DevOpsCon

AWS EKS Anywhere: Multi-cluster communication with Cilium

Max Körbächer | Co-Founder @ Liquid Reply

Introduction

Max Körbächer

Co-Founder & Associate Partner, focusing on:

- Platform Engineering
- Application Delivery
- Cloud Native Advisory

Kubernetes Release Team from v1.17-1.24

Container & Kubernetes

Both together has changed and influenced the ICT world massively

A big bang for a total new market

Boosting open source and a community driven development to new levels

Changed the way we see infrastructure -> Infra as Apps

Security, observability, any kind of extension is seen as a simple plug & play

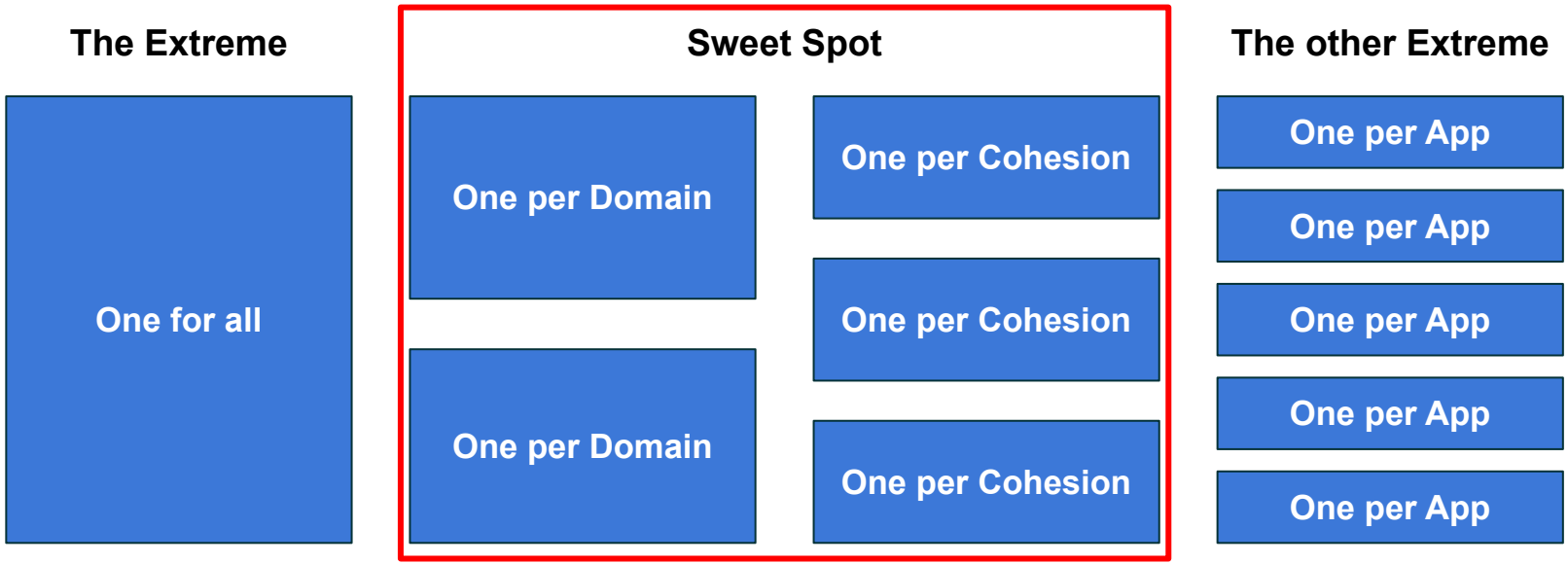
K8s abstracts away hypervisors, CSP and IaaS

K8s create a knowledge voidness

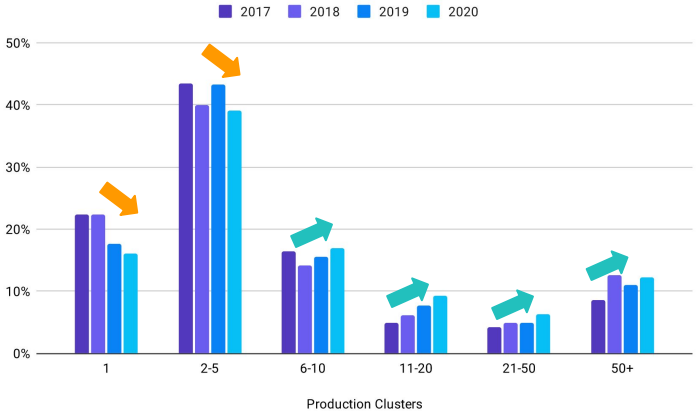
before we go deeper into the topic

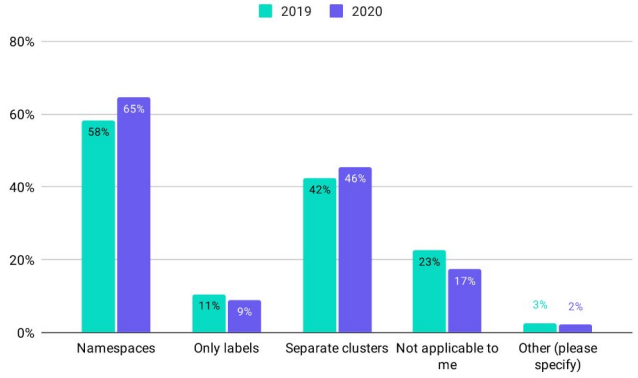
we should understand why it is so relevant

Kubernetes Clusters comes with many shapes and sizes



Adopting clusters in prod ...





Source: CNCF Survey 2020

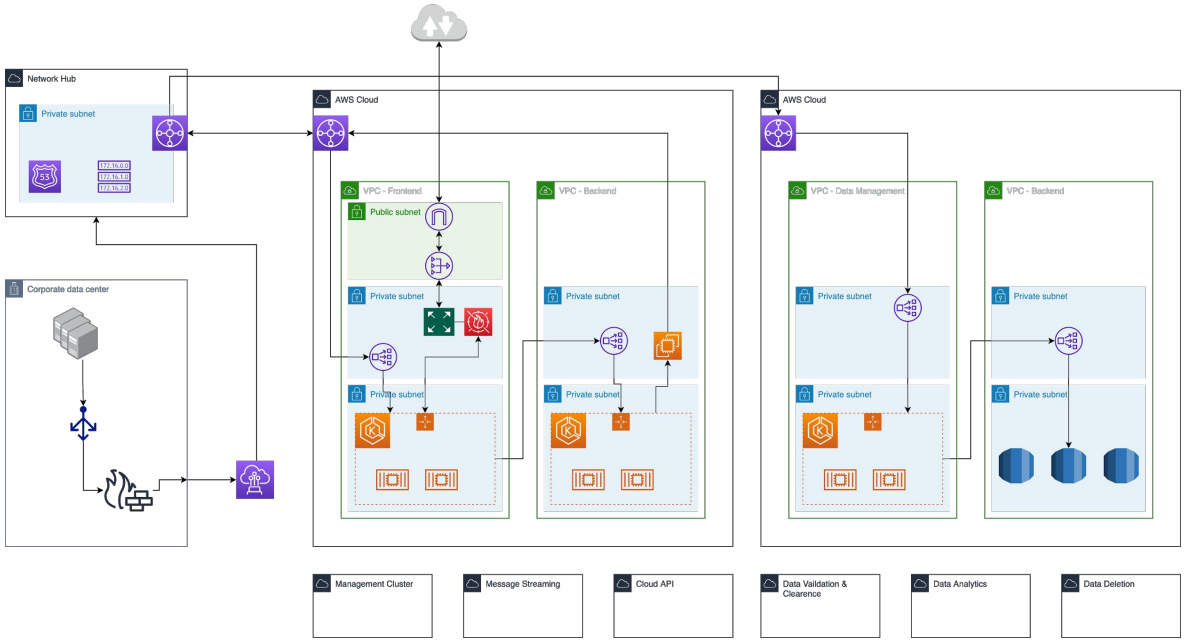
The adoption of K8s clusters in productive scenarios are growing, at the same time the average amount of clusters in production grows too.

Furthermore, multiple teams working together think more about isolation ether through namespaces or cluster separation.

But they struggle with topics like: complexity, security, cultural change, monitoring, networking, logging, lack of training and many more…

This is where our, and as it looks like, the journey of many others starts.

In many scenarios we see the same sprawl



1. Unnecessary amount of clusters
    - communication between system components goes “out of the cluster”
    - can’t call a service by it’s service name
2. Each service has unique restrictions
3. Certificate management and network encryption without fun
4. Changes on the system often requires changes in the infrastructure
5. To many failure/break points - impossible debugging

It is a stable cloud architecture, but it is not a cloud native architecture.

What is Cilium?

The swiss army knife

- Open Source Project
- Provides:
  - Networking
  - Security
  - Observability
- Linux kernel technology on eBPF
- Allows dynamic insertion of control logic into the kernel

What you can do with Cilium?

Networking

Native support for service type Load Balancer and Egress

Scalable Kubernetes CNI

Multi-cluster Connectivity

Observability

Identity-aware Visibility

Advanced Self Service Observability

Network Metrics + Policy Troubleshooting

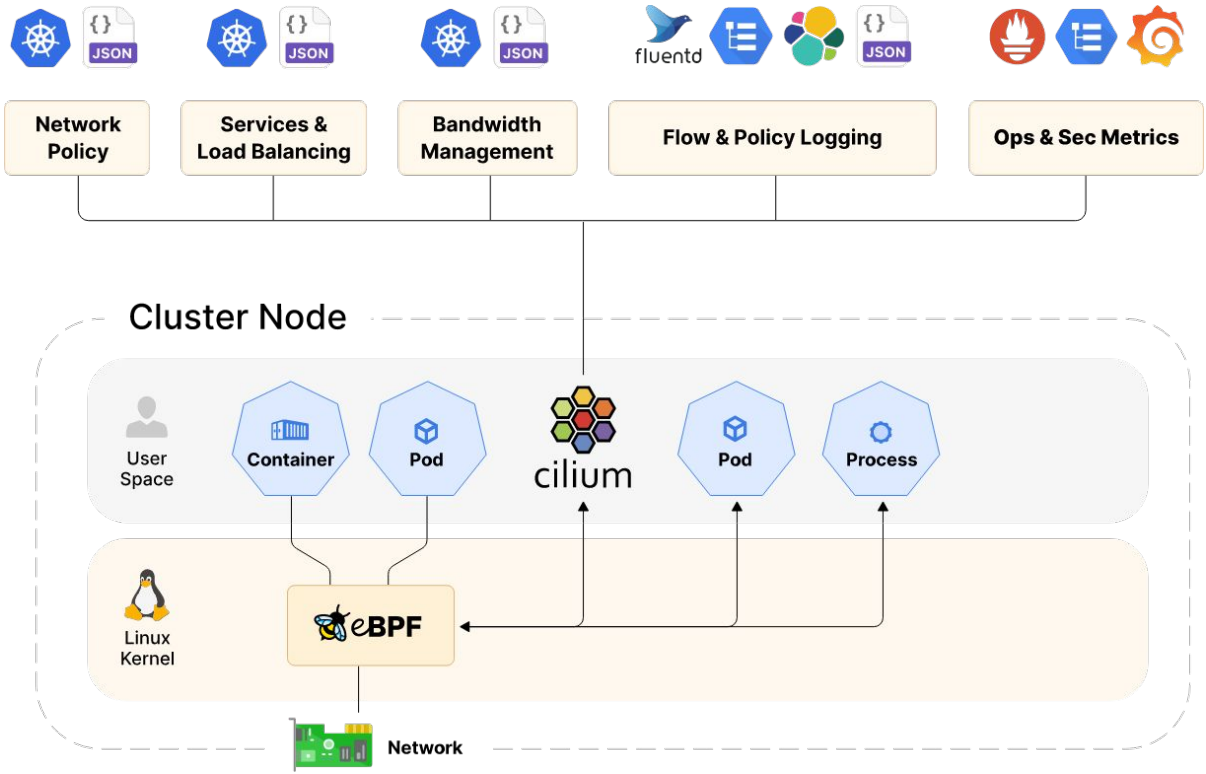
Security

Transparent Encryption

Security Forensics + Audit

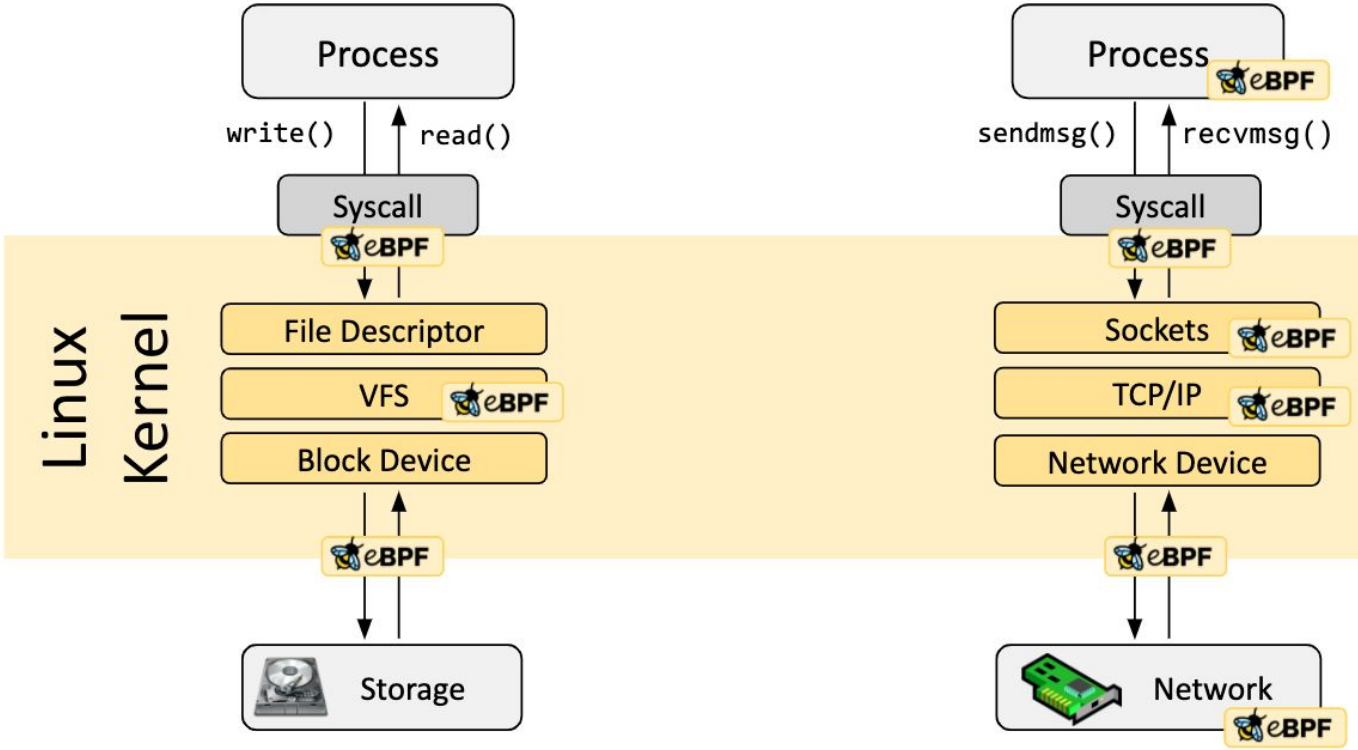
Advanced Network Policy

Ciliums Architecture



- Kernel needs to support eBPF
- Agent runs on every node
- Takes over networking, security & observability
- Workloads can be container or native running on the system

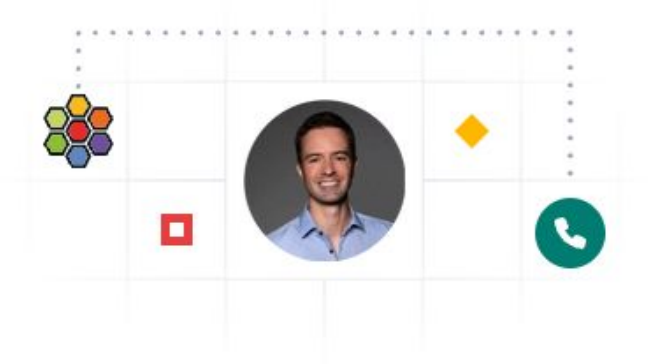
Max, WTF eBPF?



source: https://ebpf.io/

There is so much to learn about

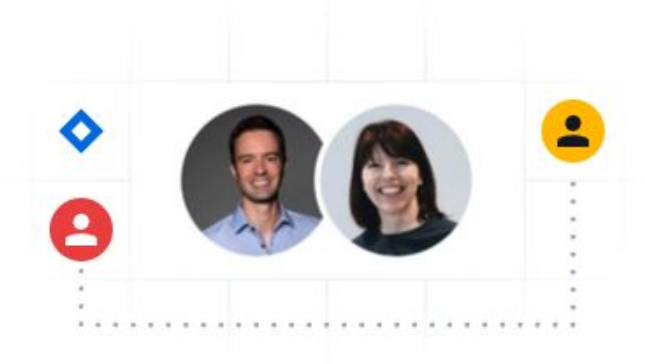
please visit cilium.io and ebpf.io



Weekly Interactive Cilium Introduction and Live Q&A

With Thomas Graf, Cilium Co-Creator

Book your seat



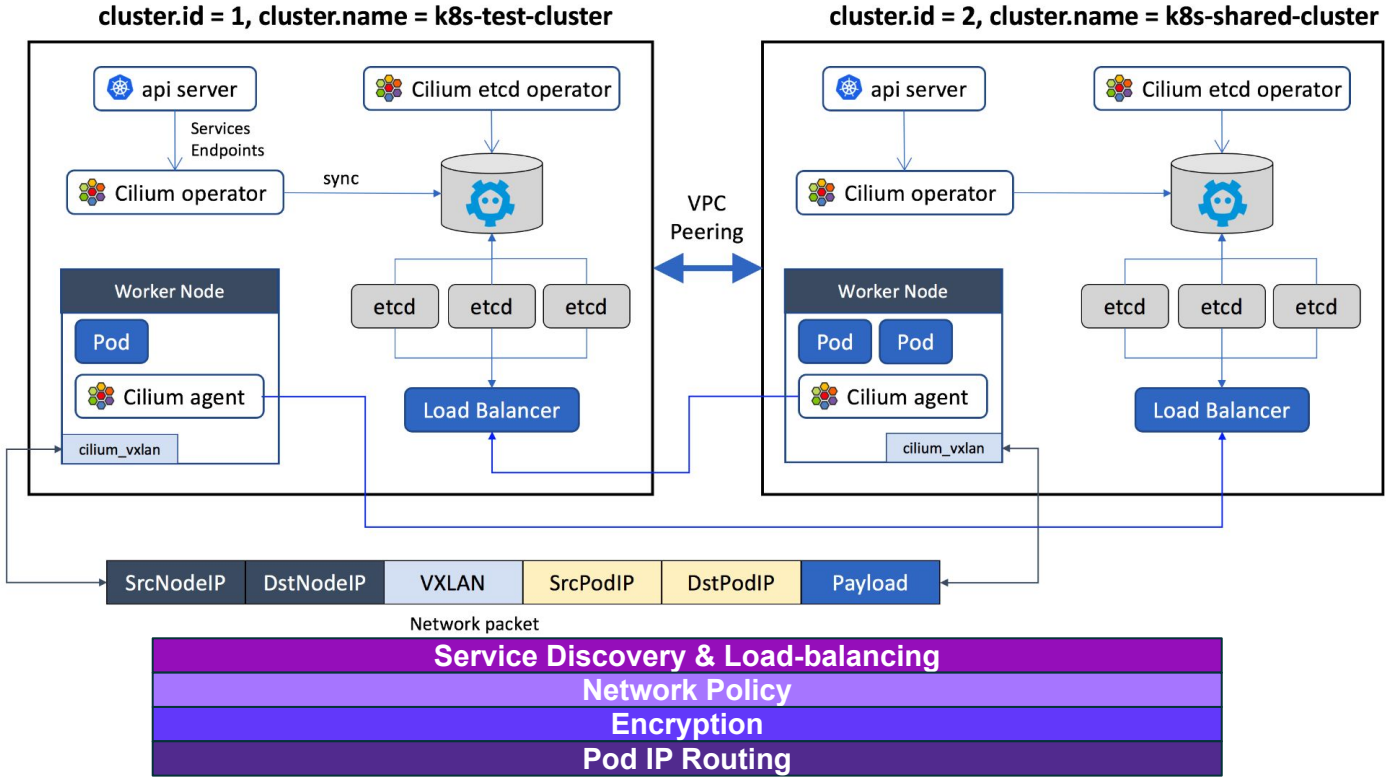
Monthly Community InstallFest

Join us at our monthly InstallFest and learn how to setup and get started with Cilium.

Join Europe

Join Americas

Clustermesh makes the cloud native magic happen



AWS EKS Anywhere

The 50 shades of K8s on AWS

Amazon EKS

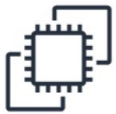
Create Kubernetes clusters (powered by Amazon EKS Distro)

Amazon EKS Anywhere

Manage EKS Distro Kubernetes clusters

Amazon EKS Distro

Download and build Kubernetes clusters with your own tooling



Amazon EC2

Deploy worker nodes for your EKS cluster

AWS Fargate

Deploy serverless containers

Self-managed resources

Your own on-premises infrastructure

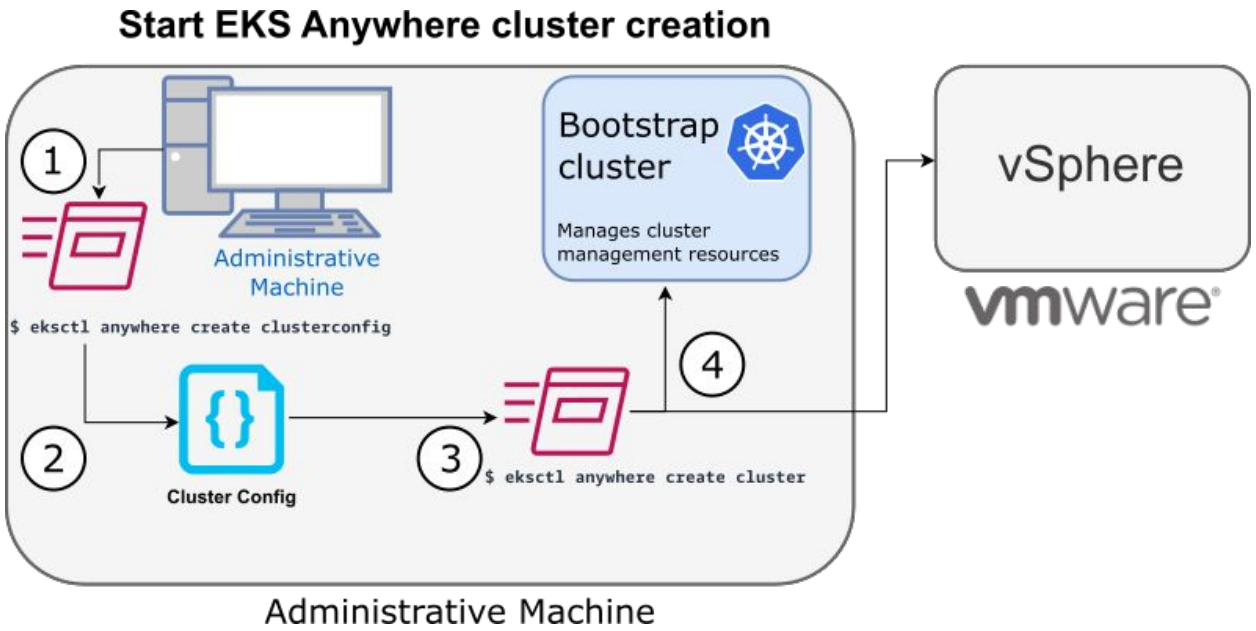
Self-managed resources

Bare metal, virtual machines, or Amazon EC2 instances

Direct Comparison of Features

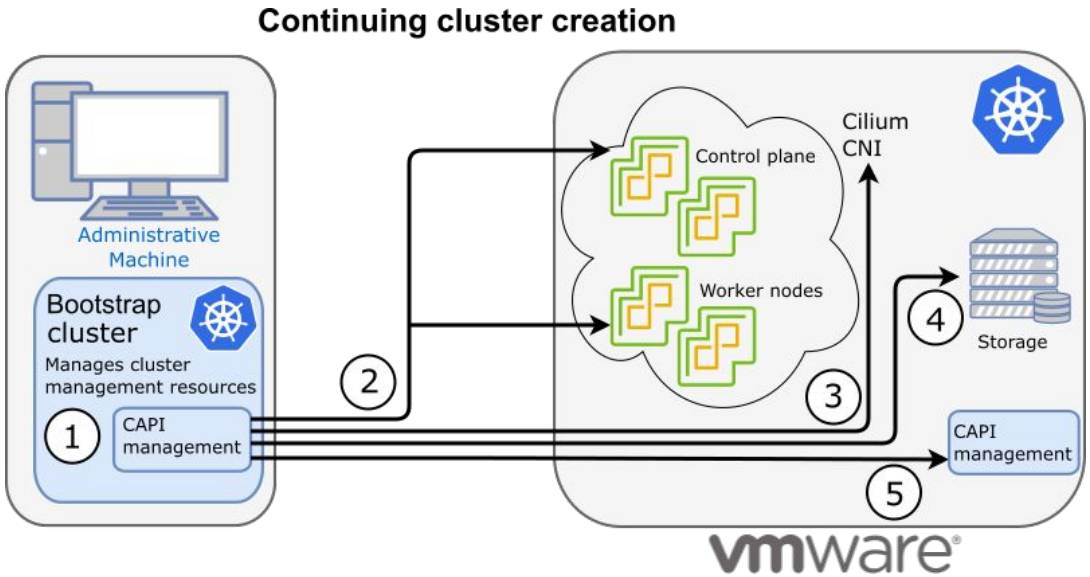
Feature	Amazon EKS	EKS on Outposts	EKS Anywhere	EKS Distro
Hardware	Managed by AWS		Managed by customer	
Deployment types	Amazon EC2, AWS Fargate (Serverless)	EC2 on Outposts	Customer Infrastructure	
Control plane management	Managed by AWS		Managed by customer	
Control plane location	AWS cloud		Customer's on-premises or data center	
Cluster updates	Managed in-place update process for control plane and data plane		CLI (Flux supported rolling update for data plane, manual update for control plane)	
Networking and Security	Amazon VPC Container Network Interface (CNI), Other compatible 3rd party CNI plugins		Cilium CNI	3rd party CNI plugins
Console support	Amazon EKS console		EKS console using EKS Connector	Self-service
Support	AWS Support		EKS Anywhere support subscription	Self-service

Bootstrapping Part 1



1. Create a config file
2. Modify the file for your needs
3. Start cluster creation
4. Authenticate and create bootstrap cluster

Bootstrapping Part 2

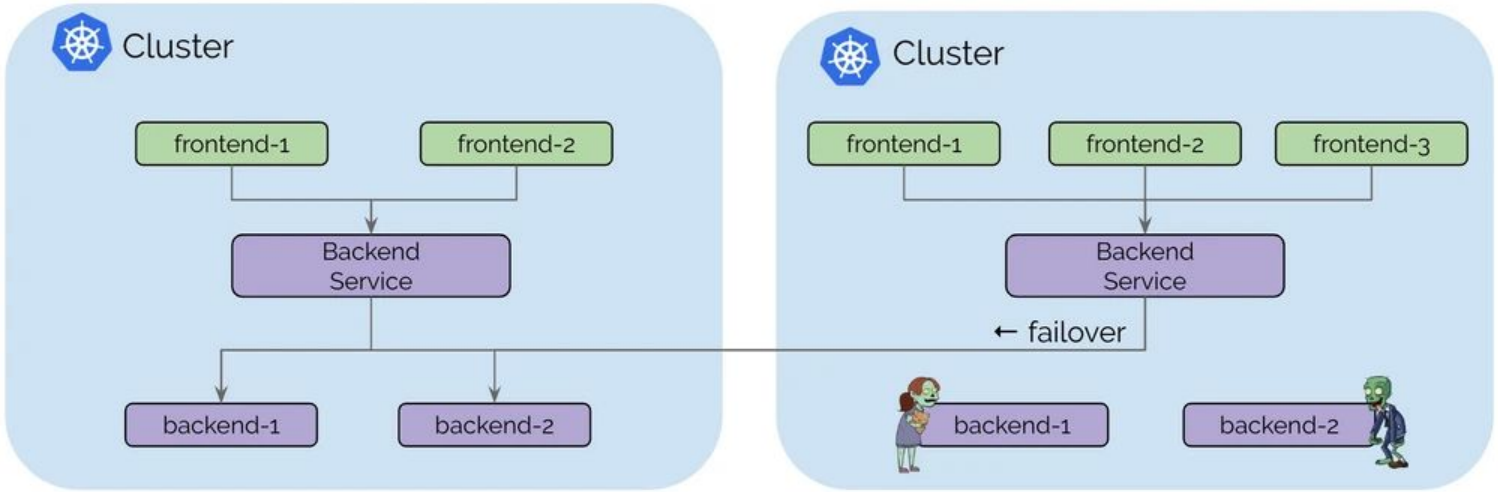


1. CAPI management started on bootstrap cluster
2. Setup the cluster on vSphere
3. Add Cilium CNI
4. Configure Storage
5. Add CAPi management to workload cluster
6. Delete the bootstrap cluster

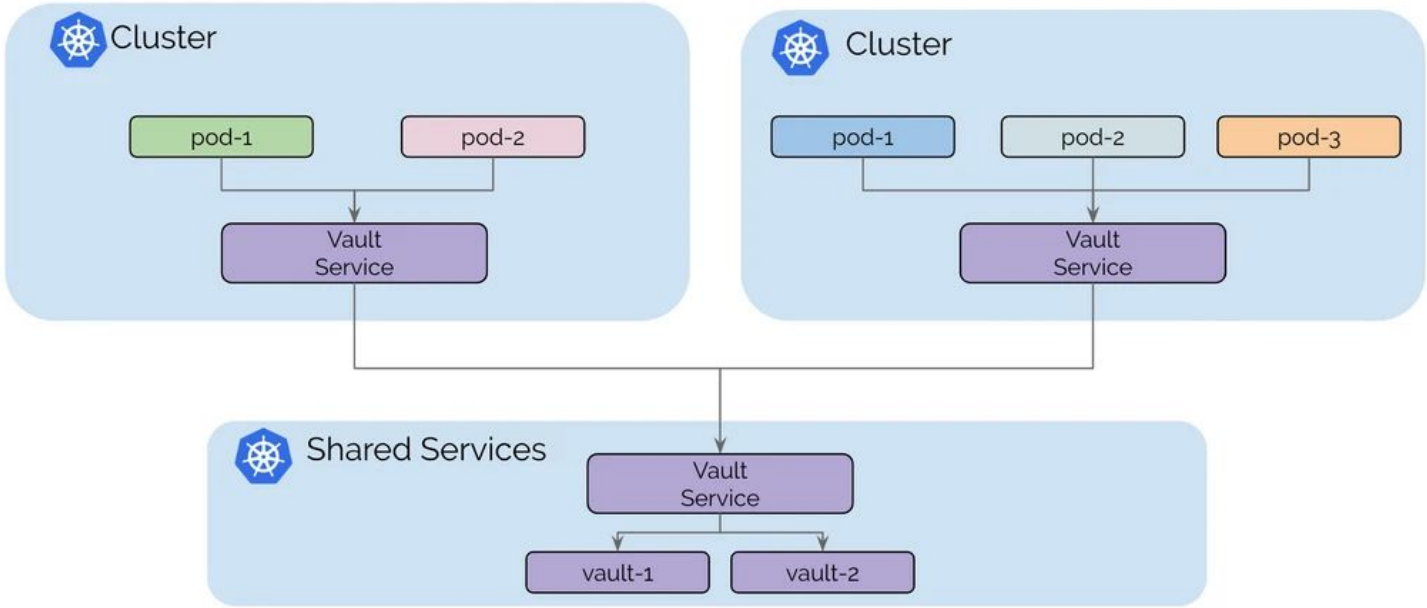
Look Into the Setup

Cluster Mesh Use Cases

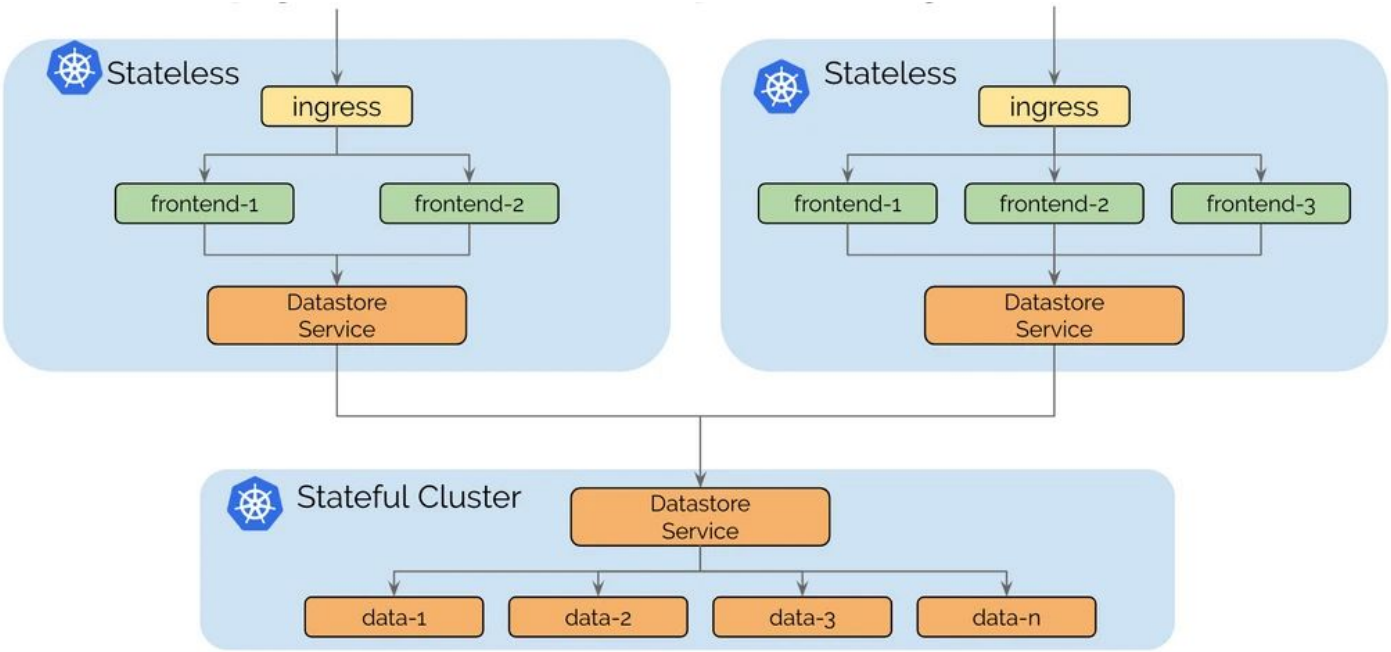
High Availability & Hybrid



Shared Services



Stateful & Stateless



Conclusion

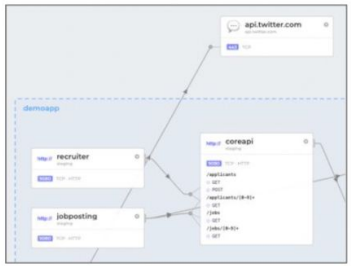
With AWS EKS Anywhere & Cilium you can implement hybrid with ease

- Networking as you need: tunneling, direct-routing or both
- Service Discovery via ”io.cilium/global-service: "true"”
- Transparent Encryption via IPsec - SPIFFE compatible
- Multicluster Network Policy
- Cross-Over paths! Having one service talking explicitly with another

Deep Insights

Application & Platform Teams

Identity & API-Aware Service Map



Identity & API-Aware Metrics & Monitoring

Identity & API-Aware Tracing

okta · Active Directory · AWS IAM

Tenant Self-Service via SSO + Role-based Access Control

Hubble Timescape (events in S3-compat object store)

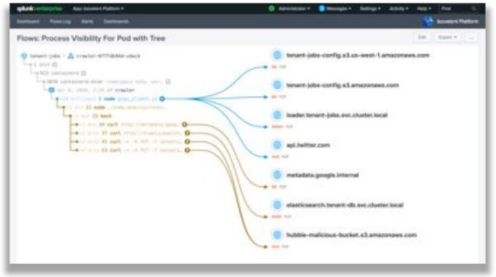
Logging Platforms

splunk> · elasticsearch

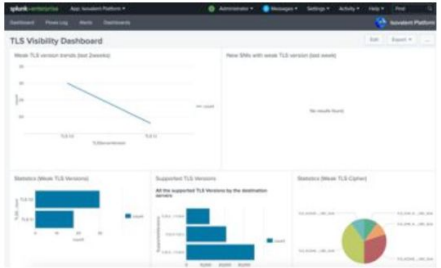
Brought Security

Security Team

Efficient Network & Runtime Visibility



Real-time Compliance & Threat Monitoring



Runtime Syscall Enforcement

✔ open("/tmp/xyz", ...)

✘ open("/etc/passwd", ...)

Efficient In-Kernel Transparent Encryption

No app modifications, FIPs-compatible.

SIEM Platforms

splunk> elasticsearch

Hubble Timescape

Zero Trust Environment

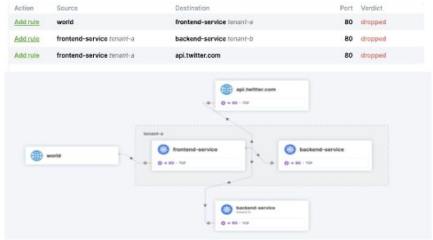
Platform & App Teams

Security Teams

Identity & API-Aware Network Policies

- K8s Network Policy
- DNS-aware Policy
- HTTP/gRPC-aware Policy
- Hierarchical Policy
- Deny Policy
- Host Policy

Network Policy Visibility & Troubleshooting



Policy Creation/Testing & GitOps Guardrails

okta · Active Directory · AWS IAM

Tenant Self-Service via SSO + Role-based Access Control

Hubble Timescape (events in S3-compat object store)

Logging Platforms

splunk> · elasticsearch