JUMP TO (#)

What is Istio?

Istio is a service mesh—a modernized service networking layer that provides a transparent and language-independent way to flexibly and easily automate application network functions. It is a popular solution for managing the different microservices that make up a cloud-native application. Istio service mesh also supports how those microservices communicate and share data with one another.

As organizations accelerate their moves to the cloud, they are, by necessity, modernizing their applications as well. But shifting from monolithic legacy apps to cloud-native ones can raise challenges for DevOps teams.

Developers must learn to assemble apps using loosely coupled microservices to ensure portability in the cloud. At the same time, ops teams must manage the new cloud-native apps within increasingly large hybrid and multi-cloud environments. Istio allows them to do this.

Istio defined

> **Istio is an open source service mesh that helps organizations run distributed, microservices-based apps anywhere. Why use Istio? Istio enables organizations to secure, connect, and monitor microservices, so they can modernize their enterprise apps more swiftly and securely.**

Istio manages traffic flows between services, enforces access policies, and aggregates telemetry data, all without requiring changes to application code. Istio eases deployment complexity by transparently layering onto existing distributed applications.

What are Istio service mesh benefits?

Achieve consistent service networking

Your networking operators can consistently manage networking for all of their services without adding developer overhead.

JUMP TO (#)

Your security operators can easily implement service-to-service security including authentication, authorization, and encryption.

Improve your application performance

Implement best practices, like canary rollouts, and get deep visibility into your applications to identify where to focus your efforts to improve performance.

How do Istio, Envoy, and Kubernetes work together?

The key to understanding Istio and the Istio architecture is to know about both Envoy and Kubernetes. It's not a question of Istio versus Envoy or Istio versus Kubernetes—they often work together to make a microservices-based containerized environment operate smoothly.

For example, service meshes like Istio are made up of both a control plane and a data plane. Istio uses an extended version of Envoy as its data plane. Envoy then manages all inbound and outbound traffic in the Istio service mesh.

Kubernetes, on the other hand, is an open source platform that gets rid of many of the manual processes involved in deploying and scaling containerized applications by automating and orchestrating them. And, although Istio is platform independent, using Istio and Kubernetes together is popular among developers.

Istio is platform-independent and designed to run in a variety of environments:

- Cloud
- On-premises
- Kubernetes
- Mesos

What is Istio used for?

Istio allows organizations to deliver distributed applications at scale. It simplifies service-to-service network operations like traffic management, authorization, and encryption, as well as auditing and observability. Here are some of the most common use cases that deliver the benefits of Istio:

JUMP TO (#)

Focus on security at the application level with strong identity-based authentication, authorization, and encryption.

Manage traffic effectively

Get fine-grained control of traffic behavior with rich routing rules, retries, failovers, and fault injection.

Monitor service mesh

Gain deep understanding of how service performance impacts matters upstream with the robust tracing, monitoring, and logging features of Istio.

Easily deploy with Kubernetes and virtual machines

Istio provides visibility and network controls for both traditional and modern workloads including containers and virtual machines.

Simplify load balancing with advanced features

Use automated load balancing for all of your traffic, along with advanced features like client-based routing and canary rollouts.

Enforce policies

Enforce policies with a pluggable policy layer and configuration API that supports access controls, rate limits, and quotas.

Related products and services

Anthos Service Mesh (https://cloud.google.com/anthos/service-mesh) brings you Google's years of experience building and delivering services at scale. It enables you to adopt site reliability engineering (SRE) and zero trust best practices to deliver quality services quickly and at scale without compromising security. When using Anthos, you can consistently manage service networking anywhere you require.

JUMP TO (#)

Anthos Service Mesh

The fully managed service mesh for your complex microservices architectures.

(https://cloud.google.com/anthos/service-mesh)

SOLUTION

Application modernization

Google Cloud's application modernization platform lets you develop and run applications anywhere, using cloud-native technologies.

(https://cloud.google.com/solutions/application-modernization)

Take the next step

Start your next project, explore interactive tutorials, and manage your account.

Go to console (https://console.cloud.google.com/)

Need help getting started?

Contact sales (https://cloud.google.com/contact/)

Work with a trusted partner

Find a partner (https://cloud.withgoogle.com/partners/)

Get tips & best practices

See tutorials (https://cloud.google.com/docs/tutorials/)

JUMP TO (#)