IAM Quiz

Which service enables AWS customers to manage users and permissions in AWS?

1. Amazon Cognito
2. AWS Identity and Access Management (IAM)
3. AWS Identity Manager (AIM)
4. AWS Directory Service

Which service enables AWS customers to manage users and permissions in AWS?

1. Amazon Cognito
2. **AWS Identity and Access Management (IAM)**
3. AWS Identity Manager (AIM)
4. AWS Directory Service

Every user you create in the IAM system starts with which permission.

1. Partial permissions
2. Full permissions
3. No permissions

Every user you create in the IAM system starts with which permission.

1. Partial permissions
2. Full permissions
3. **No permissions**

Which of the following should you do to secure your AWS root user? (Select TWO.)

A. Assign the root user to the “admins” IAM group.

B. Use the root user for day-to-day administration tasks.

C. Enable MFA.

D. Create a strong password.

Which of the following should you do to secure your AWS root user? (Select TWO.)

A. Assign the root user to the “admins” IAM group.

B. Use the root user for day-to-day administration tasks.

C. Enable MFA.

D. Create a strong password.

How does multi-factor authentication work?

A. Instead of an access password, users authenticate via a physical MFA device.

B. In addition to an access password, users also authenticate via a physical MFA device.

C. Users authenticate using tokens sent to at least two MFA devices.

D. Users authenticate using a password and also either a physical or virtual MFA device.

How does multi-factor authentication work?

A. Instead of an access password, users authenticate via a physical MFA device.

B. In addition to an access password, users also authenticate via a physical MFA device.

C. Users authenticate using tokens sent to at least two MFA devices.

D. **Users authenticate using a password and also either a physical or virtual MFA device.**

What is an IAM role?

A. A set of permissions allowing access to specified AWS resources

B. A set of IAM users given permission to access specified AWS resources

C. Permissions granted a trusted entity over specified AWS resources

D. Permissions granted an IAM user over specified AWS resources

What is an IAM role?

A. A set of permissions allowing access to specified AWS resources

B. A set of IAM users given permission to access specified AWS resources

C. Permissions granted a trusted entity over specified AWS resources

D. Permissions granted an IAM user over specified AWS resources

After creating a new IAM user which of the following must be done before they can successfully make API calls?

1. Add a password to the user.
2. Enable Multi-Factor Authentication for the user.
3. Assign a Password Policy to the user.
4. Create a set of Access Keys for the user

After creating a new IAM user which of the following must be done before they can successfully make API calls?

1. Add a password to the user.
2. Enable Multi-Factor Authentication for the user.
3. Assign a Password Policy to the user.
4. **Create a set of Access Keys for the user**

Within the IAM service a GROUP is considered as a:

1. A collection of AWS accounts
2. It’s the group of EC2 machines that gain the permissions specified in the GROUP.
3. There’s no GROUP in IAM, but only USERS and RESOURCES.
4. A collection of users.

Within the IAM service a GROUP is considered as a:

1. A collection of AWS accounts
2. It’s the group of EC2 machines that gain the permissions specified in the GROUP.
3. There’s no GROUP in IAM, but only USERS and RESOURCES.
4. **A collection of users.**

An organization has 100 employees. The organization wants to set up AWS access for each department. Which of the below mentioned options is a possible solution?

1. Create IAM roles based on the permission and assign users to each role
2. Create IAM users and provide individual permission to each
3. Create IAM groups based on the permission and assign IAM users to the groups
4. It is not possible to manage more than 100 IAM users with AWS

An organization has 100 employees. The organization wants to set up AWS access for each department. Which of the below mentioned options is a possible solution?

1. Create IAM roles based on the permission and assign users to each role
2. Create IAM users and provide individual permission to each
3. **Create IAM groups based on the permission and assign IAM users to the groups**
4. It is not possible to manage more than 100 IAM users with AWS

You are setting up a blog on AWS. In which of the following scenarios will you need AWS credentials? (Choose 3)

1. Sign in to the AWS management console to launch an Amazon EC2 instance
2. Sign in to the running instance to instance some software
3. Launch an Amazon RDS instance
4. Log into your blog's content management system to write a blog post
5. Post pictures to your blog on Amazon S3

You are setting up a blog on AWS. In which of the following scenarios will you need AWS credentials? (Choose 3)

1. **Sign in to the AWS management console to launch an Amazon EC2 instance**
2. Sign in to the running instance to instance some software
3. **Launch an Amazon RDS instance**
4. Log into your blog's content management system to write a blog post
5. **Post pictures to your blog on Amazon S3**

Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which two IAM best practices should you consider implementing? Choose 2 answers

1. Create individual IAM users for everyone in your organization
2. Configure MFA on the root account and for privileged IAM users
3. Assign IAM users and groups configured with policies granting least privilege access
4. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate

Your organization is preparing for a security assessment of your use of AWS. In preparation for this assessment, which two IAM best practices should you consider implementing? Choose 2 answers

1. Create individual IAM users for everyone in your organization
2. **Configure MFA on the root account and for privileged IAM users**
3. **Assign IAM users and groups configured with policies granting least privilege access**
4. Ensure all users have been assigned and are frequently rotating a password, access ID/secret key, and X.509 certificate