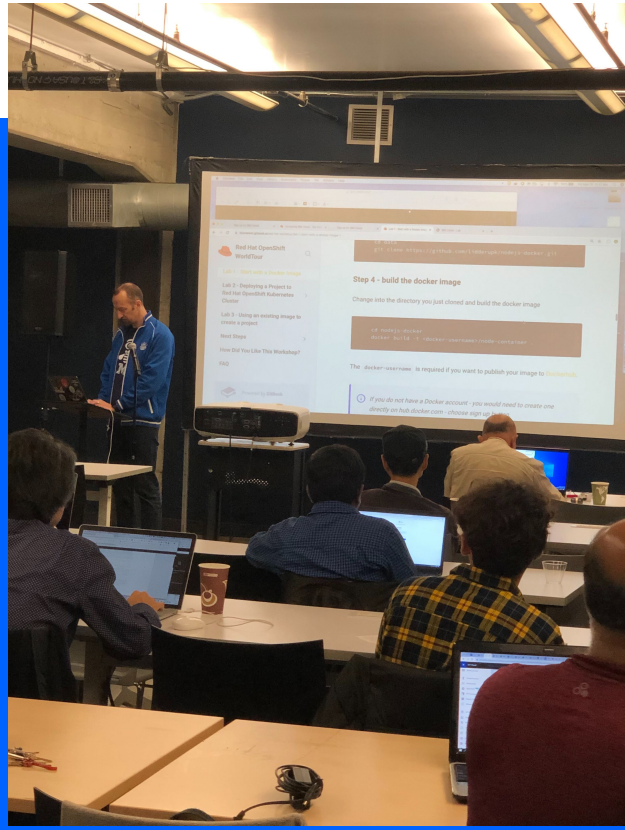
NeuVector and IBM on Microservice Mesh with Istio

Intro and Protecting Your Service Mesh

Tracy Walker | Solution Engineer | NeuVector

Marek Sadowski | Developer Advocate | IBM

ibm.biz/202010-istio



V1 2020 10 01

IBM **Developer**

IBM

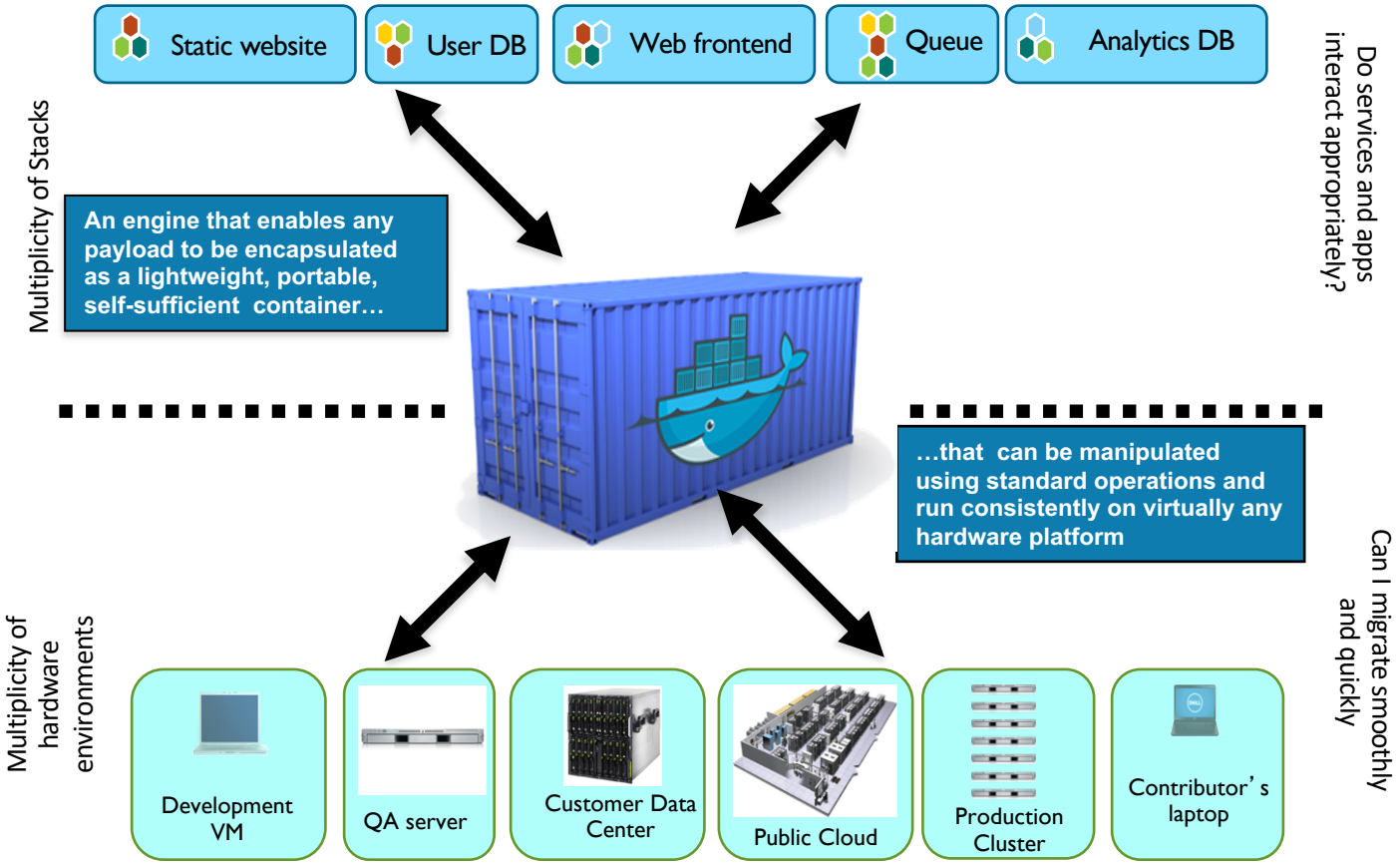
Agenda:

1. Warm up with Docker
2. Hands-on
3. Istio – an introduction to microservice mesh
4. claim your Kubernetes cluster and try to use managed Istio **Hands-on**
5. Network Visibility when using a Service Mesh
6. Layer 7 Network Policy Enforcement & Micro-Segmentation Violations

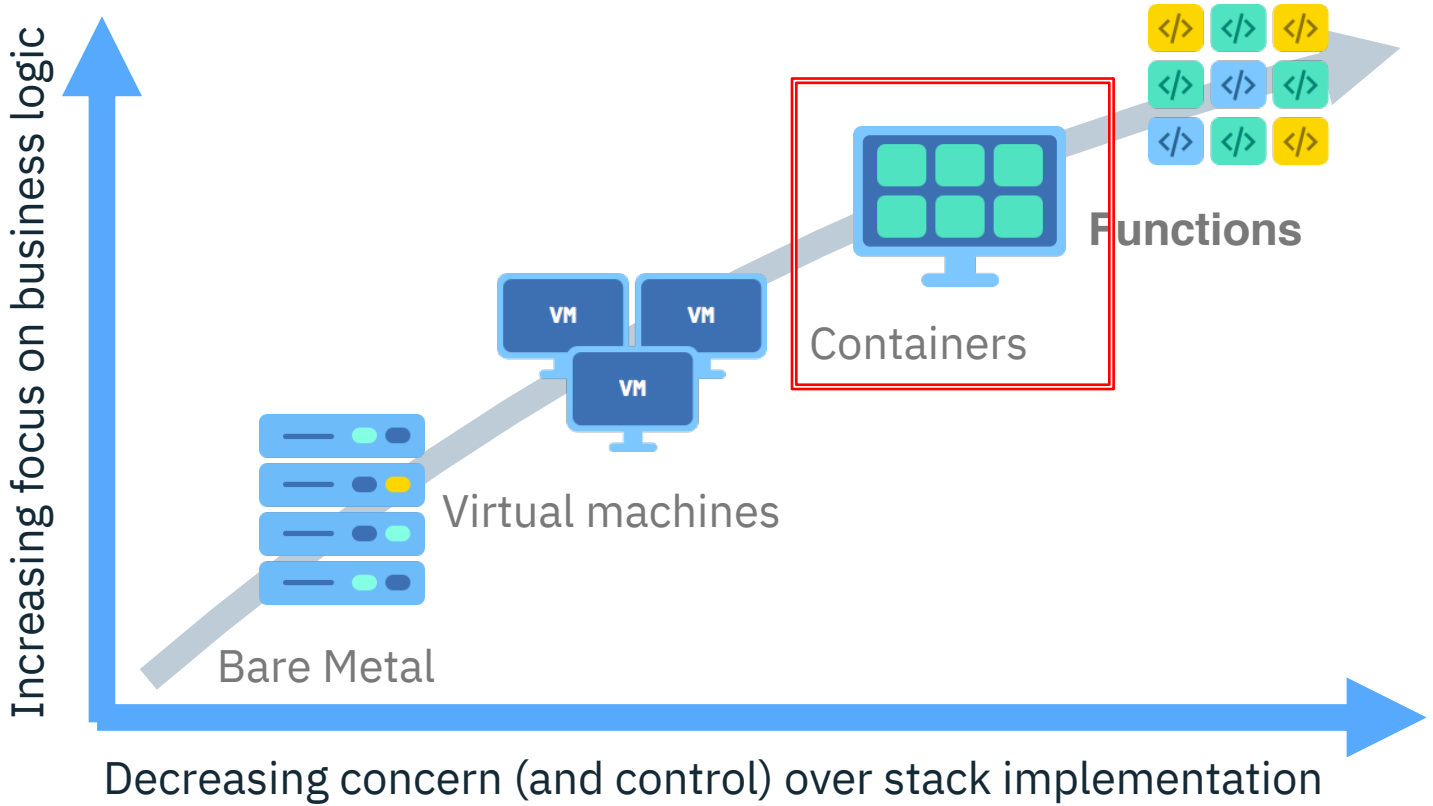
THE POLL

Why Containers?

The Solution - A Shipping Container for Code

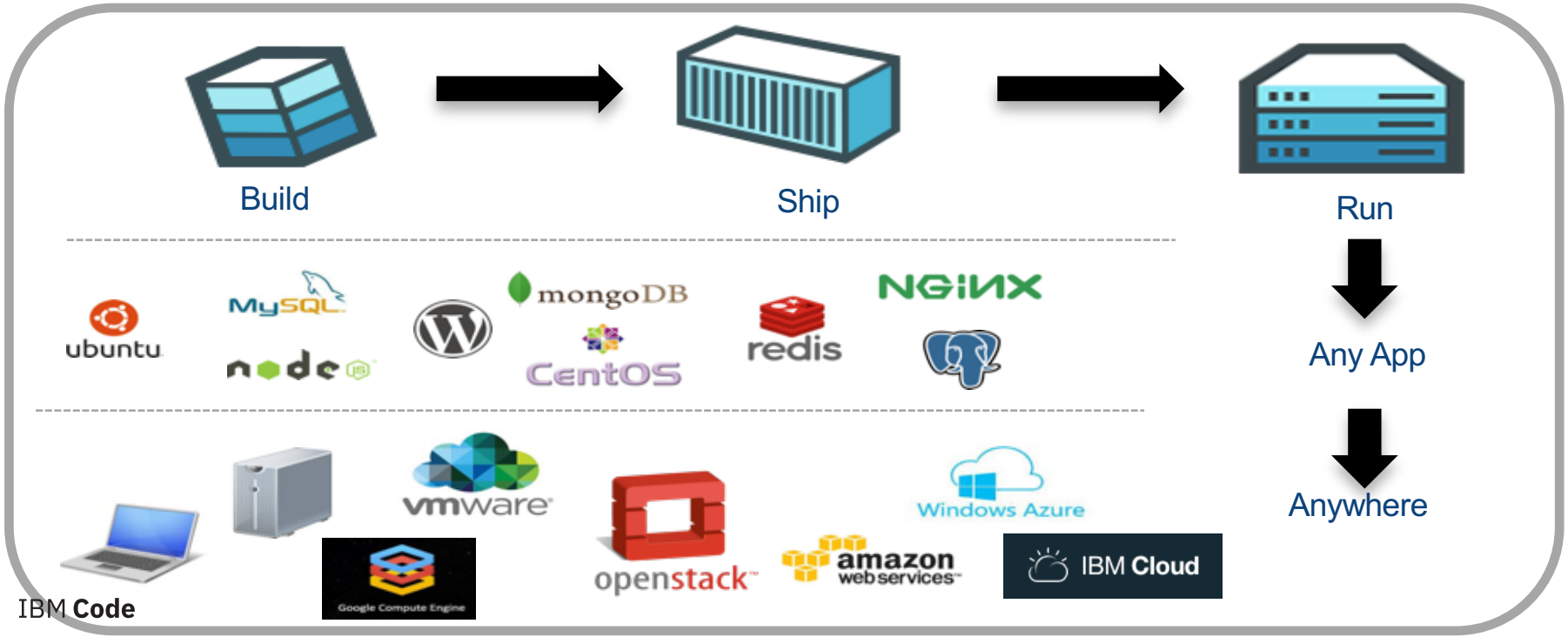


How we got here



Docker Mission

Docker is an **open platform** for building distributed applications for **developers** and **system administrators**



Docker Component Overview

Docker Engine

- Manages containers on a host
- Accepts requests from clients
  - REST API
- Maps container ports to host ports
  - E.g. 80 → 3582

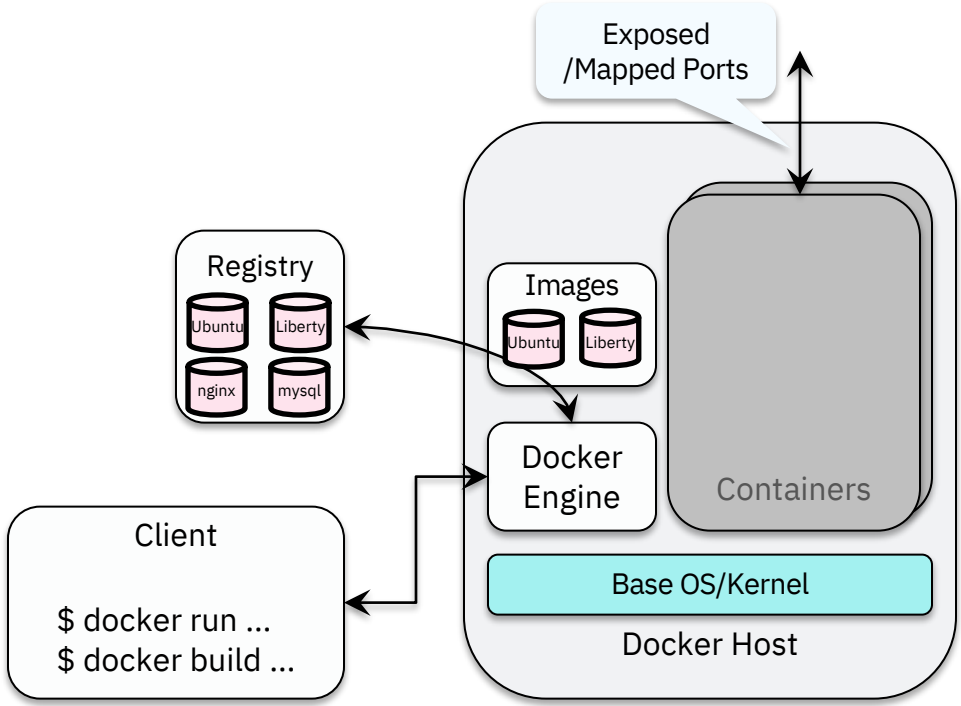
Images

Docker Client

- Drives engine
- Drives "builder" of Images

Docker Registry

- Image DB



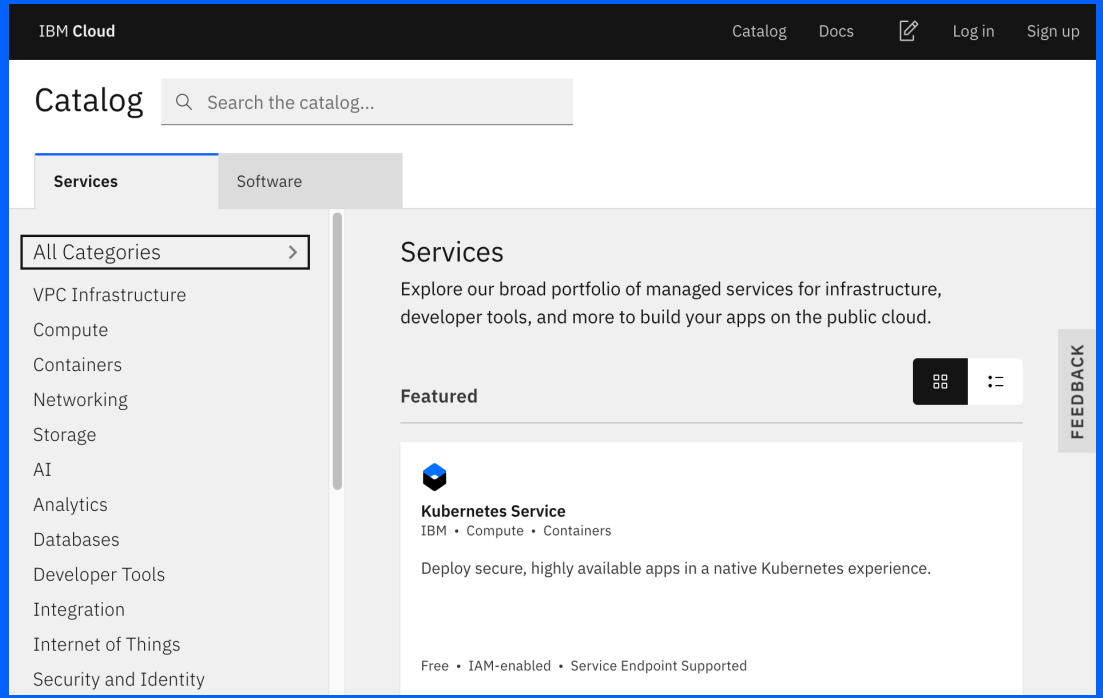
Hands-on

LAB
building a translation service with Watson:

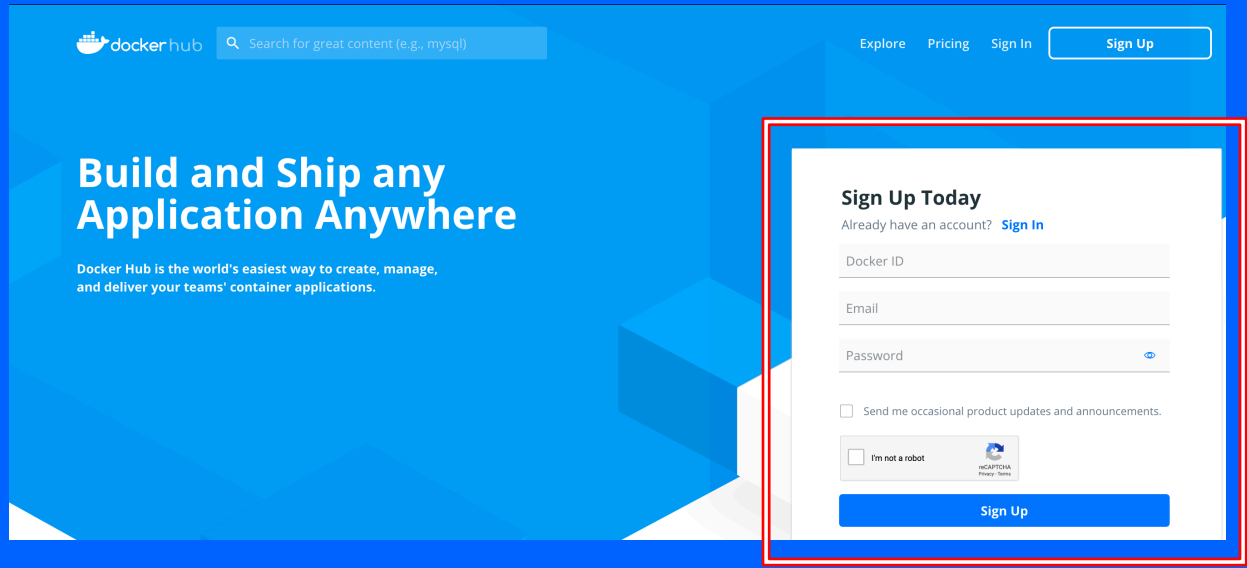
http://ibm.biz/202010-istio-lab0

IBM Cloud Catalog

https://cloud.ibm.com/catalog



Download FREE Docker Desktop and use your terminal on your computer
or just sit back and watch



Second part –
the orchestration
of successful API deployment

Containers

Everyone’s container journey starts with one container....

Containers

At first the growth is easy to handle....

Containers

But soon it is overwhelming... chaos reigns

Container Orchestration

Allows users to define how to coordinate the containers in the cloud when the multi-container packaged application is deployed.

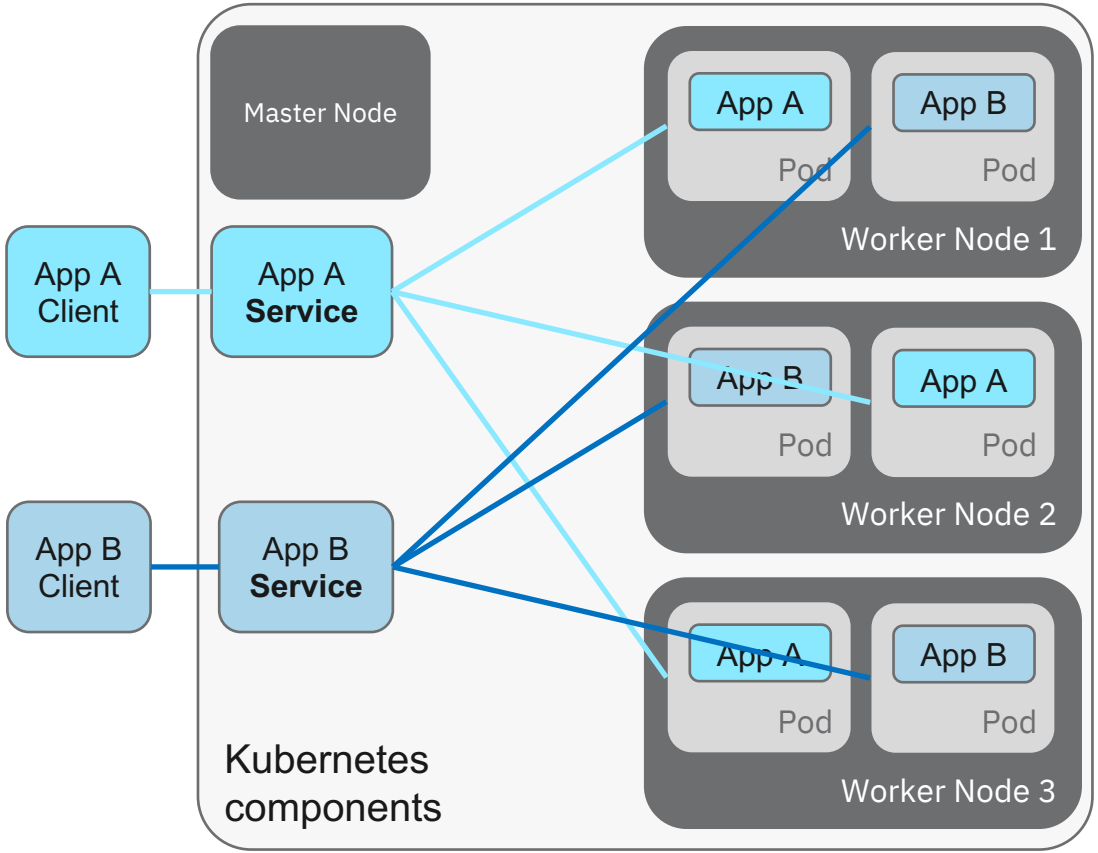
- Scheduling
- Cluster management
- Service discovery
- Provisioning
- Monitoring
- Configuration management

What is Kubernetes?

- Container orchestrator
- Manage applications, **not machines**
- Designed for extensibility
- Open source project managed by the Linux Foundation

Kubernetes Architecture: Workloads

- Container
  - Packaging of an app
- Pod
  - Unit of deployment
- Service
  - Fixed endpoint for 1+ pods



Kubernetes

Intelligent Scheduling

Self-healing

Horizontal scaling

Service discovery & load balancing

Automated rollouts and rollbacks

Secret and configuration management

Challenges with Microservices

Security

Canary deployments

A/B testing

Retries and Circuit breaking

Rate limiting

Fault injection

Policy management

Telemetry

What is a ‘Service Mesh’ ?

A network for services, not bytes

- Observability
- Resiliency
- Traffic Control
- Security
- Policy Enforcement

Istio

An open platform to connect, manage, and secure microservices

http://istio.io

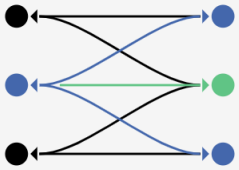
IBM Code

Istio community partners

- RedHat
- Pivotal
- WeaveWorks
- Tigera
- Datawire
- Scytale (SPIFFE)
- Microsoft
- Uber (Jaeger)

Istio

Connect, secure, control, and observe services.

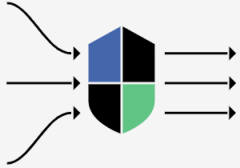


Connect

Intelligently control the flow of traffic and API calls between services, conduct a range of tests, and upgrade gradually with red/black deployments.

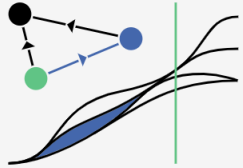
Secure

Automatically secure your services through managed authentication, authorization, and encryption of communication between services.



Control

Apply policies and ensure that they're enforced, and that resources are fairly distributed among consumers.



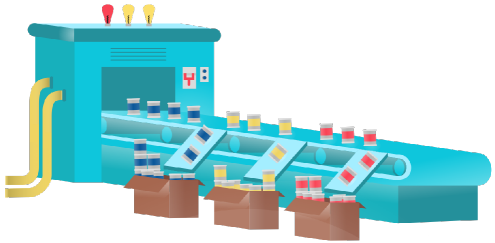
Observe

See what's happening with rich automatic tracing, monitoring, and logging of all your services.

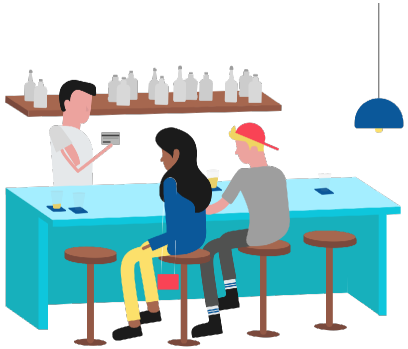
Istio

WHERE ISTIO FINDS ITS PLACE

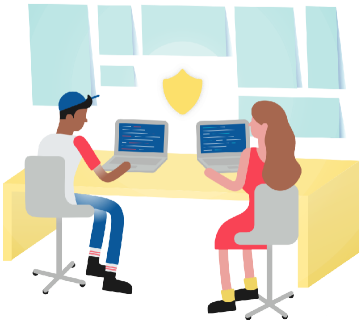
Intelligent Routing and Load Balancing



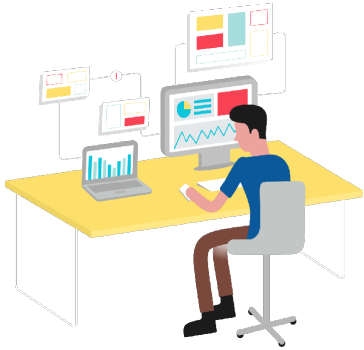
Fleet Wide Policy Enforcement



Resiliency across Languages and Platforms



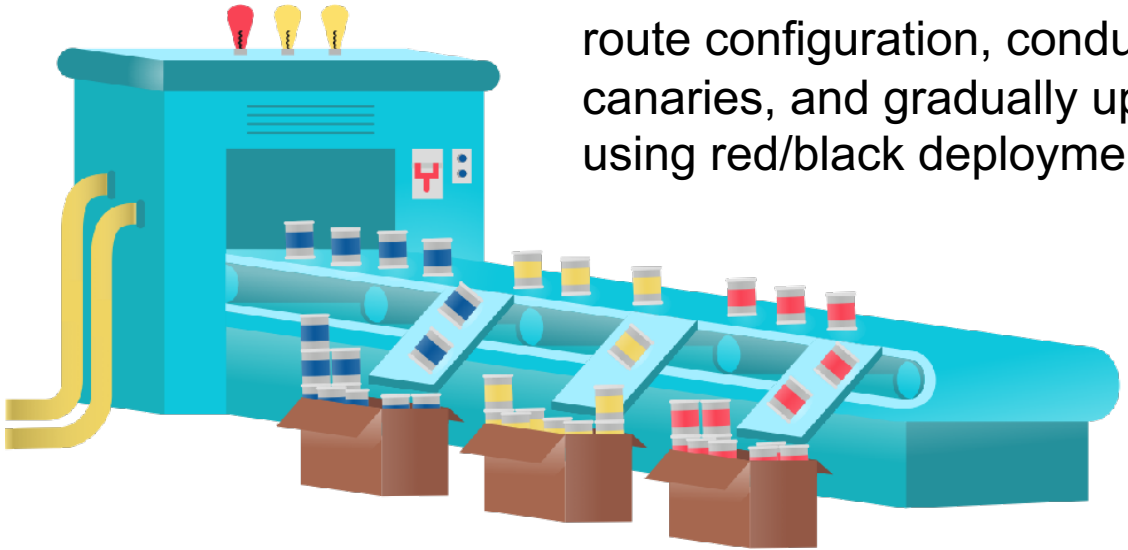
In-Depth Telemetry and Reporting



Istio

WHERE ISTIO FINDS ITS PLACE

Intelligent Routing and Load Balancing

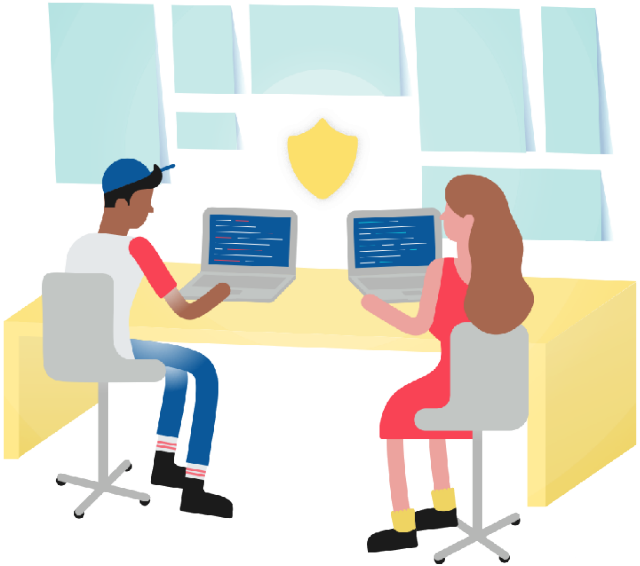


Control traffic between services with dynamic route configuration, conduct A/B tests, release canaries, and gradually upgrade versions using red/black deployments.

Istio

WHERE ISTIO FINDS ITS PLACE

Resiliency across Languages and Platforms



Increase reliability by shielding applications from flaky networks and cascading failures in adverse conditions.

Istio

WHERE ISTIO FINDS ITS PLACE

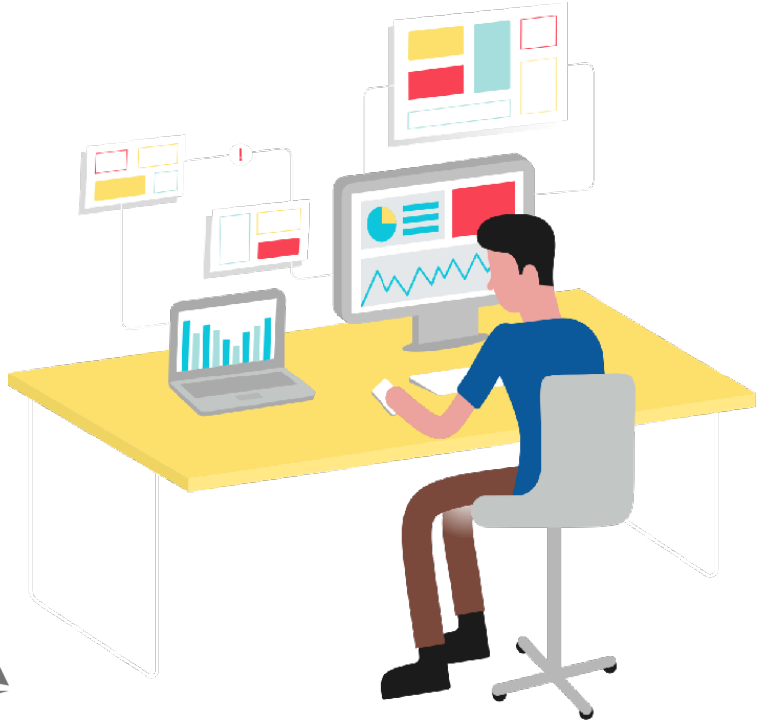
Fleet Wide Policy Enforcement

Apply organizational policy to the interaction between services, ensure access policies are enforced and resources are fairly distributed among consumers.

Istio

WHERE ISTIO FINDS ITS PLACE

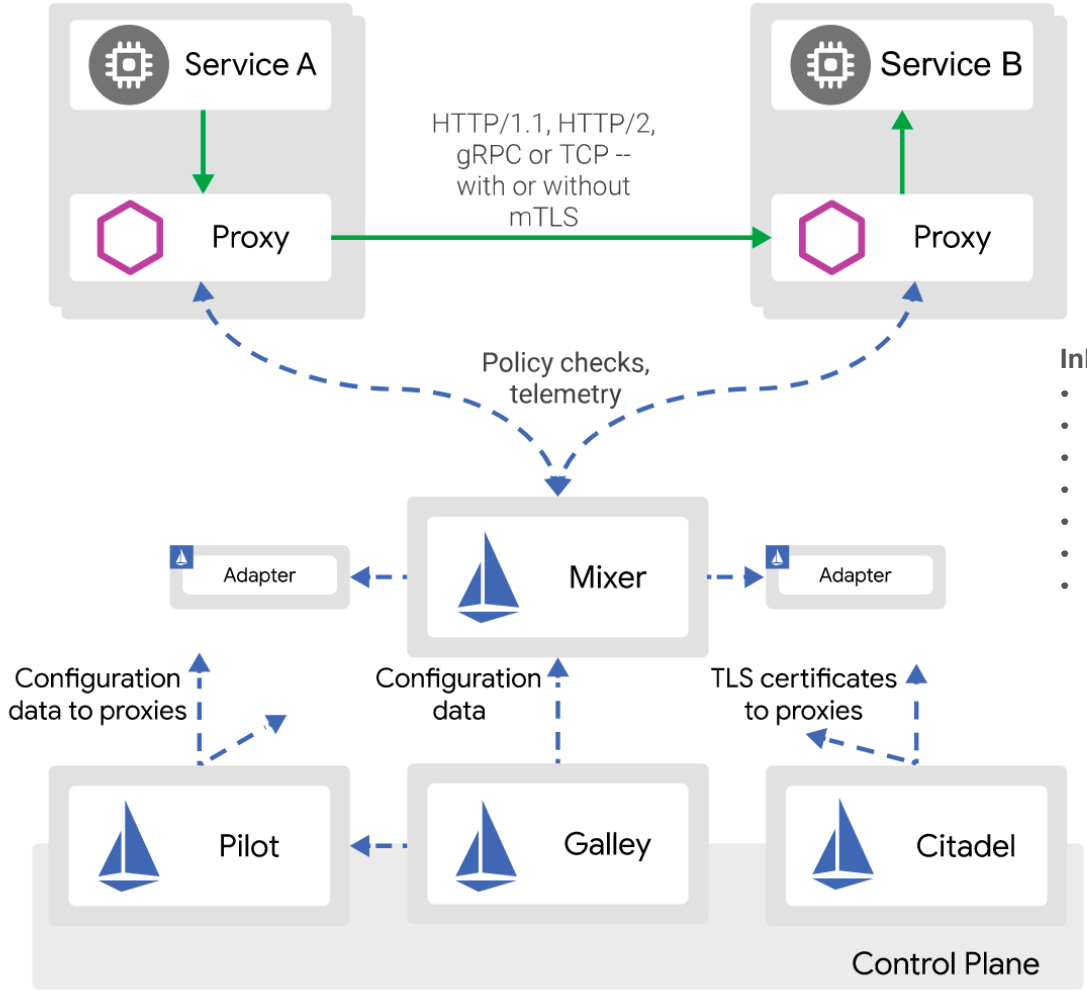
In-Depth Telemetry and Reporting



Understand the dependencies between services, the nature and flow of traffic between them and quickly identify issues with distributed tracing.

Outbound features:

- Service authentication
- Load balancing
- Retry and circuit breaker
- Fine-grained routing
- Telemetry
- Request Tracing
- Fault Injection



Inbound features:

- Service authentication
- Authorization
- Rate limits
- Load shedding
- Telemetry
- Request Tracing
- Fault Injection

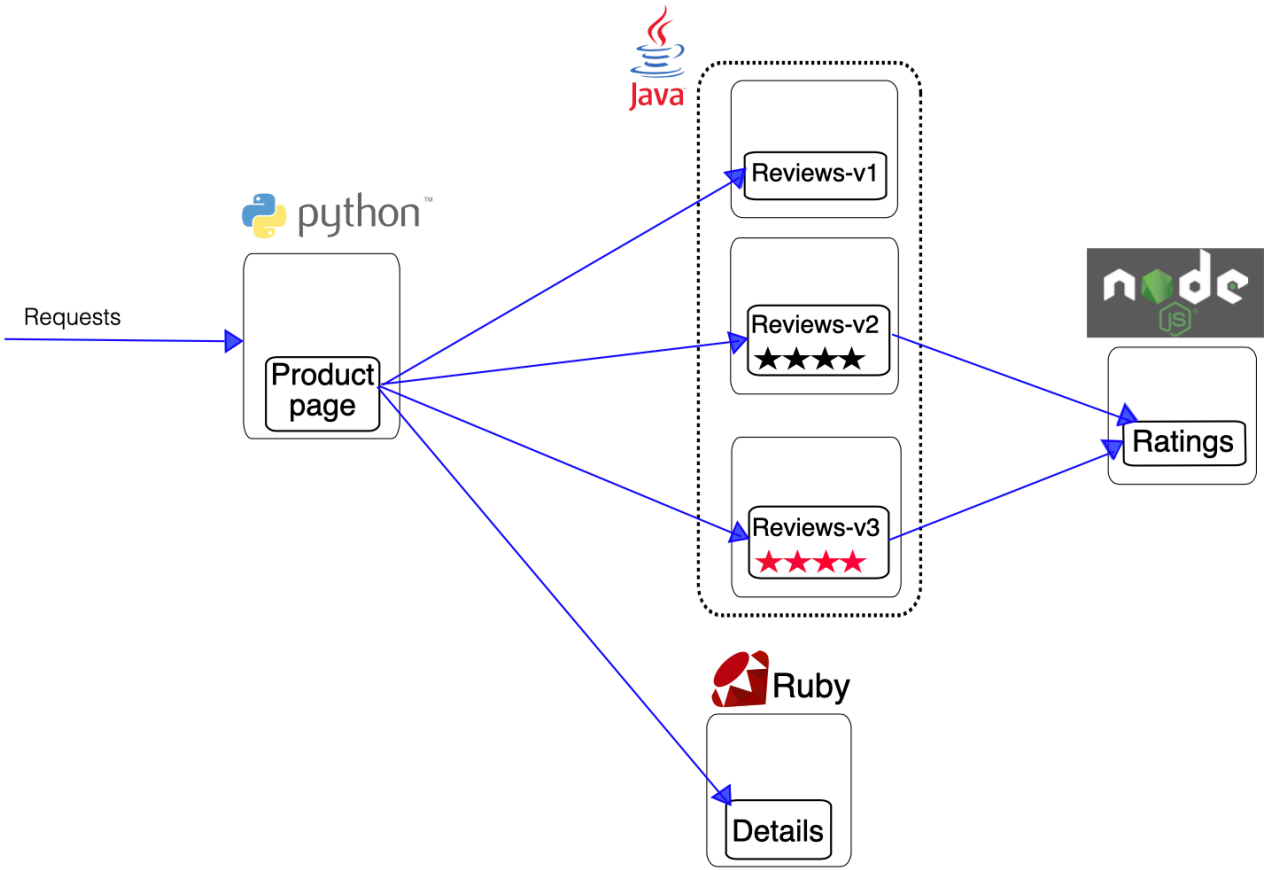
What is Envoy

- **Out of process architecture**: Let's do a lot of really hard stuff in one place and allow application developers to focus on business logic.
- **Modern C++11 code base**: Fast and productive.
- **L3/L4 filter architecture**: A TCP proxy at its core. Can be used for things other than HTTP (e.g., MongoDB, redis, stunnel replacement, TCP rate limiter, etc.).
- **HTTP L7 filter architecture**: Make it easy to plug in different functionality.
- **HTTP/2** first! (Including **gRPC** and a nifty gRPC HTTP/1.1 bridge).
- **Service discovery** and **active health checking.**
- **Advanced load balancing**: Retry, timeouts, circuit breaking, rate limiting, shadowing, etc.
- Best in class **observability**: stats, logging, and tracing.
- **Edge proxy**: routing and TLS.

Lyft's Envoy: From monolith to service mesh
Matt Klein, Software Engineer @Lyft

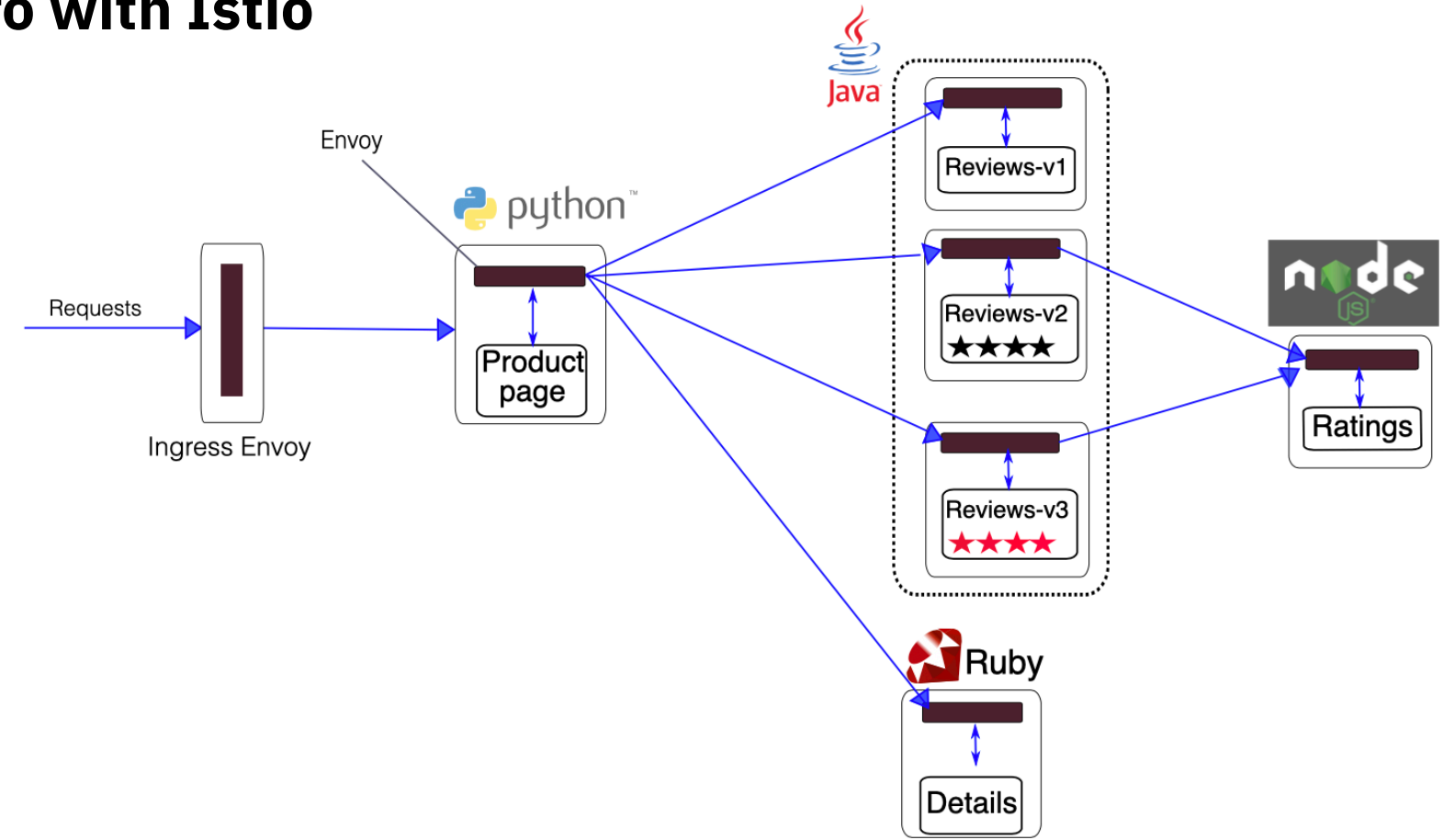
https://www.youtube.com/watch?v=RVZX4CwKhGE

Bookinfo



Bookinfo Application without Istio

Bookinfo with Istio



Bookinfo Application

Lab 1: follow steps here: http://ibm.biz/202010-istio-lab1