Deployment of a RedHat OpenShift Workload Domain in the First Region

16 JUL 2020

VMware Validated Design 6.0.1

VMware Cloud Foundation 4.0.1

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Deployment of a RedHat OpenShift Workload Domain in the First Region

1

The *Deployment of a RedHat OpenShift Workload Domain Workload Domain in the First Region* documentation provides step-by-step instructions for installing and configuring the virtual infrastructure workload domain with RedHat OpenShift installed on top of it, based on VMware Validated Design.

The *Deployment of a RedHat OpenShift Workload Domain Workload Domain in the First Region* documentation does not contain step-by-step instructions for performing all required post-configuration tasks because their nature often depends on the requirements of your organization.

Intended Audience

The *Deployment of a RedHat OpenShift Workload Domain Workload Domain in the First Region* documentation is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to deploy in a short time and manage a software-defined data center (SDDC) that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required VMware Software

Deployment of a RedHat OpenShift Workload Domain Workload Domain in the First Region is compliant and validated with certain product versions. See VMware Validated Design Release Notes.

Required Third-Party Software

Deployment of a RedHat OpenShift Workload Domain Workload Domain in the First Region is compliant and validated with a certain version of the OpenShift Container Platform. See VMware Validated Design Release Notes.

Before You Apply This Guidance

The sequence of the documentation of this design follows the stages for implementing and maintaining an SDDC. See Documentation Map for VMware Validated Design.

To deploy a workload domain by following the prescriptive path of VMware Validated Design, your environment must have a certain configuration. To apply *Deployment of a RedHat OpenShift Workload Domain Workload Domain in the First Region*, you must:

- Complete the *Planning and Preparation Workbook* with your deployment options included.
- Deploy a single-region SDDC management domain. See *Deployment of the Management Domain in the First Region*.
- Optionally, read *Architecture and Design for a Red Hat OpenShift Workload Domain*.

The same requirement applies if you are following the VMware Cloud Foundation documentation to deploy a virtual infrastructure workload domain. See the VMware Cloud Foundation documentation.

Prepare the Environment for Deployment of a Virtual Infrastructure Workload Domain in Region A

2

Before you start the deployment of the Workload Domain, your environment must meet target prerequisites and be in a specific starting state. Prepare the platform by deploying and configuring the necessary infrastructure, operational, and management components.

- Prepare ESXi Hosts for Implementation of a Virtual Infrastructure Workload Domain in Region A

  To prepare the virtual infrastructure layer of the workload domain, you first install ESXi on all the hosts that will form the shared edge and workload cluster for the workload domain, then you configure the management network, DNS, NTP, and SSH services.

Prepare ESXi Hosts for Implementation of a Virtual Infrastructure Workload Domain in Region A

To prepare the virtual infrastructure layer of the workload domain, you first install ESXi on all the hosts that will form the shared edge and workload cluster for the workload domain, then you configure the management network, DNS, NTP, and SSH services.

Procedure

1. Prerequisites for Installation of ESXi Hosts for a Virtual Infrastructure Workload Domain in Region A
2. Install ESXi Interactively on All Hosts for a Virtual Infrastructure Workload Domain in Region A
3. Configure the Network on All Hosts for a Virtual Infrastructure Workload Domain in Region A

   After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.
4. Configure the Virtual Machine Network Port Group on All Hosts for a Virtual Infrastructure Workload Domain in Region A

   You perform the network configuration for each ESXi host by using the VMware Host Client.

5 Configure SSH and NTP on All Hosts for a Virtual Infrastructure Workload Domain in Region A

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service. You also configure the NTP service to avoid time synchronization issues in the SDDC.

Prerequisites for Installation of ESXi Hosts for a Virtual Infrastructure Workload Domain in Region A

You must prepare for the installation and configuration of all VMware ESXi™ hosts in the shared edge and workload cluster.

Before you start:

- Download the ESXi ISO.
- Make sure that you have a host machine for SDDC access. You use this host to connect to the data center and perform configuration steps.
- Verify that you have the completed Planning and Preparation Workbook with the deployment option included.
- Verify the **Prerequisite Checklist** sheet in the Planning and Preparation Workbook.

Install ESXi Interactively on All Hosts for a Virtual Infrastructure Workload Domain in Region A

Install ESXi on all hosts in the shared edge and workload cluster interactively.

Repeat this procedure for all hosts in the shared edge and workload cluster. Enter the respective values from the completed Planning and Preparation Workbook.

Procedure

1. Power on the sfo01-w01-esx01 host.
2. Mount and boot from ESXi ISO.
3. On the **Welcome to the VMware ESXi Installation** screen, press Enter to start the installation.
4. On the **End User License Agreement (EULA)** screen, press F11 to accept the EULA.
5. On the **Select a Disk to Install or Upgrade** screen, select the internal SD card to install ESXi on and press Enter.
6. On the **Please select a keyboard layout** screen, select the keyboard layout and press Enter.
7. On the **Enter a root password** screen enter the ***esxi_root_user_password***, enter the password a second time to confirm the spelling, and press Enter.
8. On the **Confirm Install** screen, press F11 to start the installation.
9. On the **Installation Complete** screen, press Enter to reboot the host.
10. Repeat this procedure for all remaining hosts.

Configure the Network on All Hosts for a Virtual Infrastructure Workload Domain in Region A

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

Perform the following tasks to configure the host network settings:

- Configure the network adapter (vmk0) and VLAN ID for the Management Network.
- Configure the IP address, subnet mask, gateway, DNS server, and FQDN for the ESXi host.

Repeat this procedure for all hosts in the shared edge and workload cluster. Enter the respective values from the completed *Planning and Preparation Workbook*.

Procedure

1 Open the DCUI on the sfo01-w01-esx01.sfo.rainpole.io ESXi host.

   a Open a console window to the host.

   b Press F2 to enter the DCUI.

   c Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure the network.

   a Select **Configure Management Network** and press Enter.

   b Select **VLAN (Optional)** and press Enter.

   c Enter **1631** as the VLAN ID for the Management Network and press Enter.

   d Select **IPv4 Configuration** and press Enter.

   e Configure the IPv4 network settings and press Enter.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.31.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.31.253

   f Select **DNS Configuration** and press Enter.

g Configure the DNS settings and press Enter.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.16.11.5
Alternate DNS Server	172.16.11.4
Hostname	sfo01-w01-esx01.sfo.rainpole.io

h Select **Custom DNS Suffixes** and press Enter.

i Ensure that there are no suffixes listed and press Enter.

3 Press Escape to exit and press Y to confirm the changes.

4 Repeat this procedure for all remaining hosts.

Configure the Virtual Machine Network Port Group on All Hosts for a Virtual Infrastructure Workload Domain in Region A

You perform the network configuration for each ESXi host by using the VMware Host Client.

You configure the VLAN ID of the VM Network port group on the vSphere Standard Switch. This configuration provides connectivity and common network configuration for the virtual machines that reside on each host.

You repeat this procedure for all hosts in the shared edge and workload cluster.

Procedure

1 In a Web browser, log in to the first ESXi host for the VI workload domain by using the VMware Host Client.

Setting	Value
URL	https://sfo01-w01-esx01.sfo.rainpole.io/ui
User name	root
Password	*esxi_root_user_password*

2 Click **OK** to join the Customer Experience Improvement Program.

3 Configure a VLAN for the VM Network port group.

a In the navigation pane, click **Networking**.

b Click the **Port groups** tab, select the **VM network** port group, and click **Edit Settings**.

c On the **Edit port group - VM network** page, enter 1631 for **VLAN ID**, and click **Save**.

4 Repeat this procedure for all remaining hosts.

Configure SSH and NTP on All Hosts for a Virtual Infrastructure Workload Domain in Region A

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service. You also configure the NTP service to avoid time synchronization issues in the SDDC.

Repeat this procedure for all hosts in the shared edge and workload cluster.

Procedure

1 In a Web browser, log in to the first ESXi host for the VI workload domain by using the VMware Host Client.

Setting	Value
URL	https://sfo01-w01-esx01.sfo.rainpole.io/ui
User name	root
Password	*esxi_root_user_password*

2 Configure and start the TSM-SSH service.
   a In the navigation pane, click **Manage** and click the **Services** tab.
   b Select the **TSM-SSH** service, and click the **Actions** menu.
   c Select **Policy** and click **Start and stop with host**.
   d To start the service, click **Start**.
3 Configure and start the NTP service.
   a In the navigation pane, click **Manage**, and click the **System** tab.
   b Click **Time & date** and click **Edit settings**.
   c On the **Edit time configuration** page, select the **Use Network Time Protocol (enable NTP client)** radio button, and change the NTP service startup policy to **Start and stop with host**.
   d In the **NTP servers** text box, enter **`ntp.sfo.rainpole.io`**, and click **Save**.
   e To start the service, click **Actions**, select **NTP service**, and click **Start**.
4 Repeat this procedure for all remaining hosts.

Virtual Infrastructure Workload Domain Implementation in Region A

3

To deploy the workload domain end-to-end by using automation, use SDDC Manager.

Procedure

1 Prerequisites for a Virtual Infrastructure Workload Domain Deployment in Region A

Before you start the deployment of the workload domain, verify that your environment fulfills the requirements for this process.

2 Create a Network Pool in SDDC Manager for a Virtual Infrastructure Workload Domain in Region A

In order to commission and use ESXi hosts for the workload domain, you must first create a network pool in SDDC Manager which is used to assign IP addresses to the vMotion and vSAN VMkernel ports.

3 Commission ESXi Hosts in SDDC Manager for a Virtual Infrastructure Workload Domain in Region A

After the network pool has been created, you can commission the ESXi hosts that you prepared for your workload domain.

4 Deploy a Virtual Infrastructure Workload Domain by Using SDDC Manager in Region A

After all hosts are commissioned in SDDC Manager, deploy the workload domain using a JSON specification by using the SDDC Manager API Explorer.

5 Create an NSX-T Edge Cluster by using SDDC Manager for the Virtual Infrastructure Workload Domain in Region A

For availability of the routing services and connectivity to the external network, you create a two-node cluster of NSX-T Edge nodes.

Prerequisites for a Virtual Infrastructure Workload Domain Deployment in Region A

Before you start the deployment of the workload domain, verify that your environment fulfills the requirements for this process.

Verify that your environment satisfies the following prerequisites for the deployment of the workload domain.

Table 3-1. Deployment Prerequisites

Prerequisite	Value
Environment	■ Verify that the management domain has been deployed and is operating normally. ■ Verify that your environment is configured for deployment of the workload domain. See Chapter 2 Prepare the Environment for Deployment of a Virtual Infrastructure Workload Domain in Region A.
Physical Network	Verify that your environment meets all physical network requirements, all host names and IP addresses are allocated for external services and domain components.
Active Directory	Verify that Active Directory is configured with all child domains and all service accounts, groups, and computer objects are created and configured.
DNS	Verify that DNS entries are configured for the root and child domains.
NTP Services	Verify that you have external to the SDDC, two NTP servers configured with time synchronization operational on all ESXi hosts and AD domain controllers.
Software Features	■ Verify that you have the completed Planning and Preparation Workbook with the deployment option included. ■ Verify the **Prerequisite Checklist** sheet in the Planning and Preparation Workbook.

Create a Network Pool in SDDC Manager for a Virtual Infrastructure Workload Domain in Region A

In order to commission and use ESXi hosts for the workload domain, you must first create a network pool in SDDC Manager which is used to assign IP addresses to the vMotion and vSAN VMkernel ports.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the navigation pane, click **Administration > Network Settings**.

3 On the **Network Settings** page, click **Create network pool**.

4 On the **Create Network Pool** page, enter **`sfo-w01-np01`** as network pool name and select the **vSAN** check box.

5 In the **vSAN Network Information** pane, enter the values and click **Add**.

Setting	Value
VLAN ID	1633
MTU	9000
Network	172.16.33.0
Subnet Mask	255.255.255.0
Default Gateway	172.16.33.253
Included IP Address Ranges	172.16.33.101 to 172.16.33.104

6 In the **vMotion Network Information** pane, enter the values and click **Add**.

Setting	Value
VLAN ID	1632
MTU	9000
Network	172.16.32.0
Subnet Mask	255.255.255.0
Default Gateway	172.16.32.253
Included IP Address Ranges	172.16.32.101 to 172.16.32.104

7 Click **Save**.

Commission ESXi Hosts in SDDC Manager for a Virtual Infrastructure Workload Domain in Region A

After the network pool has been created, you can commission the ESXi hosts that you prepared for your workload domain.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 On the **SDDC Manager Dashboard**, click **Commission hosts** to start the **Commission hosts** wizard.

3 Complete the checklist to verify that you comply with all requirements to commission the hosts, and click **Proceed**.

4 On the **Host Addition and Validation** page, add all hosts for the workload domain.

a Under **Add Hosts**, enter the values and click **Add**.

Setting	Value
Host FQDN	sfo01-w01-esx01.sfo.rainpole.io
Storage Type	vSAN
Network Pool Name	sfo-w01-np01
User Name	root
Password	*root_password*

b Repeat to add the remaining hosts for the workload domain.

5 Under **Hosts Added**, select the **FQDN** check box to select all hosts and click the **Confirm FingerPrint** check box.

6 Click **Validate All**.

7 After you see the `Host Validated Successfully` message, click **Next**.

8 On the **Review** page, click **Commission**.

Deploy a Virtual Infrastructure Workload Domain by Using SDDC Manager in Region A

After all hosts are commissioned in SDDC Manager, deploy the workload domain using a JSON specification by using the SDDC Manager API Explorer.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the navigation pane, select **Developer Center**.

3 On the **VMware Cloud Foundation Developer Center** page, select the **API Explorer** tab.

4 Retrieve the unique IDs for each ESXi for the workload domain.

   a Expand **APIs for managing Hosts** and click **GET /v1/hosts**.

   b In the **status** text box, enter `UNASSIGNED_USEABLE` and click **Execute**.

   c In the **Response** section click **PageOfHost**.

   d Save the `id` value of each host for your workload domain to use it later.

5 Prepare a JSON specification to deploy the workload domain.

a Copy an paste the JSON specification in a text editor.

```
{
  "domainName": "sfo-w01",
  "orgName": "Rainpole",
  "vcenterSpec": {
    "name": "sfo-w01-vc01",
    "networkDetailsSpec": {
        "ipAddress": "172.16.11.64",
        "dnsName": "sfo-w01-vc01.sfo.rainpole.io",
        "gateway": "172.16.11.1",
        "subnetMask": "255.255.255.0"
  },
  "rootPassword": "vcenter_root_password",
  "datacenterName": "sfo-w01-dc01"
},
  "computeSpec": {
      "clusterSpecs": [
        {
          "name": "sfo-w01-cl01",
          "hostSpecs": [
              {
                "id": "REPLACE_WITH_ID_FOR_sfo01-w01-esx01.sfo.rainpole.io",
                "licenseKey":"esxi-hosts-license-that-exists-in-sddc-manager",
                "hostNetworkSpec": {
                       "vmNics": [
                           {
                           "id": "vmnic0",
                           "vdsName": "sfo-w01-cl01-vds01"
                        },
                        {
                           "id": "vmnic1",
                           "vdsName": "sfo-w01-cl01-vds01"
                        }
                    ]
                 }
              },
              {
                "id": "REPLACE_WITH_ID_FOR_sfo01-w01-esx02.sfo.rainpole.io",
                "licenseKey":"esxi-hosts-license-that-exists-in-sddc-manager",
                "hostNetworkSpec": {
                       "vmNics": [
                           {
                           "id": "vmnic0",
                           "vdsName": "sfo-w01-cl01-vds01"
                        },
                        {
                           "id": "vmnic1",
                           "vdsName": "sfo-w01-cl01-vds01"
                        }
                    ]
                 }
              },
```

```
            {
              "id": "REPLACE_WITH_ID_FOR_sfo01-w01-esx03.sfo.rainpole.io_ID",
              "licenseKey":"esxi-hosts-license-that-exists-in-sddc-manager",
              "hostNetworkSpec": {
                     "vmNics": [
                         {
                         "id": "vmnic0",
                         "vdsName": "sfo-w01-cl01-vds01"
                      },
                      {
                         "id": "vmnic1",
                         "vdsName": "sfo-w01-cl01-vds01"
                      }
                   ]
                }
            },
             {
              "id": "REPLACE_WITH_ID_FOR_sfo01-w01-esx04.sfo.rainpole.io",
              "licenseKey":"esxi-hosts-license-that-exists-in-sddc-manager",
              "hostNetworkSpec": {
                     "vmNics": [
                         {
                         "id": "vmnic0",
                         "vdsName": "sfo-w01-cl01-vds01"
                      },
                      {
                         "id": "vmnic1",
                         "vdsName": "sfo-w01-cl01-vds01"
                      }
                   ]
                 }
              }
            ],
     "datastoreSpec": {
         "vsanDatastoreSpec": {
             "failuresToTolerate": 1,
             "licenseKey": "vsan-license-key",
             "datastoreName": "sfo-w01-cl01-ds-vsan01"
        }
    },
    "networkSpec": {
     "vdsSpecs": [
       {
         "name": "sfo-w01-cl01-vds01",
         "portGroupSpecs": [
           {
             "name": "sfo01-w01-cl01-vds01-pg-mgmt",
             "transportType": "MANAGEMENT"
           },
           {
             "name": "sfo01-w01-cl01-vds01-pg-vsan",
             "transportType": "VSAN"
           },
           {
              "name": "sfo01-w01-cl01-vds01-pg-vmotion",
```

```
              "transportType": "VMOTION"
            }
          ]
        }
      ],
          "nsxClusterSpec": {
              "nsxTClusterSpec": {
                  "geneveVlanId": 1634
                }
            }
           }
         }
        ]
      },
    "nsxTSpec": {
      "nsxManagerSpecs": [
      {
        "name": "sfo-w01-nsx01a",
        "networkDetailsSpec": {
            "ipAddress": "172.16.11.76",
            "dnsName": "sfo-w01-nsx01a.sfo.rainpole.io",
            "gateway": "172.16.11.1",
            "subnetMask": "255.255.255.0"
      }
     },
     {
          "name": "sfo-w01-nsx01b",
          "networkDetailsSpec": {
              "ipAddress": "172.16.11.77",
              "dnsName": "sfo-w01-nsx01b.sfo.rainpole.io",
              "gateway": "172.16.11.1",
              "subnetMask": "255.255.255.0"
       }
      },
      {
          "name": "sfo-w01-nsx01c",
          "networkDetailsSpec": {
              "ipAddress": "172.16.11.78",
              "dnsName": "sfo-w01-nsx01c.sfo.rainpole.io",
              "gateway": "172.16.11.1",
              "subnetMask": "255.255.255.0"
          }
      }
],
      "vip": "172.16.11.75",
      "vipFqdn": "sfo-w01-nsx01.sfo.rainpole.io",
      "licenseKey": "nsx-t-data-center-license-key",
      "nsxManagerAdminPassword": "wld_nsxt_password"
      }
}
```

b Replace the vCenter Server **root** user password, ESXi hosts **root** user password, and NSX-T Manager **admin** user password.

c Replace the license keys for vCenter Server, ESXi hosts, vSAN, and NSX-T Data Center.

d Replace the ESXi hosts `id` value with the ones that you previously saved.

e Save the JSON specification to use it for the deployment of the workload domain.

6 Validate your workload domain JSON file.

a Expand **APIs for managing Domains**, click **POST /v1/domains/validations**.

b In the **Value** text box, enter the content of your workload domain JSON specification file and click **Execute**.

c In the confirmation dialog box, click **Continue**.

d In the **Response** section, expand the **result** and verify the response is `SUCCEEDED`.

7 Deploy the workload domain by using the JSON specification file.

a Expand **APIs for managing Domains** and click **POST /v1/domains**.

b In the **Value** text box, enter the content of your workload domain JSON specification file and click **Execute**.

c In the confirmation dialog box, click **Continue**.

8 Monitor the progress of the deployment from the **Tasks list** pane.

Create an NSX-T Edge Cluster by using SDDC Manager for the Virtual Infrastructure Workload Domain in Region A

For availability of the routing services and connectivity to the external network, you create a two-node cluster of NSX-T Edge nodes.

To support the communication between tenant workloads deployed on the network segments in NSX-T Data Center with tenant workloads deployed on external networks, you configure dynamic routing for the shared edge and workload cluster. Deploy the NSX-T Edge cluster for the workload domain from the SDDC Manager API Explorer by using a JSON specification. You take a sample JSON specification, enter the values for your environment, and use that specification for the deployment.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the navigation pane, click **Developer Center**.

3 On the **VMware Cloud Foundation Developer Center** page, click the **API Explorer** tab.

4 Retrieve the unique ID for the shared edge and workload cluster.
   a Expand **APIs for managing Clusters**, click **GET /v1/clusters**, and click **Execute**.
   b In the **Response** section click **PageOfCluster** and click **Cluster (**sfo-w01-cl01).
   c Save the `ID of the cluster` value to use it later.
5 Prepare a JSON specification to deploy an NSX-T Edge Cluster.
   a Copy an paste the JSON specification in a text editor.
   b Replace the passwords for **admin**,**root**,**audit** users, and **bgp** password.
   c Replace the "`<!REPLACE WITH sfo-w01-cl01 CLUSTER ID !>`" value with the one for the shared edge and workload cluster that you previously saved.
   d Save the JSON specification to use it for the deployment of the NSX-T Edge cluster.
6 Validate your JSON specification.
   a Expand **APIs for managing NSX-T Edge Clusters**, click **POST /v1/edge-clusters/validations**.
   b In the **Value** text box, enter the content of your JSON specification file and click **Execute**.
   c In the confirmation dialog box, click **Continue**.
   d In the **Response** section click **Validation UUID** and copy the ID from **ID of the Validation**.
   e Expand **APIs for managing NSX-T Edge Clusters**, click **GET /v1/edge-clusters/validations/{id}**.
   f Paste the ID from the ID of the Validation into the **Value** box and click **Execute**.
   g In the **Response** section expand the **Validation** result and check the **resultStatus** is `SUCCEEDED`.
7 Run the workflow that deploys the NSX-T Edge cluster for the workload domain in SDDC Manager.
   a Expand **APIs for managing NSX-T Edge Clusters** and click **POST /v1/edge-clusters**.
   b In the **Value** text box, paste the JSON specification that you prepared and click **Execute**.
   c In the confirmation dialog box, click **Continue**.
8 Monitor the progress of the deployment from the **Tasks list** pane.

What to do next

Verify that routing occurs in both the north-south and east-west directions.

- North-south traffic leaving or entering the workload domain, for example, a virtual machine on an overlay network communicating with an end-user device on the corporate network.
- East-west traffic remains in the workload domain, for example, two virtual machines on the same or different segments that communicate to each other.

Post-Deployment Configuration for a Virtual Infrastructure Workload Domain in Region A

4

After you deploy the workload domain by using SDDC Manager, to reach full functionality and operability, perform post-deployment product configuration tasks.

Procedure

1 Join the Virtual Infrastructure Workload Domain vCenter Server to Active Directory in Region A

After you have successfully deployed the workload domain, you must add the Workload domain vCenter Server to your Active Directory. Then add the Active Directory domain as an identity source to vCenter Single Sign-On. Users in the Active Directory domain become visible to vCenter Single Sign-On and can be assigned permissions to view or manage components.

2 Join the ESXi Hosts for the Virtual Infrastructure Workload Domain to Active Directory in Region A

You join the ESXi hosts of the workload domain to Active Directory so that access can be controlled through Active Directory. Repeat this procedure for all hosts in the workload domain.

3 Configure an Active Directory group as the Admin group for all ESXi Hosts of the Virtual Infrastructure Workload Domain in Region A

You assign an Active Directory group as an admin group to each ESXi host of the workload domain to control full administrative access by using Active Directory. Perform this procedure for all hosts in the workload domain.

4 Rename the Resource Pool for the NSX-T Edge Cluster Nodes of the Virtual Infrastructure Workload Domain in Region A

You rename the resource pool dedicated for the NSX-T Edge cluster nodes to **sfo-w01-cl01-rp-sddc-edge** to align to a consistent naming standard.

5 Group the NSX-T Edge Cluster Nodes in a VM and Template Folder for the Virtual Infrastructure Workload Domain in Region A

Create a folder in the workload domain to group the NSX-T Edge cluster nodes and move them to that folder.

6 Move Management and Network Components for the Virtual Infrastructure Workload Domain to the Designated VM Folders in Region A

You move the workload domain vCenter Server and NSX-T Manager cluster nodes deployed in the management domain to designated folders for these components.

7 Enable Health Check on the vSphere Distributed Switch for the Virtual Infrastructure Workload Domain in Region A

You enable the functionality so that vSphere Distributed Switch Health Check verifies that all VLANs are trunked to all ESXi hosts attached to the vSphere Distributed Switch and the MTU sizes match the physical network.

8 Install Signed Certificates on Virtual Infrastructure Workload Domain Components in Region A

Replace the self-signed certificates of vCenter Server and NSX-T Manager Cluster with signed certificates from the Microsoft Certificate Authority using SDDC Manager for the workload domain.

9 Disable Taking Snapshots for NSX-T Data Center Appliances for the Virtual Infrastructure Workload Domain in Region A

If you are deploying VMware Validated Design 6.0, you manually disable snapshots on NSX-T Data Center appliances. Snapshots and clones are not supported for NSX-T Data Center appliances. Disable the snapshots creation for all NSX-T Data Center appliances in the workload domain.

10 Integration of Workspace ONE Access and NSX-T Data Center for the Virtual Infrastructure Workload Domain in Region A

To provide role based access for the NSX-T Data Center instance for the workload domain, integrate it with Workspace One Access.

Join the Virtual Infrastructure Workload Domain vCenter Server to Active Directory in Region A

After you have successfully deployed the workload domain, you must add the Workload domain vCenter Server to your Active Directory. Then add the Active Directory domain as an identity source to vCenter Single Sign-On. Users in the Active Directory domain become visible to vCenter Single Sign-On and can be assigned permissions to view or manage components.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > Administration**.

3 Under **Single Sign On**, select **Configuration**.

4 On the **Configuration** page, click the **Identity Provider** tab and select **Active Directory Domain**.

5 Select the sfo-w01-vc01.sfo.rainpole.io radio button and click **Join AD**.

6 In the **Join Active Directory Domain** dialog box, enter the settings, and click **Join**.

Setting	Value
Domain	sfo.rainpole.io
Username	svc-domain-join
Password	*svc-domain-join_password*

7 To apply the changes, reboot the vCenter Server appliance.

a Open a Web browser and go to https://sfo-w01-vc01.sfo.rainpole.io:5480.

b Log in to the vCenter Server Appliance Management Interface with the following credentials.

Setting	Value
Username	root
Password	*root_password*

c On the **Summary** page, select **Actions > Reboot**.

d In the **System Reboot** dialog box, click **Yes**.

e Wait for the reboot process to finish.

8 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

9 Verify that the vCenter Server has successfully joined the domain.

a In the **Administration** inventory, under **Single Sign On**, select **Configuration**.

b On the **Configuration** page, select the **Active Directory Domain** tab.

c Select the **sfo-w01-vc01.sfo.rainpole.io** radio button and verify that it has been joined to the Active Directory domain sfo.rainpole.io.

Join the ESXi Hosts for the Virtual Infrastructure Workload Domain to Active Directory in Region A

You join the ESXi hosts of the workload domain to Active Directory so that access can be controlled through Active Directory. Repeat this procedure for all hosts in the workload domain.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > Hosts and Clusters**.

3 Expand **sfo-w01-vc01.sfo.rainpole.io > sfo-w01-dc01 > sfo-w01-cl01**.

4 Select the **sfo01-w01-esx01.sfo.rainpole.io** ESXi host and click the **Configure** tab.

5 Under **System**, select **Authentication Services**.

6 On the **Authentication Services** page, click **Join Domain**.

7 On the **Join Domain** page, enter the settings and click **OK**.

Setting	Value
Domain	sfo.rainpole.io
User name	svc-domain-join
Password	*svc-domain-join_password*

8 Repeat the steps for all ESXi Hosts in the workload domain.

Configure an Active Directory group as the Admin group for all ESXi Hosts of the Virtual Infrastructure Workload Domain in Region A

You assign an Active Directory group as an admin group to each ESXi host of the workload domain to control full administrative access by using Active Directory. Perform this procedure for all hosts in the workload domain.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > Hosts and Clusters**.

3 Expand **sfo-w01-vc01.sfo.rainpole.io > sfo-w01-dc01 > sfo-w01-cl01**.

4 Select the **sfo01-w01-esx01.sfo.rainpole.io** ESXi host and click the **Configure** tab.

5 Under **System**, select **Advanced System Settings**.

6 Click **Edit** and in the **Filter** text box, enter **esxAdmins**.

7 Click the **Value** text box for **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** and enter **ug-esxi-admins** as the value and click **OK**.

8 Repeat this procedure for all remaining hosts in the workload domain.

Rename the Resource Pool for the NSX-T Edge Cluster Nodes of the Virtual Infrastructure Workload Domain in Region A

You rename the resource pool dedicated for the NSX-T Edge cluster nodes to **`sfo-w01-cl01-rp-sddc-edge`** to align to a consistent naming standard.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > Hosts and Clusters**.

3 Expand **sfo-w01-vc01.sfo.rainpole.io > sfo-w01-dc01 > sfo-w01-cl01**.

4 Right-click the only resource pool and click **Rename**.

5 In the **Rename** dialog box, enter **`sfo-w01-cl01-rp-sddc-edge`** and click **OK**.

Group the NSX-T Edge Cluster Nodes in a VM and Template Folder for the Virtual Infrastructure Workload Domain in Region A

Create a folder in the workload domain to group the NSX-T Edge cluster nodes and move them to that folder.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > VMs and Templates**.

3 Expand **sfo-w01-vc01.sfo.rainpole.io > sfo-w01-dc01**.

4 Create the folder for the NSX-T Edge cluster nodes.
   a Right-click **sfo-w01-dc01** and select **New Folder > New VM and Template Folder**.
   b In the **New Folder** window, enter **sfo-w01-fd-edge** and click **OK**.
5 Move the NSX-T Edge cluster nodes to the designated VM folder.
   a Under **sfo-w01-dc01**, drag-and-drop the sfo-w01-en01 to the sfo-w01-fd-edge folder.
   b Under **sfo-w01-dc01**, drag-and-drop the sfo-w01-en02 to the sfo-w01-fd-edge folder.

Move Management and Network Components for the Virtual Infrastructure Workload Domain to the Designated VM Folders in Region A

You move the workload domain vCenter Server and NSX-T Manager cluster nodes deployed in the management domain to designated folders for these components.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-m01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > VMs and Templates**.
3 Expand **sfo-m01-vc01.sfo.rainpole.io > sfo-m01-dc01**.
4 Click **sfo-m01-dc01** and click the **VMs** tab.
5 Move the sfo-w01-vc01 workload domain vCenter Server to the **sfo-m01-fd-mgmt** folder.
   a Right-click the sfo-w01-vc01 VM and click **Move to Folder**.
   b In the **Move to folder** dialog box, select **sfo-m01-fd-mgmt** and click **OK**.
6 Move the NSX-T Manager cluster nodes to the **sfo-m01-fd-nsx** folder.
   a Select all three nodes **sfo-w01-nsx01a**, **sfo-w01-nsx01b**, and **sfo-w01-nsx01c**.
   b Right-click a selected node, and click **Move to Folder**.
   c In the **Move to folder** dialog box, click **Yes** to confirm you want to move all three objects.
   d In the **Move to folder** dialog box, select **sfo-m01-fd-nsx** and click **OK**.

Enable Health Check on the vSphere Distributed Switch for the Virtual Infrastructure Workload Domain in Region A

You enable the functionality so that vSphere Distributed Switch Health Check verifies that all VLANs are trunked to all ESXi hosts attached to the vSphere Distributed Switch and the MTU sizes match the physical network.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > Networking**.

3 Expand **sfo-w01-vc01.sfo.rainpole.io > sfo-w01-dc01**.

4 Select the **sfo-w01-cl01-vds01** vSphere Distributed Switch and click the **Configure** tab.

5 On the **Configure** tab, click **Health Check** and click **Edit**.

6 In the **Edit Health Check Settings** dialog box, select the settings and click **OK**.

Setting	Value
VLAN and MTU state	Enabled
Teaming and failover state	Enabled

Install Signed Certificates on Virtual Infrastructure Workload Domain Components in Region A

Replace the self-signed certificates of vCenter Server and NSX-T Manager Cluster with signed certificates from the Microsoft Certificate Authority using SDDC Manager for the workload domain.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the navigation pane, click **Inventory > Workload Domains**.

3 On the **Virtual Infrastructure (VI)** page, from the table, click the **sfo-w01** workload domain.

4 On the **sfo-w01** page, click the **Security** tab.

5 Generate CSR files for the target components.

a From the table, select the check boxes for the `vcenter` and `nsxt_manager` resources.

b Click **Generate CSR**.

c In the **Generate CSRs** dialog box, configure the settings and click **Generate CSR**.

Setting	Value
Algorithm	RSA
Key Size	2048
Organizational Unit	IT
Organization	Rainpole
Locality	San Francisco
State	CA
Country	US - United States

6 Generate signed certificates for each component.

a From the table, select the check boxes for the `vcenter` and `nsxt_manager` resources.

b Click **Generate Signed Certificates**.

c In the **Generate Certificates** dialog box, from the **Select Certificate Authority** drop-down menu, select **Microsoft**.

d Click **Generate Certificates**.

7 Install the generated signed certificates for each component.

a From the table, select the check boxes for the `vcenter` and `nsxt_manager` resources.

b Click **Install Certificates**.

Disable Taking Snapshots for NSX-T Data Center Appliances for the Virtual Infrastructure Workload Domain in Region A

If you are deploying VMware Validated Design 6.0, you manually disable snapshots on NSX-T Data Center appliances. Snapshots and clones are not supported for NSX-T Data Center appliances. Disable the snapshots creation for all NSX-T Data Center appliances in the workload domain.

This procedure does not apply to VMware Validated Design 6.0.1 and later. Starting with VMware Validated Design 6.0.1, taking snapshots for NSX-T Data Center appliances is disabled by default.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Select **Menu > VMs and Templates**.

3 Expand **sfo-m01-vc01.sfo.rainpole.io > sfo-m01-dc01**.

4 Expand the **sfo-m01-fd-nsx** folder to see all NSX-T Manager cluster nodes.

5 Power off the first NSX-T Data Center appliance.

   a Right-click the **sfo-w01-nsx01a** VM and select **Power > Shut Down Guest OS**.

   b In the **Confirm Guest Shut Down** dialog box, click **Yes** and wait for the VM to shut down.

6 Disable snapshots on the first NSX-T Data Center appliance.

   a Right-click the **sfo-w01-nsx01a** VM and click **Edit Settings**.

   b Click the **VM Options** tab and expand **Advanced**.

   c Under **Configuration Parameters**, click **Edit Configuration**.

   d In the **Configuration Parameters** dialog box, click **Add Configuration Params**.

   e Enter the configuration and click **OK**.

Setting	Value
Name	snapshot.MaxSnapshots
Value	0

   f Click **OK** to save the changes.

7 Right-click the **sfo-w01-nsx01a** VM and select **Power > Power On** to power on the appliance that you configured.

8 Repeat this procedure for the remaining NSX-T Data Center appliances for the workload domain.

Node Type	Location in VMs and Templates Inventory	Node Name
NSX-T Data Center Manager appliances for the workload domain	sfo-m01-vc01.sfo.rainpole.io > sfo-m01-dc01 > sfo-m01-fd-nsx	sfo-w01-nsx01a sfo-w01-nsx01b sfo-w01-nsx01c
NSX-T Data Center Edge nodes for the workload domain	sfo-w01-vc01.sfo.rainpole.io > sfo-w01-dc01 > sfo-w01-fd-edge	sfo-w01-en01 sfo-w01-en02

Integration of Workspace ONE Access and NSX-T Data Center for the Virtual Infrastructure Workload Domain in Region A

To provide role based access for the NSX-T Data Center instance for the workload domain, integrate it with Workspace One Access.

Obtain the Certificate Thumbprint of Workspace ONE Access for the Virtual Infrastructure Workload Domain in Region A

Before you configure the integration of Workspace ONE Access with NSX-T Data Center, you must obtain the certificate thumbprint from the Workspace ONE Access instance.

Procedure

1 Log in to vCenter Server by using a Secure Shell (SSH) client.

Setting	Value
FQDN	sfo-m01-vc01.sfo.rainpole.io
User name	root
Password	*vcenter_server_root_password*

2 To switch to the bash shell, run the `shell` command .

3 To retrieve the SHA-256 thumbprint of the Workspace ONE Access certificate, run the command .

```
openssl s_client –connect sfo–wsa01.sfo.rainpole.io:443 < /dev/null 2> /dev/null | openssl x509
–sha256 –fingerprint –noout –in /dev/stdin
```

4 Save the fingerprint to later integrate NSX-T Data Center with Workspace ONE Access.

Integrate Workspace One and NSX-T Data Center for the Virtual Infrastructure Workload Domain in Region A

You create a remote app access client to integrate NSX-T Data Center Workspace ONE Access. You use the certificate thumbprint, ClientID, and shared secret, to register NSX-T Data Center to identify it as a trusted consumer of the Workspace ONE Access identity and authentication services.

Procedure

1 In a Web browser, log in to the region-specific Workspace ONE Access instance in Region A by using the administration interface.

Setting	Value
URL	https://sfo-wsa01.sfo.rainpole.io/admin
User name	admin
Password	*region_a_wsa_admin_password*
Domain	System Domain

2 On the main navigation bar, from the **Catalog** drop-down menu, select **Settings**.

3 In the left pane, click **Remote app access**.

4 Click **Clients** and click **Create client**.

5 In the **Create client** dialog box, configure the settings, and click **Add**.

Setting	Value
Access type	Service Client Token
Client ID	sfo-w01-nsx01-oauth
Scope	admin
Shared secret	Generate and save a shared secret
Issue Refresh Token	Selected
Token type	Bearer
Access Token Time-To-Live (TTL)	8 hours
Refresh Token Time-To-Live (TTL)	1 month
Idle Token Time-to-Live (TTL)	4 days

6 In a Web browser, log in to the workload domain NSX-T administration interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io
User name	admin
Password	*nsx_admin_password*

7 Configure the integration between NSX-T Data Center and Workspace ONE Access.

a On the main navigation bar, click **System**.

b In the left pane, click **Users and roles**, click the **VMware Identity Manager** tab, and click **Edit**.

The **Edit VMware Identity Manager configuration** dialog box opens.

c In the **Edit VMware Identity Manager configuration** dialog box, configure the settings and click **Save**.

Setting	Value
Integration VMware Identity Manager	Enabled
VMware Identity Manager Appliance	sfo-wsa01.sfo.rainpole.io
OAuth Client ID	sfo-w01-nsx01-oauth
OAuth Client Secret	*Previously generated shared secret*
SSL Thumbprint	*SHA-256 Thumbprint*
NSX Appliance	sfo-w01-nsx01.sfo.rainpole.io

Important To log in with a local account in NSX-T Data Center after you configure Workspace ONE Access as an identity provider, you must append `/login.jsp?local=true` to the NSX-T Manager URL.

Configure Role-Based Access Control for NSX-T Data Center for the Virtual Infrastructure Workload Domain in Region A

After you integrate Workspace ONE Access with NSX-T Data Center, you configure role based access controls to manage access to NSX-T Data Center.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **System**.

3 In the left pane, click **Users and roles** and click the **Users** tab.

4 From the **Add** drop-down menu, click **Role assignments for VIDM**, configure the settings, and click **Save**.

Setting	Value for Group
User/User Group Name	ug-nsx-enterprise-admins@rainpole.io
Roles	Enterprise Admins
Type	VIDM User

Deployment of Red Hat OpenShift

5

After you have completed the required configurations in your workload domain, you can deploy Red Hat OpenShift in your SDDC.

Prerequisites

Prerequisites for Deployment of Red Hat OpenShift 4 in a Virtual Infrastructure Workload Domain

Several internal and external prerequisites must be met before you can begin the deployment of Red Hat OpenShift in a VMware Cloud Foundation virtual infrastructure workload domain.

Infrastructure Prerequisites

You must prepare multiple items for the deployment of Red Hat OpenShift.

- Linux host with access to your software-defined data center (This design is validated with a Fedora Linux 31 host)
- Web server configured on the Linux host
- NFS export
  - Allowed in: 192.168.23.0/24, 192.168.24.0/24
  - Size: 100GB
- Configure additional DNS records
- Obtain additional VMware software
- Obtain Red Hat OpenShift software

Table 5-1. Additional Required DNS Records

Host Name	IP Address	Record Type
control-plane-0.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.10	A
control-plane-1.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.11	A

Table 5-1. Additional Required DNS Records (continued)

Host Name	IP Address	Record Type
control-plane-2.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.12	A
worker-0.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.20	A
worker-1.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.21	A
worker-2.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.22	A
bootstrap.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.30	A
etcd-0.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.10	A
etcd-1.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.11	A
etcd-2.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.12	A
api.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.10	A
api.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.11	A
api.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.12	A
api.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.30	A
api-int.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.10	A
api-int.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.11	A
api-int.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.12	A
api-int.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.30	A
*.apps.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.20	A
*.apps.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.21	A
*.apps.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.22	A
_etcd-server-ssl._tcp.sfo-w01-ocp01.sfo.rainpole.io	etcd-0.sfo-w01-ocp01.sfo.rainpole.io	SRV
_etcd-server-ssl._tcp.sfo-w01-ocp01.sfo.rainpole.io	etcd-1.sfo-w01-ocp01.sfo.rainpole.io	SRV
_etcd-server-ssl._tcp.sfo-w01-ocp01.sfo.rainpole.io	etcd-2.sfo-w01-ocp01.sfo.rainpole.io	SRV

VMware Software

- To facilitate the operation of the Red Hat OpenShift cluster with NSX-T Data Center, download the NSX Container Plugin 3.0.1 package.

- To provide observability for your OpenShift cluster, you must have an account for the Tanzu Observability by Wavefront service.

Red Hat OpenShift Software

Before you can start the deployment, you must obtain multiple Red Hat OpenShift components:

- Obtain your pull secret from the Red Hat OpenShift Cluster website.
- Download `openshift-install` Red Hat OpenShift 4.3 installation binaries.
- Download `oc` and `kubectl` Red Hat OpenShift 4.3 command-line interface binaries.
- Download the Red Hat CoreOS 4.3 virtual appliance OVA.

Create and Deploy a New SSH Key on Your Linux Host

To perform key-based login across nodes in the Red Hat OpenShift cluster, a new SSH key must be created and configured on the Linux jumphost

Procedure

1. Log in to your Linux host by using a Secure Shell (SSH) client.
2. Generate a new SSH key.

```
ssh-keygen -t rsa -b 4096 -n '' -f ~/.ssh/id_rsa_ocp43
```

3. Decrypt the encrypted SSH key.

```
openssl -in ~/.ssh/id_rsa_ocp43 -out id_rsa_ocp43
```

4. Modify the permissions so that you can read and write but can not execute the file.

```
chmod 600 ~/.ssh/id_rsa_ocp43
```

5. Start the `ssh-agent` program as a background task.

```
eval "$(ssh-agent -s)"
```

6. Add the new SSH private key to the `ssh-agent` program.

```
ssh-add ~/.ssh/id_rsa_ocp43
```

Extract the Red Hat OpenShift Installation and Command-Line Interface Tools

To facilicate the installation and operation of Red Hat OpenShift, you must download and configure installation and client binaries.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Extract the Red Hat OpenShift installation program and client.

```
tar –zxvf openshift–install–linux–4.3.xx.tar.gz
tar –zxvf openshift–client–linux–4.3.xx.tar.gz
```

3 Move the extracted programs to a location in your $PATH environment variable.

```
mv openshift–install oc kubectl /usr/local/bin
```

Create the Red Hat OpenShift Installation Configuration File

The Red Hat OpenShift `install–config.yaml` file provides configuration options to the installation program and facilitates the creation of its manifest files.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Create a working folder for the installation of Red Hat OpenShift.

```
mkdir ~/ocp
```

3 Go to the working folder for the installation of Red Hat OpenShift.

```
cd ~/ocp
```

4 Create an `install–config.yaml` installation file with the following contents.

```
apiVersion: v1
baseDomain: sfo.rainpole.io
compute:
– hyperthreading: Enabled
  name: worker
  replicas: 0
controlPlane:
  hyperthreading: Enabled
  name: control–plane
  replicas: 3
metadata:
  name: sfo–w01–ocp01
networking:
  networkType: NCP
  clusterNetwork:
  – cidr: 100.100.0.0/16
    hostPrefix: 23
  serviceNetwork:
  – 100.200.0.0/16
  machineCIDR: 192.168.23.0/24
platform:
```

```
  vsphere:
    vcenter: sfo-w01-vc01.sfo.rainpole.io
      username: administrator@vsphere.local
      password: <admin password>
      datacenter: sfo-w01-dc01
      defaultDatastore: sfo-w01-cl01-ds-vsan01
pullSecret: '<pull secret>'
sshKey: '<ssh public key>'
```

Extract and Configure the Configuration and Image Files for the NSX Container Plugin

The NSX Container Plugin allows Red Hat OpenShift nodes to attach to the NSX-T Manager and create segments, load balancers, and NAT rules, for use in the Red Hat OpenShift cluster.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Create a folder for the NSX Container Plugin configuration and image files.

```
mkdir ~/ncp-config
```

3 Extract the compressed contents of the *nsx-container-3.0.1.16118386.zip* package.

```
unzip your-filepath/nsx-container-3.0.1.16118386.zip
```

4 Copy the NSX Container Plugin image and configuration files to the newly created folder.

```
cp your-filepath/nsx-container-3.0.1.16118386/Kubernetes/nsx-ncp-rhel-3.0.1.16118386.tar ~/ncp-config
cp your-filepath/nsx-container-3.0.1.16118386/OpenShift/openshift4.tar.gz ~/ncp-config
```

5 Extract the compressed contents of the `openshift4.tar.gz` archive.

```
cd ~/ncp-config
tar -zxvf openshift4.tar.gz
cd openshift4
```

6 Edit the `cluster-network-17-nsx-ncp-config.yaml` file, enter the following changes, and save the file.

```
[coe]

adaptor = openshift4

cluster = sfo-w01-ocp01

[nsx_v3]

policy_nsxapi = True
```

```
nsx_api_user = admin

nsx_api_password = <NSX-T Admin password>

nsx_api_managers = 172.16.11.76, 172.16.11.77, 172.16.11.78

insecure = True

external_ip_pools = sfo-w01-ocp01-ip-pool-nat

tier0_gateway = sfo-w01-tier0-01

single_tier_topology = True

external_ip_pools_lb = sfo-w01-ocp01-ip-pool-lb

overlay_tz = <Resource ID of overlay-tz-sfo-w01-nsx01.sfo.rainpole.io>

edge_cluster = <Resource ID of sfo-w01-ec01 NSX-T Edge Cluster>

configure_t0_redistribution = True

[k8s]

apiserver_host_ip = api-int.sfo-w01-ocp01.sfo.rainpole.io

apiserver_host_port = 6443

baseline_policy_type = allow_cluster
```

7 Edit the `cluster-network-20-nsx-node-agent-config.yaml` file, enter the following changes, and save the file.

```
[k8s]

apiserver_host_ip = api.sfo-w01-ocp01.sfo.rainpole.io

apiserver_host_port = 6443

[coe]

adaptor = openshift4

cluster = sfo-w01-ocp01

[nsx-node-agent]

ovs_uplink_port = ens192
```

8 Configure the NSX Container Plugin image in the `cluster-network-19-nsx-ncp.yaml` file.

   a Edit the `cluster-network-19-nsx-ncp.yaml` file.

   b Replace all occurrences of `image: nsx-ncp` with `image: registry.local/3.0.1.16118386/nsx-ncp-rhel:latest`.

   c Save the file.

9 Repeat the previous step for the `cluster-network-21-nsx-ncp-bootstrap.yaml`, `cluster-network-22-nsx-node-agent.yaml` files.

Create the Red Hat OpenShift Manifest and Ignition Configuration Files

To create machines by using Ignition, you need Ignition config files. The OpenShift Container Platform installation program creates the Ignition config files that you need to deploy your cluster. These files are based on the information that you provide to the installation program directly or through an install-config.yaml file. OpenShift Container Platform uses the manifest files to create pods on the node.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Go to the working folder for the installation of the OpenShift Container Platform.

```
cd ~/ocp
```

3 Create the OpenShift Container Platform manifest files.

```
openshift-install create manifests
```

4 Edit the `manifests/cluster-scheduler-02-config.yaml`, change the `mastersSchedulable` value to **`false`**, and save the file.

5 Copy the NSX Container Plugin configuration files to the manifests folder.

```
cp ~/ncp-config/openshift4/cluster-network* manifests/
```

6 Create the Ignition configuration files.

```
openshift-install create ignition-configs
```

7 Create the `append-bootstrap.ign` file with the following contents and save.

```
{
  "ignition": {
    "config": {
      "append": [
        {
          "source": "http://<jumphost-ip-address>/bootstrap.ign",
```

```
          "verification": {}
        }
      ]
    },
    "timeouts": {},
    "version": "2.1.0"
  },
  "networkd": {},
  "passwd": {},
  "storage": {},
  "systemd": {}
}
```

8 Move the `bootstrap.ign` file to the `/var/www/html` folder.

```
mv bootstrap.ign /var/www/html/
```

9 Change permissions for the `bootstrap.ign` file to allow read and execute access.

```
chmod 755 /var/www/html/bootstrap.ign
```

10 Convert the `master.ign`, `worker.ign`, and `append–bootstrap.ign` files to the base64 format.

```
base64 –w0 append–bootstrap.ign > append–bootstrap.64
base64 –w0 master.ign > master.64
base64 –w0 worker.ign > worker.64
```

Configure DHCP on your NSX-T Data Center Instance

You must configure NSX-T Data Center to support Red Hat OpenShift nodes IP address assignment by using DHCP.

Create a DHCP Profile in NSX-T Manager

To allow virtual machines attached to an NSX-T Data Center overlay segment to use your DHCP server, you must configure a DHCP relay profile in NSX-T Manager.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 On the **Networking** tab, under **IP Management**, click **DHCP**.

4 Click the **Add DHCP Profile** button.

5 On the **Add DHCP Profile** window, configure the settings and click **Save**.

Setting	Value
Profile Name	dc01sfo.sfo.rainpole.io
Profile Type	DHCP Relay
Server IP Address	172.16.11.5

Configure NSX-T Tier-1 Gateway to Use DHCP Relay

Add the DHCP relay profile to the Tier-1 Gateway to use it on an overlay segment attached to that Tier-1 Gateway.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, click **Tier-1 Gateways**.

4 Click the vertical ellipses next to **sfo-w01-tier1-01** and click **Edit**.

5 Under **IP Address Management**, click the **No Dynamic IP Allocation** link.

6 In the **Set IP Address Management** dialog box, configure the settings and click **Save**.

Setting	Value
Type	DHCP Relay
DHCP Relay	dc01sfo.sfo.rainpole.io

7 Click **Close Editing**.

Configure IP Prefixes on the Tier-0 Gateway

Define IP Prefixes on the Tier-0 Gateway for use by the the Red Hat OpenShift cluster. You configure the IP Prefixes so their corresponding routes are advertised northbound through BGP.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, click **Tier-0 gateways**.

4 Select the **sfo-w01-ec01-t0-gw01.sfo.rainpole.io** gateway and, from the ellipsis menu, click **Edit**.

5 Create a new IP prefix list.

a Expand the **Routing** section and,next to **IP prefix** list, click **1**.

b In the**Set IP prefix list** dialog box, click **Add IP prefix list**.

c Enter `sfo-w01-cl01-prefix-list` as the prefix name and, under **Prefixes**, click **Set**.

d In the **Set prefixes** dialog box, click **Add Prefix**, configure the settings. and click **Add**.

Setting	Value
Network	192.168.23.0/24
ge	-
le	-
Action	Permit

e Click **Apply** and click **Save**.

6 Repeat the previous step twice to create two additional IP prefix sets `sfo-w01-cl01-lb` and `sfo-w01-cl01-nat` with the following sets.

Setting	Value	Value
Network	sfo-w01-cl01-lb	sfo-w01-cl01-nat
Network	192.168.24.0/24	192.168.25.0/24
ge	28	28
le	32	32
Action	Permit	Permit

7 In the **Set IP Prefix List** dialog box, click **Close**.

8 On the **Tier-0 gateway** page, click **Close Editing**.

Configure Route Maps on the Tier-0 Gateway

Configure and apply a route map on the Tier-0 Gateway. You apply this configuration to instruct the Tier-0 Gateway to advertise the newly defined routes.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, click **Tier-0 gateways**.

4 Select the **sfo-w01-ec01-t0-gw01.sfo.rainpole.io** gateway and, from the ellipsis menu, click **Edit**.

5 Create the `sfo-w01-cl01-route-map` route map.

   a Expand the **Routing** section and, in the **Route maps** section, click **Set**.

   b In the **Set route maps** dialog box, click **Add route map**.

   c Enter **`sfo-w01-cl01-route-map`** as the name.

   d In the **Match criteria** column, click **Set**.

   e In the **Set match criteria** dialog box, click **Add match criteria**.

   f In the **Members** column, click **Set**.

   g In the Select IP Prefix dialog box, select the check box next to `sfo-w01-cl01-prefix-list` and click **Save**.

   h In the **Action** column, select **Permit** and click **Add**.

i In the **Set match criteria** dialog box, add two additional match criteria with the following settings and click **Apply**.

Setting	Value for 2nd Match Criteria	Value for 3rd Match Criteria
Type	IP Prefix	IP Prefix
Members	sfo-w01-cl01-lb	sfo-w01-cl01-nat
Action	Permit	Permit

j In the **Set route maps** dialog box, click **Save** and click **Close**.

6 Configure route re-distribution.

a Expand the **Route re-distribution** section and, next to **Route re-distribution**, click **1**.

b In the **Set route re-distribution** dialog box, from the ellipsis drop-down menu for the default route re-distribution, click **Edit**.

c From the **Route map** drop-down menu, select **sfo-w01-cl01-route-map** and click **Add**.

d In the **Set route re-distribution** dialog box, click **Apply**.

7 On the **Tier-0 gateway** page, under **Route re-distribution**, click **Save** and click **Close editing**.

Deploy NSX-T Data Center Resources for Red Hat OpenShift

To deploy a Red Hat OpenShift Cluster by using software-defined networking, cluster nodes must be deployed to an overlay segment. IP pools must also be configured on the NSX-T Manager to provide resources for the NSX-T Container Plug-in to consume as it configures components for the Red Hat OpenShift cluster.

Add an Overlay Segment for Red Hat OpenShift Nodes

You must deploy an NSX-T overlay segment for use by the cluster nodes.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, click **Segments**.

4 Click the **Add Segment** button and configure the settings.

Setting	Value
Segment Name	sfo-w01-ocp01-mgmt
Connectivity	sfo-w01-tier1-01 | Tier1
Transport Zone	overlay-sfo-w01-nsx01.sfo.rainpole.io | Overlay
Subnets	192.168.23.1/24

5 Click the **Set DHCP Config** link.

6 Configure the settings and click **Apply**.

Setting	Value
DHCP Type	DHCP Relay
DHCP Profile	dc01sfo.sfo.rainpole.io

7 Click **Save** and click **No**.

Add IP Pools for Red Hat OpenShift

You must deploy two IP pools for use by the NSX-T Container Plug-in during Red Hat OpenShift cluster deployment.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, click **IP Pools**.

4 On the **IP Address Pools** page, click the **Add IP Address Pool** button to configure a new pool.

   a Enter **`sfo-w01-ocp01-ip-pool-nat`** as the name and, under **Subnets**, click **Set**.

   b In the **Set Subnets** dialog box, click the **Add Subnet** drop-down menu and select **IP Block**.

c Configure the settings and click **Add**.

Setting	Value
IP Range	192.168.24.1-192.168.24.254
CIDR	192.168.24.0/24

d Click **Apply** and click **Save**.

5 Repeat the previous step to configure another IP Pool.

Setting	Value
Name	sfo-w01-ocp01-ip-pool-lb
IP Range	192.168.25.1-192.168.25.254
CIDR	192.168.25.0/24

Upload the Red Hat CoreOS Virtual Appliance to vCenter Server as a Template

To deploy Red Hat OpenShift cluster nodes, you must deploy and configure the Red Hat CoreOS 4.3 virtual appliance to the virtual infrastructure workload domain. You also convert the appliance to a template.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Create a new VM and template folder for the Red Hat OpenShift components.

a From the **VMs and Templates** inventory , right-click the **sfo-w01-dc01** data center and select **New Folder > New VM and Template Folder**.

b In the **New Folder** dialog box, enter `sfo-w01-ocp01` and click **OK**.

3 Deploy the Red Hat CoreOS 4.3 virtual appliance to your workload domain.

a Right click the **sfo-w01-ocp01** folder and click **Deploy OVF Template** to open the **Deploy OVF Template** wizard.

b On the **Select an OVF template** page, select **Local file**, click **Upload Files**, select the Red Hat CoreOS 4.3 OVA, and click **Next**.

c On the **Select a name and folder** page, enter **rhcos–43** as virtual machine name, make sure the **sfo-w01-ocp01** folder is selected, and click **Next**.

d On the **Select a compute resource** page, select the **sfo-w01-cl01** vSphere Cluster and click **Next**.

e On the **Review details** page, click **Next**.

f On the **Select storage** page, select the **sfo-w01-cl01-ds-vsan01** vSAN datastore and click **Next**.

g On the **Select networks** page, select **sfo-w01-ocp01-mgmt** as the VM network and click **Next**.

h On the **Customize template** page, click **Next** and finish the deployment.

4 Edit the settings of the virtual machine.

a Right-click the **rhcos-43** virtual machine and click **Edit Settings**.

b In the **Edit Settings** dialog box, click the **Virtual Hardware** tab and configure the settings.

Setting	Value
CPU	4
Memory	16 GB
Hard disk 1	120 GB

c Click the **VM Options** tab, expand the **Advanced** menu, and click **Edit configuration**.

d In the **Configuration parameters** dialog box, click **Add configuration params**.

e Enter `disk.EnableUUID` as the name, enter `1` as the value, and click **OK**.

f Click **OK** to close the **Edit Settings** dialog box.

5 Right-click the **rhcos-43** virtual machine, select **Template > Convert to Template** and confirm the action.

Deploy the OpenShift Cluster Nodes

You deploy 3 control plane nodes and 3 worker nodes for the Red Hat OpenShift cluster. On vSphere user-provisioned infrastructure (UPI), you deploy the nodes as virtual machines from the previously uploaded and configured Red Hat CoreOS template. You first deploy a bootstrap node that is required to deploy the control plane and worker nodes. You delete the bootstrap node post-deployment.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Create a new resource pool.

a From the **Hosts and Clusters** inventory, right-click the **sfo-w01-cl01** cluster and click **New Resource Pool**.

b On the **New Resource Pool** dialog box, configure the following and then click **OK**.

Setting	Value
Name	sfo-w01-ocp01
CPU > Shares	Normal
Memory > Shares	Normal

3 Deploy the bootstrap node.

a From the **VMs and Templates** inventory, right-click the **rhcos-43** template and click **New VM from This Template**.

b On the **Select a name and folder** page, enter **`bootstrap`** as virtual machine name, select **sfo-w01-ocp01** as inventory, and click **Next**.

c On the **Select a compute resource** page, select **sfo-w01-ocp01** as the destination compute resource and click **Next**.

d On the **Select storage** page, select the **sfo-w01-cl01-ds-vsan01** vSAN datastore and click **Next**.

e On the **Select clone options** page, click **Next**.

f On the **Customize vApp properties** page, expand **Uncategorized**, and enter the property.

Setting	Value
Ignition config data encoding	base64
Ignition config data	<value_of_append-bootstrap.64>

g Click **Next** and finish the deployment.

4 Repeat the previous step three times to deploy the three control plane nodes.

Use the value of the `master.64` file for the `Ignition config data` property.

Setting	Value for node 1	Value for node 2	Value for node 3
Virtual machine name	control-plane-0	control-plane-1	control-plane-2
Ignition config data	*value_of_master.64_file*	*value_of_master.64_file*	*value_of_master.64_file*

5 Deploy the first worker node.

a From the **VMs and Templates** inventory, right-click the **rhcos-43** template and click **New VM from This Template**.

b On the **Select a name and folder** page, enter **`worker–0`** as virtual machine name, select **sfo-w01-ocp01** as inventory, and click **Next**.

c On the **Select a compute resource** page, select **sfo-w01-ocp01** as the destination compute resource and click **Next**.

d On the **Select storage** page, select the **sfo-w01-cl01-ds-vsan01** vSAN datastore and click **Next**.

e On the **Select clone options** page, select the **Customize this virtual machine's hardware** check box and click **Next**.

f On the **Customize hardware** page, enter the settings and click **Next**.

Setting	Value
CPU	2
Memory	8 GB

g On the **Customize vApp properties** page, expand **Uncategorized**, and enter the property.

Setting	Value
Ignition config data encoding	base64
Ignition config data	*value_of_worker.64_file*

h Click **Next** and finish the deployment.

6 Repeat the previous step twice to deploy the remaining `worker–1` and `worker–2` worker nodes.

Use `worker–1` and `worker–2` respectively as virtual machine name during the deployments of the two nodes.

Update Your DHCP Reservations with the MAC Addresses of the Nodes

After you have deployed all nodes, you gather the actual values of the MAC addresses of your node and update the previously created DHCP reservations on your Domain Controller. After a reservation is updated, you can power on the respective node.

Procedure

1 In a Web browser, log in to the Workload domain vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-w01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **VMs and Templates** inventory, right-click the **bootstrap** virtual machine and click **Edit Settings**.

3 In the **Edit Settings** dialog box, expand **Network adapter 1**.

4 Copy the value of the MAC Address, save it in a text editor, and click **OK**.

5 Go to your Domain Controller and update your DHCP reservation for the `bootstrap` node with the actual MAC address value.

6 After the DHCP reservation is updated, go back to the vSphere Client.

7 From the **VMs and Templates** inventory, right-click the **bootstrap** virtual machine and select **PowerPower On**.

8 Perform the procedure six times for the three control plane and three worker nodes.

Deploy the NSX Container Plugin to Red Hat OpenShift Nodes

The NSX Container Plugin image is not public, so you must upload it and load it to the local registry of each control plane and worker nodes.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Copy the NSX Container Plugin image to the fist control plane node.

```
scp -i path_to_private_key ~/ncp-config/nsx-ncp-rhel-3.0.1.16118386.tar core@192.168.23.10:/tmp/
nsx-ncp-rhel-3.0.1.16118386.tar
```

3 Load the NSX Container Plugin image to the local image registry of the fist control plane node.

```
ssh –i path_to_private_key core@192.168.32.10 'sudo podman load < /tmp/nsx–ncp–
rhel–3.0.1.16118386.tar'
```

4 Repeat the procedure five times for the two remaining control plane nodes and the three worker nodes.

Configure the NSX-T Overlay Segment for the NSX Container Plugin

You must tag the logical switch ports for each control node and each worker node in the Red Hat OpenShift cluster so that they can be identified by the NSX Container Plugin.

Procedure

1 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 On the main navigation bar, click **Networking**.

3 In the navigation pane, click **Segments**.

4 Select the **sfo-w01-ocp01-mgmt** segment and, from the ellipsis menu, click **Edit**.

5 In the **Ports** column, click the number link to configure the ports.

6 Add two tag and scope pairs on the respective port for the `worker-0` node.

a Select the port that contains `worker-0` in the name and, from the ellipsis menu, click **Edit**.

b Add the following tag and scope pair and click the plus button.

Setting	Value
Tag	worker-0
Scope	ncp/worker-0

c Add another tag and scope pair, click the plus button, and click **Save** in the port edit area.

Setting	Value
Tag	sfo-w01-ocp01
Scope	ncp/cluster

7 Repeat the previous step for the remaining control plane and worker node ports.

Use the respective node name for the Tag in the first pair. The second pair to be configured is the same for all ports.

Setting	Values for port that contains worker-1	Values for port that contains worker-2	Values for port that contains control-0	Values for port that contains control-1	Values for port that contains control-2
Tag	worker-1	worker-2	control-0	control-1	control-2
Scope	ncp/worker-1	ncp/worker-2	ncp/control-0	ncp/control-1	ncp/control-2

Complete Red Hat OpenShift Bootstrap and Installation

After the Red Hat OpenShift nodes have been deployed and configured to work with the NSX Container Plugin, the bootstrap and installation process can continue.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Run openshift-install to monitor the bootstrap process completion.

```
openshift-install wait-for bootstrap-complete --dir=home_directory/ocp
```

After the process completes, you see similar output in your console.

```
[user@jumphost ~]# openshift-install wait-for bootstrap-complete --dir=home_directory/ocp
INFO Waiting up to 30m0s for the Kubernetes API at https://api.sfo-w01-
ocp01.sfo.rainpole.io:6443...
INFO API v1.16.2 up
INFO Waiting up to 30m0s for bootstrapping to complete...
INFO It is now safe to remove the bootstrap resources
```

3 In a Web browser, log in to the NSX-T Local Manager for the VI workload domain by using the user interface.

Setting	Value
URL	https://sfo-w01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

4 From **Hosts and Clusters** inventory, right-click the **bootstrap** virtual machine and click **PowerPower Off**.

5 Right-click the **bootstrap** virtual machine and click **Delete from Disk**.

6 Remove the bootstrap related DNS records from your DNS.

Hostname	IP Address	Record Type
bootstrap.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.30	A
api.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.30	A
api-int.sfo-w01-ocp01.sfo.rainpole.io	192.168.23.30	A

7 Go back to your Secure Shell (SSH) client and run `openshift-install` to monitor the installation process completion.

```
openshift-install wait-for install-complete --dir=home_directory/ocp
```

After the process completes, you see similar output in your console.

```
[user@jumphost ~]# openshift-install wait-for install-complete --dir=home_directory/ocp
INFO Waiting up to 30m0s for the cluster at https://api.sfo-w01-ocp01.sfo.rainpole.io:6443 to
initialize...
INFO Waiting up to 10m0s for the openshift-console route to be created...
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=home_directory/ocp/auth/kubeconfig'
INFO Access the OpenShift web-console here: https://console-openshift-console.apps.sfo-w01-
ocp01.sfo.rainpole.io
INFO Login to the console with user: kubeadmin, password: dagIs-sIzXJ-TTaIE-hytfg
```

8 Configure your `kubeconfig` to enable access to the Red Hat OpenShift cluster.

```
export KUBECONFIG=home_directory/ocp/auth/kubeconfig
```

9 Accept and sign node certificate signing requests that queued up after the installation.

```
oc get csr –o name | xargs oc adm certificate approve
```

Configure Active Directory LDAP Authentication for the Red Hat OpenShift Cluster

By configuring LDAP authentication and role-based access control for your Red Hat OpenShift cluster, you limit the access to critical resources, separate duties, and allow for auditability through named access.

Configure an LDAP Custom Resource for the Red Hat OpenShift Cluster

The LDAP custom resource allow for the cluster OAuth instance to leverage your Active Directory LDAP as authentication mechanism.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Create the LDAP secret for use in the LDAP custom resource.

```
oc create secret generic ldap-secret ––from-
literal=bindPassword=rainpole\svc_domain_join_password –n openshift-config
```

3 Create a `configmap` for the LDAP server certificate.

```
oc create configmap ca-config-map ––from-file=ca.crt=path_to_dc01rpl.rainpole.io certificate/
rainpole-root-ca.crt –n openshift-config
```

4 Create an `ldap_cr.yaml` LDAP custom resource configuration file with the following configurations and save the file.

```
apiVersion:config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
  - name: ldapidp
    mappingMethod: claim
    type: LDAP
    ldap:
      attributes:
        id:
```

```
          - name
        email:
          - UserPrincipalName
        name:
          - cn
        preferredUsername:
          - sAMAccountName
      bindDN: "CN=svc-domain-join,OU=Security Users,DC=rainpole,DC=io"
      bindPassword:
        name: ldap-secret
      ca:
        name: ca-config-map
      insecure: false
      url: "ldaps://dc01rpl.rainpole.io/OU=Security Users,DC=rainpole,DC=io?sAMAccountName??
(objectClass=person)"
```

5 Apply the LDAP custom resource configuration.

```
oc apply -f ldap_cr.yaml
```

Configure LDAP Group Sync for the Red Hat OpenShift Cluster

Performing LDAP group sync is necessary for you to assign cluster roles to users by using groups and not assign permissions per user.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Create an `ad_sync.yaml` Active Directory-based LDAP sync configuration file with the following configuration and save the file.

```
kind: LDAPSyncConfig
apiVersion: v1
url: ldaps://dc01rpl.rainpole.io
insecure: false
ca: <path>/rainpole-root-ca.crt
bindDN: CN=svc-domain-join,OU=Security Users,DC=rainpole,DC=io
bindPassword: <rainpole/svc-domain-join password>
groupUIDNameMapping:
  "CN=ug-kub-admins,OU=Security Groups,DC=rainpole,DC=io": rainpoleadmins
  "CN=ug-kub-readonly,OU=Security Groups,DC=rainpole,DC=io": rainpolereadonly
activeDirectory:
  usersQuery:
    baseDN: "OU=Security Users,DC=rainpole,DC=io"
    scope: sub
    derefAliases: never
    filter: (objectclass=person)
    pageSize: 0
  userNameAttributes: [ sAMAccountName ]
  groupMembershipAttributes: [ memberOf ]
```

3 Sync the `ug-kub-admins` and `ug-kub-readonly` groups.

```
oc adm groups sync --sync-config=ad_sync.yaml "CN=ug-kub-admins,OU=Security
Groups,DC=rainpole,DC=io" "CN=ug-kub-readonly,OU=Security Groups,DC=rainpole,DC=io" --confirm
```

4 Apply the respective cluster roles to each group.

```
oc adm policy add-cluster-role-to-group view rainpolereadonly
oc adm policy add-cluster-role-to-group cluster-admin rainpoleadmins
```

5 Login as a user from the `ug-kub-admins` group to verify the configuration.

```
oc login -u user_from_the_ug-kub-admins_group
```

Configure the Red Hat OpenShift Cluster Internal Registry

The internal registry for the Red Hat OpenShift cluster is disabled during installation as the default storage provider for vSphere does not support read-write-many access mode. You must configure the internal registry by using external NFS storage or you can implement another image registry solution.

Procedure

1 Log in to your Linux host by using a Secure Shell (SSH) client.

2 Log in to the Red Hat OpenShift cluster as a cluster-admin user.

```
oc oc login -u user_from_the_ug-kub-admins_group
```

3 Create an `nfs_storage_class.yaml` NFS storage class configuration file with the following configuration and save the file.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: nfs01
provisioner: kubernetes.io/no-provisioner
parameters:
  type: nfs
reclaimPolicy: Retain
allowVolumeExpansion: true
mountOptions:
  - debug
volumeBindingMode: Immediate
```

4 Apply the new storage class configuration.

```
oc apply -f nfs_storage_class.yaml
```

5 Create an `nfs_int-reg_pv.yaml` internal registry persistent volume configuration file with the following configuration and save the file.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: image-registry-pv
spec:
  capacity:
    storage: 100Gi
  accessModes:
  - ReadWriteMany
  nfs:
    path: <ocp-image-registry-nfs-export>
    server: <nfs server>
  persistentVolumeReclaimPolicy: Retain
  storageClassName: nfs01
```

6 Apply the new persistent volume configuration.

```
oc apply -f nfs_int-reg_pv.yaml
```

7 Create an `nfs_int-reg_pvc.yaml` internal registry persistent volume claim configuration file with the following configuration and save the file.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: image-registry-pvc
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 100Gi
  storageClassName: nfs01
```

8 Apply the new persistent volume claim configuration.

```
oc apply -f nfs_int-reg_pvc.yaml -n openshift-image-registry
```

9 Edit the internal registry operator configuration.

```
oc edit configs.imageregistry.operator.openshift.io -o yaml
```

10 Change the following configurations, save, and exit the editor.

```
spec:
  managementState: Managed
```

```
  defaultRoute: true
  storage:
    pvc:
      claim: image-registry-pvc
```

11 Log in to the internal registry by using podman on your Linux host to validate the configuration.

```
HOST=$(oc get route default-route -n openshift-image-registry --template='{{ .spec.host }}')
podman login -u $(oc whoami) -p $(oc whoami -t) --tls-verify=false $HOST
```

12 Push an image to the internal registry to verify that the operation completes successfully.

```
podman pull nginx:latest
podman tag nginx:latest $HOST/<namespace>/nginx:latest
podman push $HOST/<namespace>/nginx:latest
```

Install and Configure the Tanzu Observability by Wavefront Operator

Tanzu Observability by Wavefront is a SaaS-based platform for enterprise-grade observability and analytics. You must configure the Wavefront Operator and its components to enable metric collection and ingestion for your OpenShift cluster.

Install the Wavefront Operator

To begin the Tanzu Observability by Wavefront installation process, you must install the Wavefront Operator from OperatorHub.

Procedure

1 In a Web browser, log in to the Red Hat OpenShift Console web interface.

Setting	Value
URL	https://console-openshift-console.apps.sfo-w01-ocp01.rainpole.io
User name	kubeadmin
Password	*kubeadmin_user_password*

2 In the navigation pane, click **Projects**.

3 On the **Projects** page, click **Create Project**.

4 In the **Create Project** dialog box, enter **`wavefront`** as the name and click **Create**.

5 In the navigation pane, under **Operators**, click **OperatorHub**.

6 On the **OperatorHub** page, search for **`Wavefront`** and click the **Wavefront Operator** tile.

7 In the **Wavefront Operator** tile, click **Install**.

8 On the **Create Operator Subscription** page, select the **A specific namespace in the cluster** radio button, select the **wavefront** namespace, and click **Subscribe** .

Retrieve the Wavefront API Key

To allow your local Wavefront proxy to push metrics to your Wavefront SaaS cluster, you must first retrieve your API key and configure it later.

Procedure

1 In a Web browser, log in to your Wavefront instance.

2 Click the gear icon on the task bar and select your username.

3 Click the **API Access** tab and click the **Generate** button.

4 Copy the token value and save it to use it later.

Configure the Wavefront Operator

You must configure the Wavefront operator and its components to complete the Tanzu Observability by Wavefront deployment.

Procedure

1 In a Web browser, log in to the Red Hat OpenShift Console web interface.

Setting	Value
URL	https://console-openshift-console.apps.sfo-w01-ocp01.rainpole.io
User name	kubeadmin
Password	*kubeadmin_user_password*

2 In the navigation pane, under **Operators**, click **Installed Operators**.

3 From the **Project** drop-down menu, select **wavefront**.

4 Click the **Wavefront Operator** link and click the **YAML** tab.

5 On the **YAML** tab, edit the YAML file with values for your environment.

   a For `token` value, enter the previously generated token that you saved earlier.

   b For `url` value, enter **`https://<your_wavefront_cluster>.wavefront.com/api`**.

   c Click **Save**.

6 Click the **Wavefront Proxy** tab and click **Create WavefrontProxy**.

7 On the **Create WavefrontProxy** page, click **Create**.

8 Click the **Wavefront Collectors** tab and click **Create WavefrontCollector**.

9 On the **Create WavefrontCollector** page, click **Create**.

Results

The metric collection and ingestion for your OpenShift cluster is fully configured.