Architecture (S3 → EventBridge → Lambda → Aurora PostgreSQL),

here's a full list of **IAM Roles and Policies** needed across all AWS services as per best practices:

---

1. S3 Bucket Role (bce-q-1-ar-infs3-role)

Purpose:
Allow Informatica to dump and read files from the S3 bucket.

Policy (Custom Inline or Managed):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<your-bucket-name>",
        "arn:aws:s3:::<your-bucket-name>/*"
      ]
    }
  ]
}
```

---

2. Lambda Role (bce-q-1-ar-lambdas3-role)

Purpose:
Allow Lambda to read from S3 and write logs to CloudWatch.

Policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<your-bucket-name>",
        "arn:aws:s3:::<your-bucket-name>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
```

```
    ],
    "Resource": "arn:aws:secretsmanager:<region>:<account-id>:secret:<db-secret-name>*"
   },
   {
    "Effect": "Allow",
    "Action": [
     "rds-data:ExecuteStatement",
     "rds-data:BatchExecuteStatement",
     "rds-data:BeginTransaction",
     "rds-data:CommitTransaction",
     "rds-data:RollbackTransaction"
    ],
    "Resource": "arn:aws:rds:<region>:<account-id>:cluster:<aurora-cluster-name>"
   }
 ]
}
```

---

3. EventBridge Rule Role (bce-q-1-ar-eventbridgelambda-role)

Purpose:
Allow EventBridge to trigger Lambda on S3 events.

Trust Policy:
EventBridge itself does **not** need an IAM role to trigger Lambda. But Lambda must allow EventBridge to invoke it.

Lambda Resource-based Policy Example:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "Service": "events.amazonaws.com"
   },
```

```
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:<region>:<account-id>:function:<function-name>"
   }
 ]
}
```

---

4. Aurora PostgreSQL Access Role

Roles:

- bce-q-1-ar-lambdauauroradb-role
- bce-q-1-ar-s3aurora-role

Purpose:
Allow Lambda to connect to Aurora PostgreSQL using the Data API or Secrets Manager.

Policy:
If using RDS Data API:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "rds-data:*"
   ],
   "Resource": "arn:aws:rds:<region>:<account-id>:cluster:<aurora-cluster-name>"
  },
  {
   "Effect": "Allow",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:<region>:<account-id>:secret:<db-secret-name>*"
  }
 ]
}
```

Summary Table (Matching Excel)

Destination	Role Name	Purpose
S3 Bucket	bce-q-1-ar-infs3-role	Informatica access S3 (Put/Get/List)
S3 Bucket	bce-q-1-ar-lambdas3-role	Lambda read S3 + CloudWatch logs
Lambda	bce-q-1-ar-eventbridgelambda-role	Allow EventBridge to trigger Lambda
Aurora PostgreSQL	bce-q-1-ar-lambdauauroradb-role	Lambda DB access via RDS Data API
Aurora PostgreSQL	bce-q-1-ar-s3aurora-role	Optional: External app DB access