Red Hat Certified OpenShift Administrator

Content

1. Cluster Management

- Use the web console and command-line interface (CLI) for cluster management.
- Query, format, and filter Kubernetes resource attributes.
- Import, export, and configure Kubernetes resources.
- Locate and examine container images.
- Create and delete projects.
- Examine resources, cluster status, and logs.
- Monitor cluster events and alerts.
- Assess cluster health and troubleshoot common issues.

2. Application Deployment

- Deploy applications using resource manifests.
- Use Kustomize overlays for configuration modifications.
- Deploy from images, OpenShift templates, and Helm charts.
- Manage jobs for one-time tasks.
- Work with replica sets and labels/selectors.
- Expose applications for external access (HTTP and non-HTTP).
- Utilize operators like MetalLB and Multus.

3. Storage Management

- Create and manage secrets and configuration maps.
- Provision Persistent Storage volumes (block and file-based).
- Use storage classes and manage non-shared storage with StatefulSets.

4. Application Reliability

- Configure health probes for applications.
- Reserve and limit compute capacity.
- Scale applications to handle increased demand.

5. Application Updates

- Identify images using tags and digests.
- Roll back failed deployments.
- Manage image streams and use triggers for image management.

6. Authentication and Authorization

- Configure HTPasswd identity provider.
- Create/delete users and modify passwords.
- Manage groups and permissions.

7. Network Security

- Configure networking components and troubleshoot software-defined networking.
- Create and edit external routes and control network ingress.
- Secure traffic using TLS certificates and configure application network policies.

8. Developer Self-Service

- Configure cluster and project resource quotas.
- Set project resource requirements and limit ranges.
- Configure project templates.

9. Operator Management

- Install and delete operators as needed.

10. Application Security

- Manage service accounts and apply permissions using security context constraints.
- Create and apply secrets for sensitive information.
- Configure application access to Kubernetes APIs and CronJobs.