



## Installing OpenShift 4.5 on VMware vSphere

[New and Changed Information](#) 2

[OpenShift 4.5 on VMware vSphere](#) 2

[Prerequisites for Installing OpenShift 4.5 on VMware vSphere](#) 3

[Install OpenShift 4.5 on VMware vSphere](#) 3

[Sample Files for Installing OpenShift 4.5 on VMware vSphere](#) 5

Revised: April 7, 2022

## New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Cisco ACI CNI plug-in Release Version	Feature
5.1(1)	Support for Red Hat OpenShift 4.5 on VMware vSphere 7 User-Provisioned Infrastructure (UPI).

## OpenShift 4.5 on VMware vSphere

The Cisco Application Centric Infrastructure (ACI) supports Red Hat OpenShift 4.5 on VMware vSphere 7 User-Provisioned Infrastructure (UPI). This document provides the instructions on using Ansible playbooks to provision OpenShift 4.5 on VMware vSphere with the Cisco ACI Container Network Interface (CNI) plug-in.

The Ansible playbooks provision virtual machines (VMs) with the needed interface configuration and generate the ignition configuration files. You must deploy your own DHCP, DNS, and load-balancing infrastructure following high-availability best practices.

The Ansible playbooks are available on [GitHub](#).

The following are the Ansible playbooks:

- `asserts.yml`: This playbook performs basic validations of variable declarations in the `all.yml` file.
- `setup.yml`: This playbook performs the following tasks:
  - Configures the orchestrator node:
    - Installs Terraform, the OpenShift client, and the OpenShift installer. It creates the following: Terraform variables for the bootstrap, master, and worker nodes; the master and worker machine-config operator; the OpenShift install config file.
    - Configures load balancer node: It disables Security-Enhanced Linux (SELinux), configures HAProxy, sets up DHCP and DNS if selected.  
  
This optional step configures these three components only if you set the `provision_dhcp`, `provision_dns`, and `provision_lb` variables to true.
- `oshift_prep.yml`:
  - Sets up the install and bootstrap directories.
  - Generates manifests using `openshift-install`.
  - Adds the additional machine-config operator manifests.
  - Adds the Cisco ACI-CNI manifests.
  - Creates a backup of the manifests.
  - Sets up the bootstrap, master, and worker nodes ignition files.
  - Copies the bootstrap ignition file to the loadbalancer node.

- `create_nodes.yml`:
  - Provisions the bootstrap, master, and worker nodes, using Terraform.
  - Sets up a cron job to approve Cisco Cloud Services Routers (CSRs) if selected.
- `delete_nodes.yml`: Deletes the nodes.

## Prerequisites for Installing OpenShift 4.5 on VMware vSphere

To install OpenShift Container Platform (OCP) 4.5 on VMware vSphere, fulfill the following prerequisites:

### Cisco ACI

- Download the `acc-provision` tool version 5.1(x) or later.

Specify the “`--flavor`” option value as “`openshift-4.5-esx`,” and use the “`-z`” option. The tool creates a `.tar` archive file as specified by the “`-z`” option value. You need this archive file during installation.

Make sure that the Cisco Application Centric Infrastructure (ACI) container images that are specified as input to the `acc-provision` tool are version TBD or later.

### VMware vSphere

Obtain user credentials with privileges to create virtual machines (VMs).

### OpenShift

Obtain the following from the Red Hat website:

- The OCP4 Open Virtualization Appliance (OVA)
- OCP4 client tools
- Pull Secret

## Install OpenShift 4.5 on VMware vSphere




---

**Note** See [Sample Ansible group\\_vars/all.yml File](#), on page 6.

---

### Before you begin

Complete the tasks in the section [Prerequisites for Installing OpenShift 4.5 on VMware vSphere](#), on page 3.

It is recommended to see the *RedHat OpenShift documentation* for prerequisites and other details about Installing a Cluster on vSphere.

## Procedure

---

- Step 1** Provision the Cisco Application Centric Infrastructure (ACI) fabric using the `acc-provision` utility:
- ```
acc-provision -a -c acc_provision_input.yaml -u admin -p ### -f openshift-4.5-esx -z manifests.tar.gz
```
- Note** See [Sample acc-provision-input File, on page 5](#).
- Note** Due to Python 3 dependencies that are currently available only on RHEL8, `acc-provision` tool is supported to only run on RHEL8 operating system.
- Step 2** Once the Cisco ACI fabric is provisioned, verify that a port group with the name `system_id_vlan_kubeapi_vlan` is created under distributed switch.
- This document refers to this port group as `api-vlan-portgroup`.
- Step 3** In VMware vSphere, import the OpenShift Container Platform 4 (OCP4) Open Virtual Appliance (OVA) image.
- Specify `api-vlan-portgroup` as the port group for the network interface.
- Step 4** Provision a Red Hat Enterprise load balancer virtual machine (VM) with the network interface that is connected to the `api-vlan-portgroup`.
- The Ansible playbooks optionally configure this VM as a load balancer, DNS server, and DHCP server for the OpenShift cluster.
- Step 5** Provision a Red Hat Enterprise orchestrator VM with the network interface that is connected to the `api-vlan-portgroup`.
- The Ansible playbooks play from the orchestrator VM.
- Step 6** Perform the following tasks on the orchestrator VM:
- Clone the Git repository on GitHub: [https://github.com/noironetworks/openshift\\_vsphere\\_upi](https://github.com/noironetworks/openshift_vsphere_upi).
  - Checkout the "ocp45" branch.
  - Generate Secure Shell (SSH) keys and copy them to the load balancer VM.
  - Enable the `rhel-7-server-ansible-2.9-rpms` repository.
  - Update the Ansible package to the latest version.
  - Change the directory to the Git-cloned directory.
  - Install the Ansible module requirements:

```
ansible-galaxy install -r requirements.yaml
```
  - Edit the `groups/all.yml` and `hosts.ini` files and set the values that your site requires.

**Note** See [Sample hosts.ini file, on page 9](#).
  - Perform basic validation of variable values using the `asserts.yml` playbook:

```
ansible-playbook asserts.yml
```
  - Copy the archive file that was created by the `acc-provision` utility to the `files` directory, giving it the name `aci_manifests.tar.gz`.
  - Run the Ansible `setup` playbook:

```
ansible-playbook setup.yml
```

Running the `setup` playbook configures the orchestrator and load balancer VMs.

- l) Run the Ansible `osshift_prep` playbook:

```
ansible-playbook oshift_prep.yml
```

Running the `osshift_prep` generates the OpenShift manifests and ignition files.

- m) Run the Ansible `create_nodes` playbook:

```
ansible-playbook create_nodes.yml
```

The `create_nodes` playbook creates the VMs. After the VMs are created, the OCP4 installation process starts in the background. At this stage, you should be able to access the cluster APIs by using the `kubeconfig` files created by the installer.

The `kubeconfig` files are located at `base_dir/bootstrap/auth` directory. The `base_dir` is set in `group_vars/all.yml` file, and the default value is `/root/ocpinstall`.

---

## What to do next

You can use the commands `openshift-install wait-for bootstrap-complete` and `openshift-install wait-for install-complete` to check the progress of the installation. Execute the commands from the bootstrap directory.

## Sample Files for Installing OpenShift 4.5 on VMware vSphere

This section contains sample files that you need for installing OpenShift 4.5 on VMware vSphere.

### Sample `acc-provision-input` File

The following is a sample `acc-provision-input.yml`. The highlighted or bold values are those that you must modify to meet your site requirements.

```
#
# Configuration for ACI Fabric
#
aci_config:
  system_id: ocp4aci
  #apic-refresh-time: 1200
  apic_hosts:
    - 1.1.1.1
  vmm_domain:
    encap_type: vxlan
    mcast_range:                # Every opflex VMM must use a distinct range
      start: 225.28.1.1
      end: 225.28.255.255
    nested_inside:
      type: vmware
      name: hypflex-vswitch

# Include if nested inside a VMM:
type: vmware                # Specify the VMM vendor (supported: vmware)
name: hyperflex-vswitch    # Specify the name of the VMM domain
installer_provisioned_lb_ip: 10.213.0.201

# The following resources must already exist on the APIC.
# They are used, but not created, by the provisioning tool.
aep: hypf-aep
vrf:                        # This VRF used to create all kubernetes EPs
```

```

    name: k8s18_vrf
    tenant: common
l3out:
    name: k8s18
    external_networks:
    - k8s18_net

#
# Networks used by ACI containers
#
net_config:
    node_subnet: 192.168.18.1/24
    pod_subnet: 10.128.0.1/16      # Subnet to use for Kubernetes
                                   #   Pods/CloudFoundry containers

    extern_dynamic: 10.3.0.1/24   # Subnet to use for dynamic external IPs
    extern_static: 10.4.0.1/24   # Subnet to use for static external IPs
    node_svc_subnet: 10.5.0.1/24 # Subnet to use for service graph
    kubeapi_vlan: 35
    service_vlan: 36
    infra_vlan: 3901
    #interface_mtu: 1600
    #service_monitor_interval: 5 # IPSLA interval probe time for PBR tracking
                                   # default is 0, set to > 0 to enable, max: 65535
    #pbr_tracking_non_snat: true  # Default is false, set to true for IPSLA to
                                   # be effective with non-snat services

#
# Configuration for container registry
# Update if a custom container registry has been setup
#
kube-config:
    image_pull_policy: Always
    ovs_memory_limit: 1Gi

registry:
    image_prefix: docker.io/noirolabs
    aci_containers_controller_version: 5.1.1.0.1ae238a
    aci_containers_host_version: 5.1.1.0.1ae238a
    cnideploy_version: 5.1.1.0.1ae238a
    opflex_agent_version: 5.1.1.0.1ae238a
    openswitch_version: 5.1.1.0.1ae238a
    aci_containers_operator_version: 5.1.1.0.1ae238a
logging:
    controller_log_level: debug
    hostagent_log_level: debug
    opflexagent_log_level: debug

```

## Sample Ansible `group_vars/all.yml` File

The following is a sample `group_vars/all.yml`. The highlighted or bold values are those that you must modify to meet your site requirements.

```

#provision_dhcp
#   type: boolean, True or False
#   required: yes
#   notes: If set to true, load balancer is configured as dhcp server.
#           If false, it is assumed that the dhcp server pre-exists
provision_dhcp: True

#domainname
#   type: string, base dns domain name, cluster metadata name is added as subdomain to this
#   required: yes

```

```

domainname: ocplab.local

#provision_dns
# type: boolean, True or False
# required: yes
# notes: If set to true, load balancer is configured as dns server.
#       If false, it is assumed that the dns server pre-exists.
provision_dns: True

#dns_forwarder:
# type: ip address
# required: yes
# notes: This value is used when setting up a dhcp service and also for 'forwarders' value in dns configuration.
dns_forwarder: 172.28.184.18

#loadbalancer_ip:
# type: ip address or resolvable hostname
# required: yes
# notes: This host is configured as load balancer for cluster and also as dhcp and dns server if required
loadbalancer_ip: 192.168.18.201. This IP address is the same as the one that you configure in
installer_provisioned_lb_ip in the acc-provision config.

#auto_approve_csr:
# type: boolean
# required: yes
# notes: when set to true, sets up a cron job to auto approve openshift csr
auto_approve_csr: True

#proxy_env
#
proxy_env:
  #donot remove dummy field, irrespective of whether setup needs a proxy or not.
  dummy: dummy
  #set the http/https proxy server, if setup does not need proxy, comment the below values.
  #these values are used for ansible tasks and also passed on to openshift installer
  http_proxy: http://1.1.1.1:80
  https_proxy: http://1.1.1.1:80
  no_proxy: 1.2.1.1,1.2.1.2

#packages
# defines the urls to download terraform, openshift client and openshift-install tools from.
packages:
  validate_certs: False
  terraform_url: https://releases.hashicorp.com/terraform/0.12.26/terraform_0.12.26_linux_amd64.zip
  openshift_client_linux_url:
https://mirror.openshift.com/pub//openshift-v4/x86_64/clients/ocp/4.5.18/openshift-client-linux-4.5.18.tar.gz
  openshift_install_linux_url:
https://mirror.openshift.com/pub//openshift-v4/x86_64/clients/ocp/4.5.18/openshift-install-linux-4.5.18.tar.gz

#default_aci_manifests_archive:
# default filename that is searched under files directory.
# this can be overridden by passing extra parameter aci_manifests_archive on ansible command line
default_aci_manifests_archive: aci_manifests.tar.gz

#vsphere
vsphere:
  server: hypf.local.lab
  user: administrator@vsphere.local
  passwd: xxxx
  allow_unverified_ssl: true
  datacenter_name: hypflex-dc
  cluster_name: hypflex-cluster
  datastore_name: noiro
  RHCOS_template_name: RHCOS443

```

```

#base_dir
# type: directory path
# required: yes
# notes: All install files and directories are created under this directory
base_dir: /root/ocpinstall

#bootstrap node variables
bootstrap_vars:
  node_mac: 00:50:56:b2:c7:a1 #required
  node_ip: 192.168.18.210 #required
  cpu_count: 8 #optional: defaults to 4
  memory_KB: 16384 #optional: defaults to 8192
  disk_size_MB: 40 #optional: defaults to 40

masters_vars:
  cpu_count: 8 #optional: defaults to 4
  memory_KB: 16384 #optional: defaults to 16384
  disk_size_MB: 40 #optional: defaults to 40
  nodes:
    #mac address and ip address for each node is required
    - master-1:
      api_mac: 00:50:56:b2:c7:b1
      ip: 192.168.18.211
    - master-2:
      api_mac: 00:50:56:b2:c7:b3
      ip: 192.168.18.212
    - master-3:
      api_mac: 00:50:56:b2:c7:b5
      ip: 192.168.18.213

workers_vars:
  cpu_count: 8 #optional: defaults to 4
  memory_KB: 16384 #optional: defaults to 16384
  disk_size_MB: 40 #optional: defaults to 40
  nodes:
    #mac address and ip address for each node is required
    - worker-1:
      api_mac: 00:50:56:b2:c7:c1
      ip: 192.168.18.214
    - worker-2:
      api_mac: 00:50:56:b2:c7:c3
      ip: 192.168.18.215

#user_ssh_key:
# required: no
# notes: if specified this key is setup on nodes, else ssh key of current
# user is used.
user_ssh_key: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD...

#additional_trust_bundle:
# required: no
# notes: use this field to add a certificate for private repository
#
# example:
#additional_trust_bundle: |
# -----BEGIN CERTIFICATE-----
# MIIDDCCAfQCCQDuOnV7XBjpODANBgkqhkiG9w0BAQsFADBIMQswCQYDVQQGEwJV
# UzELMAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ21zY28xDjAM
# -----END CERTIFICATE-----

#openshift_pullsecret:
# required: yes
# example:

```



```
# openshift_pullsecret: {"auths":{"cloud.openshift.com":{"auth":.....}}
openshift_pullsecret: xxx
```

## Sample `hosts.ini` file

The following is a sample `hosts.ini`. The highlighted or bold values are those that you must modify to meet your site requirements.

```
[orchestrator]
192.168.18.200
```

```
[lb]
192.168.18.201
```

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA 95134-1706  
USA

**Asia Pacific Headquarters**  
CiscoSystems(USA)Pte.Ltd.  
Singapore

**Europe Headquarters**  
CiscoSystemsInternationalBV  
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).