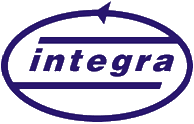
**Configuration Review Document**

**Red Hat OpenShift Container Platform 4.16**

**V 1.1**

**Client: Tata Consultancy Services**

****



**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 herein 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**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Release Version | Release Date | Description of the Release | Created By | Approved By |
| 0.1 | 26-08-2024 | Cluster installation | Sai Akhil/Sowjanya/Kiran | Murali K Muddada |
| 0.2 | 30-08-2024 | Updated ELK Details | Sai Akhil/Sowjanya/Kiran | Murali K Muddada |
| 0.3 | 02-09-2024 | Updated Prometheus and Graphana Details | Sai Akhil/Sowjanya/Kiran | Murali K Muddada |
| 0.4 | 05-09-2024 |  | Sai Akhil/Sowjanya/Kiran | Murali K Muddada |
| 0.5 | 18-02-2024 | Updated Redhat Virtualization details updated |  |  |

**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 Executive Summary 5](#_Toc176798949)

[1.1 Objective 5](#_Toc176798950)

[1.2 A. OpenShift 4.16 PROD 5](#_Toc176798951)

[1.3 Environment 7](#_Toc176798952)

[2 Review of OCP cluster 8](#_Toc176798953)

[2.1 Node Resource Sizing 8](#_Toc176798954)

[2.2 Storage Sizing 9](#_Toc176798955)

[2.3 Registry conﬁguration 9](#_Toc176798956)

[2.4 Router conﬁguration 9](#_Toc176798957)

[2.5 Logging conﬁguration 11](#_Toc176798958)

[2.6 Monitoring conﬁguration 11](#_Toc176798959)

[2.7 PV Reclaim Policy 11](#_Toc176798960)

[2.8 Certiﬁcate for \*.apps 12](#_Toc176798961)

[2.9 SMTP integration 14](#_Toc176798962)

[2.10 NTP integration 14](#_Toc176798963)

[2.11 Log forwarding 14](#_Toc176798964)

[2.12 Deletion of Kubeadmin 15](#_Toc176798965)

[2.13 Cluster Registration & Subscription 15](#_Toc176798966)

[2.14 Resource Quota/Limit Ranges for Project 15](#_Toc176798967)

[2.15 Egress Conﬁguration 15](#_Toc176798968)

[2.16 ETCD Encryption 16](#_Toc176798969)

[2.17 ETCD Backups 16](#_Toc176798970)

[2.18 Mirror Registry services 16](#_Toc176798971)

[2.19 MCP State for Master/Workers 17](#_Toc176798972)

[2.20 Cluster/Node Health 17](#_Toc176798973)

[2.20.1 Operators Health 17](#_Toc176798974)

[2.21 Active Alerts 18](#_Toc176798975)

[2.22 Cluster Sample Operators 18](#_Toc176798976)

[2.23 Mirror registry certiﬁcate change 18](#_Toc176798977)

[3 Best Practices 19](#_Toc176798978)

# Executive Summary

This report is the outcome of the OpenShift conﬁguration review for the PROD cluster for TCS.

## Objective

1. Red Hat Consulting was engaged by the TCS to perform conﬁguration review, based on design documents, consulting engagement report and best practices.
2. Below are the recommendations for the observations that need further action.

## A. OpenShift 4.16 PROD

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Component** | **Observation** | **Recommendation** |
| 1 | Storage Sizing | The cluster's storage includes large Persistent Volumes (PVs) up to 2Ti, mostly bound to critical namespaces | Define PV/PVC as per HLD for monitoring components. |
| 2 | Registry configuration | Image registry is configured with NFS PV, with no node selector labels.  Also, no push/pull activity is performed on image registry as mount point doesn't have any repositories or blobs available. | Validate push/pull activity on image registry and required labels in configs.image registry CR. |
| 3 | Monitoring configuration | The monitoring stack is operational. |  |
| 4 | PV Reclaim Policy | CSI is defined with default reclaim policy of delete. |  |
| 6 | ETCD Encryption | ETCD/Api server encryption is configured. | [https://docs.openshift.com/container-platform/4.16](https://docs.openshift.com/container-platform/4.1)[/securi](https://docs.openshift.com/container-platform/4.12/security/encrypting-etcd.html) [ty/encrypting-etcd.html](https://docs.openshift.com/container-platform/4.12/security/encrypting-etcd.html) |
| 7 | ETCD Backups | ETCD backup is done and stored in bastion node. | <https://access.redhat.com/solutions/5843611> |
| 8 | SMTP  integration | SMTP is configured. | Configure alert manager and its integration with SMTP as per,  [https://docs.openshift.com/container-platform/4.16/monit](https://docs.openshift.com/container-platform/4.12/monitoring/managing-alerts.html) [oring/managing-alerts.html](https://docs.openshift.com/container-platform/4.12/monitoring/managing-alerts.html) |
| 9 | Deletion of Kubeadmin | A Kubeadmin account exists on the cluster. This should be removed post authentication (htpass wd/LDAP) is properly deﬁned. |  |
| 10 | Active Alerts | Active warning Alerts on cluster to be validated. | Validate all active alerts as defined on the OCP console. |
| 11 | Resource Quota | There is no resource quota or limit ranges set per project level. | As best practice it is recommended to have quota, limit ranges defined for the projects. |
| 12 | Log forwarding | Configured ELK inside OCP cluster. | Configure log forwarding as per documentation,  [https://docs.openshift.com/container-platform/4.16/loggin](https://docs.openshift.com/container-platform/4.12/logging/log_collection_forwarding/log-forwarding.html) [g/log\_collection\_forwarding/log-forwarding.html](https://docs.openshift.com/container-platform/4.12/logging/log_collection_forwarding/log-forwarding.html) |
| 14 | Ingress Configuration | As per HLD, Self-signed certificates is configured. | Self-signed certificates on ingress along with proper labels to make them run on master nodes. |
| 15 | Node Sizing OCP | Sizing is as per HLD 3 masters and 3 Workers are deployed. |  |
| 16 | OCP Cluster Operators | Cluster operators are in a healthy state. |  |
| 17 | Users and Groups | Only htpasswd authentication is enabled, with only few users are created under htpasswd and no groups are defined. No LDAP/AD configuration is in place. | It is not recommended to give cluster access to every user.  It is a good practice to create groups, add users to the group and restrict access to the groups by proper permissions. |
| 18 | Volume Snapshots | Volume snapshot testing is done. | Best practice is to take relevant snapshots of the PVC configured for the applications. |
| 19 | Cluster Sample Operator | Cluster sample operator is in a running state. |  |
| 20 | Authentication | Only htpasswd auth mechanism is configured. |  |
| 21 | Cluster Registration | OCP prod cluster has been registered |  |
| 22 | Cluster Network | Configured as per HLD. | IP Range once defined can't be changed. |
|  | Redhat Virtualization | Configured and created VM’s as per the HLD |  |

* Result in Orange refers to the major observations that need to be addressed on priority.
* Result in Yellow refers to those observations that need to be addressed as 2nd priority.
* Result in Green refers to those observations that are in-line with design scope.

## Environment

|  |  |  |
| --- | --- | --- |
| **Product** | **Environment** | **Version** |
| OpenShift Container Platform | PROD | 4.16 |

# Review of OCP cluster

Each of the following sections provides a brief description and a list of recommended actions. Additional explanations are provided where additional clarity is required.

## Node Resource Sizing

Investigation: Is the resource sizing deployed as per the Design?

Observation: Node resource size for OCP cluster is as per design, however discrepancies w.r.t disk size for mirror registry.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No** | **Hostname** | **IP** | **CPU** | **Memory** |
| 1 | vlocpsrvm1.valpocp.vedantaconnect.com | 10.101.143.14 | 16 | 128 |
| 2 | vlocpsrvm2.valpocp.vedantaconnect.com | 10.101.143.15 | 16 | 128 |
| 3 | vlocpsrvm3.valpocp.vedantaconnect.com | 10.101.143.16 | 16 | 128 |
| 4 | vlocpsrvw1.valpocp.vedantaconnect.com | 10.101.143.17 | 24 | 256 |
| 5 | vlocpsrvw2.valpocp.vedantaconnect.com | 10.101.143.18 | 24 | 256 |
| 6 | vlocpsrvw3.valpocp.vedantaconnect.com | 10.101.143.19 | 24 | 256 |
| 7 | bastion.valpocp.vedantaconnect.com | 10.101.143.22 | 8 | 16 |

Assessment: OCP resource sizing is as per design. Cluster created with 3 master, 3 worker nodes. RHCOS OS installable for both master and worker.

vlocpsrvm1.valpocp.vedantaconnect.com

|  |
| --- |
| [core@vlocpsrvm1 ~]$ lsblk  NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  sda 8:0 0 447.1G 0 disk  ├─sda1 8:1 0 1M 0 part  ├─sda2 8:2 0 127M 0 part  ├─sda3 8:3 0 384M 0 part /boot  └─sda4 8:4 0 446.6G 0 part /var  /sysroot/ostree/deploy/rhcos/var  /usr  /etc  /  /sysroot |

vlocpsrvm2.valpocp.vedantaconnect.com

|  |
| --- |
| [core@vlocpsrvm2 ~]$ lsblk  NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  sda 8:0 0 447.1G 0 disk  ├─sda1 8:1 0 1M 0 part  ├─sda2 8:2 0 127M 0 part  ├─sda3 8:3 0 384M 0 part /boot  └─sda4 8:4 0 446.6G 0 part /var  /sysroot/ostree/deploy/rhcos/var  /usr  /etc  /  /sysroot |

vlocpsrvm3.valpocp.vedantaconnect.com

|  |
| --- |
| [core@vlocpsrvm3 ~]$ lsblk  NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  sda 8:0 0 447.1G 0 disk  ├─sda1 8:1 0 1M 0 part  ├─sda2 8:2 0 127M 0 part  ├─sda3 8:3 0 384M 0 part /boot  └─sda4 8:4 0 446.6G 0 part /var  /sysroot/ostree/deploy/rhcos/var  /usr  /etc  /  /sysroot |

vlocpsrvw1.valpocp.vedantaconnect.com

|  |
| --- |
| [core@vlocpsrvw1 ~]$ lsblk  NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  loop1 7:1 0 1T 0 loop  loop2 7:2 0 1T 0 loop  loop3 7:3 0 15G 0 loop  sda 8:0 0 446.1G 0 disk  ├─sda1 8:1 0 1M 0 part  ├─sda2 8:2 0 127M 0 part  ├─sda3 8:3 0 384M 0 part /boot  └─sda4 8:4 0 445.6G 0 part /var/lib/kubelet/pods/a2bd171b-7682-4891-b4c1-9eb803a77797/volume-subpaths/nginx-conf/nmstate-console-plugin/1  /var/lib/kubelet/pods/f4db53ba-fc30-42a1-8450-b3bcd7f41c31/volume-subpaths/nginx-conf/monitoring-plugin/1  /var  /sysroot/ostree/deploy/rhcos/var  /usr  /etc  /  /sysroot |

vlocpsrvw2.valpocp.vedantaconnect.com

|  |
| --- |
| ---  [core@vlocpsrvw2 ~]$ lsblk  NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  loop2 7:2 0 1T 0 loop  loop3 7:3 0 2T 0 loop  sda 8:0 0 446.1G 0 disk  ├─sda1 8:1 0 1M 0 part  ├─sda2 8:2 0 127M 0 part  ├─sda3 8:3 0 384M 0 part /boot  └─sda4 8:4 0 445.6G 0 part /var/lib/kubelet/pods/f7f26fb3-4bf4-4926-b93d-0e74b4672cdd/volume-subpaths/nginx-conf/kubevirt-console-plugin/1  /var/lib/kubelet/pods/0c4390d8-21f8-410d-994d-8bc1f4f25c05/volume-subpaths/nginx-conf/monitoring-plugin/1  /var  /sysroot/ostree/deploy/rhcos/var  /usr  /etc  /  /sysroot |

vlocpsrvm3.valpocp.vedantaconnect.com

|  |
| --- |
| Last login: Thu Jan 30 05:50:24 2025 from 10.101.143.22  [core@vlocpsrvw3 ~]$ lsblk  NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  loop0 7:0 0 2T 0 loop  loop1 7:1 0 15G 0 loop  sda 8:0 0 1.7T 0 disk  └─3600062b2167bed802f092dca0520fe77  253:0 0 1.7T 0 mpath  sdb 8:16 0 446.1G 0 disk  ├─sdb1 8:17 0 1M 0 part  ├─sdb2 8:18 0 127M 0 part  ├─sdb3 8:19 0 384M 0 part /boot  └─sdb4 8:20 0 445.6G 0 part /var/lib/kubelet/pods/42604f7e-0ab0-40d0-8b28-32e806eb8579/volume-subpaths/nginx-conf/kubevirt-console-plugin/1  /var  /sysroot/ostree/deploy/rhcos/var  /usr  /etc  /  /sysroot |

## Storage Sizing

Investigation: Is storage conﬁgured as per the Design?

Observation: All the external storage used for OCP clusters are not deﬁned.

PROD:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OCP Component** | **Access Type** | **Storage type** | **Size** | **Env** |
| Internal Registry | RWX | NFS | 500GB | Prod |
| Monitoring | RWO | Block | 400 GB(2 \* 200 GB) | Prod |
| Alert Manager | RWO | Block | 15 GB(2 \* 7.5GB) | Pord |

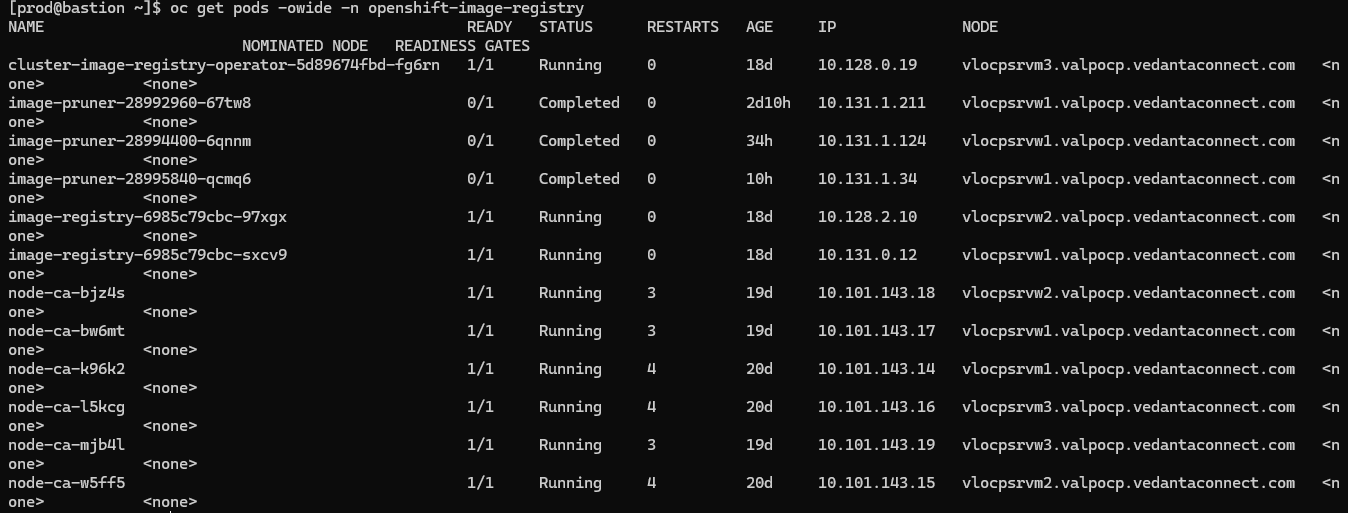
Assessment: OK.

## Registry conﬁguration

Investigation: Is the registry conﬁgured in HA and PV is conﬁgured?

Observation: PV size is deﬁned as per design and using NFS as storage option.

Note: Red Hat recommends using the Object storage for registry backend.

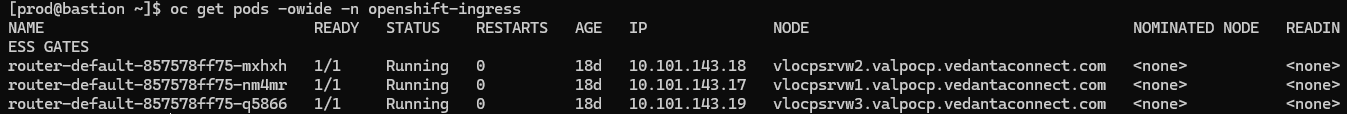


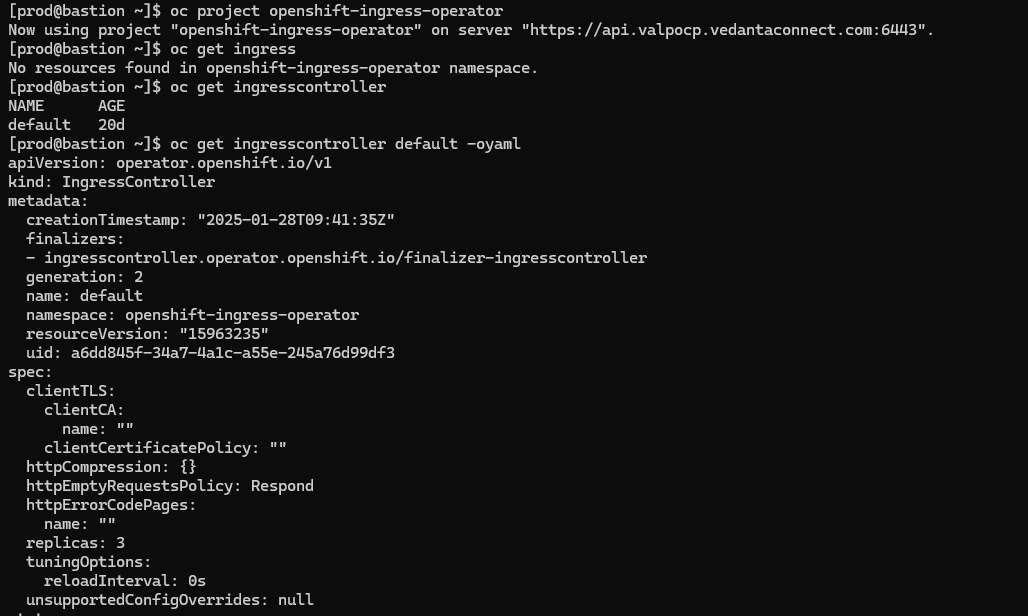
Assessment:Registry conﬁguration lacks image push/pull validation.

## Router conﬁguration

Investigation: Are all the router pods (Default) conﬁgured for HA?

Observation: Router pods are scaled across 3 worker nodes to ensure HA capability.



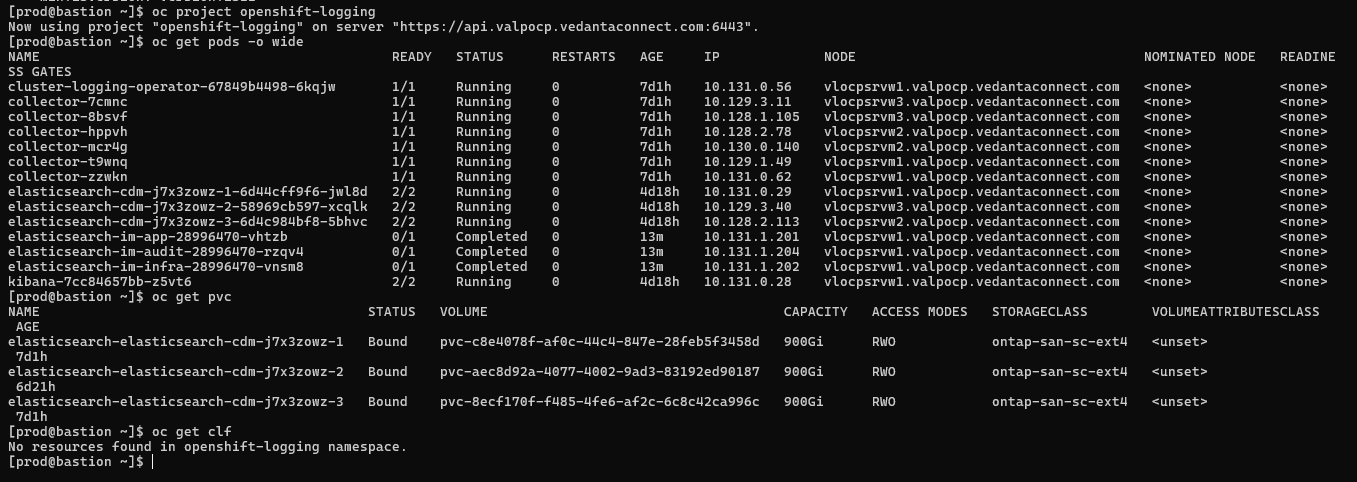


Assessment: Router pods are scaled across the 3 worker nodes to ensure HA. The IngressController is configured with replicas, ensuring that both router pods are available and functioning properly.

## Logging conﬁguration

Investigation:- Is the logging stack (EFK) conﬁgured with appropriate resources including the PV & HA for Elasticsearch pods? Is the retention period set accordingly for logging data as per HLD?

Observation: The logging stack's Elasticsearch pods are distributed across 3 worker nodes, each configured with Persistent Volumes (PVs) of 900Gi capacity. The cluster-logging operator is running as expected.

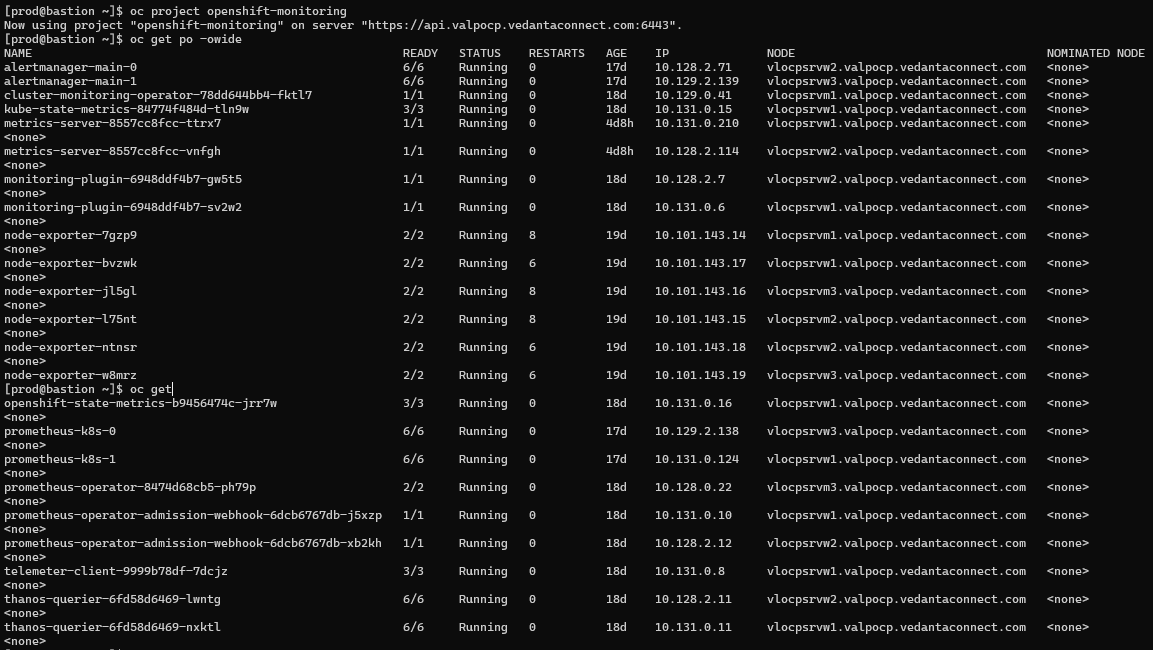
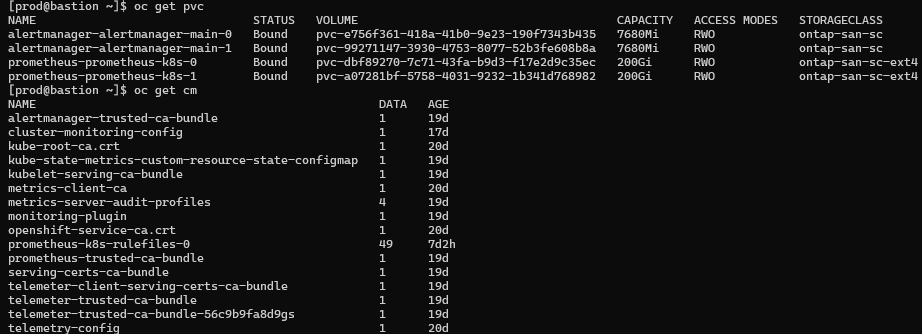


Assessment: The Elasticsearch pods are correctly distributed across 3 worker nodes with bound PVs, which supports HA and ensures data persistence. The absence of ClusterLogForwarder resources may indicate that log forwarding is not configured, which could affect log management according to HLD specifications. Addressing the image pull issues and verifying log forwarding setup is crucial to maintaining the integrity and functionality of the logging stack.

## Monitoring conﬁguration

Investigation:-Is the monitoring stack (Prometheus, Alertmanager) conﬁgured with appropriate resources including the PVs for Prometheus & Alertmanager pods? Is the retention period set accordingly for Prometheus data as per HLD?

Observation: The Prometheus and Alertmanager pods are currently running. Persistent Volume Claims (PVCs) are present in the openshift-monitoring namespace, indicating that the pods may using persistent storage. However, the necessary ConfigMaps for the monitoring stack are configured correctly.

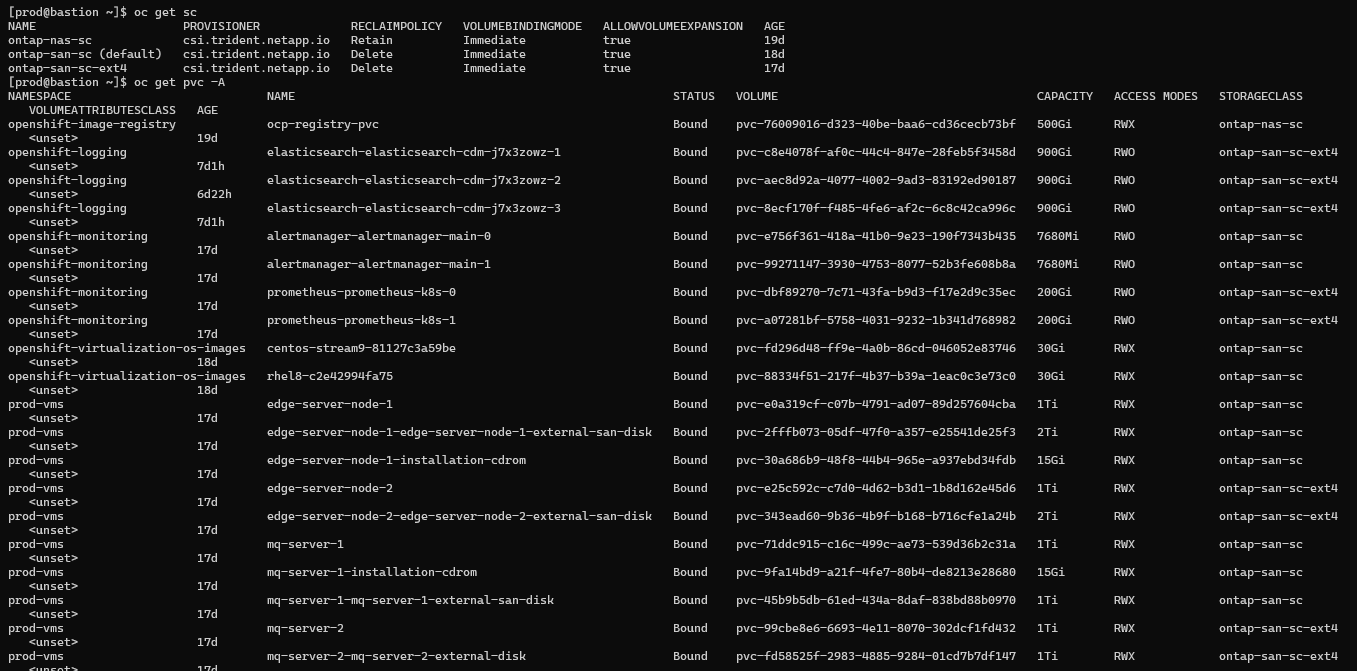
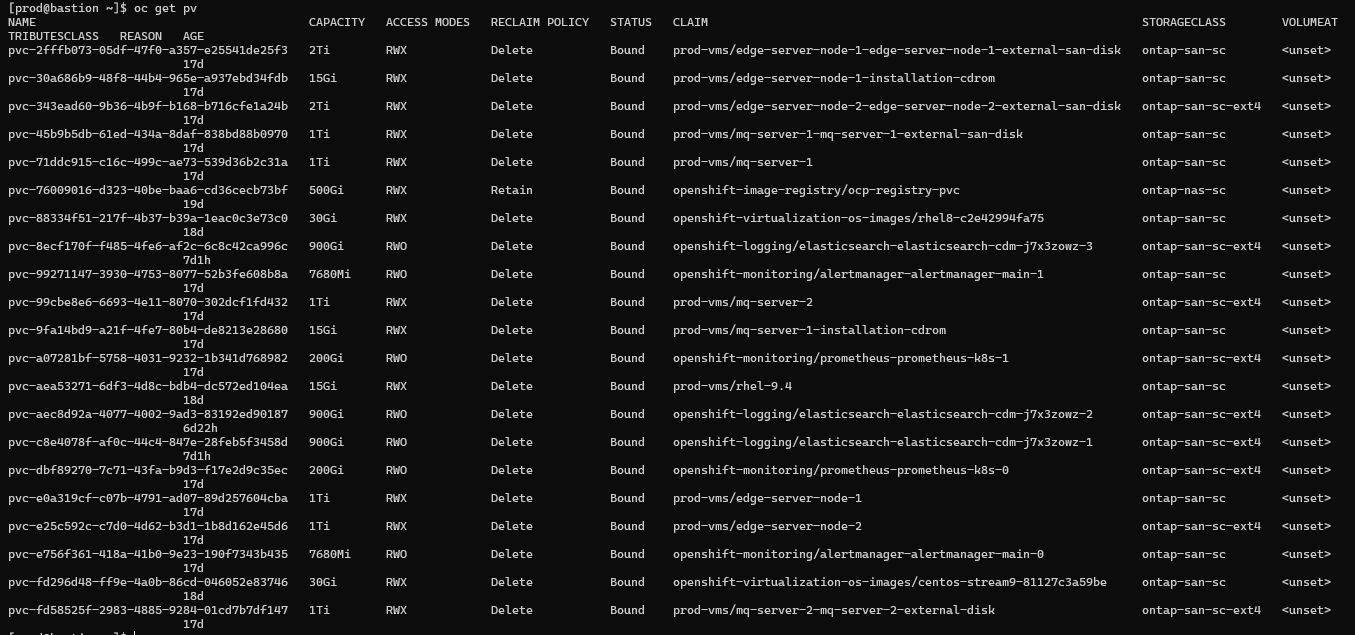
 

Assessment: The monitoring stack is operational.

## PV Reclaim Policy

Investigation: Is Reclaim Policy set to “Retain” for all the PVs on the cluster as the default would be “Delete”?

Observation: Storage Class are conﬁgured with delete (default) as reclaim policy.

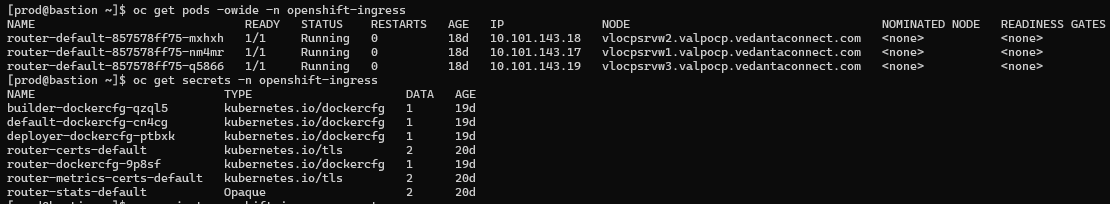
Assessment: As a best practice, conﬁgure the [reclaim](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.12/html-single/storage/index" \l "reclaiming_understanding-persistent-storage) policy for infrastructure components or for application microservice as Retain. Below is the list

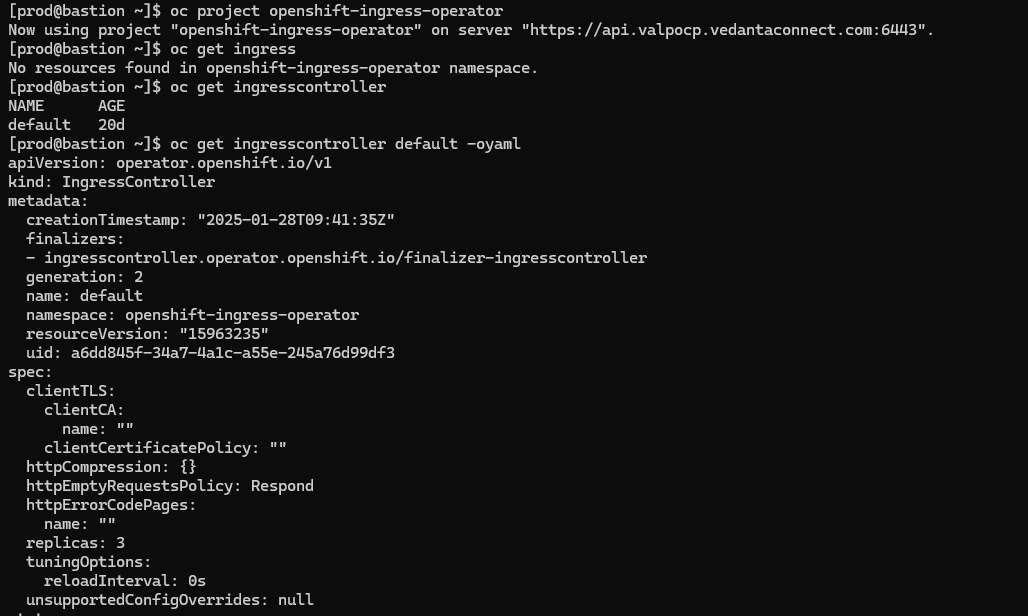
* + 1. Registry
    2. Monitoring
    3. Application(As per Requirement)

## Certiﬁcate for \*.apps

Investigation: Is the Ingress using self-signed or custom CA cert?

Observation: Self signed is assigned as per the HLD for ingress



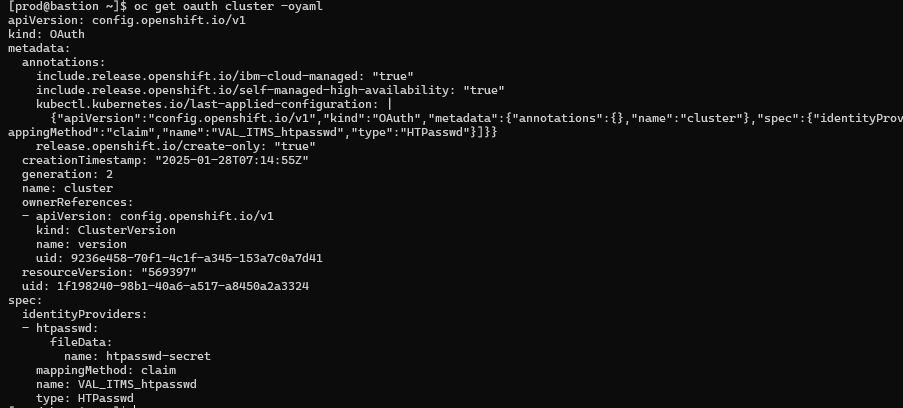


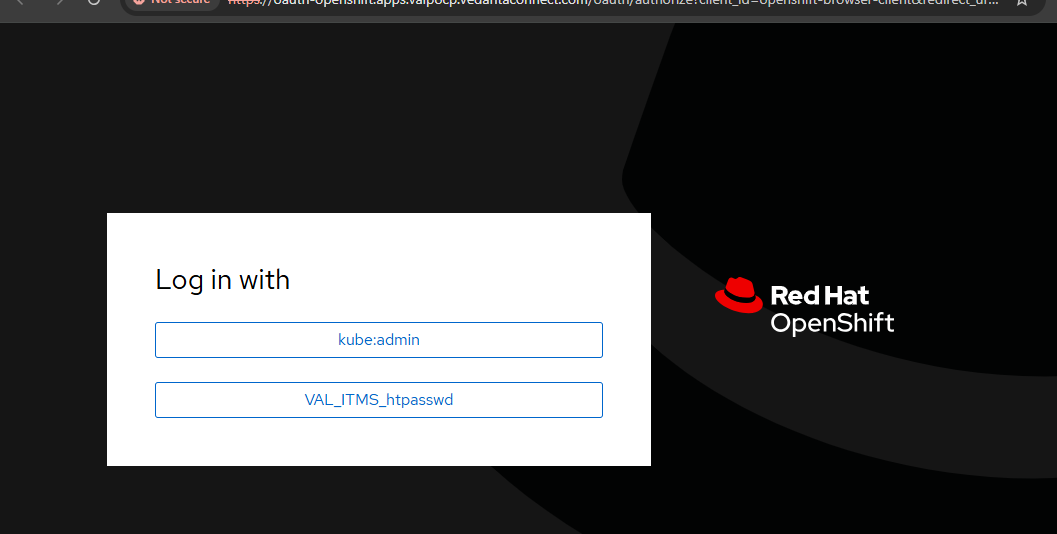
Assessment: Router is using self-signed certificates.

## LDAP integration.

Investigation: Is the cluster integrated with the htpasswd/LDAP server?

Observation: Cluster is integrated with htpasswd but not with LDAP/AD.





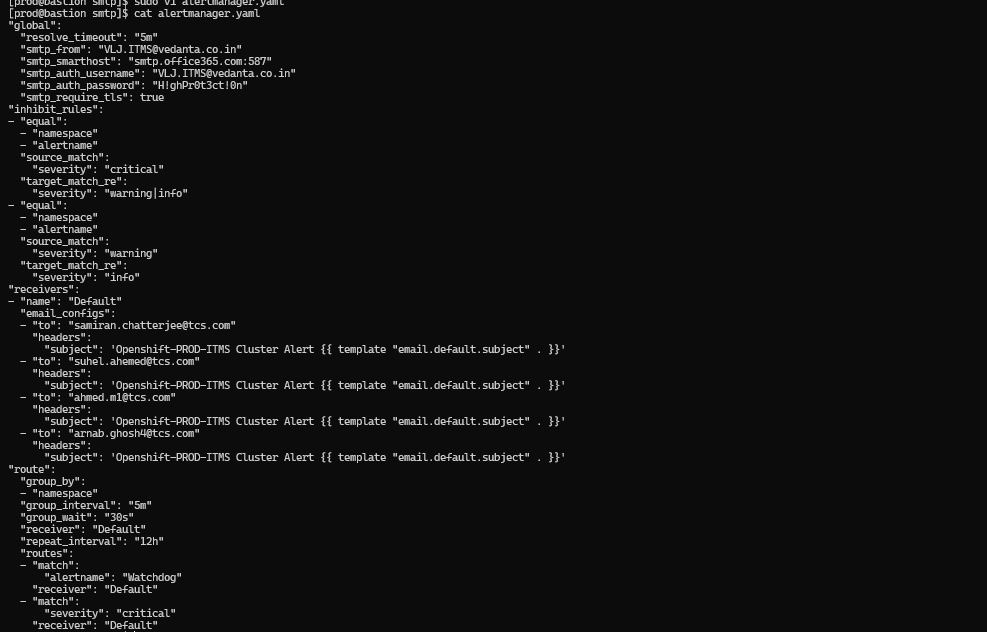


Assessment: Kubeadmin user to be disabled.

## SMTP integration

Investigation: Is the cluster integrated with the SMTP server & able to notify alerts via emails?

Observation: SMTP is conﬁgured.

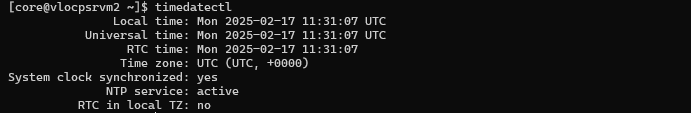


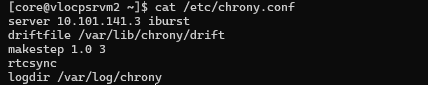
Assessment: Ok.

## NTP integration

Investigation: Is the cluster integrated with the NTP server & able to sync the time with the centralized time server?

Observation: Yes, all the cluster nodes have been integrated with the NTP server and they are able to sync the time.



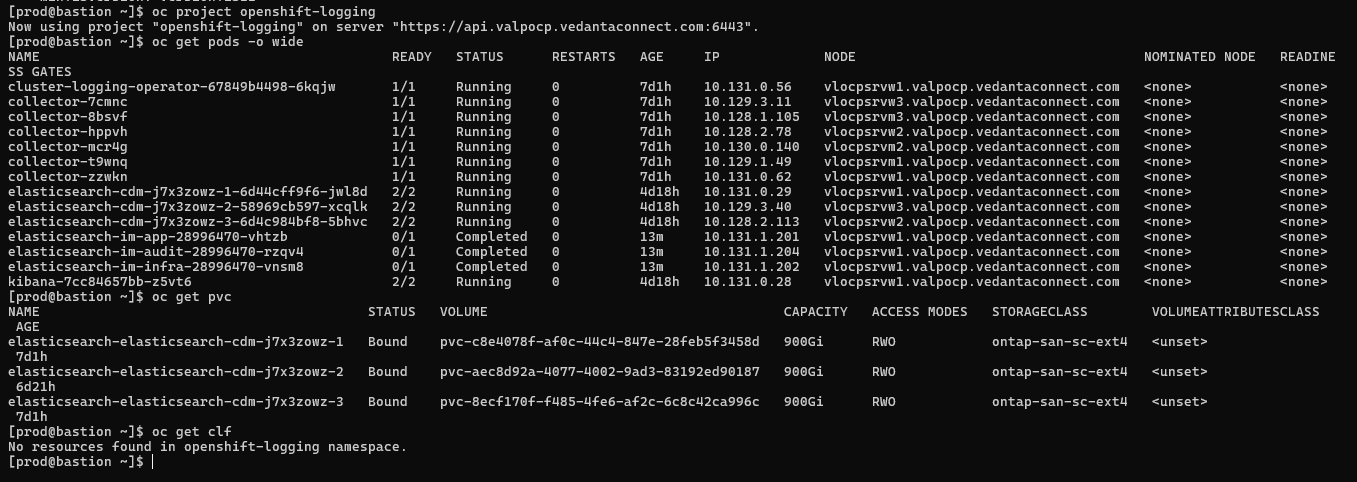


Assessment: OCP cluster has been intrgrated with NTP server.

## Log forwarding

Investigation: Is log forwarding conﬁgured to send the logs to the log server?

Observation: Configured ELK inside the cluster.

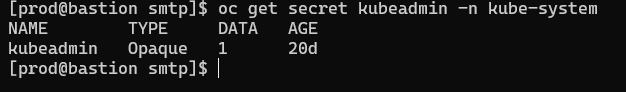


Assessment: Configured ELK inside the cluster.

## Deletion of Kubeadmin

Investigation: Is the Kubeadmin account removed from the cluster?

Observation: No, the Kubeadmin account exists on the cluster.

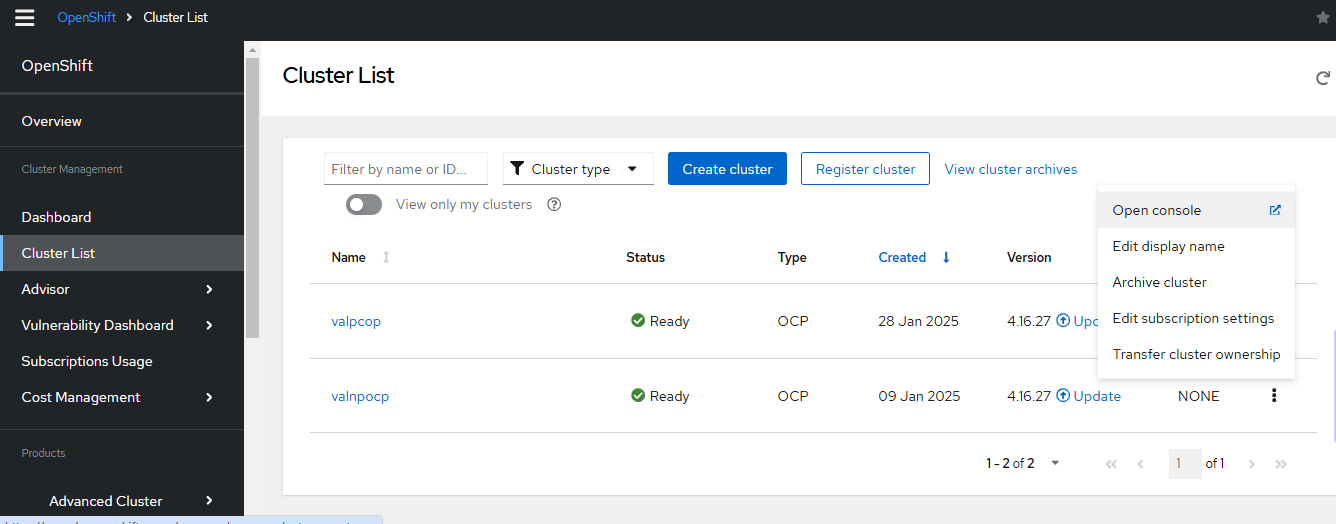


Assessment: As a best practice, it is recommended to delete the Kubeadmin user.

## Cluster Registration & Subscription

Investigation: Is the cluster registered & subscribed?

Observation: OCP prod cluster has been registered.

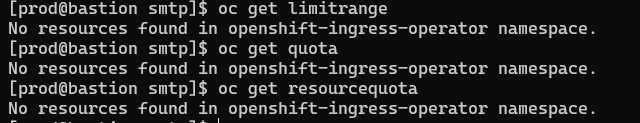


Assessment: OK

## Resource Quota/Limit Ranges for Project

Investigation: Is the cluster conﬁgured with project-level resource quota or limit-ranges?

Observation: Quota/Ranges have not been conﬁgured for projects.

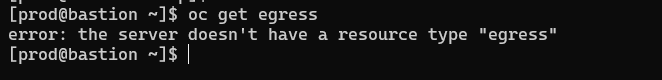


Assessment: No Resource Quota/Ranges has been conﬁgured.

## Egress Conﬁguration

Investigation: Is the node assigned egress IP and namespace labeled to use the same?

Observation: No egress deﬁnition deﬁned.

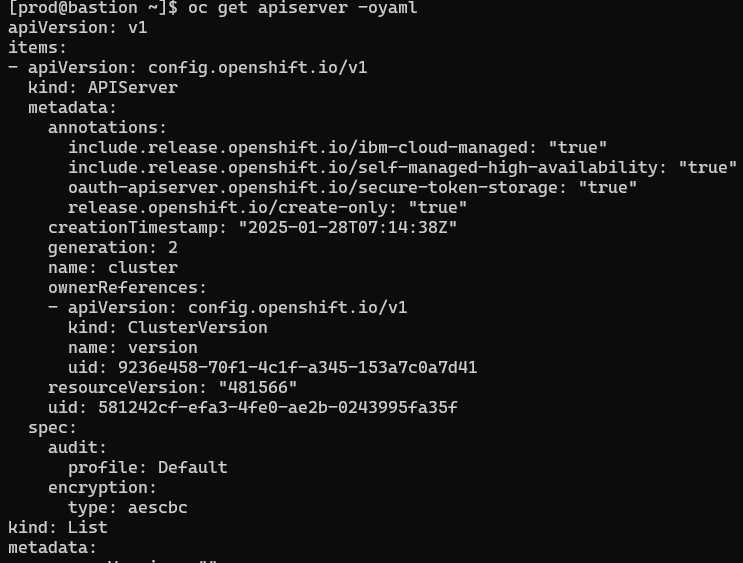


Assessment:As per the HLD egress is not required.

## ETCD Encryption

Investigation: Is the cluster conﬁgured with etcd encryption?

Observation: ETCD is encrypted.

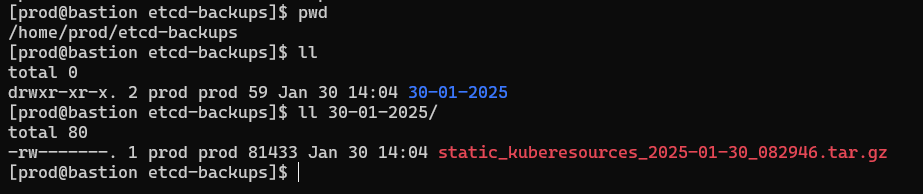


Assessment: ETCD is encrypted.

## ETCD Backups

Investigation: Is ETCD backups being performed & the backed-up ﬁles are stored outside the cluster?

Observation: ETCD backup is taken and backup files are stored in bastion node.

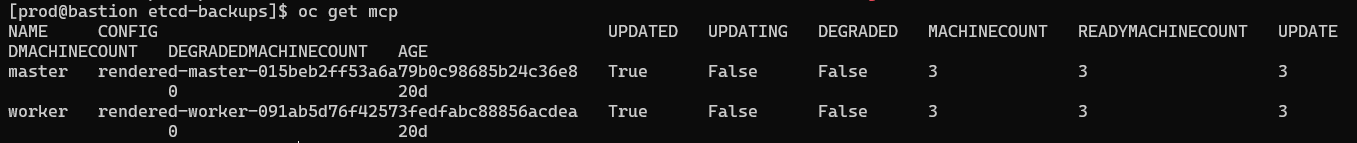


Assessment: OK

## MCP State for Master/Workers

Investigation: Is the cluster MCP conﬁgured and updated?

Observation: MCP for both workers and masters look ok.

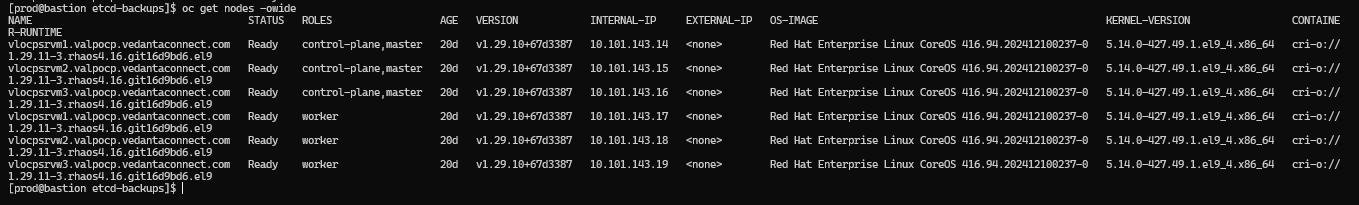


Assessment: MCP for worker/master looks ok.

## Cluster/Node Health

Investigation: Are all the OCP nodes in Readystate?

Observation: Node status is in ready state.

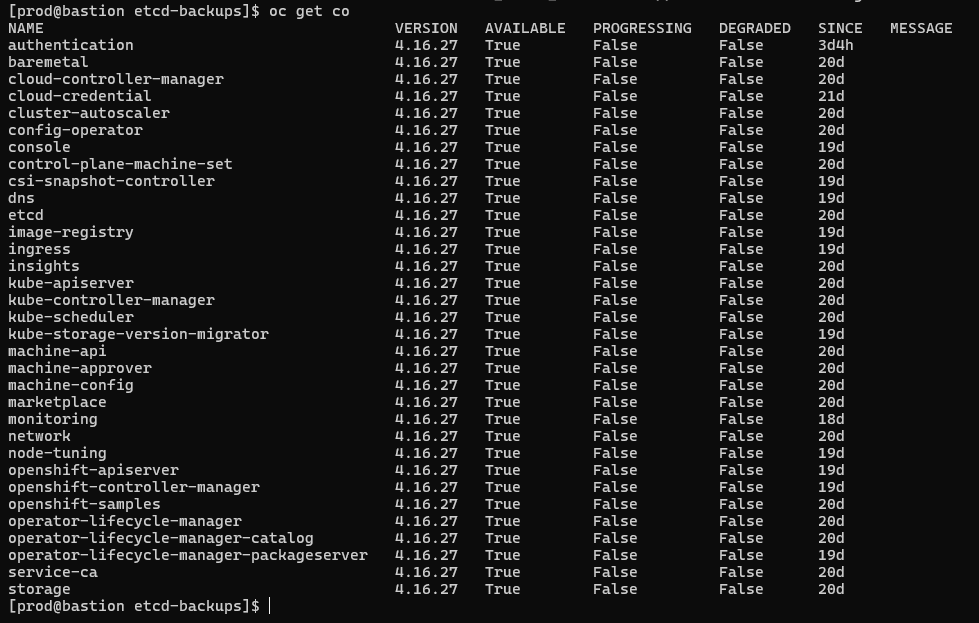


Assessment: All nodes are in Ready state.

### Operators Health

Investigation: Are all cluster operators in “Available” state?

Observation: Below are the cluster operators and its version



Assessment: Cluster Operators are in Healthy State.

## Active Alerts

Investigation: Are there any active alerts generated?

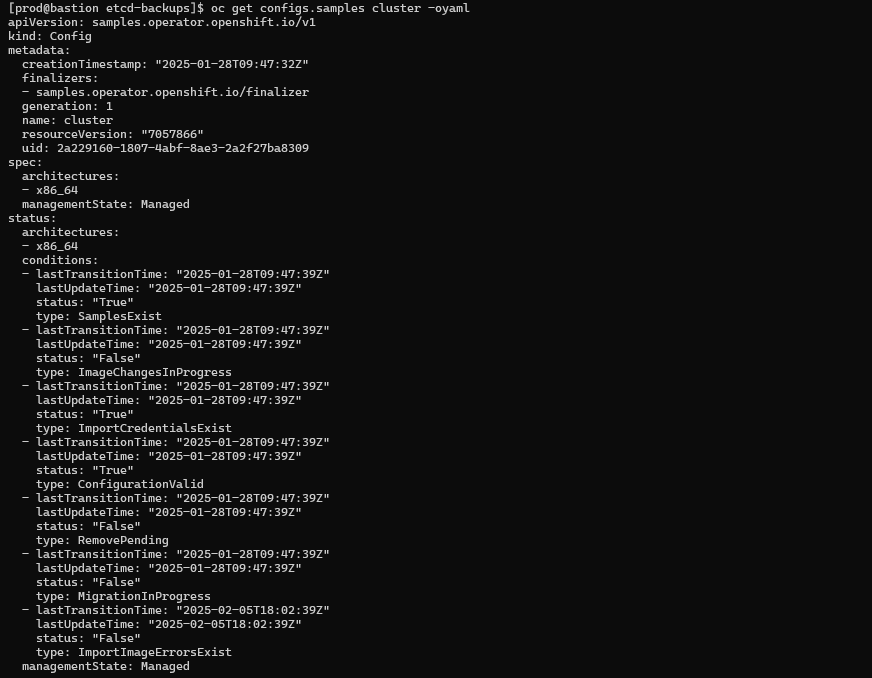
Observation: Observed platform alerts being ﬁred, needs validation.

Assessment: All the active Warning alerts need to be investigated further.

## Cluster Sample Operators

Investigation: Is cluster sample operator enabled?

Observation: cluster sample operator in Managed state.



Assessment: Ok, Cluster sample operator is enabled.

## Virtualization operator

Investigation: Is Virtualization operator enabled?

Observation: virtualization operator installed and configured, also VM’s are created as per the HLD

# Best Practices

1. Always set Project level limits.
2. Conﬁgure pod disruption budget5.
3. Structured LDAP groups sync with OCP roles. Already created user groups which are stored in an LDAP server. OpenShift can sync those LDAP records with internal OpenShift Container Platform records, enabling you to manage your groups in one place.
4. ETCD Best Practices6 should be followed for better performance.
5. As best practice, applications should be conﬁgured with required liveness/readiness probes.
6. Application YAMLs should be deﬁned to request/limit memory and CPU for better utilization.
7. Starting with OCP 4.11 onwards the conﬁguration in CRI-O is deprecated in favor of the conﬁguration in the KubeletConﬁg, and the default podPidsLimit changed to 4096. Increase this based on performance run. Follow [link](https://access.redhat.com/solutions/5366631) for reference.
8. Based on the application's requirement to use storage, the below document can be taken into consideration before deployment.

<https://access.redhat.com/solutions/6221251>

For more on SCCs refer,

<https://connect.redhat.com/en/blog/important-openshift-changes-pod-security-standards> [https://docs.openshift.com/container-platform/4.16/authentication/managing-security-context-constraints.html](https://docs.openshift.com/container-platform/4.12/authentication/managing-security-context-constraints.html)

**Thank You**

Visit us at www.integramicro.com