



adaptTo()

APACHE SLING & FRIENDS TECH MEETUP
BERLIN, 25-27 SEPTEMBER 2017

**Internet Scale Content Management with Apache Oak on
Kubernetes**

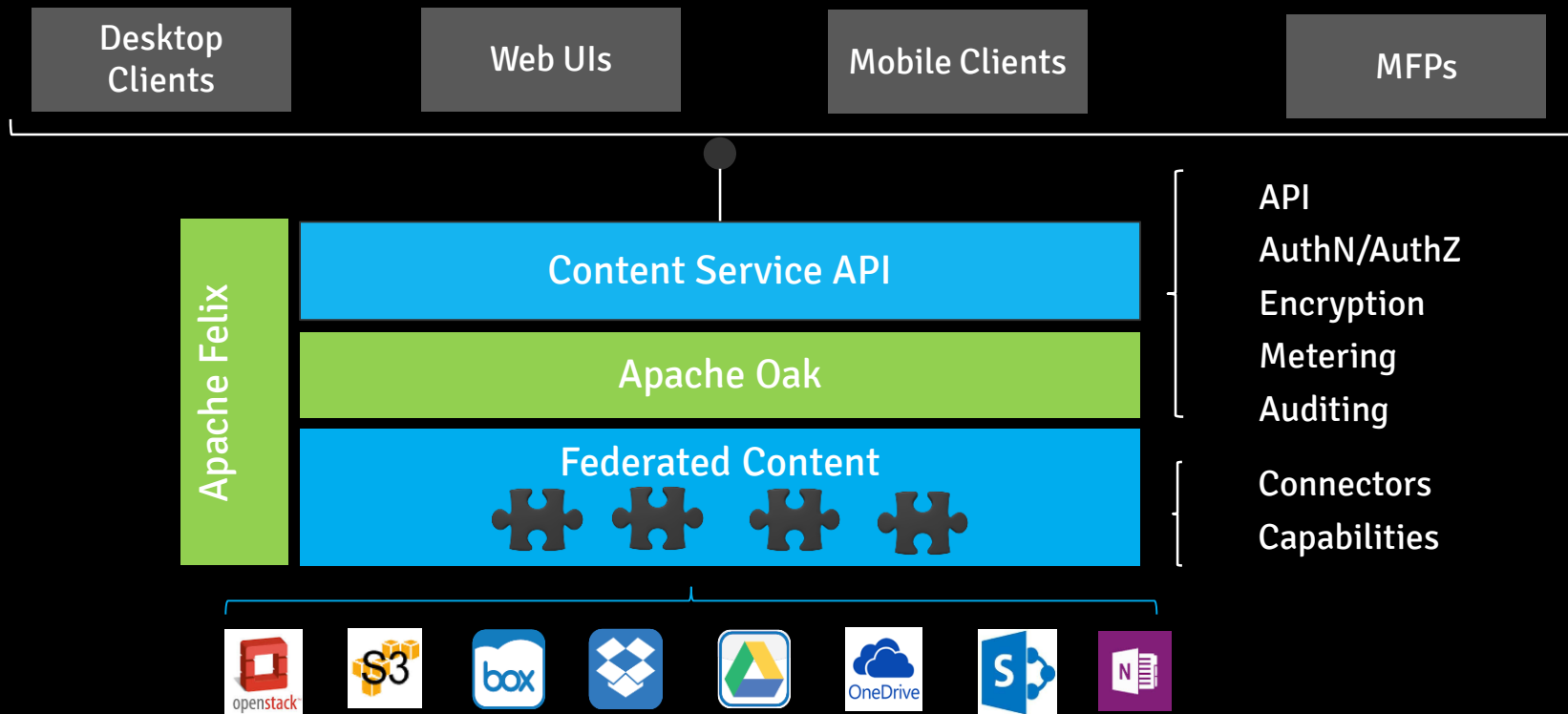
Fernando Saito, Galo Gimenez, HP Inc

Content at HP

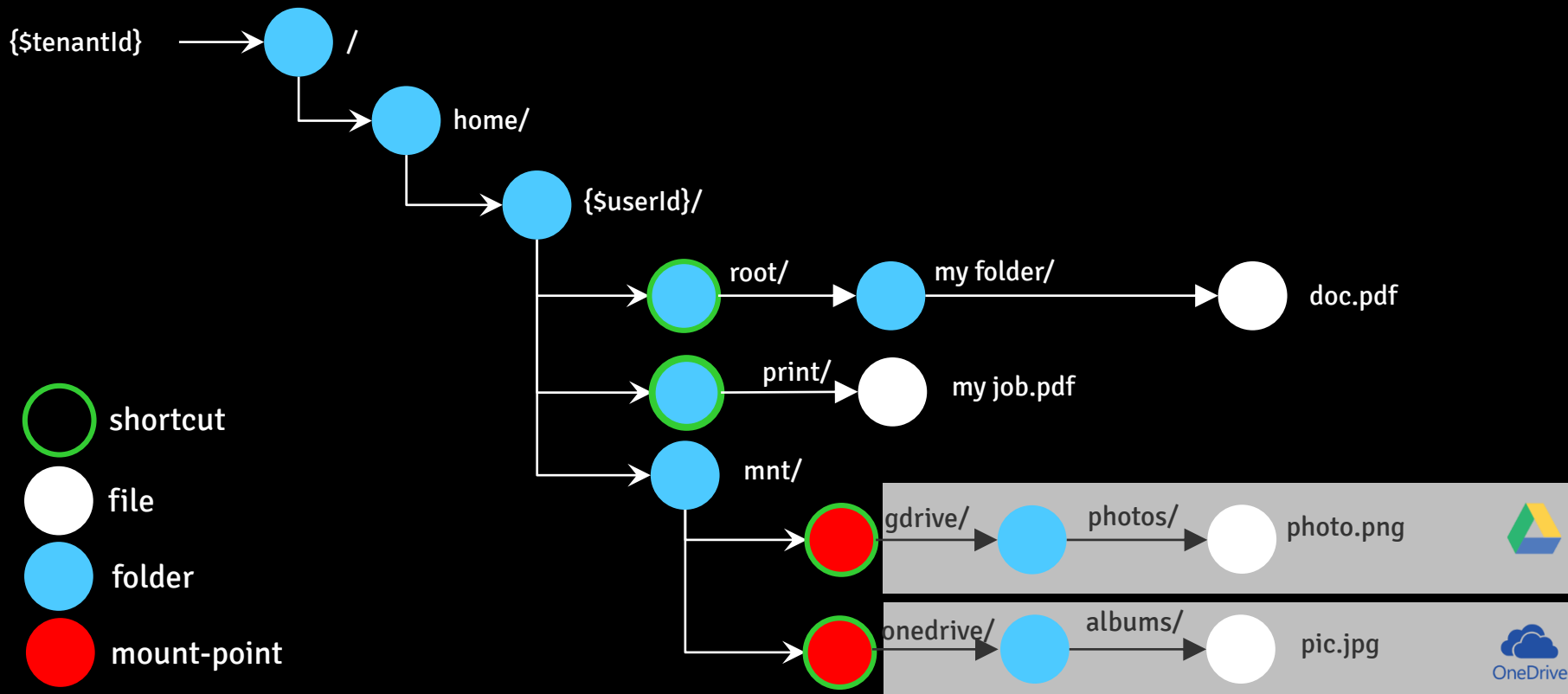
- HP is in the business of transforming digital objects to physical objects, and physical objects to digital objects
- Digital objects come in multiple forms, 3D models, documents, intermediate rendered artifacts, print jobs, etc.
- Our secure document management platform allows HP devices and applications access and store content
- 65M devices connected, ~50K documents per hour



SDM Content Service Architecture

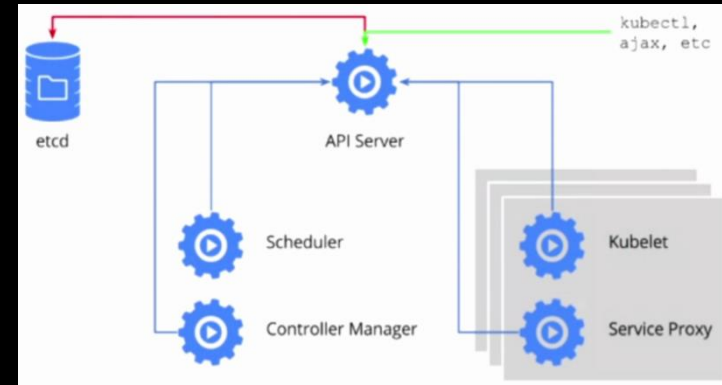


Federated Content Structure



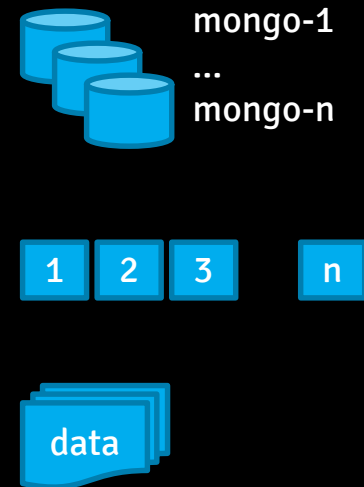


- A container scheduler system inspired in Google experience running containers
- Pods – scheduling containers in the same node
- Discovery – DNS based discovery allows legacy workloads to work
- Stateless and Statefull workloads



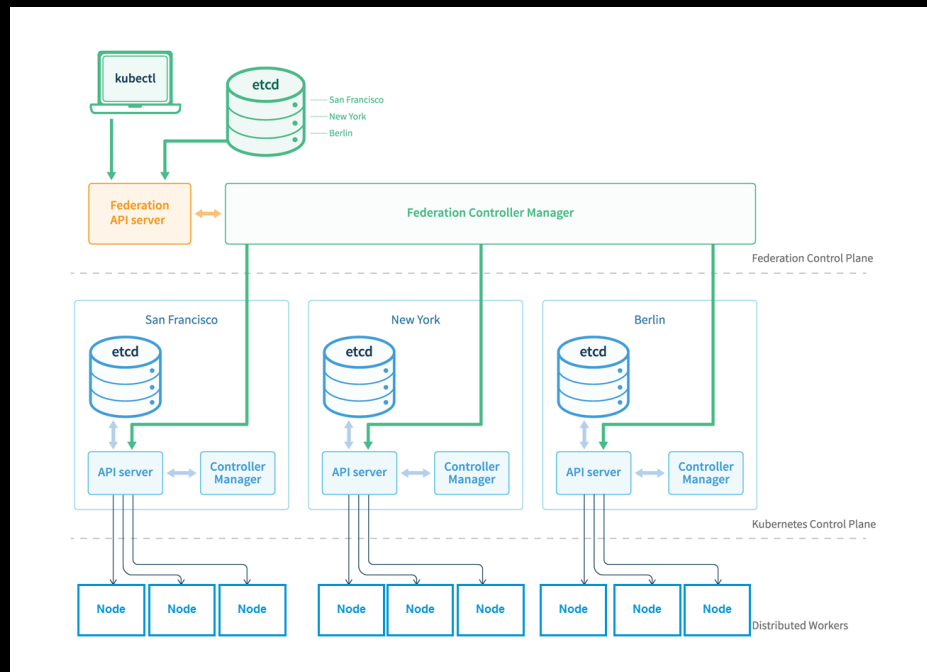
Kubernetes StatefulSets

- Designed for state full apps – i.e. Oak, MongoDB
- Consistent Naming – (Journaling has the same node names, Mongo replicas)
- Ordered start – (Solves race conditions setting up MongoDB)
- Attached to permanent storage – (Can use local Lucene Indexes and H2 caches)



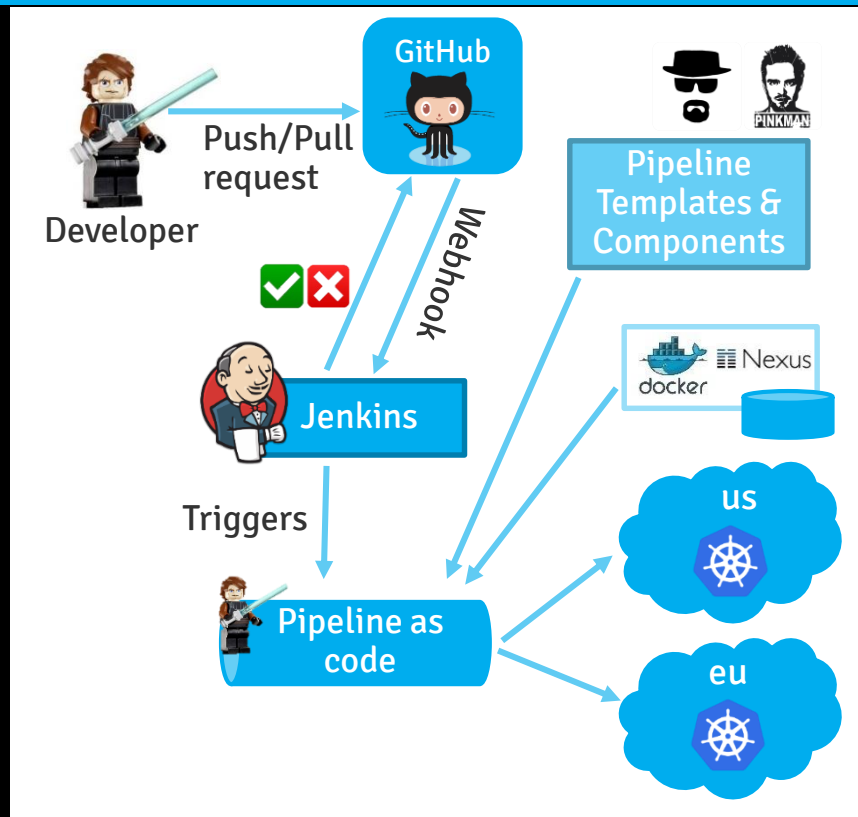
Kubernetes Federation

- Single API to access multiple Kubernetes Clusters
- Cluster state reconciliation
- Federated Services

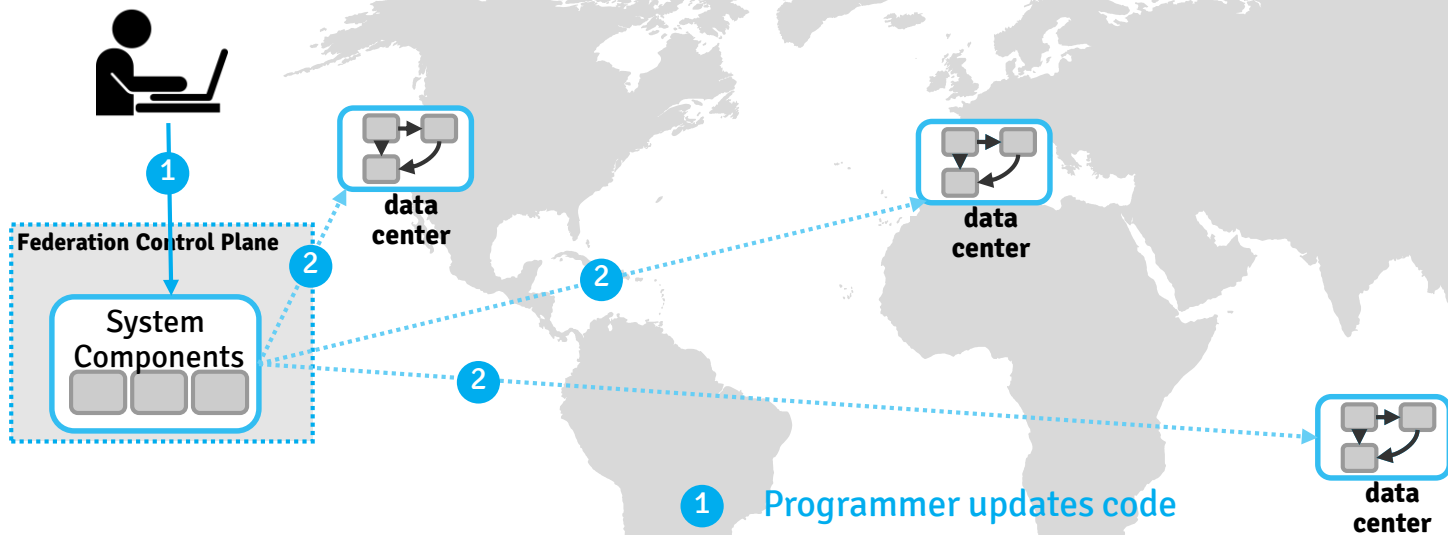


But Federation still lags some features

- Custom deployment toolset
- Multiple kubernetes clusters contexts
- Annotation modifiers
 - Region and Environment specific configurations
 - Regional and Global DNS
 - Public and Private names
- Resource quota



Global Deployment

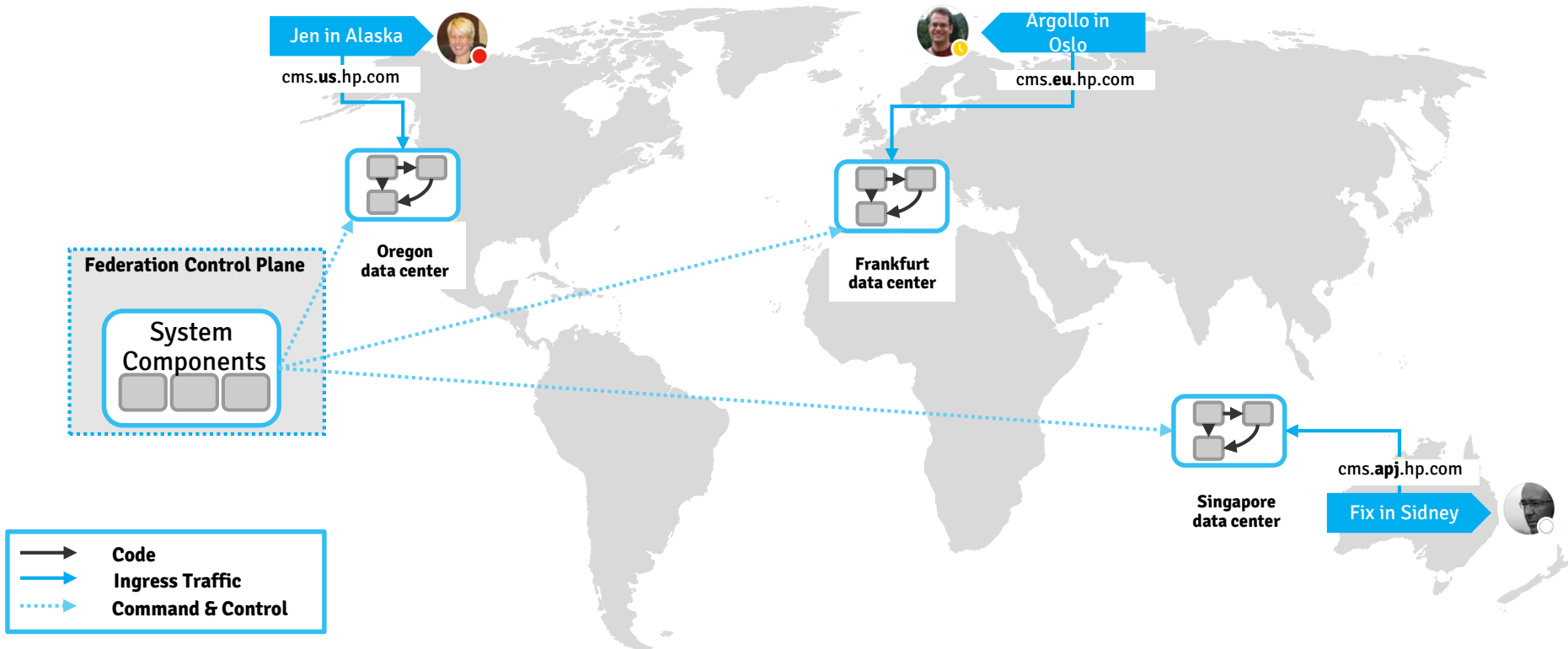


- 1 Programmer updates code
- 2 Container built, tested, and deployed globally



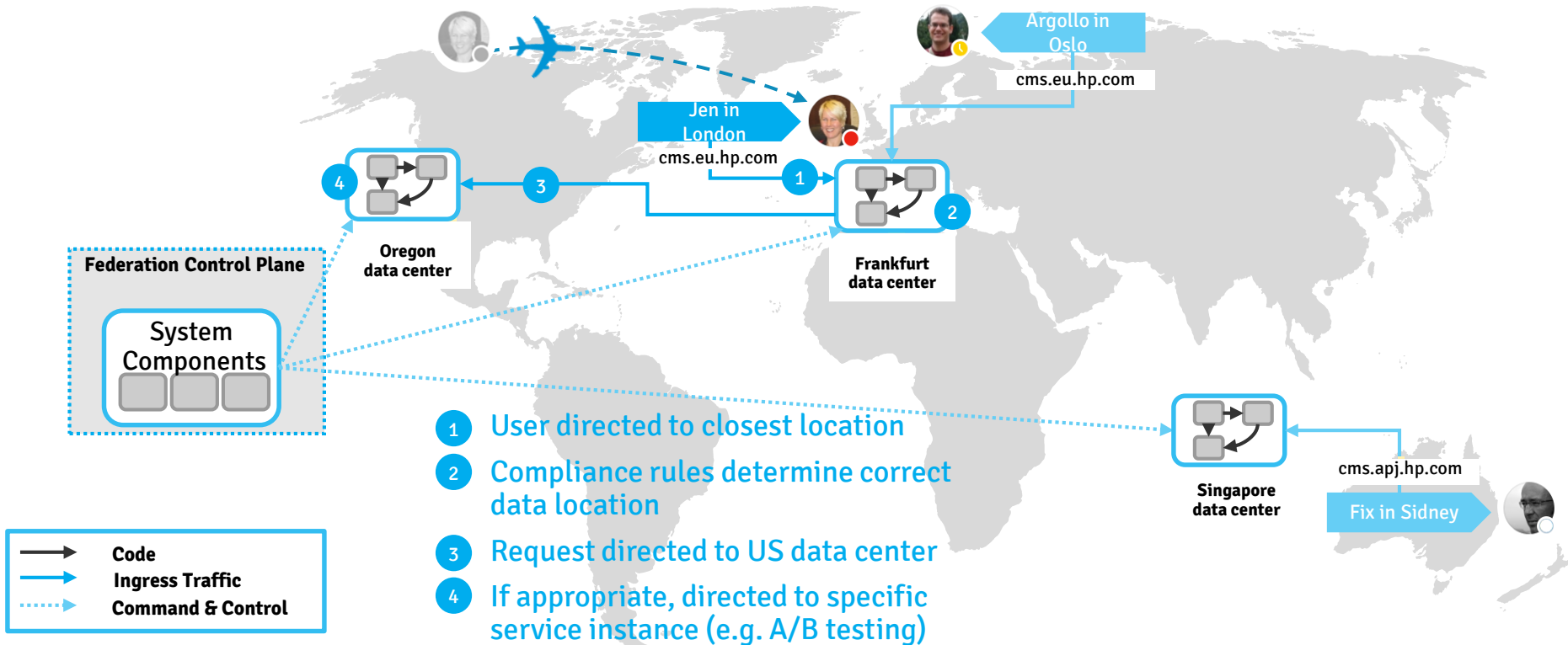
Optimize Customer Experience

User data is stored in the data center appropriate for that user based on global data compliance policies



Routing Customers to the Right Data Center

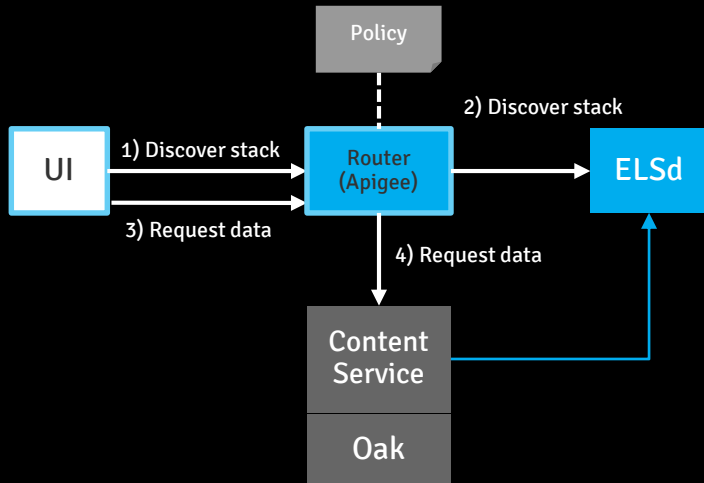
User initially served from closest datacenter based on location, but data still stored in appropriate data center



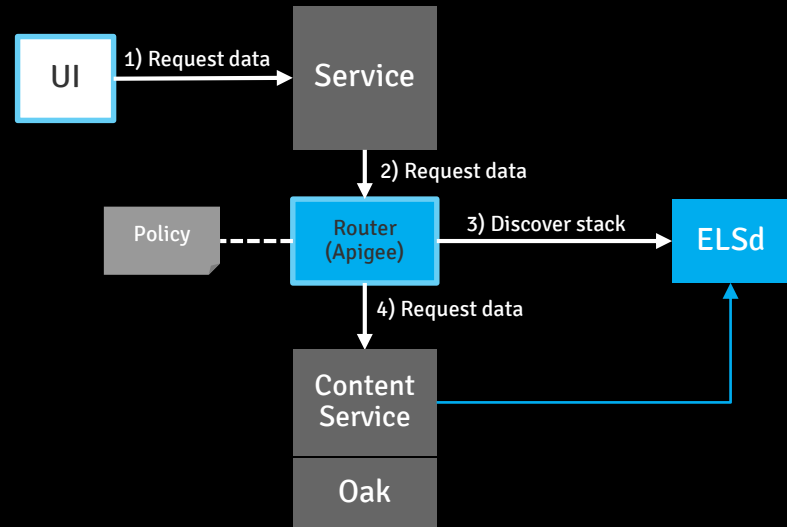
Data Discovery – Router & Entity Locator

- The router extracts a routing key (on JWT or SAML token) to locate the service instance where the record is stored
- ELSd allows multiple services to store metadata about records they own
- Services update ELSd entity to service instance mapping. Consistency checks run periodically
- Client and server-side routing

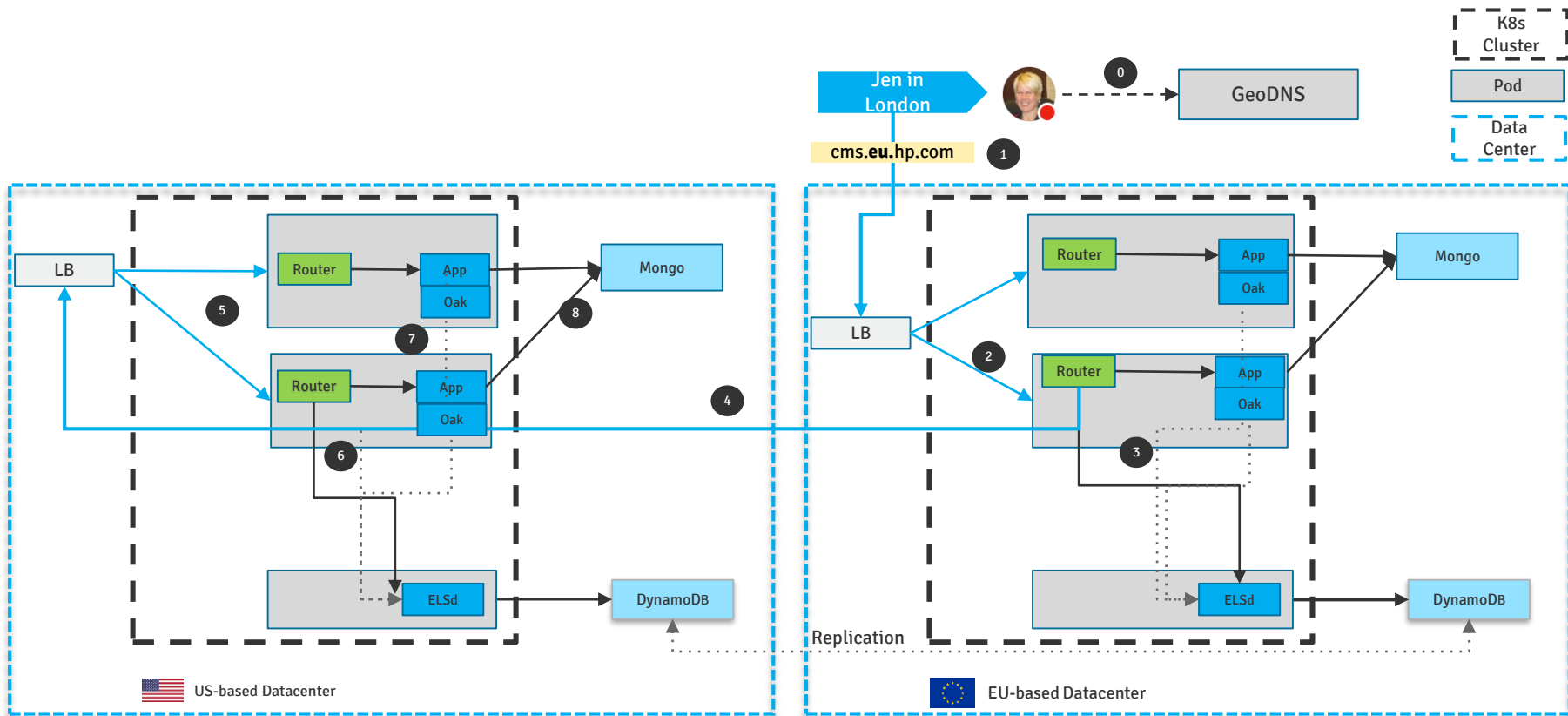
Client-side Routing



Server-side Routing



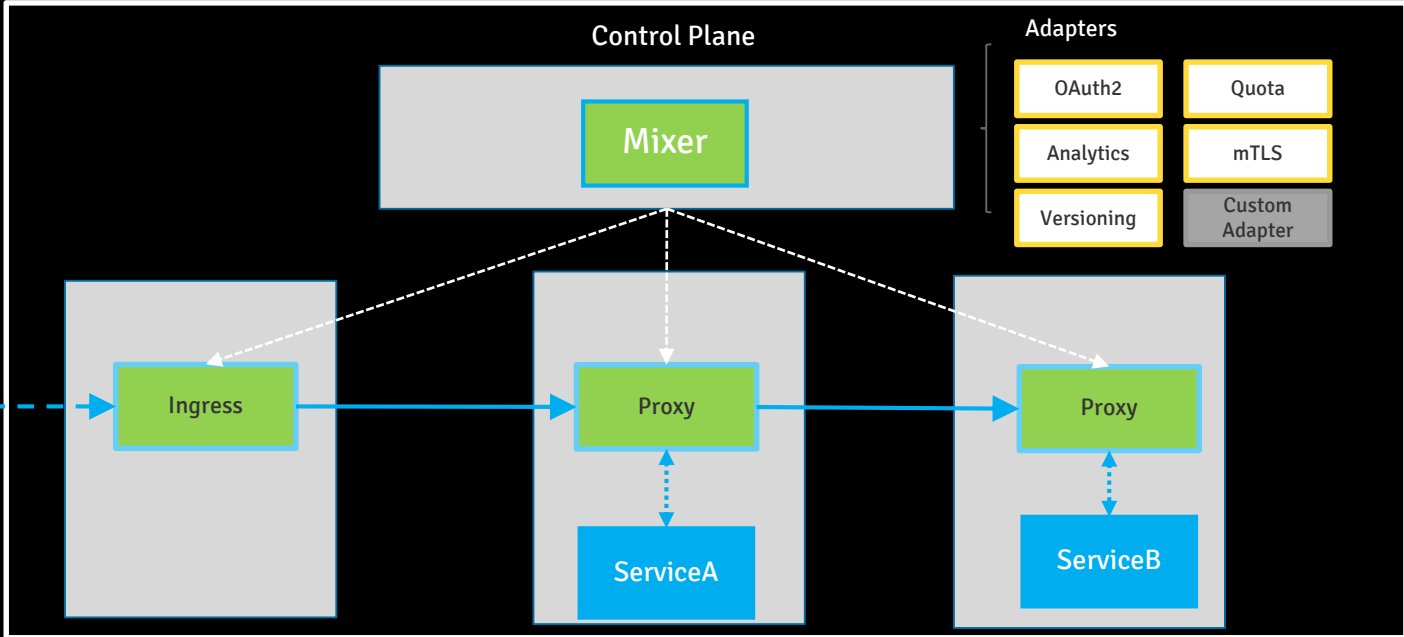
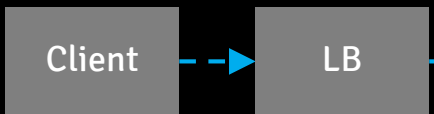
Data Localization



Next Steps - Istio Control Plane

Services are enriched by the Istio infrastructure on admission to the Kubernetes cluster
 Ingress applies policies to external traffic. Proxy applies policies to internal traffic
 Control plane for policy, telemetry, security,...

gRPC
 ----->
 HTTPS1.1/2 TLS + JWT
 - - - ->
 HTTPS Secure mTLS + JWT
 - - - ->
 HTTP1.1/2
 - - - ->



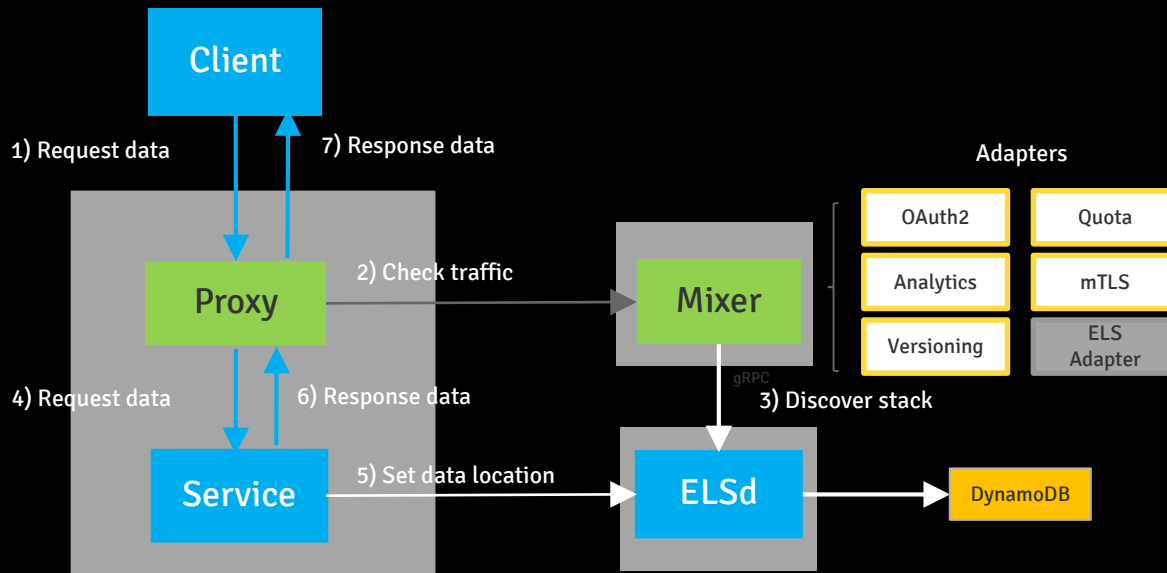
Istio
 Cluster
 Pod

Next Steps - Entity Locator Service

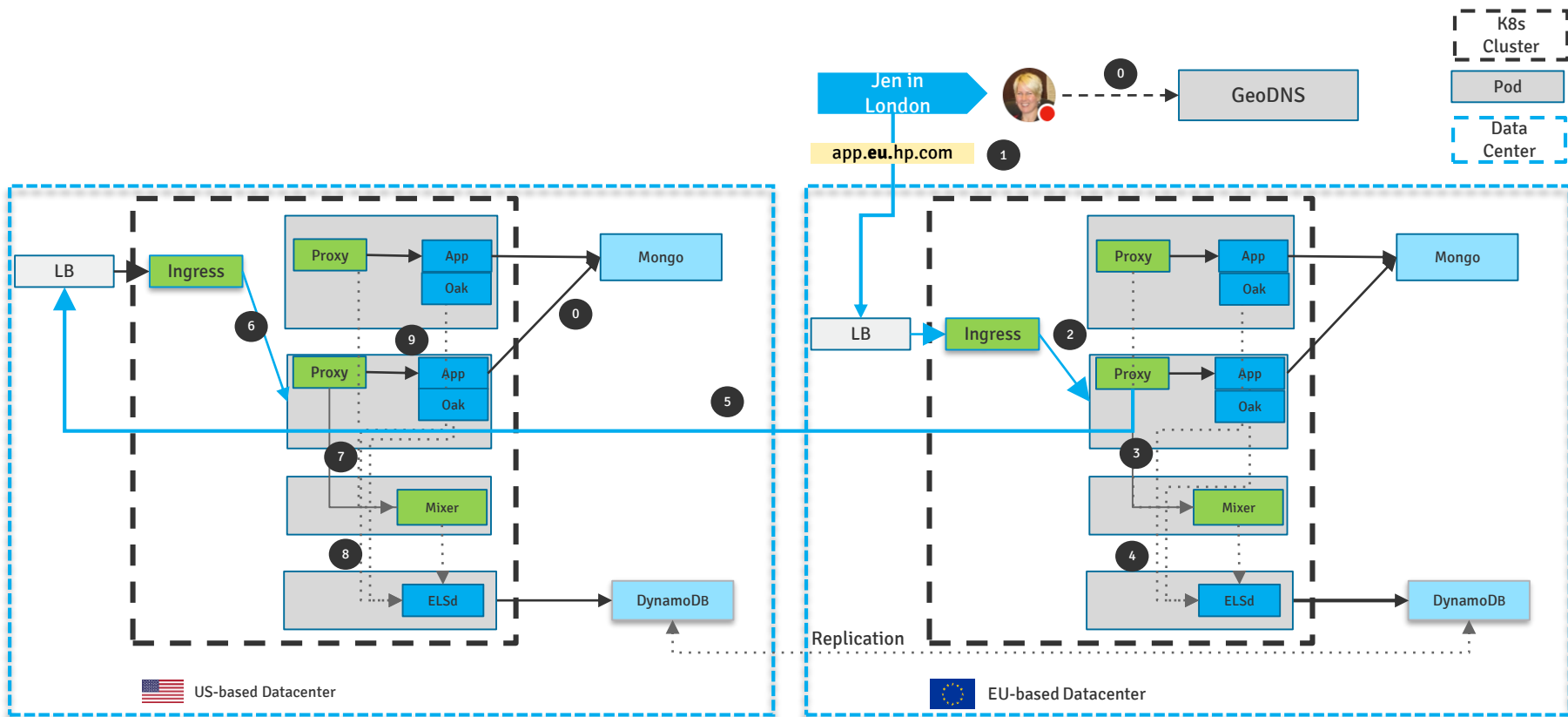
ELS allows multiple services to store metadata about records they own

It provides an client- and server-side routing

The service is globally replicated using AWS DynamoDB – every change is pushed to other instances immediately



Next Steps - Data Localization



Thanks / Danke