VMware Cloud Director Extension for VMware Tanzu Mission Control 1.0

Table of Contents

Release Notes

Includes product enhancements and notices, bug fixes, and resolved issues.

VMware Cloud Director Extension for VMware Tanzu Mission Control 1.0 Release Notes

This document contains the following sections

- Introduction
- About
- Compatibility
- Caveats and Limitations
- Known Issues

Introduction

VMware Cloud Director Extension for VMware Tanzu Mission Control 1.0 | 18 JAN 2024 | Build 1.0.0-23084897

Check for additions and updates to these release notes.

About

VMware Cloud Director® Extension for VMware Tanzu Mission Control™ is the first VMware SaaS offering that is purpose-built and designed for highly regulated and sovereign environments without any hyperscaler or SaaS dependencies.

Services Providers who are currently offering Kubernetes infrastructure as a Service to run container workloads in a multi-tenant environment, using VMware Cloud Director® Container Service Extension™, can now centrally manage their Kubernetes clusters, and apply IT policies seamlessly using this new VMware Cloud Director Extension for VMware Tanzu Mission Control offering.

From VMware Cloud Director Container Service Extension 4.2, service providers can allow their tenants to not only run container workloads, but also manage multi-cluster Tanzu Kubernetes Grid environment at scale with a unified and centralized interface. Service providers can build economies of scale with their multi-tenant CaaS infrastructure while their end customers can get benefit from application modernization leveraging container ready infrastructure. VMware Cloud Director Extension for VMware Tanzu Mission Control also provides seamless single sign-on for VMware Cloud Director users to access the VMware Tanzu Mission Control Self-Managed UI.

Compatibility

The following product versions are compatible with VMware Cloud Director Extension for VMware Tanzu Mission Control:

Product	**Version**
Tanzu Mission Control Self-Managed	1.1
VMware Cloud Director	10.4.3, 10.5.1
VMware Cloud Director Container Service Extension	4.2
Kubernetes Container Clusters UI plugin	4.2
Tanzu Kubernetes Grid	2.1.1, 2.2, 2.3.1, 2.4
Object Storage Extension	2.2.2 and newer versions

For clusters that host VMware Cloud Director Extension for VMware Tanzu Mission Control, it is necessary that the cluster has the compatible Kubernetes components configured.
For more information, see the **Compatibility Updates** section in VMware Cloud Director Container Service Extension 4.2 Release Notes.

Caveats and Limitations

VMware Cloud Director Extension for VMware Tanzu Mission Control does not support the use of non-English characters in usernames or full names.

The VMware Cloud Director UI may not be used to update or delete the VMware Cloud Director Extension for VMware Tanzu Mission Control if the CLI is used for installation.

Solution add-ons use an encryption key when transmitting or storing some information. VMware Cloud Director generates and stores this value when the VMware Cloud Director UI is used for installation. The CLI installation method requires the user to provide this encryption key for all operations because VMware Cloud Director does not store it.

Existing clusters must be updated to trust Harbor repositories with self-signed certificates

The cluster used to operate VMware Cloud Director Extension for VMware Tanzu Mission Control, and any tenant cluster attached to VMware Cloud Director Extension for VMware Tanzu Mission Control pulls images and Tanzu package information from the configured Harbor repository. It is necessary to configure those clusters to trust the self-signed certificate used by the Harbor service. To establish that trust, it is necessary to recreate all cluster nodes, and update the `kapp-controller` configuration to trust the certificates.

For more information, see Configure VMware Cloud Director Extension for VMware Tanzu Mission Control with self-signed certificates (94799).

Known Issues

VMware Cloud Director UI Tasks pane can show multiple `GetFullEntity` calls for one cluster.

The VMware Cloud Director UI **Tasks** pane can show multiple `getFullEntity` calls for one cluster. In VMware Cloud Director UI **Tasks** pane, search on the cluster name, and you can see frequent `getFullEntity` calls. This can happen when a VMware Tanzu Mission Control attach attempt is performed, and it fails for some reason. The VMware Cloud Director Container Service Extension backend, or Projector component, attempts to reconcile or retry the operation for about 90 minutes. Regardless of whether the operation succeeds or not in that duration, you will notice `getFullEntity` calls being indefinitely made for every minute in the VMware Cloud Director **Task** pane.

This is due to a bug in VMware Cloud Director 10.5.1 and 10.4.3. VMware Cloud Director does not clean up successful or expired operations from the `operations-to-be-retried` set in the Cluster RDE.

Workaround

Identify and remove problematic elements from the `RDE.entity.status.projector.retrySet`.

All or any elements with an empty body, partial body or with a missing `creationTimeStamp` field need to be removed cleanly from `RDE.entity.status.projector.retrySet` using the VMware Cloud Director workaround detailed in the VMware Cloud Director 10.5.1 Release Notes.

Once the `RDE.entity.status.projector.retrySet` becomes empty, you should not see any further `getFullEntity` calls on the cluster for every minute.

API calls

1. Retrieve the `cluster-id` from the **Cluster Information** page in the Kubernetes Container Clusters UI.
2. In Postman, and perform `Get https://vcd/cloudapi/1.0.0/entities/cluster-id;` save the ETag from the response headers.
3. Modify the body to remove all or any problematic elements from `RDE.entity.status.projector.retrySet`.
4. In Postman, perform a `PUT` with the modified body `https://vcd/cloudapi/1.0.0/entities/ {cluster-id}`.

   a. Use with the same ETag retrieved in Step 2, and insert it as a value for the header with the key `If-Match`.
   b. Ensure the VMware Cloud Director workaround in Using the VMware Cloud Director API, attempting to delete an item with a `secure` field from an array in an RDE instance results in the item not being fully deleted is followed here to include or modify the request payload.

5. If update fails with ETag error, repeat Step 2.

For more information on using ETags, see VMware Cloud Director Open API.

TMC Attachment Status column can display a cluster's status switching from Ready to another value after the cluster has been successfully attached.

After a cluster is successfully attached in VMware Cloud Director Extension for VMware Tanzu Mission Control, and shows the **TMC Attachment Status** as **Ready**, the status value can later change, for example to **Unknown**. It can happen if there are resource constraints on the cluster, and the cluster intermittently gets disconnected from VMware Cloud Director Extension for VMware Tanzu Mission Control.

Workaround:

Ensure that the cluster resources are sufficient for the cluster agent extensions to run successfully. Cluster agent extensions are installed when cluster is attached to VMware Cloud Director Extension for VMware Tanzu Mission Control. For more information, see Memory and CPU Usage by Cluster Agent Extensions.

The Kubernetes Container Clusters UI plugin 4.2.0 loads the cluster list and the cluster information page extremely slowly.

This behavior occurs if the user has access to VMware Tanzu Mission Control, but the service is inaccessible. The cluster list datagrid and cluster information page will display a spinner, and then the UI will eventually render successfully.

There are two workarounds for this issue:

- Remove VMware Tanzu Mission Control access from tenant organizations. In this situation, VMware Tanzu Mission Control is inaccessible anyway.
- Uninstall VMware Tanzu Mission Control from solutions add-ons. For more information, see Remove a Solution Add-On From VMware Cloud Director.

The Kubernetes Container Clusters 4.2 UI cannot recognize the VMware Tanzu Mission Control attachment status for manually attached clusters

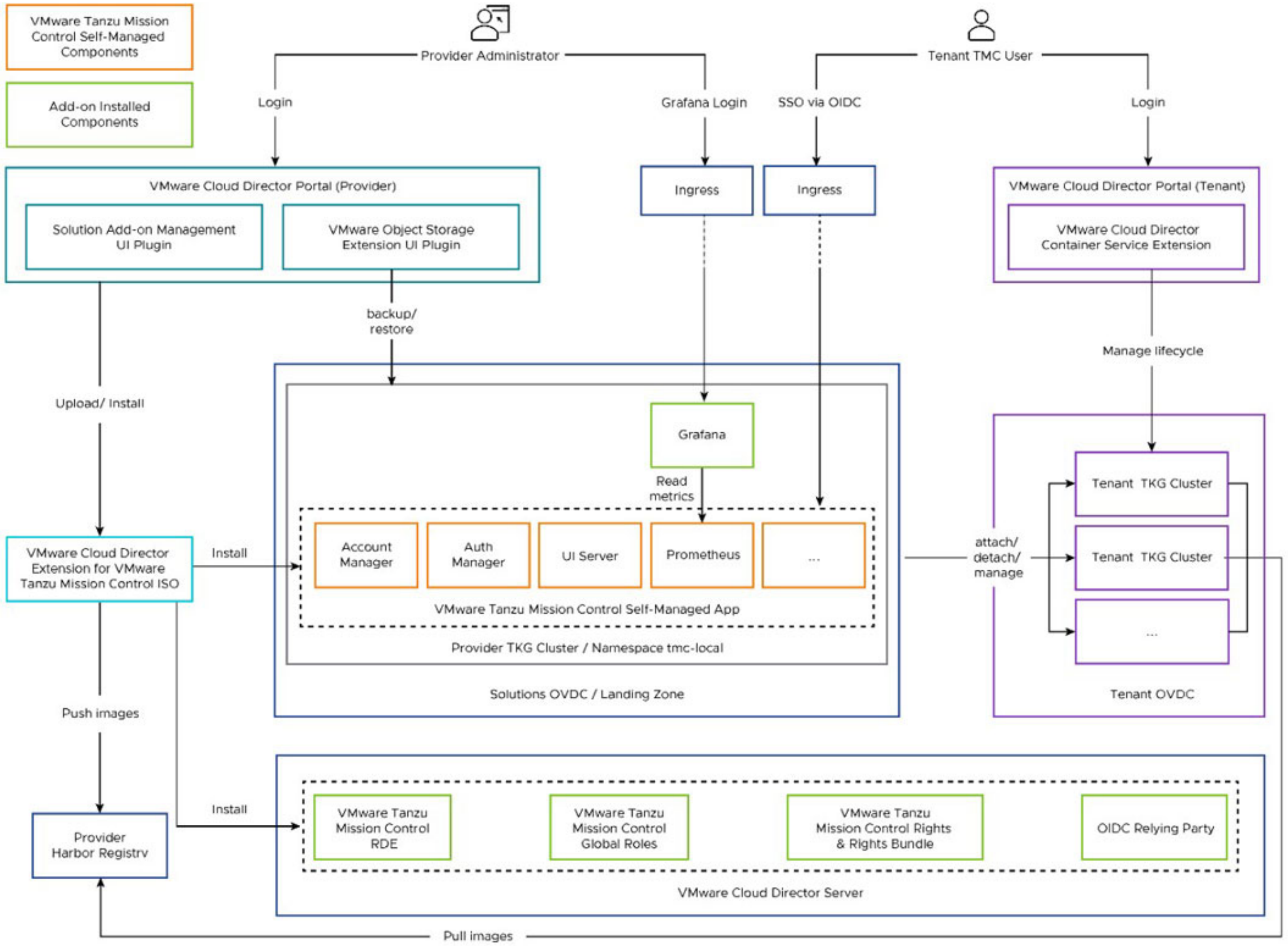
Existing clusters that were manually attached to VMware Tanzu Mission Control display a blank status in the **TMC Attachment Status** column in the **Cluster Information** page of Kubernetes Container Clusters 4.2 UI.

Installing, Configuring and Using VMware Cloud Director Extension for VMware Tanzu Mission Control as a Service Provider

VMware Cloud Director Extension for VMware Tanzu Mission Control is an on-premises VMware Tanzu® Mission Control™ integrated into VMware Cloud Director®. Tenant users can consume VMware Tanzu Mission Control functionality using VMware Cloud Director, and VMware Cloud Director® Container Service Extension™ in a multi-tenant way.

Service providers who offer Kubernetes Infrastructure as a Service to run container workloads in a multi-tenant environment using VMware Cloud Director Container Service Extension can now centrally manage their Kubernetes clusters, and apply IT policies seamlessly using VMware Cloud Director Extension for VMware Tanzu Mission Control.

The following diagram details the how service providers and tenant users can consume VMware Cloud Director Extension for VMware Tanzu Mission Control, and how it interacts with supporting products.


VMware Tanzu Mission Control Self-Managed Components
Add-on Installed Components
Provider Administrator
Tenant TMC User
Login
Grafana Login
SSO via OIDC
Login
VMware Cloud Director Portal (Provider)
Solution Add-on Management UI Plugin
VMware Object Storage Extension UI Plugin
Ingress
Ingress
VMware Cloud Director Portal (Tenant)
VMware Cloud Director Container Service Extension
backup/ restore
Manage lifecycle
Upload/ Install
Grafana
Read metrics
Account Manager
Auth Manager
UI Server
Prometheus
...
VMware Tanzu Mission Control Self-Managed App
Provider TKG Cluster / Namespace tmc-local
Solutions OVDC / Landing Zone
VMware Cloud Director Extension for VMware Tanzu Mission Control ISO
Install
attach/ detach/ manage
Tenant TKG Cluster
Tenant TKG Cluster
...
Tenant OVDC
Push images
Install
Provider Harbor Registry
VMware Tanzu Mission Control RDE
VMware Tanzu Mission Control Global Roles
VMware Tanzu Mission Control Rights & Rights Bundle
OIDC Relying Party
VMware Cloud Director Server
Pull images

Compatibility

VMware Cloud Director Extension for VMware Tanzu Mission Control interacts with several products. To ensure VMware Cloud Director Extension for VMware Tanzu Mission Control operates successfully, it is beneficial to examine these compatibility details.

Table 1: Interoperability

Product	Supported Versions
VMware Cloud Director	10.4.3, 10.5.1
VMware Cloud Director Container Service Extension	4.2
Kubernetes Container Clusters UI plugin	4.2
Tanzu Kubernetes Grid	2.1.1, 2.2, 2.3.1, 2.4
VMware Cloud Director Object Storage Extension	2.2.2 and newer versions
VMware Tanzu Mission Control Self-Managed	1.1.0

Before you begin

Before you can install , and use VMware Cloud Director Extension for VMware Tanzu Mission Control, it is necessary to prepare your environment so it is compatible.

Ensure the following components are in place for VMware Cloud Director Extension for VMware Tanzu Mission Control to operate successfully.

- Install VMware Cloud Director 10.5.1. For more information, see the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.
- Install VMware Cloud Director Container Service Extension 4.2, and Kubernetes Container Clusters 4.2 UI plugin. For more information, see Installing, Configuring, and Upgrading VMware Cloud Director Container Service Extension as a Service Provider.
- Configure a Solution Organization. This is used to configure the Solution Add-On Landing Zone. This is usually the same organization that is used to host the VMware Cloud Director Container Service Extension server. For more information, see Create an Organization.
- Configure a Tenant Organization. For more information, see Create an Organization.
- Deploy a Harbor registry to host the VMware Cloud Director Extension for VMware Tanzu Mission Control images.
- Configure the Solution Add-On Landing Zone. For more information, see Configure Your Solution Add-On Landing Zone.
- Install VMware Cloud Director® Object Storage Extension™ to back up the cluster that hosts VMware Cloud Director Extension for VMware Tanzu Mission Control. For more information, see Installing, Configuring, and Upgrading VMware Cloud Director Object Storage Extension.
- Configure DNS records for the DNS zone to the external IP of VMware Cloud Director Extension for VMware Tanzu Mission Control, for example, `tmc.mycloud.local → 10.100.1.2`. It is necessary to map the following subdomains to the same external IP:

Sub domains
`<tmc_zone>`

Table continued on next page

Continued from previous page

Sub domains
`alertmanager.<tmc_zone>`
`auth.<tmc_zone>`
`blob.<tmc_zone>`
`gts.<tmc_zone>`
`gts-rest.<tmc_zone>`
`landing.<tmc_zone>`
`pinniped-supervisor.<tmc_zone>`
`prometheus.<tmc_zone>`
`grafana.<tmc_zone>`
`s3.<tmc_zone>`
`console.s3.<tmc_zone>`
`tmc-local.s3.<tmc_zone>`

Certificate Management for VMware Tanzu Mission Control

There are several TLS certificates used to deliver VMware Cloud Director Extension for VMware Tanzu Mission Control. These include VMware Cloud Director, VMware Tanzu Mission Control, and the container registry that hosts VMware Tanzu Mission Control images. These protect the communication between the services and VMware Cloud Director Container Service Extension clusters.

- The service provider and tenant user VMware Cloud Director Container Service Extension clusters pull container images and Carvel `PackageRepositories` from the container registry.
- VMware Tanzu Mission Control services on the service provider VMware Cloud Director Container Service Extension cluster connect to VMware Cloud Director as part of an OAuth handshake.
- Tenant users connect to VMware Tanzu Mission Control services through the UI or CLI.
- VMware Tanzu Mission Control components on tenant VMware Cloud Director Container Service Extension clusters connect to VMware Tanzu Mission Control services as part of the management communication.

Choosing a Certificate Authority

Each of these certificates may be signed by an external certificate authority or by an internal self-signed certificate authority. There are some implications to consider when deciding a certificate type for installation.

- Using externally-signed certificates for all services results in the easiest experience for users.
- It is recommended to use the same certificate authority for VMware Cloud Director and VMware Tanzu Mission Control.

  NOTE
  If you use different certificate authorities, it is necessary to provide the certificate authority for VMware Tanzu Mission Control to the **TLS CA Bundle** parameter during installation.

- If the container registry uses a self-signed certificate, it is necessary to submit it to the **Harbor CA Bundle** parameter during installation.

  NOTE
  It is necessary to update any existing clusters to include this certificate authority in their CAPI and `kapp-controller` configuration before you attach them to VMware Tanzu Mission Control. For more information, see Configure VMware Cloud Director Extension for VMware Tanzu Mission Control with self-signed certificates (94799).

NOTE
If you use self-signed certificates for the container registry, it is necessary to enter the certificates as part of the VMware Cloud Director Container Service Extension service provider workflow. For more information, see Create an Airgapped Environment.

Configuring the VMware Tanzu Mission Control certificates

Once you choose a certificate authority, the following two configuration options are available.

- If supported by your certificate authority, you may be able to configure a `cert-manager.ioClusterIssuer` on the VMware Cloud Director Container Service Extension cluster to provision certificates during installation. This means you do not need to manually configure the certificates for each DNS name, and that `cert-manager` handles certificate rotation when applicable.

  NOTE
  If self-signed certificates are used for VMware Tanzu Mission Control, it is possible to configure a `ClusterIssuer` that grants certificates from a self-signed certificate authority. For more information, see Configure VMware Cloud Director Extension for VMware Tanzu Mission Control with self-signed certificates (94799).

- If you do not want to use `cert-manager`, you can generate the certificates independently. The certificates can be configured during the VMware Cloud Director Extension for VMware Tanzu Mission Control installation process, or directly on the cluster that hosts VMware Tanzu Mission Control.

  Configuring the certificates during installation only works if you have a single certificate with Subject Alternative Names (SANs) for all DNS entries. Provide the certificate and key during the installation process using the **TLS Certificate** and **TLS Private Key** parameters. Set the **Certificate Provider** parameter to `import`.

  You can also load the certificates directly onto the cluster if you have individual certificates for each DNS entry, or would prefer to manage them. For more information, see the **Importing Certificates** section of Preparing your cluster to host Tanzu Mission Control Self-Managed, and set the **Certificate Provider** parameter to `pre-installed`.

  NOTE
  If you use a different certificate authority than the one you use for VMware Cloud Director, it is necessary to provide the certificate authority for VMware Tanzu Mission Control to the **TLS CA Bundle** parameter during installation.

Rotating a Self-Signed Certificate Authority

If you use self-signed certificates for the container registry, VMware Cloud Director or VMware Tanzu Mission Control services, it is recommended to use a self-signed certificate authority (CA). A CA is generally created with a longer validity than is used for service certificates. You can use the CA when you configure the connection between services so that individual certificates can be rotated without having to reconfigure all components with a new certificate.

Perform the following additional processing when the CA expires:

- Update all clusters to include the new CA in their CAPI definition so container images can be pulled from the container registry.
- Update the `kapp-controller` configuration on all clusters so `PackageRepository` and `Package` definitions may be pulled from the container registry.
- Update VMware Tanzu Mission Control to allow the services to connect to VMware Cloud Director during the authentication process.
- Re-attach all attached clusters to VMware Tanzu Mission Control after the new certificates are deployed. This will re-establish trust with the new CA. For more information, see Re-establish cluster connection after certificate rotation.

User Roles and Rights

Access to VMware Cloud Director Extension for VMware Tanzu Mission Control is managed by a rights bundle, and two roles in VMware Cloud Director. These roles are referred to as the**TMC Administrator** and**TMC Member** role, but you can configure specific names for these roles during installation. These roles are used to configure **Access Policies** when an organization is initially onboarded to VMware Tanzu Mission Control. The**TMC Administrator** can modify these policies to give access to any user or role they choose after the initial onboarding.

For more information on VMware Tanzu Mission Control roles, see *`Access Control`* in the *`VMware Tanzu Mission Control Concepts`* documentation.

Table 2: Rights Bundle

Rights Bundle	Description
vmware:tmc_tenant	This rights bundle contains the privileges that an organization needs to avail of VMware Cloud Director Extension for VMware Tanzu Mission Control.

Table 3: User Roles

Global Role in VMware Cloud Director	Default Value	Rights	Mapped Role in VMware Tanzu Mission Control
TMC Administrator	**tmc:admin**	• **VIEW: VMWARE:TMC** • Enable OIDC Server • Inherited rights from existing**Kubernetes Cluster Author Role** in VMware Cloud Director. • Inherited rights from existing**Organization Administrator** role in VMware Cloud Director.	Service Admin
TMC Member	**tmc:member**	• **VIEW: VMWARE:TMC** • Enable OIDC Server • Inherited rights from existing**Kubernetes Cluster Author Role** in VMware Cloud Director.	Service Member

You can set the values for these roles during installation of the solution. The values will apply to all organizations in VMware Cloud Director. The solution will create roles with the rights above if they do not already exist. If the role exists before the installation of VMware Cloud Director Extension for VMware Tanzu Mission Control, the solution will add the following two rights to each role:

- **VIEW: VMWARE:TMC**
- **Enable OIDC Server**

> **NOTE**
> By default,**TMC Administrator** users cannot view or manage VMware Tanzu Mission Control attachable clusters from the VMware Cloud Director UI. Additional rights like**Administrator View: VMWARE:CAPVCDCLUSTER** and/or**Administrator Full Control: VMWARE:CAPVCDCLUSTER** are necessary for this user to manage those clusters. However, the**TMC Administrator** user can manage all these clusters from VMware Tanzu Mission Control portal.

NOTE

- Service providers cannot attach any clusters from tenant organizations to VMware Tanzu Mission Control from VMware Tanzu Mission Control UI or Kubernetes Container Clusters UI, even though they are assigned with the**TMC Administrator** role. This privilege only allows service providers to log in to the VMware Tanzu Mission Control UI.
- Service providers cannot view tenant clusters in VMware Tanzu Mission Control UI.
- Service providers cannot view VMware Tanzu Mission Control attachment status in Kubernetes Container Clusters UI.

NOTE

If an external IDP is used for all organizations, tenant administrators may assign multiple roles to their users through the appropriate claims. In this case the**TMC Administrator** and**TMC Member** role may be minimally privileged with the rights above. This will not work if any organization is using VMware Cloud Director local users as those users may only be assigned to a single role.

Information for Tenant Administrators

Once VMware Cloud Director Extension for VMware Tanzu Mission Control is installed in the organization's VMware Cloud Director environment, service providers must advise organization tenant administrators to assign tenants users in their organization to either the**TMC Administrator** or**TMC Member** role.

NOTE

Ensure VMware Cloud Director tenant users have the `fullname` populated in the user object for VMware Tanzu Mission Control Self-Managed login to work correctly. The `email` may be used to create per-user access policies but is not required.

NOTE

It is necessary for a user with the**TMC Administrator** role to login to VMware Tanzu Mission Control to initialize the organization default settings, before any user with the**TMC Member** role can use the service through the Kubernetes Container Clusters UI.

Install VMware Cloud Director Extension for VMware Tanzu Mission Control

Follow the steps in this section to install VMware Cloud Director Extension for VMware Tanzu Mission Control.

1. Download VMware Cloud Director Extension for VMware Tanzu Mission Control ISO file from the Broadcom Support Portal.
2. Click **More › Kubernetes Container Clusters › CSE Management › Tanzu Mission Control**.
3. In the **Create a new Tanzu Mission Control Instance in Add-ons** tab, click **Go to Add-ons**.
4. Upload the VMware Cloud Director Extension for VMware Tanzu Mission Control ISO file to VMware Cloud Director, and deploy an instance. For detailed instructions, see Upload a Solution Add On, and Deploy an Instance of a Solution Add-On. For configuration details, see Installation Parameters.

   NOTE

   The Solution Add-On installation process in VMware Cloud Director may take up to 120 minutes to complete.

5. After you have successfully installed VMware Cloud Director Extension for VMware Tanzu Mission Control, copy the Tanzu Standard package repository images and inspection images to your private image registry. For instructions, see `Copying Tanzu Standard and inspection images` in the `Installing and Running VMware Tanzu Mission Control Self-Managed` documentation.

The VMware Cloud Director Extension for VMware Tanzu Mission Control add on is installed, and the add on tile appears in the **Solutions Add-On Landing Zone**. You can access VMware Cloud Director Extension for VMware Tanzu Mission Control through the Kubernetes Container Clusters UI in VMware Cloud Director, and perform cluster operations. To do this, click **More › Kubernetes Container Clusters › CSE Management › Tanzu Mission Control**.

Publish the VMware Cloud Director Extension for VMware Tanzu Mission Control add on to tenant organizations.

Installation Parameters

When you install VMware Cloud Director Extension for VMware Tanzu Mission Control, you can enter these specific parameters.

Parameter	Description	Example	Required
Add-On Instance Name	Name of the instance to be created	`tmc-1`	Y
DNS Zone	Provide DNS zone to configure VMware Tanzu Mission Control endpoints, for example, `tmc.mycloud.local`	`tmc.mycloud.local`	Y
Contour Envoy Load Balancer IP	Provide the Load balancer IP of Contour Envoy, i.e., 10.100.1.2. TMC DNS Zone should be mapped to this IP. To retrieve this parameter, in VMware Cloud Director UI, navigate to **Edge Gateway Settings**, and select one free IP in the **Allocated IPs** tab.	`10.100.1.2`	Y
Harbor URL	Provide Harbor project path for pushing or pulling VMware Tanzu Mission Control packages during VMware Cloud Director Extension for VMware Tanzu Mission Control installation.	`harbor-repo.mycloud.local/vcd_tmcl`	Y
Harbor User Name	Provide Harbor username for basic authentication		Y
Harbor Password	Provide Harbor password for basic authentication		Y
Harbor CA Bundle	Provide the CA bundle file in PEM format of the Harbor server. It is required if the Harbor server certificate is not signed by a well-known certificate authority. **NOTE** It is only necessary to input this value for self-signed certificates. If you are using publicly-signed certificates, leave this value empty.		N
Kube Cluster Name	Provide the Kubernetes cluster name for VMware Cloud Director Extension for VMware Tanzu Mission Control deployment. This cluster needs to reside in the Solution Add-on organization.	`tmc`	Y
Certificate Provider	Set the way to provide certificates for TMC server. Allowed values are: `cluster-issuer`, `import` and `pre-installed`. Defaults to `cluster-issuer`.	`cluster-issuer`	N
Cluster Issuer Name	Provide the existing cluster issuer name for `cert-manager`. This parameter is required when`cert-provider` is `cluster-issuer`.	`acme-cluster-issuer`	N

Table continued on next page

Continued from previous page

Parameter	Description	Example	Required
MinIO Root Username	Set MinIO root user name. Defaults to `minioadmin`.	`minioadmin`	N
MinIO Root User Password	Set MinIO root user password. If left blank, a random password will be generated. Format: no less than 8 characters, minimum of 1 digit, minimum of 1 special character (@$!%*#.,-_=*), and minimum of 1 letter.	`P@ssw0rd`	N
PostgreSQL Password	Set the VMware Cloud Director Extension for VMware Tanzu Mission Control`PostgreSQL` password. If left blank, a random password is generated. Format: no less than 8 characters, minimum of 1 digit, minimum of 1 special character (-._~), and minimum of 1 letter.	`P_ssw0rd`	N
Grafana Admin Username	Set the default Grafana admin user name. Defaults to `admin`.		N
Grafana Admin Password	Set the default Grafana admin user password. If left blank, a random password will be generated. Format: no less than 8 characters, minimum of 1 digit, minimum of 1 special character, and minimum of 1 letter.		N
Deploy Timeout	Sets the timeout in seconds for VMware Tanzu Mission Control packages installation. This value defaults to 7200.	`7200`	N
Admin Role Name	Set the administrative user role name for VMware Tanzu Mission Control. The default value is `tmc:admin` if it's not given.		N
Member Role Name	Set the member user role name for VMware Tanzu Mission Control. The default value is `tmc:member` if it is not given.		N
TLS Certificate	Provide the TLS certificate in PEM format for VMware Cloud Director Extension for VMware Tanzu Mission Control services. This parameter is required when cert-provider is `import`.		N
TLS Private Key	Provide the TLS private key in PEM format for VMware Cloud Director Extension for VMware Tanzu Mission Control services. This parameter is required when `cert-provider` is `import`.		N
TLS CA Bundle	Provide the CA bundle in PEM format of the TLS certificates for VMware Cloud Director Extension for VMware Tanzu Mission Control services. This parameter is only allowed when cert-provider is **import**.		N

Table continued on next page

Continued from previous page

Parameter	**Description**	**Example**	**Required**
	NOTE If the VMware Tanzu Mission Control certificates are signed by the same certificate authority as the VMware Cloud Director certificate, this value should be left empty. Otherwise, it should be filled, whether the certificates are self-signed or publicly-signed.		
Extra Installation Values	Set extra values of VMware Cloud Director Extension for VMware Tanzu Mission Control configuration in YAML format. The full specification of the YAML is at Configuration key values for installing Tanzu Mission Control Self-Managed.		N

Table continued on next page

Continued from previous page

<table>
<tr><th>Parameter</th><th>Description</th><th>Example</th><th>Required</th></tr>
<tr><td></td><td>
<b>NOTE</b>
It is necessary to set the following sizing parameters with appropriate values during the installation process. It is not possible to set or change these parameters after the installation process.
<b>Table 4: Sizing Parameters</b>
<table>
<tr><th>Sizing Parameter</th><th>Description</th></tr>
<tr><td><code>size</code></td><td>The size of the VMware Tanzu Mission
Control stack. If the value is not assigned, the default value is used. The acceptable values are <code>small</code> and <code>medium</code>. The default value is <code>small</code>.</td></tr>
<tr><td><code>prometheusVolumeSize</code></td><td>Persistent volume size for Prometheus data volume. The value is generally given in Gibibytes (100 GiB). The defaults to 5GiB.</td></tr>
</table>
<table>
<tr><th>Keys</th><th>Instruction</th></tr>
<tr><td><ul><li><code>dnsZone, minio.username</code></li><li><code>harborProject</code></li><li><code>contourEnvoy.loadBalancerIP</code></li><li><code>clusterIssuer</code></li></ul></td><td>These keys must not be set in the YAML since the add-on has dedicated input parameters for them.</td></tr>
<tr><td><ul><li><code>contourEnvoy.serviceType</code></li><li><code>authenticationType</code></li></ul></td><td>These keys must not be set because they have constant values for VMware</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

Table continued on next page

Table continued on next page

Continued from previous page

<table>
<tr><th>Parameter</th><th>Description</th><th>Example</th><th>Required</th></tr>
<tr><td></td><td>
<i>Continued from previous page</i>
<table>
<tr><th>Keys</th><th>Instruction</th></tr>
<tr><td></td><td>Cloud Director.</td></tr>
<tr><td>• <code>oidc.clientID</code>
• <code>oidc.clientSecret</code>
• <code>oidc.issuerType</code>
• <code>oidc.issuerURL</code>
• <code>certificateImport</code></td><td>These keys must not be set because the add-on will generate values based on VMware Cloud Director configuration.</td></tr>
<tr><td>• <code>trustedCAs</code>
• <code>corsPolicyAllowedOrigins</code></td><td>The add-on appends values to these keys based on VMware Cloud Director configuration.</td></tr>
<tr><td>• <code>minio.password</code>
• <code>postgres.password</code>
• <code>telemetry</code>
• <code>idpGroupRoles.admin</code>
• <code>idpGroupRoles.member</code></td><td>If these keys are given, they overwrite the default values, but the add-on input parameters take precedence over them.</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

Installation Troubleshooting

The following error message can appear when you attempt to install VMware Cloud Director Extension for VMware Tanzu Mission Control:

```
INFO Wait for the grafana PackageInstall to be reconciled action=hook event=PostCreate
> kubectl -n tmc-grafana-install get pkgi

NAME                  PACKAGE NAME               PACKAGE VERSION   DESCRIPTION
                                       AGE

tmc-grafana-install   grafana.tanzu.vmware.com                     Reconcile failed:
Package grafana.tanzu.vmware.com not found   14m

>
```

Reason and fix:

The tanzu-standard `PackageRepository` is not present, or was created outside of the global kapp-controller namespace. Install the tanzu-standard `PackageRepository`.

For more troubleshooting information, see Troubleshooting your Tanzu Mission Control Self-Managed Deployment.

Update VMware Cloud Director Extension for VMware Tanzu Mission Control Configuration

You can update the installation values of the VMware Cloud Director Extension for VMware Tanzu Mission Control instance.

1. Log in to VMware Cloud Director, click **More › Kubernetes Container Clusters › CSE Management › Tanzu Mission Control**.
2. Click **All Actions › Update.**
3. Find the instance, click on the triple-dot menu, and click **Update**.
4. Edit the installation parameters, and select **Confirm**.

> **NOTE**
> Once you update the installation parameters, there is approximately a 15 to 30 minute delay for these changes to come into effect.

Upgrade VMware Cloud Director Extension for VMware Tanzu Mission Control

You can upgrade the instance of VMware Cloud Director Extension for VMware Tanzu Mission Control to the latest version. When an upgrade is available, a notification appears in the **Instance Details** page.

1. Log in to VMware Cloud Director, click **More › Solution Add-On Management › Upload.**
2. Upload the VMware Cloud Director Extension for VMware Tanzu Mission Control ISO file to VMware Cloud Director. For detailed instructions, see Upload a Solution Add On.
3. Find the solution type **Tanzu Mission Control**, and click **Details**.
4. Find the instance, click on the triple-dot menu, and click **Upgrade**.
5. In the **Upgrade Instance** window, click **Next**.
6. Select the version you want to upgrade to, and click **Upgrade**.

> **NOTE**
> It is necessary to upgrade the instance of VMware Cloud Director Extension for VMware Tanzu Mission Control you used in the Initial GA to VMware Cloud Director Extension for VMware Tanzu Mission Control 1.0. To do this, follow the upgrade workflow above. When you select **Upgrade**, the first attempt will fail, and display the below error in the **Task Details** window:
>
> ```
> The addon RDE instance has been updated, please retry the upgrade.
> ```
>
> To complete the upgrade to VMware Cloud Director Extension for VMware Tanzu Mission Control 1.0, it is necessary to click **Retry Upgrade**.

Monitor a VMware Cloud Director Extension for VMware Tanzu Mission Control Cluster

You can monitor the health of VMware Tanzu Mission Control Self-Managed services on the cluster that hosts VMware Cloud Director Extension for VMware Tanzu Mission Control. It is beneficial to use this feature to check that the cluster is operating correctly, and is in good health.

1. Log in to VMware Cloud Director, click **More › Kubernetes Container Clusters › CSE Management › Tanzu Mission Control**.
2. Click **All Actions › Monitor.**
3. Login to Grafana, and view the health of your cluster.

NOTE
If you forget the username and password or you choose to auto-generate the password for the Grafana admin user, complete the following steps to get the username and password of the Grafana admin user:

1. Download the `kubeconfig` file of the Kubernetes cluster on which the VMware Cloud Director Extension for VMware Tanzu Mission Control is installed in the **Cluster Information** page in Kubernetes Container Clusters. For more information, see Manage Clusters.
2. Configure kubectl to use the downloaded `kubeconfig` file.
3. Run the following kubectl commands to get the username and password for the Grafana admin user:

```
kubectl -n tmc-local get secret grafana -o jsonpath='{.data.admin-user}'
| base64 -d
```

```
kubectl -n tmc-local get secret grafana -o jsonpath='{.data.admin-
password}' | base64 -d
```

Backup and Restore Clusters

When you use VMware Cloud Director Extension for VMware Tanzu Mission Control, it is important to backup and restore the cluster that hosts VMware Cloud Director Extension for VMware Tanzu Mission Control. When you back up and restore clusters, the data can be restored from an earlier point in time if an unplanned event occurs.

It is necessary to manually backup and restore the cluster that hosts VMware Cloud Director Extension for VMware Tanzu Mission Control through VMware Cloud Director Object Storage Extension. For instructions, see Backing up and restoring Kubernetes clusters.

NOTE
You may experience some errors when you back up and restore VMware Tanzu Mission Control in Tanzu Kubernetes Grid 2.1.1 and newer versions. For more information, see VMware Cloud Director Object Storage Extension 2.2.2 Release Notes.

Remove VMware Cloud Director Extension for VMware Tanzu Mission Control

When you delete VMware Cloud Director Extension for VMware Tanzu Mission Control, you permanently remove all of its resources and data associated with the management of tenant clusters. The tenant clusters will not be deleted.

Ensure the **TMC Administrator** and **TMC Member** roles have been removed from all local users or groups before you remove VMware Cloud Director Extension for VMware Tanzu Mission Control. The removal process attempts to unpublish these roles from all organizations. A warning displays if that is not possible. The removal process will proceed despite these warnings.

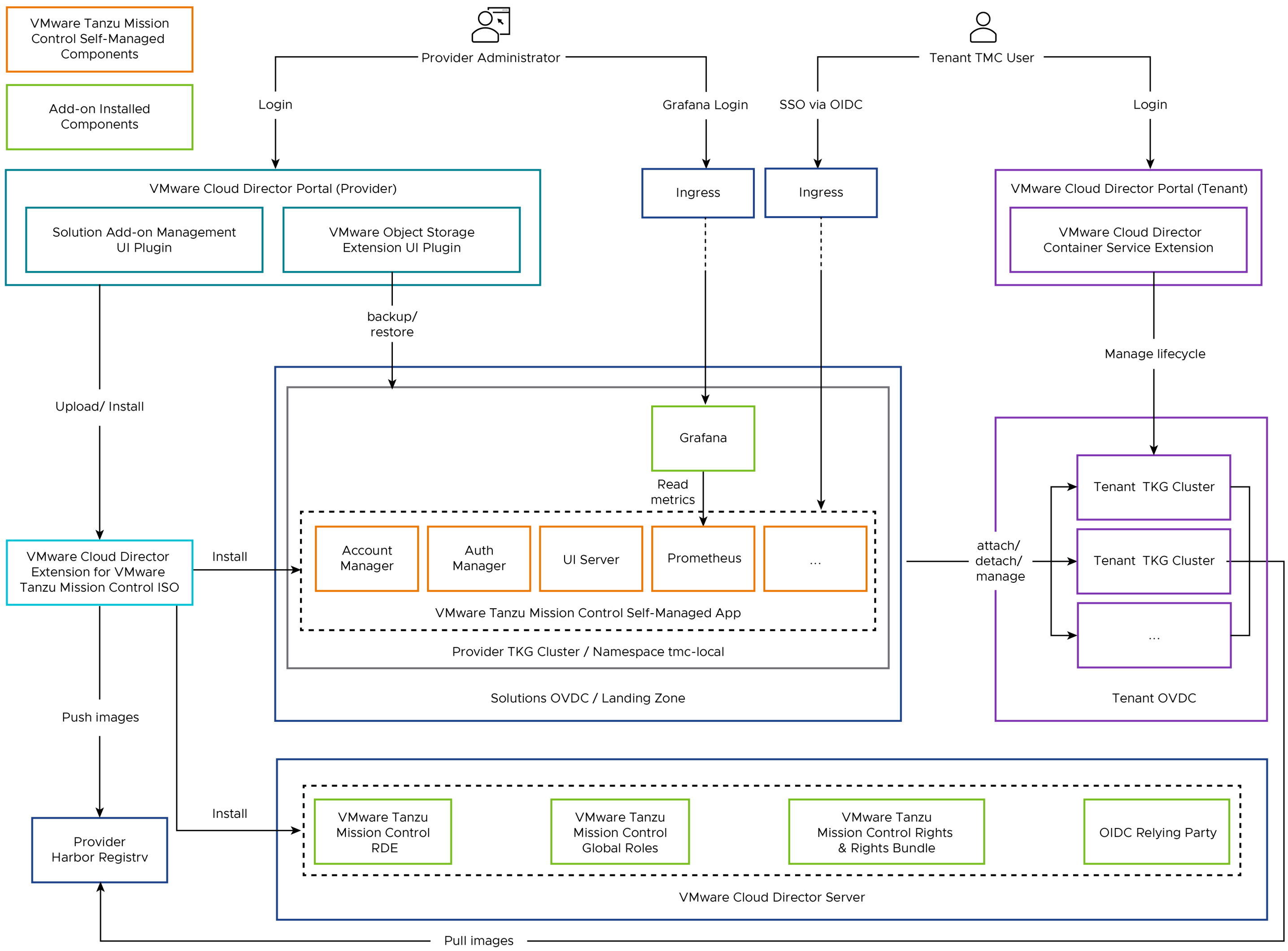
1. Log in to VMware Cloud Director, click **More › Kubernetes Container Clusters › CSE Management › Tanzu Mission Control**.
2. Click **All Actions › Remove**.
3. In the **Solution Add-On Management** page, click the three dots next to the **Tanzu Mission Control Self-Managed**, and click **Remove**.
4. A pop-up window appears. If you want to remove VMware Cloud Director Extension for VMware Tanzu Mission Control Add-On, click **Remove** to confirm.

The VMware Cloud Director Extension for VMware Tanzu Mission Control instance is removed, and does not appear in the **Solution Add-On Landing Zone**. VMware Cloud Director Extension for VMware Tanzu Mission Control is also removed from the cluster.

Using VMware Cloud Director Extension for VMware Tanzu Mission Control as a Tenant User

VMware Cloud Director Extension for VMware Tanzu Mission Control is an on-premises VMware Tanzu® Mission Control™ integrated into VMware Cloud Director®. Tenant users can consume VMware Tanzu Mission Control functionality using VMware Cloud Director, and VMware Cloud Director® Container Service Extension™ in a multi-tenant way.

Service providers who offer Kubernetes Infrastructure as a Service to run container workloads in a multi-tenant environment using VMware Cloud Director Container Service Extension can now centrally manage their Kubernetes clusters, and apply IT policies seamlessly using VMware Cloud Director Extension for VMware Tanzu Mission Control.The following diagram details the how service providers and tenant users can consume VMware Cloud Director Extension for VMware Tanzu Mission Control, and how it interacts with supporting products.



VMware Tanzu Mission Control Self-Managed Components
Add-on Installed Components
Provider Administrator
Login
Grafana Login
Tenant TMC User
SSO via OIDC
Login
VMware Cloud Director Portal (Provider)
Solution Add-on Management UI Plugin
VMware Object Storage Extension UI Plugin
Ingress
Ingress
VMware Cloud Director Portal (Tenant)
VMware Cloud Director Container Service Extension
backup/ restore
Manage lifecycle
Upload/ Install
Grafana
Read metrics
Tenant TKG Cluster
Tenant TKG Cluster
...
attach/ detach/ manage
VMware Cloud Director Extension for VMware Tanzu Mission Control ISO
Install
Account Manager
Auth Manager
UI Server
Prometheus
...
VMware Tanzu Mission Control Self-Managed App
Provider TKG Cluster / Namespace tmc-local
Solutions OVDC / Landing Zone
Tenant OVDC
Push images
Install
Provider Harbor Registry
VMware Tanzu Mission Control RDE
VMware Tanzu Mission Control Global Roles
VMware Tanzu Mission Control Rights & Rights Bundle
OIDC Relying Party
VMware Cloud Director Server
Pull images

Tenant User Roles

When VMware Cloud Director Extension for VMware Tanzu Mission Control is published to your organization, two roles are available for users. These roles are specific to VMware Cloud Director Extension for VMware Tanzu Mission Control, and users should be assigned the appropriate role depending on their interaction with the service. When you are assigned one of these roles, you can access VMware Tanzu Mission Control services directly through the Kubernetes Container Clusters UI plugin in VMware Cloud Director.

> **NOTE**
> Service providers can customize the name of these roles during VMware Cloud Director Extension for VMware Tanzu Mission Control installation. Ensure you check the value you should use for each role with your service provider.

It is the responsibility of tenant administrators to assign either the**TMC Administrator** or**TMC Member** user roles to members of their organization, depending on their interaction with VMware Cloud Director Extension for VMware Tanzu Mission Control. For instructions to assign these roles to tenant users, see Assign User Roles.

Global Role	Default Value	Rights	Mapped Role in VMware Tanzu Mission Control
TMC Administrator	**tmc:admin**	• **VIEW: VMWARE:TMC** • Enable OIDC Server • Inherited rights from existing**Kubernetes Cluster Author Role** in VMware Cloud Director. • Inherited rights from existing**Organization Administrator** role in VMware Cloud Director.	Service Admin
TMC Member	**tmc:member**	• **VIEW: VMWARE:TMC** • Enable OIDC Server • Inherited rights from existing**Kubernetes Cluster Author Role** in VMware Cloud Director.	Service Member

For more information on VMware Tanzu Mission Control roles, see `Access Control` in the `VMware Tanzu Mission Control Concepts` documentation.

> **NOTE**
> Ensure VMware Cloud Director tenant users have the `fullname` populated in the user object for VMware Tanzu Mission Control Self-Managed login to work correctly. The `email` may be used to create per-user access policies but is not required.

NOTE
By default,**TMC Administrator** users cannot view or manage VMware Tanzu Mission Control attachable clusters from the VMware Cloud Director UI. Additional rights like**Administrator View: VMWARE:CAPVCDCLUSTER** and/or**Administrator Full Control: VMWARE:CAPVCDCLUSTER** are necessary for this user to manage those clusters. However, the**TMC Administrator** user can manage all these clusters from VMware Tanzu Mission Control portal.

Assign User Roles

It is the responsibility of tenant administrators to assign either the **TMC Administrator** or **TMC Member** user roles to members of their organization, depending on their interaction with VMware Cloud Director Extension for VMware Tanzu Mission Control.

1. Log in to VMware Cloud Director tenant portal, and click **Administration › Users**.
2. From the list of users, select a user, and click **Edit**.
3. In the **Edit User** window, from the **Available Roles** list, select **tmc:admin**, **tmc:member**, or the customized role names your service provider may have generated during VMware Cloud Director Extension for VMware Tanzu Mission Control installation.
4. Click **Save**.

TMC Administrator Advice

After the tenant administrator in your organization assigns the**TMC Administrator** role to you, and you have access to VMware Cloud Director Extension for VMware Tanzu Mission Control, it is necessary to perform the steps outlined in this section before users with the**TMC Member** role can use the service.

- Login to the VMware Tanzu Mission Control portal to initialize onboarding for the organization.
- **TMC Member** users have to select a cluster group at the time of cluster attachment to VMware Tanzu Mission Control. If they choose **Default**, other users from the same organization can access the cluster from the VMware Tanzu Mission Control portal. To avoid this, you can create isolated/user-specific cluster groups for your**TMC Member** users. This extra-level isolation ensures higher security for clusters. For detailed instructions, see *Create a Cluster Group* in the *Using VMware Tanzu Mission Control* documentation.
- You can reference VMware Cloud Director users and roles in the VMware Tanzu Mission Control access policies. For more information on VMware Tanzu Mission Control roles, see *Access Control* in the *VMware Tanzu Mission Control Concepts* documentation.
  - **Groups:** Reference the full VMware Cloud Director role name to be assigned to the policy.
  - **Users:** Reference the email address for the VMware Cloud Director user to be assigned to the policy. You can use the **username** field if the user does not have an email address associated with their user.

Cluster Requirements

To ensure that a cluster is attachable or detachable, it is necessary to have at least the following cluster sizing configuration.

Table 5: Minimal Cluster Sizing

Parameter	Detail
Control Plane	
Number of Nodes	1
Sizing Policy	TKG Small
Worker Pool	

Table continued on next page

Continued from previous page

Parameter	Detail
Number of Nodes	2
Sizing Policy	TKG Small

For more information, see VMware Tanzu Mission Control Documentation for *`Requirements for Registering a Tanzu Kubernetes Cluster with Tanzu Mission Control`*.

The above sizing policy definitions are created by VMware Cloud Director Container Service Extension. To learn more about these sizing policies, see Add Tanzu Kubernetes Grid VM Sizing Policies to Organization Virtual Data Centers.

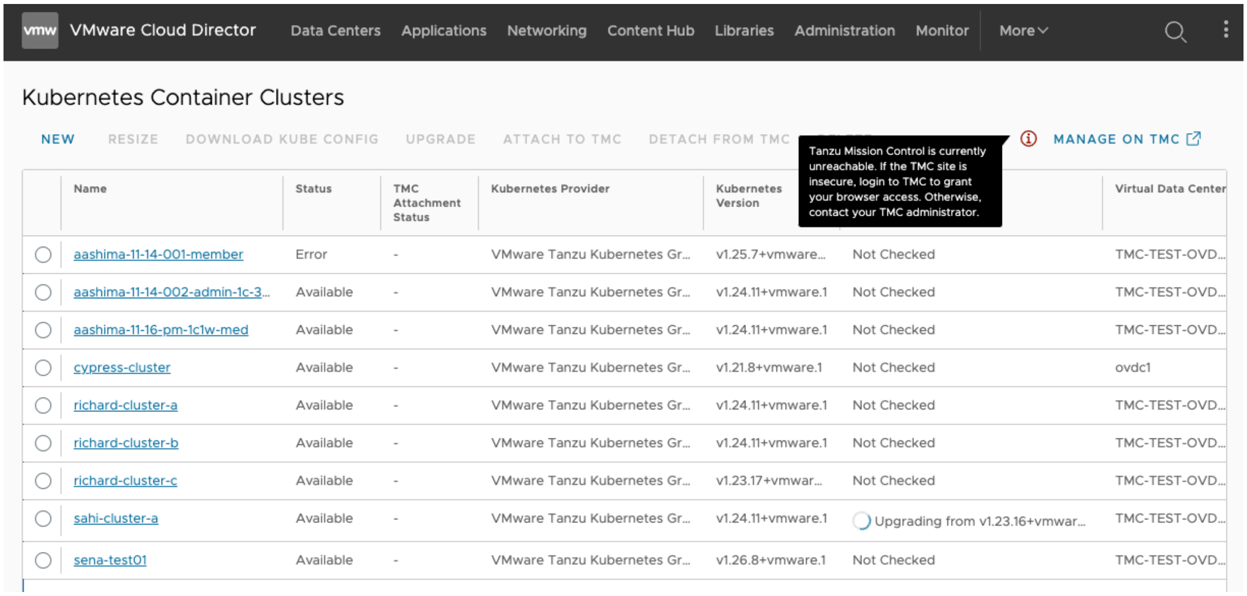
Manage on TMC

You can manage VMware Cloud Director Container Service Extension clusters through the VMware Tanzu Mission Control portal. You can access the VMware Tanzu Mission Control portal directly from the Kubernetes Container Clusters UI, through the **Manage on TMC** button.

> **NOTE**
> To attach clusters to VMware Tanzu Mission Control, see Attach a Cluster and Attach an Existing Cluster.

1. Log in to VMware Cloud Director, click **More › Kubernetes Container Clusters**.
2. In the **Kubernetes Clusters** tab, click **Manage on TMC**.

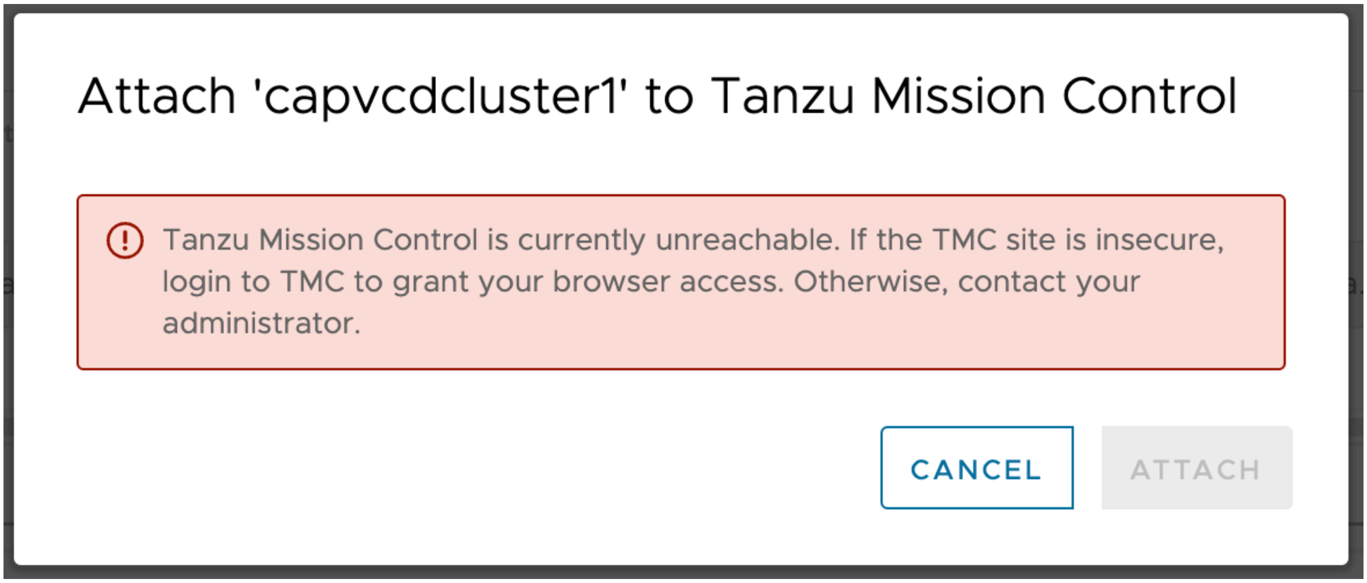
   NOTE
   If you see a warning circle next to the **Manage on TMC** button, allow your browser to trust it.

   Tanzu Mission Control is currently unreachable. If the TMC site is insecure, login to TMC to grant your browser access. Otherwise, contact your TMC administrator.

	Name	Status	TMC Attachment Status	Kubernetes Provider	Kubernetes Version		Virtual Data Center
○	aashima-11-14-001-member	Error	-	VMware Tanzu Kubernetes Gr...	v1.25.7+vmware...	Not Checked	TMC-TEST-OVD...
○	aashima-11-14-002-admin-1c-3...	Available	-	VMware Tanzu Kubernetes Gr...	v1.24.11+vmware.1	Not Checked	TMC-TEST-OVD...
○	aashima-11-16-pm-1c1w-med	Available	-	VMware Tanzu Kubernetes Gr...	v1.24.11+vmware.1	Not Checked	TMC-TEST-OVD...
○	cypress-cluster	Available	-	VMware Tanzu Kubernetes Gr...	v1.21.8+vmware.1	Not Checked	ovdc1
○	richard-cluster-a	Available	-	VMware Tanzu Kubernetes Gr...	v1.24.11+vmware.1	Not Checked	TMC-TEST-OVD...
○	richard-cluster-b	Available	-	VMware Tanzu Kubernetes Gr...	v1.24.11+vmware.1	Not Checked	TMC-TEST-OVD...
○	richard-cluster-c	Available	-	VMware Tanzu Kubernetes Gr...	v1.23.17+vmwar...	Not Checked	TMC-TEST-OVD...
○	sahi-cluster-a	Available	-	VMware Tanzu Kubernetes Gr...	v1.24.11+vmware.1	Upgrading from v1.23.16+vmwar...	TMC-TEST-OVD...
○	sena-test01	Available	-	VMware Tanzu Kubernetes Gr...	v1.26.8+vmware.1	Not Checked	TMC-TEST-OVD...

   You may also see a similar warning at the time of cluster attachment. Allow your browser to trust VMware Tanzu Mission Control.



Attach 'capvcdcluster1' to Tanzu Mission Control

Tanzu Mission Control is currently unreachable. If the TMC site is insecure, login to TMC to grant your browser access. Otherwise, contact your administrator.

3. Sign in to the VMware Tanzu Mission Control portal, and manage or view your clusters.

   NOTE
   It is not recommended to attach clusters directly through the VMware Tanzu Mission Control portal, as this can result in ambigous behavior, such as naming conflicts.

Detach a Cluster

You can detach a VMware Cloud Director Container Service Extension cluster from VMware Tanzu Mission Control directly through the Kubernetes Container Clusters UI plugin. When you detach a cluster, VMware Tanzu Mission Control stops managing the cluster as the VMware Tanzu Mission Control agent is removed.

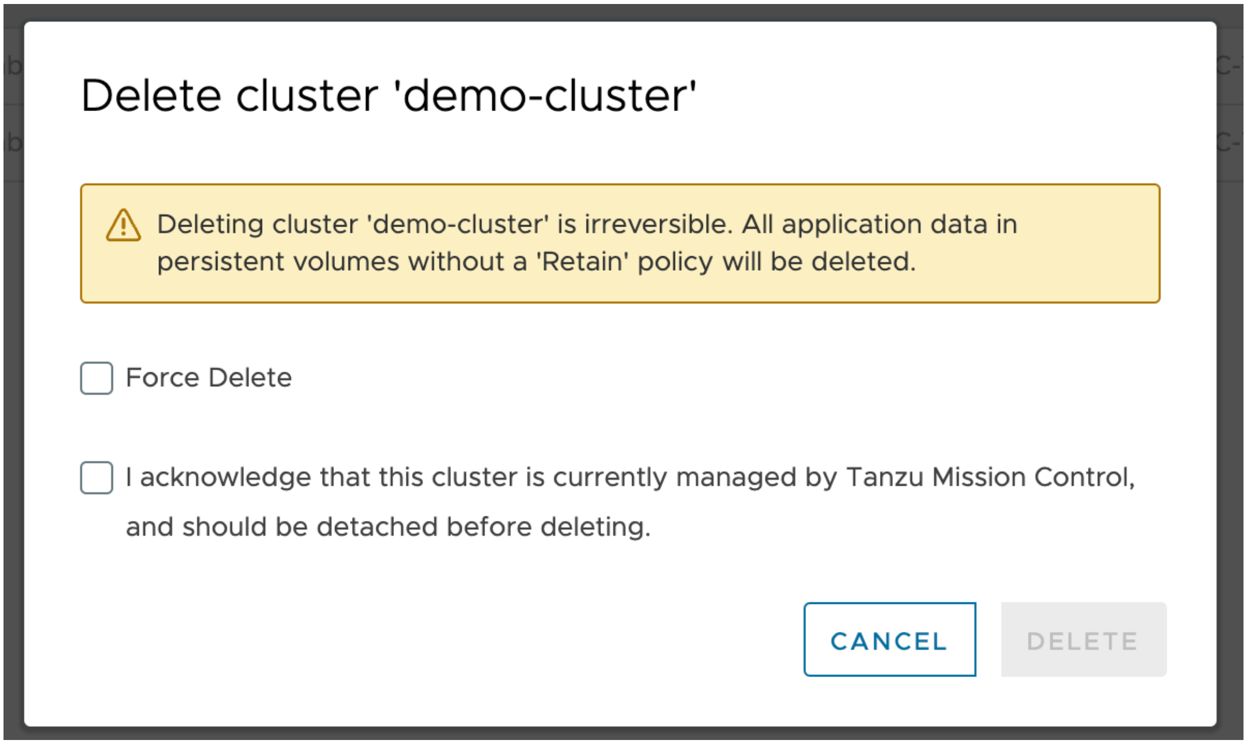
To detach a cluster after it is created, complete the following steps:

1. Log in to VMware Cloud Director, click **More › Kubernetes Container Clusters**.
2. In the **Kubernetes Clusters** tab, in the datagrid, click on the name of the cluster you want to detach, and click **Detach from TMC**.
3. In the **Detach** cluster window, select the checkbox if you want to detach the cluster from VMware Tanzu Mission Control without stopping the VMware Tanzu Mission Control agent running on the cluster.

   NOTE
   If you select this option, the VMware Tanzu Mission Control agent should be manually removed later based on VMware Tanzu Mission Control guidelines. For detailed instructions, see *Remove a Cluster from Your Organization* in the *Using VMware Tanzu Mission Control* documentation.

4. Click **Detach**.

NOTE
When you attempt to delete a cluster and the cluster is still attached to VMware Tanzu Mission Control, the Kubernetes Container Clusters UI reminds you to detach the cluster before you delete it.
If you do not detach a cluster before you delete it in the Kubernetes Container Clusters UI, you may see a stranded entry for that cluster in VMware Tanzu Mission Control.



Delete cluster 'demo-cluster'

⚠ Deleting cluster 'demo-cluster' is irreversible. All application data in persistent volumes without a 'Retain' policy will be deleted.

☐ Force Delete

☐ I acknowledge that this cluster is currently managed by Tanzu Mission Control, and should be detached before deleting.

Documentation Legal Notice

Information about the documentation legal notice.

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

vmware®

by Broadcom