

Provider workflows for CSE Beta for Cloud Providers

The below document describes Enabling CSE Beta for Cloud Providers during the Beta Program.

Setup Solution Org:

- The purpose of the solution organization is to host provider solutions such as Container service extension. The provider admin can host the Container service extension in the solution org, create and shared Catalog and upload Tanzu Kubernetes Grid Kubernetes OVAs.
- Networking pre-requisites:
- Provider/system admin can create an Edge gateway, a routed network to connect the container service extension server.
- For proper function of CSE Server, please allow access of CSE Server to VCD API End point (please consider Load Balancer configuration of VCD cells, in case you have External IP/Service IP for multiple VCD Cells). This also means, to create Edge firewall rules to allow traffic from CSE server to VCD API Endpoint IP address.
- Upload Tanzu Kubernetes Grid Templates
- Provider/system admin creates a catalog to upload TKG OVAs. Please download following two OVAs from the VMware Customer Service Portal. Please note for this beta program only following two TKG OVA's are supported.
 1. [ubuntu-2004-kube-v1.22.9+vmware.1-tkg.1-2182cbabee08edf480ee9bc5866d6933.ova](https://customerconnect.vmware.com/en/downloads/details?downloadGroup=TKG-142&productId=988&rPId=65946ed3c93616a02968be452fe1934a1d37c)
 2. [ubuntu-2004-kube-v1.21.8+vmware.1tkg.2https://customerconnect.vmware.com/en/downloads/details?downloadGroup=TKG-142&productId=988&rPId=65946ed3c93616a02968be452fe1934a1d37c.ova](https://customerconnect.vmware.com/en/downloads/details?downloadGroup=TKG-142&productId=988&rPId=65946ed3c93616a02968be452fe1934a1d37c)

Sizing Policy for Control plane and Worker plane VMs for TKG Clusters:

Provider/system admin must create sizing policies based on Standard TKG VM sizing definition for the customer's Kubernetes workload clusters. (Reference link - <https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmwaretanzuhttps://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmwaretanzu-kubernetes-grid-15/GUID-mgmt-clusters-config-vsphere.htmlkubernetesgrid-15/GUID-mgmt-clusters-config-vsphere.html>) Below Table shows

sizing guidelines to create TKG cluster sizing policy. The recommended practice is to choose a default sizing policy for tenant VDCs. Disk sizes are not considered while creating sizing policy on VMware Cloud Director provider portal.

Size name	CPU/Memory
Small	2 CPU, 4 GB RAM
Medium	2 CPU, 8 GB RAM
Large	4 CPU, 16 GB RAM
Extra Large	8 CPU, 32 GB RAM

- Register RDE Entity Types

Provider/system admin must define and create new entity types for Beta.

Please use following API call using POSTMAN or API Explorer on VCD: Download the payload files from [this location](#):

- VCDKE Config Entity Type

- Create an interface to create VCD KE RDE using following API call:

POST <https://{{vcd}}/cloudapi/1.0.0/interfaces>

API URL Body:

```
{  
    "name": "VCDKEConfig",  
    "version": "0.5.0",  
    "vendor": "vmware",  
    "nss": "VCDKEConfig"  
}
```

- The instance created by this API URL serves as CSE Server Configuration. Please find the Payload for this API call from the CSE Beta Document titled as: VCDKE Config Entity.

API URL:

POST <https://{{vcd}}/cloudapi/1.0.0/entityTypes>

- CAPVCD Cluster Entity Type

- The instance created by this API URL represents the tenant cluster in the VCD. Please find API Payload from CSE Beta Document titled as CAPVCD Entity Type.

API URL:

POST <https://{{vcd}}/cloudapi/1.0.0/entityTypes>

VCDKE Config Instance

- The API URL is as follows: Please find the Payload for this API call from the CSE Beta Document titled as: VCDKE Config RDE API URL:

POST <https://{{vcd}}/cloudapi/1.0.0/entityTypes/urn:vcloud:type:vmware:VCDKEConfig:0.5.0>

For this POST Action, please modify following Key, values to match your VCD Environment:
Payload Section:

```
"vcdConfig":{  
  "serviceAccount":{  
    "site":"https://atl1-vcd-static-128-7.eng.vmware.com",  
    "userOrgName":"system",  
    "password":"sysadmin password",  
    "username":"service-acct",  
    "refreshToken":""  
  }  
},
```

Key, Values to Change. Please refrain from changing any other values in the section.

```
"site":"<your VCD API Endpoint URL>",  
"username":"administrator<your sysadmin username>",  
"password":"<sysadmin password>",
```

Resolve RDE Instance by executing following API:

GET <https://{{vcd}}/cloudapi/1.0.0/entities/types/vmware/VCDKEConfig/0.5.0>
// retrieve id of the first element

POST <https://{{vcd}}/cloudapi/1.0.0/entities/<id>/resolve>

- Start CSE Server:
- Download CSE Server from CSE Beta Download Page in the provider/solution or created in the first step.
 - a. Power on/Instantiate CSE Server. Input system administrator credentials when prompted for CSE service account (Note that CSE service account role will have a limited set of privileges for GA).These are same credentials used in the VCD KE

API Call in previous step. The below screenshot showcases input of the VCD credentials while setting up the CSE server from the OVA.

Create a vApp from an OVF file

- 1 Select Source
- 2 Review Details
- 3 Select vApp Name
- 4 Configure Resources
- 5 Configure Networking
- 6 Custom Properties**
- 7 Customize Hardware
- 8 Network Mapping
- 9 Ready to Complete

Custom Properties

CSE Server Properties

VCD host	https://atl1-vcd-static-128-222.eng.vmware.com
CSE service account username	administrator
CSE service account password	ca\$hC0w
CSE service account's org	system

CANCEL PREVIOUS NEXT

- b. Ensure CSE server's vapp network has outbound connectivity.
2. Login to the VM to check if CSE server has started.
 - a. To check the CSE Service status, execute following command `systemctl status cse`
 - b. For troubleshooting purpose, please follow below steps to retrieve VCD KE logs:
 1. Log in to CSE Server and navigate to `~/cse.log` location. OR
 2. Run `journalctl -axel -u cse` (or) `journalctl -b <negative-number>` for the previous boot

This concludes the Provider/Organization setup and running the Container Service Extension service with Cluster API.

3. Tenant setup

Setup customer organization.

- To create TKG clusters from customer organization provider must setup Edge Gateway, Routed Network, enable NSX Advanced Load balancer and allow Outbound internet traffic for TKG Clusters.
- For the created routed network, configure primary, secondary DNS and DNS suffix to ensure successful DNS resolution of outbound traffic.

- Cluster deployments need to happen only in those ovdcs with the routed network on NSX-T. VMs need to be able to access the internet and the VCD API Endpoint. Ensure DNS is set up correctly. Create SNAT rule for the internal IPs if required.
- Note that the clusters are created with load balancer IP(s) chosen from the external IP range specified in the Tier-0 gateway.
- References:
- NSX T Reference documentation - <https://docs.vmware.com/en/VMware-Cloud-Director/9.7/com.vmware.vcloud.install.doc/GUID-A4489E87-0107-4CBF-98BChttps://docs.vmware.com/en/VMware-Cloud-Director/9.7/com.vmware.vcloud.install.doc/GUID-A4489E87-0107-4CBF-98BC-01BDF5C4DDEE.html01BDF5C4DDEE.html>
- NSXT LB with VCD <https://docs.vmware.com/en/VMware-Cloud-Director/10.2/VMware-Cloud-Director-Service-Provider-Admin-PortalGuide/GUID-1D3014BC-4792-40E8-99E1-A8F0FFC691FE.html>

Publish UI plugin

- Download UI plugin from the CSE Beta Downloads page and upload it to VCD Portal and publish it to desired customer organizations.

Publish right bundles and create a global role

- Publish the vmware:capvcdCluster:1.1.0 right bundle to the desired tenant organizations
- Provider needs to edit the default right bundle to add the belowmentioned rights.
 - User > Manage user's own API token
 - vApp > Preserve ExtraConfig Elements during OVA Import and Export (follow the KB to enable this right on VCD)
 - Gateway > View Gateway
 - Gateway Services > NAT Configure, Load Balancer Configure
- Create a global role with the user role 'cluster-Author' and assign these rights to the desired tenant organizations.
 - vApp > Preserve ExtraConfig Elements during OVA Import and Export (follow the [KB](#) to enable this right on VCD, If needed)
 - Rights from the default vApp Author role
 - Right 'Full Control: VMWARE:CAPVCDCLUSTER'
 - Rights required for CPI
 - a. Gateway > View Gateway

- b. Gateway Services > NAT Configure (adds NAT View)
 - c. > Load Balancer Configure (adds Load Balancer View)
 - d. Access Control > User > Manage user's own API TOKEN
- Rights required for CSI
 -
 - a. Access Control > User > Manage user's own API TOKEN
 - b. Organization VDC > Create a Shared Disk

As a best practice, Tenant admins or provider admins need to assign the above created global role capabilities to “cluster author” for the desired users to begin managing cluster deployments”.