5 stages to Istio production success

Design and implement a fully operational Istio service mesh using open-source best practices alongside industry recognized cloud native solutions for advanced security.

Venafi tetrate

About this guide

Istio is a popular service mesh that can help companies to improve the security, reliability, and observability of their microservices. Venafi and Tetrate have come together to produce this technical guide which provides advice and recommendations on how to deploy Istio for production success.

The guide covers the most important aspects of Istio deployment, from installing the Istio control plane to configuring Istio for different use cases and it is created for both experienced and inexperienced Istio users. It is a valuable resource for anyone who wants to successfully deploy Istio in their organization.

"Istio is a powerful platform with the tools organizations need at the center of their security, networking and observability strategies. Istio's CNCF graduation is a significant turning point in the project's journey: recognition of Istio's maturity, stability and widespread adoption within the cloud-native community. With its innovative approach to managing service-to-service communication, Istio has proven its value in real-world deployments and engaged a world-wide user base."

Zack Butcher, Founding and Principal Engineer at Tetrate

Contents

Introduction to Istio

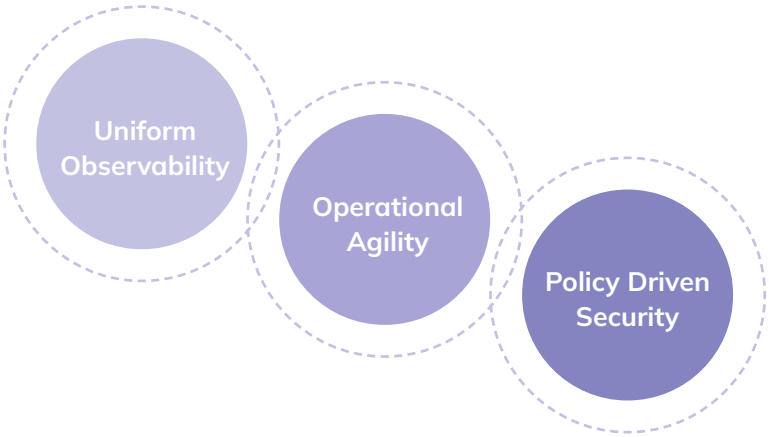
Istio is highly valued by many businesses because it offers a wide range of advanced development, operations, and security features. It effectively addresses various challenges that arise when running large-scale polyglot and distributed applications. Service meshes, which sit on top of Kubernetes, provide a powerful way to handle common issues in running distributed applications for production. Istio stands out as one of the top service mesh implementations, offering extensive features for workload security, network traffic management, and application behavior monitoring.

"When adopting Istio it is important to start with a firm set of objectives that will bring value to your Kubernetes operation, which will enhance the work of both the security teams and the platform engineering teams. Driving adoption to the benefit of both these teams will help ensure you can achieve Istio production success"

Matt Barker, Global Head of Cloud Native Services at Venafi

Why use a service mesh?

In a cloud-native Kubernetes environment, a service mesh acts as a dedicated infrastructure layer that centralizes various concerns related to communication between services across the network. It offers a seamless and language-independent platform, making it simple and adaptable to automate application workload functions. Importantly, it enables clear separation of policies between application stacks and network stacks. This demarcation enhances security and facilitates efficient governance.



Istio is based around three key principles: ensuring consistent observability, enhancing operational flexibility, and implementing security through policy-driven approaches.

Istio architecture

The Istio architecture can be broadly understood as consisting of two main components: the control plane and the data plane.

The control plane handles configuration-related tasks, such as defining traffic routing rules and network policies. These configurations are then distributed to the data plane, specifically to the proxies. Additionally, Istio enables service-to-service authentication and authorization by issuing TLS certificates to the workloads within the mesh.

In the data plane, Envoy proxies are injected as high-performance and programmable container instances into Kubernetes Pods. This follows the “sidecar” pattern, where each workload is accompanied by a proxy. The proxy containers intercept all incoming and outgoing network traffic, serving as a point for enforcing policies. Since the Envoy proxies operate at Layer 7, they can enforce traffic routing configurations based on attributes like HTTP headers or apply authorization policies to direct traffic to specific back-end services.

Istio security principles

The Istio security model is built around 3 principle factors.

The first is strong workload identities driven by powerful policy enforcement, and transparent mTLS encryption which is essential for authentication and authorisation. These are abstracted away from application workloads, meaning there are no changes required to business logic or the underlying infrastructure.

Second, defence-in-depth allows for Istio policies to be layered with existing security systems which further strengthens the security of the mesh and communications outside of the network perimeter.

Thirdly, the service mesh is able to implement and adhere the primary Zero Trust principles of user and application authentication, device or machine authentication, and trust. This is facilitated by having a root trust enabling transparent TLS, as well as secure identity management, certificate issuance and rotation.

mTLS for transparent service to service encryption

Mutual TLS (mTLS) is a mechanism for authentication between two parties using public-key certificates. It enables bi-directional encryption of traffic and provides transparent service to service encryption.

In Istio's case, identity management using mTLS is provided using the SPIFFE format as well as automating key and certificate generation, distribution and rotation. In contrast to end-user authentication where only the server certificate is used to establish authentication, in service to service authentication the client and server must use the X.509 certificates in order to establish proof of both identities.

There are essentially 2 options when looking to adopt Istio as a service mesh which depend on the application requirements. Permissive uses a combination of mTLS encrypted and unencrypted traffic between services which can be useful for supporting legacy services that are not yet migrated to Istio, and enable access for legacy clients which reside outside of the mesh. By comparison, the strict mTLS option enforces traffic encryption between all services as well as control plane components by default.

Kubernetes certificate management

Certificate management is a key enabler of the service mesh model and is responsible for X.509 certificate issuance and lifecycle management. It facilitates identity in the mesh and is the critical framework for establishing trust. It provides the means for transparent adoption as well as automation and rotation at scale.

Within a single “island” mesh, this works well for service to service communication, however this model will not work well for infrastructure that requires inter-mesh communication. To support service to service communication between meshes the trust solution must support a different set of identities from another mesh environment.

This requires the Istio CA to extend support for communication using intermediate certificates so clusters from each mesh have a root CA “out-of-cluster” which CAs from each mesh implicitly trusts. In reality for the enterprise, the model to support cross-cluster multi-mesh trust should be bootstrapped using certificates from a preferred private issuer. This is a common requirement for modern enterprise environments.

A real-world challenge with certificate management when using Istio is how to integrate with existing enterprise PKI solutions and ensure certificates are rooted in the enterprise chain of trust. For the majority of enterprises the open source cert-manager project is the preferred solution to meet this requirement.

Stage 1

Create a single tenant Istio service mesh using cert-manager for Ingress machine identity management

Mutual Transport Layer Security (mTLS) is a critical Kubernetes security aspect that is often the main reason for creating an Istio service mesh. To ensure mTLS between pods and automate the issuance and renewal of X.509 certificates for Istio sidecar proxies, a single-tenant vanilla Istio deployment should be created to facilitate an automated process for enforcing mTLS between pods within Istio.

By default, the Istiod control plane component provides the root machine identity Issuer or Certificate Authority (CA) for the Istio mesh, which means it issues and manages the certificates for the sidecar proxies in the mesh.

When it comes to Ingress traffic, the certificates are typically issued using cert-manager. cert-manager is very likely already established within the organisation to automate TLS encryption for Ingress traffic using public CAs. By relying on cert-manager's well-established integration with popular Issuers or Certificate Authorities (CAs), Istio can be configured to use cert-manager to issue and rotate Ingress certificates.

Use Tetrate Istio Distro to:

- Deploy a basic Istio environment to a single cluster
- Establish 1st principles using mutual authentication for mesh workloads
- Secure pod-to-pod traffic in the cluster using Istiod for mTLS authentication

Use cert-manager to:

- Automatically issue and manage certificates for ingress traffic in Istio

Stage 2

Extend Istio service mesh for seamless inter-service with mTLS

Istio should now be used with open source cert-manager for certificate generation and renewal for Istio sidecar proxies. cert-manager's task is to now automate and enforce mTLS between pods residing in Istio. In this sense cert-manager becomes the default machine identity solution by managing certificates for both public facing and internal, pod to pod mesh workloads.

cert-manager fulfils this task by using its istio-csr component to replace Istio's default capability for self-signed certificates. istio-csr is an agent that enables Istio workload and control plane components to be secured using cert-manager. This enhances the Istio solution by providing dynamic machine identity provisioning using the enterprise root Issuer for private certificates. This hardens overall security for the mesh solution and will allow policy-based certificate management as a next step.

Using cert-manager means developer teams will not have to change their current deployment process, so developer automation and tooling remain consistent and unaffected by the need to introduce the Istio solution.

Use cert-manager to:

- Enforce mTLS throughout the mesh to invoke the istio-csr agent for automated certificate signing
- Ensure the mesh identities are anchored to the enterprise root Issuer for private certificates

Use Venafi TLS Protect for Kubernetes to:

- Monitor multi-cluster cert-manager configurations
- Ensure version consistency for cert-manager across clusters
- Enforce security policy compliance for mesh workloads

Stage 3

Use identity and policy-based authorization controls for inter-service traffic flows

In a constantly scaling and ephemeral mesh environment, authenticated and trusted machine identities are crucial for validating the identity of mesh workloads. This protects the security of the mesh environment and the workloads running within it. If the machine identity is not authenticated or trusted, the workload will not be able to access other workloads in the mesh environment.

Istio authorization should be deployed for dynamic workload-to-workload, and end-user-to-workload access control enforcement. The highly ephemeral nature of application workloads deployed in a mesh environment while being constantly scaled up and down requires mesh identities to be observed and proactively validated using trusted private Issuers or CAs.

Intermediate or subordinate CAs are often used in a service mesh alongside root CAs. However, managing the lifecycle of intermediate CAs can be complex, especially when deploying Istio across multiple clusters. Security teams need access to tooling that extends their existing policy-driven security controls to seamlessly operate in Istio service mesh environments.

Use Venafi TLS Protect for Kubernetes to:

- Monitor machine identity activity across the mesh
- Manage certificate activity for security audit
- Enforce security policies for intermediate CAs
- Enforce Infosec standard policies for certificate issuance

Use Tetrate Service Bridge to:

- Deploy Istio authorization policies to define the rules that govern access to services in the mesh

Stage 4

Multi cluster service mesh observability, security and scalability.

Having a detailed view of machine identities and how they relate to mesh traffic routing within a mesh is important. Before the production phase can begin, security teams need to enforce the highest standards for signing private machine identities for mesh workloads. Scalability must be built into the Istio solution with workload-level visibility and metrics across traffic patterns.

The volume of machine identities will scale quickly once the mesh is deployed to production so security teams need solutions for machine identity issuance at scale along with options for automated key rotation and audit logging. This will allow developer teams to maintain very high levels of workload automation, whilst allowing security teams to sustain an enterprise-wide strong security posture.

It is important to consider the impact of application release velocity and lifecycle management across multiple clusters, which can be a complicated task with increased levels of interconnectivity. Canary deployment enables gradual version release, routing a portion of traffic to the new version. Blue/Green deployment tests new versions in a separate environment whilst retaining a production-like setup. Traffic shaping controls offer reliability-enhancing features like rate limiting, circuit breaking, and fault injection. These techniques optimize deployment, testing and traffic control in Istio service mesh environments.

Use Venafi Firefly to:

- Keep confidential PKI key material safe
- Simplify setup of multi-cluster Istio

Use Tetrate Service Bridge to:

- Build a detailed view of mesh traffic patterns
- Provide advanced traffic management capabilities for routing and load balancing
- Improve overall centralized monitoring and logging

Stage 5

Multi-cloud production Istio using trust domains with SPIFFE machine identities

Advanced security policies using SPIFFE machine identities can be critical to achieving a hardened security posture. SPIFFE (Secure Production Identity Framework For Everyone) is an open standard for securely identifying services in dynamic and distributed environments. It integrates with cert-manager to provide fully observable, advanced identity-driven secure communication for workloads.

Governance for the full mesh environment can bring additional challenges around how trust is distributed so having access to proven specific design patterns to build trust domains will help achieve the desired level of traffic management and security.

In Istio, a SPIFFE trust domain is a logical boundary within which workload instances are assigned unique identities. The trust domain provides a secure boundary for communication between workloads within the same domain and enables secure communication between workloads in different trust domains.

The service mesh can be configured to require that all services use SPIFFE machine identities. This ensures that only authorized services can communicate with each other with all communication encrypted and mutually authenticated. This allows security teams to enforce true cloud native policy and ensure a validated and observable root of trust exists for every workload.

Use Venafi TLS Protect for Kubernetes to:

- Build advanced identity-driven workload security using trust domains
- Operate cert-manager at scale
- Enforce security policies using SPIFFE IDs

Use Tetrate Service Bridge to:

- Operate Istio across multi-cloud and hybrid-cloud infrastructure

Solutions from Venafi for Istio production success

Venafi

cert-manager is a powerful open source machine identity management tool that automates the issuance, renewal, and rotation of TLS and mutual TLS certificates for workloads running in Kubernetes. It can be used to secure Istio workloads by issuing machine identities to Istio proxies and gateways. Venafi is the original inventor of the cert-manager project which is now maintained by the Cloud Native Computing Foundation (CNCF). https://cert-manager.io/

Venafi TLS Protect for Kubernetes is a cloud native machine identity solution and provides important security capabilities for Istio deployments. It enhances the security and management of TLS certificates within the Istio service mesh running on Kubernetes. TLS Protect for Kubernetes automates the issuance, rotation, and lifecycle management of certificates, ensuring secure communication between Istio workloads while simplifying certificate management tasks for security and operations teams. It integrates seamlessly with Kubernetes-native workflows, improving the overall security posture and operational efficiency of Istio deployments.
https://venafi.com/tls-protect-for-kubernetes/

Firefly is a lightweight, high velocity machine identity issuer from Venafi which provides enhanced security when used with Istio. It enforces secure and trusted communication within the Istio service mesh by only allowing approved Certificate Authorities to issue machine identities for istio workloads. Firefly enables security and architecture teams to enforce policies for strengthened security and compliance.
https://venafi.com/firefly/

Solutions from Tetrate for Istio production success

Tetrate Istio Distro (TID) is a 100% upstream distribution of Istio from Tetrate. It offers several advantages such as simplified installation, management, and operation of Istio in production environments. It provides additional features and enhancements, including multi-cluster support, improved observability, security enhancements, and enterprise support, making it an ideal choice for organizations looking to leverage the benefits of Istio in a scalable and reliable manner.
https://istio.tetratelabs.io/

Tetrate Service Bridge (TSB) is an application connectivity and security platform that enables secure and reliable communication between applications across multiple clouds and environments. It provides a unified and managed service mesh infrastructure, simplifying connectivity and governance for microservices. Its advantages include centralized observability, fine-grained traffic control, seamless cross-cluster communication, and enhanced security through auditable mutual TLS encryption and access controls, making it easier for organizations to build and manage resilient and scalable distributed systems.
https://tetrate.io/tetrate-service-bridge/

Dedicated field support and consulting for Istio

Venafi's cloud native consulting is built around expertise from Jetstack Consult, Venafi's dedicated team of experts providing cloud native consulting and technology services which specializes in high scale Istio service mesh deployments. This team has a proven and exemplary track record working alongside platform engineering and security teams to help them successfully deploy Istio service mesh solutions.

- **Planning and design:** Proper planning and design are crucial before deploying Istio. Jetstack Consult helps companies assess their application architecture, identify the services to be secured in the mesh, and plan the traffic routing, security policies, and observability requirements.
- **Infrastructure preparation:** Companies often require help to ensure their infrastructure meets the prerequisites for Istio deployment which is essential to mitigate unforeseen complexities that can arise further into the program.
- **Adoption strategy:** Jetstack Consult helps to define and validate this crucial initial deployment stage before expanding Istio's usage across the entire application landscape, ensuring a smoother transition and mitigating potential risks.
- **Monitoring and troubleshooting:** Setting up comprehensive monitoring and troubleshooting capabilities is essential for successful Istio deployment.

To find out more about Venafi Jetstack Consult visit www.venafi.com/jetstack-consult/

Venafi is the cybersecurity market leader in identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. To learn more, visit www.venafi.com

Rooted in open source, Tetrate was founded to solve the application networking and security challenges created by modern computing so enterprises can innovate with speed and safety in hybrid and multi-cloud environments. As applications evolve into collections of decentralized microservices, monitoring and managing the network communications and security among those myriad services becomes challenging. This is why some of the largest financial institutions, governments and other enterprises rely on Tetrate to deliver modern application networking and security. Find out more at www.tetrate.io