DAL-EMR-ROLES:

This CloudFormation stack is used to create roles. It creates 3 roles for EMR

1.EMR Service role

2.InstanceProfileRole

3.instanceprofile

As part of this roles managed policies are attached as mentioned in the cloud formation stack

Clear data permission boundary is attached to all three roles as part of standard practice

This stack will provide three output variables that can be accessed in other cloud formation stacks present in the aws account

Output variables holds the arn for newly created 3 roles as part of this stack

**Input parameters for the stack:**

PermissionBoundary

**output variable names for the stack:**

DAL-EMR-ROLES:EMRClusterServiceRole::Arn

DAL-EMR-ROLES:EMRClusterinstanceProfile::Arn

DAL-EMR-ROLES:EMRClusterinstanceProfileRole::Arn

DAL-KMS-S3:

**Dependency:**

This stack depends on DAL-EMR-ROLES stack .so DAL-EMR-ROLES should be created prior to DAL-KMS-S3

This stack will add additional permissions to the roles created in previous stack (DAL-EMR-ROLES)

This stack will create a policy which will allow kms actions on all resources present in the account and also allow S3:putObject,s3:GetObject and S3:DeleteObject actions on all resources available in the account

This policy later attached to below mentioned roles

- DAL-EMR-EMRClusterInstanceProfileRole

- DAL-EMR-EMRClusterServiceRole

DAL-PRIVATE-SECURITY

This stack will allow to create 3 security groups that are needed to run emr in private subnet

1. InstanceMasterSecurityGroup:
2. InstanceSlaveSecurityGroup
3. InstanceServiceAccessSecurityGroup:

Currently in the stack we opened 22 port to enable SSH access to EMR .other ports which are needed for livy,jupyter hub need to be added to the stack

**Input parameters for the stack**

1.cidrip

2.vpcid

**Output parameters for the stack**

DAL-PRIVATE-SECURITY:EMRMasterSecurityGroupId::GroupId

DAL-PRIVATE-SECURITY:EMRServiceAccessSecurityGroupId::GroupId

DAL-PRIVATE-SECURITY:EMRSlaveSecurityGroupId::GroupId

DAL-EMR-STACK

This stack will allow to create an EMR cluster by using roles and security groups created in the previous stack.

Currently kmskey and ec2key pair is created with the help of console .you can get the details from admin team or can be create through aws cli

Below are the parameters that are used as input parameters

How to test services after EMR service up and running

How to create users