Security Measures in VMware Tanzu™ Mission Control™

Assurance through Technology and Practices

KEY HIGHLIGHTS OF SECURITY IN TANZU MISSION CONTROL

- TLS everywhere
- Identity and access management
- OAuth token-based authentication and authorization
- Encryption for data at rest
- Change control and configuration management
- Security incident reporting
- Vulnerability scanning and patch management

This paper presents an overview of the security measures implemented in VMware Tanzu Mission Control. It briefly describes how VMware approaches security for Tanzu Mission Control, the key mechanisms and processes VMware uses to manage information security as well as the shared responsibility model for providing security in a modern cloud computing environment.

Tanzu Mission Control is a software-as-a-service (SaaS) control plane that securely integrates with Kubernetes clusters to support a wide array of operations, including lifecycle management through Cluster API. To support these operations, Tanzu Mission Control installs a software agent on the Kubernetes cluster.

Tanzu Mission Control works with two key platforms: the VMware Cloud Services Platform, which authenticates users and controls access by organization, and Amazon Elastic Compute Cloud (Amazon EC2), which provides the infrastructure.

Driving Principles

The security of VMware Cloud Services is of the utmost importance. VMware balances the control pane's various security needs with a set of controls and management processes designed to mitigate risk and enhance Tanzu Mission Control. The controls and processes were created based on the following driving principles, which help establish rules and guidelines for security:

- Risk – Understand the threat landscape, build a solid platform, and leverage all decision makers when calculating risk in order to best manage it.
- Controls – Strike a balance between effectiveness and efficiency by implementing compensating controls appropriate for the associated risk.
- Security – Provide preventative and protective capabilities to ensure a secure service.

Security in Tanzu Mission Control

This section describes how security works in Tanzu Mission Control by looking at the agent, identity and access management, key management, and data storage.

Agent Security

When you attach a Kubernetes cluster to or create a cluster through Tanzu Mission Control, the control plane installs an agent in a namespace on the cluster. The agent lets you manage that cluster with centralized configurations and policies through the control plane. It uses only outbound HTTPS communications over port 443 to connect with Tanzu

Mission Control; it does not listen for new connections. Thus, there is no need to open a port on your firewall to receive inbound communications.

The agent includes several extensions that securely communicate with and implement changes requested by the control plane of Tanzu Mission Control and monitor the health of the Kubernetes cluster. Communications take place over HTTPS encrypted with TLS; there are no unencrypted communications in Tanzu Mission Control.

The agent is installed in a common namespace named `vmware-system-tmc` and runs as a set of native Kubernetes pods, deployments, and services. It requires Kubernetes cluster administrator privileges because it must be able to both automatically install the extensions with a YAML file from Tanzu Mission Control and perform various management functions. The most privileged extensions run as a Kubernetes cluster administrator, not as root from a host perspective.

The core agent is composed of the following services:

- `agent-updater` – Ensures the latest version of the agent is running and performs the proper updates when needed.
- `extension-manager` – Manages the lifecycle of all the extensions and communicates with the Kubernetes API server (kube-apiserver) through REST operations. The extension manager reads extension definitions made available by the extension updater.
- `extension-updater` – Fetches the set of Tanzu Mission Control extension definitions applicable to the cluster on which it is running and makes them available. The extension updater is also responsible for providing/rotating credentials so extensions can access Tanzu Mission Control resources. And along with the extension manager, it is responsible for self-detaching a cluster from Tanzu Mission Control upon request by the user.

The agent also provides a set of extensions, some of which may be installed or removed, depending on the functionality being defined in the cluster.

The current list of extensions is:

- `cluster-auth-pinniped`– Enables Tanzu Mission Control/Cloud Services Platform user authentication on all managed Kubernetes clusters (Pinniped is an OpenID Connect-based, seamless authentication system for Kubernetes).
- `cluster-health-extension` – Gathers health information from the cluster.
- `gatekeeper-operator-manager` – Watches for Tanzu Mission Control-managed policies deployed to the cluster to determine whether Gatekeeper should be installed (or removed).
- `inspection-extension` – Manages conformance scans on the cluster.
- `intent-agent` – Watches the control plane for commands (or *intents*), which are fetched and applied to the cluster (intents are simply Kubernetes resources, typically CRs for which extensions are listening) and acts as a controller for user-initiated actions, such as backing up resources with Velero or scanning for Kubernetes cluster conformance with Sonobuoy.
- `policy-sync-extension` – Applies the policies received from the control plane.
- `policy-webhook` – Defines how and when the Kubernetes API server should delegate admission requests to Gatekeeper, including which resources are to be enforced and what the failure policy is in case the admission controller is unavailable.

- `sync-agent` – Pushes cluster state in the form of Kubernetes resources back to the Tanzu Mission Control control plane, achieving bidirectional communication when paired with the intent agent.
- `tmc-observer` – Gathers logs during extension updates.

Some extensions are optional and are deployed only if an additional Tanzu product is also in use. The current list of optional extensions is:

- `data-protection` – Works with Velero to perform backup-and-restore operations.
- `tsm-operator-extension` – Provides integration functionality with Tanzu Service Mesh.
- `wavefront-extension` – Provides integration functionality with Tanzu Observability.

The control plane of Tanzu Mission Control communicates with the agent and its extensions by using TLS-encrypted gRPC, which operates over HTTP/2, through TCP port 443. The agent and its extensions connect to Tanzu Mission Control through the standard machine-to-machine OAuth 2.0 client credentials grant flow, defined in RFC 6749, by using its own credentials (a client ID and secret) to authenticate and obtain an access token and by pinning a certificate against a certificate authority. The agent manages the lifecycle of the OAuth token used by the extensions.

The lifecycle of the agent and all its extensions is managed entirely by Tanzu Mission Control. It is not currently possible for users to install those extensions from internal registries or to manually control their lifecycles.

Identity and Access Management in Tanzu Mission Control

You connect to Tanzu Mission Control by using VMware Cloud Services Platform, which authenticates users and controls access. The platform gives you a standard OAuth token and restricts access by organization. Then, for Kubernetes clusters created through Tanzu Mission Control, the OAuth token from Cloud Services Platform controls access to those clusters in your organization by using your organization ID. Cloud Services Platform is configured to limit access to those organizations to which you are explicitly granted access. The access control policies you set through Cloud Service Platform and Tanzu Mission Control translate into Kubernetes role-based access control policies on the clusters created with Tanzu Mission Control.

Cloud Services Platform is a centralized service, managed separately and independently from Tanzu Mission Control, which provides services to other SaaS offerings by VMware in addition to Tanzu Mission Control.

On Cloud Services Platform, VMware uses a commercial solution to secure, store and tightly control access to tokens, passwords, certificates, API keys and other secrets and/or personally identifiable information.

Identity and Access Management for Attached Clusters

If you attached your clusters from another cloud provider, such as AWS or Google Cloud Platform (GCP), your access to those clusters remains controlled by the external cloud provider's access control systems and any token you received from them. The security of those clusters and your access to them is governed by the cluster's cloud provider.

For example, if you attach your own Kubernetes clusters running on GCP to Tanzu Mission Control, your access to those clusters continues to use the existing identity access management (IAM) mechanisms of GCP and your GCP Kubernetes cluster, not the IAM systems of VMware. When you use Tanzu Mission Control to make changes to a cluster attached from another cloud provider, such as GCP, the Tanzu Mission Control agent manages those changes on the cluster by communicating with Tanzu Mission Control through the agent's established connection with TLS.

When you attach a cluster from another cloud provider, such as GCP, Tanzu Mission Control gives the cluster a temporary join token. After the cluster is joined to Tanzu Mission Control, the cluster receives a session-based OAuth token through HTTP over TLS for use by the agent and its extensions.

Tanzu Mission Control installs Pinniped as an agent extension, in order to ensure a consistent, Cloud Services Platform-driven identity for all clusters under the same organization.

Key Management

Key management for Tanzu Mission Control infrastructure is handled by standard AWS key management systems. The shared key management systems, which include Vault by HashiCorp and AMS Key Management Service, are managed by Amazon under the standard security policies and practices of AWS. Cryptographic keys used by self-encrypting drives are managed by AWSs as well. Tanzu Mission Control does not currently support the use of your own keys.

Data Storage and Management

The VMware Data Processing Addendum, Privacy Policy, and Terms of Service disclose to customers what type of usage data is collected during their use of VMware Cloud Services. The type of data VMware collects is outlined in our Data Privacy agreement, and the methods by which we use the data is clearly stated and available publicly, on our website. This data collection is necessary to deliver the services outlined in the service descriptions for both VMware Cloud Services and Tanzu Mission Control.

With Tanzu Mission Control, the data of your workloads is not collected or stored, and Tanzu Mission Control has no visibility into data of your actual workloads. The data that Tanzu Mission Control does collect, and store includes metadata about clusters, nodes, hostnames, resource utilization, names of pods, namespace names, labels, regions, zones and other information about the environment in which workloads are running. Sensitive Kubernetes objects, such as secrets, are not stored.

The collected data is stored in three different services: Amazon Relational Database Service (RDS) (currently being phased out in favor of a Postgres DB on EC2 instance with disk encryption), S3 buckets using the SSE-S3 encryption mechanism, and the AWS-managed Kafka service, which is used only for transient data coming from clusters under management. All these services are secured by Amazon’s standard policies and practices.

If you choose to use Velero for backup-and-restore operations for your clusters, the Velero extension stores your data in your Amazon S3 data store.

Shared Responsibility

VMware Cloud Services uses a shared responsibility model for security, which ensures a high security model and eliminates single points of failure. Three parties—VMware, which delivers the service; AWS, which delivers the underlying infrastructure; and the customers who consume the service—share responsibility within the overall security landscape for services that run on VMware Cloud Services. VMware is responsible for ensuring security for the management layer. AWS is responsible for the security of the underlying physical infrastructure of the data center across all regions and availability zones as well as edge locations. And customers continue to own and operate the security and compliance of the actual workloads by extending their policies and controls to public clouds.

Code, Application, and Interface Security

VMware has well-established controls in place to protect all application, program, or object source code, including the Tanzu Mission Control agent. It also has a security development lifecycle process and a security organization that focuses on ensuring VMware Cloud Services implements industry standard operational and security controls. The security development lifecycle program is designed to identify and mitigate security risk during the development phase of VMware software products, including that of the Tanzu Mission Control agent, so that the development group's software is safe for release to customers. Code undergoes a rigorous review for security and quality, including penetration testing and external audits. VMware uses manual and automated source code analysis tools to detect security defects in code as well as known security vulnerabilities in applications and application dependencies before putting code into production. Critical vulnerabilities are addressed before deployment.

Change Control and Configuration Management

VMware's security development lifecycle and change management processes guide personnel to ensure appropriate reviews and authorizations are in place prior to implementing new technologies or changes within the production environment.

VMware Cloud Services has a comprehensive testing system that covers the entire lifecycle of the release. Continuous testing occurs on the software development pipelines for products and components, such as the Tanzu Mission Control agent.

VMware generates builds from approved components and runs these through a variety of end-to-end integration and validation tests. Additionally, VMware runs performance tests, feature stress tests, security scans, vulnerability tests and system tests at scale for every cycle. Vulnerabilities are handled through the VMware vulnerability management procedures.

Vulnerability and Patch Management

VMware's comprehensive vulnerability management program includes vulnerability scanning and penetration testing. VMware patches or upgrades all network, utility and security equipment after analyzing the severity and impact of potential vulnerabilities. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical patches are installed in a timely manner, while non-critical patches are included in the predefined patch schedule and applied within commercially reasonable time frames. Patch testing and rollback procedures are completed by the QA team to ensure compatibility with and minimal impact to the production environment. VMware reviews its vulnerability and patch management process against industry standards, including ISO 27001.

Security Incident Reporting and Management

The VMware Incident Response program's plans and procedures have been developed in alignment with the ISO 27001 standard. VMware maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. See the VMware Data Processing Addendum.

Accreditation and Compliance

VMware continuously monitors existing and emerging security standards and requirements and integrates applicable requirements into our cloud service compliance programs. As VMware partners with you on enabling your compliance, you, as the customer, are required to ensure the service offering meets your compliance and regulatory obligations.

You can review the current list of security standards and accreditations that Tanzu Mission Control has been subject to in this link: https://cloud.vmware.com/products/trust-center.html. Search for "VMware Tanzu Mission Control."

Conclusion

This paper briefly describes the security measures implemented in Tanzu Mission Control and the key mechanisms VMware uses to manage security. If you have additional questions about Tanzu Mission Control, contact your VMware representative.

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