IAM and Security

1. You have been asked by your employer to create an identical copy of your production environment in another Region for disaster recovery purposes. In the list below, which AWS resources would you NOT need to recreate, because they are available universally across the console? [Select 2]
   1. Route53, IAM Roles, ELB, EC2Key Pairs, SG.
2. You are a solutions architect working for a construction company. Your company is migrating their production estate to AWS, and you are in the process of setting up access to the AWS console using Identity Access Management (IAM). You have created 15 users for your system administrators. What further steps do you need to take to enable your system administrators to get access to the AWS console in a secure fashion? [Select 2]
   1. Give the system administrators the secret access key and access key id, and tell them to use these credentials to log in to the AWS console.
   2. Get the system administrator to download the cli and configure this on their laptop, using their user names and passwords.
   3. Generate a password for each user and give these passwords to your system administrators.
   4. Have each user setup MFA once they have logged into the console.
3. You are working in the media industry, and you have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security.
   1. Save the API credentials locally in each EC2 instance.
   2. Get the API credentials using the EC2 instance user data.
   3. Save your API credentials in a public GitHub repository.
   4. Don’t save your credentials, instead create a role in IAM and assign this role to an EC2 instance when you first create it.
4. Your company has asked you to investigate the use of KMS for storing and managing keys in AWS. From the options listed below, what key management features are available in KMS?
   1. Generate keys, disable and re-enable keys and import keys into a custom key store.
   2. Generate keys, disable and delete keys operate as a private, native hardware security module(HSM)
   3. Import your own keys, disable and re-enable keys and migrate keys between the default KMS key store and a custom key store.
   4. Import your own keys, disable and re-enable keys and define key management roles in IAM.
5. You are a developer at a fast-growing startup. 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 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? [Select 2]
   1. Create an additional AWS root account for each user.
   2. Give your users and root account credentials so that they can also sign in.
   3. Create individual user accounts with minimum necessary rights and tell the staff to login to the console using the credentials provided.
   4. Create a customized sign-in link such as “yourcompany.signin.aws.amazon.com/console” for your new users to use to sign in with.
6. When editing permissions (policies and ACLs), to whom does the concept of the "Owner" refer?
   1. There is no special concept of owner in AWS
   2. The owner is IAM role used to create the object via the CUI, CLI or API
   3. Owner refers to the identity and email address used to create the AWS account
   4. The owner is the IAM user who created the object via GUI, CLI, or API
7. A company allows its developers to attach existing IAM policies to existing IAM roles to enable faster experimentation and agility. However, the security operations team in concerned that the developers could attach the existing administrator policy, which would allow the developers to circumvent any other security policies.
   1. Create an SNS topic to send an alert every time a developer creates a new policy.
   2. User service control policies to disable IAM activity across all accounts in the organizational unit.
   3. Prevent the developers from attaching any policies and assign all IAM duties to the security operations team.
   4. Set an IAM permissions boundary to the developer IAM role that explicitly denies attaching the administrator policy.
8. The principal element of an IAM policy refers to the specific entry that should be allowed or denied permission, whereas the translates to everyone except the specified entity.
   1. NotPrincipal
   2. Vendor
   3. Principal
   4. Action.
9. What is the default maximum number of Access Keys per user?

A. 10

B. 15

C. 2

D. 20

|  |  |  |
| --- | --- | --- |
| No | Answer | Explanation |
| 1 | A,B | EC2 Key Pairs, Security Groups, and ELBs are region-specific |
| 2 | C,D | You should generate a password for each user and give these passwords to your system administrators. You should then have each user set up multi factor authentication once they have been able to log in to the console. You cannot use the secret access key and access key id to log in to the AWS console; rather, these credentials are used to call Amazon API’s. |
| 3 | D |  |
| 4 | D | There are many features which are native to the KMS service. However, of the above, only import your own keys, disable and re-enable keys and define key management roles in IAM are valid. Importing keys into a custom key store and migrating keys from the default key store to a custom key store are not possible. Lastly operating as a private, native HSM is a function of CloudHSM and is not possible directly within KMS |
| 5 | C, D |  |
| 6 | C |  |
| 7 | D | The permissions boundary for an IAM entity sets the maximum permissions that the entity can save. This can change the effective permissions for that user or role. The effective permissions for an entity are the polices that are granted by all the policies that affect the user or role. |
| 8 | A |  |
| 9 | c |  |
|  |  |  |





