Questions Outline:

- Install RHACM
- Import Managed cluster
- Permission Management
- Policy Management
- Deploy Application
- Update app using Kustomize
- Install RHACS
- Import Cluster into RHACS
- Monitor a vulnerable image
- Vulnerability Management

Quest1: Install RHACM

- Install the RHACM operator
- Use update channel as release-2.4
- Use a project as open-cluster-management
- Approval Method Manual
- Crea a multiclusterhub object
- Access the RHACM as below link

https://multicloud-console.apps.ocp4.example.com/

Question 2: Import Managed Cluster

- Import managed cluster ocp4-mng.example.com cluster through RHACM
- Identify cluster as
- name: managed-cluster
- Imported cluster should be in Ready state

Question 3: Permission Management

- Create a cluster set as production and add a cluster name as local-cluster
- Create a cluster set as stage and ad cluster name as managed-cluster

- Provide admin role to prod-admin user to production cluster set
- Provide view role to developer user to production cluster set
- Provide admin role to stage-admin user to state cluster set

Question 4: Policy management

- Create a policy to ensure that stage name space does not exist in production environment
- Use the below spec for policy configuration
- Name: policy-project
- namespace: policy-reference
- cluster selector environment: production
- Remediation: enforce

- Create a policy to restrict containers created in user project to value as specified below
- Name: policy-restrict
- namespace: policy-limit
- cluster selector environment: stage
- limit range name: project-limit
- Memory:
- default request: 128Mi
- Default limit: 512 Mi
- Project to exclude default, all Kubernetes and OpenShift infra projects.

Question 5: Deploy Application

- Create a new MySQL application using the following specification
- Name: MySQL
- namespace: MySQL
- repository type: Git
- URL: https://github.com/yourforknames/do480-apps
- Branch: Main
- path: MySQL
- Deploy the application to stage cluster

- Active Window: Friday 5:30AM and 5:30PM (US eastern Time)
- Note: (Not for Exam) for this for practice

https://github.com/redhattraining/DO480-apps/

Questions 6: Update app using kustomize

- Configure and deploy MySQL Application Using RHAM gitops
- Add the env=prod labels to local cluster
- Use main-kustomize for initial base content
- Create a new prod-kustomize branch
- Use the kustomize to build and test the base
- Add kustomization.yaml file to call base application resources
- The base directory contents are located at

http://github.com/yor-fork/do480-apps (branch prod-Kustomize)

- Create Overlays directory for production
- overlay need to have kustomize route (route will be given in exam)
- Build an overlay in production cluster that uses the namePrefix
- transformer to set prod- as the name prefix
- Deploy the application in production cluster
- Windows should be always active
- Once application deployed its should be accessible via link below

http://prod-todo.apps.ocp4.example.com/todo/

Question 7: Install RHACS

- Install and configure RHACS using Operator
- Use the latest channel for subscription
- Install operator in namespace rhacs-operator
- Activate the central service
- Access the RHACS using following URL
- https://central-stackrox.apps.ocp4.example.com
- Create and test and integration of RHACs syslog
- Integration name: remotelog

- logging facility: local0

- Receive host: workstation.lab.example.com
- Receive port 514
- Test the connection to verify that works.

Question: 8 Import a managed cluster to RHACS

- Import The cluster:
- name: Managed-cluster
- Secured cluster instance should be active
- Imported cluster should report healthy

Question 9: Monitor Vulnerable Image

- Deploy an application in project area69 using below image
- **quay.io/redhattraining/hello-world-nginx: latest** in managed-cluster
- Image deployed should be updated in rhacs vulnerability dashboard
- Search result shows the image with active state.
- Add the image to the watch images in RHACS
- The image status should show Scanning via watch tag status.

Question 10: Vulnerability Management

- Create a RHACS policy to prevent the deployment of image that use the debian:10 operating systems
- Name: Debian-policy
- Severity: High
- Categories: Vulnerability Management
- Life cycle stage: Deploy
- Response method: inform and enforce
- configure enforcement behaviour: Enforce on deploy