Naman - Fine-Grained IAM Policies

User: Naman
Document Type: IAM Policy Implementation Guide

Table of Contents

Lab Account Policies

1. SageMaker Policy

SageMaker Core Access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerNotebookInstances",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateNotebookInstance",
                "sagemaker:DescribeNotebookInstance",
                "sagemaker:StartNotebookInstance",
                "sagemaker:StopNotebookInstance",
                "sagemaker:DeleteNotebookInstance",
                "sagemaker:ListNotebookInstances",
                "sagemaker:UpdateNotebookInstance",
                "sagemaker:CreateNotebookInstanceLifecycleConfig",
                "sagemaker:DescribeNotebookInstanceLifecycleConfig",
                "sagemaker:ListNotebookInstanceLifecycleConfigs",
                "sagemaker:UpdateNotebookInstanceLifecycleConfig",
                "sagemaker:DeleteNotebookInstanceLifecycleConfig"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SageMakerTrainingJobs",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:ListTrainingJobs",
                "sagemaker:StopTrainingJob",
                "sagemaker:CreateHyperParameterTuningJob",
                "sagemaker:DescribeHyperParameterTuningJob",
                "sagemaker:ListHyperParameterTuningJobs",
```

```
                "sagemaker:StopHyperParameterTuningJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:DescribeAutoMLJob",
                "sagemaker:ListAutoMLJobs",
                "sagemaker:StopAutoMLJob"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SageMakerModelsAndEndpoints",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateModel",
                "sagemaker:DescribeModel",
                "sagemaker:ListModels",
                "sagemaker:DeleteModel",
                "sagemaker:CreateEndpointConfig",
                "sagemaker:DescribeEndpointConfig",
                "sagemaker:ListEndpointConfigs",
                "sagemaker:DeleteEndpointConfig",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeEndpoint",
                "sagemaker:ListEndpoints",
                "sagemaker:UpdateEndpoint",
                "sagemaker:DeleteEndpoint",
                "sagemaker:InvokeEndpoint",
                "sagemaker:InvokeEndpointAsync"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SageMakerStudio",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain",
                "sagemaker:DescribeDomain",
                "sagemaker:ListDomains",
                "sagemaker:UpdateDomain",
                "sagemaker:DeleteDomain",
                "sagemaker:CreateUserProfile",
                "sagemaker:DescribeUserProfile",
                "sagemaker:ListUserProfiles",
                "sagemaker:UpdateUserProfile",
                "sagemaker:DeleteUserProfile",
                "sagemaker:CreateApp",
                "sagemaker:DescribeApp",
                "sagemaker:ListApps",
                "sagemaker:DeleteApp"
            ],
            "Resource": "*"
        }
    ]
}
```

2. QuickSight Policy - Business Intelligence

QuickSight Analytics Access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QuickSightUserManagement",
            "Effect": "Allow",
            "Action": [
                "quicksight:RegisterUser",
                "quicksight:DescribeUser",
                "quicksight:UpdateUser",
                "quicksight:DeleteUser",
                "quicksight:ListUsers",
                "quicksight:CreateGroup",
                "quicksight:DescribeGroup",
                "quicksight:UpdateGroup",
                "quicksight:DeleteGroup",
                "quicksight:ListGroups",
                "quicksight:CreateGroupMembership",
                "quicksight:DescribeGroupMembership",
                "quicksight:DeleteGroupMembership",
                "quicksight:ListGroupMemberships"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSightDataSources",
            "Effect": "Allow",
            "Action": [
                "quicksight:CreateDataSource",
                "quicksight:DescribeDataSource",
                "quicksight:UpdateDataSource",
                "quicksight:DeleteDataSource",
                "quicksight:ListDataSources",
                "quicksight:DescribeDataSourcePermissions",
                "quicksight:UpdateDataSourcePermissions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSightDatasets",
            "Effect": "Allow",
            "Action": [
                "quicksight:CreateDataSet",
                "quicksight:DescribeDataSet",
                "quicksight:UpdateDataSet",
                "quicksight:DeleteDataSet",
```

```
                "quicksight:ListDataSets",
                "quicksight:DescribeDataSetPermissions",
                "quicksight:UpdateDataSetPermissions",
                "quicksight:CreateIngestion",
                "quicksight:DescribeIngestion",
                "quicksight:ListIngestions",
                "quicksight:CancelIngestion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSightDashboardsAnalyses",
            "Effect": "Allow",
            "Action": [
                "quicksight:CreateDashboard",
                "quicksight:DescribeDashboard",
                "quicksight:UpdateDashboard",
                "quicksight:DeleteDashboard",
                "quicksight:ListDashboards",
                "quicksight:ListDashboardVersions",
                "quicksight:DescribeDashboardPermissions",
                "quicksight:UpdateDashboardPermissions",
                "quicksight:UpdateDashboardPublishedVersion",
                "quicksight:CreateAnalysis",
                "quicksight:DescribeAnalysis",
                "quicksight:UpdateAnalysis",
                "quicksight:DeleteAnalysis",
                "quicksight:ListAnalyses",
                "quicksight:DescribeAnalysisPermissions",
                "quicksight:UpdateAnalysisPermissions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSightTemplatesThemes",
            "Effect": "Allow",
            "Action": [
                "quicksight:CreateTemplate",
                "quicksight:DescribeTemplate",
                "quicksight:UpdateTemplate",
                "quicksight:DeleteTemplate",
                "quicksight:ListTemplates",
                "quicksight:ListTemplateVersions",
                "quicksight:DescribeTemplatePermissions",
                "quicksight:UpdateTemplatePermissions",
                "quicksight:CreateTheme",
                "quicksight:DescribeTheme",
                "quicksight:UpdateTheme",
                "quicksight:DeleteTheme",
                "quicksight:ListThemes",
                "quicksight:ListThemeVersions"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

---

3. Bedrock Policy - AI/ML Services

Bedrock AI Operations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BedrockFoundationModels",
            "Effect": "Allow",
            "Action": [
                "bedrock:ListFoundationModels",
                "bedrock:GetFoundationModel",
                "bedrock:InvokeModel",
                "bedrock:InvokeModelWithResponseStream",
                "bedrock:GetModelInvocationLoggingConfiguration",
                "bedrock:PutModelInvocationLoggingConfiguration",
                "bedrock:DeleteModelInvocationLoggingConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Sid": "BedrockCustomModels",
            "Effect": "Allow",
            "Action": [
                "bedrock:CreateModelCustomizationJob",
                "bedrock:GetModelCustomizationJob",
                "bedrock:ListModelCustomizationJobs",
                "bedrock:StopModelCustomizationJob",
                "bedrock:DeleteCustomModel",
                "bedrock:GetCustomModel",
                "bedrock:ListCustomModels",
                "bedrock:CreateProvisionedModelThroughput",
                "bedrock:GetProvisionedModelThroughput",
                "bedrock:UpdateProvisionedModelThroughput",
                "bedrock:DeleteProvisionedModelThroughput",
                "bedrock:ListProvisionedModelThroughputs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "BedrockAgents",
            "Effect": "Allow",
            "Action": [
                "bedrock:CreateAgent",
                "bedrock:GetAgent",
                "bedrock:UpdateAgent",
```

```
                "bedrock:DeleteAgent",
                "bedrock:ListAgents",
                "bedrock:CreateAgentVersion",
                "bedrock:GetAgentVersion",
                "bedrock:ListAgentVersions",
                "bedrock:DeleteAgentVersion",
                "bedrock:CreateAgentAlias",
                "bedrock:GetAgentAlias",
                "bedrock:UpdateAgentAlias",
                "bedrock:DeleteAgentAlias",
                "bedrock:ListAgentAliases",
                "bedrock:PrepareAgent",
                "bedrock:InvokeAgent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "BedrockKnowledgeBases",
            "Effect": "Allow",
            "Action": [
                "bedrock:CreateKnowledgeBase",
                "bedrock:GetKnowledgeBase",
                "bedrock:UpdateKnowledgeBase",
                "bedrock:DeleteKnowledgeBase",
                "bedrock:ListKnowledgeBases",
                "bedrock:AssociateAgentKnowledgeBase",
                "bedrock:DisassociateAgentKnowledgeBase",
                "bedrock:GetAgentKnowledgeBase",
                "bedrock:ListAgentKnowledgeBases",
                "bedrock:UpdateAgentKnowledgeBase",
                "bedrock:CreateDataSource",
                "bedrock:GetDataSource",
                "bedrock:UpdateDataSource",
                "bedrock:DeleteDataSource",
                "bedrock:ListDataSources",
                "bedrock:StartIngestionJob",
                "bedrock:GetIngestionJob",
                "bedrock:ListIngestionJobs",
                "bedrock:Retrieve",
                "bedrock:RetrieveAndGenerate"
            ],
            "Resource": "*"
        },
        {
            "Sid": "BedrockGuardrails",
            "Effect": "Allow",
            "Action": [
                "bedrock:CreateGuardrail",
                "bedrock:GetGuardrail",
                "bedrock:UpdateGuardrail",
                "bedrock:DeleteGuardrail",
                "bedrock:ListGuardrails",
                "bedrock:CreateGuardrailVersion",
                "bedrock:GetGuardrailVersion",
```

```
                "bedrock:ListGuardrailVersions",
                "bedrock:DeleteGuardrailVersion"
            ],
            "Resource": "*"
        }
    ]
}
```

---

4. Supporting Services Policy

S3, IAM, and Other Required Services

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3DataAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:PutBucketAcl",
                "s3:GetBucketNotification",
                "s3:PutBucketNotification",
                "s3:GetObjectVersion",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::*",
                "arn:aws:s3:::*/*"
            ]
        },
        {
            "Sid": "IAMRoleManagement",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:CreateRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "ECRAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "ecr:CreateRepository",
                "ecr:DescribeRepositories",
                "ecr:ListImages"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AthenaAccess",
            "Effect": "Allow",
            "Action": [
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:ListQueryExecutions",
                "athena:StartQueryExecution",
                "athena:StopQueryExecution",
                "athena:GetWorkGroup",
                "athena:ListWorkGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "rds:DescribeDBInstances",
                "rds:DescribeDBClusters",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeVpcSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "STSAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:GetCallerIdentity",
                "sts:DecodeAuthorizationMessage"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackResources",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EC2NetworkAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:DetachNetworkInterface"
            ],
            "Resource": "*"
        }
    ]
}
```

---

5. Consolidated Policy

Combined Policy for Data Science Workflow

```
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DataScienceFullWorkflow",
            "Effect": "Allow",
            "Action": [
                "sagemaker:*",
                "bedrock:InvokeModel",
                "bedrock:InvokeModelWithResponseStream",
                "bedrock:ListFoundationModels",
                "bedrock:GetFoundationModel",
                "bedrock:CreateAgent",
                "bedrock:GetAgent",
                "bedrock:InvokeAgent",
                "quicksight:CreateAnalysis",
                "quicksight:DescribeAnalysis",
                "quicksight:UpdateAnalysis",
                "quicksight:ListAnalyses",
                "quicksight:CreateDashboard",
                "quicksight:DescribeDashboard",
                "quicksight:UpdateDashboard",
                "quicksight:ListDashboards",
                "quicksight:CreateDataSet",
                "quicksight:DescribeDataSet",
                "quicksight:ListDataSets",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "iam:PassRole",
                "iam:GetRole",
                "iam:ListRoles",
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "cloudwatch:PutMetricData",
                "cloudwatch:GetMetricStatistics",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StartQueryExecution"
            ],
            "Resource": "*"
        }
    ]
}
```

6. Read-Only Cross-Service Policy

Monitoring and Audit Access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "sagemaker:Describe*",
                "sagemaker:List*",
                "quicksight:Describe*",
                "quicksight:List*",
                "bedrock:List*",
                "bedrock:Get*",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "iam:GetRole",
                "iam:ListRoles",
                "athena:GetQueryExecution",
                "athena:ListQueryExecutions"
            ],
            "Resource": "*"
        }
    ]
}
```