**Document Title**: Owner and Administrator Setup

**Project Title**: Hatching Sparrow CRM

**Date**: 6/12/2024

**Author(s)**: Ryan O’Connor, Full Stack Software Engineer

**Confidentiality:** N/A

**Lead Engineer's Complete Setup Guide**

**Owner's Actions**

**1. Sign in to AWS Management Console**

* Sign in using the root account or an IAM user with administrative permissions.

**2. Access AWS Organizations**

* In the AWS Management Console, go to the "AWS Organizations" service.

**3. Create the Lead Engineer Organizational Unit (OU)**

1. Navigate to "AWS Organizations" from the AWS Management Console.
2. Click on "Organizational units" on the left-hand side.
3. Click "Create organizational unit."
4. Name the OU "Lead Engineers" and click "Create organizational unit."

**4. Move the Lead Engineer Account to the Lead Engineers OU**

1. Navigate to "AWS Organizations."
2. Click on "Accounts" on the left-hand side.
3. Select the Lead Engineer's account.
4. Click "Move" at the top of the page.
5. Select the "Lead Engineers" OU and click "Move."

**5. Create an IAM Policy for Lead Engineer Permissions**

1. Navigate to the "IAM" service from the AWS Management Console.
2. Click on "Policies" on the left-hand side.
3. Click "Create policy."
4. In the JSON tab, paste the following policy document to allow full administrative access:

json

Copy code

{

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

"Statement": [

{

"Effect": "Allow",

"Action": "\*",

"Resource": "\*"

}

]

}

1. Click "Next: Tags," then "Next: Review."
2. Name the policy (e.g., "LeadEngineerAdminPolicy") and click "Create policy."

**6. Create a Role for the Lead Engineer and Attach the Policy**

1. Navigate to the "IAM" service from the AWS Management Console.
2. Click on "Roles" on the left-hand side.
3. Click "Create role."
4. Select "AWS account" and then "Another AWS account."
5. Enter your AWS Account ID (if needed) and click "Next: Permissions."
6. Search for the policy created earlier (e.g., "LeadEngineerAdminPolicy") and select it.
7. Click "Next: Tags," then "Next: Review."
8. Name the role (e.g., "LeadEngineerAdminRole") and click "Create role."

**7. Assign the Role to the Lead Engineer Account**

1. Navigate to the "IAM" service from the AWS Management Console.
2. Click on "Users" on the left-hand side.
3. Select the Lead Engineer's user account.
4. Click "Add permissions."
5. Choose "Attach policies directly."
6. Search for and select the "LeadEngineerAdminRole."
7. Click "Next: Review" and then "Add permissions."

**Lead Engineer's Actions**

**1. Create Remaining Organizational Units (OUs)**

1. Navigate to "AWS Organizations" from the AWS Management Console.
2. Click on "Organizational units" on the left-hand side.
3. Click "Create organizational unit."
4. Name the OUs accordingly: "Software Engineers," "Interns," "Consultants."
5. Click "Create organizational unit" for each.

**2. Move Accounts to the Appropriate OUs**

1. Navigate to "AWS Organizations."
2. Click on "Accounts" on the left-hand side.
3. Select the account you want to move.
4. Click "Move" at the top of the page.
5. Select the appropriate OU and click "Move."

**3. Create IAM Policies**

**Lead Engineers Policy:**

1. Navigate to the "IAM" service from the AWS Management Console.
2. Click on "Policies" on the left-hand side.
3. Click "Create policy."
4. In the JSON tab, paste the following policy document:

json

Copy code

{

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

"Statement": [

{

"Effect": "Allow",

"Action": "\*",

"Resource": "\*"

}

]

}

1. Click "Next: Tags," then "Next: Review."
2. Name the policy (e.g., "LeadEngineersFullAccess") and click "Create policy."

**Software Engineers Policy:**

1. Navigate to "Policies" and click "Create policy."
2. In the JSON tab, paste the following:

json

Copy code

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:\*",

"s3:\*",

"dynamodb:\*",

"rds:\*",

"lambda:\*",

"cloudwatch:\*"

],

"Resource": "\*"

},

{

"Effect": "Deny",

"Action": [

"iam:\*",

"organizations:\*",

"billing:\*"

],

"Resource": "\*"

}

]

}

1. Click "Next: Tags," then "Next: Review."
2. Name the policy (e.g., "SoftwareEngineersAccess") and click "Create policy."

**Interns Policy:**

1. Navigate to "Policies" and click "Create policy."
2. In the JSON tab, paste the following:

json

Copy code

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:ListBucket",

"ec2:DescribeInstances",

"cloudwatch:GetMetricData"

],

"Resource": "\*"

}

]

}

1. Click "Next: Tags," then "Next: Review."
2. Name the policy (e.g., "InternsReadOnly") and click "Create policy."

**Consultants Policy:**

1. Navigate to "Policies" and click "Create policy."
2. In the JSON tab, paste the following:

json

Copy code

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:\*",

"s3:\*",

"dynamodb:\*",

"rds:\*",

"lambda:\*",

"cloudwatch:\*",

"iam:CreateServiceLinkedRole",

"iam:PassRole"

],

"Resource": "\*"

},

{

"Effect": "Deny",

"Action": [

"iam:CreateUser",

"iam:DeleteUser",

"iam:PutRolePolicy",

"organizations:\*",

"billing:\*"

],

"Resource": "\*"

}

]

}

1. Click "Next: Tags," then "Next: Review."
2. Name the policy (e.g., "ConsultantsAccess") and click "Create policy."

**4. Create IAM Roles**

**For Lead Engineers:**

1. Navigate to "IAM" service.
2. Click on "Roles" on the left-hand side.
3. Click "Create role."
4. Choose "AWS account" and "Another AWS account."
5. Enter the AWS Account ID if needed.
6. Click "Next: Permissions."
7. Search for and select the "LeadEngineersFullAccess" policy.
8. Click "Next: Tags," then "Next: Review."
9. Name the role (e.g., "LeadEngineerRole") and click "Create role."

**For Software Engineers:**

1. Navigate to "Roles" and click "Create role."
2. Choose "AWS account" and "Another AWS account."
3. Enter the AWS Account ID if needed.
4. Click "Next: Permissions."
5. Search for and select the "SoftwareEngineersAccess" policy.
6. Click "Next: Tags," then "Next: Review."
7. Name the role (e.g., "SoftwareEngineerRole") and click "Create role."

**For Interns:**

1. Navigate to "Roles" and click "Create role."
2. Choose "AWS account" and "Another AWS account."
3. Enter the AWS Account ID if needed.
4. Click "Next: Permissions."
5. Search for and select the "InternsReadOnly" policy.
6. Click "Next: Tags," then "Next: Review."
7. Name the role (e.g., "InternRole") and click "Create role."

**For Consultants:**

1. Navigate to "Roles" and click "Create role."
2. Choose "AWS account" and "Another AWS account."
3. Enter the AWS Account ID if needed.
4. Click "Next: Permissions."
5. Search for and select the "ConsultantsAccess" policy.
6. Click "Next: Tags," then "Next: Review."
7. Name the role (e.g., "ConsultantRole") and click "Create role."

**5. Assign Roles to Users**

1. Navigate to "IAM" service.
2. Click on "Users" on the left-hand side.
3. Select the user to assign a role.
4. Click "Add permissions."
5. Choose "Attach policies directly."
6. Search for and select the appropriate role (e.g., "LeadEngineerRole," "SoftwareEngineerRole," "InternRole," "ConsultantRole").
7. Click "Next: Review" and then "Add permissions."

**Summary of Steps**

**Owner:**

1. Sign in to AWS Management Console.
2. Access AWS Organizations.
3. Create the Lead Engineers OU.
4. Move the Lead Engineer's account to the Lead Engineers OU.
5. Create an IAM policy for Lead Engineer permissions.
6. Create a role for the Lead Engineer and attach the policy.
7. Assign the role to the Lead Engineer's account.

**Lead Engineer:**

1. Create remaining OUs: Software Engineers, Interns, Consultants.
2. Move accounts to the appropriate OUs.
3. Create IAM policies for each role.
4. Create IAM roles and attach the corresponding policies.
5. Assign roles to the respective users.