IDENTITY & ACCESS MANAGEMENT

Source: https://www.cloudconformity.com/conformity-rules/IAM/

1.1 Avoid the use of root account => Never use root account for day to day operations.

1.2 Use MFA for all user accounts that have password => Enable Multi Factor Authentication for every user

1.3 Ensure credentials inactive for 90 days or greater are disabled

- AWSCLI command "**aws iam list-users**" will give you PasswordLastUsed date and time to find the accounts. Also command "**aws iam list-access-keys <username>**" will give the user's AccessKeyMetaData in an array. If the array is empty and PasswordLastUsed is more than 90 days, account can be disabled immediately. AccessKeyMetaData array empty means user is not enabled for API access.

1.4 Ensure Access Keys are rotated every 90 days or less

- To rotate access keys, you should follow these steps:

1. Create a second access key in addition to the one in use.
2. Update all your applications to use the new access key and validate that the applications are working.
3. Change the state of the previous access key to inactive.
4. Validate that your applications are still working as expected.
5. Delete the inactive access key.

- "aws iam list-access-keys --user-name Alice" => gives AccessKeyMetadata for user Alice which gives output as User Name, Status, Create date and AccessKeyId.
- Now create new access key using: "aws iam create-access-key --user-name Alice" will give you User Name, Status, Creation Date, SecretAccessKey and AccessKeyId.
- Now If you use command "aws iam list-access-keys --user-name Alice" to list AccessKeyMetadata, it will display two arrays with two key details.
- Now distribute the new key across all the applications and ensure all the applications are working fine
- Finally disable the old key using command : "aws iam update-access-key --access-key-id AKIAI44QH8DHBEXAMPLE --status Inactive --user-name Alice"
- Verify once again the keys for user Alice. Old key should be inactive now: use the command: "aws iam list-access-keys --user-name Alice"
- Validate still the applications are working as expected.
- Now dételé the inactive access key using command: "aws iam delete-access-key --access-key-id AKIAI44QH8DHBEXAMPLE --user-name Alice" . This operation is irreversible. If you delete the key, you cannot restore back.
- Finally once again check the keys for user Alice. It should show only one key which is new and active. Use the command: "aws iam list-access-keys --user-name Alice"

1.5 to 1.11 are Password Policy Settings:
IAM=> Account Settings => Password Policy => Change password policy

1.12 There should be no root account access key exists. Means never enable API access for root account. Check the key for root account using the command: "**aws iam list-access-keys root**" and this should return empty AccessKeyMetadata array.

1.13 Ensure MFA is enabled for the root account

1.14 Ensure security questions are registered in the AWS account

- Go to AWS management console => AWS accounts settings page at https://console.aws.amazon.com/billing/home?#/account/ => Scroll down to Configure Security Challenge Questions and enable them

1.15 Ensure IAM policies are attached only to groups or roles

- Attach policies to groups/roles instead directly to user accounts

1.16 Maintain Current contact details

- Go to My Account => Contact Information => Edit/Update the information

1.17 Ensure Security contact information is registered

- Go to My Account =>Alternate Contacts=> Update Billing/Operations/Security Contact details

1.18 Ensure IAM instance roles are used for AWS resource access from instances

1.19 Ensure a support role has been created to manage incidents with AWS Support

- https://docs.aws.amazon.com/awssupport/latest/user/getting-started.html#accessing-support
- https://gsl.dome9.com/D9.AWS.IAM.25.html

1.20 Do not setup access keys during initial user setup for all IAM users that have a console password

1.21 Ensure IAM policies that allow full "*:*" administrative privileges are not created Proprietary