Task #2 – Account creation, roles, billing, alerting

What to do

Sub-task 1 – Create AWS Account

Follow this link to create account. Note, accounts are usually activated within a few minutes, but the process might take up to 24 hours.

Sub-task 2 – Secure account

Follow general AWS recommendations. Here mentioned some of them, but feel free to read full article (best-practices):

- Lock away your AWS account root user access keys (reference)
- Avoid using AWS account root user
- Grant least privilege
- Use permissions with AWS managed policies
- Configure a strong password policy for your users
- Enable MFA

Sub-task 3 – Set Budgets/Alerts

Avoid surprising charges, so control cost carefully:

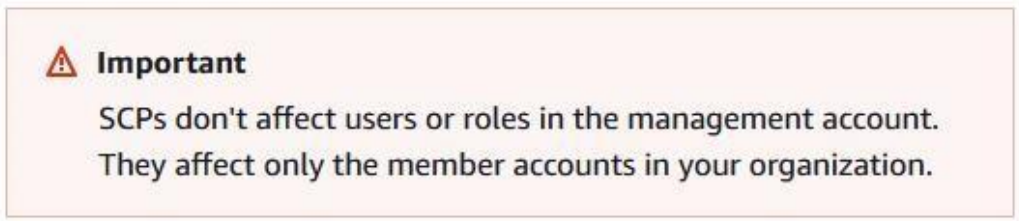
- Setup free tier notifications (link)
- Setup budget reached notifications (ex. 40%, 80%, 100%) manually (via console). Alert should be sent to your email.

** Optional: Setup Budgets using IaaC (Infrastructure as a Code)*

Sub-task 4 – Optional Task - Setup SCP

** Optional Task is not mandatory for completion this module but highly recommended, if you don't have a time to complete it - just skip it*

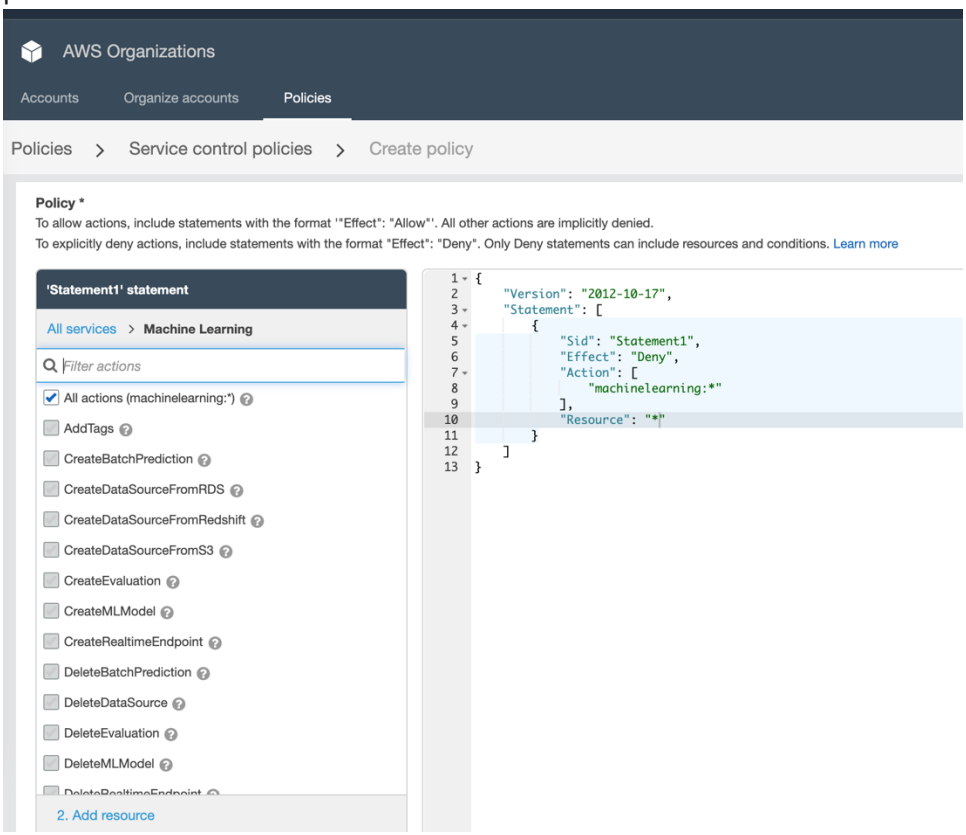
Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. SCPs offer central control over the maximum available permissions for all accounts in your organization.



You can configure the service control policies (SCPs) in your organization to work as either of the following:

- A deny list – actions are allowed by default, and you specify what services and actions are prohibited
- An allow list – actions are prohibited by default, and you specify what services and actions are allowed

Recommended to start from **allow** list (link). Create organization and new policy. Visual editor will help adding necessary statements. You can review Intro and identify usage of which resources should not be prohibited.



To test the applied SCP you could create a member account under your organization.

What should I remember?

1. **Once you create AWS Account -> Setup Multi-factor Authentication**
2. **Do NOT share your account**
3. **Do NOT commit your account Credentials into the Git**
4. **Terminate/Remove all created resources/services once you finish Module**
5. **Please Do not forget to delete NAT Gateway if you used it.**
6. **Do NOT keep instance running if you don't use it**
7. **Carefully keep track of billing and working instances so you don't exceed limits**