Istio Service Mesh Improvement

Lin Sun
Senior Technical Staff Member, IBM

@linsun_unc
What exactly is service mesh?
A Service Mesh is...

- Language neutral
- Dummy initialization
- Visibility
- Smart attachment to your service
What is Istio?

- An **open** service mesh platform
- Provides **standard attachment** to your application container
- Provides user interfaces to configure policies for the attachment, **without redeploying** your application
- Enables **clear separation** from the application (Dev) and attachment (Ops)
Deploy pods and services to the mesh

`istioctl kube-inject`

`kubectl label namespace {namespace} istio-injection=enabled`

https://istio.io/docs/setup/kubernetes/additional-setup/sidecar-injection/
Deploy pods and services to the mesh

- Add named service port for each service port
- Declare containerPort configuration for each pod port
- Pod must have a service associated
- Label deployments with app and version
- Don’t use UID 1337
- Do you have NET_ADMIN privilege?

https://istio.io/docs/setup/kubernetes/prepare/requirements/
Updates on 1.1 - Defaults

- Outbound traffic is open by default
- Mixer policy check is disabled by default.
- Istio ingress is removed
- Servicegraph is deprecated in favor of Kiali
- Envoy Access logs are disabled by default
- Control plane monitoring port change from 9093 to 15014
- Built-in Istio StatsD collector has been removed
Updates on 1.1 - Install

- Multiple install profiles are available. Choose one to start with.
- Check if your cluster has sufficient resource: default control plane and sidecar cpu and memory request have increased.
- Istio-init chart is available in addition to the istio chart
- Istio-remote chart is consolidated into the istio chart as an install profile
- Many installation options changed
Updates on 1.1 - Telemetry & Policy

- Kiali - enabled by default in the demo profile
- You can bring in your own StatsD collector
- Various tracing and performance improvement
- Addons no longer exposed by default
Updates on 1.1 - Network

- Consumer: New Sidecar Resource
- Producer: Restrict Visibility of Services
- Namespace scoping
- ServiceEntry resource simplification
- Locality-Aware Routing
- Single Control Plane Multicluster and Multiple Control Plane Multicluster

---

New namespace isolation in the ‘Sidecar’ resource in @IstioMesh 1.1.0 taking the RAM cost of istio on one of our clusters down from 43gb to 17gb. Not to mention reducing CPU cycles on pilot by 90%, yes, 90. Great work folks.
Updates on 1.1 - Security

- Improved support for readiness and liveness probes
- Cluster RBAC Config
- Alpha SDS support for identity provision
- External cert for ingress gateway
- Customized trust domain
Updates on 1.1 - Galley

- Pilot now subscribes to Istio resources info from Galley
- Galley uses validation web hook to validate Istio resources

```bash
$ k apply -f bookinfo-gateway.yaml
virtualservice.networking.istio.io/bookinfo unchanged
Error from server: error when creating "bookinfo-gateway.yaml": admission webhook "pilot.validation.istio.io" denied the request: configuration is invalid: port name must be set: number:80 protocol:"HTTP"
```
Updates on 1.1 - istioctl

Lin Sun @linsun_unc · Mar 10
I can save my fingers from typing extensively now with @IstioMesh for gateway, virtual service, destination rule and service entry now 🎉

Lin Sun @linsun_unc · Feb 21
Need to validate your @IstioMesh install, try the new Istioctl experimental verify-install cmd!

```bash
$ istioctl validate -f bookinfo-gateway.yaml
Error: 1 error occurred:
* error validating resource (networking.istio.io/v1alpha3, Kind=Gateway Name=bookinfo-gateway Namespace=): port name must be set: number:80 protocol:"HTTP"
```
Istio 1.2

• Major Theme: Predictable Release
• Released in June 2019
• Code Mauve
• Promote existing alpha features to beta, beta feature to stable
• Various Usability improvements
  – containerPort annotation
  – Istioctl simplification
Istio Themes

• Project Sustainability
• Layering & Extensibility
• Improved Experience
• Performance & Scalability
Layering And Extensibility

- Mixer v1 will go away
- Extensibility v2
- Envoy WASM support
- Improve Performance and Scalability
Improved Experience

• New installer
  – Roll out to demo profile first
• Istio Operator
• Better mTLS rollout
• Continued Multi-Cluster improvement
• Basic Mesh Federation patterns
How are you using Istio or service mesh today?
What is your pain point with Istio/service mesh?
How to contribute?

- Gain membership Status
- Contributor Get Started in istio/community repo
- Existing contributors list and approver list
- Gain approver/lead status
- Attend Meetings or Contribute to WG discussions via email or slack
What is good in the community?

- Be respectful
- Be proactive
- Don’t sign up things but not do it
- Provide active updates on GitHub
- Gain respect through work and help others
What is bad in the community?

- Ask people to do things then disappear
- Show intention to work on WIs then never do it
- Ask questions that others can find answers within a few minutes via google search
- Not provide feedback: positive or negative
- Comment here and there but not get concrete work done.