IT3061 – Massive Data Processing and Cloud Computing
Year 3, Semester 2
Practical Sheet 7

Cloud Security

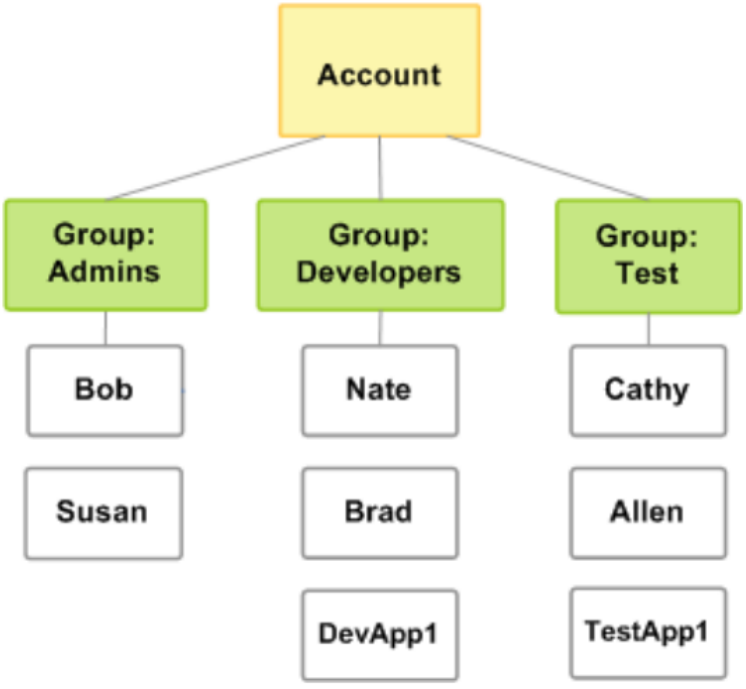
These practical aims to discuss about Security services provided by AWS and Azure.

AWS Identity and Access Management (IAM)

This practical aims how to give access to AWS resources by creating AWS Identity and Access Management (IAM) users in the AWS account.

The first task is to set up an administrators group for your AWS account. (Note - Having an administrators group for your AWS account isn't required, but it is strongly recommend.)

The following figure shows a simple example of an AWS account with three groups. Here one group is for administrators (called Admins). There's also a Developers group and a Test group. Each group has multiple users. Each user can be in more than one group, although the figure doesn't illustrate that. You can't put groups inside other groups. You use policies to grant permissions to groups.



Creating your first IAM admin user and user group

This procedure describes how to use the AWS Management Console to create an IAM user for yourself and add that user to a user group that has administrative permissions from an attached managed policy.

1. Sign in to the IAM console as the account owner by choosing Root user and entering your AWS account email address. On the next page, enter your password.

Note - We strongly recommend that you adhere to the best practice of using the Administrator IAM user below and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.

2. Enable access to billing data for the IAM admin user that you will create as follows:
    a. On the navigation bar, choose your account name, and then choose Account.
    b. Next to IAM User and Role Access to Billing Information, choose Edit. You must be signed in as the root user for this section to be displayed on the account page.
    c. Select the check box to Activate IAM Access and choose Update.
    d. On the navigation bar, choose Services and then IAM under Security, Identity, & Compliance to return to the IAM console.

3. In the navigation pane, choose Users and then choose Add users.

4. On the Details page, do the following:
    a. For Username, type Administrator.
    b. Select the check box for AWS Management Console access, select Custom password, and then type your new password in the text box.
    c. By default, AWS forces the new user to create a new password when first signing in. You can
    d. optionally clear the check box next to User must create a new password at next sign-in to allow the new user to reset their password after they sign in.
    e. Choose Next: Permissions.

5. On the Permissions page, do the following:
    a. Choose Add user to group.
    b. Choose Create group.
    c. In the Create group dialog box, for Group name type Administrators.
    d. Select the check box for the Administrator Access policy.
    e. Choose Create group.

f. Back on the page with the list of user groups, select the check box for your new user group. Choose Refresh if you don't see the new user group in the list.
g. Choose Next: Tags.

6. (Optional) On the Tags page, add metadata to the user by attaching tags as key-value pairs.

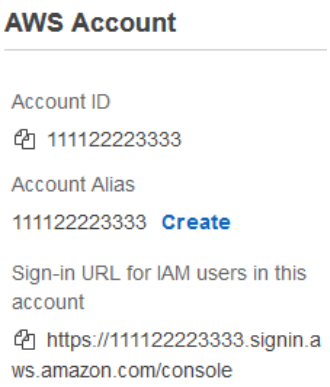
7. Choose Next: Review. Verify the user group memberships to be added to the new user. When you are ready to proceed, choose Create user.

8. (Optional) On the Complete page, you can download a .csv file with login information for the user,or send email with login instructions to the user.

How IAM users sign in to your AWS account

After you create IAM users (with passwords), those users can sign in to the AWS Management Console. To sign in, they need your account ID or alias. They can also sign in from a custom URL that includes your account ID.

You can find the sign-in URL for an account on the Dashboard page in the IAM console.



To create a sign-in URL for your IAM users, use the following pattern:
https://account-ID-or-alias.signin.aws.amazon.com/console

IAM users can also sign in at the following endpoint and enter the account ID or alias manually, instead of using your custom URL:
https://signin.aws.amazon.com/console

Use the following link to learn more about this service.

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Azure Active Directory

This service allows users to securely control access to services and resources while offering data security and protection. Create and manage users and groups and use permissions to allow and deny access to resources.

Use the following link to learn more about this service.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

Azure Role-Based Access Control (RBAC)

Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Use the following link to learn more about this service.

https://docs.microsoft.com/en-us/azure/role-based-access-control/check-access