazon EKS

# Access the Code

Scan to try it & view the code

SERVICEMESH ACADEMY

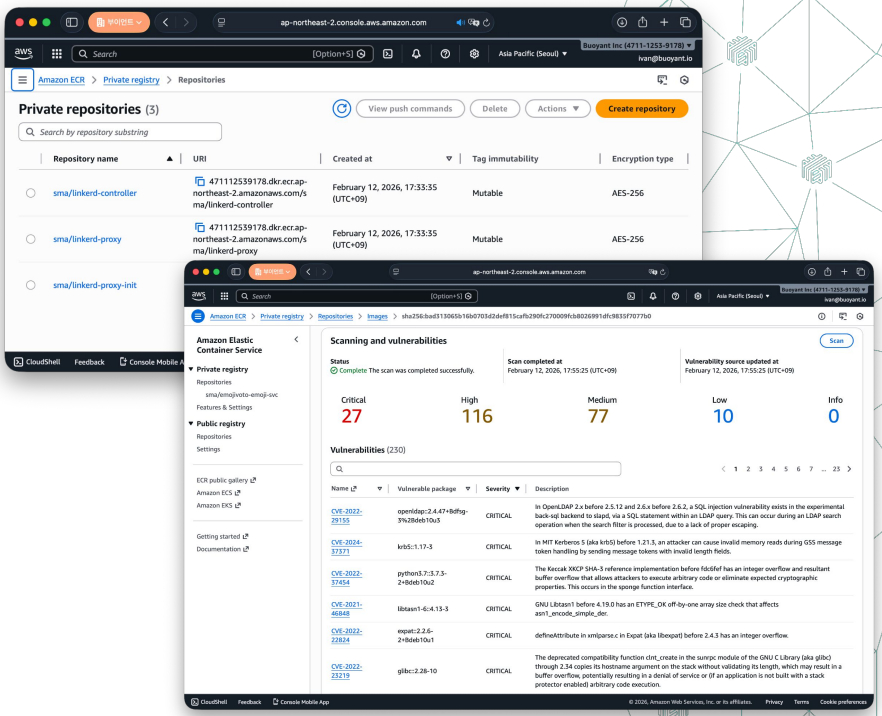
# AWS Services

| | |
|---|---|
| AWS Elastic Container Registry | Fully managed Docker container registry that makes it easy to store, share, and deploy container images. |
| Amazon EKS | Managed service and certified Kubernetes conformant to run Kubernetes on AWS and on-premises. |
| AWS Cloud Watch | Service used to collect and visualize metrics and logs, and to trigger notifications or actions when a metric crosses a threshold. |
| AWS Managed Grafana | Fully managed Grafana service on AWS that lets you build dashboards and explore/visualize metrics, logs, and traces from many sources |
| Amazon Prometheus | AWS's fully managed, serverless Prometheus-compatible service for collecting, storing, querying and alerting on metrics |
| AWS Private Certificate Authority | Managed service for creating and operating your own private certificate authorities (root and subordinate CAs) and issuing private X.509 certificates |

SERVICEMESH ACADEMY

# AWS Elastic Container Registry

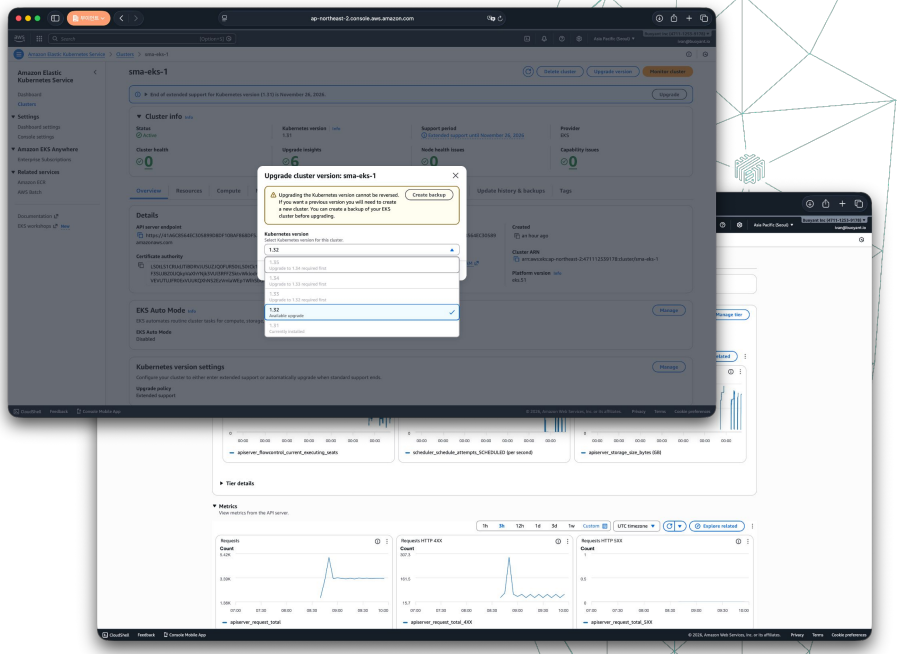
- **Securely store and version** container images in private or public repositories.
- **Control access with IAM** (and repository policies), and enforce tag immutability to prevent accidental overwrites.
- **Automatically scan images for vulnerabilities** (Basic scanning by default; enable Enhanced scanning for continuous findings).
- **Sign and verify images** (e.g., with ECR signing) to support supply-chain integrity.
- **Replicate images across regions/accounts** to improve availability and reduce cross-region pull latency.




SERVICEMESH ACADEMY

# Amazon EKS

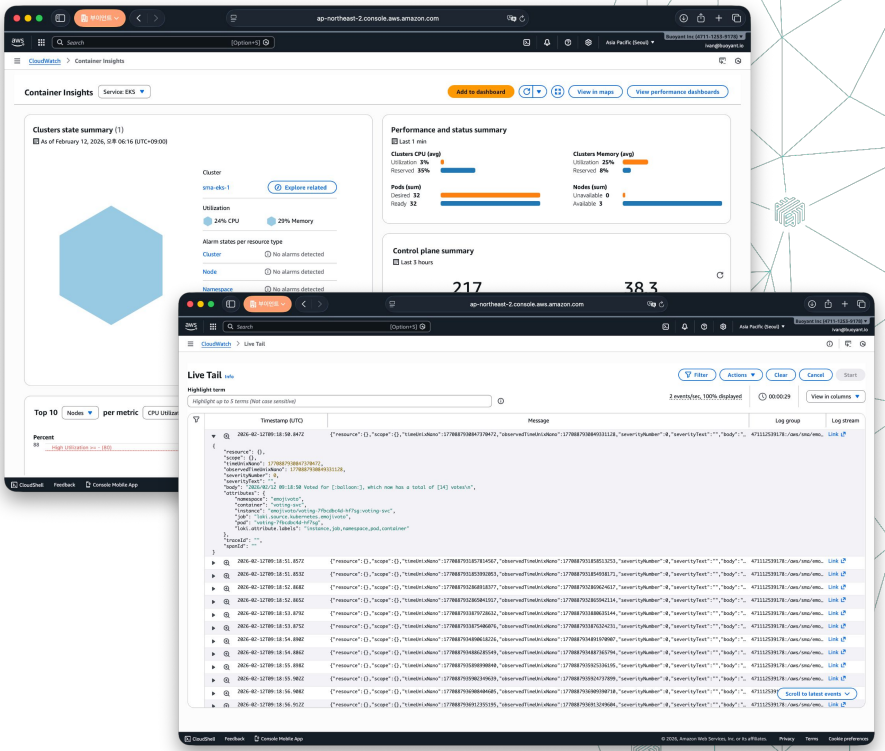
- **Run Kubernetes without managing the control plane** (AWS handles availability, upgrades, and patching).
- **Choose compute that fits your workload**: Managed Node Groups (EC2), Fargate (serverless pods), or self-managed nodes.
- **Scale safely and predictably** with Cluster Autoscaler / Karpenter and managed add-ons for core components.
- **Secure clusters with IAM + RBAC,** private endpoints, and network policies (via supported CNI options).
- **Integrate observability with CloudWatch /Prometheus**-compatible metrics, logs, and tracing.
- **Simplify lifecycle operations** with versioned upgrades, add-on management, and blue/green-style rollout patterns.




SERVICEMESH ACADEMY

# AWS Cloud Watch

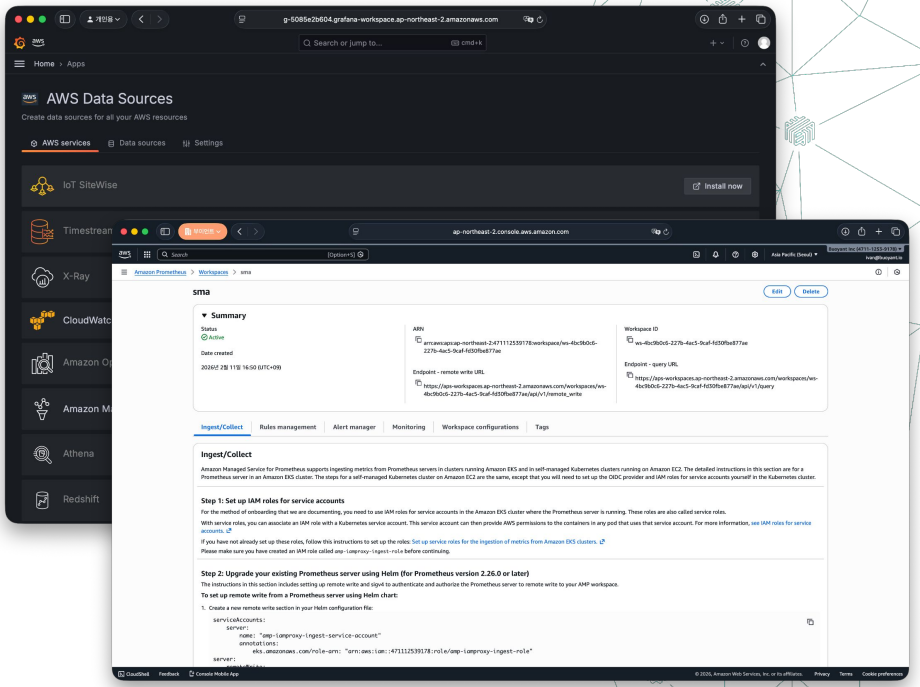
- **Collect metrics, logs, and traces** from AWS services, containers (EKS), and applications.
- **Centralize and explore logs** with Log Groups, Insights queries, and live tail for fast troubleshooting.
- **Create dashboards** to visualize service health and key SLO/SLA indicators.
- **Set alarms on metrics and log patterns** to notify or trigger automated actions when thresholds are breached.
- **Detect unusual behavior** with anomaly detection for metrics and logs (where enabled).
- **Integrate with incident workflows** (SNS/PagerDuty/Chat tools) and downstream analytics/export as needed.




SERVICEMESH ACADEMY

# AWS Managed Grafana & Prometheus

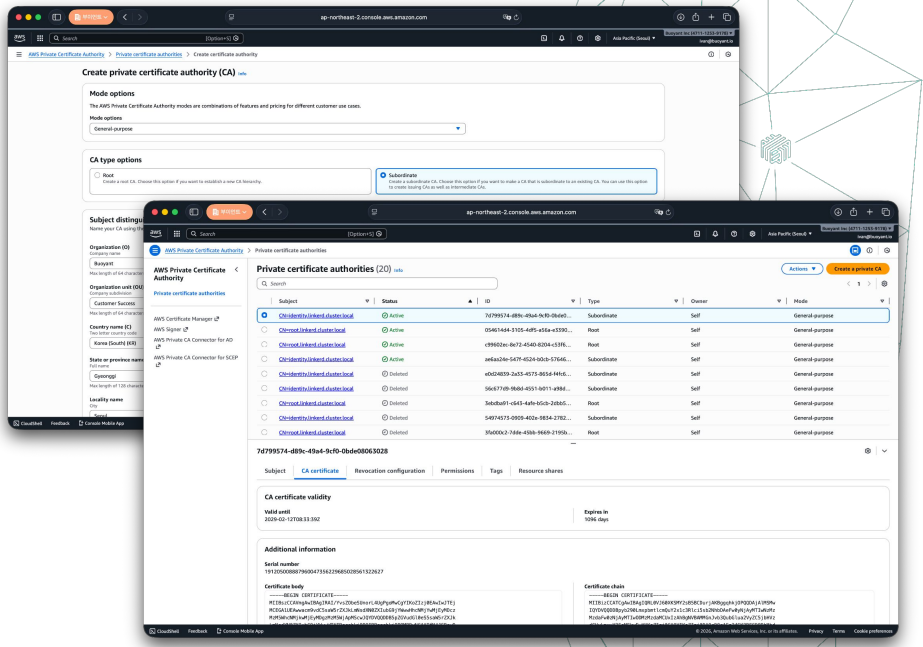
- **Use Prometheus for metrics + Grafana for dashboards,** without operating the underlying infrastructure.
- **Amazon Managed Service for Prometheus (AMP)** ingests, stores, and queries Prometheus metrics **at scale** (multi-AZ, managed upgrades/operations).
- **Amazon Managed Grafana (AMG)** provides **hosted Grafana workspaces** with built-in AWS data source integrations.
- **Secure access with IAM Identity Center (SSO) or SAML**, plus fine-grained permissions for teams.




SERVICEMESH ACADEMY

# AWS Private Certificate Authority

- **Create and operate private CAs** to issue TLS certificates for internal services, workloads, and devices.
- **Build a CA hierarchy** (root + subordinate CAs) to separate high-trust roots from day-to-day issuance.
- **Control who can manage vs. issue certificates** using IAM policies and scoped permissions.
- **Protect CA private keys in AWS-managed HSMs**, reducing key exposure and operational risk.
- **Audit CA activity** (issuance, revocation, configuration changes) for compliance and incident review.
- **Integrates with AWS services** and automation to request, rotate, and revoke certs at scale.



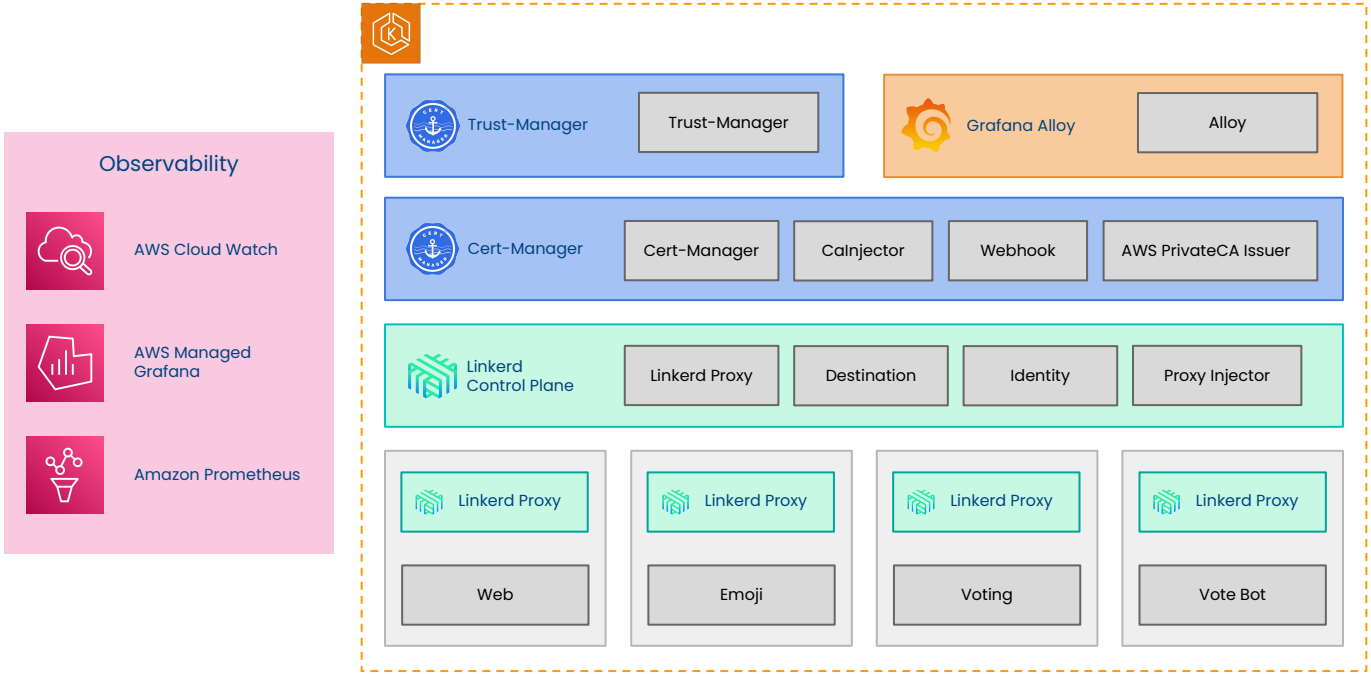

SERVICEMESH ACADEMY

# Tools

| | |
|---|---|
| Cert-Manager | Extensible X.509 certificate controller for Kubernetes and OpenShift workloads. |
| Trust-Manager | Controller that orchestrates bundles of trusted X.509 certificates in Kubernetes and OpenShift clusters. |
| Grafana Alloy | Open source OpenTelemetry collector with built-in Prometheus pipelines and support for metrics, logs, traces, and profiles. |
| Buoyant Enterprise for Linkerd | Hardened distribution of Linkerd designed to meet the demands of the modern enterprise. |

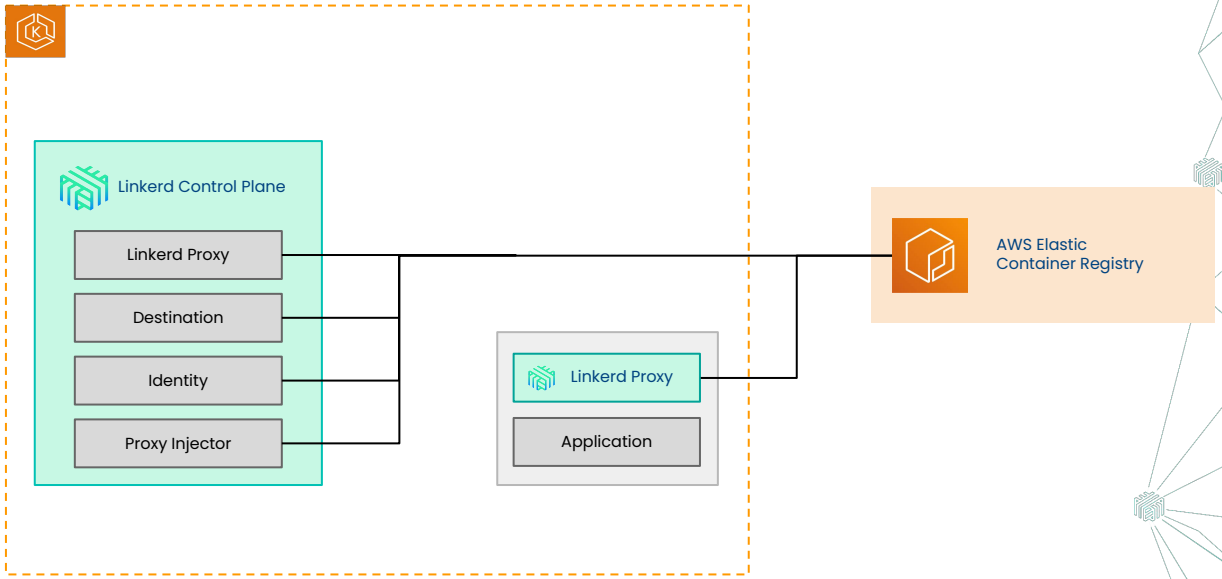
SERVICEMESH ACADEMY

# Architecture



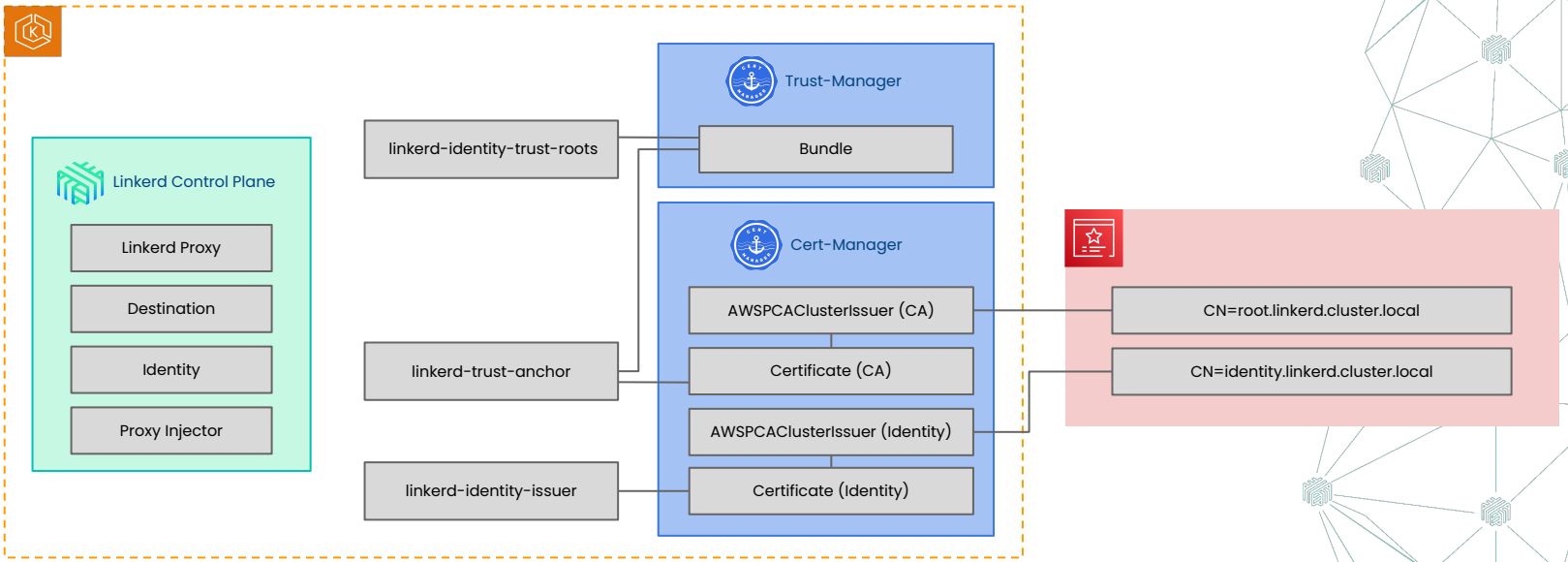

SERVICEMESH ACADEMY

# Image Mirroring



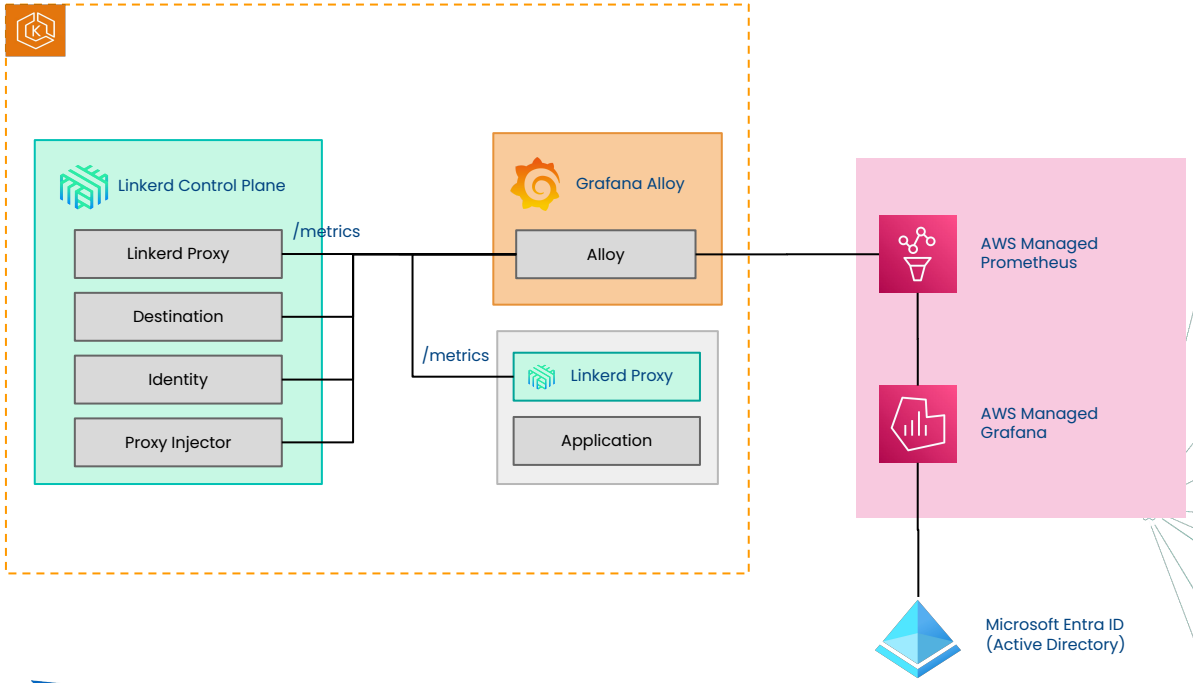

SERVICEMESH
ACADEMY

# Certificates



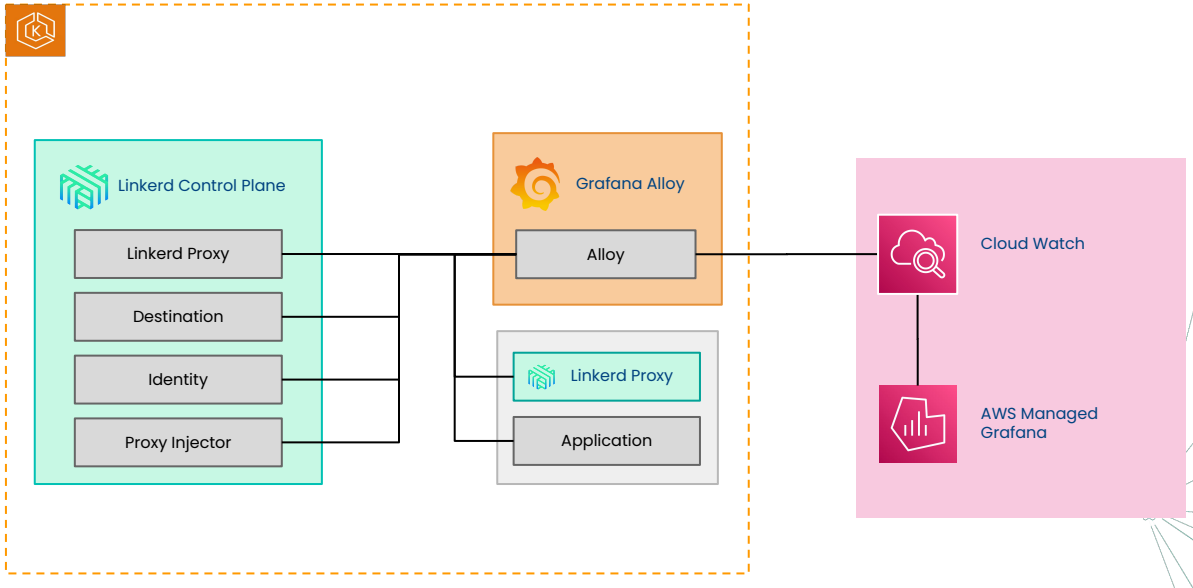

SERVICEMESH ACADEMY

# Metrics



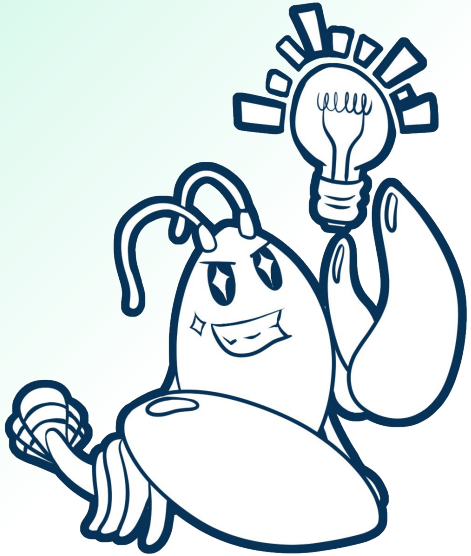

SERVICEMESH ACADEMY

# Logs




SERVICEMESH ACADEMY

# Q&A



SERVICEMESH ACADEMY