Red Hat Training and Certification

CS229
Deploying Production AWS ROSA Clusters: Creation, Configuration, and Application Integration

Course Description

Create and configure production-grade ROSA clusters as part of a larger AWS customer's footprint and then integrate applications on ROSA with AWS services while keeping a good security posture.

Deploying Production AWS ROSA Clusters: Creation, Configuration, and Application Integration (CS229) teaches how to configure ROSA clusters as part of pre-existing AWS environments and how to integrate ROSA with AWS services commonly used by IT operations teams, such as Amazon CloudWatch. This course also teaches how to integrate applications deployed on ROSA with AWS services in a way that cluster administrators and platform engineers retain control of credentials and roles required by applications to access AWS services instead of exposing those credentials to application developers.

Course content summary

- Create ROSA STS PrivateLink clusters
- Connect PrivateLink ROSA clusters to existing VPCs and enable administrators and developers to access those clusters
- Configure dedicated machine pools and node/pod autoscaling
- Configure node, cluster, and audit log forwarding to Amazon CloudWatch
- Configure authentication and group sync with Amazon Cognito
- Integrate with external container registries such as ECR and Quay.io to deploy applications from private image repositories
- Configure storage classes to enable application access to different EBS volume types
- Configure storage classes and security contexts to enable application access to shared EFS storage volumes
- Configure pod identity using STS/IRSA to enable application access to AWS services such as database (Aurora), integration (SQS), and object storage (S3)
- Provision AWS services for applications using the AWS Controllers for Kubernetes (ACK)
- Federate and query application metrics (application workload monitoring) with Amazon Managed Prometheus Service
- Aggregate and query structured application logs with Amazon CloudWatch
- Configure custom domains and TLS certificates for secure public access to applications

Audience for this course

- Primary: ROSA Administrators, Platform Engineers, Cloud Administrators, System Administrators and other infrastructure-related IT roles who are responsible for providing and supporting infrastructure for applications deployed on AWS
- Secondary: Enterprise Architects, Site Reliability Engineers, DevOps Engineers, and other application-related IT roles who are responsible for designing infrastructure for applications deployed on AWS

Recommended training

- DO120 - Introduction to Red Hat OpenShift on AWS (ROSA) or equivalent experience: “I know how to create and access a public ROSA cluster.”
- AWS administration at the level of either AWS Certified SysOps Administrator - Associate or AWS Certified Solutions Architect - Associate, or equivalent experience: “I know how to manage AWS infrastructure services.”
- Basic knowledge of OpenShift from DO080 Technical Overview: “I know basic concepts of OpenShift and containers.”
- It is recommended that learners also enroll in the Red Hat Certified OpenShift Administration certification courses in addition to taking CS220 and CS221.

Outline for this course

PrivateLink Red Hat OpenShift on AWS (ROSA) Clusters
Create a PrivateLink ROSA cluster with STS and enable developers or administrators to access the API and router endpoints of the cluster.

Node and Pod Autoscaling
Configure a ROSA cluster and a workload to dynamically scale the number of cluster nodes and application pods according to load.

Integrate ROSA Clusters with Amazon Web Services
Configure ROSA clusters to forward logs to Amazon CloudWatch for long-term storage, aggregation, and analysis, and to authenticate OpenShift users by using Amazon Cognito.

Deploy Applications From External Registries
Deploy applications on Red Hat OpenShift Service on AWS (ROSA) from private container image repositories in external centralized container image registries.

Provide Amazon Storage Volumes for Applications
Configure Amazon Elastic Block Storage (EBS) or Amazon Elastic File System (EFS) volumes that meet the cost, performance, and sharing requirements of their applications.

Configure Application Access to AWS Services
Configure applications for access to shared AWS services by using Kubernetes service accounts, and provision dedicated AWS services by using Kubernetes custom resources.

OpenShift and AWS Application Observability
Configure ROSA clusters to forward application logs to Amazon CloudWatch and application metrics to Amazon Managed Service for Prometheus.

Course reference: https://www.redhat.com/en/services/training/cs229-deploying-production-aws-rosa-clusters-creation-configuration-application-integration4

Custom Domains for ROSA Applications
Expose applications to internet users with secure URLs by using human-readable DNS domains.

As a result of attending this course, students can create private ROSA clusters which are integrated with AWS infrastructure services typically employed by IT operations teams and ready to start onboarding applications and developers. Students can also integrate applications deployed on a private ROSA cluster in a way that cluster administrators and platform engineers retain control of credentials and roles required by applications to access AWS services, instead of exposing those credentials to application developers.

Course reference: https://www.redhat.com/en/services/training/cs229-deploying-production-aws-rosa-clusters-creation-configuration-application-integration4