

Revamping of Digital Architecture & Application Modernization

TKGs Learning Document

Sept 2024

**Content**

[1. Introduction 4](#_Toc180075831)

[1.1 Purpose 4](#_Toc180075832)

[1.2 Intended Audience 4](#_Toc180075833)

[1.3 Document Control 4](#_Toc180075834)

[1.4 Abbreviations 4](#_Toc180075835)

[2. Issues 4](#_Toc180075836)

[2.1 Supervisor upgrade issue 4](#_Toc180075837)

[2.1.1 Issue Description: 4](#_Toc180075838)

[2.2 Upgrading Workload Cluster 5](#_Toc180075839)

[2.2.1 Issue Description: 5](#_Toc180075840)

[2.3 Failed to attach disk to VM 6](#_Toc180075841)

[2.3.1 Issue Description: 6](#_Toc180075842)

[2.4 Administrator access Requirement 6](#_Toc180075843)

[2.4.1 Issue Description: 6](#_Toc180075844)

[2.5 DNS Profile is not supported in AVI essential license. 6](#_Toc180075845)

[2.5.1 Issue Description: 6](#_Toc180075846)

[2.6 VMware network Switch hostname 7](#_Toc180075847)

[2.6.1 Issue Description: 7](#_Toc180075848)

[2.7 TKR verson 1.27. is not supported on vcenter 8.0.2b 7](#_Toc180075849)

[2.7.1 Issue Description: 7](#_Toc180075850)

[2.8 TCP 443 port enablement supervisor cluster 7](#_Toc180075851)

[2.8.1 Issue Description: 7](#_Toc180075852)

[2.9 Port enablement between supervisor and Workload cluster 7](#_Toc180075853)

[2.9.1 Issue Description: 7](#_Toc180075854)

[2.10 Ports 6443 required to be opened between VIP/Data vLan and Workload vLan 7](#_Toc180075855)

[2.10.1 Issue Description: 7](#_Toc180075856)

[2.11 API server is unable to connect to Vcenter 8](#_Toc180075857)

[2.11.1 Issue Description: 8](#_Toc180075858)

[3. Issue Resolution 8](#_Toc180075859)

[3.1 Supervisor upgrade issue Resolution 8](#_Toc180075860)

[3.1.1 Resolution Summary: 8](#_Toc180075861)

[3.2 Upgrading Workload Cluster 8](#_Toc180075862)

[3.2.1 Resolution Summary: 8](#_Toc180075863)

[3.3 Failed to attach disk to VM 9](#_Toc180075864)

[3.3.1 Resolution Summary: 9](#_Toc180075865)

[3.4 Administrator Access Requirement 10](#_Toc180075866)

[3.4.1 Resolution Summary: 10](#_Toc180075867)

[3.5 DNS profile is not supported in AVI essential license 11](#_Toc180075868)

[3.5.1 Resolution Summary: 11](#_Toc180075869)

[3.6 VMware Network Switch hostname 11](#_Toc180075870)

[3.6.1 Resolution Summary 11](#_Toc180075871)

[3.7 TKR verson 1.27.11 is not supported on vcenter 8.0.2b 11](#_Toc180075872)

[3.7.1 Resolution Summary 11](#_Toc180075873)

[3.8 TCP 443 port enablement supervisor cluster 12](#_Toc180075874)

[3.8.1 Resolution Summary 12](#_Toc180075875)

[3.9 Ports enablement between supervisor and workload cluster nodes. 12](#_Toc180075876)

[3.9.1 Resolution Summary 12](#_Toc180075877)

[3.10 Ports 6443 required to be opened between VIP/Data vLan and Workload vLan. 13](#_Toc180075878)

[3.10.1 Resolution Summary 13](#_Toc180075879)

[3.11 API server is unable to connect to vcenter 13](#_Toc180075880)

[3.11.1 Resolution Summary 13](#_Toc180075881)

# Introduction

## Purpose

This document serves to provide a comprehensive overview of the issues encountered during the installation and upgrade of **Tanzu Kubernetes Grid (TKG)** within **Bank of Baroda (BoB) environment**. It also outlines the corresponding resolutions for these issues.

## Intended Audience

Following stakeholders are the targeted audience for this artifact:

* Platform Lead
* Delivery Leads
* Integration team

## Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Contributor (s) | Changes |
| 0.1 | Sept 23, 2024 | Umesh Yadav | Initial draft based on the Installation and Upgradation Issues |
| 02 | Nov 2024 | Umesh Yadav | Intended Audience, Abbreviations and few Issues have been updated. |
|  |  |  |  |

## Abbreviations

|  |  |  |
| --- | --- | --- |
| No. | Abbreviation | Description |
| 1 | BoB | Bank of Baroda |
| 2 | TKR | Tanzu Kubernetes Release |
| 3 | VDS | Vsphere Distributed Switch |
| 4 | CAPI | Cluster API |
| 5 | GSLB | Global Server Load Balancing |
|  |  |  |
|  |  |  |

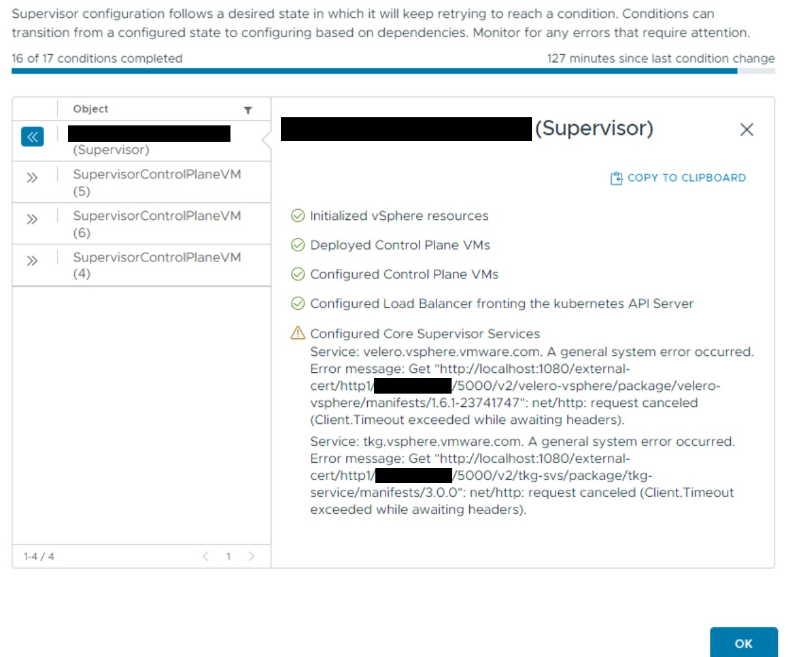
# Issues

## 2.1 Supervisor upgrade issue

### 2.1.1 Issue Description:

After updating Supervisor Services on vCenter 8.0 Update 3, configuration remains stuck at **"Configured Core Supervisor Services"**

**For Resolution refer section:** [**3.1 Supervisor upgrade issue Resolution**](#_3.1_Supervisor_upgrade)



* When checking details of the update process, at least one of the following error messages can be seen:  
  (**172.16.90.213** the virtual IP of the Supervisor Cluster)
* The network communication on TCP/5000 is blocked/not working between vCenter Server and the Supervisor Cluster.

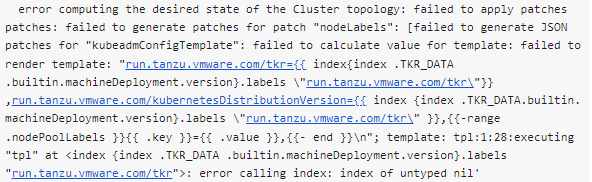
## Upgrading Workload Cluster

### 2.2.1 Issue Description:

Upgrade the workload cluster from tkr version 1.26.13 to 1.27.11

While workload cluster upgrade using tkr version below error was arising.

**For Resolution refer section: 3.2** [**Upgrading Workload Cluster**](#_Upgrading_Workload_Cluster)

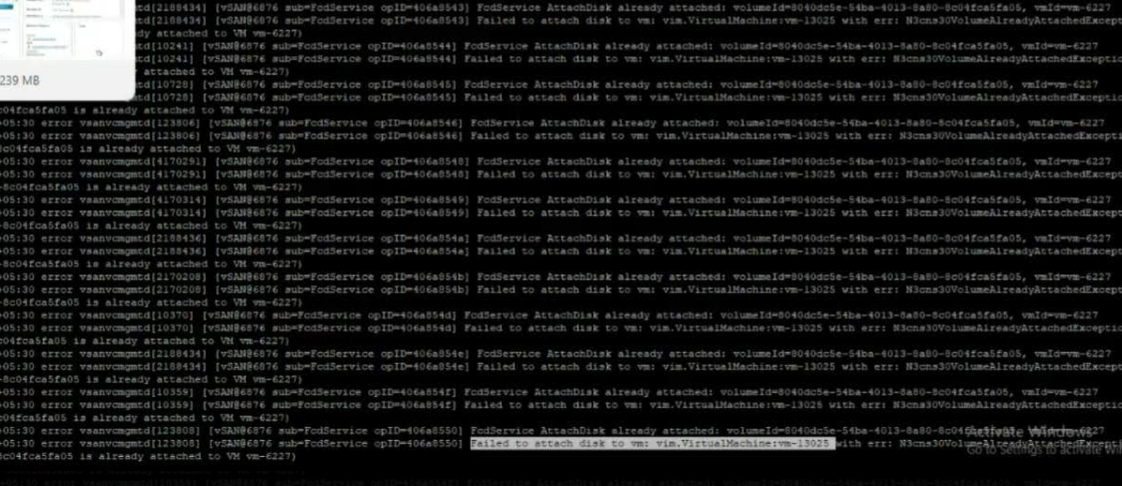


## 2.3 Failed to attach disk to VM

### 2.3.1 Issue Description:

We identified in the **vsanvcmgmt.log** that there was a recurring error when attaching the volume. Kubernetes scheduled the pod to the worker node **pktr8**, but the volume attachment always failed with the following error

**For Resolution refer section:** [**3.3 Failed to attach disk to VM**](#_3.3_Failed_to)



## 2.4 Administrator access Requirement

### 2.4.1 Issue Description:

Administrator access required to deploy Supervisor clusters on vsphere.

Without the necessary privileges, the deployment process may fail, resulting in incomplete installations or misconfigurations of the Supervisor Cluster.

**For Resolution refer section:** [**3.4 Administrator Access Requirement**](#_3.4_Administrator_Access)

## 2.5 DNS Profile is not supported in AVI essential license.

### 2.5.1 Issue Description:

Without support for DNS Profile in the Essential License, you won't be able to use DNS-based features for traffic management. This includes advanced DNS health checks, intelligent routing based on DNS records, and other DNS-based load balancing techniques.

**For Resolution refer section:** [**3.5 DNS profile is not supported in AVI essential license**](#_3.5_DNS_profile)

## 2.6 VMware network Switch hostname

### 2.6.1 Issue Description:

Hostname of the VMware network switch (VDS) should be in the small letter, AVI LB recognize the VDS in small letter.

If the VDS hostname includes uppercase letters, AVI LB may fail to identify the switch, causing issues in network traffic management and load balancing operations.

**For Resolution refer section:** [**3.6 VMware Network Switch hostname**](#_3.6_VMware_Network)

## 2.7 TKR verson 1.27. is not supported on vcenter 8.0.2b

### 2.7.1 Issue Description:

If Tanzu Kubernetes Release (TKR) version **1.27** is not supported on **vCenter 8.0.2b**, it means that this specific combination has compatibility issues, which can lead to potential problems in deploying or managing Kubernetes clusters on the VMware environment.

**For Resolution refer section:** [**3.7 TKR verson 1.27.11 is not supported on vcenter 8.0.2b**](#_3.7_TKR_verson)

## 2.8 TCP 443 port enablement supervisor cluster

### 2.8.1 Issue Description:

TCP port 443 should be open bidirectional between the Supervisor Cluster, TKG Workload Cluster, and the vCenter server.

This port is the standard for **HTTPS traffic**, used for secure communication between various systems. In a VMware environment, port 443 is critical for enabling secure data exchange between components such as the vCenter server, Supervisor Cluster, and TKG Workload Cluster.

**For Resolution refer section:** [**3.8 TCP 443 port enablement supervisor cluster**](#_3.8_TCP_443)

## 2.9 Port enablement between supervisor and Workload cluster

### 2.9.1 Issue Description:

Without ports 6443 and 443 open, the communication between supervisor nodes and workload nodes will be hindered, resulting in delays or failures in deploying applications and managing workloads

**For Resolution refer section:** [**3.9 Ports enablement between supervisor and workload cluster nodes.**](#_3.9_Ports_enablement)

## 2.10 Ports 6443 required to be opened between VIP/Data vLan and Workload vLan

### 2.10.1 Issue Description:

Port **6443** is the standard port used for communication with the Kubernetes API server. If this port is not open between the VIP/Data VLAN and the Workload VLAN, Kubernetes components and tools like kubectl will not be able to communicate with the API server.

**For Resolution refer section:** [**3.10 Ports 6443 required to be opened between VIP/Data vLan and Workload vLan.**](#_3.10_Ports_6443)

## 2.11 API server is unable to connect to Vcenter

### 2.11.1 Issue Description:

* If the **vpxd service** on the vCenter server fails or is not running, the API server cannot establish a connection to vCenter.
* This service failure means that the API requests sent to vCenter are not processed, resulting in the inability to manage or retrieve information about the virtual environment.

**For Resolution refer section:** [**3.11 API server is unable to connect to vcenter**](#_3.11_API_server)

# 3. Issue Resolution

## 3.1 Supervisor upgrade issue Resolution

### 3.1.1 Resolution Summary:

Allow network communication between vCenter Server to the virtual/shared IP of the Supervisor Cluster via TCP/5000, where the container registry is running on. During the next configuration attempt, the issue should be solved.

## Upgrading Workload Cluster

### 3.2.1 Resolution Summary:

First, we stop CAPI and tkg package reconcile to allow disable capi validation webhook temporarily.

|  |
| --- |
| kubectl patch pkgi [svc-tkg.vsphere.vmware.com](http://svc-tkg.vsphere.vmware.com/) -n vmware-system-supervisor-services --type merge -p '{"spec":{"paused":true}}'  kubectl patch pkgi tanzu-cluster-api -n {your-namespace} --type merge -p '{"spec":{"paused":true}}' |

**Disable capi validation webhook temporally to allow downgrading workaround**

* 1. **backup capi validating webhook, delete it, then patch cluster object, add capi validating webhook back.**

kubectl get validatingwebhookconfigurations capi-validating-webhook-configuration -o yaml >  capi-validating-webhook-configuration.yaml

kubectl delete validatingwebhookconfigurations capi-validating-webhook-configuration

* 1. **Edit the cluster and downgrade the k8s version**
  2. **Add the webhook back**

     kubectl apply -f capi-validating-webhook-configuration.yaml

* 1. **Remove the resourceVersion from the metadata.annotation line.**

kubectl edit validatingwebhookconfigurations capi-validating-webhook-configuration

Using below steps we then updated the cluster to 1.27

<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-with-tanzu-tkg/GUID-EB911F21-B1C5-4C3C-9023-E37F8CFBF013.html>

Nodes then started to be provisioned and the cluster upgraded.

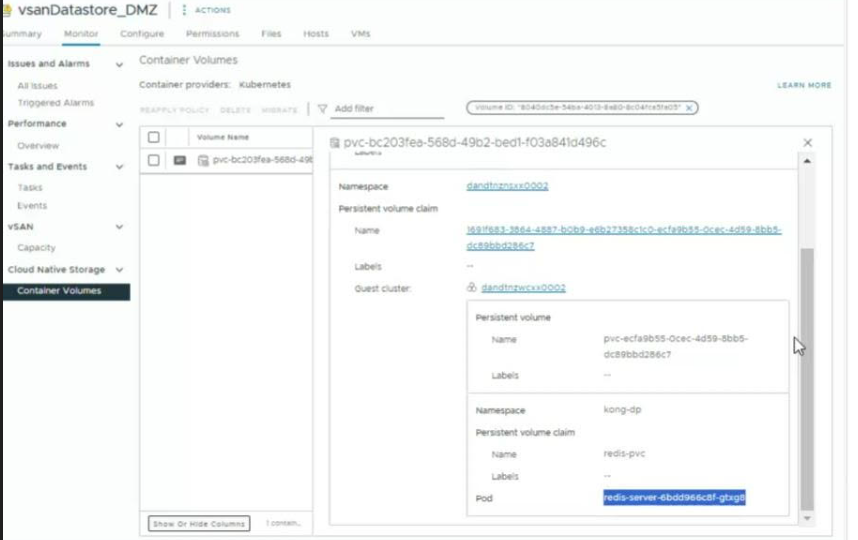
## 3.3 Failed to attach disk to VM

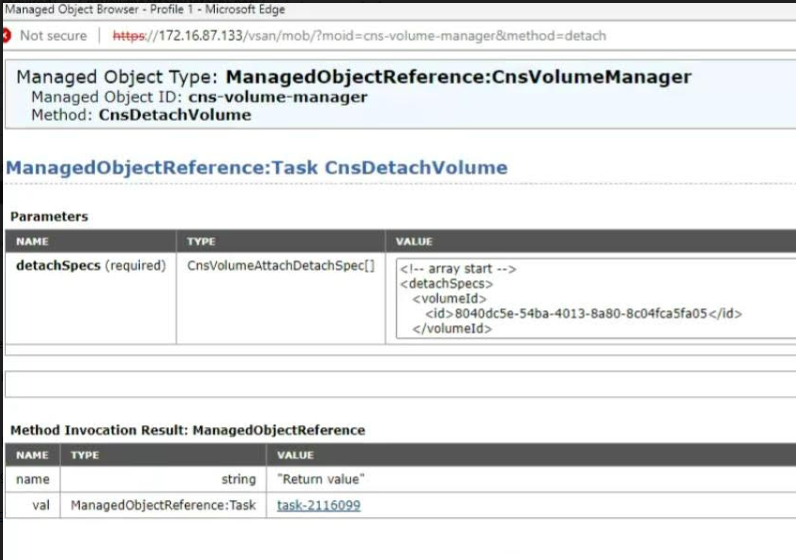
### 3.3.1 Resolution Summary:

<https://knowledge.broadcom.com/external/article/320774/fcdservice-attachdisk-already-attached-e.html>

So we followed the above steps

We managed to successfully detach the volume from the node.





we identified this as volume and it matched the new redis pod.

## 3.4 Administrator Access Requirement

### 3.4.1 Resolution Summary:

Created TKG\_ADMINISTRATOR user with all admin access.

Supervisor Clusters on vSphere typically requires administrative privileges due to the infrastructure-level configurations and permissions needed for setting up and managing Kubernetes clusters. However, there are ways to work around administrative requirements by using **Role-Based Access Control (RBAC)** and appropriate **delegation of permissions** in vSphere

## 3.5 DNS profile is not supported in AVI essential license

### 3.5.1 Resolution Summary:

This is not required for our environment as it operates on L4, as confirmed by VMware Team, So this option was not selected

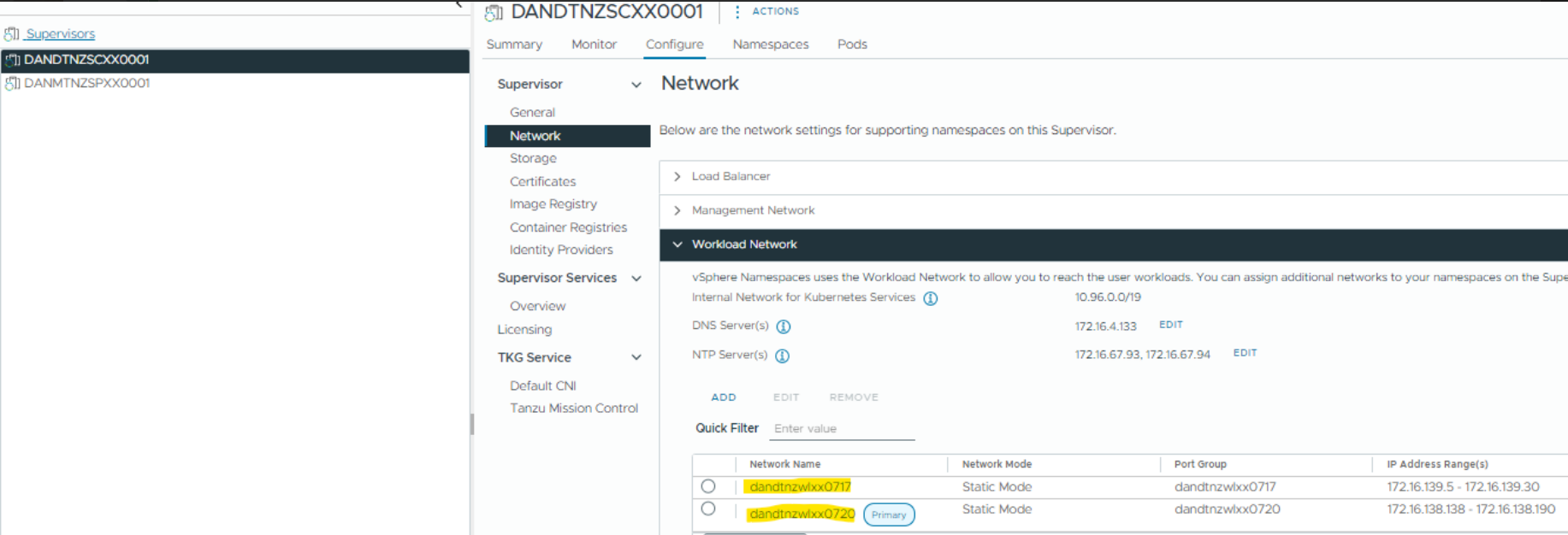
* Features like Global Server Load Balancing (GSLB), which rely on DNS-based load balancing, are typically not available.
* The ability to create and manage DNS profiles to perform load balancing using DNS queries is also excluded

## 3.6 VMware Network Switch hostname

### 3.6.1 Resolution Summary

Updated the VDS name in small letter from the CAPITAL.

The **hostname** of the **vSphere Distributed Switch (VDS)** must be written in **lowercase** because the AVI Load Balancer recognizes and references VDS in **small letters**. If the hostname of the VDS is in uppercase or mixed case, AVI LB might not properly recognize or associate with the VDS, leading to issues during configuration or deployment.

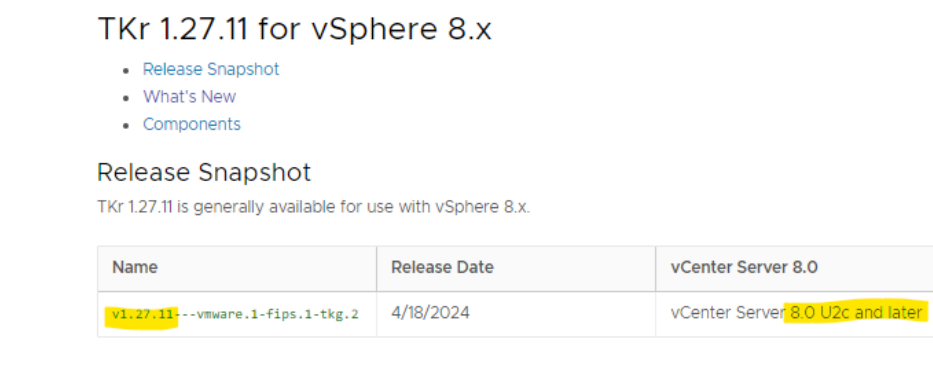


## 3.7 TKR verson 1.27.11 is not supported on vcenter 8.0.2b

### 3.7.1 Resolution Summary

TKR version 1.26.13 is supported, so this version is installed. Will deploy TKR version 1.27.11 when vCenter will upgrade to 8.2c or 8.3

The **Tanzu Kubernetes Release (TKR) version 1.27** not being supported on **vCenter 8.0.2b** could be due to compatibility issues between the specific **TKR version** and the **vSphere with Tanzu** version.



## 3.8 TCP 443 port enablement supervisor cluster

### 3.8.1 Resolution Summary

Created a new request to open the port Bi-directonal.

To ensure proper communication within your **VMware Tanzu Kubernetes Grid (TKG)** environment, it is essential that **TCP port 443** is open for **bidirectional traffic** between the following components:

1. **Supervisor Cluster** ↔ **vCenter Server**
2. **TKG Workload Cluster** ↔ **vCenter Server**
3. **Supervisor Cluster** ↔ **TKG Workload Cluster**

## 3.9 Ports enablement between supervisor and workload cluster nodes.

### 3.9.1 Resolution Summary

Created a new request to open the ports.

To ensure smooth communication, make sure that **TCP port 443** is open in both directions between:

* The **Supervisor Cluster** and the **vCenter Server**.
* The **TKG Workload Clusters** and the **vCenter Server**.
* The **Supervisor Cluster** and **TKG Workload Clusters**.

## 3.10 Ports 6443 required to be opened between VIP/Data vLan and Workload vLan.

### 3.10.1 Resolution Summary

Created a new request to open the ports.

API interactions between the **VIP/Data VLAN** and the **Workload VLAN**.

## 3.11 API server is unable to connect to vcenter

### 3.11.1 Resolution Summary

 vpxd service was restarted on the vCenter and issue was resolved.

The **vpxd service** (vCenter Server service) is responsible for handling all management tasks within the **vCenter Server**, including virtual machine provisioning, cluster management, and interaction with **ESXi hosts**.