

IAM Assignment Doc

1. 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
 - a) Read Only Access
 - b) Power User Access
 - c) AWS Cloud Formation Read Only Access
 - d) Administrator Access
2. IAM's Policy Evaluation Logic always starts with a default _____ for every request, except for those that use the AWS account's root security credentials
 - a) Permit
 - b) Deny
 - c) Cancel
3. Using Amazon IAM, can I give permission based on organizational groups?
 - a) Yes but only in certain cases
 - b) No
 - c) Yes always
4. In regards to IAM you can edit user properties later, but you cannot use the console to change the _____.
 - a) user name
 - b) password
 - c) default group
5. 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.
 - a) FALSE
 - b) This is configurable
 - c) TRUE
6. Every user you create in the IAM system starts with _____.
 - a) Full permissions
 - b) no permissions
 - c) partial permissions
7. Within the IAM service a GROUP is regarded as a:
 - a) A collection of AWS accounts
 - b) It's the group of EC2 machines that gain the permissions specified in the GROUP.
 - c) There's no GROUP in IAM, but only USERS and RESOURCES.

d) A collection of users.

IAM Tasks

1. Create a 5 users and assign following permission, note that any change in single policy must affect all users
 - a. S3FullAccess
 - b. EC2ReadAccess
 - c. RDSFullAccess
 - d. CloudFormationFullAccess
2. Create a role that allows EC2 to have Full Access of S3
3. Create a User name "John", then create a policy will following permissions
 - a. S3 list all buckets
 - b. Read only access to EC2And attach this policy to user John.
4. Create a user and copy the existing policies from above user John.
5. Design a password policy based on the following configuration
 - a. Password length - > 8
 - b. One uppercase letter
 - c. One numeric character
 - d. Password expiration period set to 30 days