<table>
<tr><th>Policy Name</th><th>Policy Permissions</th></tr>
<tr><td colspan="2">User running the CFN stack needs full permission on these services:

AWS IAM, Amazon ECR, AWS Batch, AWS Lambda, Amazon CloudWatch, AWS Glue, Amazon S3, AWS StepFunction, Amazon Redshift, AWS Secrets Manager, Amazon EC2 – SecurityGroup, AWS LakeFormation (if Selected Yes for the CFN parameter UseAWSLakeFormationForGlueCatalog)</td></tr>
<tr><td>AWSBatchServiceRole (Managed Policy)</td><td><pre>
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeKeyPairs",
            "ec2:DescribeImages",
            "ec2:DescribeImageAttribute",
            "ec2:DescribeSpotInstanceRequests",
            "ec2:DescribeSpotFleetInstances",
            "ec2:DescribeSpotFleetRequests",
            "ec2:DescribeSpotPriceHistory",
            "ec2:DescribeVpcClassicLink",
            "ec2:DescribeLaunchTemplateVersions",
            "ec2:CreateLaunchTemplate",
            "ec2:DeleteLaunchTemplate",
            "ec2:RequestSpotFleet",
            "ec2:CancelSpotFleetRequests",
            "ec2:ModifySpotFleetRequest",
            "ec2:TerminateInstances",
            "ec2:RunInstances",
            "autoscaling:DescribeAccountLimits",
            "autoscaling:DescribeAutoScalingGroups",
            "autoscaling:DescribeLaunchConfigurations",
            "autoscaling:DescribeAutoScalingInstances",
            "autoscaling:CreateLaunchConfiguration",
            "autoscaling:CreateAutoScalingGroup",
            "autoscaling:UpdateAutoScalingGroup",
            "autoscaling:SetDesiredCapacity",
</pre></td></tr>
</table>

```
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateContainerAgent",
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ecs:TagResource",
      "Resource": [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "RunInstances"
        }
      }
    }
  ]
}
```

AmazonECSTaskExecutionRolePolicy	{
	   "Version": "2012-10-17",
	   "Statement": [
	      {
	         "Effect": "Allow",
	         "Action": [
	            "ecr:GetAuthorizationToken",
	            "ecr:BatchCheckLayerAvailability",
	            "ecr:GetDownloadUrlForLayer",
	            "ecr:BatchGetImage",
	            "logs:CreateLogStream",
	            "logs:PutLogEvents"
	         ],
	         "Resource": "*"
	      }
	   ]
	}

GlueCatalogAccessPolicy	{
	   "Version": "2012-10-17",
	   "Statement": [
	      {
	         "Action": [
	            "glue:Get*",
	            "glue:BatchGetPartition"
	         ],
	         "Resource": "*",
	         "Effect": "Allow",
	         "Sid": "GlueCatalogAccessPolicy"
	      }
	   ]
	}

AWSGlueServiceRole (Managed Policy)	{
	   "Version": "2012-10-17",
	   "Statement": [
	      {
	         "Effect": "Allow",
	         "Action": [
	            "glue:*",
	            "s3:GetBucketLocation",
	            "s3:ListBucket",
	            "s3:ListAllMyBuckets",
	            "s3:GetBucketAcl",
	            "ec2:DescribeVpcEndpoints",
	            "ec2:DescribeRouteTables",

```
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket"
      ],
      "Resource": [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
```

	]
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "logs:CreateLogGroup",
	        "logs:CreateLogStream",
	        "logs:PutLogEvents"
	      ],
	      "Resource": [
	        "arn:aws:logs:*:*:/aws-glue/*"
	      ]
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "ec2:CreateTags",
	        "ec2:DeleteTags"
	      ],
	      "Condition": {
	        "ForAllValues:StringEquals": {
	          "aws:TagKeys": [
	            "aws-glue-service-resource"
	          ]
	        }
	      },
	      "Resource": [
	        "arn:aws:ec2:*:*:network-interface/*",
	        "arn:aws:ec2:*:*:security-group/*",
	        "arn:aws:ec2:*:*:instance/*"
	      ]
	    }
	  ]
	}

RedshiftAccessIAMPolicy	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": [
	        "redshift:resumeCluster",
	        "redshift:pauseCluster",
	        "redshift:describeClusters",
	        "redshift:modifyClusterParameterGroup",
	        "redshift:createClusterParameterGroup",

	"redshift:describeClusterParameters",
	"redshift:resizeCluster",
	"redshift:createCluster",
	"redshift:GetClusterCredentials",
	"redshift:RebootCluster"
	],
	"Resource": [
	"arn:aws:redshift:us-east-1:<ACCOUNT_ID>:cluster:rs*",
	"arn:aws:redshift:us-east-1:<ACCOUNT_ID>:dbname:rs*/*",
	"arn:aws:redshift:us-east-1:<ACCOUNT_ID>:dbuser:rs*/*",
	"arn:aws:redshift:us-east-1:<ACCOUNT_ID>:parametergroup:rs*"
	],
	"Effect": "Allow"
	},
	{
	"Action": [
	"ec2:Describe*",
	"redshift:restoreFromClusterSnapshot",
	"redshift:describeClusterSnapshots",
	"redshift-data:ExecuteStatement",
	"redshift-data:ListStatements",
	"redshift-data:GetStatementResult",
	"redshift-data:DescribeStatement"
	],
	"Resource": [
	"*"
	],
	"Effect": "Allow"
	}
	]
	}

LambdaInvokePolicy	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Action": [
	"lambda:InvokeFunction"
	],
	"Resource": "arn:aws:lambda:us-east-1:<ACCOUNT_ID>:function:redshift-node-config-lf-o-RedshiftConfigTestingLam-hZjftvXgnhzn",
	"Effect": "Allow"
	}
	]

	}

RedshiftBucketAccessIAMPolicy	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Action": [
	"s3:GetBucketLocation",
	"s3:GetObject",
	"s3:ListMultipartUploadParts",
	"s3:ListBucket",
	"s3:ListBucketMultipartUploads",
	"s3:PutObject",
	"s3:ListObjects"
	],
	"Resource": [
	"arn:aws:s3:::<stack-created-bucket>",
	"arn:aws:s3:::<stack-created-bucket>/*",
	"arn:aws:s3:::<audit_log_bucket>/user_config.json"
	],
	"Effect": "Allow",
	"Sid": "RedshiftConfigTestingBucketAccess"
	},
	{
	"Action": [
	"s3:GetBucketLocation",
	"s3:GetObject",
	"s3:ListMultipartUploadParts",
	"s3:ListBucket",
	"s3:ListBucketMultipartUploads",
	"s3:ListObjects"
	],
	"Resource": [
	"arn:aws:s3:::redshift-simple-replay-ra3/*",
	"arn:aws:s3:::redshift-simple-replay-ra3",
	"arn:aws:s3:::<audit_log_bucket>/*",
	"arn:aws:s3:::<audit_log_bucket>"],
	"Effect": "Allow",
	"Sid": "RedshiftWhatIfExternalBucketAccess"
	}
	]
	}

RedshiftMLAccessPolicy	{
	"Version": "2012-10-17",
	"Statement": [{

	"Action": ["cloudwatch:PutMetricData", "logs:CreateLogGroup", "logs:CreateLogStream", "logs:DescribeLogStreams", "logs:PutLogEvents", "ecr:BatchCheckLayerAvailability", "ecr:BatchGetImage", "ecr:GetAuthorizationToken", "ecr:GetDownloadUrlForLayer", "sagemaker:*Job*"], "Resource": "*", "Effect": "Allow", "Sid": "RedshiftMLAccessPolicy" }] }

AWSBasicLambdaExecutionRole (Managed Policy)	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"logs:CreateLogGroup",
	"logs:CreateLogStream",
	"logs:PutLogEvents"
	],
	"Resource": "*"
	}
	]
	}

RedshiftAccessPolicy	{ "Version": "2012-10-17", "Statement": [{ "Action": ["iam:CreateServiceLinkedRole"], "Resource": ["arn:aws:iam::<ACCOUNT_ID>:role/aws-service-role/redshift.amazonaws.com/AWSServiceRoleForRedshift"], "Effect": "Allow" }, { "Action": ["iam:PassRole"], "Resource": ["arn:aws:iam::<ACCOUNT_ID>:role/redshift-node-config-lf-option-RedshiftIAMRole-7OR1UWVPFI5J"

```
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:ListSecrets"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-
1:<ACCOUNT_ID>:secret:SecretRedshiftMasterUser-XxwmVIsypCVo-
W3BsxW",
      "Effect": "Allow"
    },
    {
      "Action": [
        "batch:SubmitJob"
      ],
      "Resource": [
        "arn: aws:batch:us-east-1:<ACCOUNT_ID>:job-
definition/RedshiftPerformanceTest-0f382f6e169b8cc:1",
        "arn:aws:batch:us-east-1:<ACCOUNT_ID>:job-
queue/RedshiftPerformanceTesti-pxhNpFedGeoSnivb"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "batch:DescribeJobs"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "glue:StartCrawler"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```