4 IAM ::

Global Infrastructure ::

https://aws.amazon.com/about-aws/global-infrastructure/

https://www.infrastructure.aws/

https://docs.aws.amazon.com/general/latest/gr/rande.html

https://aws.amazon.com/blogs/security/demystifying-ec2-resource-level-permissions/

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policies-ec2-console.html#ex-read-only

1. User Creation

- with out policies

- with policies

- with multiple policies

- MFA for individual account

- users with password & access keys(optional will teach in python)

- Customizing the userlogin url

2. Group Creation

- importance of groups (not passwords to login)

- adding policies to group

- adding users to the group

- removing policies to the group

Note: Note that a group is not truly an "identity" in IAM because it cannot be identified as a Principal in a permission policy.

It is simply a way to attach policies to multiple users at one time.

3. Policies

- inline policies & customer managed policies

- explain about ARN (Amazon Resource Name)

- Create our own custom policy and attach it to the user

Example:

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Stmt1586284206482",

"Action": [

"iam:Get\*",

"iam:List\*"

],

"Effect": "Allow",

"Resource": "\*"

}

]

}

- Create s3 buckets (dvs-hyd,dvs-blr) and create customer based polices

===================================

NOTE: WILL COVER BELOW IN EC2

4. Configuring Aws Cli

Ref: For installing Bash in windows10

https://itsfoss.com/install-bash-on-windows/

GitBash For windows:

https://git-scm.com/download/win

- Create credentials & explain them the usecase of access & secret keys

5. Roles

STS --> Security Token Services

Notes:

 Roles don’t have access keys

 Roles don’t used for login in to the console

 They don’t’ have username & password

 They have short time credentials