The Salesforce Service Mesh

- Our Istio Journey

Pratima Nambiar, Architect
pnambiar@salesforce.com

Agenda - The Salesforce Service Mesh

Our Istio Journey

- Background - Why Service Mesh ?
- Initial Service Mesh implementation
- Why Istio
- Istio POC
- Progressive adoption of Istio
- Features we are watching and expect to adopt

Background - Why Service Mesh ?

Security / Compliance

- mTLS everywhere using specific set of ciphers
- FIPS compliance in some deployments
- Zero Trust

Reliability

- #1 core value - **trust** translates into ensuring high availability

Observability

- Single pane of glass monitoring solution vs. fragmented islands of observability

Build an application networking layer that provides all the required plumbing for making service-to-service communication secure, reliable, observable so that service owners can focus on business logic

Design Principles

Keep it simple

Solve for the current business use cases and make incremental progress

Favor incremental adoption of technologies and controlled exposure of features (Eg. envoy and istio)

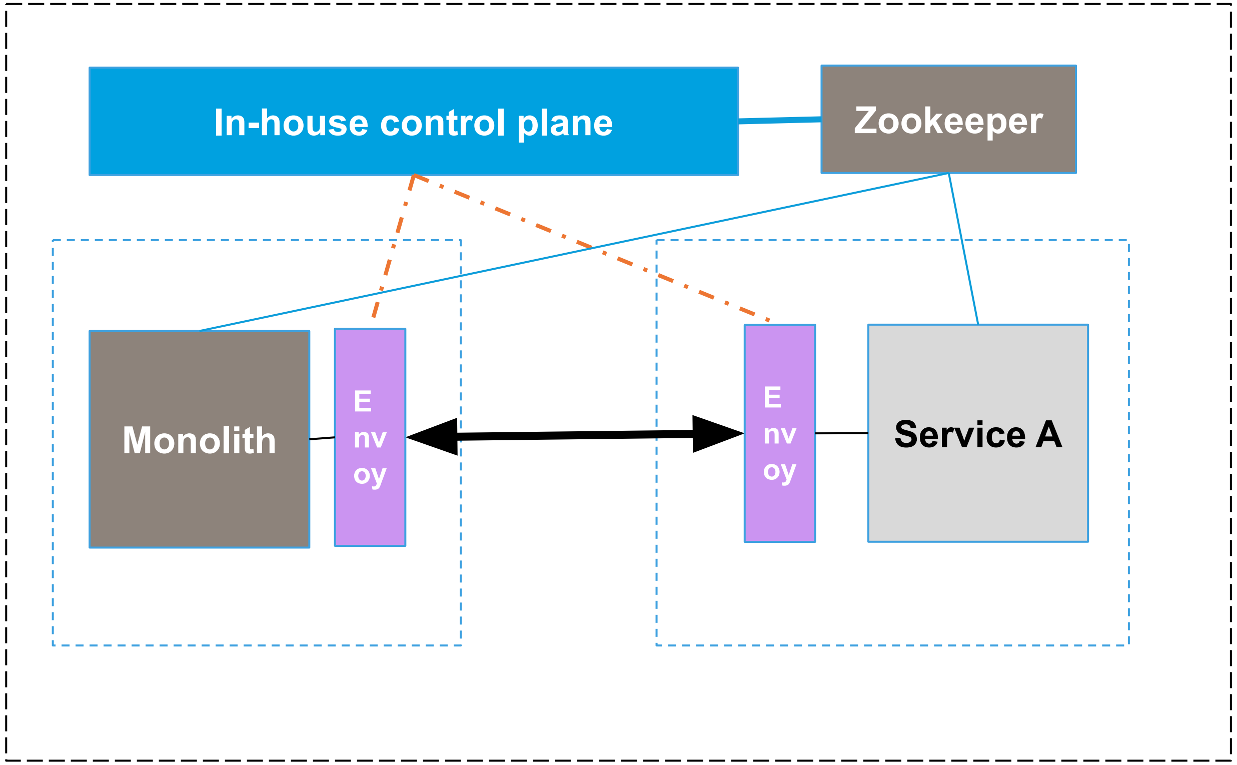
Make the application networking layer as transparent as possible

Invest time in horizon scanning

Pre-Istio Service Mesh

- Started with another open source data plane
- Switched to envoy and built our own XDS implementation
  - Solve for the most common use cases
  - Zookeeper backed EDS
  - Opinionated configuration for resiliency based on our test framework
  - Metrics for visibility to our internal metrics system

mid 5 digits # of envoys in production



Why Istio

As service mesh adoption grew keeping up our control plane to solve for new use cases was challenging

- StatefulSets
- TCP services
- Redis
- Service specific config

Pivot to Istio was strategic

- Initial review indicated it's sophisticated features would meet our ends.
- Strong active community - ~275 contributors and has grown significantly since then.

Istio POC

Minimum viable product

- mTLS using our internal CA
- Bare metal / Kubernetes service support
- Metrics to our internal metrics system
- Set good defaults for resilience policies

Istio Contributions

- Support for custom CA.
- Performance related fixes for bare metal
- Resiliency fixes for pilot and envoy communication
- Envoy metrics service configurable

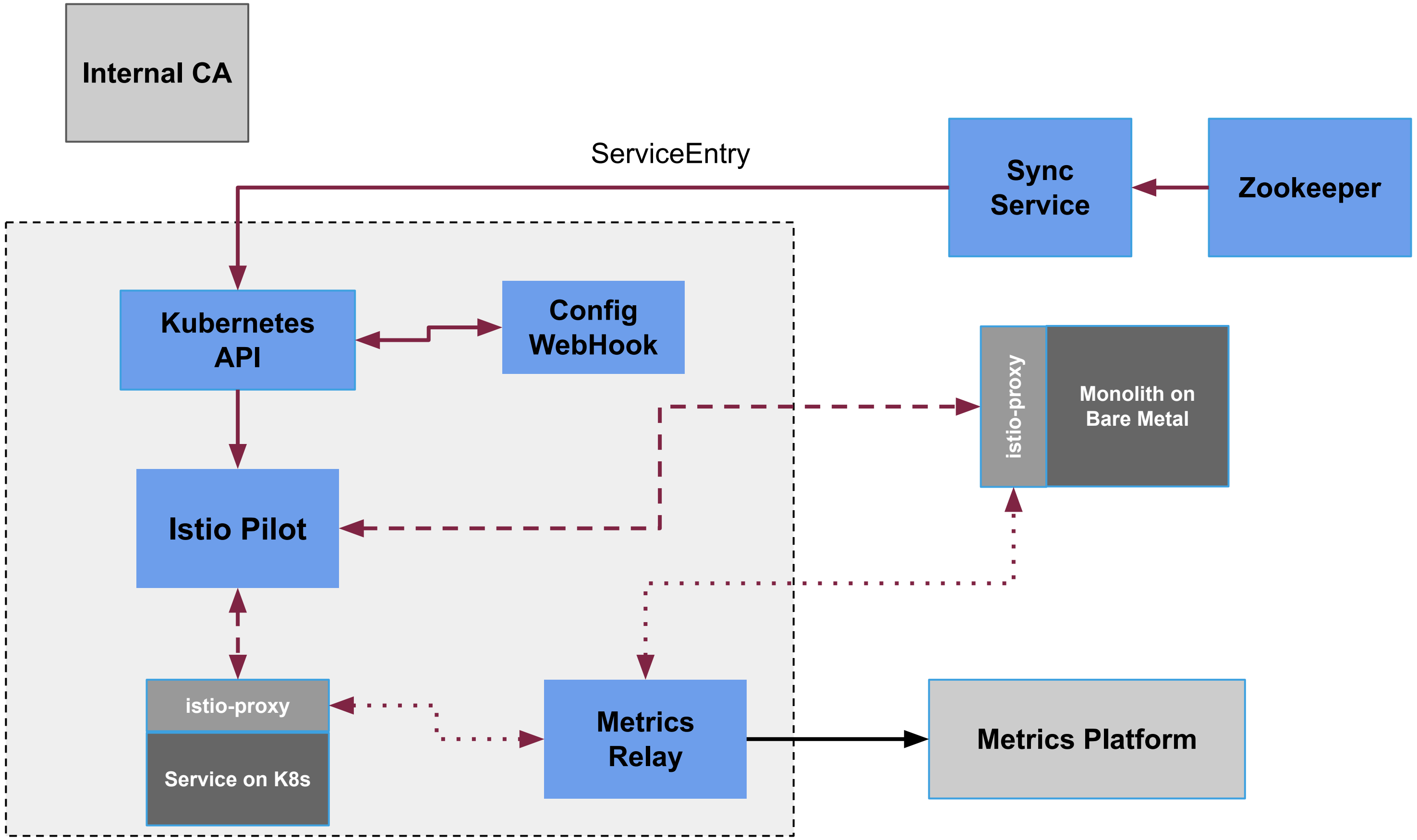
What we liked

- CRDs for defining mesh configuration
  - Easier to read
  - Can plugin to our tools and pipelines

What could have been better

- Very little support for mesh wide configuration
- Istio converts all K8s services into sidecar configuration.

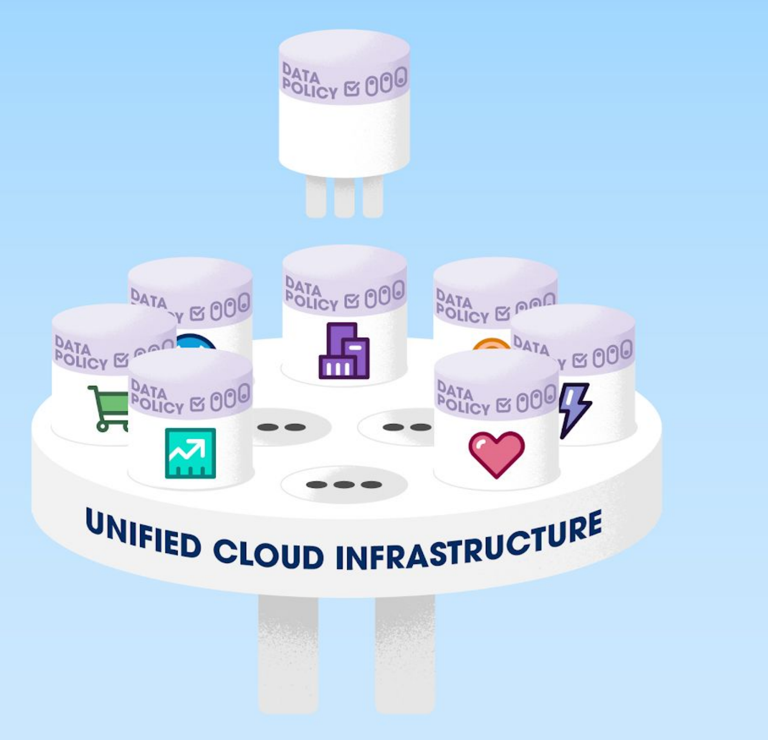
Istio based Service Mesh



Salesforce Hyperforce

Salesforce's pivot to run on public cloud infrastructure presented additional challenges:

- Zero Trust Architecture
- Increased adoption of dynamic infrastructure
- Multi Substrate



Istio Adoption - Continued

New Use Cases - QPid, Solr, Zookeeper, Redis

Blue/Green Deployment of our monolith

Declarative authorization policies using Envoy Filters

OPA based authorization for more finer grained/sophisticated rules

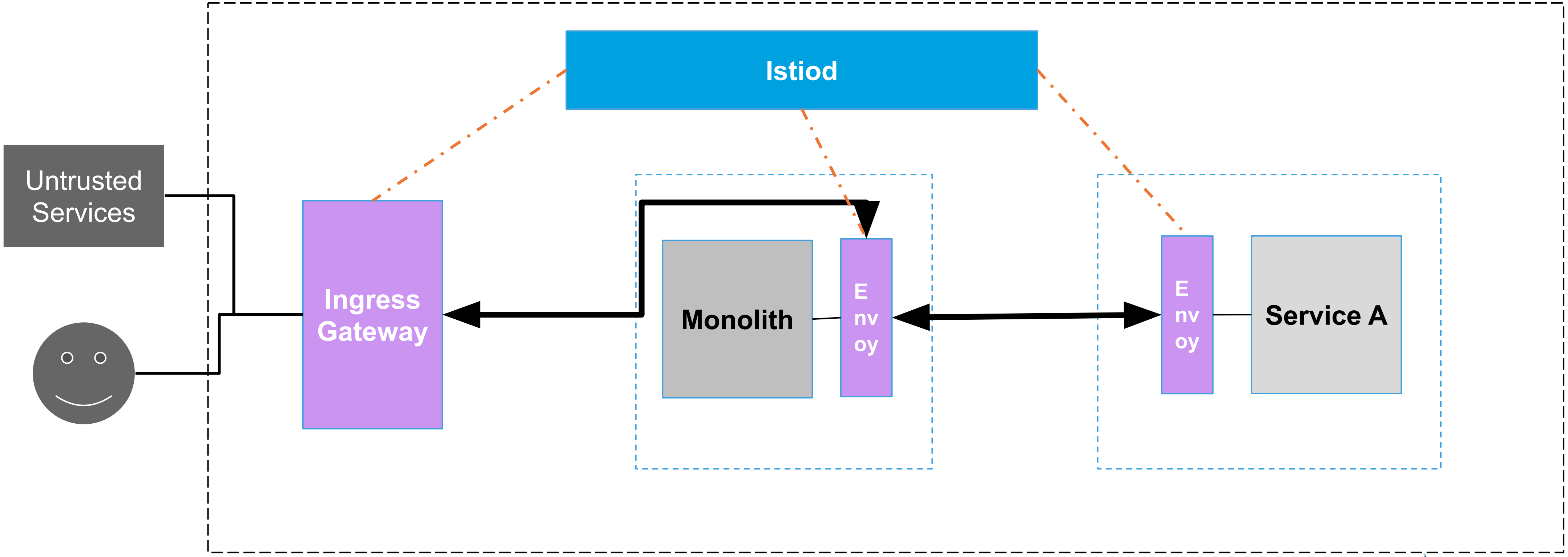
Out-of-the-box health signals for all services for SRE using envoy telemetry

Istio deployment & upgrades managed via spinnaker pipelines

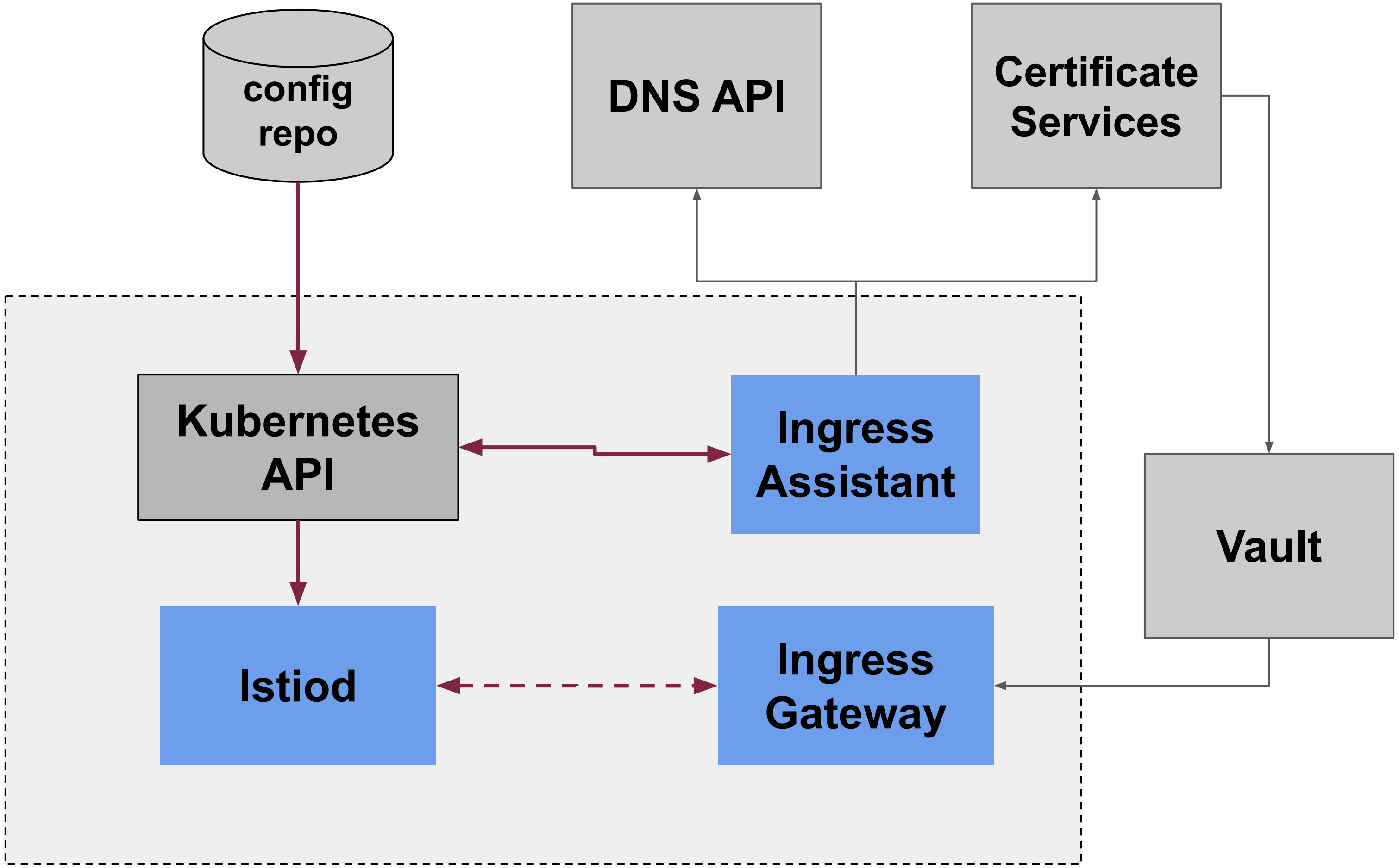
Istio Adoption - Ingress Gateway

Ingress Gateway as our edge proxy for all traffic from the public internet

DNS and Certificates API integration to support our complex DNS/certificates requirements



Istio Adoption - Ingress Gateway



Istio adoption - coming soon

HBase on Service Mesh

Auto registration for services running on bare metal

DNS Proxy for TCP multi cluster support

Sophisticated Traffic Shifting

JWT based Authentication/Authorization

Integrations for Service Protection

Rate limiting

Features we are watching

Support for mesh spanning multiple Kubernetes clusters

WebAssembly technology for proxy extensions

Improvements to DNS Proxy (Statefulset support)

Scale - Better support for larger meshes

- Reduced proxy initialization times
- Optimized config delivery (Delta Xds)
- Improved Envoy -> control plane load balancing

Egress Gateway evolution

Smoother upgrades

Thank You