**MOC Openshift Migration from Version 3.x to 4.x**

* OpenShift Container Platform 4 introduces architectural changes and enhancements,
* With OpenShift Container Platform 3, administrators individually deployed Red Hat Enterprise Linux (RHEL) hosts, and then installed OpenShift Container Platform on top of these hosts to form a cluster.
* OpenShift Container Platform 4 includes new technologies and functionality, such as Operators, MachineSets, and Red Hat Enterprise Linux CoreOS (RHCOS), which are core to the operation of the cluster. This technology shift enables clusters to self-manage some functions previously performed by administrators.

## **The migration process from OpenShift 3 to 4 can be completed in 5 steps:**

1. Spin up a new cluster running OpenShift 4.
2. Configure the new OpenShift 4 cluster.
3. Create a migration plan which includes how to handle data from the applications that are being migrated.
4. Run migration plan.
5. Move your DNS or Load-balancer configuration to your new cluster.

## **Tools for Automated Migration**

### **Control Plane Migration Assistance Tool**

The Control Plane Migration Assistance tool helps you configure the new cluster OCP4 cluster that will be the destination for the applications that are being migrated from your existing OCP 3 cluster. This tool reduces the possibility for human error in the configuration process, matching when possible the existing settings in the source cluster. It also allows you to review the resources that will be applied to the new cluster.

### **Cluster Application Migration Tool (CAM)**

The Cluster Application Migration tool (CAM) migrates stateful and stateless applications from the source cluster on OCP 3 to a destination cluster running the latest OpenShift. It also can migrate applications between OCP 4 clusters. It is installed on your destination cluster via an Operator. Through the rich user interface take advantage of the simplified, customizable workflows. Decide which applications to start with and which migration approach best fits each application and your needs.

## **Features of Openshift 4.3**

**Encryption to strengthen the security of containerized applications on OpenShift**

* The latest release of Red Hat OpenShift brings stronger platform security that better meets the needs of enterprises and government organizations handling extremely sensitive data and workloads with FIPS (Federal Information Processing Standard) compliant encryption (FIPS 140-2 Level 1). FIPS validated cryptography is mandatory for US federal departments that encrypt sensitive data
* OpenShift 4.3 brings support for encryption of etcd, which provides additional protection for secrets at rest. Customers will have the option to encrypt sensitive data stored in etcd, providing better defense against malicious parties attempting to gain access to data such as secrets and config maps stored in ectd

### **Better access controls to comply with company security practices**

* Customers can deploy OpenShift clusters to customer-managed, pre-existing VPN / VPC (Virtual Private Network / Virtual Private Cloud) and subnets on AWS, Microsoft Azure and Google Cloud Platform
* With “bring your own” VPN / VPC, as well as with support for disconnected installs, users can have more granular control of their OpenShift installations and take advantage of common best practices for security used within their organizations
* OpenShift admins have access to a new configuration API that allows them to select the cipher suites that are used by the Ingress controller, API server and OAuth Operator for Transport Layer Security (TLS)

### 

### **OpenShift Container Storage 4 across the cloud**

* Enhanced with multi cloud gateway technology from Red Hat’s acquisition of NooBaa, OpenShift Container Storage 4 offers greater abstraction and flexibility. Customers can choose data services across multiple public clouds, while operating from a unified Kubernetes-based control plane for applications and storage
* enhanced built-in data protection features, such as encryption, anonymization, key separation and erasure coding
* deployed and managed by Operators, bringing automated lifecycle management to the storage layer, and helping with easier day 2 management.

### **Automation to enhance day two operations with OpenShift**

* automated health checking and remediation
* ability to register a private Operator catalog within OperatorHub. Customers with air-gapped installs can find this especially useful in order to take advantage of Operators for highly-secure or sensitive environments.
* Kubernetes cluster administrators can monitor known container image vulnerabilities in pods running on their Kubernetes cluster. If the container registry supports image scanning, such as Quay with Clair, then the Operator will expose any vulnerabilities found via the Kubernetes API
* Other notable features in OpenShift 4.3 include application monitoring with Prometheus (TP), forwarding logs off cluster based on log type (TP), Multus enhancements (IPAM), SR-IOV (GA), Node Topology Manager (TP), re-size of Persistent Volumes with CSI (TP), iSCSI raw block (GA) and new extensions and customizations for the OpenShift Console.

Openshift Platform 3 vs Platform 4

Architecture differences

Openshift 4

* OpenShift Container Platform 4 uses Red Hat Enterprise Linux CoreOS (RHCOS), which is designed to run containerized applications, and provides efficient installation, Operator-based management, and simplified upgrades.
* RHCOS enables OpenShift Container Platform 4 to manage and automate the deployment of the underlying container host.
* In OpenShift Container Platform 4.2, you use the OpenShift installation program to create a minimum set of resources required for a cluster. Once the cluster is running, you use Operators to further configure your cluster and to install new services. After first boot, Red Hat Enterprise Linux CoreOS (RHCOS) systems are managed by the Machine Config Operator (MCO) that runs in the OpenShift Container Platform cluster.
* With OpenShift Container Platform 3, administrators individually deployed Red Hat Enterprise Linux (RHEL) hosts, and then installed OpenShift Container Platform on top of these hosts to form a cluster.
* Administrators were responsible for properly configuring these hosts and performing updates.
* To install OpenShift Container Platform 3.11, you prepared your Red Hat Enterprise Linux (RHEL) hosts, set all of the configuration values your cluster needed, and then ran an Ansible playbook to install and set up your cluster.