MAY 2021

VMware Cloud Provider Lifecycle Manager Deployment Guide

A Natural Partnership

For Cloud and Service Providers

Bhaskar Gupta

Cloud Services Business Unit

May 2021

Table of Contents

List of Figures

List of Tables

Introduction

This technical white paper is intended for VMware Cloud Provider Program, cloud providers who are interested in automated deployment and configuration of components like VMware Cloud Director, Usage Meter, vRealize Operations Manager Tenant App, RabbitMQ using the tool VMware Cloud Provider Lifecycle Manager. The content below describes the architecture, pre-requisites, and deployment procedure of VMware Cloud Provider Lifecycle Manager. This document also covers the procedure to deploy additional components as mentioned above and perform Day-2 activities like upgrades/patches and configuration of the deployed components.

Architecture

VMware Cloud Provider Lifecycle Manager is designed as an application that provides a REST API, which allows triggering the required tasks.

The underlying implementation to integrate with the corresponding products VMware Cloud Director, vRealize Operations Manager Tenant App, RabbitMQ and Usage Meter is designed as generic product tasks.

To deploy or manage a solution, VMware Cloud Provider Lifecycle Manager requires a definition of the necessary tasks (deployment + validation, configuration, upgrade tasks) and product binaries (e.g., OVA). The REST API generic structure is applicable to different types of solutions.

VMware Cloud Provider Lifecycle Manager needs access to the repository (mounted NFS or locally) which contains OVA files, upgrade packages, etc.

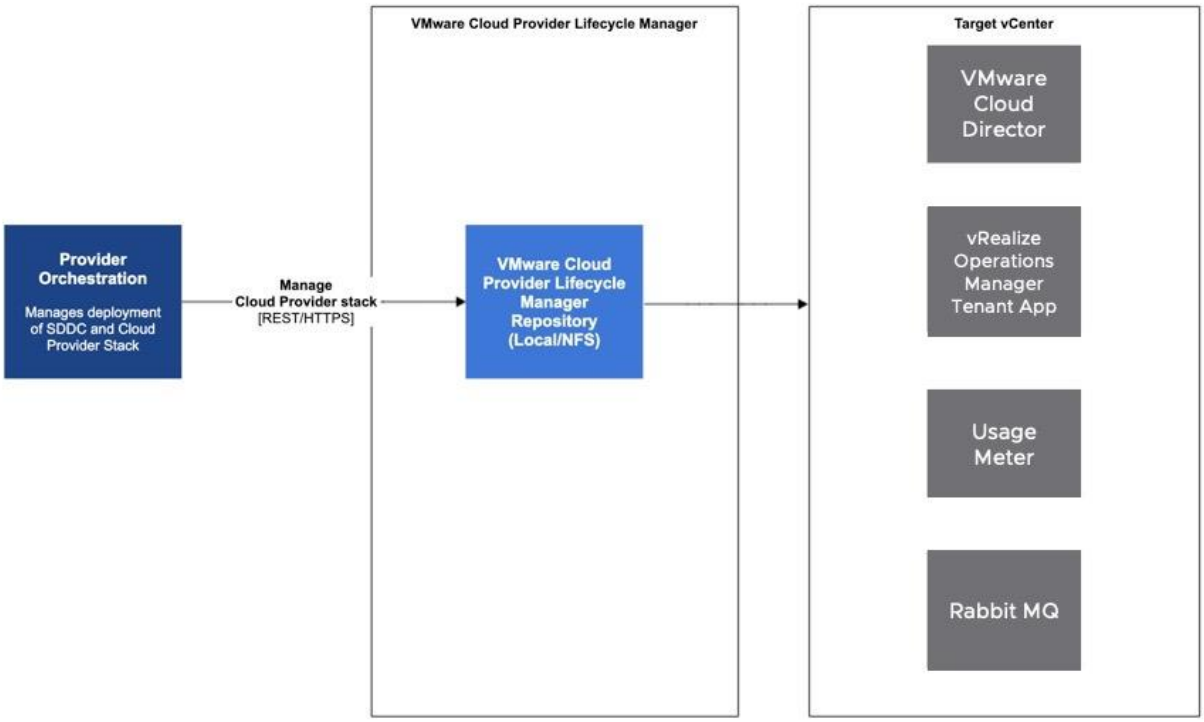

Figure 1:VMware Cloud Provider Lifecycle Manager workflow

Deployment

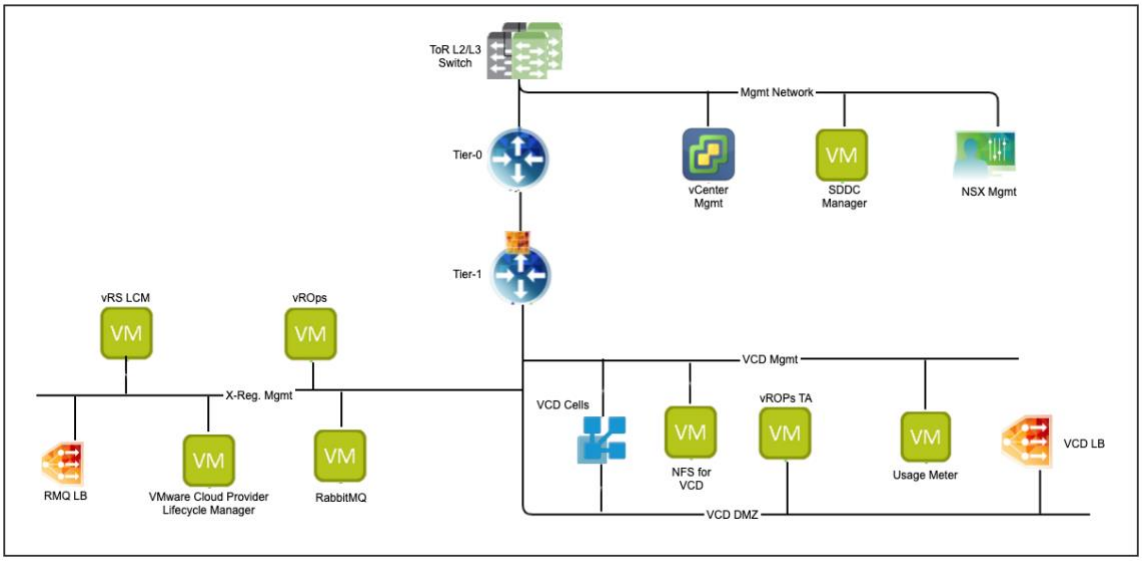

Figure 2:Example of logical network deployment

Workload Execution

Once a request is triggered by VMware Cloud Provider Lifecycle Manager's REST API, then it will execute the corresponding task defining a list of actions.

REST controller is deployed and is responsible for receiving a request, define and execute the tasks asynchronously. Each task will be associated with an ID which can be used to query the state of the task.

VMware Cloud Provider Lifecycle Manager Entity Structure

In VMware Cloud Provider Lifecycle Manager, products are deployed as part of a Lifecycle Manager environment. This allows grouping of different products to a single environment.

Such an environment requires a deployment infrastructure to be defined, as well as the products that should be deployed. The deployment infrastructure defines all necessary infrastructure for the deployment, such as vCenter URL and credentials, target cluster, datastores and networks, etc.

The products follow a generic definition pattern that defines basic common product fields and requires product-specific details to be specified as properties. This way, the API is not aware of the products themselves, but defines only the common fields. This allows VMware Cloud Provider Lifecycle Manager to expose an API that is common for all supported products and will enable other products to be easily added to it.

In addition to environments, infrastructure components, such as vCenter Servers, NSX-T Managers and vRealize Operations Manager instances will be managed as datacenter components. Such components are not deployed and lifecycle-managed by VMware Cloud Provider Lifecycle Manager. However, these components are used with products deployed by VMware Cloud Provider Lifecycle Manager.

Interoperability Matrix

Support Key

Y	Supported
N	Not Supported

Products	Versions	Deployment using VMware Cloud Provider Lifecycle Manager	Upgrade using VMware Cloud Provider Lifecycle Manager
VMware Cloud Director	10.2.x	Y	Y
	10.1.x	Y	Y
Usage Meter	4.4	Y	Y
	4.3	Y	Y
vRealize Operations Manager Tenant App	2.5	Y	Y
	2.4	Y	Y
Bitnami RabbitMQ VM	3.8.14	Y	N

Tested upgrades using VMware Cloud Provider Lifecycle Manager

Products	Source Product Version	Destination Product Version
VMware Cloud Director	10.1.3	10.2.2
	10.1.0	10.2.2
Usage Meter	4.3	4.4
	4.2	4.4
vRealize Operations Manager Tenant App	2.4	2.5

Table 1:Interoperability Matrix

Note: Linux (non-appliance) based VMware Cloud Director isn't supported as source for deployment and upgrade via VMware Cloud Provider Lifecycle Manager. For upgrades of other products, there are no requirements on specific source product versions.

Pre-requisites For VMware Cloud Provider Lifecycle Manager

API port

VMware Cloud Provider Lifecycle Manager must be set up and running. To access it via REST API, the HTTPS port **9443** must be accessible.

Product binaries

The binaries (ova files) for deploying the supported products need to be downloaded and provided to the VMware Cloud Provider Lifecycle Manager application.

The files can be downloaded locally to the VMware Cloud Provider Lifecycle Manager at */cplcmrepo* directory or mounted as NFS share to the same path.

The structure should be created as follows:

Create product repository directory

mkdir -p /opt/vmware/cplcm/cplcmrepo/{rmq/rmq_version-number/ova,usage/um_version-number/ova,vcd/vcd_version-number/ova,vropsta/vrops_version-number/ova}

***Example**,[user@localhost]$ mkdir -p /opt/vmware/cplcm/cplcmrepo/{rmq/3.8.14/ova,usage/4.3.0/ova,vcd/10.2.2/ova,vropsta/2.5.0/ova}*

Create repository directory for product update files

mkdir -p /opt/vmware/cplcm/cplcmrepo/{rmq/rmq_version-number/update,usage/um_version-number/update,vcd/vcd_version-number/update,vropsta/vrops_version-number/update}

***Example**,[user@localhost]$ mkdir -p /opt/vmware/cplcm/cplcmrepo/{rmq/3.8.14/update,usage/4.3.0/update,vcd/10.2.2/update,vropsta/2.5.0/update}*

The directory structure is mentioned below:

<product type>/<version>/ova|update/<file>

Note: The solution subdirectory specifies the version of the OVA or the patch.

```
├── rmq
│   └── 3.8.14
│       └── ova
│           └── bitnami-rabbitmq-3.8.14-0-linux-debian-10-x86_64-nami.ova
├── usage
│   ├── 4.3.0
│   │   └── ova
│   │   │   └── Usage_Meter_Agent-4.3.0.0-xxxxx_OVF10.ova
│   │   └── update
│   │       └── ums-system-upgrade_to_4.3.shar
│   └── 4.4.0
│       ├── ova
│       │   └── Usage_Meter_Agent-4.4.0.0-xxxxxx_OVF10.ova
│       └── update
│           └── Usage_Meter_Agent-4.4.0.0-xxxxxx_Upgrade.iso
├── vcd
│   ├── 10.1.2
│   │   └── ova
│   │       └── VMware_Cloud_Director-10.1.2.xxxxxx_OVF10.ova
│   └── 10.2.2
│       ├── ova
│       │   └── VMware_Cloud_Director-10.2.2.xxxxxx_OVF10.ova
│       └── update
│           └── VMware_Cloud_Director_10.2.2.xxxxxx_update.tar.gz
└── vropsta
    ├── 2.4.0
    │   └── ova
    │       └── vROps-Tenant-App-for-vCD-2.4.0.xxxxxx_OVF10.ova
    └── 2.5.0
        ├── ova
        │   └── vROps-Tenant-App-for-vCD-2.5.0.xxxxxx_OVF10.ova
        └── update
            └── vROps-Tenant-App-for-vCD-2.5.0.xxxxxx-updaterepo.iso
```

Firewall Ports

Port	Protocol	Direction	Target	Description
9443	TCP	Inbound / Outbound	Management network	Port used for VMware Cloud Provider Lifecycle Manager REST API.
22	TCP	Inbound / Outbound	Management network	SSH connection to the VMware Cloud Provider Lifecycle Manager machine to configure and set up deployment binaries.
22	TCP	Outbound	Deployed products (VCD, RMQ, vROPS TA, UM)	SSH used to configure deployed products.
53	TCP/UDP	Inbound / Outbound	DNS Server	DNS will be used to resolve IPs and hostnames and validate corresponding records for requested deployments. The DNS server provided in the payload will be used for validation purposes.
123	UDP	Outbound	NTP server	Configure NTP server to ensure time is in sync.
443	TCP	Outbound	vCenter (Mgmt and resource) NSX Manager VCD (cells and load balancer) vROPS vROPS Tenant App Usage Meter 4.3	HTTPS traffic to access and configure deployed products as well as validate infrastructure components.
5671 *	TCP, UDP	Outbound	RabbitMQ	AMQP port used for RabbitMQ AMQP service. This port can be customized; thus, the corresponding port must be accessible.
15671 *	TCP	Outbound	RabbitMQ Management Interface	Management port used for RabbitMQ Management Interface. This port can be customized; thus, the corresponding port must be accessible.
8443	TCP	Outbound	Usage Meter 4.2	Port used for HTTPS traffic to access Usage Meter 4.2 Rest API.
	ICMP	Inbound / Outbound	VCD cells vROPS Tenant App Usage Meter RabbitMQ	Ping is performed to check if deployed machines are running or existing prior to deployment.

**** Can be customized during deployment.***

Table 2: Firewall Ports

Pre-requisites for Product deployment

VMware Cloud Director Deployment

For deploying VMware Cloud Director using VMware Cloud Provider Lifecycle Manager, the following prerequisites must be met:

Deployment files

The corresponding product deployment binary (ova) for VMware Cloud Director with the required version need to be available in VMware Cloud Provider Lifecycle Manager.

Routing

From	To	Description
VMware Cloud Provider Lifecycle Manager	vCenter (infra)	VMware Cloud Provider Lifecycle Manager must be able to access the vCenter to deploy the VCD cells.
VMware Cloud Provider Lifecycle Manager	vCenter (resource)	VMware Cloud Provider Lifecycle Manager must be able to access resource vCenter to validate access for VCD.
VMware Cloud Director	vCenter (resource)	The resource vCenter will be configured as PVDC in VCD, thus must be accessible.
VMware Cloud Provider Lifecycle Manager	NSX-T Manager	VMware Cloud Provider Lifecycle Manager must be able to access NSX-T Manager to validate access for VCD.
VMware Cloud Director	NSX-T Manager	VCD will access NSX-T Manager to manage the PVDC.
VMware Cloud Director	NFS Mount	All VCD cells will mount the NFS share, thus must have access to it.
VMware Cloud Director	VMware Cloud Director	All VCD cells must be able to communicate with each other (e.g., access database, etc).
VMware Cloud Director	VCD Load Balancer	The Load Balancer VIP will be configured as base endpoint in VCD, thus must be accessible.
VMware Cloud Director Load Balancer	VMware Cloud Director	The Load Balancer must be able to access all VCD cells on port 443 and 8443 (console proxy).
VMware Cloud Director	RabbitMQ (LB)	VCD will access the RabbitMQ instance (or load balancer) via AMQP on defined port (default: SSL 5671).
VMware Cloud Director	NTP	NTP server must be accessible by all VCD cells.
VMware Cloud Director	DNS	DNS server must be accessible by all VCD cells.

Table 3: Routing for VMware Cloud Director

Ports

Port	Protocol	Description
53	TCP, UDP	DNS
111	TCP, UDP	NFS
123	TCP, UDP	NTP
443	TCP	Access API / user interface. Access NSX-T and vCenters configured as PVDCs.
920	TCP, UDP	NFS.
2049	TCP, UDP	NFSD (if needed, for VMware Cloud Provider Lifecycle Manager to be able to mount NFS share).
5432	TCP	Postgres Database.
5671	TCP, UDP	Access RabbitMQ (AMQP).

Table 4: Ports for VMware Cloud Director

See VMware Cloud Director Documentation for additional port requirements.

Service Accounts

The following (service) accounts must be available for deploying and configuring VMware Cloud Director:

System	Usage
Management VC	Account used to deploy the VCD cells in the management vCenter.
Resource VC	Service account used for registering the vCenter in VCD.
Resource NSX-T Manager	Service account used for registering the NSX-T Manager in VCD.
RabbitMQ	Service account to access RabbitMQ (this can be created directly during RMQ deployment).

Table 5:Service Accounts for VMware Cloud Director

Additional Prerequisites

- NFS share - an NFS share must be accessible to all VMware Cloud Director cells. The share needs to be empty before deployment and read/write access should be available without authentication.
- VMware Cloud Director Load Balancer - a load balancer has to be pre-configured to provide access to all VMware Cloud Director cells.
- DNS - DNS A and PTR records should exist for each VMware Cloud Director cell and the load balancer to enable forward and reverse lookup of IP addresses and hostnames.
- Certificates - certificates should be pre-created and passed into the VMware Cloud Director deployment (otherwise self-signed certificates will be generated by the VMware Cloud Director cell deployment).
- Provider VDC:
  - vCenter cluster or dedicated resource pool available to be configured for Provider VDC (if root resource pool of the cluster is used, no resource pool name should be specified)
  - Storage profile preconfigured in vCenter, including compliant datastores
  - NSX-T Manager is accessible and provides overlay transport zone that can be used for network pool.
  - NSX-T tier0 gateway is available and a subnet that is accessible to be used for configuring a VMware Cloud Director external network

RabbitMQ Deployment

For deploying RabbitMQ using VMware Cloud Provider Lifecycle Manager, the following prerequisites have to be met.

Deployment files

The corresponding product deployment binary (ova) for RabbitMQ with the required version has to be available in VMware Cloud Provider Lifecycle Manager.

Routing

From	To	Description
VMware Cloud Provider Lifecycle Manager	vCenter (infra)	VMware Cloud Provider Lifecycle Manager has to be able to access the vCenter to deploy the Rabbit MQ nodes.
RabbitMQ	RabbitMQ	All RabbitMQ nodes have to be able to communicate with each other.
RabbitMQ Load Balancer	RabbitMQ	The Load Balancer has to be able to access all RabbitMQ nodes on port 5671 (or other port, if configured differently). In addition, the RabbitMQ management port 15671 can be configured for the load balancer as well.
VMware Cloud Director	RabbitMQ (LB)	VCD will access the RabbitMQ instance (or load balancer) via AMQP on defined port (default: SSL 5671).
vROPS tenant app	RabbitMQ (LB)	vROPS tenant app will access RabbitMQ AMQP service.
RabbitMQ	NTP	The NTP server(s) have to be accessible by all RabbitMQ nodes.
RabbitMQ	DNS	DNS server(s) have to be accessible by all RabbitMQ nodes.

Table 6:Routing for RabbitMQ

Ports

Port	Protocol	Description
53	TCP, UDP	DNS.
123	TCP, UDP	NTP.
4369	TCP	epmd, a peer discovery service used by RabbitMQ nodes and CLI tools.
5671	TCP, UDP	AMQP SSL.
5672	TCP, UDP	AMQP non-ssl (if non-ssl is required).
15671	TCP	RabbitMQ management interface.
25672	TCP	RabbitMQ inter-node and CLI tools communication.
35672, 35673	TCP	CLI tools (Erlang distribution client ports) for communication with nodes.

Table 7:Ports for RabbitMQ

Service Accounts

The following (service) accounts must be available for deploying and configuring RabbitMQ

System	Usage
Management VC	Account used to deploy the RabbitMQ nodes in the management vCenter.

Table 8:Service Accounts for RabbitMQ

Additional prerequisites

- RabbitMQ Load Balancer – A load balancer has to be pre-configured to provide access to all RabbitMQ nodes.
- DNS – DNS A and PTR records have to exist for each RabbitMQ node and the load balancer to enable forward and reverse lookup of IP addresses and hostnames.

Usage Meter Deployment

For deploying Usage Meter using VMware Cloud Provider Lifecycle Manager, the following prerequisites have to be met:

Deployment files

The corresponding product deployment binary (ova) for Usage Meter with the required version need to be available in VMware Cloud Provider Lifecycle Manager.

Routing

From	To	Description
VMware Cloud Provider Lifecycle Manager	vCenter (infra)	VMware Cloud Provider Lifecycle Manager has to be able to access the vCenter to deploy the Usage Meter appliance.
Usage Meter	ums.cloud.vmware.com	Usage Meter must be able to access UMS cloud infrastructure (port 443) to be able to send usage reporting data and complete registration process. A proxy can be configured to reach vCloud Usage Insight, in which case that proxy has to be reachable.
Usage Meter	NTP	The NTP server(s) have to be accessible by the Usage Meter appliance.
Usage Meter	DNS	DNS server(s) have to be accessible by the Usage Meter appliance.

Usage Meter	vCenter	Usage Meter should be able to access all vCenter instances (management and resource) in order to enable metering.
Usage Meter	NSX-T	Usage Meter should be able to access all NSX-T Manager VIPs (management and resource) in order to enable metering.
Usage Meter	VMware Cloud Director	Usage Meter should be able to access VCD public endpoint in order to enable metering.
Usage Meter	vRealize Operations Manager	Usage Meter should be able to access vROPS in order to enable metering.

Table 9:Routing for Usage Meter

Ports

Port	Protocol	Description
53	TCP, UDP	DNS
123	TCP, UDP	NTP
443	TCP	Access products and execute API commands for metering. Also used to access ums.cloud.vmware.com, or corresponding proxy.
7443	TCP	Access PSC server product and execute API.
443	TCP	UI and API for Usage Meter (inbound).
proxy port	TCP	If a proxy is configured, that proxy's port has to be accessible.

Table 10:Ports for Usage Meter

See official Usage Meter documentation for additional port requirements.

Service Accounts

The following (service) accounts must be available for deploying and configuring Usage Meter.

System	Usage
Management VC	Account used to deploy Usage Meter Appliance in the management vCenter.
Management and Resource VC	Service account used for collecting usage from vCenter instances.
Management and Resource NSX-T Manager	Service account used for collecting usage from NSX-T.
vROPS	Service account used for collecting usage from vROPS.
VCD	Service account used for collecting usage from VCD.

Table 11: Service Accounts for Usage Meter

Additional prerequisites

- To be able to register usage metering for supported products, the Usage Meter appliance must be registered in VMware's Commerce Portal. This has to be done manually after deploying the Usage Meter appliance. The Usage Meter integration cannot be configured before the VMware Cloud Provider Commerce Portal registration.
- DNS – DNS A and PTR records have to exist for the Usage Meter appliance to enable forward and reverse lookup of IP addresses and hostnames.

vRealize Operations Manager Tenant App deployment

For deploying vRealize Operations Manager Tenant App using VMware Cloud Provider Lifecycle Manager, the following prerequisites have to be met:

Deployment files

The corresponding product deployment binary (ova) for vRealize Operations Manager Tenant App with the required version has to be available in VMware Cloud Provider Lifecycle Manager.

Routing

From	To	Description
VMware Cloud Provider Lifecycle Manager	vCenter (infra)	VMware Cloud Provider Lifecycle Manager has to be able to access the vCenter to deploy the vROPS Tenant App.
vROPS Tenant App	NTP	The NTP server(s) have to be accessible by vROPS Tenant App.
vROPS Tenant App	DNS	DNS server(s) have to be accessible by vROPS Tenant App.
vROPS Tenant App	RabbitMQ (LB)	vROPS tenant app will access RabbitMQ AMQP service.
vROPS Tenant App	vRealize Operations Manager	vROPS tenant app will access vROPS API for authentication and access to metrics.
vROPS Tenant App	VMware Cloud Director	vROPS tenant app will access VCD API.
public	vROPS Tenant App proxy/VIP	External access to vROPS Tenant App UI should be available to either the vROPS Tenant App UI directly or the proxy that is configured.

Table 12: Routing for vRealize Operations Manager Tenant App

Ports

Port	Protocol	Description
53	TCP, UDP	DNS
123	TCP, UDP	NTP
443	TCP	HTTPS port to access vROPS tenant app UI (inbound). HTTPS port to access vROPS and VCD (outbound).
5671 (or other, if configured)	TCP, UDP	AMQP SSL

Table 13: Ports for vRealize Operations Manager Tenant App

Service Accounts

The following (service) accounts must be available for deploying and configuring vRealize Operations Manager Tenant App

System	Usage
Management VC	Account used to deploy vROPS Tenant App in the management vCenter.
vROPS	Service account to connect vROPS Tenant App with vROPS.
VCD	Service account to connect vROPS Tenant App with VCD.
RabbitMQ	Service account to connect vROPS Tenant App with RabbitMQ.

Table 14: Service Accounts for vRealize Operations Manager Tenant App

Additional prerequisites

- vROPS – vRealize Operations Manager must be deployed and accessible by vRealize Operations Tenant App.
- VMware Cloud Director integration should be configured completely, the management pack for VMware Cloud Director must be installed in vRealize Operations Manager.

- DNS – DNS A and PTR records have to exist for the vROPS Tenant App appliance to enable forward and reverse lookup of IP addresses and hostnames.

Setting Up VMware Cloud Provider Lifecycle Manager

Currently VMware Cloud Provider Lifecycle Manager is shipped as a docker container image that has to be operated on a host environment.

This below section describes how to set up a host in order to execute the docker image for VMware Cloud Provider Lifecycle Manager.

Setup VMware Cloud Provider Lifecycle Manager

Deploy Photon OS 3 (base)

Get the latest Photon OS image and deploy in vCenter: https://github.com/vmware/photon/wiki/Downloading-Photon-OS

Configure Networking

Setup networking settings on the deployed VM.

If needed, check Photon OS documentation:

- Configure static IP: https://vmware.github.io/photon/assets/files/html/3.0/photon_admin/setting-a-static-ip-address.html
- Configure DNS: https://vmware.github.io/photon/assets/files/html/3.0/photon_admin/adding-a-dns-server.html

Make sure docker service is running

Install (if not already installed) and run the docker service.

[user@localhost]$ systemctl start docker

Configure iptables

Run the following command to configure Photon OS's firewall iptables:

[user@localhost]$ iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 9443 -j ACCEPT

[user@localhost]$ iptables -A OUTPUT -p tcp -m state --state NEW -m tcp --dport 9443 -j ACCEPT

Prepare VMware Cloud Provider Lifecycle Manager directories

Log directory

Create log directory:

[user@localhost]$ mkdir -p /opt/vmware/cplcm/log

*[user@localhost]$ chmod 766 /opt/vmware/cplcm/log/**

Repository directory

The files required for deployment (e.g., ova files) have to be stored in a specific file structure.

Either create a new directory and upload the deployment files or mount an existing directory to the host VM.

Create repository directory

Create the product folders:

[user@localhost]$ mkdir -p /opt/vmware/cplcm/cplcmrepo/{rmq/rmq_version-number/ova,usage/um_version-number/ova,vcd/vcd_version-number/ova,vropsta/vrops_version-number/ova}

[user@localhost]$ chmod -R 777 /opt/vmware/cplcm/cplcmrepo

Upload the ova files for the different products to the corresponding created folders.

Ova files for Usage Meter and VMware Cloud Director can be obtained from my.vmware.com.

The ova file for vRealize Operations Manager Tenant App can be obtained from VMware marketplace:
2.4: https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director#resources
2.5: https://marketplace.cloud.vmware.com/services/details/vrealize-operations-management-pack-for-vcloud-director-5-4?slug=true

The ova file for RMQ can be downloaded from: https://bitnami.com/redirect/to/1377792/bitnami-rabbitmq-3.8.14-0-linux-debian-10-x86_64-nami.ova

Mount an existing shared directory

Instead of creating the repo folder structure and upload the files to the host VM, an existing pre-configured directory can be mounted to the machine as well.

Therefore, just add the NFS mount details to the fstab file and mount the directory.

 # Add nfs share to /etc/fstab

echo "<nfs-server>:<nfs_dir_path> /cplcmrepo nfs defaults 0 0" >> /etc/fstab

 # Mount the newly added nfs share

mount /cplcmrepo

Import docker image

The docker image file (vcplcm.<version>.tar.gz) should be uploaded to the Photon machine (e.g., to /tmp/ directory)
Then the image can be imported using the following command:

docker load --input /tmp/vcplcm.<version>.tar.gz

Start the docker container

Once imported, start the docker container. The VMware Cloud Provider Lifecycle Manager application is started to run in the container automatically.

Be aware that the application can only be run if the EULA is accepted by setting the corresponding variable (EULA-ACCEPT) in the command.

 # Start docker container (run in background)

docker run –net=host –name vcplcm -e EULA-ACCEPT=<true> -e RESTAPI_USERNAME=<<username>> -e RESTAPI_PASSWORD=<<password>> -v /cplcmrepo:/cplcmrepo -v /opt/vmware/cplcm/log:/opt/vmware/cplcm/log -d –restart=always vcplcm:<version>

Alternatively, to the described command to start the container, it can also be executed with an interactive session.

This allows accessing the container's file system and might help troubleshooting.

 # Start docker container with interactive session (for troubleshooting)

docker run –net=host –name vcplcm -e EULA-ACCEPT=true -e RESTAPI_USERNAME=<<username>> -e RESTAPI_PASSWORD=<<password>> -v /cplcmrepo:/cplcmrepo -v /opt/vmware/cplcm/log:/opt/vmware/cplcm/log -v /tmp:/tmp -it –entrypoint /bin/bash –rm vcplcm:<version>

 # This just starts the container; the application still has to be started with: start-cplcm.sh

 # Certificate Management

A certificate is automatically generated upon starting the container.
Re-generate the certificate using the method mentioned below:

Mount a directory to "/opt/vmware/cplcm/security/certs" when starting the container with read and write permissions for all users (at least permission mode 666) when starting the container.

E.g.: docker run –net=host –name vcplcm -e EULA-ACCEPT=true -e RESTAPI_USERNAME=<<username>> -e RESTAPI_PASSWORD=<<password>> -v /cplcmrepo:/cplcmrepo -v /opt/vmware/cplcm/log:/opt/vmware/cplcm/log -v /opt/vmware/cplcm/security/certs:/opt/vmware/cplcm/security/certs -d –restart=always vcplcm:<version>

It will reuse the existing cert when the container is started next time.

However, custom certificate can also be provided.
For that, the easiest way is to create a PKCS12 file, call it vcplcm.p12 in that directory. The keystore password can be specified as env variable in the docker container: -e CPLCM_KEYSTORE_PW=my_pw

Using VMware Cloud Provider Lifecycle Manager

The REST API for VMware Cloud Provider Lifecycle Manager provides functionality for deploying, upgrading and managing the related products.

The general API documentation is provided with a swagger UI available in the VMware Cloud Provider Lifecycle Manager application: https://*<cplcm-host>:<port>/swagger-ui.html*

API Version

The API will support versioning, so that changes in the API will not affect previous versions.

Therefore, an initial, unauthenticated call can be made to the endpoint to retrieve the current product version and supported API versions:

Method: GET

URL: https://VMware Cloud Provider Lifecycle Manager IP:9443/api/about

Sample response:

```
{
  "productVersion": "1.0.0",
  "buildNumber": "1234",
  "apiVersions": [
    {
      "apiVersion": "v1",
      "deprecated": false
    }
  ]
}
```

This provides the information that API version "v1" is the latest version to use.

It is recommended to work with API versions that are NOT deprecated, as the deprecated versions will be removed in a future update.

Authentication

Once, the API version is defined, a JSESSIONID has to be retrieved for further working with the REST API.

This is done by executing a call to the session endpoint:

Method: POST

URL: https://VMware Cloud Provider Lifecycle Manager IP:9443/api/v1/session

Body:

```
{
  "username": "local username",
  "password": "password"
}
```

Response:

```
{"JSESSIONID":"A2410EE49F55AEC9976A17EDA379F5A9"}
```

The username and password have to be provided in the json body to this request.

The username and password are defined, depending on the VMware Cloud Provider Lifecycle Manager configuration. At this point, this is defined as an environment variable in its runtime.

This session ID has to be used for all subsequent API calls – provided as a header "JSESSIONID".

Deploy Product

To deploy one or several products, Lifecycle Manager environment has to be created.

In a future version, this environment will be managed by VMware Cloud Provider Lifecycle Manager and the corresponding product details will be stored.
In this initial release with limited availability, no information about the requested environment is stored in VMware Cloud Provider Lifecycle Manager.
This is also the reason that no other API calls to retrieve information about or update an environment or product are supported in this version.

To create an environment, execute the below POST request.

Method: POST

URL: /api/{apiVersion}/lcm/environment?action=DEPLOY

Header: name: JSESSIONID – value: a valid jsessionid

Sample bodies:

Deploy VMware Cloud Director

API call at high level

- Define Environment Name and ID
- Products
  - Properties:
    - VMware Cloud Director Installation ID
    - System name
    - Database password
    - Public Address
      - Console Proxy external address
      - REST API HTTP and HTTPs address
      - Tenant portal external HTTP and HTTPS address
    - Admin username, email and full name
    - NFS mount point details
    - Deployment options, disk mode, ssh
  - Certificate details
    - Product (UI)
    - Management (VAMI and database)
    - REST API
    - Tenant Portal
  - Integrations:
    - Provide VCD-vCenter Integration ID, vCenter host details with Integration user login credentials
      - Details about Provider VDC like description, hardware version, thin provisioning resource pool name, storage profile, network pool name, etc.
    - VCD-NSX Integration ID and NSX host details with integration user login credentials.
      - Details about Network Pool and VCD External Network.
    - VCD to RabbitMQ Integration ID, RabbitMQ host details with integration user login credentials.
      - RabbitMQ host properties like SSL, prefix, etc.
  - Provide VCD product ID, version, License and admin password.
    - Node Information:
      - Below details for all the VMware Cloud Director nodes need to be provided.
        - Hostname,VM name, root password and network details for both the nics.
- Deployment Infrastructure
  - vCenter details like hostname, admin password, cluster, datastore and network details like portgroup name, gateway, subnetmask, domain name, etc where VMware Cloud Director will be deployed.

Deploy Usage Meter

API call at high level

- Define Environment Name and ID
- Products
  - Properties:
    - Auditor password (password for UM auditor account, having read-only access to config and logs)
    - Proxy (Type, Host IP, port, user and password)
  - Product Type
  - Product ID
  - Usage Meter version
  - Admin password
  - Integrations
    - Provide Usage Meter-vCenter Integration ID, vCenter host details with admin login credentials
    - Usage Meter-NSX Integration ID and NSX host details with admin login credentials
    - Usage Meter-VMware Cloud Director Integration ID, VCD host details with login credentials.

        - Usage Meter-vRealize Operations Manager Integration ID, VROPs host and login credentials
    - Node Information
        - Hostname,VM name, root password and network details of usage meter to be deployed.
- Deployment Infrastructure
    - vCenter details like hostname, admin password, cluster, datastore and network details like portgroup name, gateway, subnetmask, domain name, etc where Usage Meter will be deployed.

Note: Usage Meter should be registered in VCP after deployment (and then re-run deployment to configure the collectors)

Deploy RabbitMQ

API call at high level

- Define Environment Name and ID
- Products
    - Product Type
    - Product ID
    - RabbitMQ version
    - Admin password
    - Product Properties
        - RabbitMQ Load Balancer Name, FQDN and IP
        - RabbitMQ SSL and Management port details.
        - User (svc_vcd) credentials
        - User (svc_vropsta) credentials
    - Node Information
        - Below details for all the RabbitMQ nodes need to be provided.
            - Hostname,VM name, CPU, Memory, root password and network details.
- Deployment Infrastructure
    - vCenter details like hostname, admin password, cluster, datastore and network details like portgroup name, gateway, subnetmask, domain name, etc where RabbitMQ will be deployed.

Deploy vRealize Operations Manager Tenant App

API call at high level

- Define Environment Name and ID
- Products
    - Product Type
    - Product ID
    - vRealize Operations Manager Tenant App version
    - Admin password
    - Integrations:
        - Provide vROps TA-vROPs Integration ID, vROPs host details with login credentials
        - Provide vROps TA-VCD Integration ID, VCD host details with login credentials
        - Properties:
            - RabbitMQ host, port and SSL details.
            - vROPs Tenant App Proxy URL
            - Credentials for VCD-RabbitMQ and vROPS TenantApp-RabbitMQ
    - Node Information
        - Hostname,VM name, root password and network details of vRealize Operations Manager Tenant App to be deployed.
- Deployment Infrastructure
    - vCenter details like hostname, admin password, cluster, datastore and network details like portgroup name, gateway, subnetmask, domain name, etc where Usage Meter will be deployed.

Note: The Environment ID in the API call is important and should be unique for all executions, although there can be multiple product deployments or tasks under one Environment ID, but it is advisable to keep it separate for each task.

Please refer the API reference and POSTMAN sample collection on code.vmware.com for detailed APIs.

Response

```
{
  "taskId": "1"
}
```

If the response is **OK (200),** the request to create the environment has been accepted and is being processed asynchronously. The returned taskId can now be used to check the status of the deployment.

Retrieve Task Status

To verify the status of a running task, a GET request has to be executed.

Method: GET

URL: /api/{apiVersion}/task/{taskId}

Header: name: JSESSIONID - value: a valid jsessionid

Sample response:


```
{
   "id": 1,
   "subTasks": {
      "c6765081-c5bf-4386-a3d8-498c84e8e497": {
         "name": "LcmDiscoverStep-USAGE-4.4.0-DISCOVER",
         "status": "SUCCESS",
         "message": [
            {
               "name": "Discover product",
               "status": "OK",
               "message": "Successfully updated product state.",
               "start_time": "2021-04-08-15:23:06UTC",
               "end_time": "2021-04-08-15:23:55UTC"
            }
         ],
         "nextSubTasks": {
            "SUCCESS": "28d7b09e-d16c-4dc3-ba98-17679b989b2f"
         }
      }
   },
   "status": "SUCCESS",
   "message": ""
}
```


Possible values for the status are:

- NOT_STARTED
- IN_PROGRESS
- SUCCESS
- ERROR
- CANCELLED

The message field of the task contains response messages from different steps of the task.
E.g., usually pre and post validation results are listed in the corresponding sub-section within the messages**.**

Cancel a Task

To cancel a running task, a PUT request has to be executed.

Method: PUT

URL: /api/{apiVersion}/task/{taskId}?action=cancel

Header: name: JSESSIONID - value: a valid jsessionid

Expected response code: 200

Day-2 Operations Using VMware Cloud Provider Lifecycle Manager

Some of the Day-2 Operations like node management and updating certificate using VMware Cloud Provider Lifecycle Manager is mentioned below.

Import Environments

Note that currently the VMware Cloud Provider Lifecycle Manager does not support deployed environments beyond its runtime state (it does not have internal database). It means that in order to provide day-2 operations, the existing state of the to-be-managed environments has to be imported.

Method: POST

URL: /api/v1/lcm/environment?action=IMPORT

Header: name: JSESSIONID - value: a valid jsessionid

The body payload has the same structure as the create environment method.

Please refer VMware Cloud Provider Lifecycle Manager 1.1 Deployment and Administration Guide for more details.

Get Environments

The current state can be verified using GET LCM environments method. All environments currently known to the runtime state of the VMware Cloud Provider Lifecycle Manager will be returned.

Method: GET

URL: /api/v1/lcm/environment

Header: name: JSESSIONID - value: a valid jsessionid

Manage Nodes

To manage the product nodes, additional API calls will be added to VMware Cloud Provider Lifecycle Manager's REST API.

The API calls will trigger an Ansible playbook defined for the corresponding action.

Existing (known) nodes of a particular environment and product can be retrieved using GET method:

Method: GET

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/node

Add Nodes

Method: POST

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/node

Header: name: JSESSIONID - value: a valid jsessionid

Sample Bodies

VMware Cloud Director

API calls at high level:

- Provide the below details:
  - VCD hostname and the domain name which needs to be added
  - VM name
  - Root password
  - Network details like both IP address, gateway, network name & static routes

RabbitMQ

API calls at high level:

- Provide the below details:
  - RabbitMQ hostname and the domain name which needs to be added
  - VM name

  - Root password
  - CPU and Memory details
  - Network details like IP address & network name

The JSON body for the node addition defines the node specification details.

The current environment the product is part of, should be defined in VMware Cloud Provider Lifecycle Manager prior to running this operation.
If the environment was not created as within this instance of VMware Cloud Provider Lifecycle Manager, the environment has to be imported first.

This operation will add the new node to the currently known environment.

Not all products support addition of new nodes. vRealize Operations Manager Tenant App and Usage Meter are single-node deployments only. Therefore, the product BOM file specifies the maximum number of supported nodes. If the maximum number of nodes is reached already, the API will return **error 405 - Method Not Allowed** - with a message that the product supports only deployment of X node(s).

Redeploy Nodes

Method: PUT

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/node/{nodeId}

Header: name: JSESSIONID - value: a valid jsessionid

Sample Bodies:

API calls at high level:

VMware Cloud Director

- Provide the below details:
  - VCD hostname and the domain name which needs to be added
  - VM name
  - Root password
  - Gateway
  - Network details like both IP address, network name, static routes

RabbitMQ

- Provide the below details:
  - RabbitMQ hostname and the domain name which needs to be added
  - VM name
  - Root password
  - CPU and Memory details
  - Network details like IP address & network name

The nodeId refers to the index of the node in the list of nodes, as defined in the specified environment (0-based index, first node's nodeId is 0).

The referenced node will be removed first, and then deployed again.

The JSON body for the node redeployment defines the node specification details.

The current environment the product is part of, should be defined in VMware Cloud Provider Lifecycle Manager prior to running this operation.
If the environment was not created as within this instance of VMware Cloud provider Lifecycle Manager, the environment has to be imported first.

This operation will remove and redeploy a node and update the specified node in the currently known environment.

Not all products support adding or replacing nodes. vRealize Operations Manager Tenant App and Usage Meter are single-node deployments only. Therefore, the product BOM file specifies the maximum number of supported nodes. If the maximum number of nodes is 1, that means no node can be replaced (which would actually delete the node first). The API will return **error 405 - Method Not Allowed** - with a message that the product does not support redeployment of nodes. In order to redeploy, delete the product from the environment (or the entire environment) and deploy a new product.

Update Node

To update the node's configuration (root password, ip address, CPU, memory), the following API operation will be available.

Method: PATCH

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/node/{nodeId}

Header: name: JSESSIONID - value: a valid jsessionid

Sample Body

VMware Cloud Director, Usage Meter, vRealize Operations Manager Tenant App & RabbitMQ

API calls at high level:

- Provide the below details:
  - Root password (updated password)
  - CPU and Memory details.

Delete Node

A node can be deleted with DELETE method:

Method: DELETE

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/node/{nodeId}?force=(true|false)

Header: name: JSESSIONID - value: a valid jsessionid

Manage Certificates

Update Product Certificates

During deployment, certificates used by the deployed product can be specified.

As certificates expire, these have to be updated at some point.Therefore, additional API calls will be added to VMware Cloud Provider Lifecycle Manager's REST API to allow such operations.

Depending on the product, different certificates might have to be configured. By default, it is assumed that a certificate is to be configured per node - this is regarded as the product's main certificate.

Additional certificates might be used for different services of a product and should be managed by VMware Cloud Provider Lifecycle Manager as well. These are to be specified separately in the API payload to deploy or update the product.

Method: PUT

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/certificate

Header: name: JSESSIONID - value: a valid jsessionid

Sample Bodies

API calls at high level:

VMware Cloud Director

- Product
  - Provide VCD certificate
  - VCD certificate private key
- Management
  - Provide VCD certificate
  - VCD certificate private key
- REST API
  - Provide VCD certificate
- Tenant Portal
  - Provide VCD certificate

Usage Meter

- Product
  - Provide Update Manager certificate
  - Update Manager certificate private key

vRealize Operations Manager Tenant App

- Product
  - Provide vRealize Operations Manager Tenant App certificate
  - vRealize Operations Manager Tenant App certificate private key

RabbitMQ

- Product
  - Provide RabbitMQ certificate
  - RabbitMQ certificate private key

Please refer the API reference and POSTMAN sample collection on code.vmware.com for detailed APIs.

The JSON body for the update of a product certificate defines the new certificate(s) (chain and key) to be installed for a product. The certificate should be defined in PEM format.

The certificate and privateKey in the product section of the payload refers to the main product (node) certificate. Other certificates (e.g. for API and Tenant Portal in VMware Cloud Director) are to be specified separately, e.g. **restApi** or **tenantPortal** fields for VMware Cloud Director.

If any of the available certificate is not defined, this will not be updated (e.g. if only the main certificate is defined, the restApi certificate will not be updated. If only restApi certificate is defined, the main certificate will not be updated).

The current environment the product is part of, should be defined in VMware Cloud Provider Lifecycle Manager prior to running this operation.
If the environment was not created as within this instance of VMware Cloud Provider Lifecycle Manager, the environment has to be imported first.

This operation will change the certificate in the product and update the currently known environment.

Get Certificate Information

Method: GET

URL: /api/v1/lcm/environment/{environmentId}/product/{productId}/certificate

Header: name: JSESSIONID - value: a valid jsessionid

Response Body:

```
{
  "product": {
    "certificate": "<certificate/chain PEM>",
    "validUntil": "<expiry date>",
    "thumbPrint": "<certificate thumbprint>"
  }
  "<otherCertName>": {
    "certificate": "<certificate/chain PEM>",
    "validUntil": "<expiry date>",
    "thumbPrint": "<certificate thumbprint>"
  }
}
```

The information that can be retrieved for a product certificate is the public certificate in PEM format, the validity (expiry date) and the thumbprint.

The current environment the product is part of, should be defined in VMware Cloud Provider Lifecycle Manager prior to running this operation.

Abbreviations

VCD	VMware Cloud Director
vROPS	vRealize Operations Manager
SDDC	Software Defined Datacenter
LCM	Lifecycle Manager
VCF	VMware Cloud Foundation
vROPS TA	vRealize Operations Manager Tenant App
VDC	Virtual Datacenter
BOM	Bill Of Materials

Conclusion

This deployment guide covered steps to facilitate customers to deploy VMware Cloud Provider Lifecycle Manager on VMware Cloud Foundation or any SDDC, deploy and manage components like VMware Cloud Director, Usage Meter, vRealize Operations Manager Tenant App and RabbitMQ using VMware Cloud Provider Lifecycle Manager. This document also delineates the Day 2 Operations like node management and updating certificates of the products like VMware Cloud Director, RabbitMQ, Usage Meter and vRealize Operations Tenant App.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.