RDS OS and File based Log Monitoring Privileges

AWS IAM Policy can be used to create permissions that specify which RDS actions a user, or a group of users in your AWS account can perform. IAM Policy is basically a JSON document that consists of one or more statements which defines the action to be taken on AWS resources. It can be used to determine who is allowed to create, delete, or modify RDS instances.

SQL DM for MySQL needs the following permissions to fetch the log files:

1. DescribeDBLogFiles: This API fetches a list of log files available for your instance.

2. DownloadDBLogFilePortion: This API downloads the specified log file.

For fetching the OS metrics, the following permission is needed:

1. GetMetricStatistics: This API fetches the average of CloudWatch metrics.

You can create a simple IAM Policy, giving the above permissions, for e.g:

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect":"Allow",
      "Action": [
         "rds:DescribeDBLogFiles",
         "rds:DownloadDBLogFilePortion"
         "cloudwatch:GetMetricStatistics"
      ],
      "Resource":"*"
   }]
}
```

You can restrict the Resource for the above policy using this link. In case, you want to perform either OS monitoring, or file-based log monitoring for your RDS/Aurora instance then you can include only those actions in the above policy.

You can use the default policy **CloudWatchReadOnlyAccess** provided by AWS for OS monitoring, in case you do not want to create a custom policy. Keep in mind that this policy grants more permissions than SQL DM for MySQL requires to fetch your RDS/Aurora metrics.