Accessing AWS Resources from Kubernetes

Document Level Classification

200

Introduction

When you deploy to Kubernetes, your pods run under a Kubernetes service account. Because Kubernetes is running in AWS you can use an IAM role instead of a secret access key. Also, AWS provides a special feature for Kubernetes to provide access to your specific pods instead of the entire instance they run on. This prevents cotenant workloads from accessing your AWS resources. AWS calls this feature "IAM Roles for Service Accounts".

Note that in Substrate EKS clusters, we have already provisioned the OIDC provider so you do not need to do this yourself.

Accessing S3 from Kubernetes

As noted above, the OIDC provider is already present. Also, we have already provisioned VPC endpoints for S3 so your pod can access S3 via private networking.

If you are following the AWS guide above, you only need to worry about steps 2 and 3:

2. Create a new IAM Role and Policy for your Service Account
3. Associate your Service Account with the new IAM Role

Depending on how you setup your bucket you may also need to configure a bucket policy.

AWS IAM Roles for your Services

On EKS, pods can be granted access to AWS services via IAM by attaching an IAM role to your pod's service account.

More details on how this works can be found here: https://docs.aws.amazon.com/eks/latest/userguide/iam-roles-for-service-accounts.html

Creating the IAM role & policy

The OIDC provider is already created by infra-plat for every Substrate EKS cluster.

Follow the directions here for creating the role & policy in IAM: https://docs.aws.amazon.com/eks/latest/userguide/associate-service-account-role.html

Associate the IAM role to your pod's service account

Epic App Helm Chart

If using the epic-app Helm Chart, you can enable service-account creation and set the role via annotations using the following block in your values.yaml:

```
serviceAccount:
  # Specifies whether a service account should be created
  create: true
  # Annotations to add to the service account
  annotations:
    eks.amazonaws.com/role-arn: arn:aws:iam::<AWS_ACCOUNT_ID>:role/<IAM
```

Other

Otherwise, use the instructions here to set the correct annotation for your service account: https://docs.aws.amazon.com/eks/latest/userguide/specify-service-account-role.html

---