


Assignment sheet for IAM

Assignment 1:- Create an IAM user with the username of your own wish and grant administrator policy.

User ARN `arn:aws:iam::008129116151:user/deepakv` 



Path `/`

Creation time 2022-10-29 19:01 UTC+0530

Permissions Groups Tags Security credentials Access Advisor


▼ Permissions policies (1 policy applied)

[Add permissions](#) [+ Add inline policy](#)

Policy name ▼	Policy type ▼
Attached directly	
▼  AdministratorAccess	AWS managed policy 

Assignment 2:- Hello students, in this assignment you need to prepare a developers team of avengers.

- Create 3 IAM users of avengers and assign them in developer's groups with IAM policy.

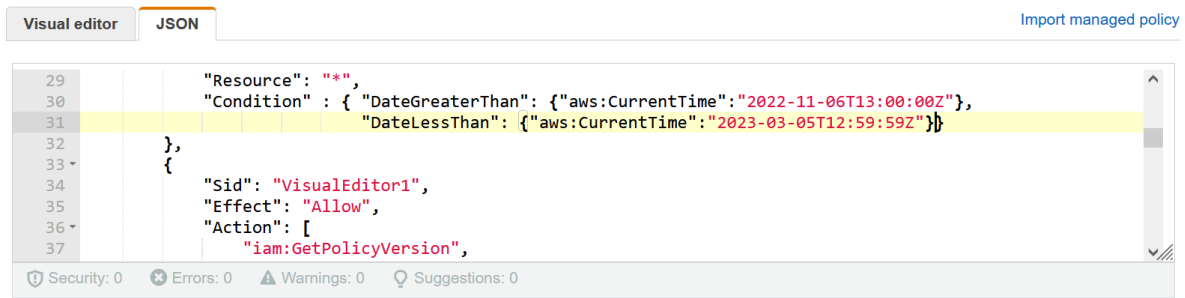
<input type="checkbox"/>	User name 	Groups	Last activity ▼	Creation time
<input type="checkbox"/>	hulk	1	None	Yesterday
<input type="checkbox"/>	thor	1	None	Yesterday
<input type="checkbox"/>	ironman	1	None	Yesterday

Assignment 3:- Define a condition in policy for expiration like

"DateGreaterThan": {"aws:CurrentTime":
"2020-04-01T00:00:00Z"},

"DateLessThan": {"aws:CurrentTime":
"2020-06-30T23:59:59Z"}

Define the span of 4 months as per your wish



```
29     "Resource": "*",
30     "Condition": {
31         "DateGreaterThan": {"aws:CurrentTime": "2022-11-06T13:00:00Z"},
32         "DateLessThan": {"aws:CurrentTime": "2023-03-05T12:59:59Z"}
33     },
34     {
35         "Sid": "VisualEditor1",
36         "Effect": "Allow",
37         "Action": [
38             "iam:GetPolicyVersion",
39         ]
40     }
41 }
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Assignment 3:- Prepare 15 authentic MCQ questions related to IAM..

Q1: An explicit Deny in IAM precedes an explicit allow?

Options: a>True b>False

Q2: Which of the following sections in a policy specifies the entities to whom access to a resource is granted or denied?

Options: a>Statement ID b>Resources c>Principal d>Conditions

Q3: Which of the following is not an IAM best practice?

Options: a>Delete user accounts, not in use b>Attach policies to individual users
c>Manage permissions by adding users to groups d>Enable MFA on user accounts

Q4: Which of the following set of credentials are used to log in to AWS programmatically? (Choose two)

Options: a>Username b>Access Key c>Password d>Secret Key

Q5: Which statement best describes IAM?

Options: a>IAM stands for Improvised Application Management, and it allows you to deploy and manage applications in the AWS Cloud.
b> IAM allows you to manage users, groups, roles, and their corresponding level of access to the AWS Platform.
c> IAM allows you to manage users' passwords only. AWS staff must create new users for your organization. This is done by raising a ticket.
d> IAM allows you to manage permissions for AWS resources only.

Q6: You have created a new AWS account for your company, and you have also configured multi-factor authentication on the root account. You are about to create your new users. What strategy should you consider in order to ensure that there is good security on this account?

Options: a> Require users to only be able to log in using biometric authentication.
b> Give all users the same password so that if they forget their password they can just ask their co-workers.

- c> Restrict login to the corporate network only.
- d> Enact a strong password policy: user passwords must be changed every 45 days, with each password containing a combination of capital letters, lowercase letters, numbers, and special symbols.

Q7: Using SAML (Security Assertion Markup Language 2.0), you can give your federated users single sign-on (SSO) access to the AWS Management Console.
Options: a> False b> True

Q8: Which of the following is not a component of IAM?
Options: a>Roles b>Users c>Organizational Units d>Groups

Q9: A new employee has just started work, and it is your job to give her administrator access to the AWS console. You have given her a username, an access key ID, and a secret access key, and you have generated a password for her. She is now able to log in to the AWS console, but she is unable to interact with any AWS services. What should you do next?
Options: a>Ensure she is logging in to the AWS console from your corporate network and not the normal internet.
b>Grant her Administrator access by adding her to the Administrators' group.
c>Tell her to log out and try logging back in again.
d>Require multi-factor authentication for her user account.

Q10: Which of the following is not a feature of IAM?
Options: a>IAM allows you to set up biometric authentication so that no passwords are required.
b>IAM offers fine-grained access control to AWS resources.
c>IAM offers centralized control of your AWS account.
d>IAM integrates with existing active directory accounts allowing single sign-on.

Q11: You are a security administrator working for a hotel chain. You have a new member of staff who has started as a systems administrator, and she will need full access to the AWS console. You have created the user account and generated the access key id and the secret access key. You have moved this user into the group where the other administrators are, and you have provided the new user with their secret access key and their access key id. However, when she tries to log in to the AWS console, she cannot. Why might that be?
Options: a>Your user is trying to log in from the AWS console from outside the corporate network. This is not possible.
b>You have not yet activated multi-factor authentication for the user, so by default, they will not be able to log in.
c>You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this password and your organization's unique AWS console login URL.
d>You have not applied the "log in from console" policy document to the user. You must apply this first so that they can log in.

Q12: You are a developer at a fast-growing start-up. Until now, you have used the root account to log in to the AWS console. However, as you have taken on more staff, you will now need to stop sharing the root account to prevent accidental damage to your AWS infrastructure. What should you do so that everyone can access the AWS resources they need to do their jobs? (Choose 2)

Options: a>Create individual user accounts with minimum necessary rights and tell the staff to log in to the console using the credentials provided.

b>Give your users the root account credentials so that they can also sign in.

c>Create a customized sign-in link such as

"yourcompany.signin.aws.amazon.com/console" for your new users to use to sign in with. d>Create an additional AWS root account for each new user.

Q13: What is an additional way to secure the AWS accounts of both the root account and new users alike?

Options: a>Implement Multi-Factor Authentication for all accounts.

b>Store the access key id and secret access key of all users in a publicly accessible plain text document on S3 of which only you and members of your organization know the address to.

c>Configure the AWS Console so that you can only log in to it from your internal network IP address range.

d>Configure the AWS Console so that you can only log in to it from a specific IP Address range

Q14: IAM group:

a>Is the same as IAM users

b>Can be used to specify permissions for a collection of users

c>Is truly an identity

d>All of these

Q15: IAM role:

a>Have credentials (password or access keys) associated with it

b>Does not have any credentials (password or access keys) associated with it

c>May or may not have credentials (password or access keys) associated with it

d>None of these

Solution of MCQs: 1b-2b-3b-4-5b-6d-7b-8c-9b-10a-11c-12a&c-13a-14b-15b

Assignment 4:- Launch your Linux instance in IAM and update your machine.

EC2 > Instances > i-0074492ade4bf797c

Instance summary for i-0074492ade4bf797c (testing server) [Info](#)

Command used to update machine:

sudo apt-get update

sudo apt-get dist-upgrade

```
aws Services Search
EC2

System information as of Sun Nov  6 04:32:26 UTC 2022

System load: 0.00146484375    Processes:           100
Usage of /:  30.4% of 7.57GB  Users logged in:    0
Memory usage: 23%            IPv4 address for eth0: 172.31.18.128
Swap usage:   0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

0 updates can be applied immediately.

*** System restart required ***
Last login: Sat Nov  5 13:44:07 2022 from 18.206.107.27
ubuntu@ip-172-31-18-128:~$
```