VMware Tanzu Service Mesh

AT A GLANCE

Tanzu Service Mesh, an enterprise-class service mesh solution, provides consistent connectivity and *security for microservices* across all Kubernetes clusters and clouds in the most demanding multi-cluster and multi-cloud environments.

Tanzu Service Mesh delivers application connectivity, resiliency, and security capabilities that add value to enterprise initiatives focused on application modernization, multi-cloud, and data protection.

KEY BENEFITS

- High Availability & Automatic Failover: Deploy and manage distributed applications across multiple clusters and multiple clouds with high availability and automatic failover
- Self-Healing & Application Resiliency: Detect and report application intent violation and implement auto-scaling and traffic routing policies across multi-cloud environments for automated self-healing
- Context-aware Security: Improve security operations with consistent security policies and attribute-based access control for microservices

Business Challenges with Microservices

The modern application is dynamic and highly adaptive to changes in demand. It lives across multiple clusters and clouds. And it is highly distributed with hundreds of microservices servicing the requirements of rapid feature releases, high resiliency, and on-demand scalability.

Decomposing a monolithic application stack into dozens or hundreds of microservices results in a distributed system. Application and platform teams now need to manage different aspects of communication between many discrete services, including:

- Establishing and maintaining operational visibility into the state of the services
- Connecting, routing, load balancing, and securing communications across distributed microservices
- Reducing latency between services in the service chain—a bottle neck that can ripple across the entire application, affecting the user experience
- Troubleshooting and identifying the root cause of problems in an application composed of many different services that have been developed with different programming frameworks and databases

Given this reality, enterprises cannot afford to continue to rely solely on the network architectures of the last decade. Enterprises need a common, multi-dimensional application connectivity framework that provides availability, resiliency, and security for modern applications with the ability to abstract connectivity, identity, and policy via declarative intents.

What is Tanzu Service Mesh?

VMware Tanzu™ Service Mesh™, built on VMware NSX®, is an enterprise-class service mesh solution that provides consistent control and security for microservices, end users, and data—across all clusters and cloudsin the most demanding multi-cluster and multi-cloud environments.

Tanzu Service Mesh simplifies the management of services that comprise a distributed application. It provides a consistent way to connect and protect thousands or tens of thousands of individual microservices by providing connectivity, resiliency, and security capabilities to value-driven enterprise initiatives focused on application modernization, multi-cloud, and data protection.

Tanzu Service Mesh makes it easier to operate and integrate your workloads through a new level of abstraction in the form of a global namespace that allows enterprises to connect, manage, and secure applications across clouds and workloads. This provides full services and application mobility, giving enterprises the freedom to choose tenancy and placement architecture based on the services and organization requirements rather than on cluster and vendor boundaries.

BENEFITS OF TANZU SERVICE MESH

VMware Tanzu Service Mesh is an enterprise-class service mesh that:

- Extends the service mesh capability (discovery, identity, policy, traffic routing, and observability) to users, services, and data
- Facilitates the development and management of distributed applications across multiple clusters, multiple clouds, and in hybrid-cloud environments with *Global Namespaces*—supporting federation across organizational boundaries, technologies, and service meshes
- Implements consistent application-layer traffic management and security policies across all clusters and clouds.
- Integrates with VMware Tanzu™ Mission Control™, VMware® Tanzu Kubernetes Grid Integrated, and VMware Tanzu™ Kubernetes Grid™ to provide a seamless user experience
- Supports third-party Kubernetes clusters in multi-cloud environments

Tanzu Service Mesh allows enterprises to stretch application boundaries across clusters and clouds. The application instances within the global namespace can be either containers running on a Kubernetes platforms. Either way, the global namespace provides secure identity, service discovery, and observability for the application.

FIGURE 1: Tanzu Service Mesh Features and Capabilities.

Use Cases for Tanzu Service Mesh

- Application Continuity – Ensure application continuity with load balancer integrations to support multi-zone and multi-region high availability and disaster recovery
- Application Resiliency – Ensure application resiliency with automated autoscaling policies to deliver on Service-Level Objectives (SLO) for multi-cloud applications
- Application Security – Secure applications and data by defining attribute-based authorization policies for service-to-service access control

Key Features

- High Availability and Automatic Failover – Integrates with AWS Route 53 and NSX Advanced Load Balancer to provide multi-zone and multi-region high availability and disaster recovery for applications
- Service Autoscaling –Includes service autoscaling that provides application owners with a way to define a Service-level Indicator (SLI) or a threshold to auto-scale microservice
- Service-Level Objectives (SLOs) – Provides a way to configure SLOs to measure and monitor the performance and health of microservice-based applications
- Attribute-based Access Control Policies –Supports the ability to define rich ABAC authorization policies for service-to-service access, allowing operators to make intent-based decisions on whether to authorize, block, or quarantine access based on a Common Vulnerability Scoring System (CVSS) score above a predefined threshold

- Traffic Encryption Policy – Offers end-to-end Mutual Transport Layer Security (mTLS) encryption configured on a per-global namespace basis that encrypts all north-south and east-west traffic between services, allowing operators to selectively apply different modes such as encryption, no encryption to the traffic
- Broad Support for Kubernetes Clusters Running on Multi-cloud Environments – Provides consistent connectivity and security for microservices across all Kubernetes clusters in the most demanding multi-cloud environments, and can support Tanzu Kubernetes Grid (TKG) clusters, Tanzu Kubernetes Grid service on vSphere with Tanzu, and third-party CNCF-conformant Kubernetes clusters
- Tanzu Mission Control Integration – Works with VMware Tanzu Mission Control to centrally and consistently manage operate, and secure Kubernetes infrastructure and modern applications across multiple teams and clouds while installing and lifecycle managing Tanzu Service Mesh data plane components in managed clusters directly from within Tanzu Mission Control

Tanzu Service Mesh Key Concepts

Global Namespaces

Global namespace, a unique concept in Tanzu Service Mesh, defines an application boundary—connecting the resources and workloads that make up the application into one virtual unit for consistent traffic routing, connectivity, resiliency, and security for applications across multiple clusters and clouds. Each global namespace is an isolated domain that provides automatic service discovery and manages service identities within that global namespace.

Resource Groups

Resource group in Tanzu Service Mesh is a collection of cluster resources of a specific type that share specific characteristics. Resource groups help enforce policies and monitor the performance of resources in a single global namespace or across the entire organization. A resource group provides a set of filters or conditions for operators to retrieve and manage a specific subset of resources for their needs.

Services

A service in Tanzu Service Mesh is an abstract concept that encapsulates business logic executed in a distributed application. A service construct is made of service versions and service instances. Each service version maps to multiple service versions, and each service maps to multiple service instances. Unlike a service in Kubernetes which exposes an application running on a set of pods as a network service, a service in Tanzu Service Mesh can represent a business logic microservice. Also in Kubernetes, services can be mapped to any of the following types of workload controllers: Deployments, ReplicaSets, StatefulSets, DaemonSet, Jobs, and CronJob.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com