**LAB# 3**

**Securing EKS Applications with AWS Secrets**

**Manager**

**\*\*Tasks\*\*:**

**1. Store a secret in AWS Secrets Manager.**

**2. Access the secret from an EKS pod.**

**3. Rotate the secret and validate updates.**

**\*\*Documentation\*\*:**

**- Kubernetes security basics.**

**- AWS Secrets Manager overview.**

**- Securely managing and accessing secrets**

**Before you can access a secret from an EKS pod, you need to store it securely in AWS Secrets Manager. Follow these steps to store a secret:**

* **Log in to the AWS Management Console.**
* **Navigate to the AWS Secrets Manager service.**
* **Click "Store a new secret."**
* **Choose the "Credentials for RDS database, Redshift cluster, or Aurora cluster" option or any other suitable option depending on your use case.**
* **Enter the secret values, such as username and password.**
* **Define the rotation policy if you plan to rotate the secret regularly.**
* **Review and confirm the settings, and then click "Store" to create the secret.**

[**https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating\_csi\_driver.html**](https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_csi_driver.html)

| apiVersion: v1 kind: Pod metadata:  name: my-app-pod spec:  containers:  - name: my-app-container  image: my-app-image  volumeMounts:  - name: secret-volume  mountPath: /mnt/secrets-store  volumes:  - name: secret-volume  csi:  driver: secrets-store.csi.k8s.io  readOnly: true  volumeAttributes:  secretProviderClass: "aws-secrets" |
| --- |

To rotate a secret stored in AWS Secrets Manager, follow these steps:

* Go to the Secrets Manager in the AWS Management Console.
* Select the secret you want to rotate.
* Click "Rotate secret."
* Configure the rotation settings and choose a Lambda function or an AWS Fargate task to perform the rotation.
* Monitor the rotation process and ensure that your application continues to function correctly with the updated secret values.

It's important to thoroughly test the rotation process and validate that your application can handle secret updates without any disruptions.