Tanmay - Fine-Grained IAM Policy Document

User: Tanmay
Document Type: IAM Policy Implementation Guide
Purpose: Granting specific AWS permissions

Table of Contents

Lab Account Policies

1. EC2 Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeInstanceAttribute",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateImage",
                "ec2:DescribeImages",
                "ec2:DeregisterImage",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolume",
                "ec2:CreateKeyPair",
                "ec2:DeleteKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:ImportKeyPair",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        }
    ]
}
```

2. VPC Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VPCPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpc",
                "ec2:DeleteVpc",
                "ec2:DescribeVpcs",
                "ec2:ModifyVpcAttribute",
                "ec2:CreateSubnet",
                "ec2:DeleteSubnet",
                "ec2:DescribeSubnets",
                "ec2:ModifySubnetAttribute",
                "ec2:CreateInternetGateway",
                "ec2:DeleteInternetGateway",
                "ec2:AttachInternetGateway",
                "ec2:DetachInternetGateway",
                "ec2:DescribeInternetGateways",
                "ec2:CreateNatGateway",
                "ec2:DeleteNatGateway",
                "ec2:DescribeNatGateways",
                "ec2:CreateRouteTable",
                "ec2:DeleteRouteTable",
                "ec2:DescribeRouteTables",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:ReplaceRoute",
                "ec2:AssociateRouteTable",
                "ec2:DisassociateRouteTable",
                "ec2:CreateNetworkAcl",
                "ec2:DeleteNetworkAcl",
                "ec2:DescribeNetworkAcls",
                "ec2:CreateNetworkAclEntry",
                "ec2:DeleteNetworkAclEntry",
                "ec2:ReplaceNetworkAclEntry",
                "ec2:ReplaceNetworkAclAssociation",
                "ec2:CreateVpcEndpoint",
                "ec2:DeleteVpcEndpoint",
                "ec2:DescribeVpcEndpoints",
                "ec2:ModifyVpcEndpoint",
                "ec2:CreateVpcPeeringConnection",
                "ec2:DeleteVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:RejectVpcPeeringConnection",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

3. IAM Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAMPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:GetRole",
                "iam:PassRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListAttachedRolePolicies",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:GetPolicy",
                "iam:ListPolicyVersions",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:GetPolicyVersion",
                "iam:TagRole",
                "iam:UntagRole"
            ],
            "Resource": "*"
        }
    ]
}
```

4. SSO Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SSOPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:ListInstances",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListAccountAssignments",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetPermissionSet"
            ],
            "Resource": "*"
        }
    ]
}
```

5. SageMaker Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerPermissions",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain",
                "sagemaker:DeleteDomain",
                "sagemaker:DescribeDomain",
                "sagemaker:ListDomains",
                "sagemaker:UpdateDomain",
                "sagemaker:CreateUserProfile",
                "sagemaker:DeleteUserProfile",
                "sagemaker:DescribeUserProfile",
                "sagemaker:ListUserProfiles",
                "sagemaker:UpdateUserProfile",
                "sagemaker:CreateApp",
                "sagemaker:DeleteApp",
                "sagemaker:DescribeApp",
                "sagemaker:ListApps",
                "sagemaker:CreateNotebookInstance",
                "sagemaker:DeleteNotebookInstance",
                "sagemaker:DescribeNotebookInstance",
                "sagemaker:ListNotebookInstances",
                "sagemaker:UpdateNotebookInstance",
                "sagemaker:CreateTrainingJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:ListTrainingJobs",
                "sagemaker:StopTrainingJob",
                "sagemaker:CreateModel",
                "sagemaker:DeleteModel",
                "sagemaker:DescribeModel",
                "sagemaker:ListModels",
                "sagemaker:CreateEndpoint",
                "sagemaker:DeleteEndpoint",
                "sagemaker:DescribeEndpoint",
                "sagemaker:ListEndpoints",
                "sagemaker:UpdateEndpoint",
                "sagemaker:CreateEndpointConfig",
                "sagemaker:DeleteEndpointConfig",
                "sagemaker:DescribeEndpointConfig",
                "sagemaker:ListEndpointConfigs",
                "sagemaker:CreatePipeline",
                "sagemaker:DeletePipeline",
                "sagemaker:DescribePipeline",
                "sagemaker:ListPipelines",
                "sagemaker:UpdatePipeline",
                "sagemaker:StartPipelineExecution",
                "sagemaker:StopPipelineExecution",
                "sagemaker:CreateProject",
                "sagemaker:DeleteProject",
                "sagemaker:DescribeProject",
                "sagemaker:ListProjects",
                "sagemaker:UpdateProject",
                "sagemaker:AddTags",
                "sagemaker:DeleteTags",
                "sagemaker:ListTags"
            ],
            "Resource": "*"
        }
    ]
}
```

6. DataZone Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DataZonePermissions",
            "Effect": "Allow",
            "Action": [
                "datazone:CreateDomain",
                "datazone:DeleteDomain",
                "datazone:GetDomain",
                "datazone:ListDomains",
                "datazone:UpdateDomain",
                "datazone:CreateProject",
                "datazone:DeleteProject",
                "datazone:GetProject",
                "datazone:ListProjects",
                "datazone:UpdateProject",
                "datazone:CreateEnvironment",
                "datazone:DeleteEnvironment",
                "datazone:GetEnvironment",
                "datazone:ListEnvironments",
                "datazone:UpdateEnvironment",
                "datazone:CreateAsset",
                "datazone:DeleteAsset",
                "datazone:GetAsset",
                "datazone:ListAssets",
                "datazone:UpdateAsset",
                "datazone:PublishAsset",
                "datazone:CreateSubscription",
                "datazone:DeleteSubscription",
                "datazone:GetSubscription",
                "datazone:ListSubscriptions",
                "datazone:UpdateSubscription",
                "datazone:CreateGlossary",
                "datazone:DeleteGlossary",
                "datazone:GetGlossary",
                "datazone:ListGlossaries",
                "datazone:UpdateGlossary",
                "datazone:TagResource",
                "datazone:UntagResource",
                "datazone:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

7. Glue Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GluePermissions",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:UpdateTable",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:UpdatePartition",
                "glue:CreateJob",
                "glue:DeleteJob",
                "glue:GetJob",
                "glue:GetJobs",
                "glue:UpdateJob",
                "glue:StartJobRun",
                "glue:BatchStopJobRun",
                "glue:GetJobRun",
                "glue:GetJobRuns",
                "glue:CreateCrawler",
                "glue:DeleteCrawler",
                "glue:GetCrawler",
                "glue:GetCrawlers",
                "glue:UpdateCrawler",
                "glue:StartCrawler",
                "glue:StopCrawler",
                "glue:CreateConnection",
                "glue:DeleteConnection",
                "glue:GetConnection",
                "glue:GetConnections",
                "glue:UpdateConnection",
                "glue:CreateClassifier",
                "glue:DeleteClassifier",
                "glue:GetClassifier",
                "glue:GetClassifiers",
                "glue:UpdateClassifier",
                "glue:TagResource",
                "glue:UntagResource",
                "glue:GetTags"
            ],
            "Resource": "*"
        }
    ]
}
```

8. Lake Formation Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationPermissions",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataLakeSettings",
                "lakeformation:PutDataLakeSettings",
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource",
                "lakeformation:ListResources",
                "lakeformation:GrantPermissions",
                "lakeformation:RevokePermissions",
                "lakeformation:BatchGrantPermissions",
                "lakeformation:BatchRevokePermissions",
                "lakeformation:ListPermissions",
                "lakeformation:AddLFTagsToResource",
                "lakeformation:RemoveLFTagsFromResource",
                "lakeformation:GetResourceLFTags",
                "lakeformation:CreateLFTag",
                "lakeformation:DeleteLFTag",
                "lakeformation:GetLFTag",
                "lakeformation:ListLFTags",
                "lakeformation:UpdateLFTag",
                "lakeformation:SearchTablesByLFTags",
                "lakeformation:SearchDatabasesByLFTags"
            ],
            "Resource": "*"
        }
    ]
}
```

9. Service Catalog Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ServiceCatalogPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListPortfolios",
                "servicecatalog:ListPortfolioAccess",
                "servicecatalog:ListPrincipalsForPortfolio",
                "servicecatalog:ListResourcesForTagOption",
                "servicecatalog:ListTagOptions",
                "servicecatalog:SearchProducts",
                "servicecatalog:SearchProductsAsAdmin",
                "servicecatalog:SearchProvisionedProducts",
                "servicecatalog:ProvisionProduct",
                "servicecatalog:UpdateProvisionedProduct",
                "servicecatalog:TerminateProvisionedProduct",
                "servicecatalog:DescribeProduct",
                "servicecatalog:DescribeProductAsAdmin",
                "servicecatalog:DescribeProvisionedProduct",
                "servicecatalog:DescribeProvisioningArtifact",
                "servicecatalog:DescribeProvisioningParameters",
                "servicecatalog:ListLaunchPaths",
                "servicecatalog:ListProvisioningArtifacts",
                "servicecatalog:ListServiceActions",
                "servicecatalog:ListServiceActionsForProvisioningArtifact",
                "servicecatalog:ExecuteProvisionedProductServiceAction"
            ],
            "Resource": "*"
        }
    ]
}
```

10. STS Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "STSPermissions",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:GetCallerIdentity",
                "sts:GetFederationToken",
                "sts:GetSessionToken",
                "sts:DecodeAuthorizationMessage"
            ],
            "Resource": "*"
        }
    ]
}
```

11. S3 Policy - Lab Account

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:PutBucketPolicy",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload",
                "s3:GetObjectTagging",
                "s3:PutObjectTagging",
                "s3:DeleteObjectTagging",
                "s3:PutBucketVersioning",
                "s3:GetBucketVersioning",
                "s3:PutLifecycleConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:PutBucketEncryption",
                "s3:GetBucketEncryption"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        }
    ]
}
```