**Deployment Document**

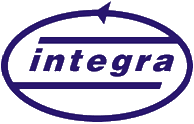
**Project**

**OCP 4.15 DR Cluster Deployment**

**v1.1**

**Client: Bank-ABC**

****



**Integra Micro Systems Pvt. Ltd.**

No. 4, 1st Floor, Bellary Road,

12th KM, Jakkur,

Bangalore 560 064, INDIA

Tel: 080-46632400

[**www.integramicro.com**](http://www.integramicro.com/)

**Disclaimer**

Copyright © 2013:  Integra Micro Systems Private Limited, Registered Office #4, Bellary Rd, 12, KM, Yashoda Nagar, Jakkur, Bangalore, Karnataka India.

All rights about this document are reserved and  shall not be , in whole or in part, copied, photocopied, reproduced, translated, or reduced to any manner including but not limited to electronic, mechanical, machine readable ,photographic, optic recording or otherwise without prior consent, in writing, of Integra Micro Systems Private Limited (the Company).

The information in this document is subject to changes without notice. This describes only the product defined in the introduction of this documentation. This document is intended for the use of prospective customers of the Company Products Solutions and or Services for the sole purpose of the transaction for which the document is submitted. No part of it may be reproduced or transmitted in any form or manner whatsoever without the prior written permission of the company. The Customer, who/which assumes full responsibility for using the document appropriately. The Company welcomes customer comments as part of the process of continuous development and improvement.

The Company, has made all reasonable efforts to ensure that the information contained in the document are adequate, sufficient and free of material errors and omissions. The Company will, if necessary, explain issues, which may not be covered by the document. However, the Company does not assume any liability of whatsoever nature, for any errors in the document except the responsibility to provide correct information when any such error is brought to company’s knowledge. The Company will not be responsible, in any event, for errors in this document or for any damages, incidental or consequential, including monetary losses that might arise from the use of this document or of the information contained in it.

This document and the Products, Solutions and Services it describes are intellectual property of the Company and/or of the respective owners thereof, whether such IPR is registered, pending for registration, applied for registration or not.

The only warranties for the Company Products, Solutions and Services are set forth in the express warranty statements accompanying its products and services. Nothing here in should be construed as constituting an additional warranty. The Company shall not be liable for technical or editorial errors or omissions contained herein.

The Company logo is a trademark of the Company. Other products, names, logos mentioned in this document, if any, may be trademarks of their respective owners.

Copyright © 2013:  Integra Micro Systems Private Limited. All rights reserved.

**Release History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Release Version | 1. Release Date | 1. Description of the release | 1. Created By | 1. Approved By |
| 0.1 | 1. 05-02-2025 | 1. First Draft | 1. Sai Akhil/Kiran | 1. Murali.K.Muddada |
| 0.2 | 08-02-2025 | Updated ELK details | 1. Sai Akhil/Kiran | 1. Murali.K.Muddada |
| 0.3 | 10-02-2025 | Updated prometheous and Graphana details | 1. Sai Akhil/Kiran | 1. Murali.K.Muddada |
| 0.4 | 12-02-202 | Added SMTP details | 1. Sai Akhil/Kiran | 1. Murali.K.Muddada |

1. **Confidentiality Statement**

Copyright © 2011-2012, Integra Micro Systems Private Limited. All rights reserved. This product or document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form, by any means electronic, mechanical, photographic, optic recording or otherwise without prior consent, in writing, of the copyright owner. Statutory declaration under section 52A of the Copyright Act 1957.

**Table of Contents**

[1 About the Guide 6](#__RefHeading___Toc7141_399447981)

[1.1 Target Audience 6](#__RefHeading___Toc7143_399447981)

[1.2 Acronyms and Abbreviations 6](#__RefHeading___Toc7145_399447981)

[2 Introduction 8](#__RefHeading___Toc7147_399447981)

[2.1 Topics Covered 8](#__RefHeading___Toc7149_399447981)

[2.2 Scope 8](#__RefHeading___Toc7151_399447981)

[2.3 Out of Scope 8](#__RefHeading___Toc7153_399447981)

[3 Implementation Details 9](#__RefHeading___Toc7155_399447981)

[3.1 Environment Setup 9](#__RefHeading___Toc7157_399447981)

[3.1.1 Network Information 9](#__RefHeading___Toc7159_399447981)

[3.1.2 Network Services 9](#__RefHeading___Toc7161_399447981)

[3.1.3 Node Information 9](#__RefHeading___Toc7163_399447981)

[3.1.4 Storage Information 9](#__RefHeading___Toc7165_399447981)

[3.1.5 Certificates 9](#__RefHeading___Toc7167_399447981)

[4 Technical Implementation 10](#__RefHeading___Toc7169_399447981)

[4.1 Check Bastion Node for all the pre-Installation requirements 10](#__RefHeading___Toc7171_399447981)

[4.1.1 Operating System Details 10](#__RefHeading___Toc7173_399447981)

[4.1.2 Block Device (Hard Disk) Details 10](#__RefHeading___Toc7175_399447981)

[4.1.3 Network Configuration 10](#__RefHeading___Toc7177_399447981)

[4.1.4 Route and Default Gateway details 10](#__RefHeading___Toc7179_399447981)

[4.1.5 Enabling Repositories 10](#__RefHeading___Toc7181_399447981)

[4.2 Installing a Connected Cluster 11](#__RefHeading___Toc7183_399447981)

[4.2.1 Configure Environmental Services in Bastion. 11](#__RefHeading___Toc7185_399447981)

[4.2.2 Generating an SSH private key and adding it to the agent 13](#__RefHeading___Toc7187_399447981)

[4.2.3 Create install-config.yaml file 13](#__RefHeading___Toc7189_399447981)

[4.2.4 Creating the Openshift/Kubernetes manifest 15](#__RefHeading___Toc7191_399447981)

[4.2.5 Create the Ignition config files 15](#__RefHeading___Toc7193_399447981)

[4.3 Deploying Openshift 16](#__RefHeading___Toc7195_399447981)

[4.3.1 Monitoring the Bootstrap Process 16](#__RefHeading___Toc7197_399447981)

[4.3.2 Remove the Bootstrap Node 16](#__RefHeading___Toc7199_399447981)

[4.3.3 Join Nodes 16](#__RefHeading___Toc7201_399447981)

[4.4 Accessing the Cluster 17](#__RefHeading___Toc7203_399447981)

[4.4.1 Accessing the Openshift Console 17](#__RefHeading___Toc7205_399447981)

[4.4.2 Accessing the Cluster Nodes. 17](#__RefHeading___Toc7207_399447981)

[4.5 Deploying Openshift Internal Registry with Persistent Storage 19](#__RefHeading___Toc7209_399447981)

[4.6 Configure System Clock Sync with NTP Server 19](#__RefHeading___Toc7211_399447981)

[4.6.1 Configure master nodes system clock sync with NTP server 20](#__RefHeading___Toc7213_399447981)

[4.7 Configuring an HTPasswd identity provider 21](#__RefHeading___Toc7215_399447981)

[4.8 Registering the Cluster 22](#__RefHeading___Toc7217_399447981)

[4.9 Encrypting the ETCD data 24](#__RefHeading___Toc7219_399447981)

[4.10 Backing Up ETCD data 24](#__RefHeading___Toc7221_399447981)

[4.11 Deploying and Configuring Openshift Logging 25](#__RefHeading___Toc7223_399447981)

[4.11.1 Install Cluster Logging Operators 25](#__RefHeading___Toc7225_399447981)

[4.11.2 Create Cluster Logging Instance 26](#__RefHeading___Toc7227_399447981)

[4.11.3 Viewing cluster logs from the Kibana dashboard 28](#__RefHeading___Toc7229_399447981)

[4.12 Applying a custom Alertmanager configuration with the SMTP details 29](#__RefHeading___Toc7231_399447981)

[4.13 Removing the kubeadmin user 30](#__RefHeading___Toc7233_399447981)

[4.14 Moving monitoring components from Worker to Infra labeled nodes 31](#__RefHeading___Toc7235_399447981)

[4.15 Configuring the default scheduler to control pod placement 33](#__RefHeading___Toc7237_399447981)

[4.16 Etcd backup Cronjob 33](#__RefHeading___Toc7398_399447981)

# About the Guide

This design document currently includes a Prod environment which will be hosted on Virtual Machines.

## Target Audience

This document is intended for Client technical staff responsible for the environment.

## Acronyms and Abbreviations

The table below provides a glossary of the terms and acronyms used within this document.

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| RH | Red Hat, Inc |
| OKE | Openshift Kubernetes Engine |
| OCP | Openshift Container Platform |
| AD | Active Directory |
| API | Application Programming Interface |
| AZ | Availability Zone |
| CA | Certificate Authority |
| CR | Custom Resource |
| DC | Data Centre |
| DNS | Domain Name System |
| DHCP | Dynamic Host Configuration Protocol |
| DVR | Distributed Virtual Routers, a networking configuration for routing using Compute and Network nodes for separate networking functions |
| FQDN | Fully Qualified Domain Name |
| Guest | Also see “VM”. This is virtual machine running on a Host. |
| HA | High-Availability or Highly-Available |
| Host | The physical hardware or the logical OS which runs virtualisation technology allowing one or more Guest OS’s to run on the hardware owned by the Host |
| KVM | Kernel-based Virtual Machine |
| L2 | Layer 2, part of the TCP/IP Network Stack |
| L3 | Layer 3, part of the TCP/IP Network Stack |
| LBaaS | Load Balancing as a Service |
| NAT | Network Address Translation |
| NIC | Network Interface Card. References a virtual or a physical port allowing network access and interface to a Host or Guest VM. |
| NTP | Network Time Protocol |
| OCP | OpenShift Container Platform |
| OS | Operating System |
| OVS | Open vSwitch, a Linux-based virtual switch appliance used in OpenStack |
| PXE | Preboot Execution Environment |
| QA | Quality Assurance |
| SAML/SAML2 | A protocol allowing authentication and federation of multiple domains |
| SAN | Storage Area Network |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| VIP | Virtual IP address |
| VLAN | Virtual LAN is a networking virtualisation technology |
| VM | Virtual machine, in OSP terms, synonymous with “Workload” or “Guest” |
| VXLAN | Virtual Extensible LAN (VXLAN) is a network virtualisation technology |
| Workload | Synonym for “Guest” or “VM” |
| K8s | Kubernetes |
| RHCOS | Red Hat CoreOS |
| DIY | Do It Yourself |
| VM | Virtual Machine |
| OCR | OpenShift Container Registry (Integrated Registry) |

# Introduction

## Topics Covered

Openshift topology - Discussion about OCP high level architecture, subsystems as well as high-level overview of process, technology and operations.

Design guidelines and architecture - Interactive discussion covering minimal HA architectures for development environment and constraints.

## Scope

The scope of this document is to describe the architecture that Red Hat can offer for Openshift. This document is the result of the design workshop and should cover all requirements that TCS put forward during the workshop. As a part of this project engagement with TCS, Red Hat team will:

● Design and validate Openshift Kubernetes Engine (OKE) 4.16 in prod Datacenters.

## Out of Scope

This document limits the discussions and recommendations only to Red Hat Components involved for TCS.

# Implementation Details

## Environment Setup

Steps to prepare or create the environment for the proposed architecture

### Network Information

*Table 1. Network Data*

|  |  |  |
| --- | --- | --- |
| **Name** | **IP Address Pool** | **Comments** |
| Cluster Network | 10.128.0.0/14 | Non Routable |
| Service Network | 172.30.0.0/16 | Non Routable |

### Network Services

*Table 2. Network Service Data*

|  |  |  |
| --- | --- | --- |
| **Services** | **Host** | **Comments** |
| DNS Server | 10.101.141.119 |  |
| DNS Server | 10.101.141.118 |  |

### Node Information

*Table 3. Nodes Data*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server FQDN** | **IP** | **Role** | **Subs Used** | **OS** |
| vlocpsrvm1.valpocp.vedantaconnect.com | 10.101.143.14 | Master/Control-Plane | N/A | RHCOS |
| vlocpsrvm2.valpocp.vedantaconnect.com | 10.101.143.15 | Master/Control-Plane | N/A | RHCOS |
| vlocpsrvm3.valpocp.vedantaconnect.com | 10.101.143.16 | Master/Control-Plane | N/A | RHCOS |
| vlocpsrvw1.valpocp.vedantaconnect.com | 10.101.143.17 | Worker | N/A | RHCOS |
| vlocpsrvw2.valpocp.vedantaconnect.com | 10.101.143.18 | Worker | N/A | RHCOS |
| vlocpsrvw3.valpocp.vedantaconnect.com | 10.101.143.19 | Worker | N/A | RHCOS |

### Storage Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Application** | **Storage Type** | **CSI Driver** | **Storage Class** | **Size** |
| Registry | File | Trident CSI | ontap-nas-sc | 500GB |
| ELK Application Deployment | block | Trident CSI | ontap-san-sc-ext4 | 3\*900GB |
| Prometheus and Grafana | block | Trident CSI | ontap-san-sc,  ontap-san-sc-ext4 | 2\*200GB, 2\*7.5GB |

*Table 4. Storage Data*

### Certificates

TCS has planned to use self-signed certificates that come with the cluster for the Wild Card (\*.apps) Domain Ingress Controller.

# Technical Implementation

## Check Bastion Node for all the pre-Installation requirements

### Operating System Details

• Bastion Node

|  |
| --- |
| [prod@bastion ~]$ cat /etc/redhat-release  Red Hat Enterprise Linux release 9.4 (Plow) |

### Block Device (Hard Disk) Details

• Bastion Node

|  |
| --- |
| [prod@bastion ~]$ df -hT  Filesystem Type Size Used Avail Use% Mounted on  devtmpfs devtmpfs 4.0M 0 4.0M 0% /dev  tmpfs tmpfs 1.8G 0 1.8G 0% /dev/shm  tmpfs tmpfs 732M 8.7M 723M 2% /run  /dev/mapper/rhel-root xfs 145G 6.2G 139G 5% /  /dev/sda1 xfs 960M 266M 695M 28% /boot  tmpfs tmpfs 366M 4.0K 366M 1% /run/user/0 |

### Network Configuration

* Bastion Node

|  |
| --- |
| [prod@bastion ~]$ cat /etc/resolv.conf  # Generated by NetworkManager  search valpocp.vedantaconnect.com  nameserver 101.101.141.119  nameserver 10.101.141.118 |

### Route and Default Gateway details

* Bastion Node

|  |
| --- |
| [prod@bastion ~]$ route -n  Kernel IP routing table  Destination Gateway Genmask Flags Metric Ref Use Iface  0.0.0.0 10.101.143.1 0.0.0.0 UG 100 0 0 eth0  10.101.143.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0 |

## Installing a Connected Cluster

### Configure Environmental Services in Bastion.

1. Install & configure Apache Web Server

|  |
| --- |
| dnf install httpd -y |

1. Change default listen port to 8080 in httpd.conf

|  |
| --- |
| sed -i 's/Listen 80/Listen 0.0.0.0:8080/' /etc/httpd/conf/httpd.conf |

1. Enable and start the service

|  |
| --- |
| systemctl enable httpd systemctl start httpd systemctl status httpd |

1. Making a GET request to localhost on port 8080 should now return the default Apache webpage

|  |
| --- |
| curl localhost:8080 |

### Generating an SSH private key and adding it to the agent

* Generate SSH Key
* Start the ssh-agent process as a background task

|  |
| --- |
| [prod@bastion ~]$ ssh-keygen -t ed25519 -f ~/.ssh/id\_rsa  [prod@bastion ~]$ eval "$(ssh-agent -s)" |

* Add your SSH private key to the ssh-agent

|  |
| --- |
| [prod@bastion ~]$ ssh-add /home/core/.ssh/id\_rsa  Identity added: /home/core/.ssh/id\_rsa **(**/home/core/.ssh/id\_rsa**)** |

### Create install-config.yaml file

|  |
| --- |
| [prod@bastion ~]$ cat /etc/resolv.conf  # Generated by NetworkManager  search valpocp.vedantaconnect.com  nameserver 101.101.141.119  nameserver 10.101.141.118  [prod@bastion ~]$ cat install-config.yaml  apiVersion: v1  baseDomain: vedantaconnect.com  compute:  - hyperthreading: Enabled  name: worker  replicas: 0  controlPlane:  hyperthreading: Enabled  name: master  replicas: 3  metadata:  name: valpocp  networking:  clusterNetwork:  - cidr: 10.128.0.0/14  hostPrefix: 23  networkType: OVNKubernetes  serviceNetwork:  - 172.30.0.0/16  platform:  none: {}  fips: false  pullSecret: '{"auths":{"cloud.openshift.com":{"auth":"b3BlbnNoaWZ0LXJlbGVhc2UtZGV2K29jbV9hY2Nlc3NfNTIwYmZkODRhMmMwNDllMWIyOGNjMTJkMTJiMGEwNTE6WDRWNUw4RTFXQzVMMUdHUzI1WVoyN0RLNlRKMFQyMjlSQUY5UzZDTDdQMkpDMjBUMFNDOU9RM0tXWE9HVThBQQ==","email":"sandip.lala@vedanta.co.in"},"quay.io":{"auth":"b3BlbnNoaWZ0LXJlbGVhc2UtZGV2K29jbV9hY2Nlc3NfNTIwYmZkODRhMmMwNDllMWIyOGNjMTJkMTJiMGEwNTE6WDRWNUw4RTFXQzVMMUdHUzI1WVoyN0RLNlRKMFQyMjlSQUY5UzZDTDdQMkpDMjBUMFNDOU9RM0tXWE9HVThBQQ==","email":"sandip.lala@vedanta.co.in"},"registry.connect.redhat.com":{"auth":"","email":"sandip.lala@vedanta.co.in"},"registry.redhat.io":{"auth":"","email":"sandip.lala@vedanta.co.in"}}}'  sshKey:'ssh-ed25519AAAAC3NzaC1lZDI1NTE5AAAAIHp70plezL4+OVjSie+oLC3K6LcQAWjB5R5iLjZ20wFM prod@bastion.valpocp.vedantaconnect.com' |

### Creating the Openshift/Kubernetes manifest

|  |
| --- |
| [core@drlonvsacmdrcmg]$ ~/openshift-install create manifests  INFO Consuming Install Config from target directory  WARNING Mak ing control-plane schedulable by setting MastersSchedulable to true for Scheduler cluster settings INFO Manifests created in: /home/core/clusterconfig/manifests and /home/core/clusterconfig/openshift |

### Create the Ignition config files

|  |
| --- |
| [prod@bastion ~]$ ~/openshift-install create ignition-configs --dir clusterconfig  INFO Consuming OpenShift Install (Manifests) from target directory  INFO Consuming Openshift Manifests from target directory  INFO Consuming Master Machines from target directory  INFO Consuming Common Manifests from target directory  INFO Consuming Worker Machines from target directory  INFO Ignition-Configs created in: clusterconfig and clusterconfig/auth |

The following files will be generated in the directory.

|  |
| --- |
| [prod@bastion ~]$ cd clusterconfig/  [prod@bastion clusterconfig]$ tree  .  ├── auth  │   ├── kubeadmin-password  │   └── kubeconfig  ├── bootstrap.ign  ├── master.ign  ├── metadata.json  └── worker.ign  1 directory, 6 files |

• Install HTTPD Package • Start and Enable httpd Service

|  |
| --- |
| [prod@bastion ~]$ sudo systemctl start httpd  [prod@bastion ~]$ sudo systemctl enable httpd  Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.  [prod@bastion ~]$ sudo systemctl status httpd  ● httpd.service - The Apache HTTP Server  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)  Active: active (running) since Wed 2025-02-05 10:52:02 IST; 19s ago  Docs: man:httpd.service(8) |

• Create a directory in /var/www/html/ and copy the ignition files

|  |
| --- |
| [prod@bastion ~]$ sudo mkdir /var/www/html/ocp4 |

• Copy ignition files from ~/clusterconfig/ to /var/www/html/ocp4/  
directory

|  |
| --- |
| [prod@bastion ~]$ sudo cp -R ~/clusterconfig/\*.ign /var/www/html/ocp4 |

• Make sure all files have required permissions and ownership

|  |
| --- |
| [prod@bastion ~]$ sudo chmod 755 /var/www/html/ocp4/  [prod@bastion ~]$ sudo chown -R apache: /var/www/html/ocp4/ |

## Deploying Openshift

Provisioning bootstrap node

|  |
| --- |
| sudo coreos-installer install /dev/sda --insecure-url http:// bastion.valpocp.vedantaconnect.com:8080/ocp/bootstrap.ign --insecure-ignition --copy-network |

Run the above command to provision the master/worker node with respect to their ignition files.

### Monitoring the Bootstrap Process

Monitoring the bootstrap process from the Bastion host at different log levels (debug, error, info)

|  |
| --- |
| ~/openshift-install --dir ~/ocp-install wait-for bootstrap-complete --log-level=debug |

### [Remove the Bootstrap Node](https://github.com/ryanhay/ocp4-metal-install#remove-the-bootstrap-node)

Wait for installation to complete

1. Collect the OpenShift Console address and kubeadmin credentials from the output of the install-complete event

|  |
| --- |
| [prod@bastion ~]$ ./openshift-install --dir ~/clusterconfig wait-for install-complete  INFO Waiting up to 40m0s (until 11:39AM IST) for the cluster at https://api.valpocp.vedantaconnect.com:6443 to initialize...  INFO Checking to see if there is a route at openshift-console/console...  INFO Install complete!  INFO To access the cluster as the system:admin user when using 'oc', run 'export KUBECONFIG=/home/prod/clusterconfig/auth/kubeconfig'  INFO Access the OpenShift web-console here: <https://console-openshift-console.apps.valpocp.vedantaconnect.com>  INFO Login to the console with user: "kubeadmin", and password: "\*\*\*\*\*\*"  INFO Time elapsed: 1s |

1. Continue to join the worker nodes to the cluster in a new tab whilst waiting for the above command to complete.

### Join Nodes

1. Setup 'oc' and 'kubectl' clients on the bastion machine.

|  |
| --- |
| export KUBECONFIG=~/ocp-install/auth/kubeconfig # Test auth by viewing cluster nodes oc get nodes |

1. View and approve pending CSRs.

Note: Once you approve the first set of CSRs additional 'kubelet-serving' CSRs will be created. These must be approved too. If you do not see pending requests wait until you do.

|  |
| --- |
| # View CSRs oc get csr  # Approve all pending CSRs oc get csr -o go-template='{{range .items}}{{if not .status}}{{.metadata.name}}{{"\n"}}{{end}}{{end}}' | xargs oc adm certificate approve # Wait for kubelet-serving CSRs and approve them too with the same command oc get csr -o go-template='{{range .items}}{{if not .status}}{{.metadata.name}}{{"\n"}}{{end}}{{end}}' | xargs oc adm certificate approve |

1. Watch and wait for the Nodes to join the cluster and enter a 'Ready' status.

|  |
| --- |
| watch oc get nodes |

|  |
| --- |
| [prod@bastion ~]$ oc get nodes  NAME STATUS ROLES AGE VERSION  vlocpsrvm1.valpocp.vedantaconnect.com Ready control-plane,master 7d20h v1.29.10+67d3387  vlocpsrvm2.valpocp.vedantaconnect.com Ready control-plane,master 7d20h v1.29.10+67d3387  vlocpsrvm3.valpocp.vedantaconnect.com Ready control-plane,master 7d20h v1.29.10+67d3387  vlocpsrvw1.valpocp.vedantaconnect.com Ready worker 7d18h v1.29.10+67d3387  vlocpsrvw2.valpocp.vedantaconnect.com Ready worker 7d18h v1.29.10+67d3387  vlocpsrvw3.valpocp.vedantaconnect.com Ready worker 7d17h v1.29.10+67d3387 |

## Accessing the Cluster

### Accessing the Openshift Console

1. Wait for the 'console' Cluster Operator to become available

|  |
| --- |
| [prod@bastion ~]$ oc get co  NAME VERSION AVAILABLE PROGRESSING DEGRADED SINCE MESSAGE  authentication 4.16.27 True False False 6d16h  baremetal 4.16.27 True False False 7d19h  cloud-controller-manager 4.16.27 True False False 7d19h  cloud-credential 4.16.27 True False False 7d22h  cluster-autoscaler 4.16.27 True False False 7d19h  config-operator 4.16.27 True False False 7d19h  console 4.16.27 True False False 6d18h  control-plane-machine-set 4.16.27 True False False 7d19h  csi-snapshot-controller 4.16.27 True False False 6d20h  dns 4.16.27 True False False 6d20h  etcd 4.16.27 True False False 7d19h  image-registry 4.16.27 True False False 6d20h  ingress 4.16.27 True False False 6d16h  insights 4.16.27 True False False 7d19h  kube-apiserver 4.16.27 True False False 7d19h  kube-controller-manager 4.16.27 True False False 7d19h  kube-scheduler 4.16.27 True False False 7d19h  kube-storage-version-migrator 4.16.27 True False False 6d16h  machine-api 4.16.27 True False False 7d19h  machine-approver 4.16.27 True False False 7d19h  machine-config 4.16.27 True False False 7d19h  marketplace 4.16.27 True False False 7d19h  monitoring 4.16.27 True False False 4d23h  network 4.16.27 True False False 7d19h  node-tuning 4.16.27 True False False 6d20h  openshift-apiserver 4.16.27 True False False 6d20h  openshift-controller-manager 4.16.27 True False False 6d20h  openshift-samples 4.16.27 True False False 7d19h  operator-lifecycle-manager 4.16.27 True False False 7d19h  operator-lifecycle-manager-catalog 4.16.27 True False False 7d19h  operator-lifecycle-manager-packageserver 4.16.27 True False False 6d20h  service-ca 4.16.27 True False False 7d19h  storage 4.16.27 True False False 7d19h |

1. Navigate to the [OpenShift Console URL](https://console-openshift-console.apps.valpocp.vedantaconnect.com) and log in as the 'admin' user.

You will get self-signed certificate warnings that you can ignore if you need to login as kubeadmin and need to the password again you can retrieve it with: **cat ~/clusterconfig/auth/kubeadmin-password.**

### Accessing the Cluster Nodes.

1. Setup 'oc' and 'kubectl' clients on the bastion machine.

|  |
| --- |
| export KUBECONFIG=~/clusterconfig/auth/kubeconfig # Test auth by viewing cluster nodes oc get nodes |

1. SSH to Master / Worker Node by the following command:

|  |
| --- |
| ssh core@<hostname or ip> |

* Verify the status of nodes.

|  |
| --- |
| [prod@bastion ~]$ oc get nodes  NAME STATUS ROLES AGE VERSION  vlocpsrvm1.valpocp.vedantaconnect.com Ready control-plane,master 14d v1.29.10+67d3387  vlocpsrvm2.valpocp.vedantaconnect.com Ready control-plane,master 14d v1.29.10+67d3387  vlocpsrvm3.valpocp.vedantaconnect.com Ready control-plane,master 14d v1.29.10+67d3387  vlocpsrvw1.valpocp.vedantaconnect.com Ready worker 14d v1.29.10+67d3387  vlocpsrvw2.valpocp.vedantaconnect.com Ready worker 14d v1.29.10+67d3387  vlocpsrvw3.valpocp.vedantaconnect.com Ready worker 14d v1.29.10+67d3387 |

* Check the status of cluster operators

|  |
| --- |
| [prod@bastion ~]$ oc get co  NAME VERSION AVAILABLE PROGRESSING DEGRADED SINCE MESSAGE  authentication 4.16.27 True False False 13d  baremetal 4.16.27 True False False 14d  cloud-controller-manager 4.16.27 True False False 14d  cloud-credential 4.16.27 True False False 15d  cluster-autoscaler 4.16.27 True False False 14d  config-operator 4.16.27 True False False 14d  console 4.16.27 True False False 13d  control-plane-machine-set 4.16.27 True False False 14d  csi-snapshot-controller 4.16.27 True False False 13d  dns 4.16.27 True False False 13d  etcd 4.16.27 True False False 14d  image-registry 4.16.27 True False False 13d  ingress 4.16.27 True False False 13d  insights 4.16.27 True False False 14d  kube-apiserver 4.16.27 True False False 14d  kube-controller-manager 4.16.27 True False False 14d  kube-scheduler 4.16.27 True False False 14d  kube-storage-version-migrator 4.16.27 True False False 13d  machine-api 4.16.27 True False False 14d  machine-approver 4.16.27 True False False 14d  machine-config 4.16.27 True False False 14d  marketplace 4.16.27 True False False 14d  monitoring 4.16.27 True False False 12d  network 4.16.27 True False False 14d  node-tuning 4.16.27 True False False 13d  openshift-apiserver 4.16.27 True False False 13d  openshift-controller-manager 4.16.27 True False False 13d  openshift-samples 4.16.27 True False False 14d  operator-lifecycle-manager 4.16.27 True False False 14d  operator-lifecycle-manager-catalog 4.16.27 True False False 14d  operator-lifecycle-manager-packageserver 4.16.27 True False False 13d  service-ca 4.16.27 True False False 14d  storage 4.16.27 True False False 14d |

## Trident CSI driver Installation and configuration

### Trident operator Installation

* Trident Binaries download and installation
* Download trident installer from

https://github.com/NetApp/trident/releases/download/v24.10.0/trident-installer-24.10.0.tar.gz

[prod@bastion trident-new-release]$ ll

drwxr-xr-x. 6 prod prod 84 Jan 24 16:55 trident-installer

-rw-r--r--. 1 prod prod 91725414 Jan 24 16:55 trident-installer-24.10.0.tar.gz

[prod@bastion trident-installer]$ ll

total 120364

drwxr-xr-x. 3 prod prod 4096 Jan 24 16:55 deploy

drwxr-xr-x. 4 prod prod 30 Jan 24 16:55 extras

drwxr-xr-x. 2 prod prod 45 Jan 24 16:55 helm

drwxr-xr-x. 7 prod prod 132 Jan 24 16:55 sample-input

-rwxr-xr-x. 1 prod prod 123244696 Jan 24 16:55 tridentctl

[prod@bastion trident-installer]$ ./tridentctl images

+--------------------+---------------------------------------------------------------+

| KUBERNETES VERSION | CONTAINER IMAGE |

+--------------------+---------------------------------------------------------------+

| v1.25.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

| v1.26.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

| v1.27.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

| v1.28.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

| v1.29.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

| v1.30.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

| v1.31.0 | netapp/trident:24.10.0 |

| | docker.io/netapp/trident-autosupport:24.10 |

| | registry.k8s.io/sig-storage/csi-provisioner:v5.1.0 |

| | registry.k8s.io/sig-storage/csi-attacher:v4.7.0 |

| | registry.k8s.io/sig-storage/csi-resizer:v1.12.0 |

| | registry.k8s.io/sig-storage/csi-snapshotter:v8.1.0 |

| | registry.k8s.io/sig-storage/csi-node-driver-registrar:v2.12.0 |

| | netapp/trident-operator:24.10.0 (optional) |

+--------------------+---------------------------------------------------------------+

...

Create trident project

…

[prod@bastion trident-installer]$ **oc new-project trident**

[prod@bastion trident-installer]$ cd deploy/crds/

[prod@bastion crds]$ ll

total 36

-rw-r--r--. 1 prod prod 1485 Jan 24 16:55 trident.netapp.io\_tridentconfigurators\_crd.yaml

-rw-r--r--. 1 prod prod 585 Jan 24 16:55 trident.netapp.io\_tridentorchestrators\_crd\_post1.16.yaml

-rw-r--r--. 1 prod prod 585 Jan 24 16:55 trident.netapp.io\_tridentorchestrators\_crd.yaml

-rw-r--r--. 1 prod prod 168 Jan 24 16:55 tridentorchestrator\_cr\_audit\_log.yaml

-rw-r--r--. 1 prod prod 261 Jan 24 16:55 tridentorchestrator\_cr\_autosupport.yaml

-rw-r--r--. 1 prod prod 178 Jan 24 16:55 tridentorchestrator\_cr\_customimage.yaml

-rw-r--r--. 1 prod prod 179 Jan 24 16:55 tridentorchestrator\_cr\_default.yaml

-rw-r--r--. 1 prod prod 203 Jan 24 16:55 tridentorchestrator\_cr\_imagepullsecrets.yaml

-rw-r--r--. 1 prod prod 195 Jan 24 16:55 tridentorchestrator\_cr.yaml

[prod@bastion crds]$ pwd

/home/prod/post\_config\_files/trident/trident-new-release/trident-installer/deploy/crds

[prod@bastion crds]$

[prod@bastion crds]$ **oc create -f trident.netapp.io\_tridentorchestrators\_crd.yaml**

[prod@bastion crds]$ cd ..

[prod@bastion deploy]$ **oc create -f bundle\_post\_1\_25.yaml**

[prod@bastion deploy]$ pwd

/home/prod/post\_config\_files/trident/trident-new-release/trident-installer/deploy

[prod@bastion deploy]$

[prod@bastion deploy]$ cd crds/

[prod@bastion crds]$ **oc create -f tridentorchestrator\_cr.yaml**

[prod@bastion crds]$ **oc get tridentorchestrators.trident.netapp.io trident -n trident**

NAME AGE

trident 13d

* Verify trident operator, controller and daemonset pods are running

[prod@bastion crds]$ oc get pods -n trident -owide

NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

trident-controller-66b97d5f8d-6p2m4 6/6 Running 0 12d 10.131.0.5 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>

trident-node-linux-46tkz 2/2 Running 21 13d 10.101.143.14 vlocpsrvm1.valpocp.vedantaconnect.com <none> <none>

trident-node-linux-5cksc 2/2 Running 19 13d 10.101.143.19 vlocpsrvw3.valpocp.vedantaconnect.com <none> <none>

trident-node-linux-cxc5s 2/2 Running 14 (24h ago) 13d 10.101.143.18 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>

trident-node-linux-fbj5d 2/2 Running 16 (24h ago) 13d 10.101.143.17 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>

trident-node-linux-g67sx 2/2 Running 14 13d 10.101.143.15 vlocpsrvm2.valpocp.vedantaconnect.com <none> <none>

trident-node-linux-j484b 2/2 Running 13 13d 10.101.143.16 vlocpsrvm3.valpocp.vedantaconnect.com <none> <none>

trident-operator-568cfdfc6b-4lcf2 1/1 Running 0 12d 10.128.2.5 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>

[prod@bastion trident-installer]$ **./tridentctl version -n trident**

+----------------+----------------+

| SERVER VERSION | CLIENT VERSION |

+----------------+----------------+

| 24.10.0 | 24.10.0 |

+----------------+----------------+

### Trident RHCOS changes

[prod@bastion netapp-csi]$ cat mcp\_iscsi.yaml

apiVersion: machineconfiguration.openshift.io/v1

kind: MachineConfig

metadata:

name: 99-worker-ontap-iscsi

labels:

machineconfiguration.openshift.io/role: master

spec:

config:

ignition:

version: 3.2.0

storage:

files:

- contents:

source:data:text/plain;charset=utf-8;base64,ZGVmYXVsdHMgewogICAgICAgIHVzZXJfZnJpZW5kbHlfbmFtZXMgbm8KICAgICAgICBmaW5kX211bHRpcGF0aHMgbm8KfQoKYmxhY2tsaXN0X2V4Y2VwdGlvbnMgewogICAgICAgIHByb3BlcnR5ICIoU0NTSV9JREVOVF98SURfV1dOKSIKfQoKYmxhY2tsaXN0IHsKfQoK

verification: {}

filesystem: root

mode: 420

path: /etc/multipath.conf

systemd:

units:

- name: iscsid.service

enabled: true

state: started

- name: multipathd.service

enabled: true

state: started

[prod@bastion trident-installer]$ cd ~/post\_config\_files/netapp-csi/

[prod@bastion netapp-csi]$ oc apply -f mcp\_iscsi.yaml

machineconfig.machineconfiguration.openshift.io/99-worker-ontap-iscsi created

### Trident Backend Config

* Create TBC(trident backend config) for ontap SAN and NAS

[prod@bastion netapp-csi]$ pwd

/home/prod/post\_config\_files/netapp-csi

[prod@bastion netapp-csi]$ ll

total 24

-rw-r--r--. 1 prod prod 477 Jan 28 18:36 backend-tbc-ontap-nas.yaml

-rw-r--r--. 1 prod prod 473 Jan 29 19:05 backend-tbc-ontap-san.yaml

-rw-r--r--. 1 prod prod 820 Jan 29 18:45 mcp\_iscsi.yaml

-rw-r--r--. 1 prod prod 261 Jan 24 16:55 storage-class-ontapnas.yaml

-rw-r--r--. 1 prod prod 283 Jan 31 12:22 storage-class-ontap-san-ext4.yaml

-rw-r--r--. 1 prod prod 260 Jan 29 19:14 storage-class-ontap-san.yaml

[prod@bastion netapp-csi]$ cat backend-tbc-ontap-san.yaml

apiVersion: v1

kind: Secret

metadata:

name: backend-tbc-ontap-san-secret

type: Opaque

stringData:

username: vsadmin

password: xxxxxxxxx

---

apiVersion: trident.netapp.io/v1

kind: TridentBackendConfig

metadata:

name: backend-tbc-ontap-san

spec:

version: 1

storageDriverName: ontap-san

managementLIF: 10.101.143.30

backendName: tbc-ontap-san

storagePrefix: prod-ocp-san

sanType: fcp

svm: svm\_san

credentials:

name: backend-tbc-ontap-san-secret

[prod@bastion netapp-csi]$ oc apply -f backend-tbc-ontap-san.yaml -n trident

secret/backend-tbc-ontap-san-secret created

tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san created

[prod@bastion netapp-csi]$ cat backend-tbc-ontap-nas.yaml

apiVersion: v1

kind: Secret

metadata:

name: backend-tbc-ontap-nas-secret

type: Opaque

stringData:

username: admin

password: xxxxxxxxx

---

apiVersion: trident.netapp.io/v1

kind: TridentBackendConfig

metadata:

name: backend-tbc-ontap-nas

spec:

version: 1

storageDriverName: ontap-nas

managementLIF: 10.101.143.33

dataLIF: 10.101.143.34

backendName: tbc-ontap-nas

storagePrefix: prod-ocp

svm: svm\_nas

credentials:

name: backend-tbc-ontap-nas-secret

[prod@bastion netapp-csi]$ oc apply -f backend-tbc-ontap-nas.yaml -n trident

secret/backend-tbc-ontap-nas-secret created

tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-nas created

[prod@bastion netapp-csi]$ oc get tbc

NAME BACKEND NAME BACKEND UUID PHASE STATUS

backend-tbc-ontap-nas tbc-ontap-nas 93317ef2-1033-4535-8630-a3e517338707 Bound Success

backend-tbc-ontap-san tbc-ontap-san 1257f90b-73ab-4f16-bee4-6efae67f1e80 Bound Success

### Trident Storage class Config

* Create storage class to bound with backend config for SAN/NAS.

[prod@bastion netapp-csi]$ cat storage-class-ontapnas.yaml

apiVersion: storage.k8s.io/v1

kind: StorageClass

metadata:

name: ontap-nas-sc

provisioner: csi.trident.netapp.io

parameters:

backendType: "ontap-nas"

provisioningType: "thin"

volumeBindingMode: Immediate

reclaimPolicy: Retain

allowVolumeExpansion: true

[prod@bastion netapp-csi]$ oc apply -f storage-class-ontapnas.yaml

storageclass.storage.k8s.io/ontap-nas-sc created

[prod@bastion netapp-csi]$ cat storage-class-ontap-san-ext4.yaml

apiVersion: storage.k8s.io/v1

kind: StorageClass

metadata:

name: ontap-san-sc-ext4

provisioner: csi.trident.netapp.io

parameters:

backendType: "ontap-san"

provisioningType: "thin"

fsType: "ext4"

allowVolumeExpansion: True

volumeBindingMode: Immediate

reclaimPolicy: Delete

[prod@bastion netapp-csi]$ oc apply -f storage-class-ontap-san-ext4.yaml

storageclass.storage.k8s.io/ontap-san-sc-ext4created

[prod@bastion netapp-csi]$ cat storage-class-ontap-san.yaml

apiVersion: storage.k8s.io/v1

kind: StorageClass

metadata:

name: ontap-san-sc

provisioner: csi.trident.netapp.io

parameters:

backendType: "ontap-san"

provisioningType: "thin"

allowVolumeExpansion: True

volumeBindingMode: Immediate

reclaimPolicy: Delete

[prod@bastion netapp-csi]$ oc apply -f storage-class-ontap-san.yaml

storageclass.storage.k8s.io/ontap-san-sc created

[prod@bastion netapp-csi]$ oc get sc

NAME PROVISIONER RECLAIMPOLICY VOLUMEBINDINGMODE ALLOWVOLUMEEXPANSION AGE

ontap-nas-sc csi.trident.netapp.io Retain Immediate true 14d

ontap-san-sc (default) csi.trident.netapp.io Delete Immediate true 13d

ontap-san-sc-ext4 csi.trident.netapp.io Delete Immediate true 12d

[prod@bastion netapp-csi]$ cd ../trident/trident-new-release/trident-installer/

[prod@bastion trident-installer]$ ./tridentctl get storageclass -n trident

+-------------------+

| NAME |

+-------------------+

| ontap-nas-sc |

| ontap-san-sc |

| ontap-san-sc-ext4 |

+-------------------+

### Identify backend for storage class

* Valiidate class to backend mapping.

[prod@bastion trident-installer]$ ./tridentctl get storageclass -n trident -o json | jq '[.items[] | {storageClass: .Config.name, backends: [.storage]|unique}]'

[

{

"storageClass": "ontap-nas-sc",

"backends": [

{

"tbc-ontap-nas": [

"data\_aggr1"

]

}

]

},

{

"storageClass": "ontap-san-sc",

"backends": [

{

"tbc-ontap-san": [

"data\_aggr1"

]

}

]

},

{

"storageClass": "ontap-san-sc-ext4",

"backends": [

{

"tbc-ontap-san": [

"data\_aggr1"

]

}

]

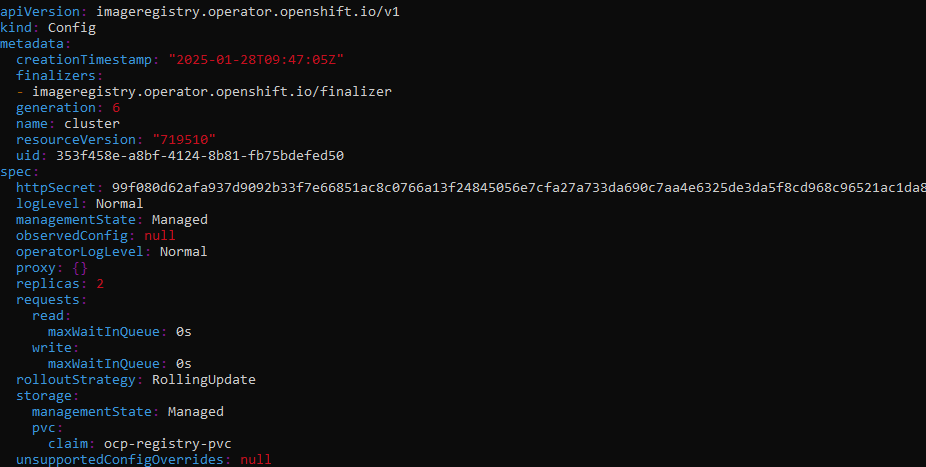
}

]

## Deploying Openshift Internal Registry with Persistent Storage

* By default, there will be no registry pod running as the registry operator’s "managementState" will be set as "Removed". Configure image registry to "Managed" state and move the registry pods to the dedicated infra nodes as shown below. Right now an object storage volume is being used inside the registry pods.

|  |
| --- |
| oc edit configs.imageregistry.operator.openshift.io/cluster |



* Create a PVC “ocp-registry-pvc” and Verify if the registry pod is running.

|  |
| --- |
| [dbpuser@bastion ~]$  [prod@bastion image-registry]$ cat pvc-provisioning.yaml  apiVersion: v1  kind: PersistentVolumeClaim  metadata:  name: ocp-registry-pvc  spec:  # SAME NAME AS THE STORAGECLASS  storageClassName: ontap-nas-sc  accessModes:  - ReadWriteMany  # Must be the same as PersistentVolume  resources:  requests:  storage: 500Gi  [prod@bastion image-registry]$ #oc apply -f pvc-provisioning.yaml  [prod@bastion image-registry]$ oc get pods  NAME READY STATUS RESTARTS AGE  cluster-image-registry-operator-5d89674fbd-fg6rn 1/1 Running 0 13d  image-registry-6985c79cbc-97xgx 1/1 Running 0 13d  image-registry-6985c79cbc-sxcv9 1/1 Running 0 13d |

## Configure System Clock Sync with NTP Server

### Configure master nodes system clock sync with NTP server

* Create a Butane config including the contents of the chrony.conf file, to configure chrony on worker nodes, create a 99-worker-chrony.bu file and use Butane to generate a MachineConfig object file, 99- worker-chrony.yaml, containing the configuration to be delivered to the nodes. Repeat the same steps for other machine-config-pool like master. .

|  |
| --- |
| [prod@bastion ntp\_config]$ cat 99-worker-chrony.bu  variant: openshift  version: 4.16.0  metadata:  name: 99-worker-chrony  labels:  machineconfiguration.openshift.io/role: worker  storage:  files:  - path: /etc/chrony.conf  mode: 0644  overwrite: true  contents:  inline: |  server 10.101.141.3 iburst  driftfile /var/lib/chrony/drift  makestep 1.0 3  rtcsync  logdir /var/log/chrony |

|  |
| --- |
| [prod@bastion ntp\_config]$./butane 99-worker-chrony.bu -o 99-worker-chrony.yaml |

* Apply the MachineConfig YAML file

|  |
| --- |
| [prod@bastion ntp\_config]$ oc create -f ./99-worker-chrony.yaml  machineconfig.machineconfiguration.openshift.io/99-worker-chrony created  [prod@bastion ntp\_config]$ pwd  /home/prod/post\_config\_files/ntp\_config  [prod@bastion ntp\_config]$ ll  total 7900  -rw-r--r--. 1 prod prod 387 Jan 24 16:55 99-master-chrony.bu  -rw-r--r--. 1 prod prod 572 Jan 24 16:55 99-master-chrony.yaml  -rw-r--r--. 1 prod prod 387 Jan 24 17:12 99-worker-chrony.bu  -rw-r--r--. 1 prod prod 572 Jan 24 17:13 99-worker-chrony.yaml  -rwxr-xr-x. 1 prod prod 8070568 Jan 24 16:55 butane |

* Once NTP config are applied, the worker and infra nodes will get rebooted and come back online.

|  |
| --- |
| [prod@bastion ntp\_config]$ ssh core@10.101.143.17  [core@vlocpsrvw1 ~]$ chronyc sources  MS Name/IP address Stratum Poll Reach LastRx Last sample  ===============================================================================  ^\* 10.101.141.3 1 10 377 896 +72us[ +98us] +/- 1015us |

|  |
| --- |
| [core@vlocpsrvw1 ~]$ chronyc tracking  Reference ID : 0A658D03 (10.101.141.3)  Stratum : 2  Ref time (UTC) : Wed Feb 05 12:23:08 2025  System time : 0.000058596 seconds fast of NTP time  Last offset : +0.000025681 seconds  RMS offset : 0.000192539 seconds  Frequency : 16.776 ppm fast  Residual freq : +0.001 ppm  Skew : 0.121 ppm  Root delay : 0.001474854 seconds  Root dispersion : 0.001345289 seconds  Update interval : 1031.3 seconds  Leap status : Normal |

Repeat the above commands on rest of master nodes to verify the system clock with NTP and make sure "System clock synchronized: yes"

## Configuring an HTPasswd identity provider

* Create a flat file with a user name and hashed password

|  |
| --- |
| [prod@bastion htpasswd]$ pwd  /home/prod/post\_config\_files/auth\_providers/htpasswd  [prod@bastion htpasswd]$ cd ..  [prod@bastion auth\_providers]$ pwd  /home/prod/post\_config\_files/auth\_providers  [prod@bastion auth\_providers]$ mkdir htpasswd  [prod@bastion auth\_providers]$ cd htpasswd/  [prod@bastion auth\_providers]$ htpasswd -cB users.htpasswd ocpadmin  New password:  Re-type new password:  Adding password for user ocpadmin |

The password used for the ocpadmin account hasn’t been disclosed here but the same has been shared with the customer.

* Create an OpenShift Container Platform Secret object that contains the HTPasswd users file

[

[prod@bastion auth\_providers]$ oc create secret generic htpass-secret --from-file=htpasswd=users.htpasswd -n openshift-config

secret/htpass-secret created

The secret key containing the users file for the --from-file argument must be named

**htpasswd**

, as shown in the above command.

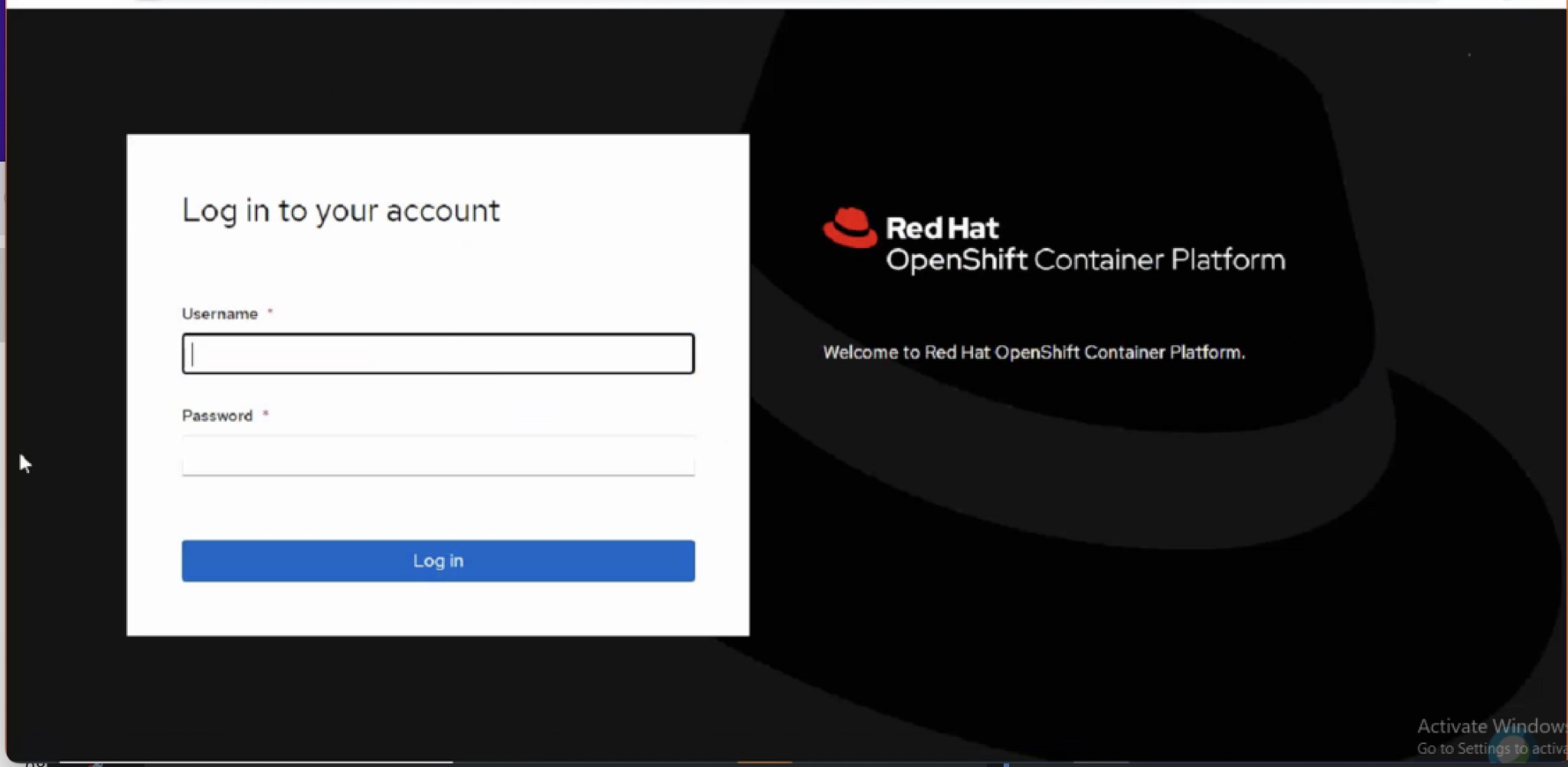
* Create HTPasswd identity provider YAML manifests as below

|  |
| --- |
| [prod@bastion htpasswd]$ cat oauth.yaml  apiVersion: config.openshift.io/v1  kind: OAuth  metadata:  name: cluster  spec:  identityProviders:  - name: VAL\_ITMS\_htpasswd  mappingMethod: claim  type: HTPasswd  htpasswd:  fileData:  name: htpasswd-secret |

* Adding HTPasswd identity provider to the cluster

|  |
| --- |
| [prod@bastion htpasswd]$ oc apply -f oauth.yaml  Warning: oc apply should be used on resource created by either oc create --save-config or oc apply oauth.config.openshift.io/cluster configured |

* Access the OCP Web Console and click on the HTPasswd identity provider & login using ocpadmin as the user with the respective password set earlier while creating the user account



* Grant the **ocpadmin** user account with **cluster-admin** access as shown below.

|  |
| --- |
| [prod@bastion htpasswd]$ oc adm policy add-cluster-role-to-user cluster-admin ocpadmin clusterrole.rbac.authorization.k8s.io/cluster-admin added: "ocpadmin"  [core@rlonvsacmdrcm1 htpasswd]$ cd .. |

Please store the 'ocpadmin' password in a secured place as it has been granted with cluster-admin privilege to manage the entire OCP cluster.

## Registering the Cluster

* Subscription and support

The cluster will be automatically registered with a 60 day evaluation subscription which does not include support. In order to receive support for your cluster, you will need to register OpenShift Container Platform 4 cluster on cloud.redhat.com.

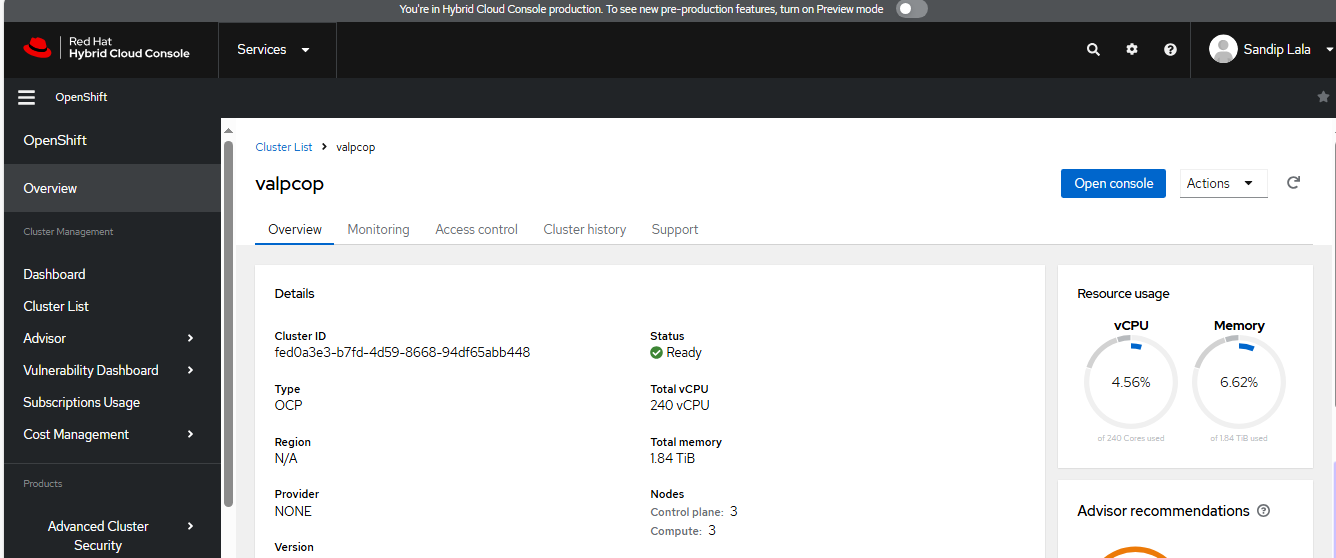
* To register a disconnected OCP 4 cluster on cloud.redhat.com the cluster profile needs to be created manually as outlined below:

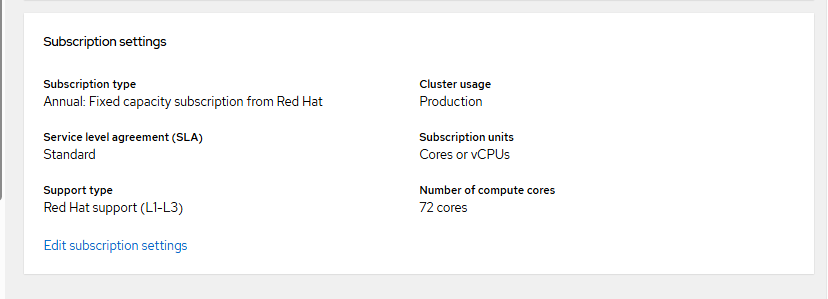
◦ Go to cloud.redhat.com and login with Vedanta\_jharsuguda login credentials.

◦ Go to the Clusters tab and select the three dots near Create cluster and click on the Register cluster button. Alternatively, use [**https://cloud.redhat.com/openshift/register**](https://cloud.redhat.com/openshift/register) ◦ ◦ Enter all the required details like cluster-id, number of sockets, memory, etc.

◦ After filling all the required details click on the Register cluster. This will create a cluster profile in disconnected mode.

◦ After that, click on the respective cluster name in the 'Clusters' tab. Edit the Subscription Settings and attach the subscription according to the cluster configuration and environment by scrolling down to 'Subscription settings'.





To get more details, Please visit the below URL:

<https://access.redhat.com/solutions/4930131>

## Encrypting the ETCD data

* Edit the apiserver object & make an entry under spec as shown below

|  |
| --- |
| [prod@bastion]$ oc edit apiserver  …  …  spec:  encryption:  type: aescbc  audit:      profile: Default |

* Verify if all the resource under **openshiftapiserver** and **kubeapiserver** are encrypted as shown below.

|  |
| --- |
| [prod@bastion ~]$oc get openshiftapiserver -o=jsonpath='{range .items[0].status.conditions[?(@.type=="Encrypted")]}{.reason}{"\n"}{.message}{"\n"}'  EncryptionCompleted  All resources encrypted: routes.route.openshift.io  [prod@bastion ~]$ oc get kubeapiserver -o=jsonpath='{range .items[0].status.conditions[?(@.type=="Encrypted")]}{.reason}{"\n"}{.message}{"\n"}'  EncryptionCompleted  All resources encrypted: secrets, configmaps |

## Backing Up ETCD data

* Login to one of the master node and perform the backup of ETCD data as shown below

|  |
| --- |
| [prod@bastion monitoring]$ ssh core@10.101.143.14  [core@vlocpsrvm1 ~]$ sudo -i  [root@vlocpsrvm1 ~]# cd /usr/local/bin/  [root@vlocpsrvm1 bin]# mkdir -p /home/core/assets/backup  [root@vlocpsrvm1 bin]# ll  total 84  -rwxr-xr-x. 1 root root 4791 Jan 28 09:57 cluster-backup.sh  -rwxr-xr-x. 1 root root 5990 Jan 28 09:57 cluster-restore.sh  -rwxr-xr-x. 1 root root 41347 Jan 29 13:03 configure-ovs.sh  -rwxr-xr-x. 1 root root 100 Jan 29 13:03 kubenswrapper  -rwxr-xr-x. 1 root root 2431 Jan 29 13:03 mco-hostname  -rwxr-xr-x. 1 root root 5733 Jan 29 13:03 nm-clean-initrd-state.sh  -rwxr-xr-x. 1 root root 1218 Jan 29 13:03 recover-kubeconfig.sh  -rwxr-xr-x. 1 root root 708 Jan 29 13:03 wait-for-primary-ip.sh  [root@vlocpsrvm1 bin]# ./cluster-backup.sh /home/core/assets/backup |

* Create a directory to store the ETCD Backup in Bastion Node

[prod@bastion ~]$ mkdir -p etcd-backups/30-01-2025

* Copy the backed up files from the master node to the Bastion node as shown below

|  |
| --- |
| [prod@bastion ~]$ scp core@10.101.143.14:/home/core/assets/backup/static\_kuberesources\_2025-01-30\_082946.tar.gz ./etcd-backups/30-01-2025/  static\_kuberesources\_2025-01-30\_082946.tar.gz 100% 80KB 12.5MB/s 00:00 |

## Deploying and Configuring Openshift Logging

### Install Cluster Logging Operators

* Install the Elasticsearch Operator
* In the OpenShift Container Platform web console, click Operators → OperatorHub.
* Choose Elasticsearch Operator from the list of available Operators, and click Install.
* Ensure that the all namespaces on the cluster is selected under Installation Mode.
* Ensure that openshift-operators-redhat is selected under Installed Namespace.
* Select Enable operator recommended cluster monitoring on this namespace.
* Select stable as the Update Channel.
* Select an Approval Strategy to Automatic
* Click Install.
* Verify that the Elasticsearch Operator installed by switching to the Operators → Installed Operators page.
* Ensure that Elasticsearch Operator is listed in all projects with a Status of Succeeded.
* Install the Cluster Logging Operator.
* In the OpenShift Container Platform web console, click Operators → OperatorHub.
* Choose Cluster Logging from the list of available Operators, and click Install.
* Ensure that the A specific namespace on the cluster is selected under Installation Mode.
* Ensure that Operator recommended namespace is openshift-logging under Installed Namespace.
* Select Enable operator recommended cluster monitoring on this namespace.
* Select stable as the Update Channel.
* Select an Approval Strategy to Automatic. Click Install.
* Verify that the Cluster Logging Operator installed by switching to the Operators → Installed Operators page.
* Ensure that Cluster Logging is listed in the openshift-logging project with a Status of Succeeded.

### Create Cluster Logging Instance

* Create a cluster logging instance YAML manifest
* Create a Cluster Logging instance

|  |
| --- |
| [prod@bastion logging]$ cat cluster-logging.yaml  kind: ClusterLogging  apiVersion: logging.openshift.io/v1  metadata:  name: instance  namespace: openshift-logging  spec:  collection:  type: vector  logStore:  elasticsearch:  nodeCount: 3  redundancyPolicy: SingleRedundancy  resources:  limits:  cpu: 2000m  memory: 16Gi  requests:  cpu: 1500m  memory: 16Gi  storage:  size: 900Gi  storageClassName: ontap-san-sc-ext4  retentionPolicy:  application:  maxAge: 7d  audit:  maxAge: 7d  infra:  maxAge: 7d  type: elasticsearch  managementState: Managed  visualization:  kibana:  replicas: 1  resources:  limits:  memory: 1Gi  requests:  cpu: 500m  memory: 1Gi  type: kibana |

* Create the ClusterLogging instance object as shown below

|  |
| --- |
| [prod@bastion logging]$ oc apply -f cluster-logging.yaml  clusterlogging.logging.openshift.io/instance created |

* Verify the cluster logging pods deployed in the openshift-logging project

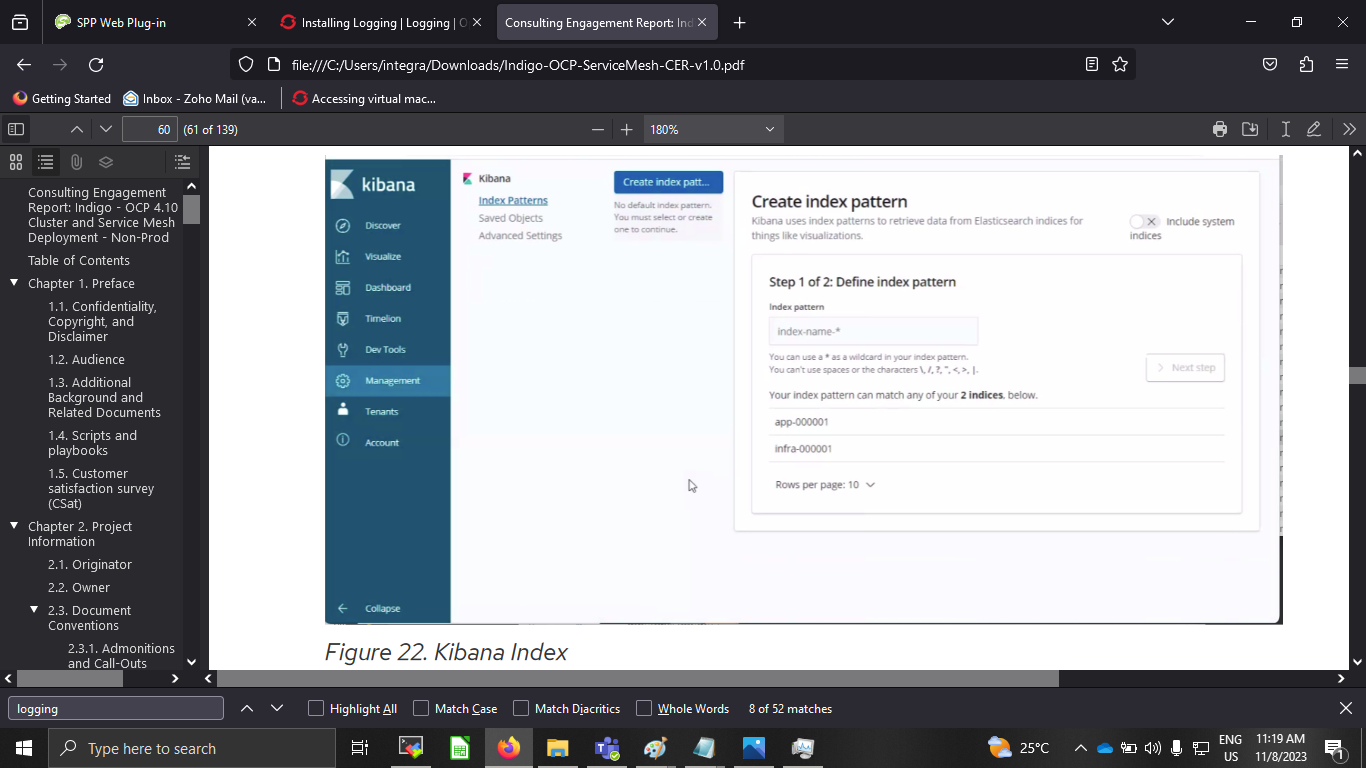
|  |
| --- |
| [prod@bastion logging]$ oc get po -o wide -n openshift-logging  NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES  cluster-logging-operator-67849b4498-6kqjw 1/1 Running 0 22h 10.131.0.56 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  collector-7cmnc 1/1 Running 0 22h 10.129.3.11 vlocpsrvw3.valpocp.vedantaconnect.com <none> <none>  collector-8bsvf 1/1 Running 0 22h 10.128.1.105 vlocpsrvm3.valpocp.vedantaconnect.com <none> <none>  collector-hppvh 1/1 Running 0 22h 10.128.2.78 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  collector-mcr4g 1/1 Running 0 22h 10.130.0.140 vlocpsrvm2.valpocp.vedantaconnect.com <none> <none>  collector-t9wnq 1/1 Running 0 22h 10.129.1.49 vlocpsrvm1.valpocp.vedantaconnect.com <none> <none>  collector-zzwkn 1/1 Running 0 22h 10.131.0.62 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  elasticsearch-cdm-j7x3zowz-1-75d96d7d99-g8jxc 2/2 Running 0 22h 10.129.3.10 vlocpsrvw3.valpocp.vedantaconnect.com <none> <none>  elasticsearch-cdm-j7x3zowz-2-75d65d7b86-56pt6 2/2 Running 2 (18h ago) 18h 10.131.0.128 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  elasticsearch-cdm-j7x3zowz-3-85fbfd6f4f-zj8fb 2/2 Running 0 22h 10.128.2.77 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  elasticsearch-im-app-28987650-7bj7t 0/1 Completed 0 7m21s 10.131.1.178 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  elasticsearch-im-audit-28987650-9hh4x 0/1 Completed 0 7m21s 10.131.1.179 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  elasticsearch-im-infra-28987650-jjxq5 0/1 Completed 0 7m21s 10.131.1.177 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  kibana-b6bcd45c7-vxjjn 2/2 Running 0 22h 10.131.0.60 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none> |

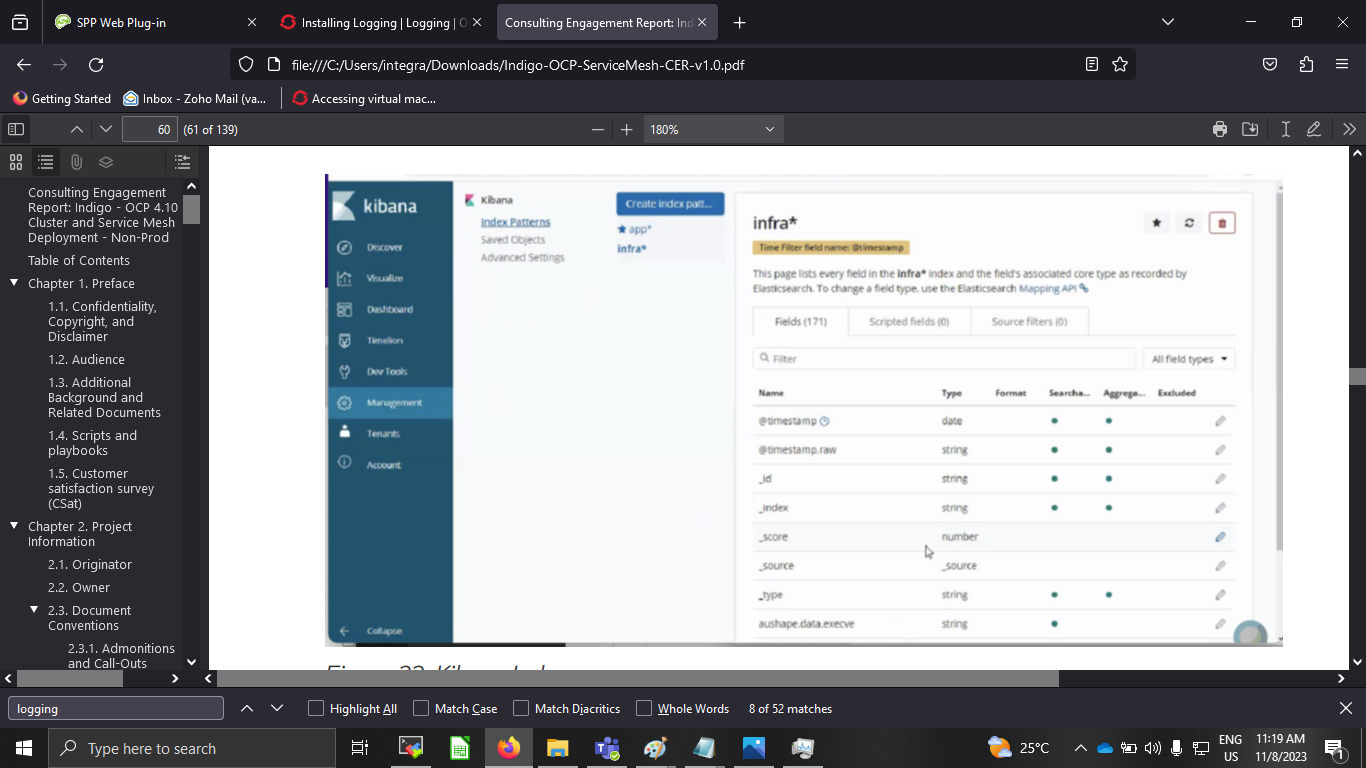
* Verify PVCs created for Elasticsearch components

|  |
| --- |
| [prod@bastion logging]$ oc get pvc -n openshift-logging  NAME STATUS VOLUME CAPACITY ACCESS MODES STORAGECLASS VOLUMEATTRIBUTESCLASS AGE  elasticsearch-elasticsearch-cdm-j7x3zowz-1 Bound pvc-c8e4078f-af0c-44c4-847e-28feb5f3458d 900Gi RWO ontap-san-sc-ext4 <unset> 22h  elasticsearch-elasticsearch-cdm-j7x3zowz-2 Bound pvc-aec8d92a-4077-4002-9ad3-83192ed90187 900Gi RWO ontap-san-sc-ext4 <unset> 18h  elasticsearch-elasticsearch-cdm-j7x3zowz-3 Bound pvc-8ecf170f-f485-4fe6-af2c-6c8c42ca996c 900Gi RWO ontap-san-sc-ext4 <unset> 22h |

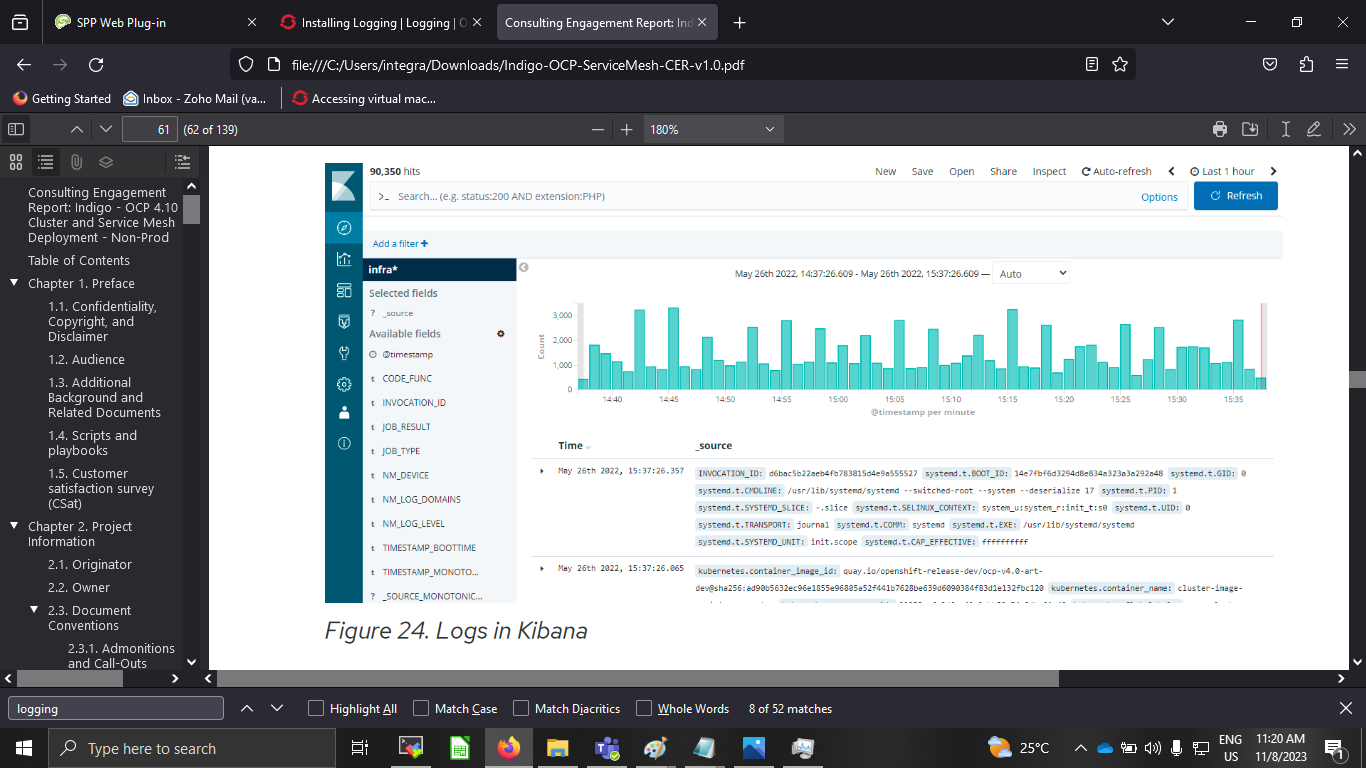
### Viewing cluster logs from the Kibana dashboard

* To define index patterns and create visualizations in Kibana
* In the OpenShift Container Platform console, click the Application Launcher and select Logging.
* Create your Kibana index patterns by clicking Management → Index Patterns → Create index pattern.
  + Users must manually create index patterns to see logs for their projects. Users should create a new index pattern named app and use the @timestamp time field to view their container logs.
  + Admin users must create index patterns for the app, infra, and audit indices using the @timestamp time field.
* Create Kibana Visualizations from the new index patterns.





* To view logs in Kibana
* In the OpenShift Container Platform console, click the Application Launcher and select  
  Logging.
* Log in using the same credentials you use to log in to the OpenShift Container Platform console.
* In Kibana, click Discover.
* Select the index pattern you created from the drop-down menu in the top-left corner: app, audit, or infra. The log data displays as time-stamped documents.
* Expand one of the time-stamped documents.



## Applying a custom Alertmanager configuration with the SMTP details

• Print the currently active Alertmanager configuration into a file **alertmanager.yaml**

|  |
| --- |
| [prod@bastion post\_config\_files]$ mkdir smtp  [prod@bastion post\_config\_files]$ cd smtp/  [prod@bastion smtp]$ oc -n openshift-monitoring get secret alertmanager-main --template='{{ index .data "alertmanager.yaml" }}' | base64 -d > alertmanager.yaml  [prod@bastion smtp]$ ll  total 4  -rw-r--r--. 1 prod prod 657 Feb 12 14:21 alertmanager.yaml |

• Edit the configuration in the exported alertmanager.yaml file

|  |
| --- |
| "global":  "resolve\_timeout": "5m"  "smtp\_from": "VLJ.ITMS@vedanta.co.in"  "smtp\_smarthost": "smtp.office365.com:587"  "smtp\_auth\_username": "VLJ.ITMS@vedanta.co.in"  "smtp\_auth\_password": "H!ghPr0t3ct!0n"  "smtp\_require\_tls": false  "inhibit\_rules":  - "equal":  - "namespace"  - "alertname"  "source\_match":  "severity": "critical"  "target\_match\_re":  "severity": "warning|info"  - "equal":  - "namespace"  - "alertname"  "source\_match":  "severity": "warning"  "target\_match\_re":  "severity": "info"  "receivers":  - "name": "Default"  "email\_configs":  - "to": "praveen.babeley@tcs.com"  "headers":  "subject": 'PROD-Openshift-ITMS {{ template "email.default.subject" . }}'  "route":  "group\_by":  - "namespace"  "group\_interval": "5m"  "group\_wait": "30s"  "receiver": "Default"  "repeat\_interval": "12h"  "routes":  - "match":  "alertname": "Watchdog"  "receiver": "Default"  - "match":  "severity": "critical"  "receiver": "Default" |

Apply the new edited configuration as shown below.

|  |
| --- |
| $ oc -n openshift-monitoring create secret generic alertmanager-main --from-file=alertmanager.yaml --dry-run -o=yaml | oc -n openshift-monitoring  replace secret --filename=-  secret/alertmanager-main replaced |

## Configuring Openshift monitoring components

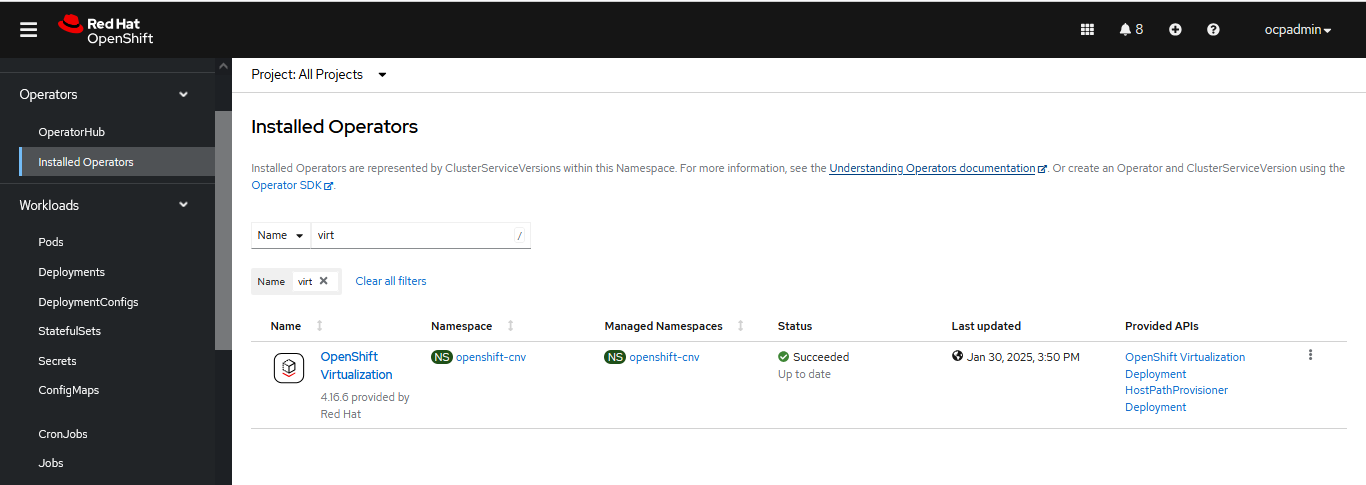
Create a configmap as shown below

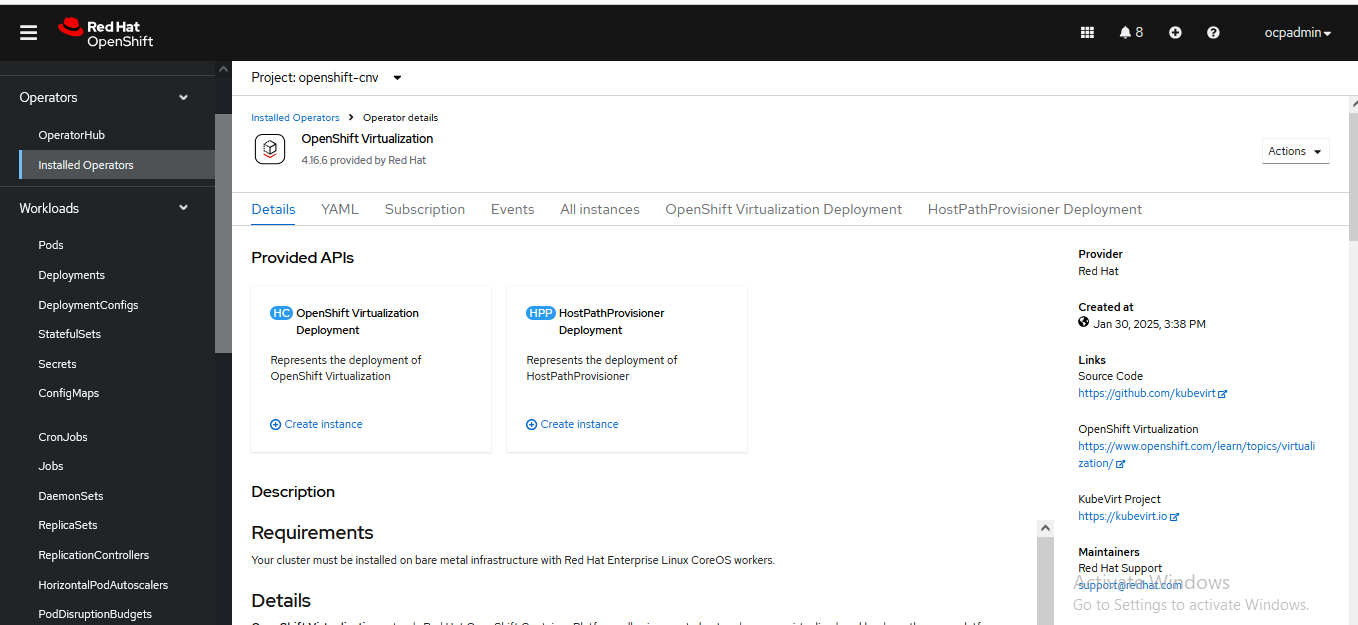
|  |
| --- |
| [prod@bastion monitoring]$ cat cluster-monitor-config.yaml  apiVersion: v1  kind: ConfigMap  metadata:  name: cluster-monitoring-config  namespace: openshift-monitoring  data:  config.yaml: |+  prometheusK8s:  volumeClaimTemplate:  metadata:  name: prometheus  spec:  storageClassName: ontap-san-sc-ext4  resources:  requests:  storage: 200Gi  retention: 14d  alertmanagerMain:  volumeClaimTemplate:  metadata:  name: alertmanager  spec:  storageClassName: ontap-san-sc  resources:  requests:  storage: 7.5Gi |

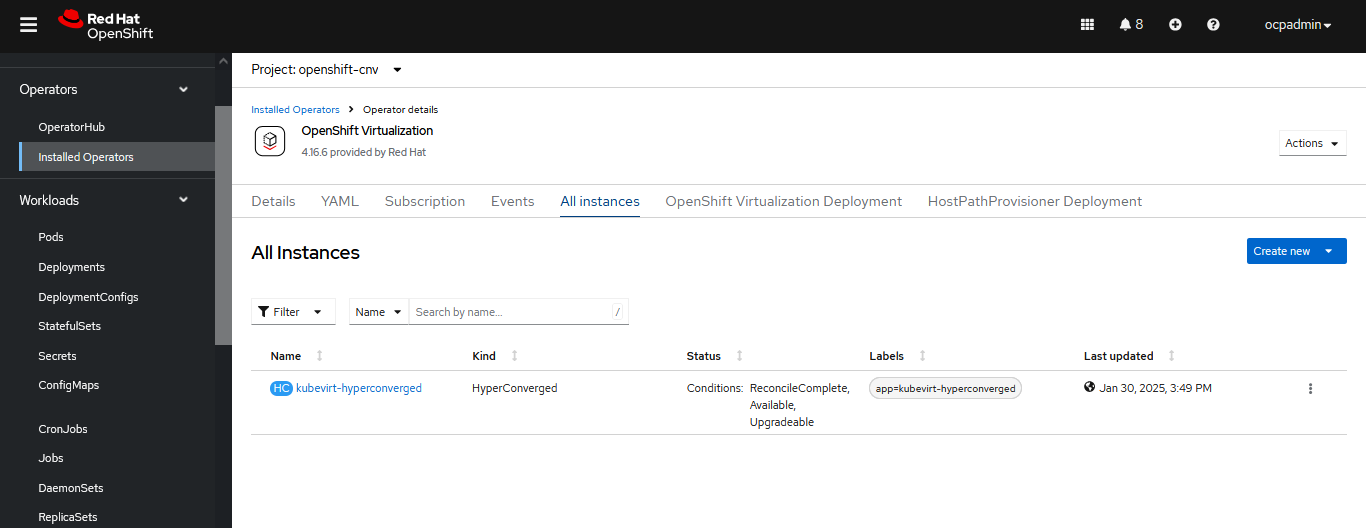
|  |
| --- |
| [prod@bastion monitoring]$ oc create -f cluster-monitoring-config.yaml |

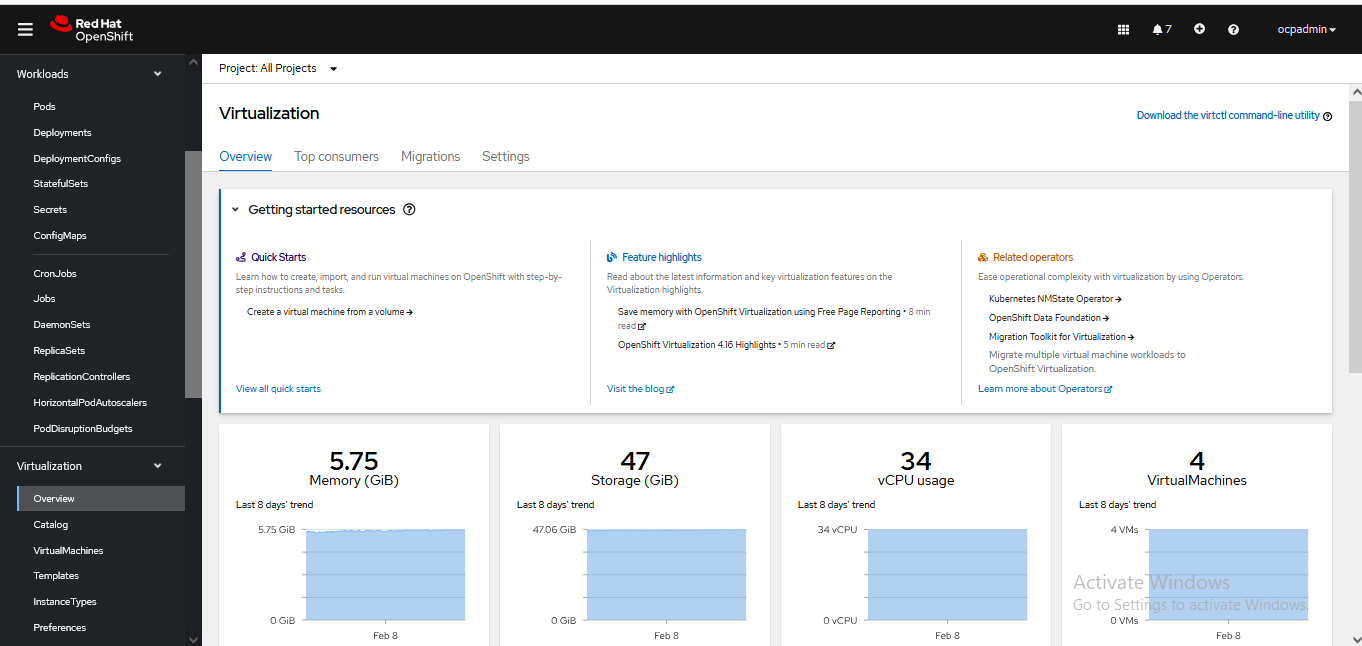
|  |
| --- |
| [prod@bastion monitoring]$ oc get po -o wide -n openshift-monitoring  NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES  alertmanager-main-0 6/6 Running 0 11d 10.128.2.71 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  alertmanager-main-1 6/6 Running 0 11d 10.129.2.139 vlocpsrvw3.valpocp.vedantaconnect.com <none> <none>  cluster-monitoring-operator-78dd644bb4-fktl7 1/1 Running 0 12d 10.129.0.41 vlocpsrvm1.valpocp.vedantaconnect.com <none> <none>  kube-state-metrics-84774f484d-tln9w 3/3 Running 0 12d 10.131.0.15 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  metrics-server-c5964b548-2rtvf 1/1 Running 0 12d 10.128.2.9 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  metrics-server-c5964b548-qkfjb 1/1 Running 0 12d 10.131.0.9 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  monitoring-plugin-6948ddf4b7-gw5t5 1/1 Running 0 12d 10.128.2.7 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  monitoring-plugin-6948ddf4b7-sv2w2 1/1 Running 0 12d 10.131.0.6 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  node-exporter-7gzp9 2/2 Running 8 13d 10.101.143.14 vlocpsrvm1.valpocp.vedantaconnect.com <none> <none>  node-exporter-bvzwk 2/2 Running 6 13d 10.101.143.17 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  node-exporter-jl5gl 2/2 Running 8 13d 10.101.143.16 vlocpsrvm3.valpocp.vedantaconnect.com <none> <none>  node-exporter-l75nt 2/2 Running 8 13d 10.101.143.15 vlocpsrvm2.valpocp.vedantaconnect.com <none> <none>  node-exporter-ntnsr 2/2 Running 6 13d 10.101.143.18 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  node-exporter-w8mrz 2/2 Running 6 13d 10.101.143.19 vlocpsrvw3.valpocp.vedantaconnect.com <none> <none>  openshift-state-metrics-b9456474c-jrr7w 3/3 Running 0 12d 10.131.0.16 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  prometheus-k8s-0 6/6 Running 0 11d 10.129.2.138 vlocpsrvw3.valpocp.vedantaconnect.com <none> <none>  prometheus-k8s-1 6/6 Running 0 11d 10.131.0.124 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  prometheus-operator-8474d68cb5-ph79p 2/2 Running 0 12d 10.128.0.22 vlocpsrvm3.valpocp.vedantaconnect.com <none> <none>  prometheus-operator-admission-webhook-6dcb6767db-j5xzp 1/1 Running 0 12d 10.131.0.10 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  prometheus-operator-admission-webhook-6dcb6767db-xb2kh 1/1 Running 0 12d 10.128.2.12 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  telemeter-client-9999b78df-7dcjz 3/3 Running 0 12d 10.131.0.8 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none>  thanos-querier-6fd58d6469-lwntg 6/6 Running 0 12d 10.128.2.11 vlocpsrvw2.valpocp.vedantaconnect.com <none> <none>  thanos-querier-6fd58d6469-nxktl 6/6 Running 0 12d 10.131.0.11 vlocpsrvw1.valpocp.vedantaconnect.com <none> <none> |

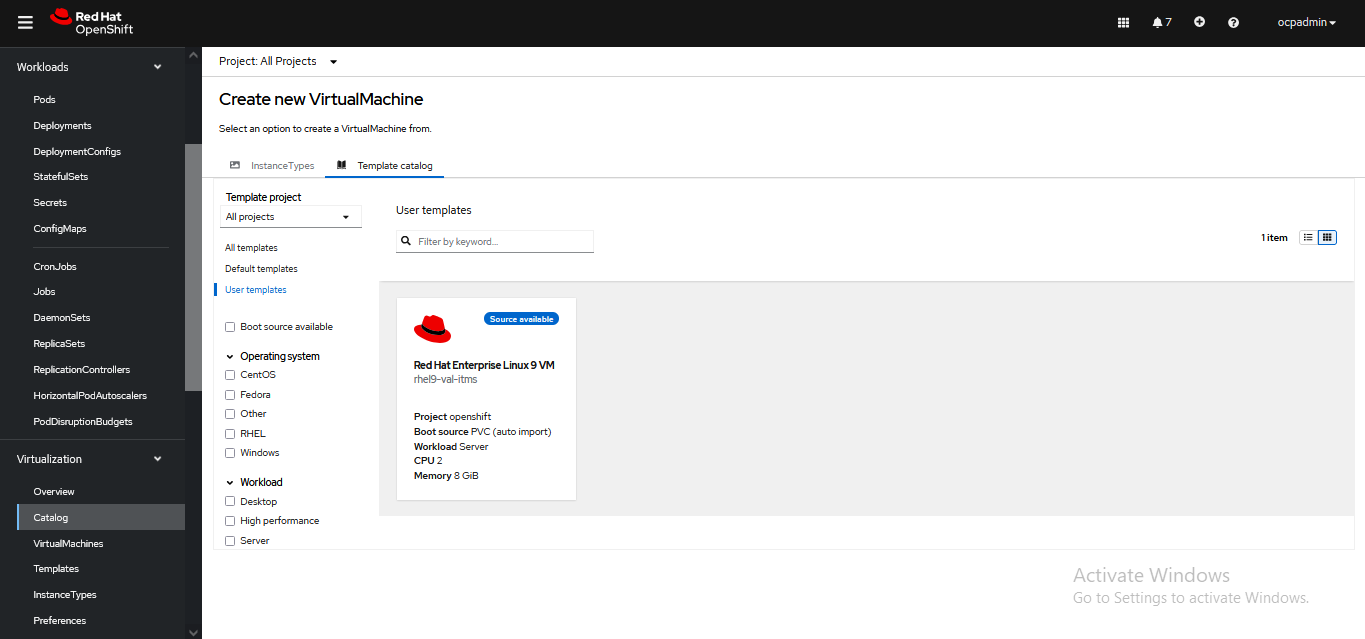
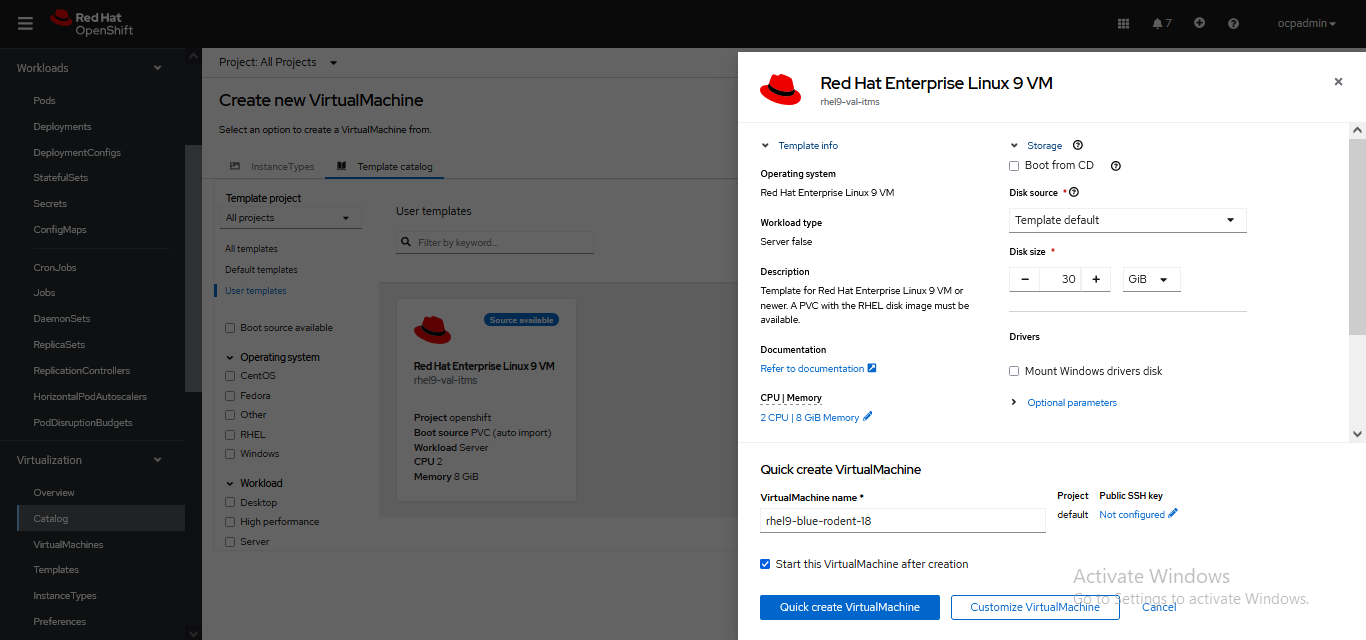
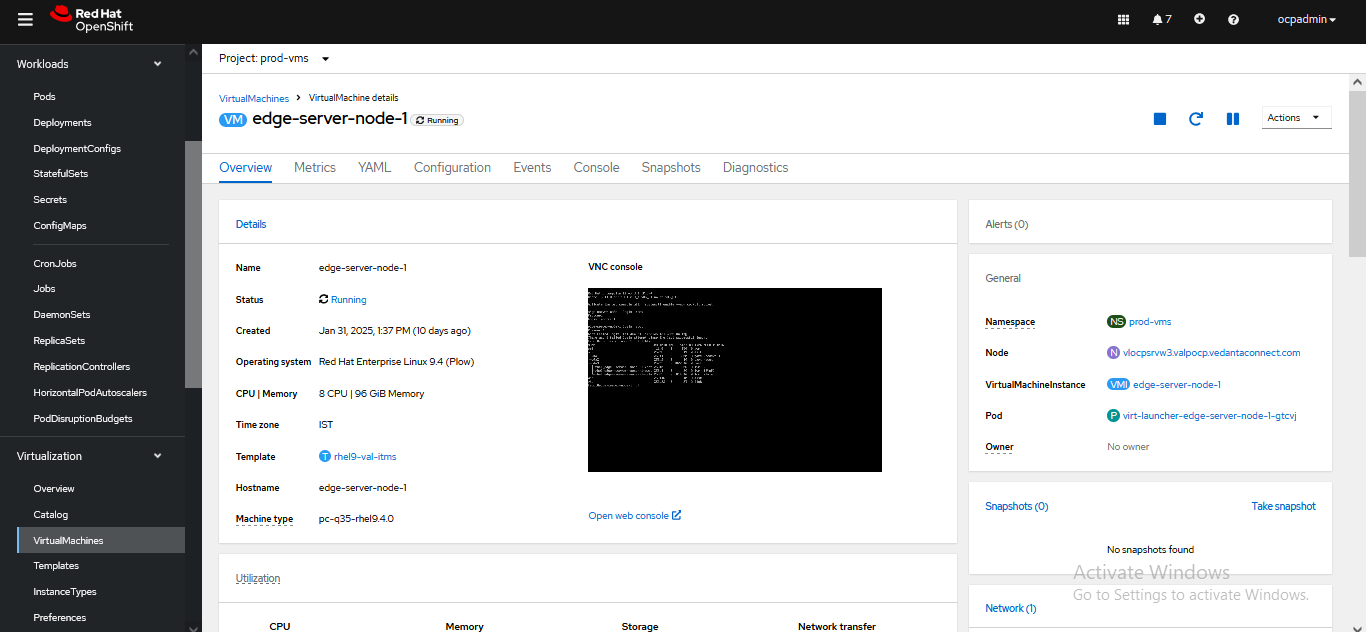
## Openshift Virtualization

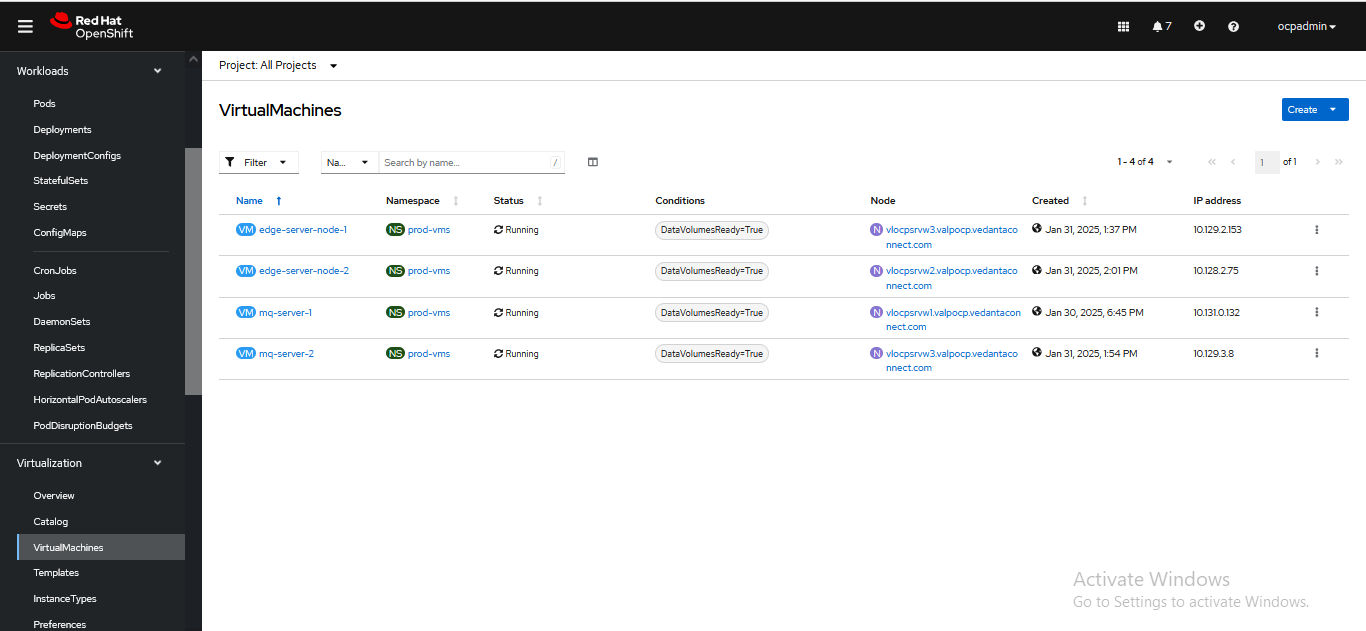










**Thank You**

1. Visit us at www.integramicro.com