

Providers Guide to Container Service Extension Install and Configuration

A Natural Partnership
For Cloud and Service Providers

Sachi Bhatt
Cloud Services Business Unit
February 2021



Table of contents

Introduction	3
CSE Architecture	3
CSE User Roles	3
Container Service Extension Installation Guide	4
1. Prepare VMware Cloud Director/Cloud Director Service with required CSE server network access.....	5
2. Install CSE service	7
3. Enable Tenant to deploy Kubernetes	11
Accessing Kubernetes Cluster:.....	12
Summary	13
Glossary.....	14

Introduction

Container Service Extension (CSE) is an extension/service that allows providers and tenants to deploy upstream Kubernetes Clusters from the VMware Cloud Director portal. With the CSE installed, tenant administrator can deploy and manage the Kubernetes cluster and provide users like dev-ops, and developers access to the Kubernetes cluster to manage and deploy an application. The Container Service Extension can deploy runtimes of Kubernetes cluster with three different options of CSE native, Tanzu Kubernetes Cluster and PKS Ent. When provider administrator selects the CSE native as the Kubernetes runtime, CSE server uses VCD native constructs to deploy Kubernetes clusters. This document covers installation and configuration steps for CSE native mode. This document covers how to install and enable tenant for Kubernetes cluster creation using Container Service extension on VMware Cloud Director (VCD) and Cloud Director service (CDs) on VMware Cloud (VMC on AWS).

CSE Architecture

There are three components on a high level:

- CSE Server
- CSE UI extension on VMware Cloud Director tenant and provider portal
- VCD-CLI plug-in

The CSE Server manages the CSE requests related to the Kubernetes cluster or node create/delete operations and CSE services. The provider uses the CSE client (UI and CLI) to manage the CSE service. The container service CSE has been used with VMware Cloud Director using AMQP till CSE 3.0 version. With CSE 3.0.1 and VCD version 10.2, VCD uses MQTT by replacing AMQP as a communication channel. This enhancement allows the provider to use the CSE extension on the Cloud Director service. The installation steps are updated based on the upgrades offered in CSE 3.0.1.

The detailed architecture is shown on the official CSE website [here](#).

CSE User Roles

The CSE User roles are designed with consideration of modern developer workflows and roles.

Cloud Administrator: The Cloud provider administrator generally serves this role. The role is responsible for installing and managing the CSE server and its configuration files and Kubernetes templates. This user-role is also responsible for enabling the CSE extension for the tenants.

Tenant administrator: The tenant administrator is responsible for creating user-roles for the developers and DevOps roles and creating and managing the Kubernetes clusters.

Dev-ops and developers and other Kubernetes users: These users interact with CSE using the `kubect1` CLI to create/delete Kubernetes clusters. These user roles do not require knowledge of VCD/CSE CLI. The following Figure demonstrates the user flow for a tenant user.

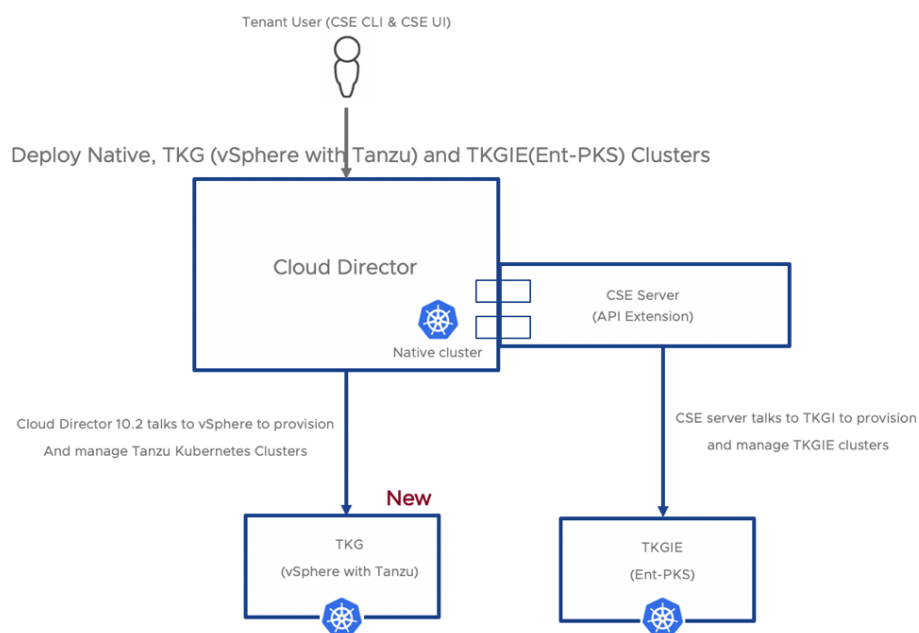


Figure 1 Container Service Extension User flow with VCD

Container Service Extension Installation Guide

This document covers the following Steps for providers to provide Kubernetes-as-services to the customers.

1. Configure CSE Server Network Access
2. Install CSE service
3. Tenant Onboarding

The following table summarizes the required steps on VCD and CDS:

Step	Sub-Step	User role	Configuration point on VMC	Description
1	Edge Gateway -SNAT	Provider admin	CDS/CSE organization	Map Internal Network IP with External Network range in Edge NAT rules table in CSE organization.
1	Firewall rules- CSE- ESXi, VC	Provider admin	VMC SDDC	Management Firewall rules to allow ESXi, VC access on SDDC.
1	Edge Gateway- SNAT for kubernetes templates	Provider admin	CDS/CSE organization	Allow internet access templates while CSE server downloads and customizes K8 templates.
1	Request public IP address	Provider admin	VMC SDDC	Allow Inbound Internet access to CSE server VM.

1	Internet Firewall Rule-CSE server SSH	Provider admin	VMC SDDC	Create Firewall rules to allow incoming SSH traffic to CSE server.
2	Install CSE service	Provider admin	CSE server	(Optional: use Public IP) Install CSE service
3	Tenant Onboarding	Provider admin	CDS/VCD Provider portal	Create rights bundles, Enable Extension for the tenant, etc.

Table 1 Summary of CSE Install, configuration steps and configuration end points

1. Prepare VMware Cloud Director/Cloud Director Service with required CSE server network access

The [white paper](#) explains Networking on Cloud Director Service in detail. The following network diagram shows the topology we will use as a reference for CSE installation and configuration throughout the document:

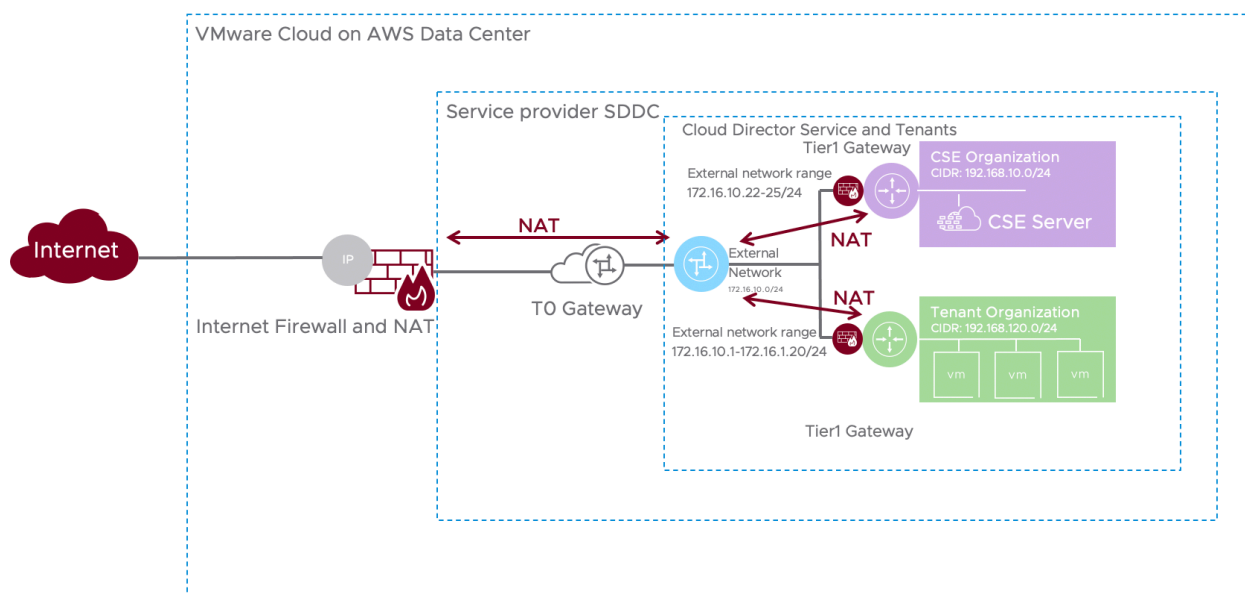


Figure 2 CSE and tenant network connectivity on CDs

Here, the assumption is made that the provider has created VCD Organization, Edge Gateway, Routed network for CSE Server Organization and an internal network for CSE organization with static IP pool. Please follow the steps to configure these network elements from the referenced white paper. Figure 2 describes the topology reference in the configuration steps:

Step 1: Create Edge SNAT rule

VMware Cloud Director | Data Centers | Applications | **Networking** | Libraries | Administration | Monitor | More

All Edge Gateways > CSEEdge

CSEEdge [OPEN IN VDC CONTEXT](#) [DELETE](#)

General

Services

Firewall

NAT

Security

Security Groups

IP Sets

Application Port Profiles

IP Management

IP Allocations

NEW

Name	Category	State	Type	External IP	Application	Internal IP	External Port	Destination IP
Allow Internet DNAT Rule for CSE Server	User defi...	Enabled	DNAT	172.16.10.22	-	192.168.10.1	Any	-
CSE Server SNAT Rule	User defi...	Enabled	SNAT	172.16.10.22	-	192.168.10.1	Any	-

Figure 3 Create SNAT/DNAT rules for the CSE server

Step 2: Create a Firewall rule to allow the CSE server's external network address to connect to the infrastructure ESXi and vCenter servers. By design, the Gateway Firewall rules are whitelisted. Figure 5 exemplifies such firewall rules, where the CSE server Group contains the external network's IP address of the CSE server from Figure 3.

< ALL SDDCs

US West SDDC | VMware Cloud on AWS | US West (Oregon)

[OPEN VCENTER](#) [ACTIONS](#)

Summary | **Networking & Security** | Add Ons | Maintenance | Troubleshooting | Settings | Support

Overview

Network

Segments

VPN

NAT

Tier-1 Gateways

Transit Connect

Security

Gateway Firewall

Distributed Firewall

Inventory

Groups

Gateway Firewall

Management Gateway | Compute Gateway | Tier1 Gateways

[+ ADD RULE](#) [CLONE](#) [UNDO](#) [DELETE](#) [Filter by Name, Path and more](#)

	Name	ID	Sources	Destinations	Services	Action
<input type="checkbox"/>	CSE Server to VC	1022	CSE_Server	vCenter	HTTPS ICMP ALL	Allow
<input type="checkbox"/>	CSE Server to ESXi	1023	CSE_Server	ESXi	HTTPS ICMP ALL	Allow

Figure 4 Management gateway firewall rules to allow communication to vCenter Server and ESXi hosts

The complete CSE server installation process requires downloading and customizing the Kubernetes template. This template customization step requires outbound internet connection. For this reason, create additional SNAT rules matching External network IP address with Internal IP address. The CSE server installation steps will consume these internal IP addresses from the IP pool.

Step 3: Create SNAT rule for Kubernetes templates downloads

The screenshot shows the VMware Cloud Director interface. On the left, the 'Networking' menu is expanded, showing 'Edges' and 'Networks'. The 'CSEEdge' edge is selected. The 'NAT' tab is active under the 'Services' section. A table lists the NAT rules:

Name	Category	State	Type	External IP	Application	Internal IP	External Port	Destination IP	Logging
Allow Internet DNAT Rule for CSE Server	User defined	Enabled	DNAT	172.16.10.22	-	192.168.10.1	Any	-	Disabled
CSE Server SNAT Rule	User defined	Enabled	SNAT	172.16.10.22	-	192.168.10.1	Any	-	Disabled
K8-1	User defined	Enabled	SNAT	172.16.10.23	-	192.168.10.2	Any	-	Disabled
K8-2	User defined	Enabled	SNAT	172.16.10.24	-	192.168.10.3	Any	-	Disabled

Figure 5 Create NAT rules for VM templates

Step 4 and Step 5: Optional: Allow Incoming SSH traffic to CSE server

If you plan to use SSH to the CSE server, we need to request a public IP address to allocate to the CSE server, create an Internet NAT rule, and allow SSH traffic to this public IP address. The following screenshots demonstrate these steps.

The screenshot shows the VMware Cloud Director interface for the 'US West SDDC'. The 'Networking & Security' tab is selected. The 'NAT' section is expanded, showing the 'Internet' tab. A table lists the NAT rules:

Name	Public IP	Service	Public Port	Internal IP	Internal Port	Firewall	Status
CDS Console Routing Rule - 10.10.32.4	[Redacted]	Provisioning & Remote Console	1902	10.10.32.4	902	Match Internal Address	Success
CDS HTTPS Routing Rule - 10.10.32.4	[Redacted]	HTTPS	1903	10.10.32.4	443	Match Internal Address	Success
CSE Server	[Redacted]	SSH	22	172.16.10.22	22	Match Internal Address	Success

Below the table, the 'Logging' section is set to 'No' and the 'Rule Enabled' status is 'Yes'.

Figure 6 Internet NAT rule to map Public IP address with external network IP address of the CSE server

The provider admin should follow the above steps for CSE service on CDs. On-prem VCD and the provider administrators can use the steps to create SNAT rules and the firewall configuration for relevant on-prem datacenter security practice. These steps are known and vary for each provider and are out of this deployment guide's scope.

After these steps are completed, verify the SSH connection to the CSE server using the allocated public IP address. It is assumed that SSH service is enabled and root login is enabled. As provider administrator, you can continue to the next steps to install the CSE server.

2. Install CSE service

This section describes steps to configure the CSE server using SSH, VCD-CLI, and the CSE commands. CSE server 3.0.1 requires python and pip versions of 3.7.3 at least. This step requires the CSE server machine to be installed in the CSE organization. The minimum memory requirement to run this CSE server is a virtual appliance with Linux based OS with 2GB of memory. Once the CSE server appliance is installed, and network configuration is completed from the above section, test the inbound and outbound

internet connection. Once the connectivity is verified, follow the steps described in the coming sections to install the CSE service on this virtual appliance. The commands are executed with `root` level user access.

```
root@cse-server:~# python3.7 --version
```

```
Python 3.7.3
```

```
root@cse-server:~# pip3.7 --version
```

```
pip 20.3.1 from /usr/local/lib/python3.8/dist-packages/pip (python 3.7)
```

The following step is optional to setup virtual environment to run the CSE server:

```
pip3.7 install virtualenv
virtualenv -p python3.7 cse
source ./cse/bin/activate
```

Install required packages to install the CSE service in the coming command:

```
sudo apt update
sudo apt install build-essential zlib1g-dev libncurses5-dev libgdbm-dev libnss3-dev libssl-dev libreadline-dev libffi-dev wget
```

Install the CSE server by following commands.

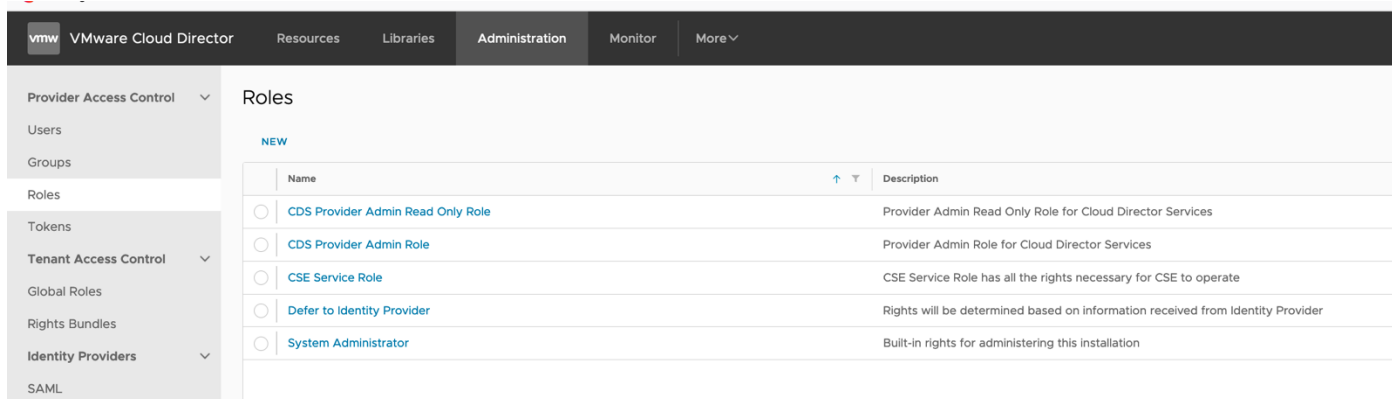
```
mkdir cse-server
cd cse-server
pip install container-service-extension
Create a service account on the CD's instance
```

This step creates a service role for the provider for the CSE operations to perform on the provider portal.

```
root@cse-server:~# cse create-service-role -v <VCD Host FQDN- Example: vcd-xxxx.yyyy.vdp.vmware.com> -s
```

use `-s --skip-ssl-verify` option if you are using a self-signed certificate. The recommendation is to use the trusted certificate.

Once the CSE server is installed successfully, and the service role is created, you can verify the provider portal's service role as shown in the following figure.



Name	Description
CDS Provider Admin Read Only Role	Provider Admin Read Only Role for Cloud Director Services
CDS Provider Admin Role	Provider Admin Role for Cloud Director Services
CSE Service Role	CSE Service Role has all the rights necessary for CSE to operate
Defer to Identity Provider	Rights will be determined based on information received from Identity Provider
System Administrator	Built-in rights for administering this installation

Figure 4 CSE service role creation on the provider portal.

Create CSE extension profile:

Login to the VMware Cloud director or Cloud director service with cloud administrator user credentials from CSE server using following command:

```
vcd login <vcd.serviceprovider.url> system <administrator user name> --password <password> -w -i
```


This login process also creates a VCD `profile.yaml` file. If the `profile.yaml` file doesn't exist, create a file to add CSE as an extension for the VCD and the same user running the CSE server. Append extension information to the `profile.yaml` file.

```
vi ~/vcd-cli/profiles.yaml
```

```
extensions:
- container_service_extension.client.cse
```

The next step is to create a CSE server configuration file. The CSE server uses information such as VCD, VC, Storage profile, Kubernetes template, and more. This step is similar to the older configuration file, except the AMQP section is now replaced by MQTT section. The following configuration file is for reference. As a provider administrator, change the VCD, VCs, broker sections based on your environment details.

```
cse sample -o config.yaml
```

Example Output:

```
mqtt:
  verify_ssl: false

vcd:
  api_version: '35.0' <for MQTT to work, API_version must be >=35.0>
  host: vcd-xxxx.yyyy.vdp.vmware.com
  log: true
  password: <CDS_Admin_password>
  port: 443
  username: <CDS_SystemAdmin>
  verify: true <use false when used ssl certificate is self-signed>

vcs:
- name: <VC_username_for_VMC_SDDC_Instance>
  password: <VC_Cloud_admin_password>
  username: <VC_cloud_admin_username> e.g. cloudadmin@vmc.local
  verify: true <use false when used ssl certificate is self-signed>

service:
  enforce_authorization: true <false>
  log_wire: false
  processors: 15
  telemetry:
    enable: true

broker:
  catalog: cse
  default_template_name: <template_name> e.g ubuntu-16.04_k8-1.17_weave-2.6.0
  default_template_revision: 0
  ip_allocation_mode: pool
  network: <Network_name_from_CSE_Organization>
  org: <Name_of_Organization_where_CSE_server_is_installed>
  remote_template_cookbook_url: http://raw.githubusercontent.com/vmware/container-service-extension-templates/master/template.yaml
  storage_profile: '<Name_of_storage_policy_for_CSE_organization, cannot be '*'>'
  vdc: <Name_of_VDC_of_CSE_Organization>
```

The storage profile information is located in the organization VDC policies section, as shown in the figure below.

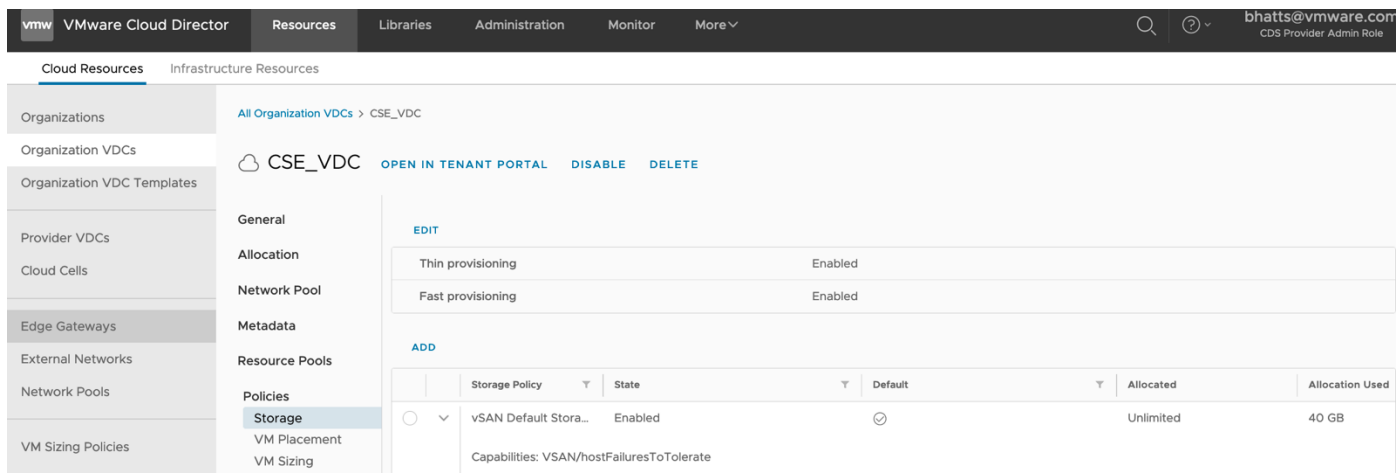


Figure 5 The organizations Storage policy on from the provider portal

After the CSE configuration file is updated with your VCD environment details, you can also check the configuration using the following command:

```
root@cse-server:~/cse-server# cse check config.yaml -s
```

```
Required Python version: >= 3.7.3
Installed Python version: 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0]
Validating config file 'config.yaml'
InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advised.
Connected to vCloud Director (vcd-bf2ff71f-2043-4f4c-b0c2-253b1cdfaba9.us-west-2.vdp.vmware.com:443)
Connected to vCenter Server 'VMC-US West SDDC' as 'cloudadmin@vmc.local' (vcenter.sddc-44-239-98-19.vmwarevmc.com)
Config file 'config.yaml' is valid
```

After the configuration file changes are complete, you can now install the CSE server with VCD and install the template specified in the `config.yaml`:

This step also requires that the administrator changes the permissions to block read, write, execute permissions by other users to secure the CSE configuration.

```
chmod 600 config.yaml
cse install -c config.yaml -t
cse template install ubuntu-16.04_k8-1.17_weave-2.6.0 2 -c config.yaml
```

Installing the template may take few mins according to the network speed. After the process is complete, you can start the CSE service.

```
root@cse-server:~/cse-server# cse run -c config.yaml -s
```

```
Required Python version: >= 3.7.3
Installed Python version: 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0]
Validating config file 'config.yaml'
InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification is strongly advised.
Connected to vCloud Director (vcd-bf2ff71f-2043-4f4c-b0c2-253b1cdfaba9.us-west-2.vdp.vmware.com:443)
Connected to vCenter Server 'VMC-US West SDDC' as 'cloudadmin@vmc.local' (vcenter.sddc-44-239-98-19.vmwarevmc.com)
Config file 'config.yaml' is valid
Successfully loaded defined entity schema to global context
Loading k8s template definition from catalog
Found K8 template 'ubuntu-16.04_k8-1.17_weave-2.6.0' at revision 2 in catalog 'cse'
Loading kubernetes runtime placement policies.
Template rules are not supported by CSE for vcd api version 35.0 or above. Skipping template rule processing.
Validating CSE installation according to config file
MQTT extension and API filters found
Found catalog 'cse'
CSE installation is valid
```

```
Started thread 'MessageConsumer' (140294175840000)
Started thread 'ConsumerWatchdog' (140294100088576)
Container Service Extension for vCloud Director
Server running using config file: config.yaml
Log files: /root/.cse-logs/cse-server-info.log, /root/.cse-logs/cse-server-debug.log
waiting for requests (ctrl+c to close)
```

Connect to VCD with the system admin credentials and enable CSE for desired tenant organization. You can skip the login step if you have already executed the step.

```
Example: vcd login vcd-xxxx.yyyy.vdp.vmware.com system <systemAdmin username> -iw
```

Password:

```
systemAdmin Logged in, org: 'system', vdc: ''
vcd cse ovd enable <VDC name of desired Tenant Organization> -o <desired Tenant> -n
You can verify if the tenant is now enabled with for CSE service by following command:
```

```
vcd cse ovd list
```

Example output:

```
root@cse-server:~# vcd cse ovd list
```

Name	ID	K8s Runtime
Org1Vdc	893f1dd1-3c88-4ecf-a111-429eb6d23239	['native']
CSE_VDC	a73491a5-a2bc-42d6-8ac2-815e67562b51	[]

Once the steps are successfully executed, the following steps are required for the tenant's organization and VDC for on-prem VCD or Cloud Director service's provider portal on VMC on AWS.

- Create and organization, Edge gateway, and Networks
- Create SNAT rules for the Kubernetes clusters.

These steps are similar to 'Prepare VMware Cloud Director/Cloud Director Service with required CSE server network accesses described in the earlier sections.

3. Enable Tenant to deploy Kubernetes

After the CSE server is installed successfully, provider can now onboard tenant. As a provider administrator following steps are required to allow each tenant to use the CSE UI plug-in.

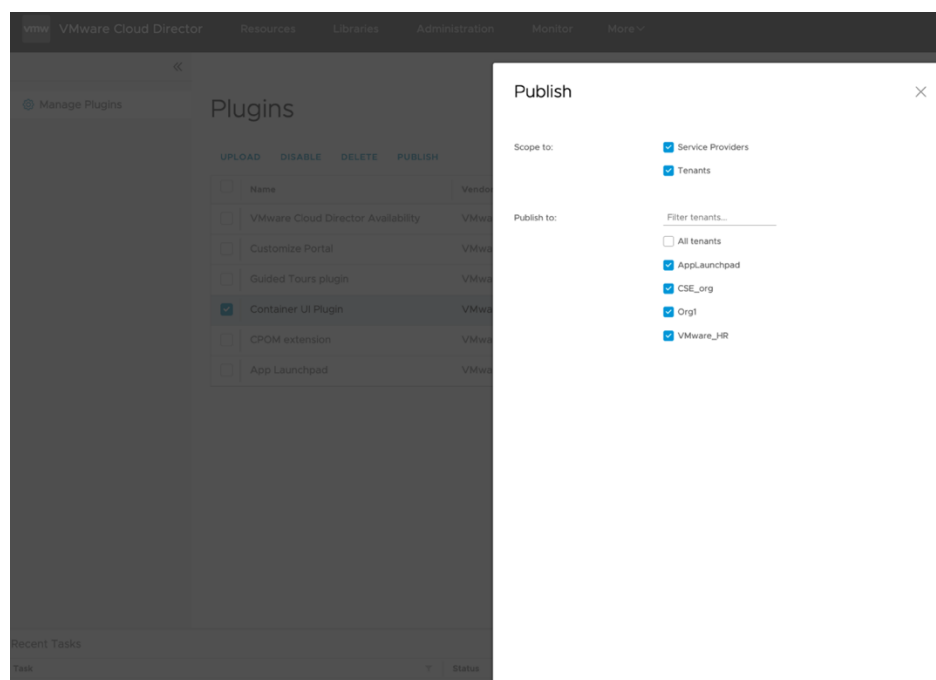


Figure 6 Publish the CSE UI plug-in to tenants

The next step is to publish the rights bundle to the tenant. The rights bundle allows tenant organization users to create, delete, and scale the Kubernetes clusters from the tenant portal. The tenant administrator can create various roles to view/create/manage Kubernetes clusters. The following figures explain how to publish rights bundles from the provider portal to a tenant or tenants.

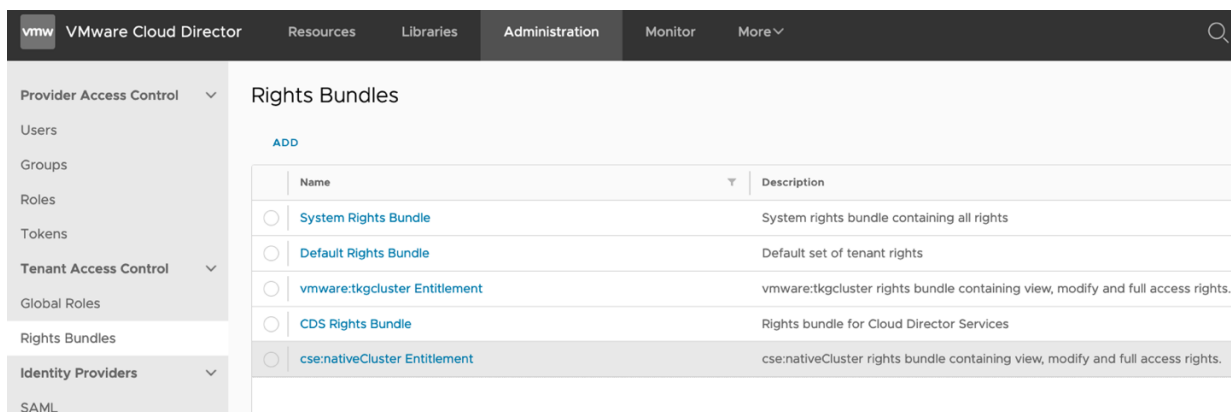


Figure 7 Publish rights bundle to tenant

The last step is to create a user role with Kubernetes cluster capabilities from the tenant portal. The Kubernetes cluster related user-roles are separate from the VCD user roles. When the customer requests Kubernetes as a Service, the tenant administrator must create the user-role from the tenant portal. The next figure shows how the tenant portal cloned a user vApp Author role with the Kubernetes cluster related capabilities.

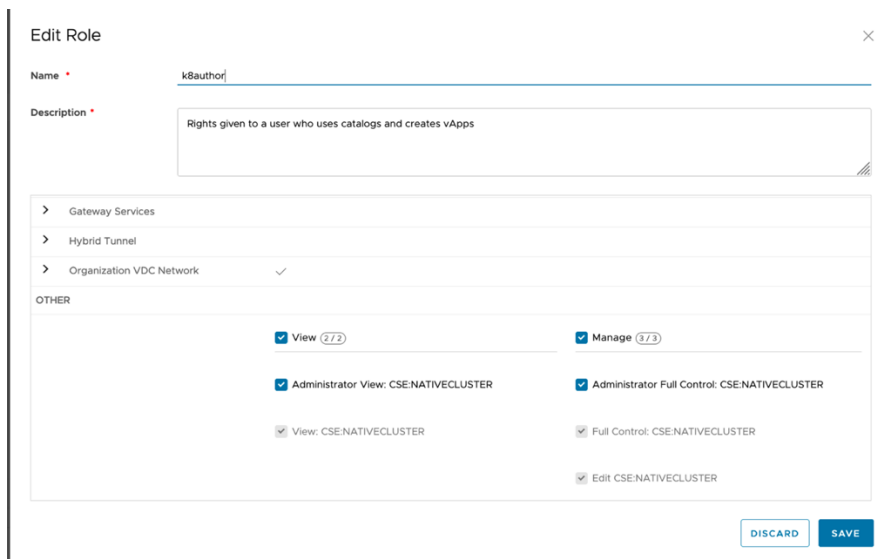


Figure 8 Create a Kubernetes cluster author role from tenant portal

Accessing Kubernetes Cluster:

The tenant user (developer or DevOps role as defined by tenant administrator) can download the `kubeconfig` from the tenant portal. This configuration includes an internal network address allocated to the Kubernetes cluster. If user decides to expose service on this Kubernetes cluster, the internal IP can be replaced by additional public IP address. The tenant administrator can request this IP address from the provider. The additional steps involve, creating Internet NAT rule and DNAT rule on Edge Gateway. Update the `kubeconfig.yaml` file with this Public IP address. These steps are similar to creating inbound SSH access using public IP address in the earlier sections of this document.

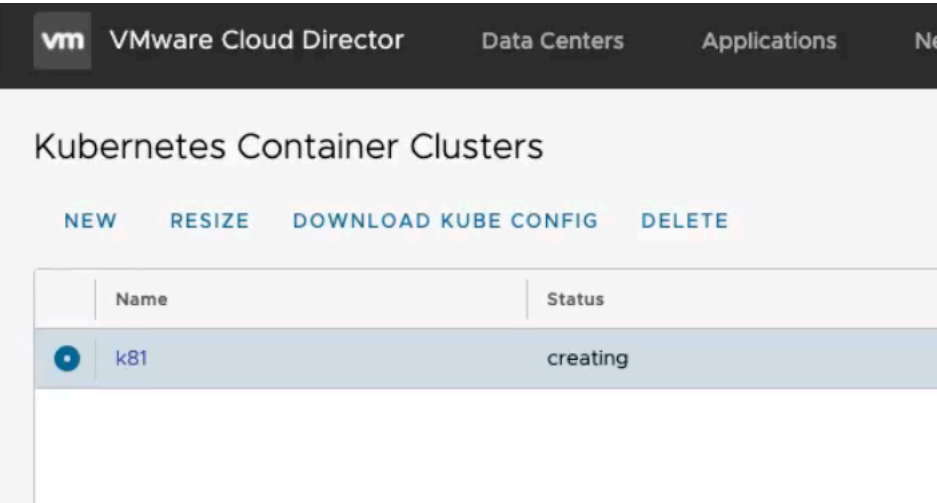


Figure 9 Download kubeconfig file

Summary

The tenant user can now use Container Service Extension with VMware Cloud Director and Cloud Director service on VMware Cloud on AWS. The steps are described in detail for the provider administrator to prepare CDs, CSE server installation, and tenant onboarding. This guide will help providers configure and serve their tenants with Container service extension for upstream Kubernetes cluster capabilities.

List of Tables

Table 1 Summary of CSE Install, configuration steps and configuration end points..... 5

List of Figures

Figure 1 Container Service Extension User flow with VCD 4

Figure 2 CSE and tenant network connectivity on CDs 5

Figure 3 Create SNAT/DNAT rules for the CSE server 6

Figure 4 Internet NAT rule to map Public IP address with external network IP address of the CSE server 6

Figure 5 Management gateway firewall rules to allow communication to vCenter Server and ESXi hosts 6

Figure 6 Create NAT rules for VM templates..... 7

Figure 7 CSE service role creation on the provider portal. 8

Figure 8 The organizations Storage policy on from the provider portal10

Figure 9 Publish the CSE UI plug-in to tenants11

Figure 10 Publish rights bundle to tenant 12

Figure 11 Create a Kubernetes cluster author role from tenant portal12

Figure 12 Download kubeconfig file.....13

Glossary

TKG cluster ~ Tanzu Kubernetes cluster ~ Tanzu Kubernetes Grid cluster ~ vSphere with Tanzu cluster

TKGI cluster	Ent-PKS cluster ~ Tanzu Kubernetes Grid Integrated Edition cluster
--------------	--

Defined entities	Runtime defined entities ~ RDE ~ Defined Entity Framework
------------------	---

Tkg entities	Tkg defined entities representing Tkg clusters
--------------	--

Native entities	Native defined entities representing Native clusters.
-----------------	---

CSE	Container Service Extension
-----	-----------------------------

VCD	VMware Cloud Director.
-----	------------------------

CDS	Cloud Director Service
-----	------------------------

SDDC	Software Defined Datacenter
------	-----------------------------



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-wp-tech-temp-a4-word-101-proof 6/20