**AWS CLOUDSHELL**

It is an alternative to using the terminal to issue commands against AWS.

So cloud shell is this icon right here on the top right corner of your screen.

And if you don't see it, just make sure you check out the clutch shell availability regions because it's not available everywhere.

So we have cloud shell in here and within cloud shell you could take a minute maybe to launch your environment. You can issue commands.

For example, you can issue the AWS commands.

cloud shell is basically a terminal in the cloud of AWS.

That's free to use.

Whenever we issue some command on the cloudshell it is going to make an API call using the account credentials.The api call is region specific but using cloudshell it is going to be the region we are currently logged into.

Okay. So the cool thing about cloud shell is

that whenever you are using the CLI, so for example

it was am list users.

* In cloud shell you seem to have complete repository.If you create a text file at any location and then you restart your cloudshell the file is goin to stick there only.
* You can also configure cloudshell for font size,light or dark theme

**SECURITY TOOLS**

IAM has the following security tools as we ca discuss as below:

**1.IAM Credentials Report**

This report is generated at account level. This report will contain all your accounts users and the status of their various credentials.

**2. IAM Access Advisor**

This one is at the user-level and the Access Advisor is going to show the service permissions granted to a user and when those services were last accessed. This will be very helpful because we are talking already about the principle of least privilege,and so using this tool, we're able to see which permissions are not used and reduce the permission a user can get to be inline with the principle of least privilege.

**GENERAL IAM GUIDELINES**

1. do not use a root accounts except when you set up your AWS account. You should have two accounts a root account and a personal account.
2. And remember, one AWS user is equal to one physical user. If a friend of yours wants to use AWS, do not give them your credentials, instead of create another user for them.
3. You can assign users to groups and assign permission to groups to make sure that security is managed at the group level.
4. Create a strong password policy. Also, if you can use and enforce the use of Multi Factor Authentication, or MFA, to really guarantee that your account is going to be safe or safer from hackers.
5. You should create and use roles whenever you're giving permissions to AWS services.
6. If you were to use AWS programmatically, or using the CLI, so the CLI or some SDK, you must generate access keys, and these access keys are just like passwords. They're very secrets, so just keep them for yourself.
7. Finally, if you wanted to audit permissions within your accounts, you can use the IAM Credentials Reports, and also IAM access analyzer.