Abhishek - Fine-Grained IAM Policies (Account-Wise)

User: Abhishek
Document Type: IAM Policy Implementation Guide

Table of Contents

Lab Account Policies

1. RDS Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RDSInstanceManagement",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "rds:StartDBInstance",
                "rds:StopDBInstance",
                "rds:RebootDBInstance",
                "rds:CreateDBSnapshot",
                "rds:DescribeDBSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

2. S3 Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3LabAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
```

```
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::labaccount-bucket",
                "arn:aws:s3:::labaccount-bucket/*"
            ]
        }
    ]
}
```

3. DMS Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DMSReplicationTasks",
            "Effect": "Allow",
            "Action": [
                "dms:DescribeEndpoints",
                "dms:DescribeReplicationTasks",
                "dms:StartReplicationTask",
                "dms:StopReplicationTask"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Glue Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GlueDataProcessing",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateJob",
                "glue:GetJob",
                "glue:StartJobRun",
                "glue:StopJobRun",
                "glue:UpdateJob",
                "glue:CreateCrawler",
                "glue:StartCrawler",
```

```
                "glue:GetCrawler",
                "glue:GetCrawlers",
                "glue:UpdateCrawler"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Lake Formation Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationAccess",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess",
                "lakeformation:GrantPermissions",
                "lakeformation:RevokePermissions",
                "lakeformation:GetResourceLFTags",
                "lakeformation:ListPermissions"
            ],
            "Resource": "*"
        }
    ]
}
```

6. Athena Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AthenaQueryExecution",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:ListWorkGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

7. IAM Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAMReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:ListRoles",
                "iam:ListPolicies",
                "iam:GetPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

8. EC2/VPC Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2VPCManagement",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Demo Internals Account Policies

1. RDS Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "RDSInstanceManagement",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances",
                "rds:StartDBInstance",
                "rds:StopDBInstance",
                "rds:RebootDBInstance",
                "rds:CreateDBSnapshot",
                "rds:DescribeDBSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

2. S3 Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3DemoAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::labaccount-bucket",
                "arn:aws:s3:::labaccount-bucket/*"
            ]
        }
    ]
}
```

3. DMS Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DMSReplicationTasks",
            "Effect": "Allow",
            "Action": [
                "dms:DescribeEndpoints",
                "dms:DescribeReplicationTasks",
```

```
                "dms:StartReplicationTask",
                "dms:StopReplicationTask"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Glue Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GlueDataProcessing",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateJob",
                "glue:GetJob",
                "glue:StartJobRun",
                "glue:StopJobRun",
                "glue:UpdateJob",
                "glue:CreateCrawler",
                "glue:StartCrawler",
                "glue:GetCrawler",
                "glue:GetCrawlers",
                "glue:UpdateCrawler"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Lake Formation Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationAccess",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess",
                "lakeformation:GrantPermissions",
                "lakeformation:RevokePermissions",
```

```
                "lakeformation:GetResourceLFTags",
                "lakeformation:ListPermissions"
            ],
            "Resource": "*"
        }
    ]
}
```

6. Athena Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AthenaQueryExecution",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:ListWorkGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

7. IAM Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAMReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:ListRoles",
                "iam:ListPolicies",
                "iam:GetPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

8. EC2/VPC Policy - Demo-Internals Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2VPCManagement",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Hackathon Account Policies

1. Lake Formation Policy - Hackathon

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationFullAccess",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess",
                "lakeformation:GrantPermissions",
                "lakeformation:RevokePermissions",
                "lakeformation:GetResourceLFTags",
                "lakeformation:ListPermissions",
                "lakeformation:ListLFTags",
                "lakeformation:GetWorkUnits",
                "lakeformation:GetWorkUnitResults"
            ],
            "Resource": "*"
        }
    ]
}
```

2. Glue Policy - Hackathon

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GlueFullAccess",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateJob",
                "glue:GetJob",
                "glue:StartJobRun",
                "glue:StopJobRun",
                "glue:UpdateJob",
                "glue:CreateCrawler",
                "glue:StartCrawler",
                "glue:GetCrawler",
                "glue:GetCrawlers",
                "glue:UpdateCrawler"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Athena Policy - Hackathon

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AthenaFullAccess",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:ListWorkGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

4. QuickSight Policy - Hackathon

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QuickSightFullAccess",
            "Effect": "Allow",
            "Action": [
                "quicksight:DescribeDashboard",
                "quicksight:ListDashboards",
                "quicksight:ListDatasets",
                "quicksight:ListAnalyses",
                "quicksight:ListUsers",
                "quicksight:CreateDataset",
                "quicksight:UpdateDataset",
                "quicksight:DeleteDataset",
                "quicksight:CreateAnalysis",
                "quicksight:UpdateAnalysis",
                "quicksight:DeleteAnalysis"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Security Guardrails Policy - Hackathon

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExplicitDenyBlockList",
            "Effect": "Deny",
            "Action": [
                "iam:*Create*",
                "iam:*Delete*",
                "iam:*Update*",
                "iam:PassRole",
                "s3:*BucketPolicy",
                "glue:Delete*",
                "lakeformation:DeregisterResource",
                "athena:Delete*",
                "quicksight:DeleteAccountCustomization",
                "quicksight:CreateAccountSubscription",
                "quicksight:DeleteAccountSubscription"
            ],
            "Resource": "*"
        }
    ]
}
```

Development Account Policies

1. Lake Formation Policy - Development

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationFullAccess",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess",
                "lakeformation:GrantPermissions",
                "lakeformation:RevokePermissions",
                "lakeformation:GetResourceLFTags",
                "lakeformation:ListPermissions",
                "lakeformation:ListLFTags",
                "lakeformation:GetWorkUnits",
                "lakeformation:GetWorkUnitResults"
            ],
            "Resource": "*"
        }
    ]
}
```

2. Glue Policy - Development

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GlueFullAccess",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateJob",
                "glue:GetJob",
                "glue:StartJobRun",
                "glue:StopJobRun",
                "glue:UpdateJob",
                "glue:CreateCrawler",
                "glue:StartCrawler",
                "glue:GetCrawler",
                "glue:GetCrawlers",
                "glue:UpdateCrawler"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

3. Athena Policy - Development

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AthenaFullAccess",
            "Effect": "Allow",
            "Action": [
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:ListWorkGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

4. QuickSight Policy - Development

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QuickSightFullAccess",
            "Effect": "Allow",
            "Action": [
                "quicksight:DescribeDashboard",
                "quicksight:ListDashboards",
                "quicksight:ListDatasets",
                "quicksight:ListAnalyses",
                "quicksight:ListUsers",
                "quicksight:CreateDataset",
                "quicksight:UpdateDataset",
                "quicksight:DeleteDataset",
                "quicksight:CreateAnalysis",
                "quicksight:UpdateAnalysis",
                "quicksight:DeleteAnalysis"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Security Guardrails Policy - Development

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExplicitDenyBlockList",
            "Effect": "Deny",
            "Action": [
                "iam:*Create*",
                "iam:*Delete*",
                "iam:*Update*",
                "iam:PassRole",
                "s3:*BucketPolicy",
                "glue:Delete*",
                "lakeformation:DeregisterResource",
                "athena:Delete*",
                "quicksight:DeleteAccountCustomization",
                "quicksight:CreateAccountSubscription",
                "quicksight:DeleteAccountSubscription"
            ],
            "Resource": "*"
        }
    ]
}
```