1. Which service enables AWS customers to manage users and permissions in AWS?
   1. AWS Access Control Service (ACS)
   2. **AWS Identity and Access Management (IAM)**
   3. AWS Identity Manager (AIM)
2. IAM provides several policy templates you can use to automatically assign permissions to the groups you create. The \_\_\_\_\_ policy template gives the Admins group permission to access all account resources, except your AWS account information
   1. Read Only Access
   2. Power User Access
   3. AWS Cloud Formation Read Only Access
   4. **Administrator Access**
3. Every user you create in the IAM system starts with \_\_\_\_\_\_\_\_\_.
   1. Partial permissions
   2. Full permissions
   3. **No permissions**
4. Groups can’t \_\_\_\_\_.
   1. be nested more than 3 levels
   2. **be nested at all**
   3. be nested more than 4 levels
   4. be nested more than 2 levels
5. The \_\_\_\_\_ service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console.
   1. Amazon RDS
   2. AWS Integrity Management
   3. **AWS Identity and Access Management**
   4. Amazon EMR
6. An AWS customer is deploying an application that is composed of an AutoScaling group of EC2 Instances. The customers security policy requires that every outbound connection from these instances to any other service within the customers Virtual Private Cloud must be authenticated using a unique x.509 certificate that contains the specific instanceid. In addition an x.509 certificates must be designed by the customer’s Key management service in order to be trusted for authentication. Which of the following configurations will support these requirements?
   1. Configure an IAM Role that grants access to an Amazon S3 object containing a signed certificate and configure the Auto Scaling group to launch instances with this role. Have the instances bootstrap get the certificate from Amazon S3 upon first boot.
   2. Embed a certificate into the Amazon Machine Image that is used by the Auto Scaling group. Have the launched instances generate a certificate signature request with the instance’s assigned instance-id to the Key management service for signature.
   3. **Configure the Auto Scaling group to send an SNS notification of the launch of a new instance to the trusted key management service. Have the Key management service generate a signed certificate and send it directly to the newly launched instance.**
   4. Configure the launched instances to generate a new certificate upon first boot. Have the Key management service poll the AutoScaling group for associated instances and send new instances a certificate signature that contains the specific instance-id.
7. When assessing an organization AWS use of AWS API access credentials which of the following three credentials should be evaluated? Choose 3 answers
   1. Key pairs
   2. **Console passwords**
   3. **Access keys**
   4. **Signing certificates**
   5. Security Group memberships (required for EC2 instance access)
8. An organization has created 50 IAM users. The organization wants that each user can change their password but cannot change their access keys. How can the organization achieve this?
   1. The organization has to create a special password policy and attach it to each user
   2. The root account owner has to use CLI which forces each IAM user to change their password on first login
   3. By default each IAM user can modify their passwords
   4. **Root account owner can set the policy from the IAM console under the password policy screen**
9. An organization has created 50 IAM users. The organization has introduced a new policy which will change the access of an IAM user. How can the organization implement this effectively so that there is no need to apply the policy at the individual user level?
   1. **Use the IAM groups and add users as per their role to different groups and apply policy to group**
   2. The user can create a policy and apply it to multiple users in a single go with the AWS CLI
   3. Add each user to the IAM role as per their organization role to achieve effective policy setup
   4. Use the IAM role and implement access at the role level
10. Your organization’s security policy requires that all privileged users either use frequently rotated passwords or one-time access credentials in addition to username/password. Which two of the following options would allow an organization to enforce this policy for AWS users? Choose 2 answers
    1. **Configure multi-factor authentication for privileged IAM users**
    2. **Create IAM users for privileged accounts (**can set password policy**)**
    3. Implement identity federation between your organization’s Identity provider leveraging the IAM Security Token Service
    4. Enable the IAM single-use password policy option for privileged users (no such option the password expiration can be set from 1 to 1095 days)
11. 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
12. A company needs to deploy services to an AWS region which they have not previously used. The company currently has an AWS identity and Access Management (IAM) role for the Amazon EC2 instances, which permits the instance to have access to Amazon DynamoDB. The company wants their EC2 instances in the new region to have the same privileges. How should the company achieve this?
    1. Create a new IAM role and associated policies within the new region
    2. **Assign the existing IAM role to the Amazon EC2 instances in the new region**
    3. Copy the IAM role and associated policies to the new region and attach it to the instances
    4. Create an Amazon Machine Image (AMI) of the instance and copy it to the desired region using the AMI Copy feature
13. 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**
14. An organization is planning to create a user with IAM. They are trying to understand the limitations of IAM so that they can plan accordingly. Which of the below mentioned statements is not true with respect to the limitations of IAM?
    1. **One IAM user can be a part of a maximum of 5 groups** (Refer [link](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html))
    2. Organization can create 100 groups per AWS account
    3. One AWS account can have a maximum of 5000 IAM users
    4. One AWS account can have 250 roles
15. Within the IAM service a GROUP is regarded 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.**
16. Is there a limit to the number of groups you can have?
    1. Yes for all users except root
    2. No
    3. Yes unless special permission granted
    4. **Yes for all users**
17. What is the default maximum number of MFA devices in use per AWS account (at the root account level)?
    1. **1**
    2. 5
    3. 15
    4. 10
18. When you use the AWS Management Console to delete an IAM user, IAM also deletes any signing certificates and any access keys belonging to the user.
    1. FALSE
    2. This is configurable
    3. **TRUE**
19. 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 (needs ssh keys)
    3. **Launch an Amazon RDS instance**
    4. Log into your blog’s content management system to write a blog post (need to authenticate using blog authentication)
    5. **Post pictures to your blog on Amazon S3**
20. An organization has 500 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
21. An organization has hosted an application on the EC2 instances. There will be multiple users connecting to the instance for setup and configuration of application. The organization is planning to implement certain security best practices. Which of the below mentioned pointers will not help the organization achieve better security arrangement?
    1. Apply the latest patch of OS and always keep it updated.
    2. **Allow only IAM users to connect with the EC2 instances with their own secret access key**. (Refer [link](http://aws.amazon.com/articles/1233/))
    3. Disable the password-based login for all the users. All the users should use their own keys to connect with the instance securely.
    4. Create a procedure to revoke the access rights of the individual user when they are not required to connect to EC2 instance anymore for the purpose of application configuration.