VMware Tanzu™ Mission Control™

Service Description

Updated as of 05 May 2020
© 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at http://www.vmware.com/download/patents.html.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned in this Service Description may be trademarks of their respective companies.

As used in this Service Description, “VMware”, “we”, or “us” means VMware, Inc., a Delaware corporation, if the billing address for your order is in the United States, or VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your order is outside the United States. Terms not defined in this Service Description are defined in the Terms of Service or elsewhere in the Agreement.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com
1. Introduction

1.1 Service Description

VMware Tanzu™ Mission Control™ (the “Service Offering”) is a centralized management platform for consistently operating and securing a customer’s Kubernetes infrastructure and modern applications across multiple teams and clouds. It makes it easier for operators to manage and scale the deployment of modern, containerized applications on Kubernetes running in multiple regions and clouds.

1.2 Technical Documentation and Training

A Quick Start guide, conceptual guides on key areas of the platform, workflow guides for navigating through key features, and FAQs are available at https://docs.vmware.com.

Public documentation that explains how to get started with the Service Offering’s API and CLI is provided at https://code.vmware.com/web/app-modernization/core-capabilities/Tanzu-Mission-Control.

1.3 Legal Terms

Use of the Service Offering is subject to the VMware cloud service offering Terms of Service, that can be found at the VMware end user terms landing page, at: https://www.vmware.com/download/eula.html


2. Service Operations

The following outlines VMware’s roles and responsibilities in providing the Service Offering. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not the duty of VMware or are assumed to be your responsibility.

2.1 Service Provisioning

VMware will provide the following provisioning services:

- VMware will provision a dedicated tenant onto our multi-tenant service offering infrastructure that is ready for your use.
- VMware will send an email to the email address specified in your request to access the Service Offering. Hyperlink(s) to activate and access the Service Offering will be provided within that email.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.

Your responsibilities include:

- Accessing the activation hyperlink(s) provided by VMware, and creating and configuring a VMware cloud services organization as needed.
- Creating user accounts in the system, and identifying users authorized to file support
requests as needed.

- Provisioning, managing, and connecting cloud accounts to the service enabling the lifecycle management of Kubernetes clusters in those accounts as needed.
  - **NOTE:** Provisioning and lifecycle management of Kubernetes clusters within Tanzu Mission Control requires purchase of VMware Tanzu™ Kubernetes Grid™. Consult your VMware sales representative for details.
- Deploying in-cluster agents as needed to attach Kubernetes clusters provisioned independently of the Service Offering for management.
- Configuring network connectivity to ensure that provisioned and attached clusters have consistent network connection to the service.

### 2.2 Support

For assistance in identifying and resolving errors, and to answer questions related to the operational use of the Service Offering, see the VMware Cloud Service Support Policies page, at https://www.vmware.com/support/policies/saas-support.html.

### 2.3 Disaster Avoidance and Disaster Recovery

The Service Offering should not be considered the database of record for your data, and you should not rely on or consider the Service Offering as the sole source of your data, nor a complete copy of your data.

We will provide the following backup and restore services:

- Management infrastructure including: the VMware Tanzu Mission Control service offering and configuration data.

You are responsible for the backup and restoration of the following:

- All Content and configurations created by you in your Kubernetes clusters, including all content, deployment files, container Images, and persistent volumes.
- Cluster inspection report content.

### 2.5 Incident and Problem Management

VMware will provide incident and problem management services (detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which VMware has direct, administrative access and control, including servers and services used to provide the Service Offering.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Your account settings in the Service Offering administrative management console.
- User-deployed and user-configured assets such as proxy agents.
- Anything else not under VMware’s direct control and administration.

### 2.6 Change Management

VMware will provide the following change management elements:

- Processes and procedures to release new code versions and bug fixes.
You are responsible for:

- Management of changes to your VMware Tanzu Mission Control settings, dashboards and other content.
- Administration of self-service features provided through the Service Offering’s system console and user portal, up to the highest permission levels granted to you.
- Cooperating with VMware when planned or emergency maintenance is required.

2.7 Data Privacy

Account Access and Credentials

The Service Offering provides features to automate functions on Kubernetes clusters into your cloud environments, including any infrastructure-as-a-service or software defined data center instances. During the association of these instances, you may, but are not required to, provide access keys, roles, or other credentials to be used by the Service Offering to take actions initiated by your authorized users. By providing such credentials, you are authorizing the Service Offering to utilize those credentials to take actions on behalf of those authorized users.

Customer credentials used by the Service Offering are stored in highly secured, encrypted databases, and are not generally available to our operators or other VMware personnel.

Deletion of Data

Following expiration or termination of the Agreement, all Content, and all personal data contained in Content, in VMware's possession will be deleted from VMware’s primary database and (if applicable) back-up database, as described in the “Termination” section, below. The only exception would be if and to the extent that VMware is required by applicable law to retain any of the personal data (in which case VMware will implement reasonable measures to isolate the personal data from any further processing).

3. Business Operations

Billing and Usage Metering

Purchasing the Service Offering

Entitlements to the Service Offering are purchased through a committed term subscription of one, or three years. Committed charges for the entire term, which are based on the number of cores under management, are payable up front. You can purchase subscriptions to the Service Offering directly from VMware. Consult your VMware sales representative for guidance on how to purchase a subscription.

For purposes of this Service Description, a core is defined as:

- A single unit of processing power on a physical chip, housing a CPU that can execute computer programs.
- In virtualized or hypervisor (VM) environments, a CPU Core is a single physical computational unit of the Processor which may be presented as one or more vCPUs.
- In public cloud environments, constructs such as “vCPUs,” “virtual CPUs,” “virtual cores,” and “dynos” are proxies for CPU Cores. In cases where these proxies are not identified as Hyperthreads, 1 proxy is recognized as one CPU Core. In cases where these proxies are identified as Hyperthreads, two proxies are recognized as one CPU Core. 2 vCPUs = one physical core.
If you wish to purchase additional subscriptions, the Subscription Terms for those additional subscriptions may not be coterminal with subscriptions already purchased. Consult your VMware sales representative for details on purchasing additional subscriptions.

You may elect to pay applicable charges for the Service Offering through redemption of VMware’s Subscription Purchasing Program (SPP) credits or VMware’s Hybrid Purchasing Program (HPP) credits (collectively, “Credits”).

Refer to the following websites for information on the Credit programs:


**Cancellation**

You cannot cancel or terminate your subscription prior to the expiration of the committed purchased Subscription Term. You are liable for all charges for the Subscription Term, regardless of whether you actually use the Service Offering for the entire Subscription Term. There is no refund for any committed charges that you paid at the time you purchased your subscription.

**Termination**

Termination of your Service Offering instance will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the environments and configurations.

We will retain your Content in our backup systems for 30 days following the effective termination date. If you wish to extract your Content from the Service Offering (to the extent you have not already done so prior to termination of your Subscription Term), you must notify us within ten (10) days after the effective termination date, and we will assist you in extracting Content from the Service Offering. You will be responsible for all fees associated with Content extraction. If you do not notify us within that 10-day period, your Content will be permanently deleted and will not be recoverable.