

CISCO *Live!*



#CiscoLive



The bridge to possible

# Your Mess Needs a Mesh

Shannon McFarland – CCIE#5245  
Distinguished Engineer – ET&I  
@eyepv6  
DEVNET-2450

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2450>



# Agenda

- The Service Mess
- What is a Service Mesh and why do I want one?
- A Service Mesh Example - Istio
  - How do I get it?
  - Contributing to Istio
- Cisco Calisti - <https://calisti.app/>

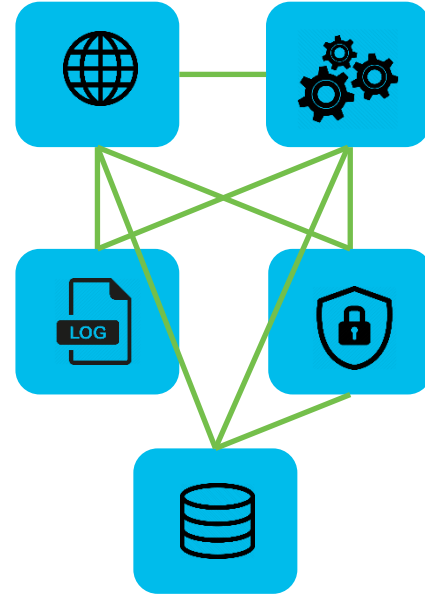
# The Service Mess



# What's a Microservice?



Monolithic Application

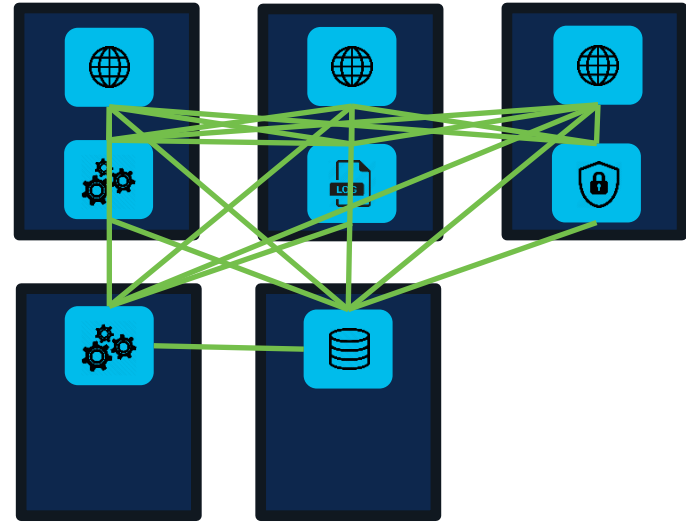


Microservice Application

# Scaling a Microservice Application



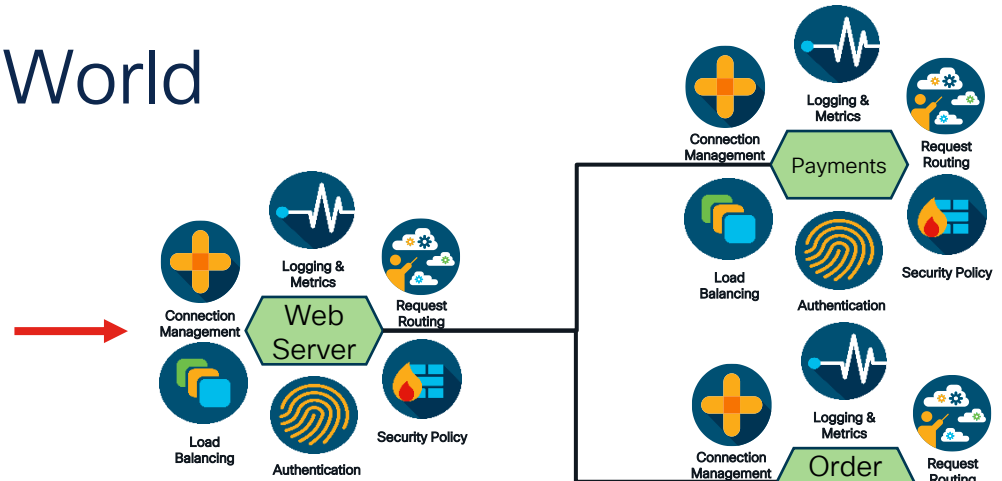
Monolithic Application



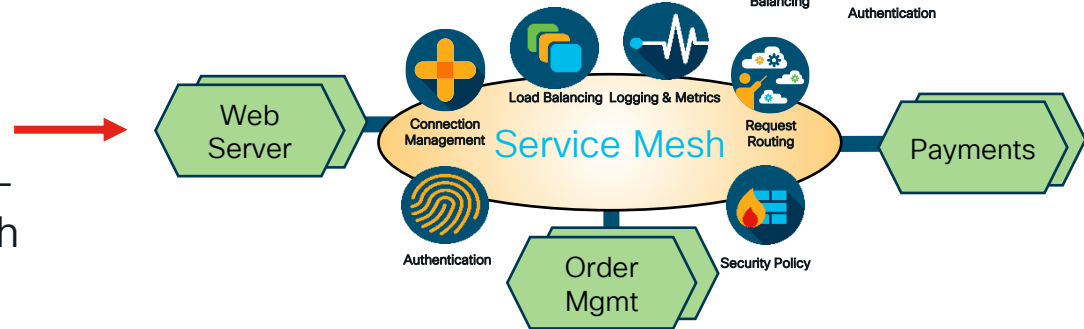
Microservice Application

# Service Features in a Microservice World

- Deploy all the service features as independent components



- Offload features for service-to-service communication to a policy-driven secure service mesh





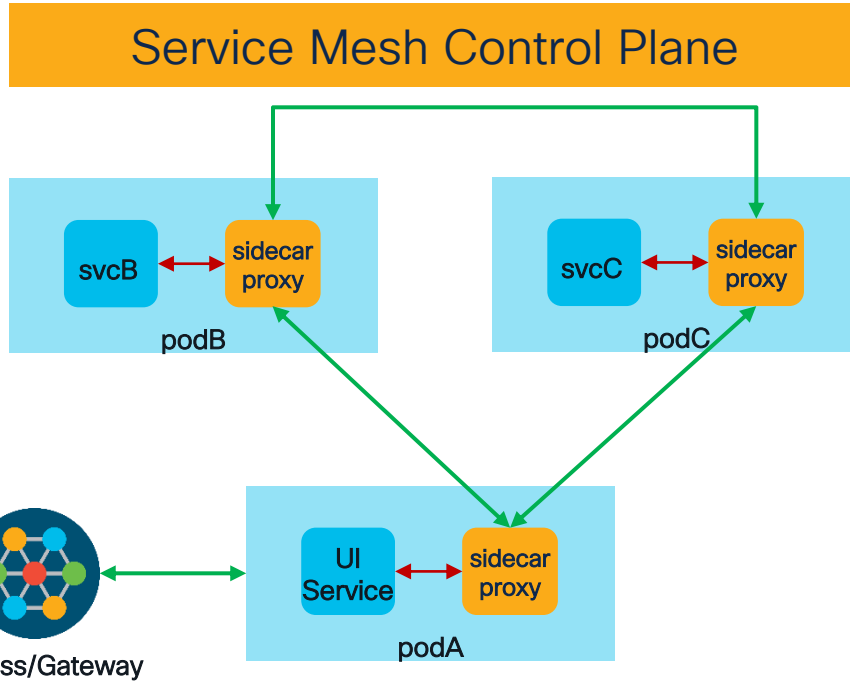
# My Application Service Requirements

- I want to deploy a microservice
- I want to deploy using Kubernetes
- I have a bunch of requirements such as the need to handle:
  - Service failures
  - Retries
  - Circuit breaking
  - Topology changes
  - Monitoring
  - Tracing
  - Encryption between services
  - and more

# What is a Service Mesh?



# What is a Service Mesh?



- Infrastructure layer for service-to-service communication
- Can use a mesh of sidecar proxies:
  - Can inspect API transactions at Layer 7 and 4 (TCP)
  - Intelligent routing rules can be applied between endpoints

# Service Mesh Options

There are many

- Application Service Meshes (L4/7)
  - <https://linkerd.io/> (CNCF)
  - <https://istio.io/>
  - <https://www.hashicorp.com/products/consul/service-mesh>
  - and others...
- Network Service Mesh (L2/3)
  - <https://networkservicemesh.io/>
- Service proxies, API gateways, etc... (A search engine is your friend)

# Service Mesh Example - Istio



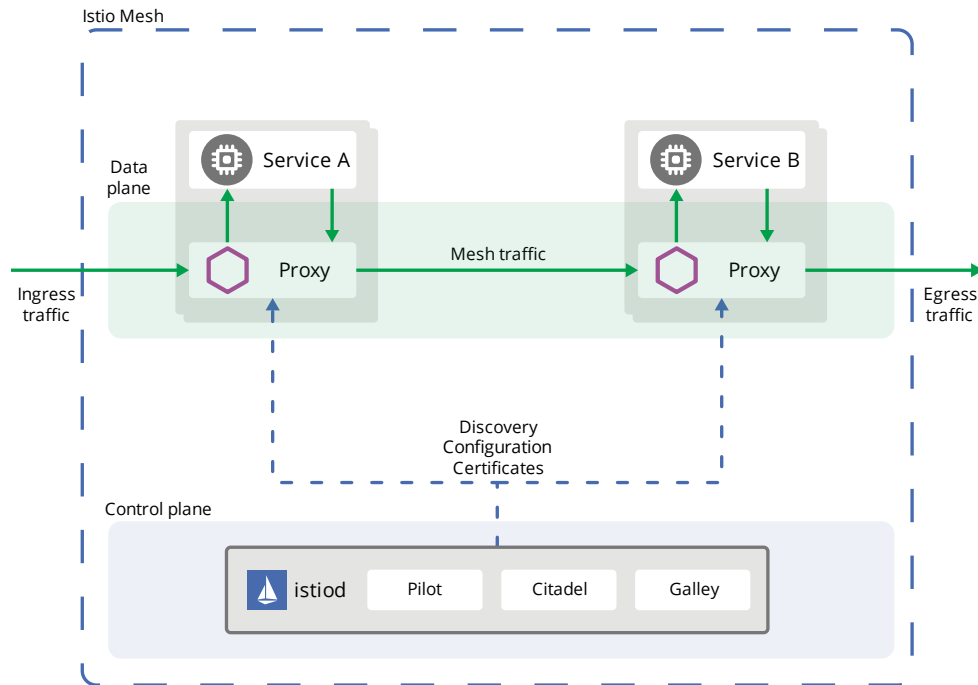
# Istio Overview

- An open-source project started by Google and IBM with help from the Envoy team at Lyft
  - <https://istio.io/>
  - <https://github.com/istio>
  - <https://www.envoyproxy.io/>
- <https://istio.io/docs/concepts/what-is-istio/>
  - Automatic load balancing for HTTP, gRPC, WebSocket, and TCP traffic
  - Fine-grained control of traffic behavior with rich routing rules, retries, failovers, and fault injection
  - A pluggable policy layer and configuration API supporting access controls, rate limits and quotas
  - Automatic metrics, logs, and traces for all traffic within a cluster, including cluster ingress and egress
  - Secure service-to-service authentication with strong identity assertions between services in a cluster

# Istio Architecture

<https://istio.io/latest/docs/ops/deployment/architecture/>

- **istiod**
  - **Pilot**
    - Handles service discovery and config data
    - Provides the Envoy proxies with the mesh topology and route rules
  - **Galley**
    - Validates user authored Istio API configuration on behalf of other control plane components
    - Top-level config ingestion, processing and distribution
  - **Citadel**
    - Provides certificates to the Envoy proxies for authentication and authorization
- **Envoy**
  - A proxy attached to every microservice
  - The connection point for a microservice to attach to the mesh

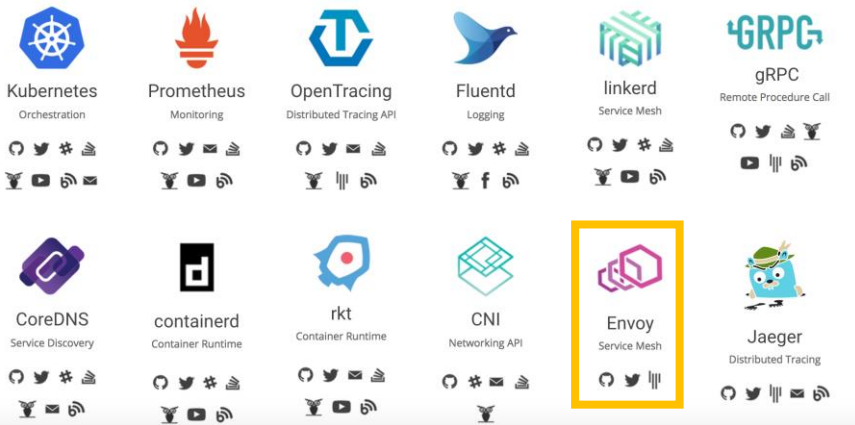


# Envoy

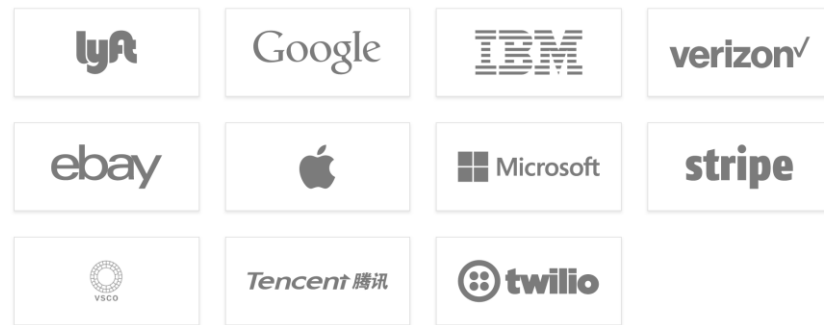
<https://www.envoyproxy.io>

- Implemented by Lyft
- A C++ based L4/L7 proxy
- Can be used independently of any service mesh (Istio)
- API driven
- Traffic routing and splitting
- Transparent proxying
- Health checks, circuit breakers, etc.

## Currently Hosted Projects



## USED BY



<https://github.com/envoyproxy/envoy>



# Istio: How Do I Get It?

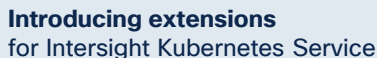
- Where to get it:
  - Istio currently is available directly from the Istio community at: <https://istio.io/about/community/join/>
  - It can also be built directly: <https://github.com/istio/istio>
  - It can be enabled as an infrastructure option in GKE
- How to install it (Kubernetes):
  - <https://istio.io/docs/setup/getting-started/>
  - Kubernetes installation is a prerequisite
  - Directly from the manifests included in the release
  - Using Helm charts included in the release

# Contribution

- Contribution Readme: <https://github.com/istio/community/blob/master/CONTRIBUTING.md>
- Contributing to the Docs: <https://istio.io/about/contribute/>
- Istio Discussion: <https://discuss.istio.io/>

# Cisco Calisti – A Service Mesh Manager

<https://calisti.app/>



## Complete application and health observability

## Security at all layers between clusters and clouds

## Multi-cloud, multi-cluster connectivity and observability

## Connect any on-prem and public cloud together

Simplifies service mesh management  
Single pane of glass, in depth metrics

## Policy-based app networking & security

# Cisco SMM Benefits

1

## Multi-Cluster Observability

- ✓ Proactive issue resolution using SLO<sup>1</sup>, error budgeting, actionable alerting when SLO's are endangered
- ✓ Faster root cause resolution using timeline view, outlier detection, traffic tapping/tracing
- ✓ Better visibility into service-to-service performance through Traffic Analytics

2

## Simplified mesh & traffic management

- ✓ Complete Istio lifecycle mgmt.
- ✓ Ensure High Availability via automated tooling, metrics
- ✓ Rich, comprehensive operations focused dashboard
- ✓ Enterprise-grade security hardening & lifecycle
- ✓ Reduced risk of day 2 deployments via canary upgrades
- ✓ Reduce human error via config validation
- ✓ VM-extensions for brownfield and external service linkage

3

## Policy based n/w & Security

- ✓ Simplified application deployment via security, observability and platform traffic management
- ✓ Respond quickly to security vulnerabilities via policy enforcement
- ✓ Avoid issues via canary deployments, circuit breakers
- ✓ DevOps friendly traffic debugging

A decorative graphic in the top right corner consisting of a dense cluster of circles in various sizes and colors, including shades of blue, green, orange, red, and yellow. The circles are arranged in a way that they appear to be floating or expanding from the right edge of the frame.

# Demo Time!

# Cisco Calisti Multicluster Setup

<https://calisti.app/>

1) Install Cisco Calisti and identify the first cluster name:

```
# smm install -a --cluster-name smm-mc-1
```

2) Install Cisco Calisti with a full Istio control plane and attach the 2<sup>nd</sup> cluster to the 1<sup>st</sup> cluster:

```
# smm istio cluster attach smm-mc-2.yaml --active-istio-control-plane
```

3) Enable Istio sidecar injection on a namespace:

```
# smm sidecar-proxy auto-inject on default
```

```
# smm istio cluster status
```

Clusters

Name	Type	Provider	Regions	Version	Distribution	Status	Message
smm-mc-1	Local	amazon	[us-east-2]	v1.21.2-13+d2965f0db10712	EKS	Ready	
smm-mc-2	Peer	amazon	[us-east-2]	v1.21.2-13+d2965f0db10712	EKS	Ready	

ControlPlanes

Cluster	Name	Version	Trust Domain	Pods
smm-mc-1	cp-v111x.istio-system	1.11.4	[cluster.local]	[istiod-cp-v111x-75b7ccbb76-6szk9.istio-system]
smm-mc-2	cp-v111x.istio-system	1.11.4	[cluster.local]	[istiod-cp-v111x-6f5d85c56f-vw2k7.istio-system]

Proxies

smm-mc-1	cp-v111x.istio-system	1.11.4	[cluster.local]	[istiod-cp-v111x-75b7ccbb76-6szk9.istio-system]	32/32
smm-mc-2	cp-v111x.istio-system	1.11.4	[cluster.local]	[istiod-cp-v111x-6f5d85c56f-vw2k7.istio-system]	5/5

# It's About The Application... Not The Infrastructure

- Service Meshes provide injection of proxy sidecars along with each microservice
- Injection is secure and automatic
- Allows the application developer to focus on the application
- The proxy sidecar connects cleanly to the microservice without additional development and regardless of the language used by the microservice
- Off-loads the authentication, authorization, telemetry (logs, metrics, tracing etc.), and network connectivity responsibilities
- Provides uniformity in both policy enforcement and telemetry collection
- Check out Cisco Calisti – Get started for free (Up to 10 nodes and 2 clusters):  
<https://calisti.app/>



# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](https://www.cisco.com/go/certs)

Pay for Learning with  
Cisco Learning Credits

(CLCs) are prepaid training  
vouchers redeemed directly  
with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams  
and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology,  
and certification training

### Cisco Modeling Labs

Network simulation platform for design,  
testing, and troubleshooting

### Cisco Learning Network

Resource community portal for  
certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation  
and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting  
Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product,  
technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification  
program empowers students  
and IT Professionals to advance  
their technical careers

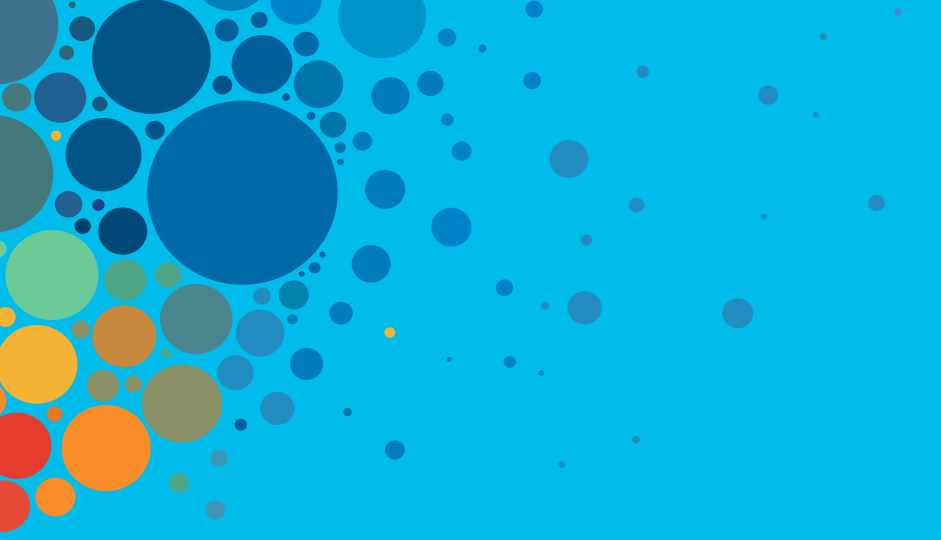
### Cisco Guided Study Groups

180-day certification prep program  
with learning and support

### Cisco Continuing Education Program

Recertification training options  
for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*



#CiscoLive