Setting Up AWS Organization and Configuring Member Accounts

This document provides a step-by-step guide to create an AWS Organization, add member accounts, and implement best practices for IAM user creation and permission management.

Prerequisites

1. An AWS account with root access.
2. Administrative privileges in your account.

Step 1: Create an AWS Organization

1. **Sign in to AWS Console**:
    - Log in to the Management Console using your root account credentials.
2. **Navigate to AWS Organizations**:
    - In the AWS Management Console, go to **Services** > **AWS Organizations**.
3. **Create an Organization**:
    - Click **Create an Organization**.
    - Choose **Enable All Features** for maximum functionality.
    - Confirm your choice.
4. **Set up a Management Account**:
    - The account used to create the organization becomes the management account.
    - Ensure MFA (Multi-Factor Authentication) is enabled on the management account.

Step 2: Add Member Accounts

1. **Create or Invite Accounts**:
    - In the AWS Organizations console, click **Accounts** > **Add an account**.
    - Choose one of the following options:
        - **Create Account**: Enter a name and email address for the new account.
        - **Invite Account**: Enter the email address of an existing AWS account.
2. **Accept Invitations**:
    - If inviting an existing account, the account owner must log in to their console and accept the invitation.
3. **Organize Accounts into Organizational Units (OUs)**:
    - Navigate to **Organizational Units** and create OUs.
    - Drag and drop accounts into relevant OUs for better organization.

4. **Apply Service Control Policies (SCPs)**:
    - Use SCPs to define permissions at the organizational or OU level. For more information please visit official documentation for SCP.

Step 3: IAM Users and Permissions Best Practices

1. **Avoid Using Root Account**:
    - Use the root account only for initial setup and emergencies. Enable MFA for the root account.
2. **Create IAM Users**:
    - Go to **IAM** > **Users** > **Add users**.
    - Provide a unique username.
    - Enable **Programmatic Access** if APIs/CLI are needed.
3. **Assign Users to Groups**:
    - Create IAM groups (e.g., Admins, Developers).
    - Attach appropriate policies to groups (e.g., `AdministratorAccess`, `PowerUserAccess`).
4. **Use Policies to Grant Permissions**:
    - Grant the **least privilege** required for tasks.
    - Use AWS-managed policies for standard permissions.
    - Create custom policies if needed.
5. **Enable MFA for IAM Users**:
    - Enforce MFA for all users in critical roles.
6. **Rotate Credentials Regularly**:
    - Implement a policy to rotate passwords and access keys periodically.
7. **Monitor Access**:
    - Use AWS CloudTrail to track account activities.
    - Set up AWS Config to monitor changes to IAM resources.
8. **Restrict Permissions with SCPs**:
    - Use SCPs at the OU level to enforce compliance (e.g., disallow certain regions or services).

Step 4: Implement Governance with AWS Config and CloudTrail

1. **Enable AWS Config**:
    - Navigate to **AWS Config** and set it up for resource tracking.
2. **Enable CloudTrail**:
    - Go to **CloudTrail** > **Create trail**.

- Save logs to an S3 bucket for auditing.

3. **Enable Trusted Access**:
   - Use **AWS Organizations** to enable trusted access for AWS Config and other AWS services.

Additional Best Practices

1. **Tag Resources**:
   - Use tags to track and categorize AWS accounts and resources.
2. **Use Budget Alerts**:
   - Set up AWS Budgets to monitor and control spending across accounts.
3. **Secure Sensitive Accounts**:
   - Apply stricter SCPs to accounts with access to sensitive data or resources.