

Hands-on exercises for Amazon Web Services Architect Associate Certification Course

Page #	Exercises
	First Steps
4	Exercise 1:The Root Account
4	Exercise 2:IAM Users and Groups
6	Exercise 3:Policy Simulator
6	Exercise 4:Password Policy
7	Exercise 5:Inline Policy
7	Exercise 6:Setup MFA
8	Exercise 7:Setup RDS
9	Exercise 8:Setup MYSQL
9	Exercise 9:Dynamo DB
9	Exercise 10:Load Balancer
9	Exercise 11:Auto Scaling
9	Exercise 12:CloudFront
10	Exercise 13:CloudWatch
10	Exercise 14:CloudTrail
10	Exercise 15:Trusted Advisor

First Step: In order to do these exercise's, you will need a Amazon Web Services account. And you can get a free account that you can access pretty well all AWS services for one year. Take a look here at this URL:

<https://aws.amazon.com/free/>

They will ask for a credit card, don't worry they won't charge you, follow the easy steps and you will be all set.

Documentation: there are lots of resources in your Oreilly Safari subscription. However there will be times you will need to look at the Amazon documentation as things change quickly at AWS. Here is the AWS master documentation link.

<https://aws.amazon.com/documentation/>

If you have a Kindle, you can also get lots of documentation in Kindle format by going to Amazon.com and searching for AWS content.

If you don't have a Kindle you can read your Kindle content using the Amazon cloud reader. That link is here:

<https://www.amazon.com/kindlecloudreader>

Exercise 1: The Root Account

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Security, Identity, and Compliance open IAM
3. Since you are using the master account for your free AWS account, you are using the Root account. The root account is not controlled by IAM. In the middle of the screen take a look at your security status. Since this is your root account, you may have five warning signs.
4. Take some time and review each of the security problems by expanding each option.
5. In the top right-hand corner click your name, and from the drop-down menu select My Security Credentials.
6. You should receive a warning, indicating that you are using the root account, and it's a best practice to use IAM. All of the options under Your Security Credentials are worthy exploring for security knowledge and for the certification test.

Exercise 2: IAM Users and Groups

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Security, Identity, and Compliance open IAM
3. On the left-hand side select Users.
4. Click Add user.
5. Enter your first name for username.
6. Under AWS Access type select both checkboxes. Take a minute and view what you are allowing by selecting both of these options.
7. Click Next:Permissions
8. Review the permissions and options that you could choose, then click Next:Review

9. Under Permissions summary, note the single managed policy that will be assigned to your new user account once created.
10. Click Create user.
11. Download the .csv file containing your security credentials for the new user. Pay careful attention to the note under Success
12. Once you've downloaded your credentials click Close.
13. Select the user account you just created and review the details for the account.
14. Click Groups
15. Click Create New Group
16. For Group Name enter Admins and click Next Step
17. On the Attach Policy screen scroll down and select AdministratorAccess
18. Click Next Step
19. Click Create Group
20. Select, and click the group you just created
21. On the Permissions tab and review the managed policy attached to this group.
22. Click the Users tab
23. Click Add Users to Group
24. Add the user account you created earlier in this exercise
25. On the left-hand side click dashboard
26. Copy the IAM users sign in link and login to AWS.
27. You will have to change your password of course
28. You have now logged in as an IAM user that has been assigned administrative access

Exercise 3: Policy Simulator

1. Log into the AWS console using your credentials for your free AWS account
2. On the right-hand side under Additional information, click the link Policy Simulator
3. On the left-hand side, click your username. Note the policies that have been assigned to your account
4. In the middle of the screen under Policy Simulator click Select service.
5. Locate and select a Service
6. Click Select All
7. Review the actions available
8. Click Run Simulation and review the permissions that are allowed or denied, depending on the service that you select

Exercise 4: Password Policy


1. Log into the AWS console using your credentials for your free AWS account.
2. Under Security, Identity, and Compliance open IAM
3. On the left-hand side select Account settings
4. Note the options that you could adjust to define a Password Policy for your IAM users
5. If you wish you can make changes to the existing password policy and then click Apply password policy

Exercise 5: Inline Policy

1. Log into the AWS console using your credentials for your free AWS account
2. Under Security, Identity, and Compliance open IAM
3. On the Permissions tab to the right, select Add in-line policy
4. Under Policy Generator, to the right, click Select
5. This is where you would select the service that was to be part of your policy
6. Select the actions, and enter the resource name the ARN.
7. For more details take a look at the link below:

http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#inline-policies

Exercise 6: Setup MFA

1. Log into the AWS console using your credentials for your free AWS account.
2. On the left choose Users
3. Choose the name of the intended MFA user
4. Click the Security credentials tab. Next to Assigned MFA device, choose the edit icon 
5. Choose A virtual MFA device, and then choose Next Step
6. At this point you would need to have already installed, a virtual MFA application such as Google Authenticator
7. For additional steps take a look at the link below

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html

Exercise 7: Setup RDS

To do this exercise, you need two private subnets in a VPC with each subnet in a different availability zone.

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Database select RDS
3. Click Get Started Now
4. Note the six DB engines choices available
5. Select PostgreSQL
6. Review the features and then click Select
7. Note the options for Production and Dev / Test
8. Select Dev/Test and click Next Step
9. Review the Instance Specifications for DB Instance class and select db.t2.micro
10. For Multi-AZ Deployment select Yes
11. For DB Instance Identifier enter Dev
12. For Master Username enter your first name
13. For Passwords enter dbpassword
14. Click Next Step
15. Under Network and Security select a VPC, and a Security Group
16. Change Publicly Accessible to No
17. Under Database Options enter a Database Name
18. Under Backup review the Backup Retention Period
19. Under Maintenance review the options for version upgrades, and Maintenance Window.
20. Click Launch DB Instance
21. In a few seconds, click View Your DB Instances
22. Take some time to review your options under Show Monitoring, and Instance Actions
23. When have finished reviewing, click Instance Actions and delete your Instance

Exercise 8: Setup MYSQL

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Database select RDS
3. Click Get Started Now, or Launch a DB Instance
4. Follow the steps for Exercise 7 as a guide

Exercise 9: Dynamo DB

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Database select DynamoDB
3. Under Additional Resources click Getting started hands-on lab.
4. This will launch a free Quick Labs

https://qwiklabs.com/searches/lab?keywords=introduction%20to%20amazon%20dynamodb&utm_source=ddbconsole&utm_medium=link&utm_campaign=ddbconsole

Exercise 10: Load Balancer

1. Use this tutorial from AWS

<http://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-network-load-balancer.html>

Exercise 11: Auto Scaling

1. Use this tutorial from AWS

<http://docs.aws.amazon.com/autoscaling/latest/userguide/create-asg.html>

Exercise 12: CloudFront

1. Head over to Quick Labs and create a free account

<https://run.qwiklab.com/searches/lab?keywords=introduction&qlcampaign=intro-labs-sm>

Exercise 13: CloudWatch

1. Head over to Quick Labs and create a free account.

<https://run.qwiklab.com/searches/lab?keywords=introduction&qlcampaign=intro-labs-sm>

Exercise 14: CloudTrail

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Management Tools, select CloudTrail
3. Review the API calls that have been made on your account
4. Click View trails
5. Read the information under Trails, then click Create trail
6. Enter Trail name
7. Scroll down to Storage location
8. Optionally create a new S3 bucket for your new Trail.
9. Review all other options before clicking Create

Exercise 15: Trusted Advisor

1. Log into the AWS console using your credentials for your free AWS account.
2. Under Management Tools click Trusted Advisor
3. After Trusted Advisor completes its checks review the Recommended Actions
4. On the left select each option and review the findings
5. On the left, click Preferences, and review the available options