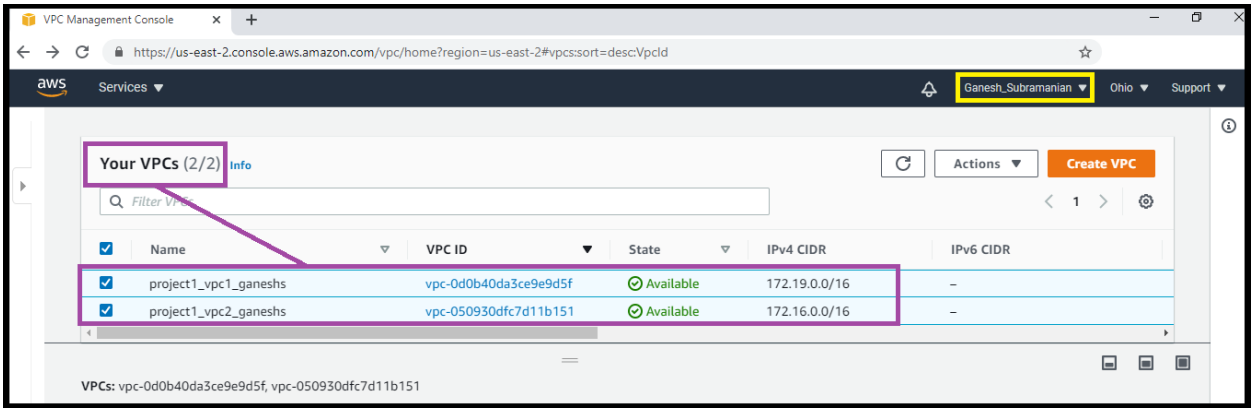
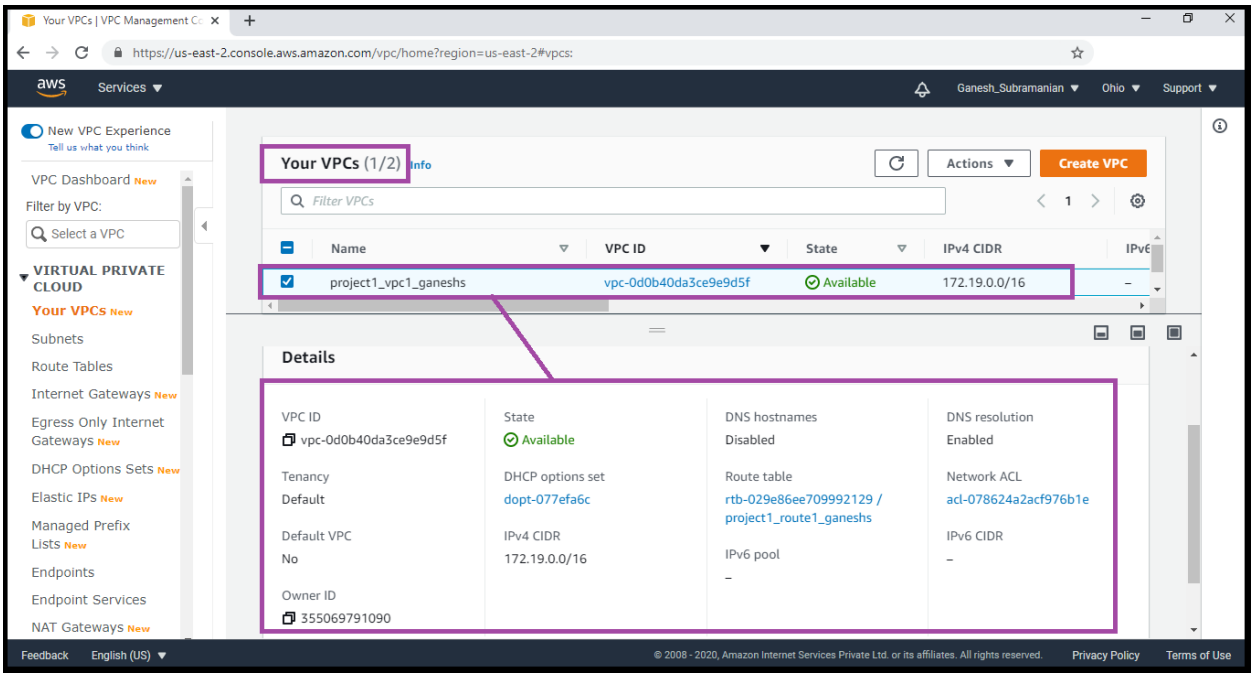
PROJECT 1:

VPC Peering

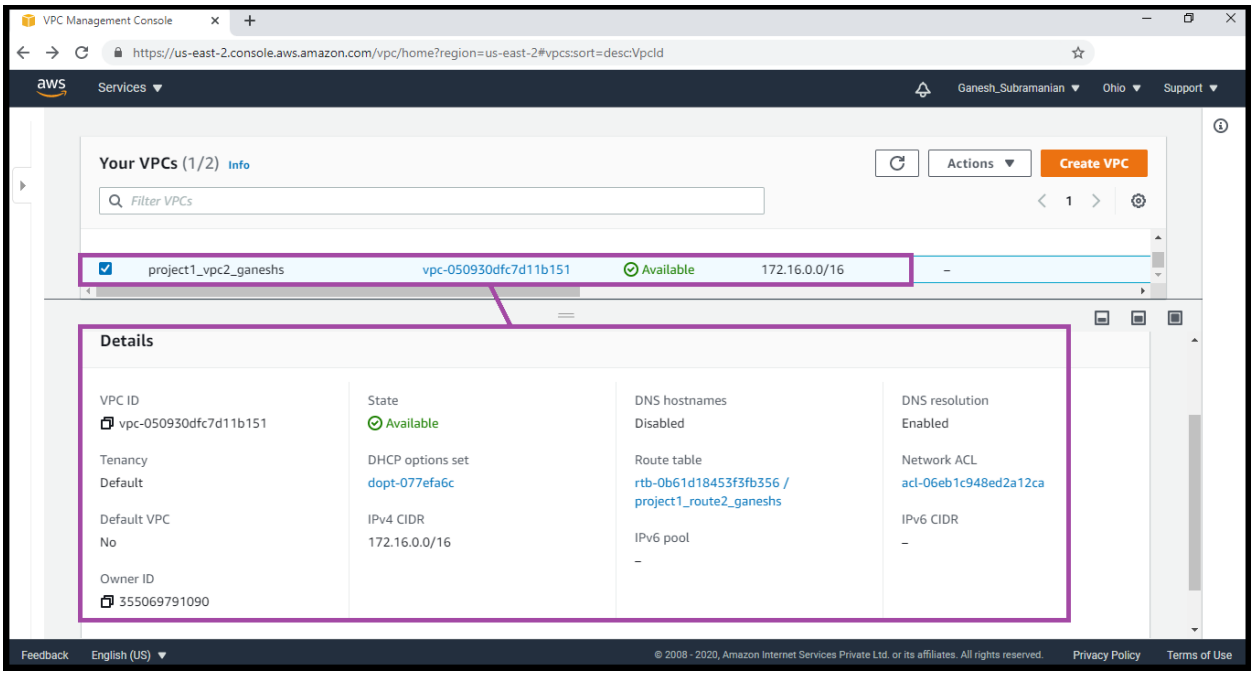
Screenshot 1: VPCs list



⇨ 2 VPC's Created: - "**project1_vpc1_ganeshs**" / "**project1_vpc2_ganeshs**".

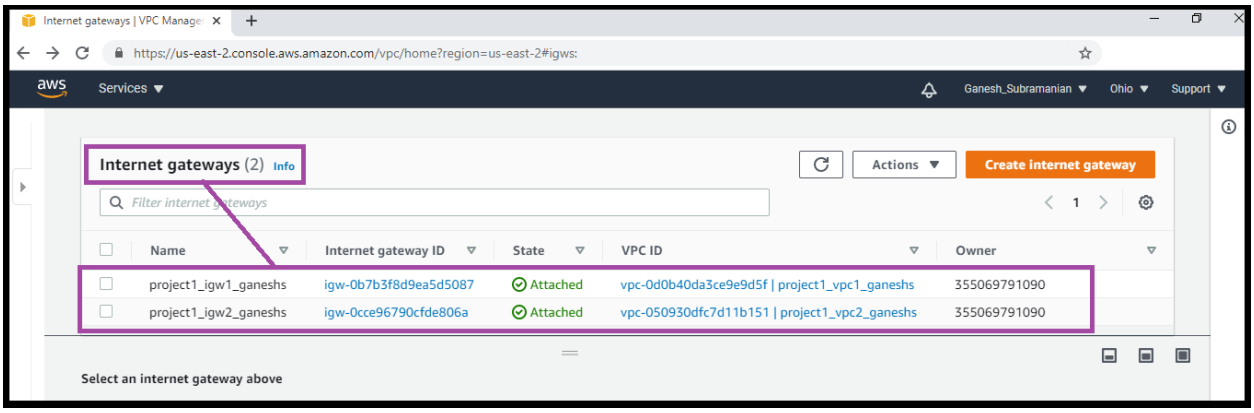


⇨ VPC 1 Details: - "**project1_vpc1_ganeshs**".



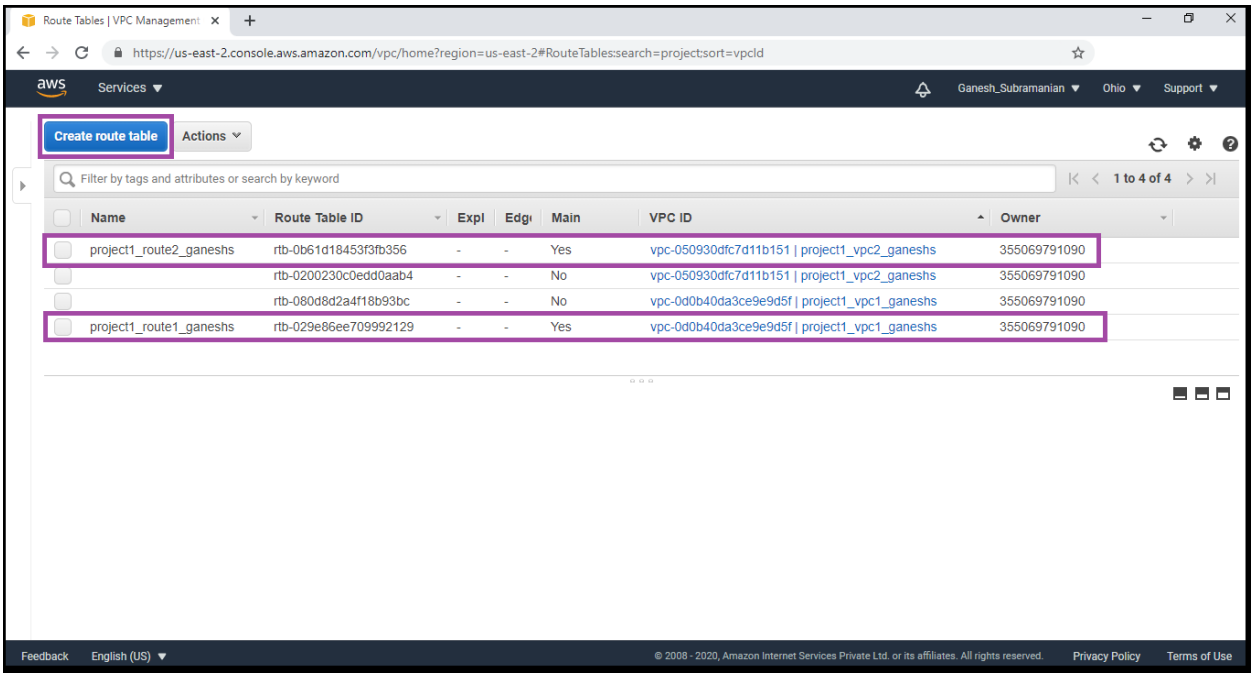
⇨ VPC 2 Details: - “**project1_vpc2_ganeshs”.**

Screenshot 2: IGW list

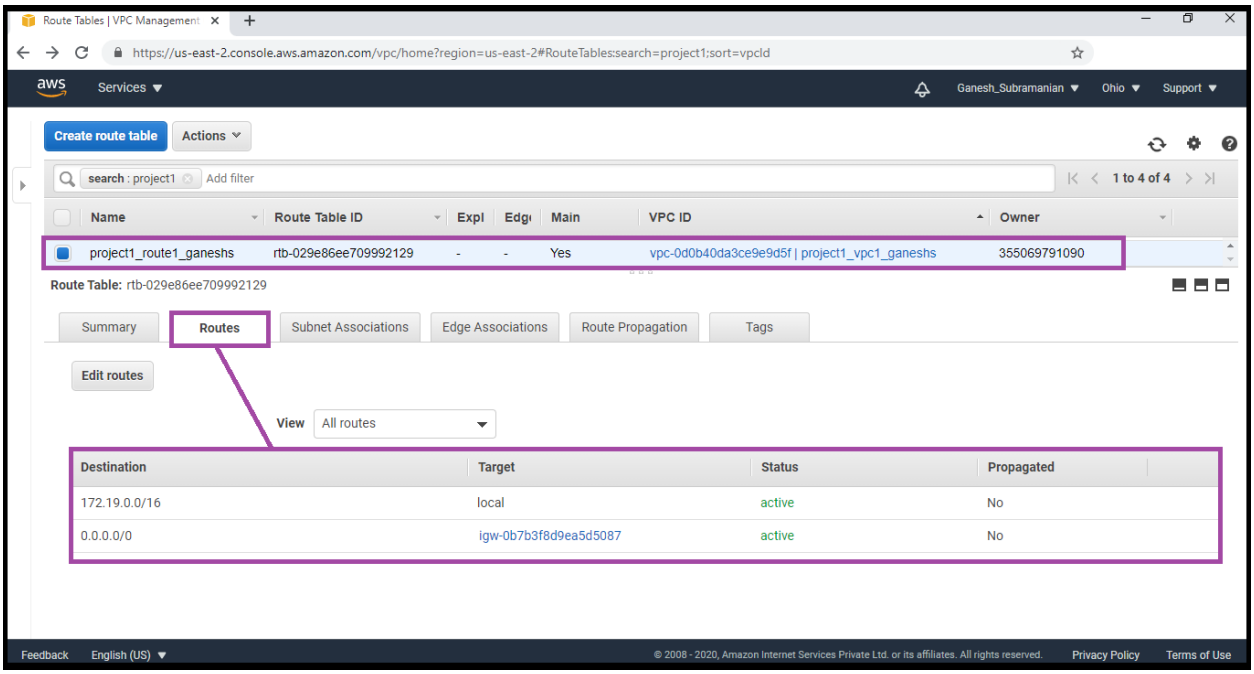


⇨ 2 IGW's Created: - "**project1_igw1_ganeshs"** / "**project1_igw2_ganeshs".**

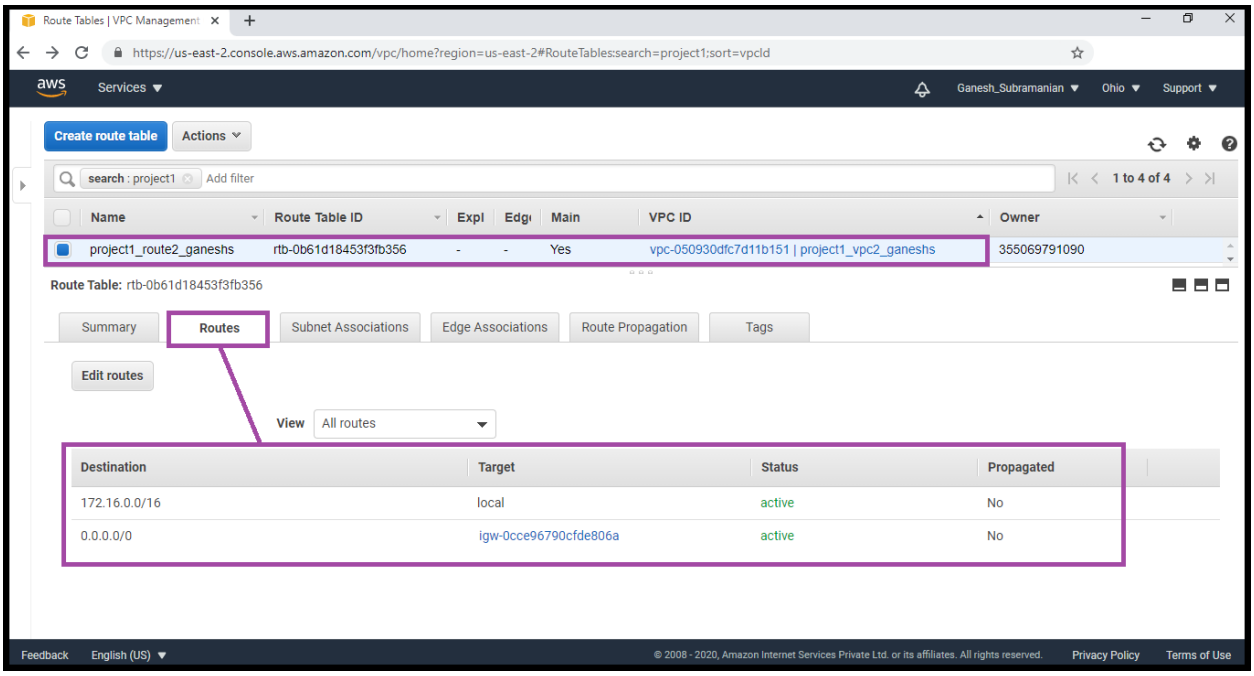
Screenshot 3: Edit Route List



⇨ 2 Route Table Created: - "**project1_route1_ganeshs"** / "**project1_route2_ganeshs".**

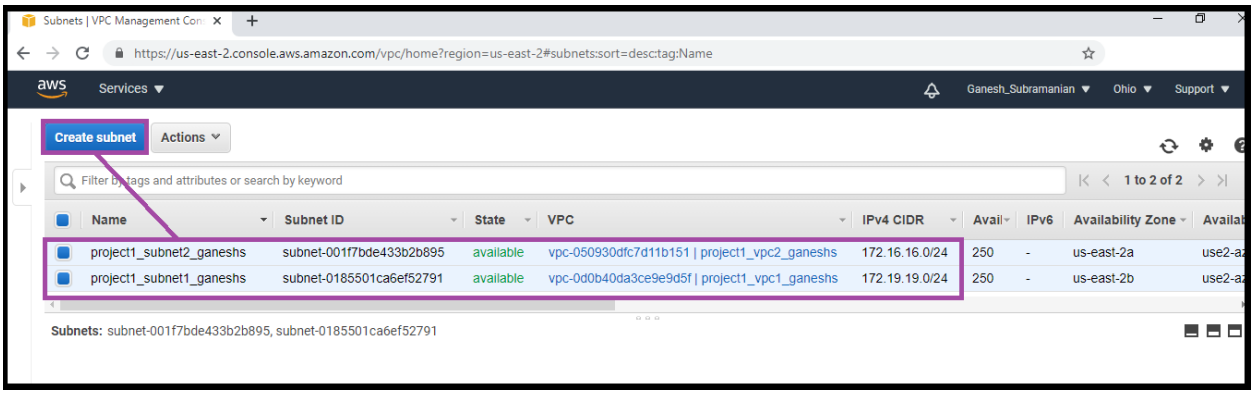


⇨ Route Table 1 Details: - “**project1_route1_ganeshs”.**

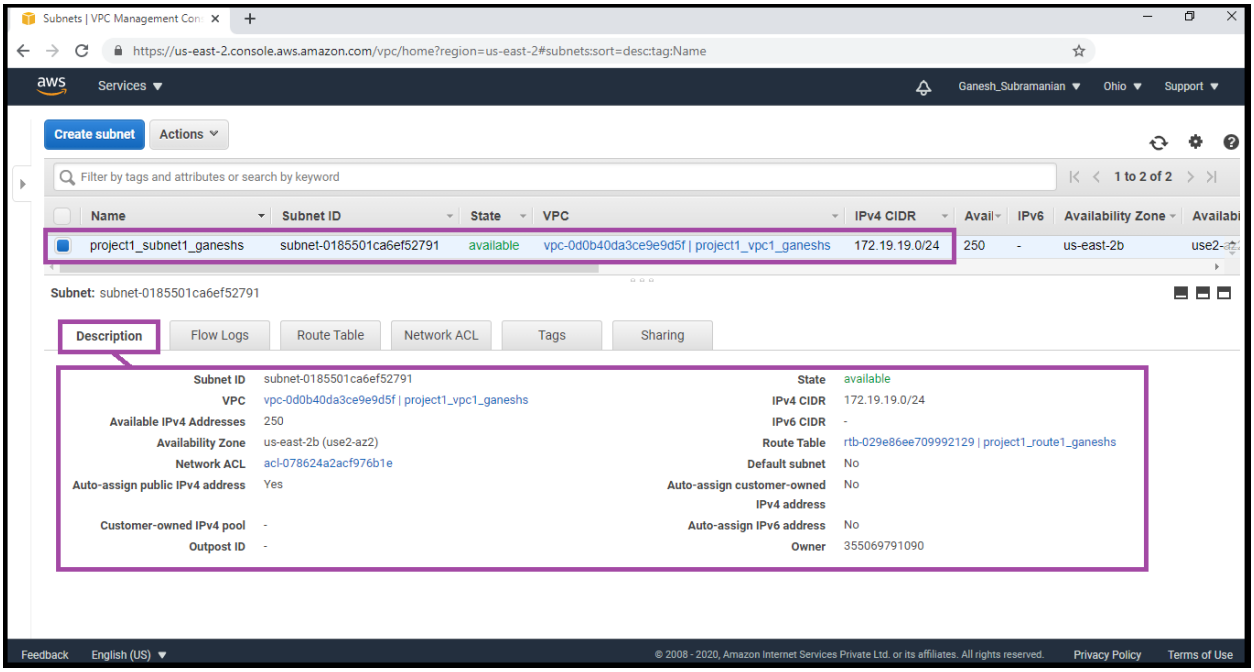


⇨ Route Table 2 Details: - “**project1_route2_ganeshs”.**

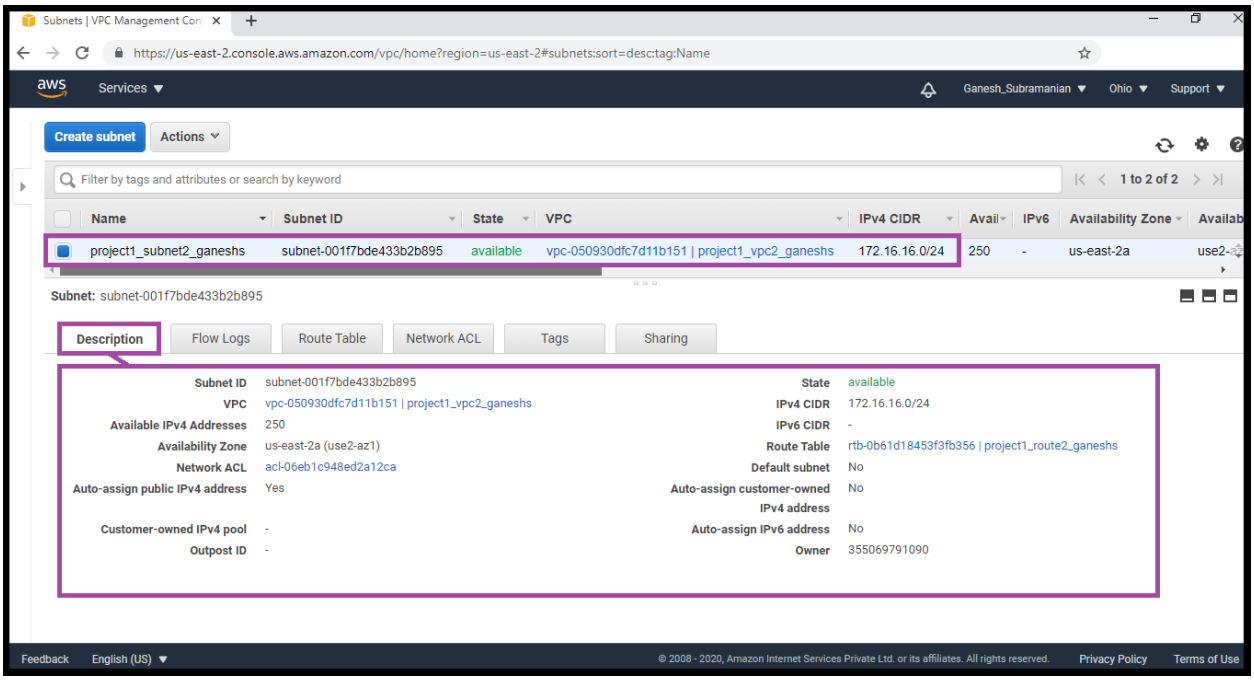
Screenshot 4: Subnet list



⇨ 2 Subnet's Created: - "**project1_subnet1_ganeshs**" / "**project1_subnet2_ganeshs".**

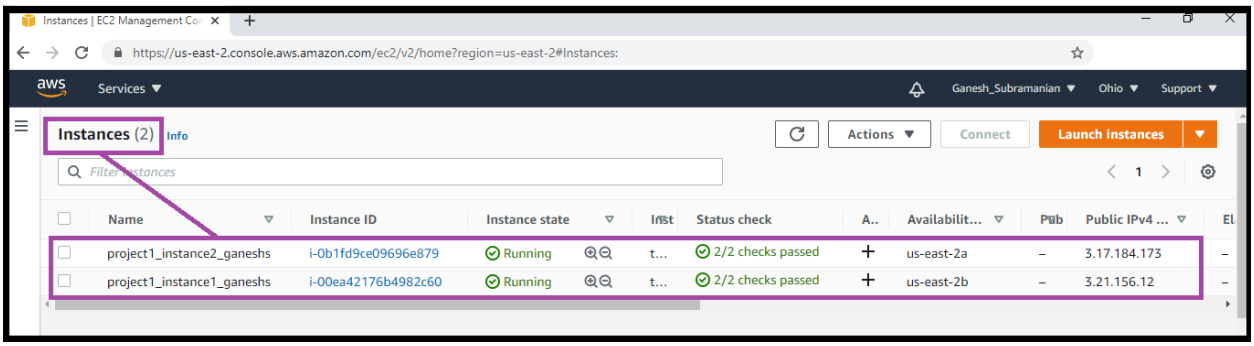


⇨ Subnet 1 Details: - "**project1_subnet1_ganeshs**".

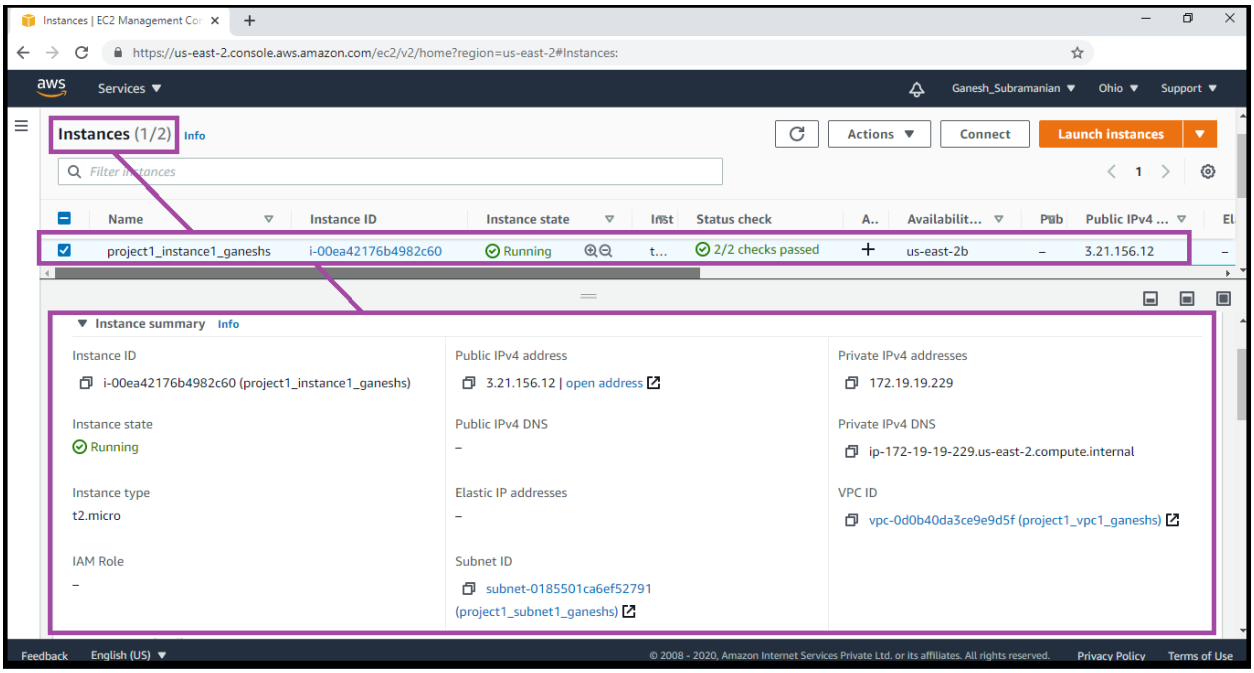


⇨ Subnet 2 Details: - “**project1_subnet2_ganeshs**”.

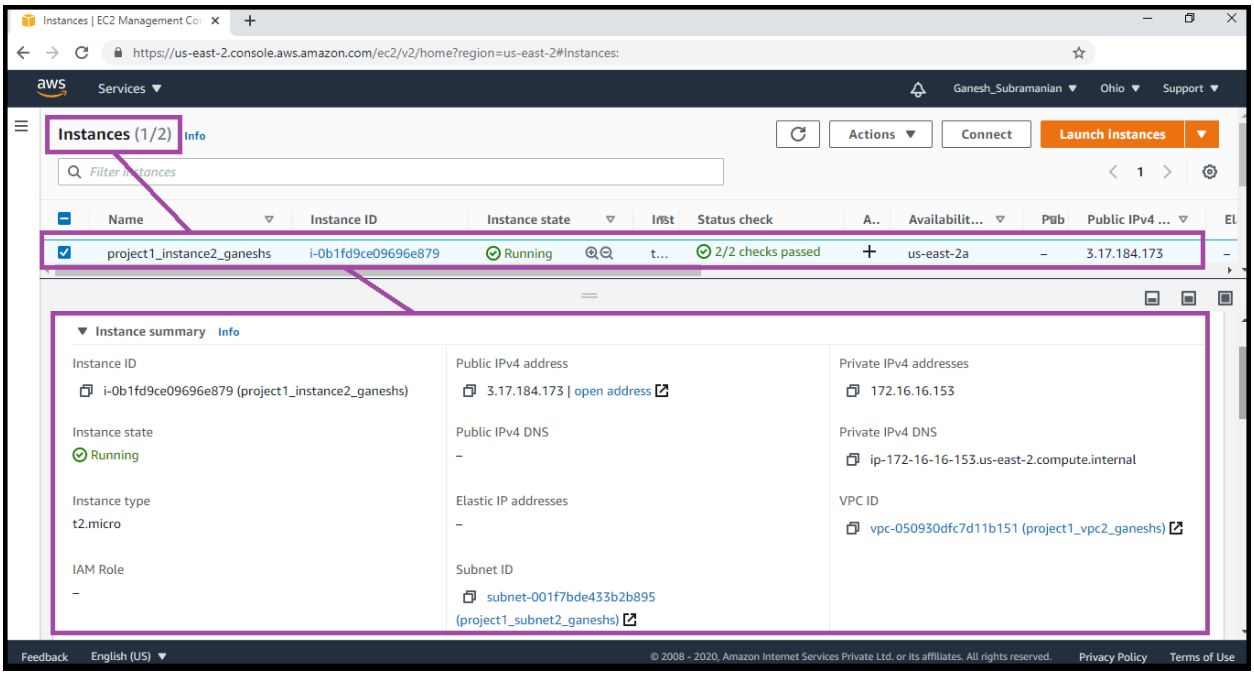
Screenshot 5: Instance details



⇨ 2 EC2 Instance's: - "**project1_instance1_ganeshs"** / "**project1_instance2_ganeshs".**

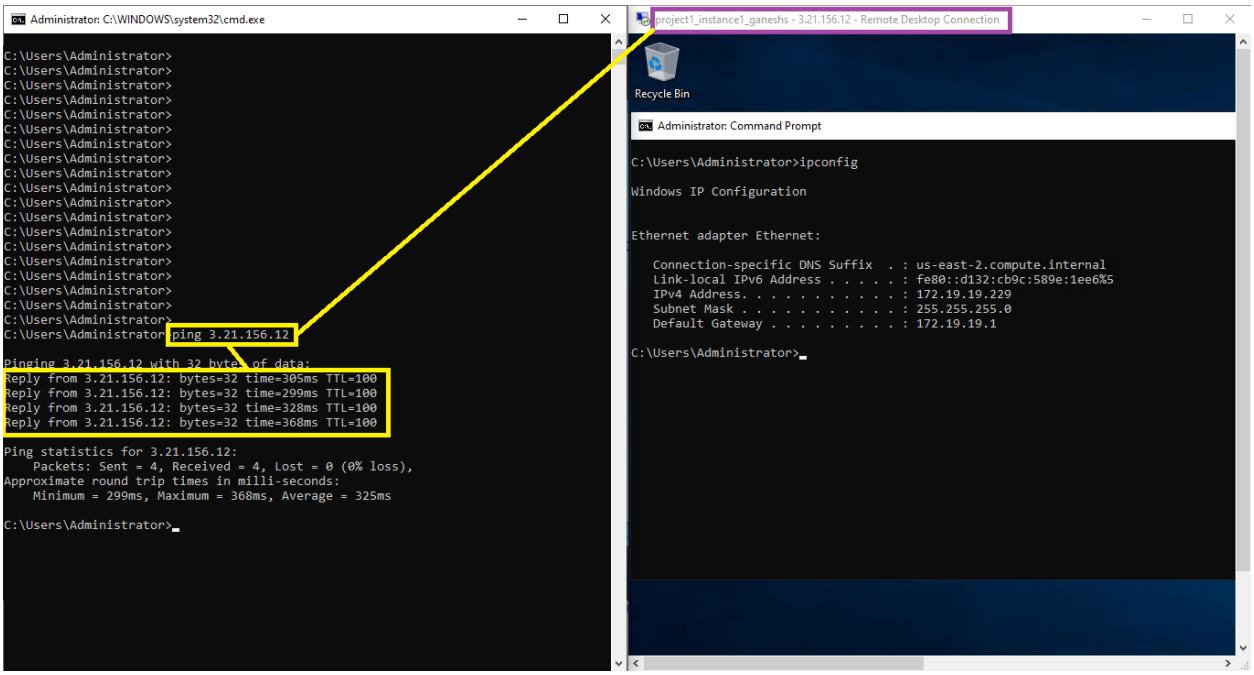


⇨ EC2 Instance 1 Details: - "**project1_instance1_ganeshs**".

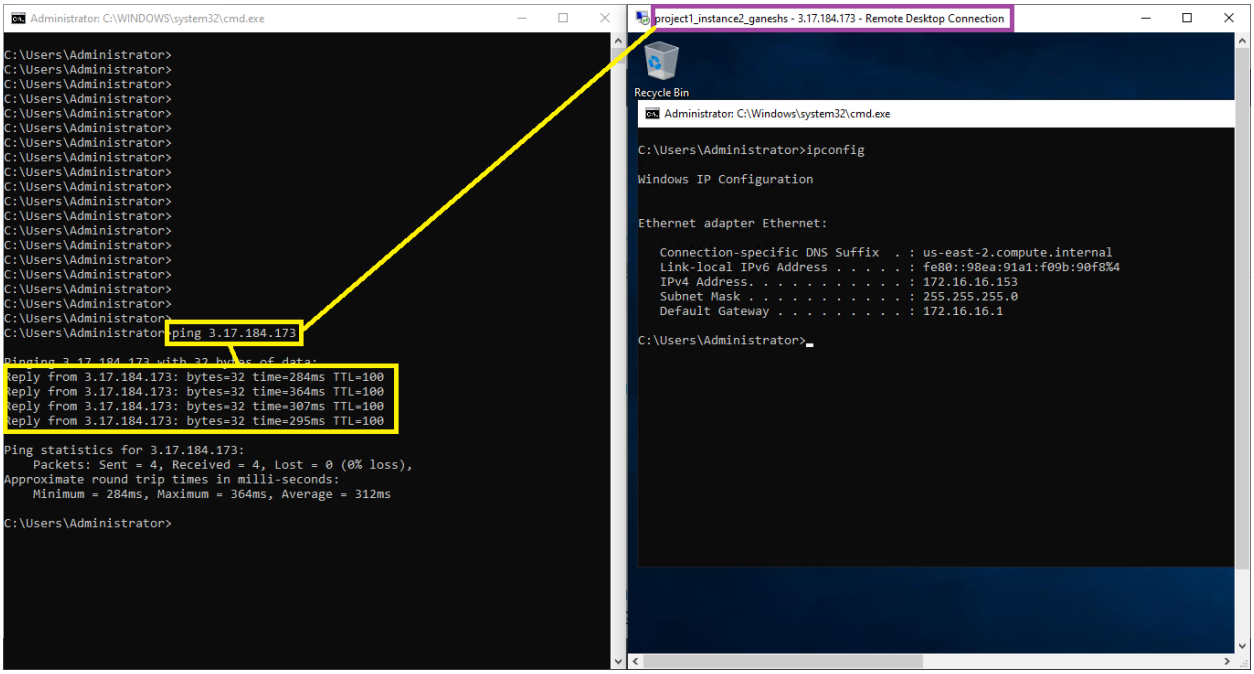


⇨ EC2 Instance 2 Details: - “**project1_instance2_ganeshs**”.

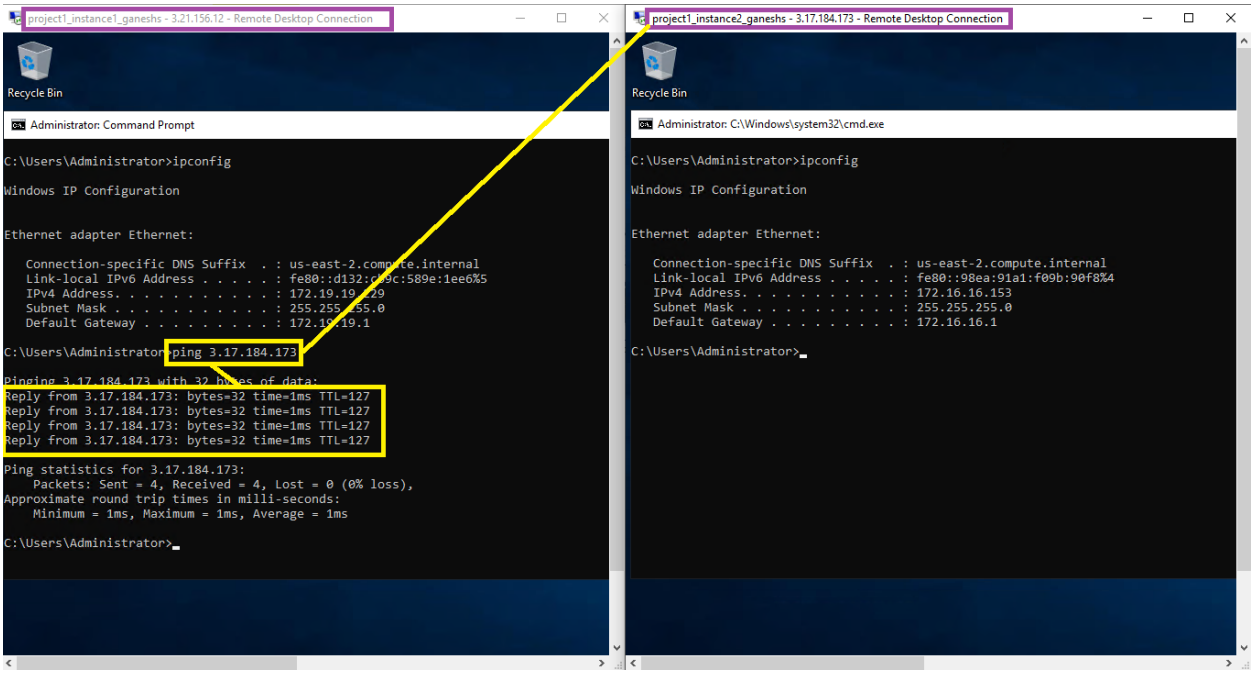
Screenshot 6: Success Public



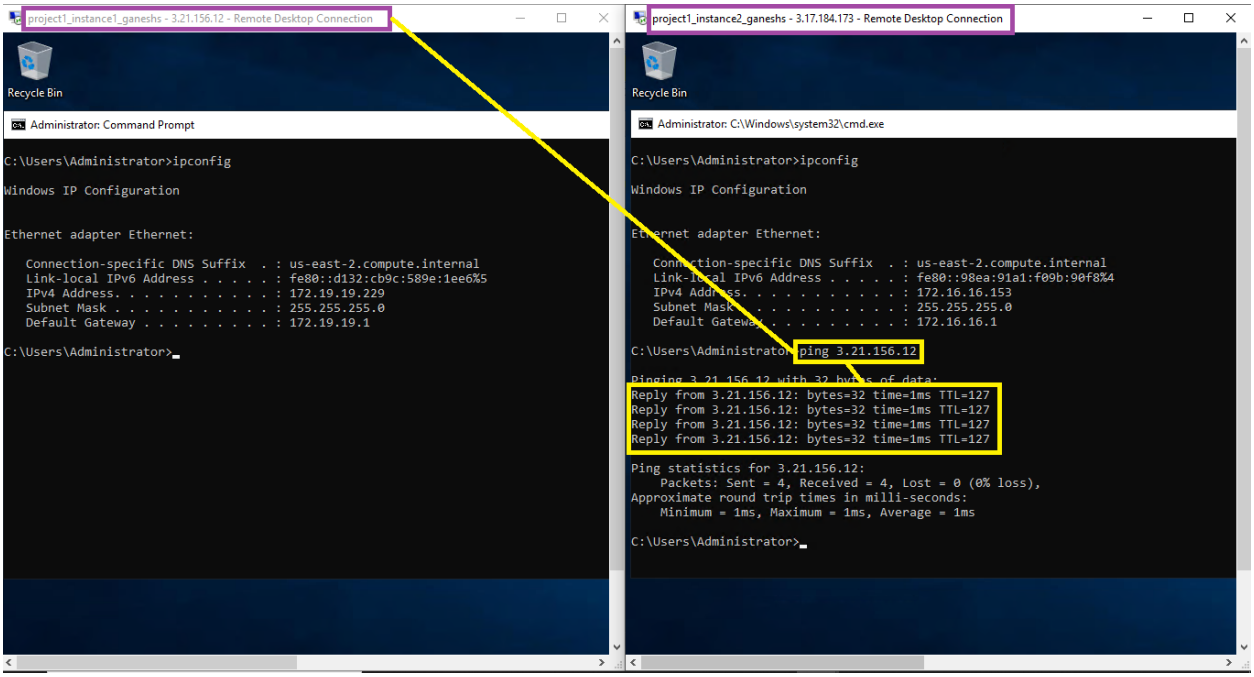
⇨ Ping from **Base Machine** to RDP1 (“**project1_instance1_ganeshs**”: - “3.21.156.12”) **(Public IP).**



⇨ Ping from **Base Machine** to RDP2 (“**project1_instance2_ganeshs**”: “3.17.184.173”) **(Public IP).**

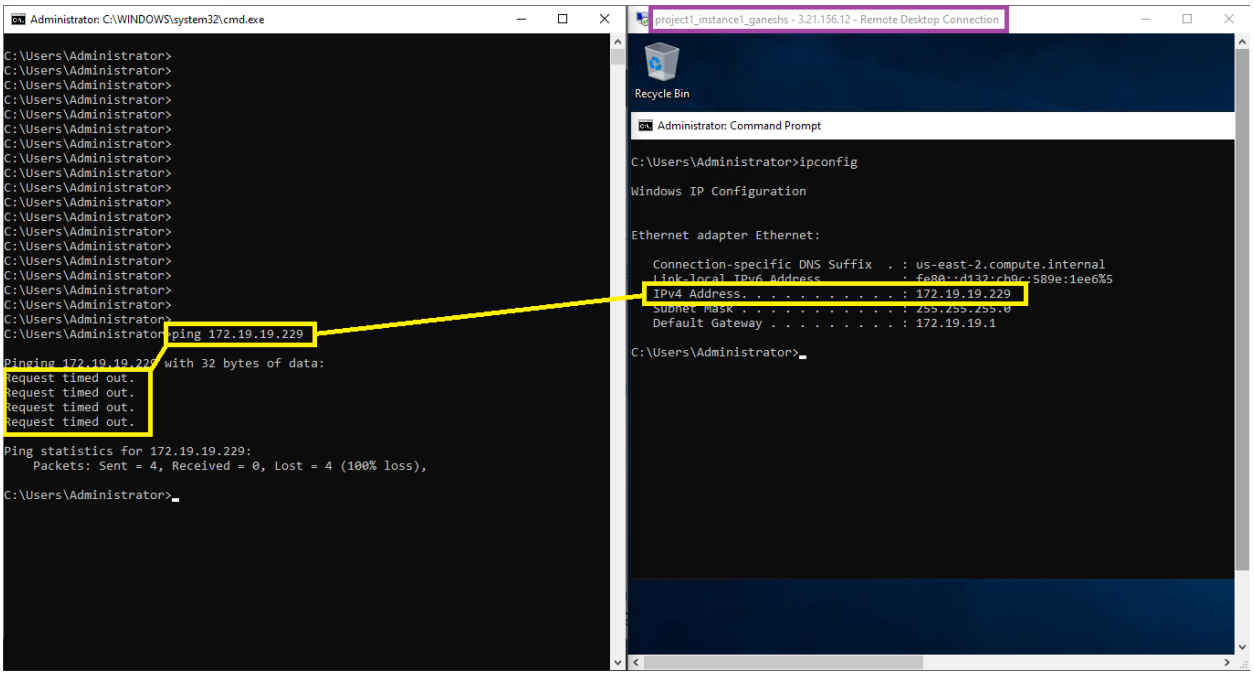


⇨ Ping from **RDP1** to **RDP2** (“**project1_instance2_ganeshs**”: - “3.17.184.173”) **(Public IP).**

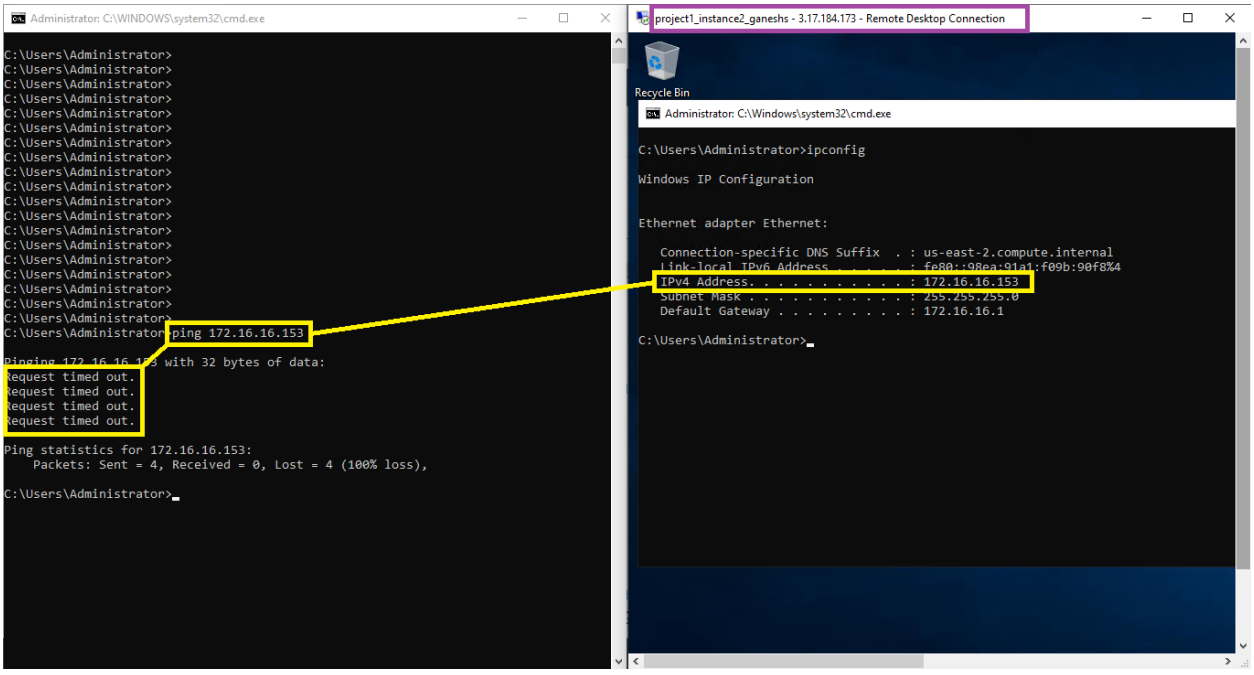


⇨ Ping from **RDP2** to **RDP1** (“**project1_instance1_ganeshs**”: - “3.21.156.12”) **(Public IP).**

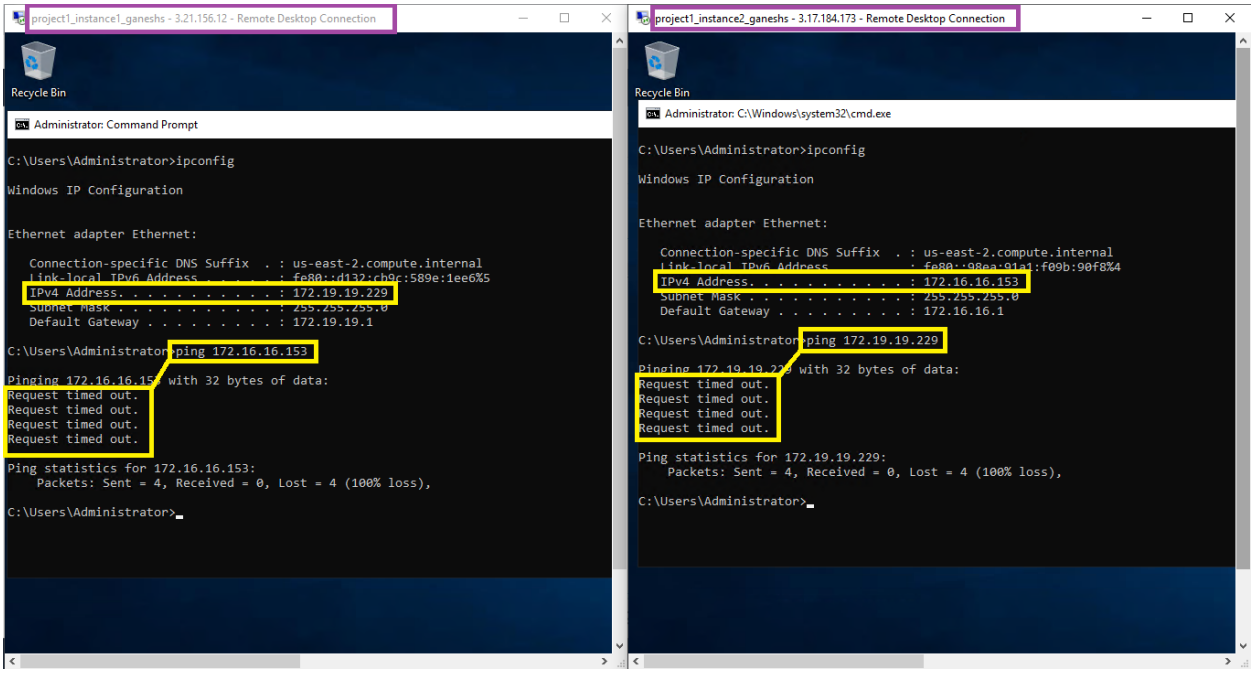
RTO private IP: -



⇨ Ping from **Base Machine** to RDP1(“**project1_instance1_ganeshs**”: - “172.19.19.229”) **(Private IP).**

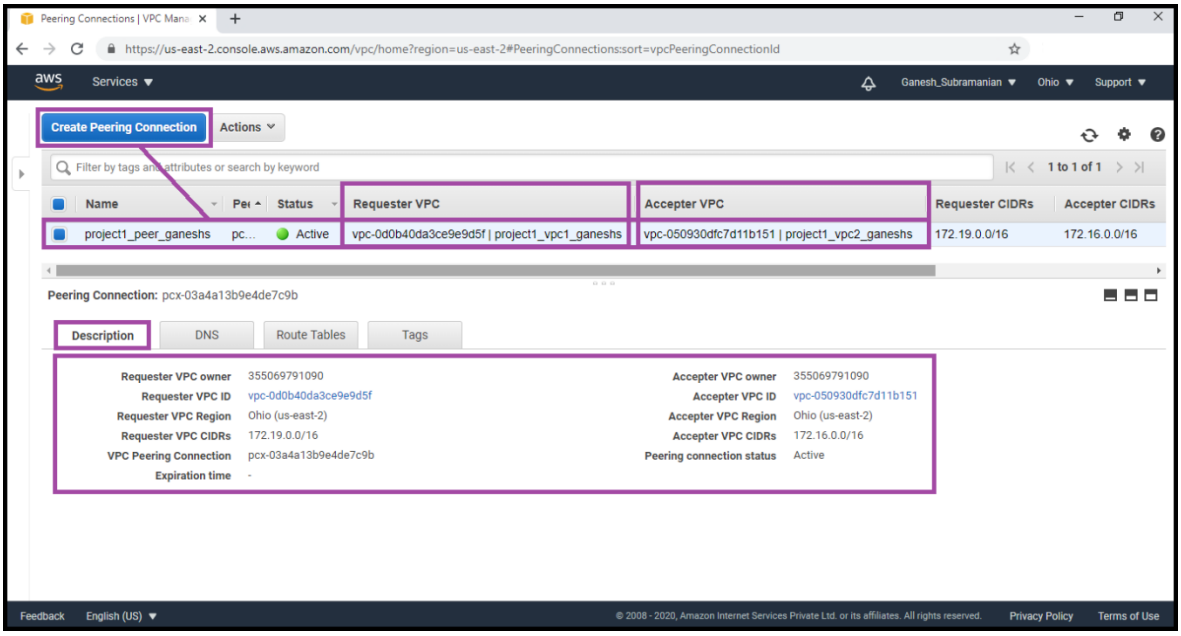


⇨ Ping from **Base Machine** to RDP2(“**project1_instance2_ganeshs**”: - “172.16.16.153”) **(Private IP).**



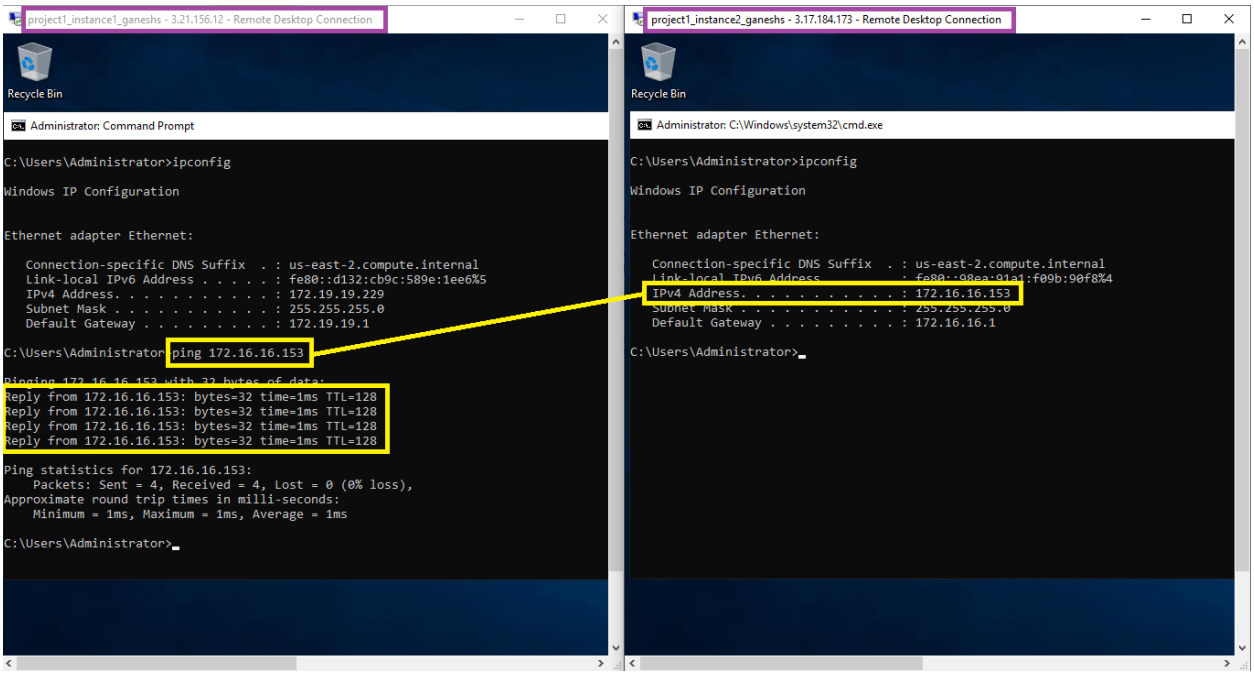
⇨ Ping from **RDP1** to **RDP2** (“**project1_instance2_ganeshs**”) and Vice versa. **(Private IP).**

Screenshot 7: Peering with Requestor and Acceptor

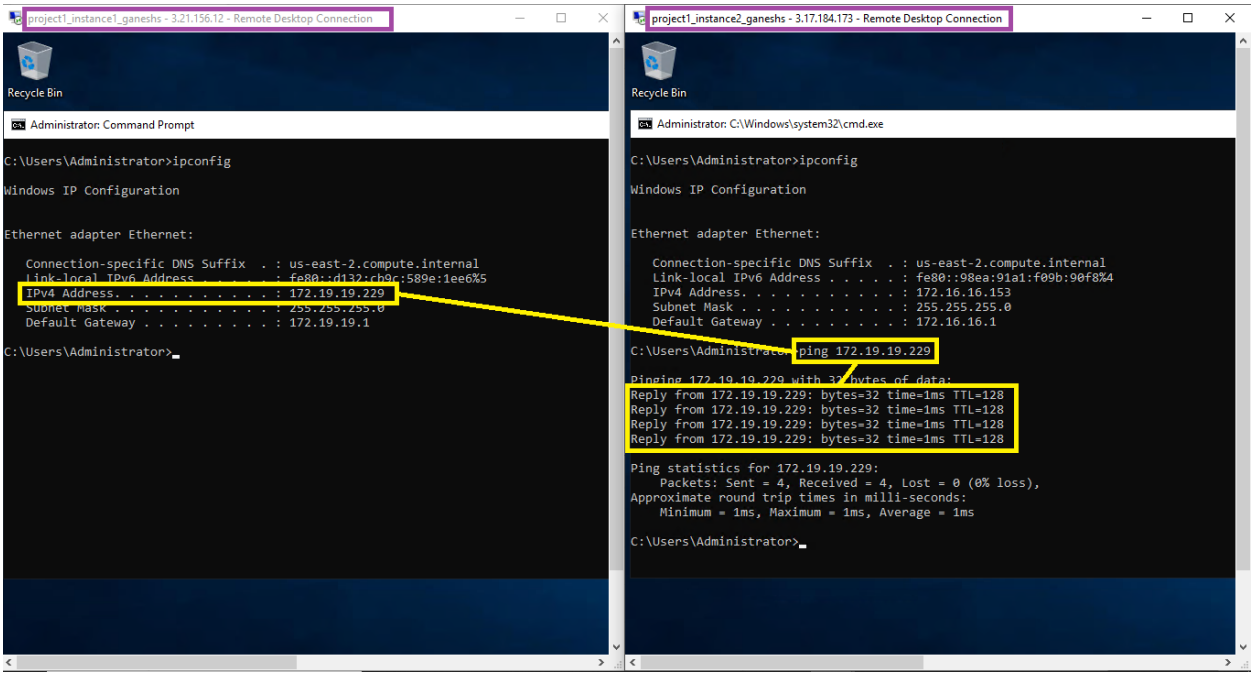


⇨ Peering Connection Created: - “project1_peer_ganeshs” where the **Requestor** is “**project1_vpc1_ganeshs**” and **Acceptor** is “**project1_vpc2_ganeshs**”.

Screenshot 8: Success for Private



⇨ Ping from **RDP1** to **RDP2** (“**project1_instance2_ganeshs**”: - 172.16.16.153) **(Private IP).**



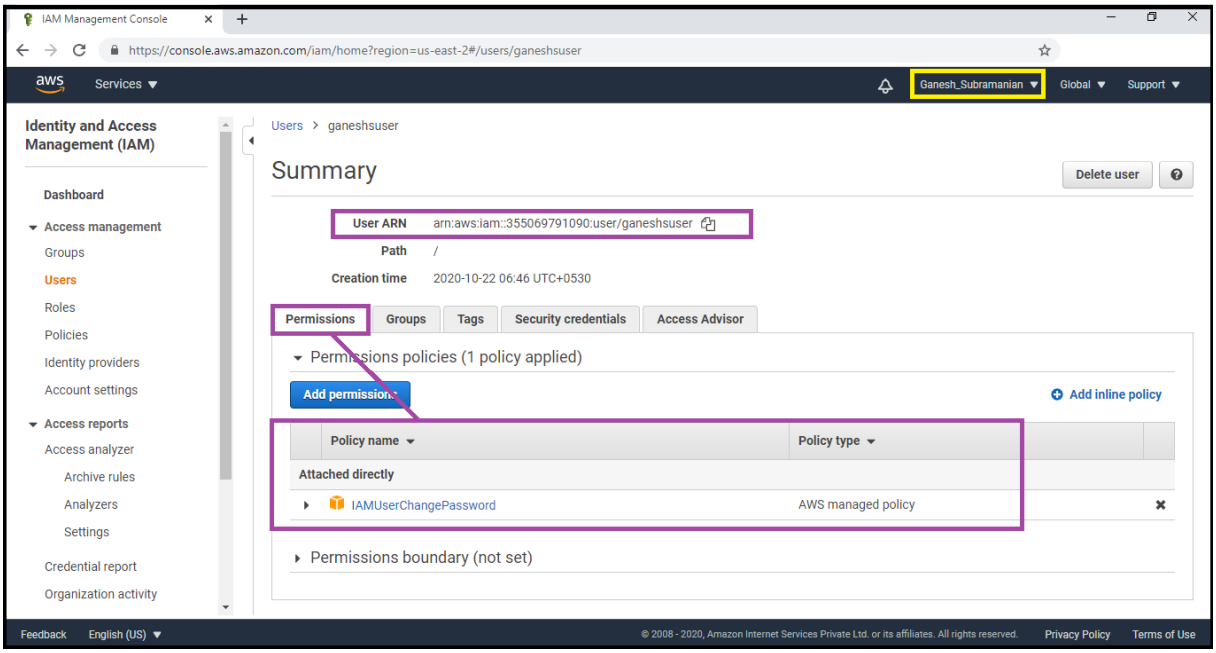
⇨ Ping from **RDP2** to **RDP1** (“**project1_instance1_ganeshs**”: - 172.19.19.229) **(Private IP).**

PROJECT 2:

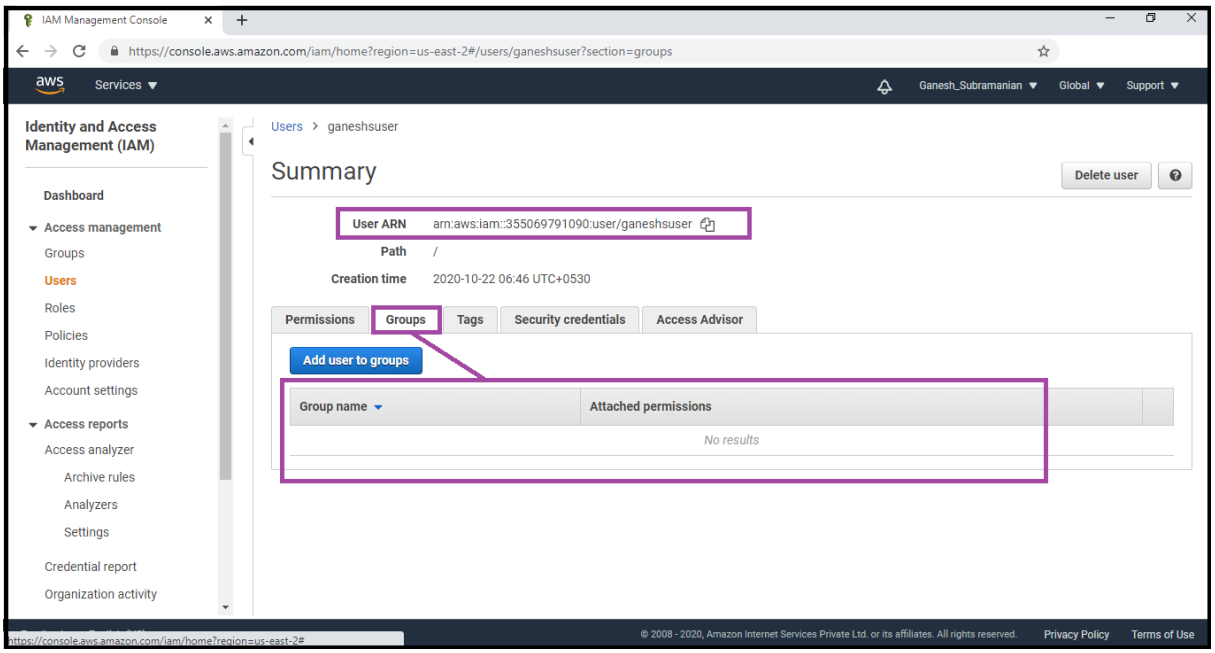
IAM

Task 1: Creating users without permissions-IAM password policy check.

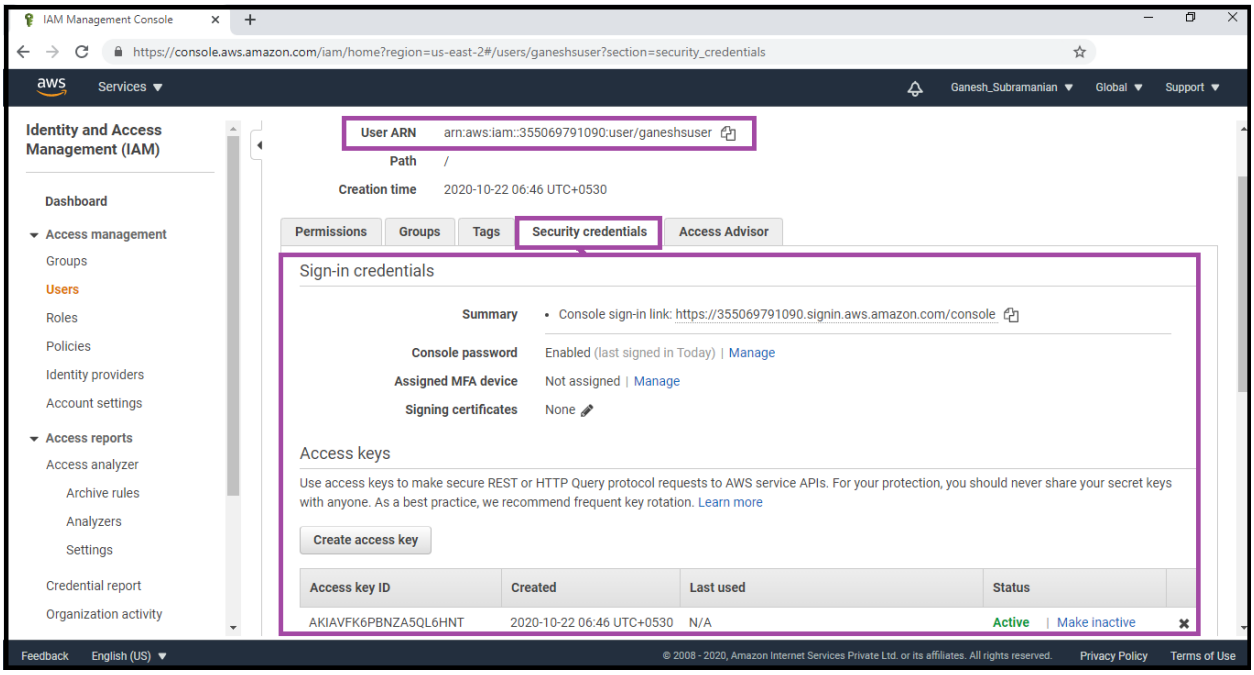
Screenshot 1: user summary with all tab information



⇨ **IAM** User Summary "**ganeshsuser**" with **Permission** Details.



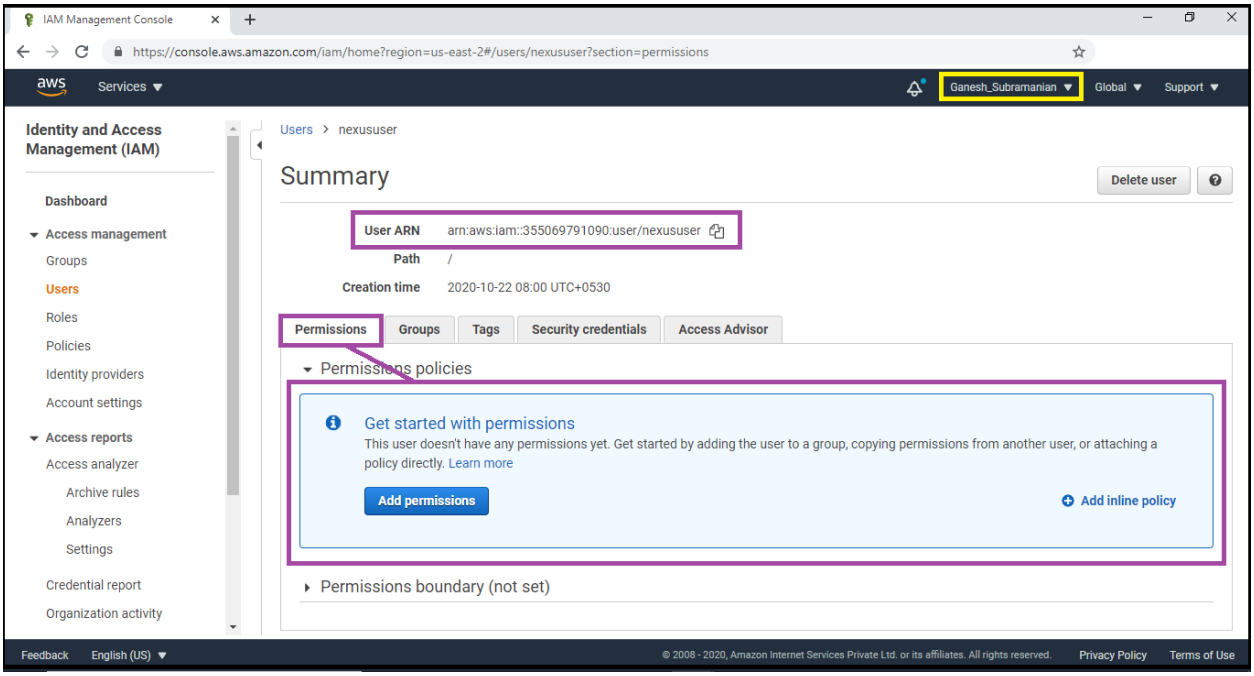
⇨ **IAM** User Summary "**ganeshsuser**" with **Group** Details.



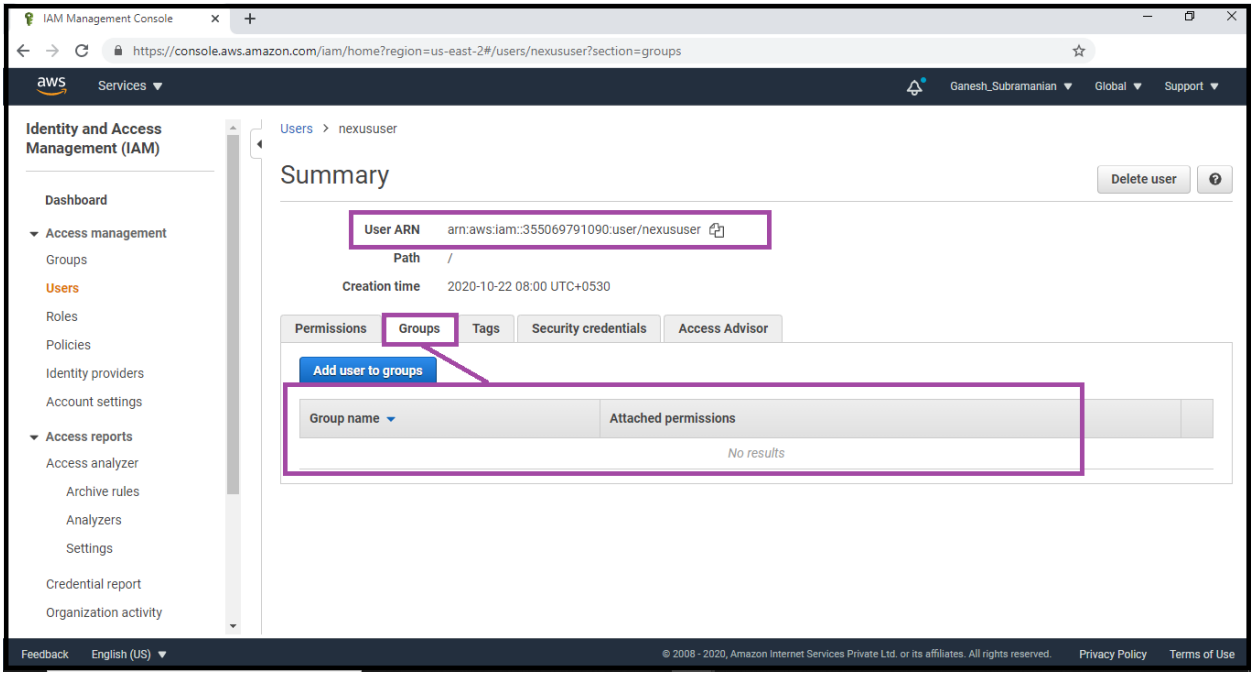
⇨ **IAM** User Summary "**ganeshsuser**" with **Security Credentials** Details.

Task 2: Creating users without the IAM password policy.

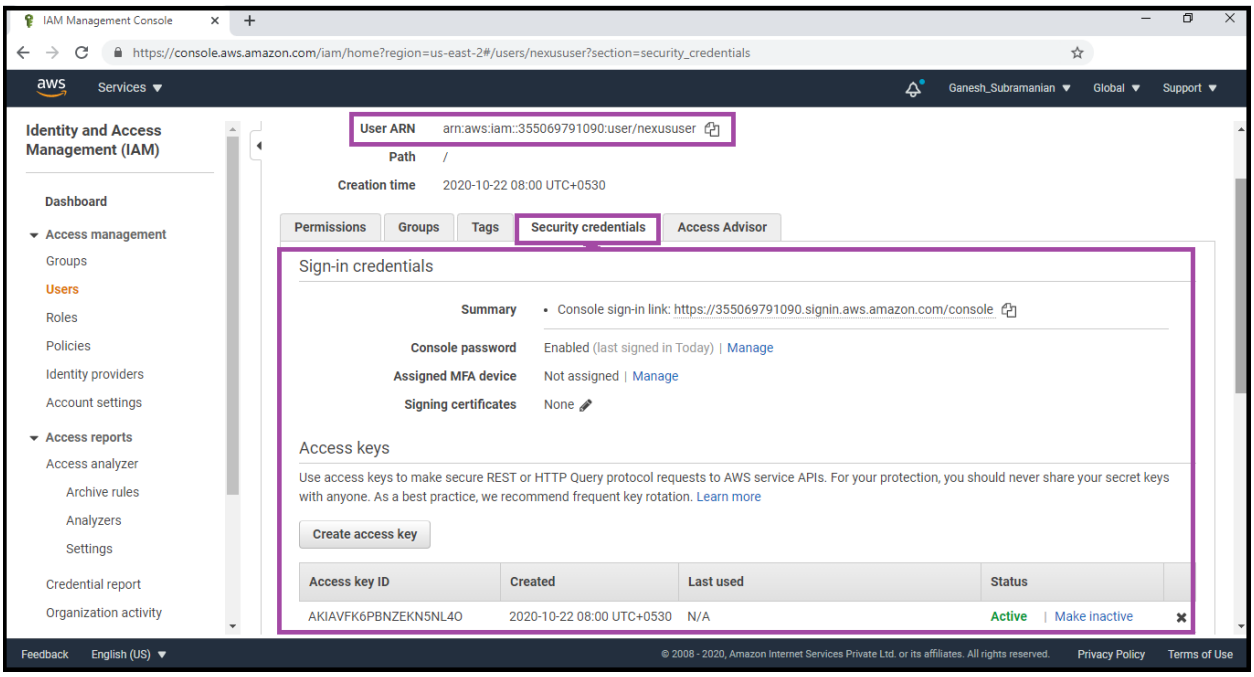
Screenshot 2: user summary with all tab information



⇨ **IAM** User Summary "**nexususer**" with **Permission** Details.



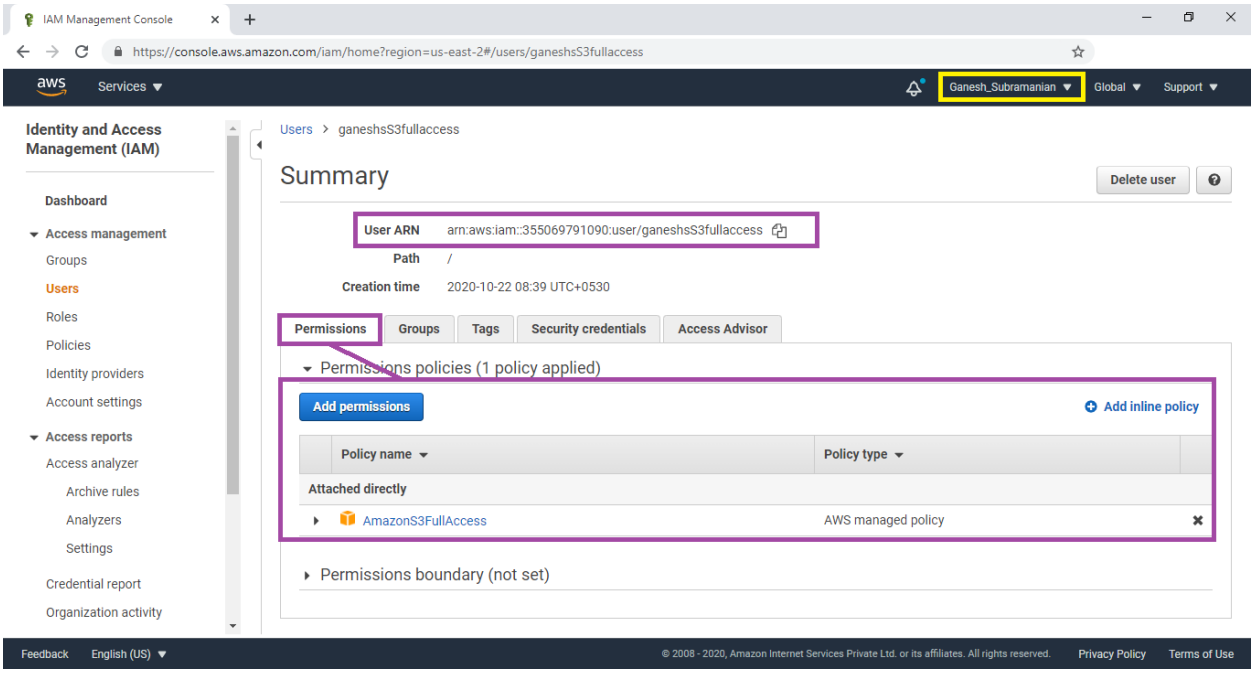
⇨ **IAM** User Summary "**nexususer**" with **Group** Details.



⇨ **IAM** User Summary "**nexususer**" with **Security Credentials** Details.

Task 3: Create a user with S3 full access

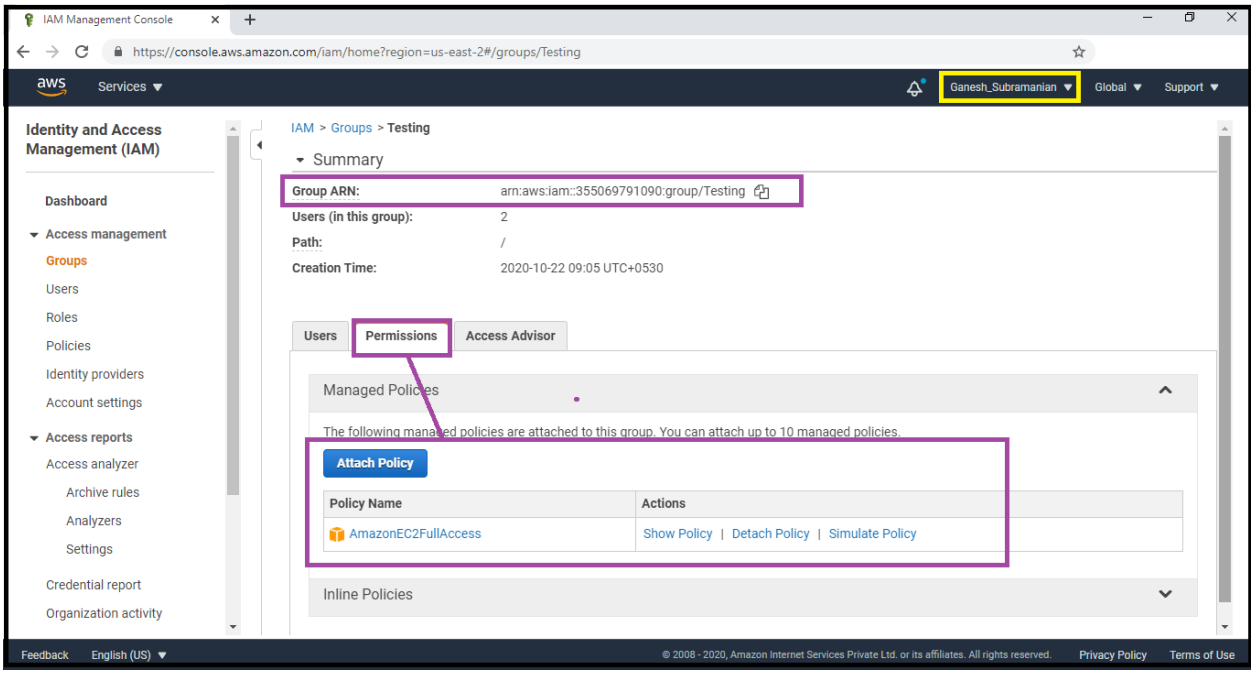
Screenshot 3: User summary



⇨ **IAM** User Summary "**ganeshsS3fullaccess**" with **Permission** Details.

Task4: Create a group with ec2 full access

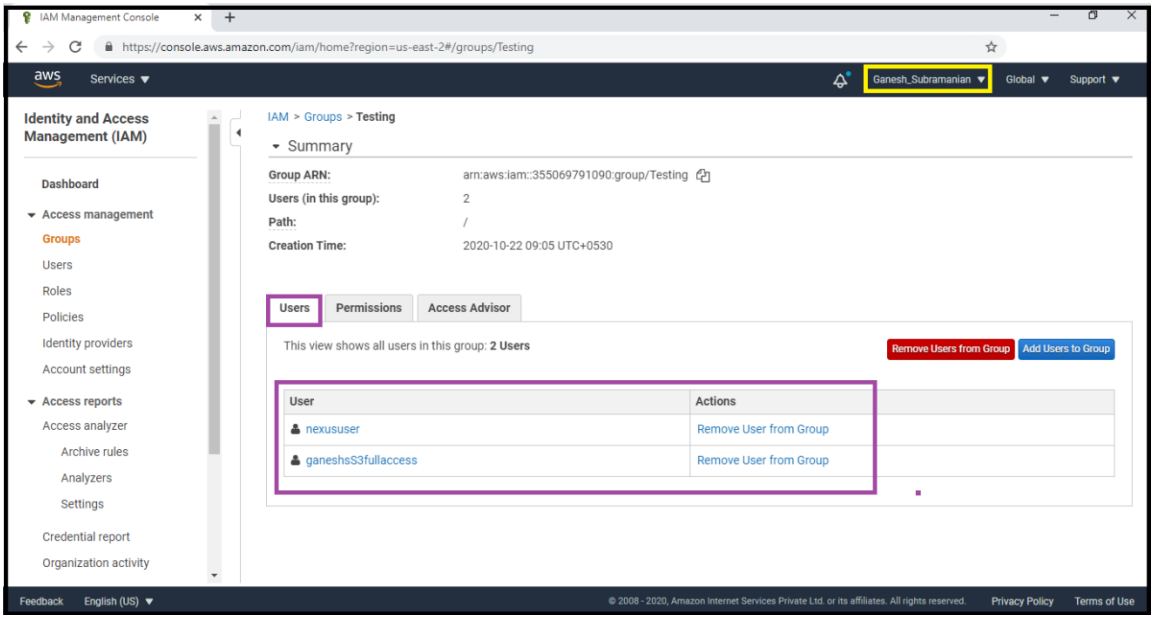
Screenshot 4: group summary



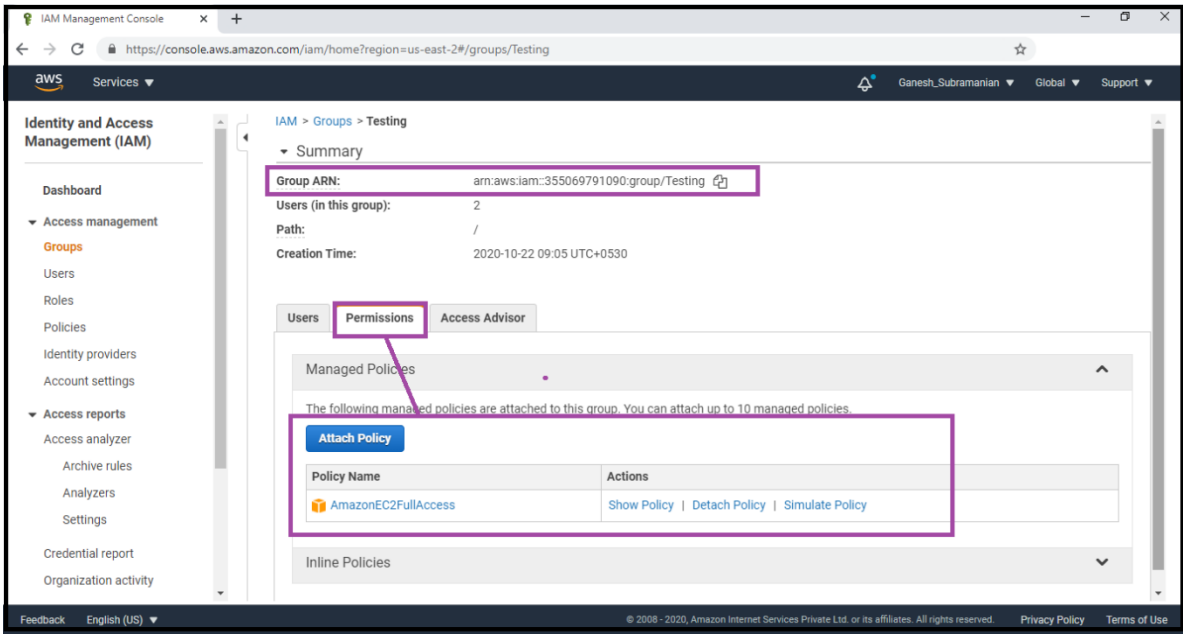
⇨ **IAM** Group "**Testing**" with **Permission** Details.

Task 5: Add user to a group and check if user policy and the group policy is reflecting on the user

Screenshot 5: user summary with permissions

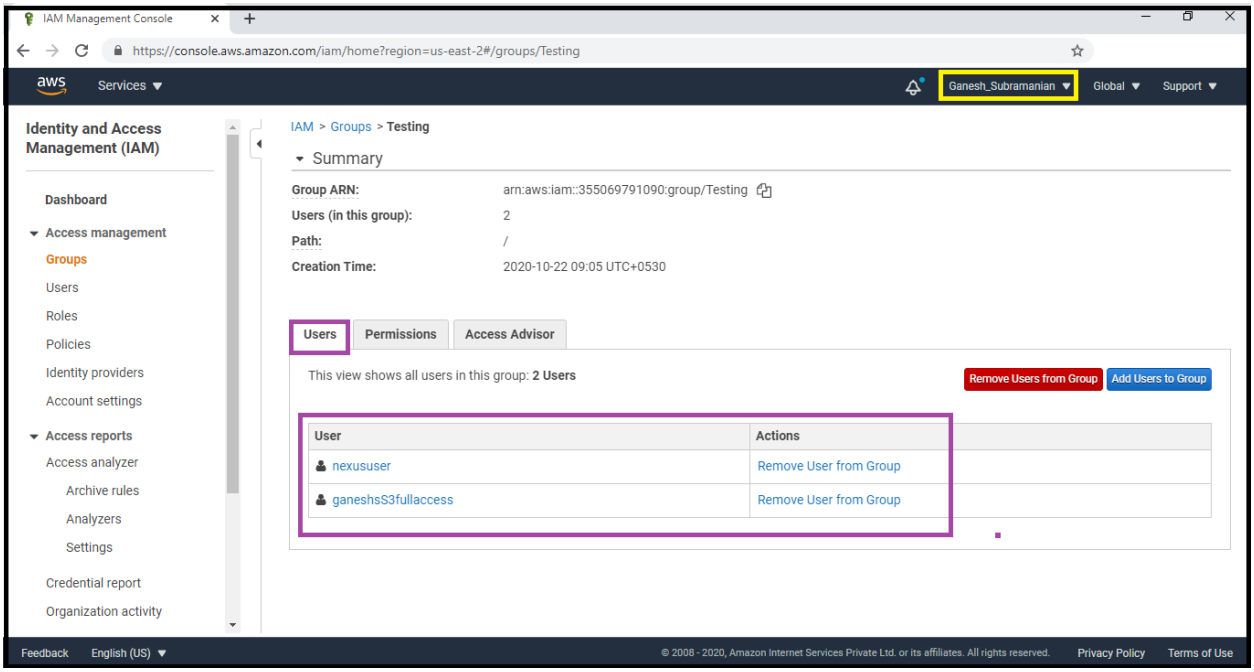


⇨ **IAM** Group “**Testing**” with 2 Users Attached Details (“**nexususer**”, “**ganeshsS3fullaccess**”).



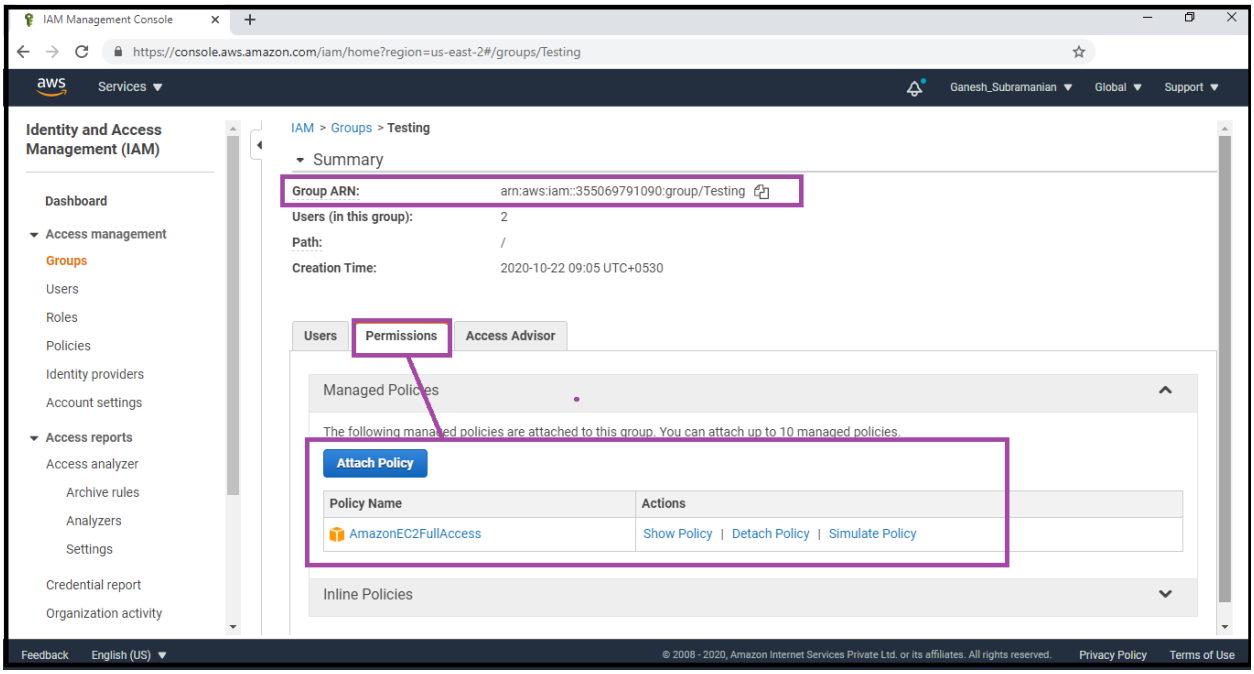
⇨ **IAM** Group “Testing” with Permission Details.

Screenshot 6: login as this user show that this policy is in effect

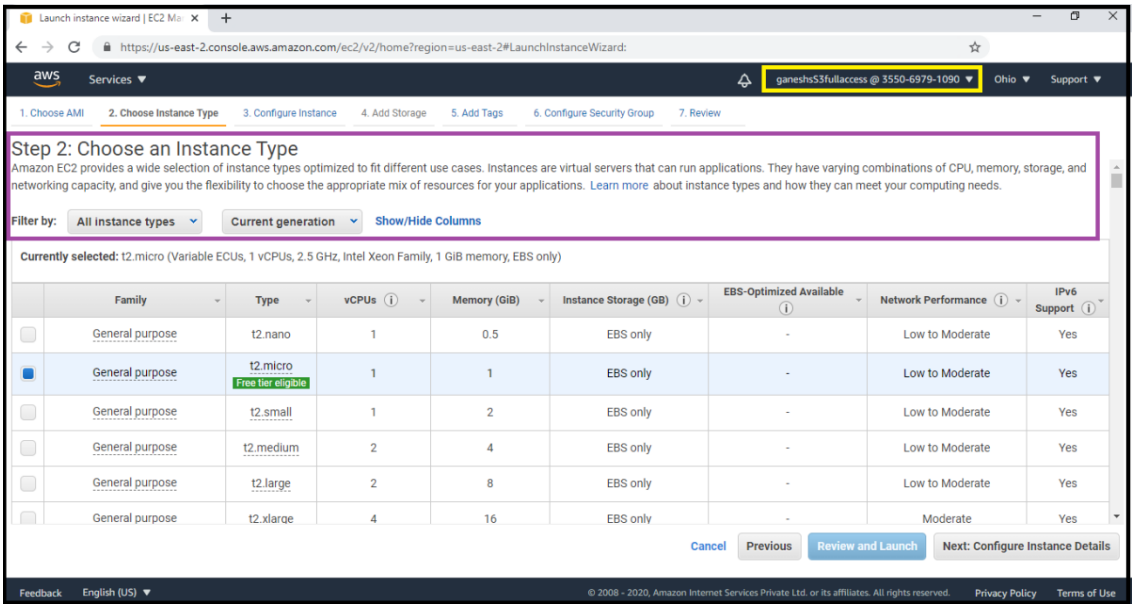


⇨ **IAM** Group "**Testing (EC2 Full access)**" with 2 Users Attached Details.

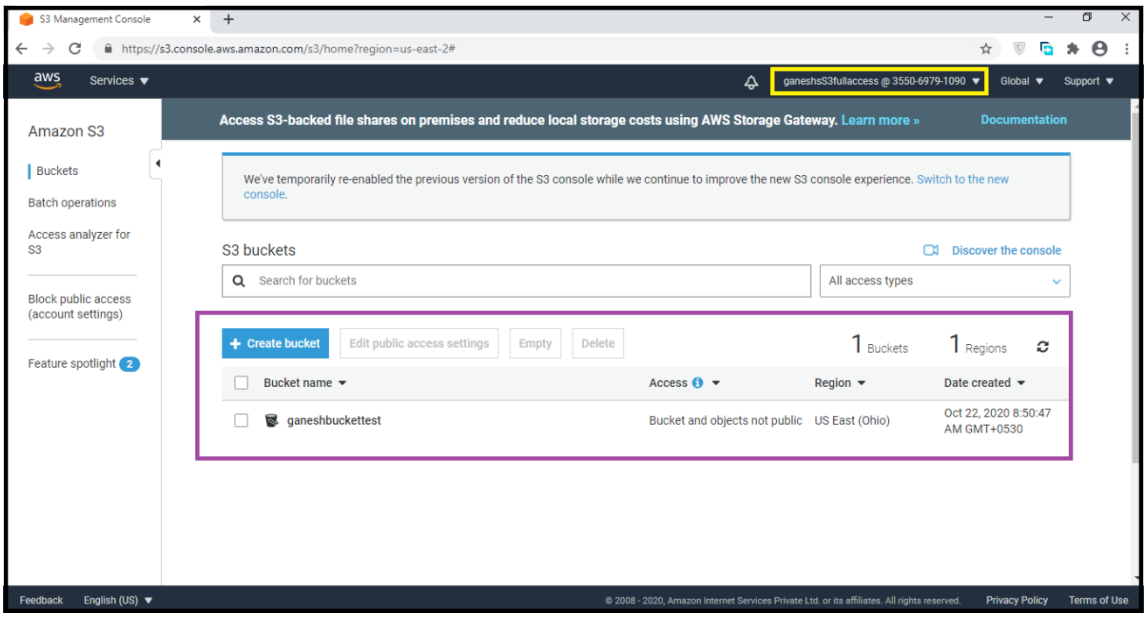
➔ "**nexususer**" (User 1: - No Access at User Level).
➔ "**ganeshsS3fullaccess**" (User 2: - S3 Full Access at User Level).



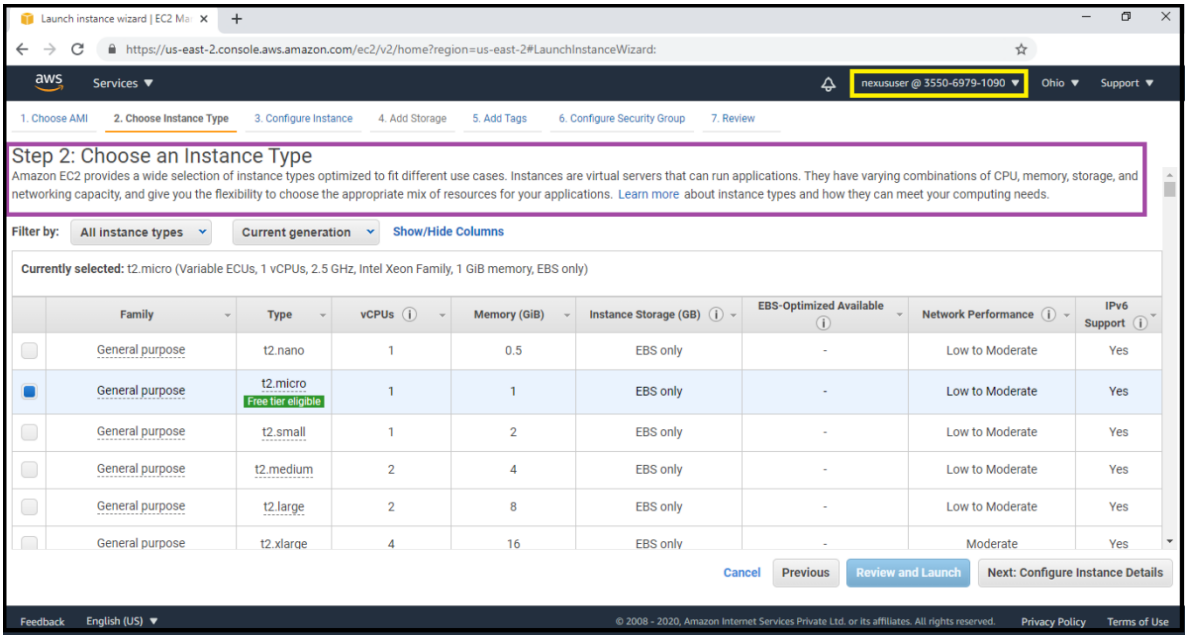
⇨ IAM Group "**Testing**" with **EC2FullAccess Permission** Details.



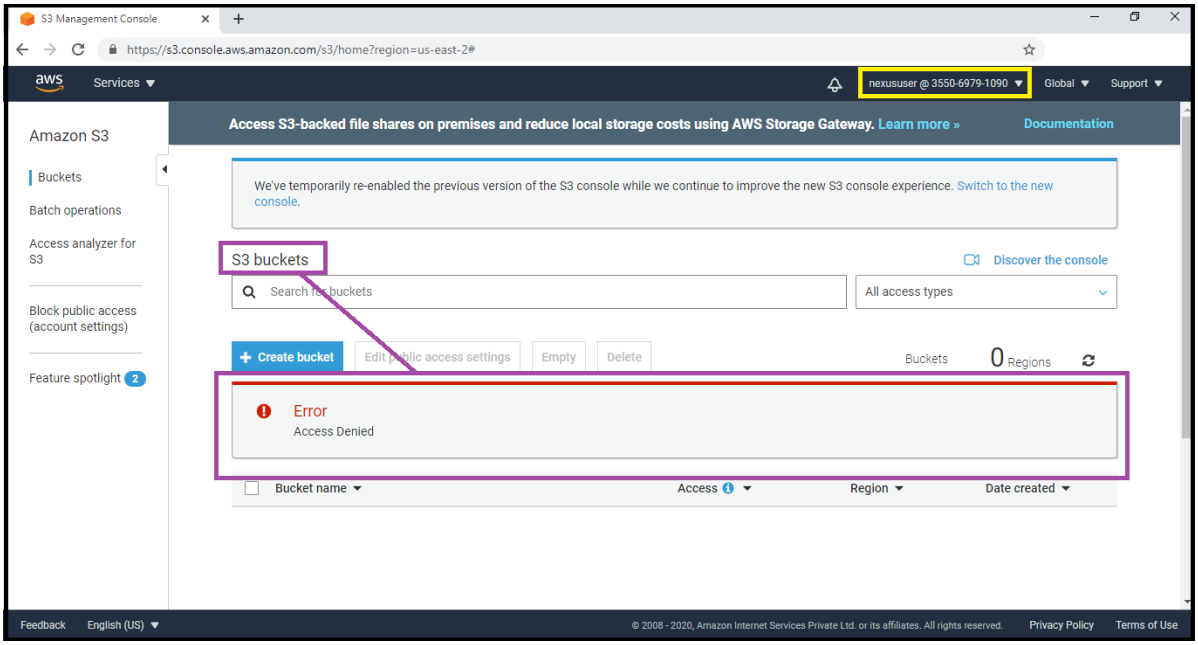
⇨ Logged in as User "**ganeshsS3fullaccess**" which has S3 full access at **User Level** & it's been attached to the Group "**Testing**" which has EC2 full access at the **Group Level**; The User "**ganeshsS3fullaccess**" is able to **Create a New Instance successfully**.



⇨ User "**ganeshsS3fullaccess**" which has S3 full access at **User Level** & it's been attached to the Group "**Testing**" which has EC2 full access at the **Group Level**; The User "**ganeshsS3fullaccess**" is able to **Create a S3 Bucket successfully**.



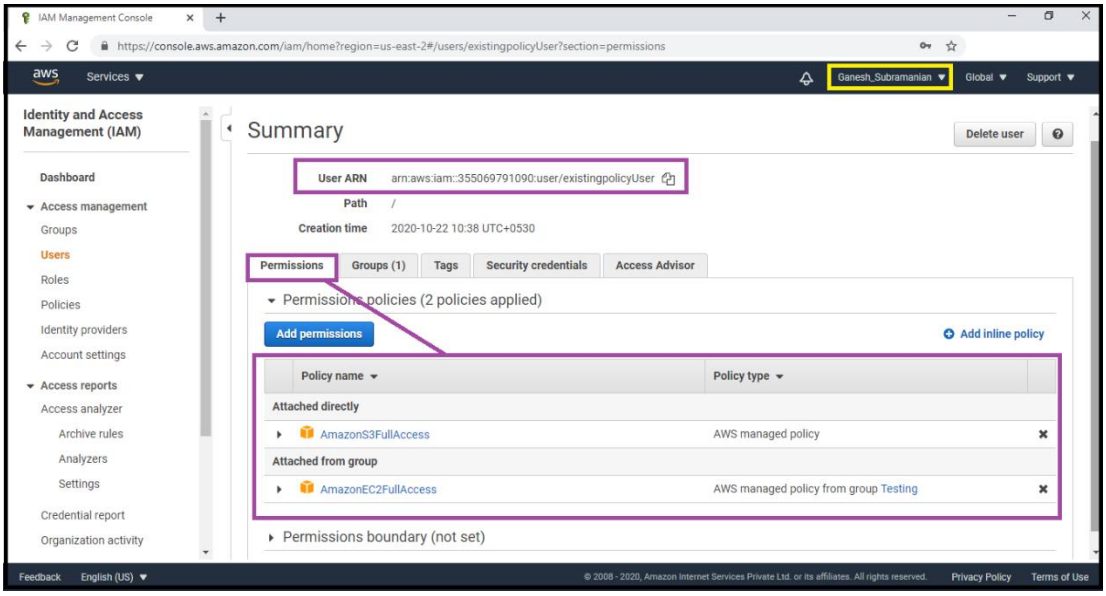
⇨ Logged in as User "**nexususer**" which has been attached to the Group "**Testing**" which has EC2 full access at the Group Level; The User "**nexususer**" is able to **Create a New Instance successfully**.



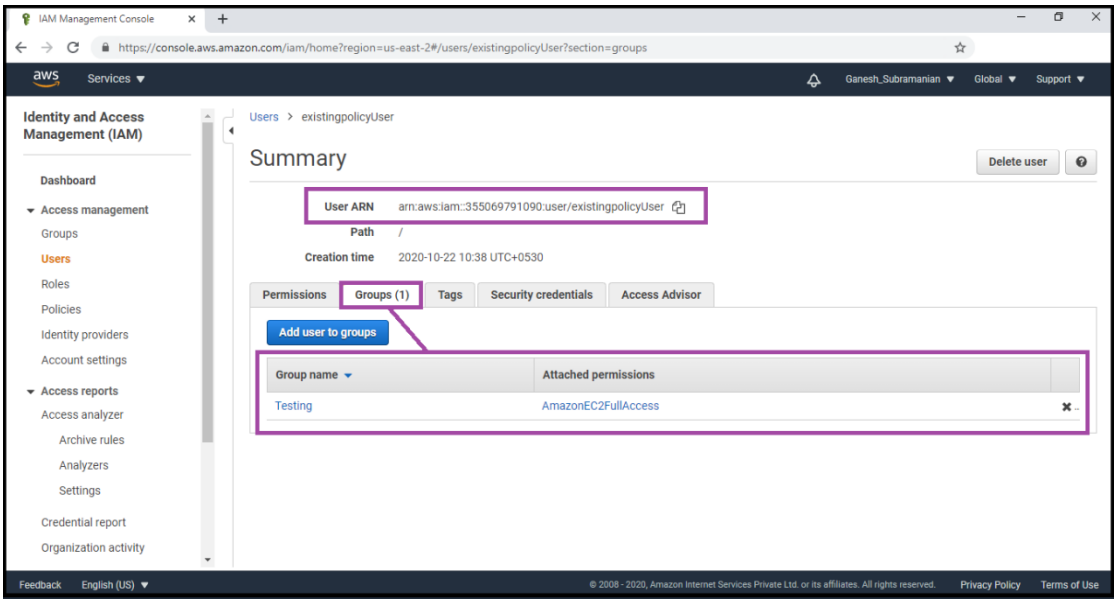
⇨ User "**nexususer**" which has **DOES NOT** have S3 full access at User Level & it's been attached to the Group "**Testing**" which has EC2 full access at the Group Level; The User "**nexususer**" is **Unable** to Create a S3 Bucket successfully.

Task 6: Copy policies from the existing user

Screenshot 7: attach user summary of the user from which you create a new user

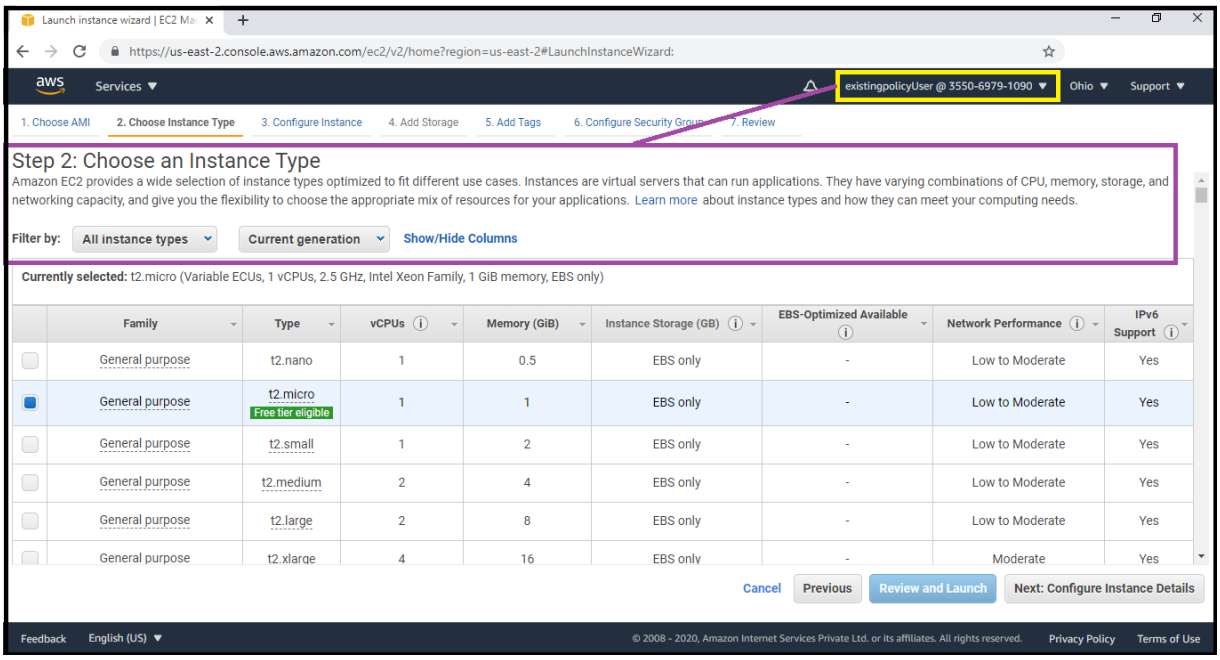


⇨ New User "**existingpolicyUser**" which is given the permission Copied from existing user "**ganeshsS3fullaccess**" where the User "**ganeshsS3fullaccess**" has S3 full access at User Level & EC2 full access at Group Level.

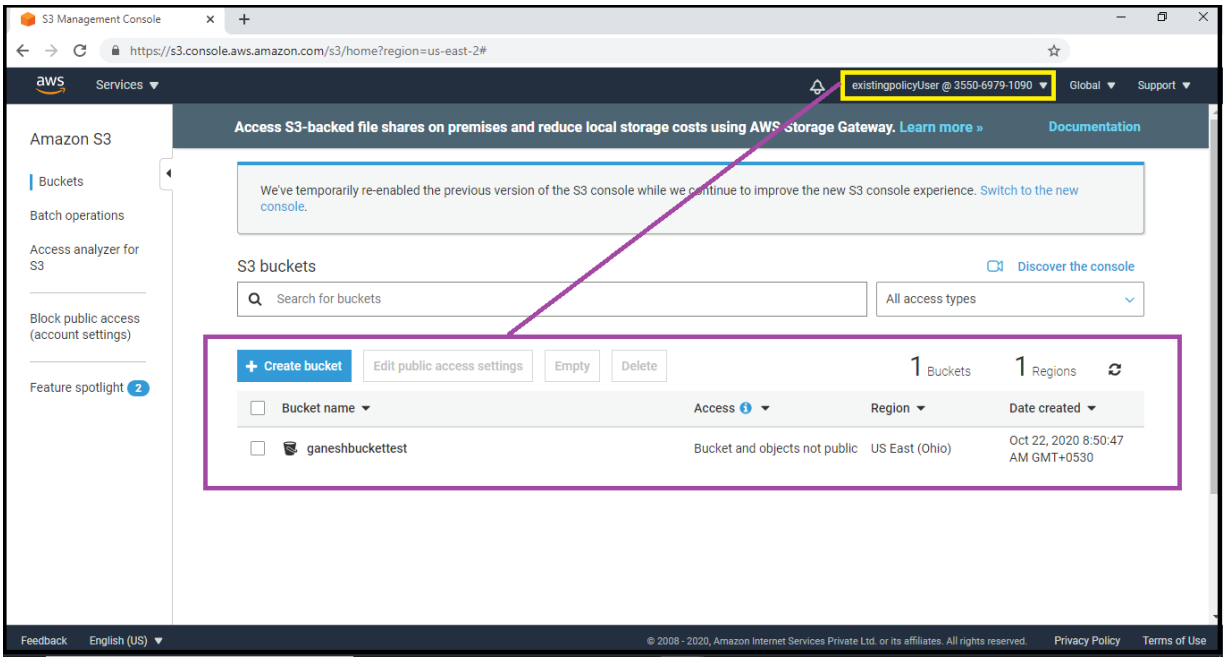


⇨ New User "**existingpolicyUser**" which is given the permission Copied from existing user "**ganeshsS3fullaccess**" where the User "**ganeshsS3fullaccess**" has S3 full access at User Level & EC2 full access at Group Level.

Screenshot 8: login as this user show that this policy is in effect

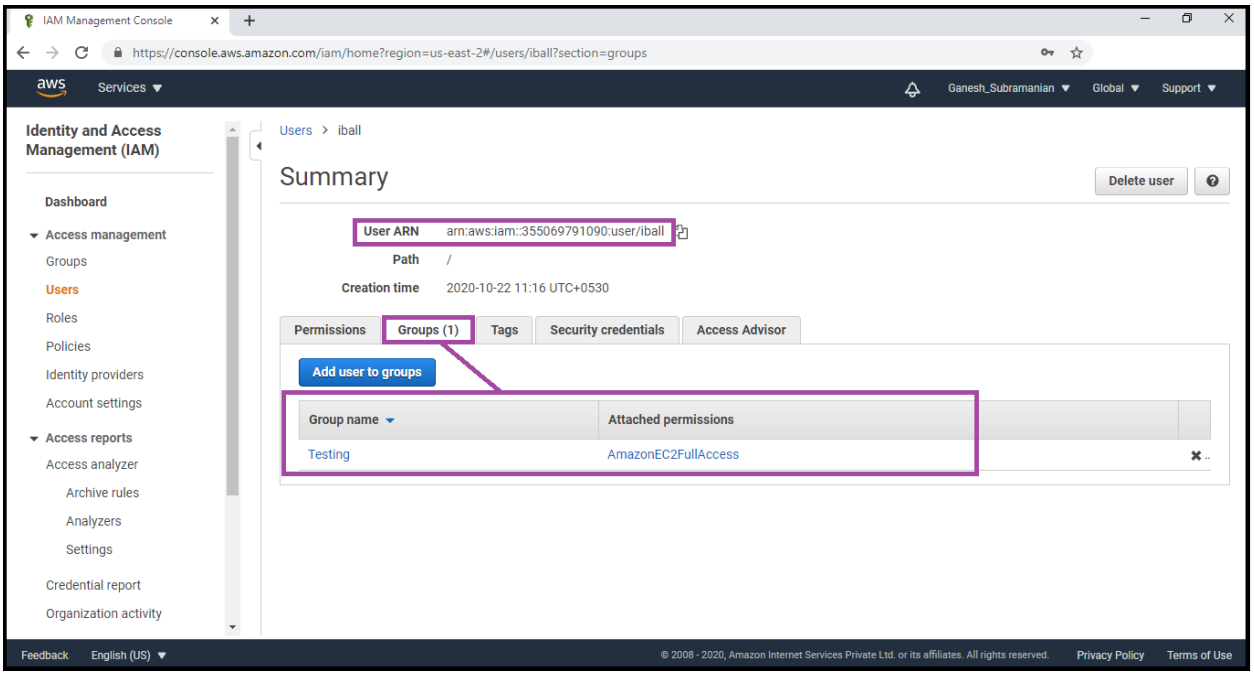


⇨ Logged in as New User "**existingpolicyUser**" and it has **EC2 full access.**

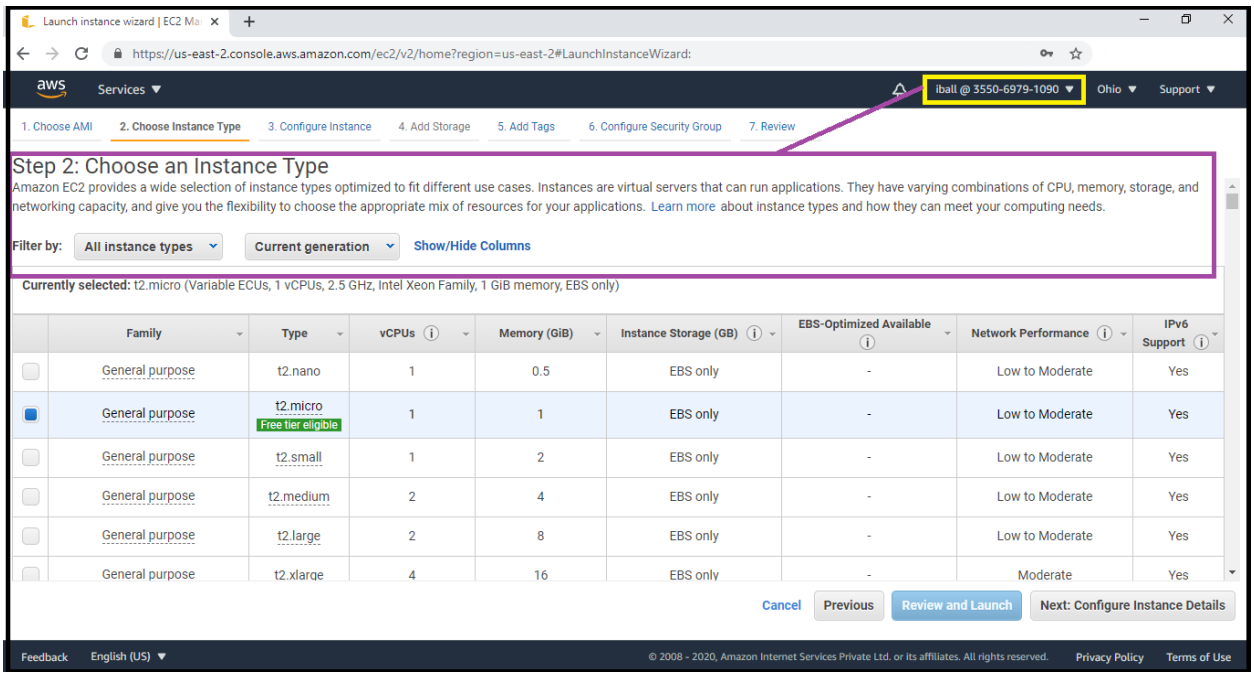


⇨ Logged in as New User "**existingpolicyUser**" and it has **S3 full access.**

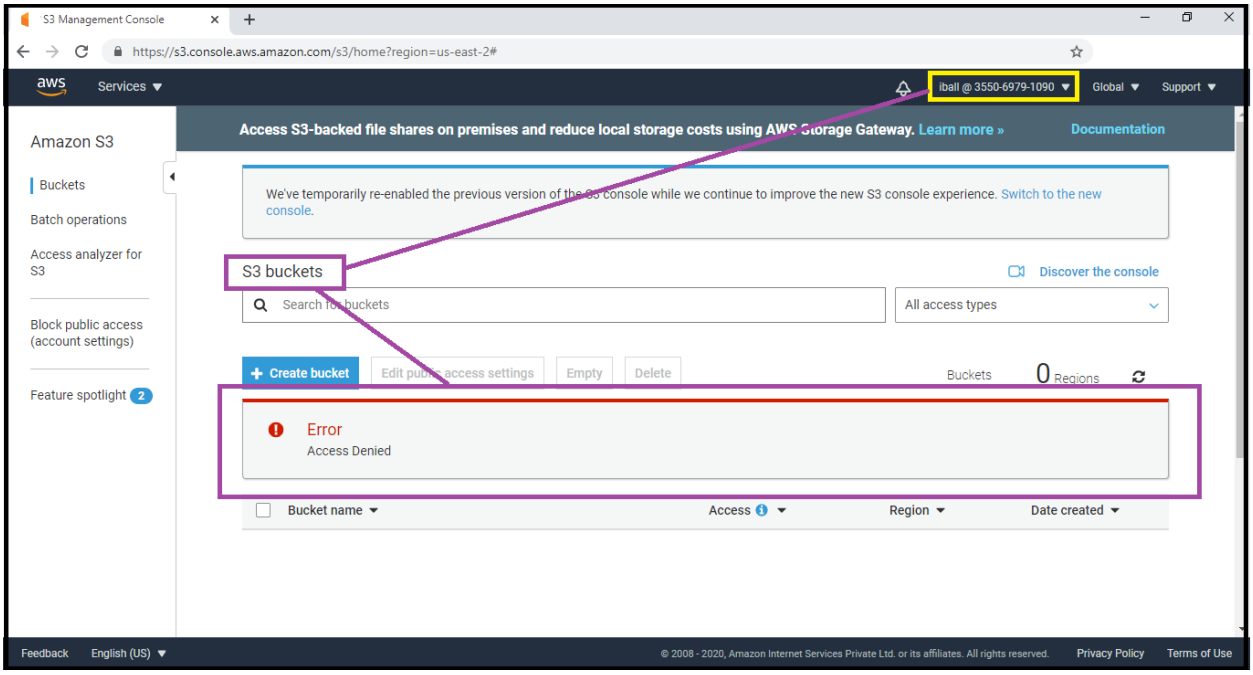
Task 7: Add user to a group in the process of creating a user



⇨ New User "**iball**" which is Added to User Group of "**Testing**" which has **EC2 full access**.



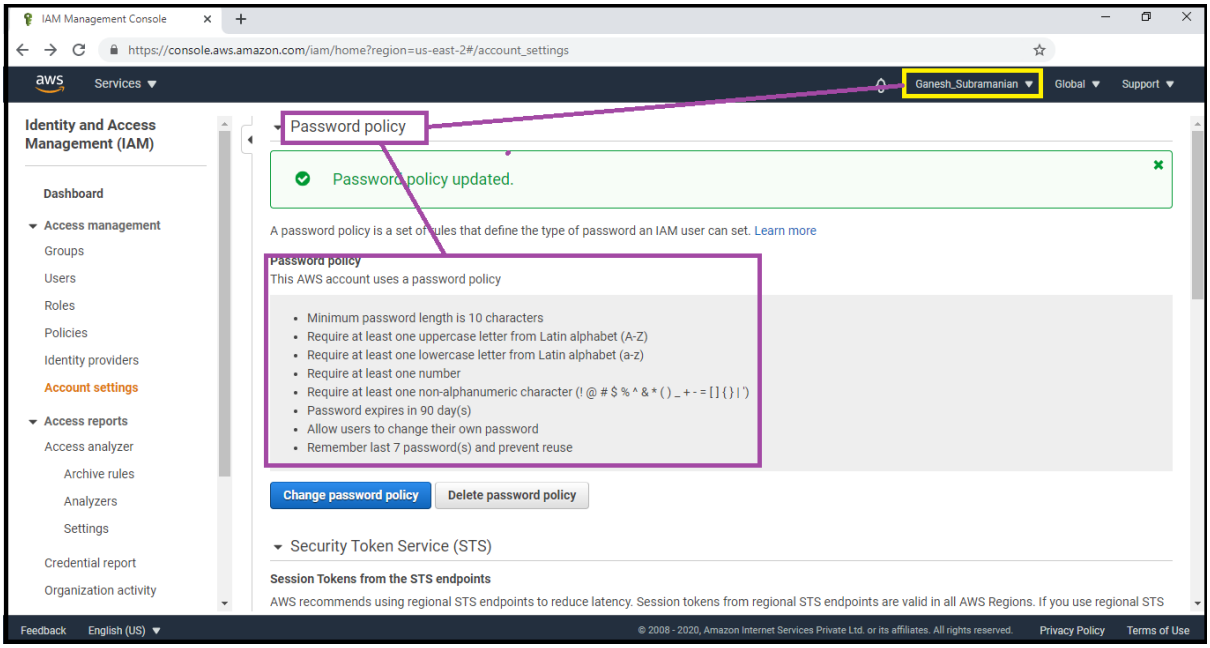
⇨ Logged in as New User "**iball**" and it has **EC2 full access**.



⇨ Logged in as New User "**iball**" and it **Does Not have S3 full access**, since "**Testing**" Group has **EC2 Full Access only.**

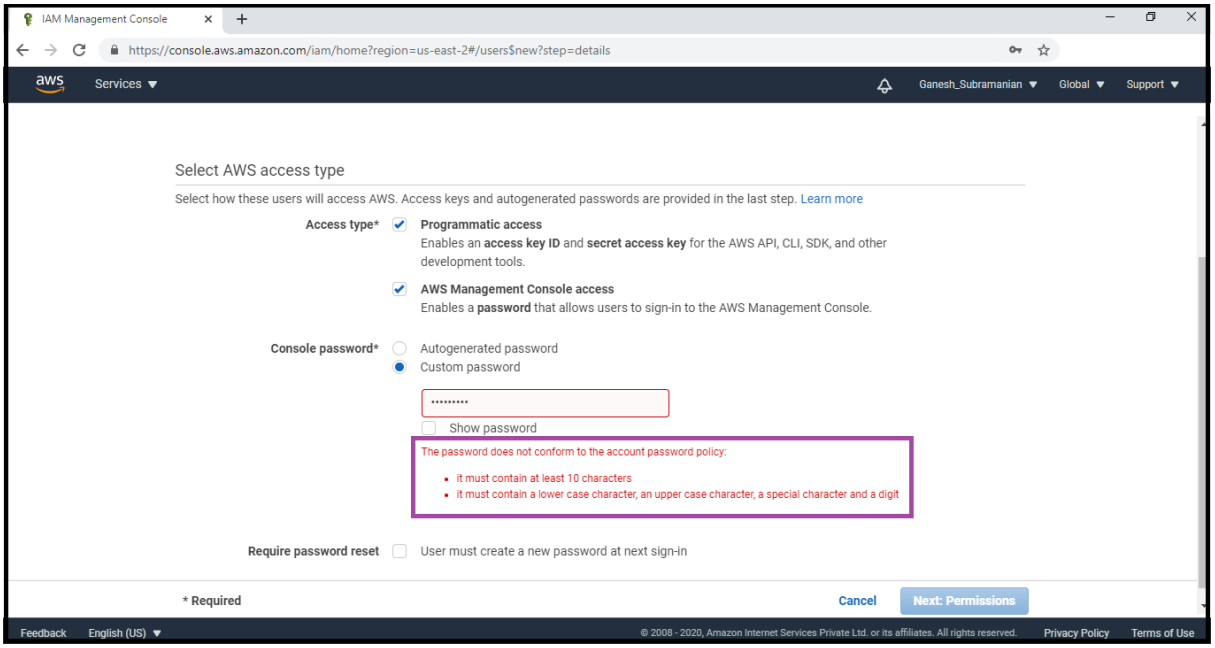
Task8: setting a password policy

Screenshot 9: password policy screen

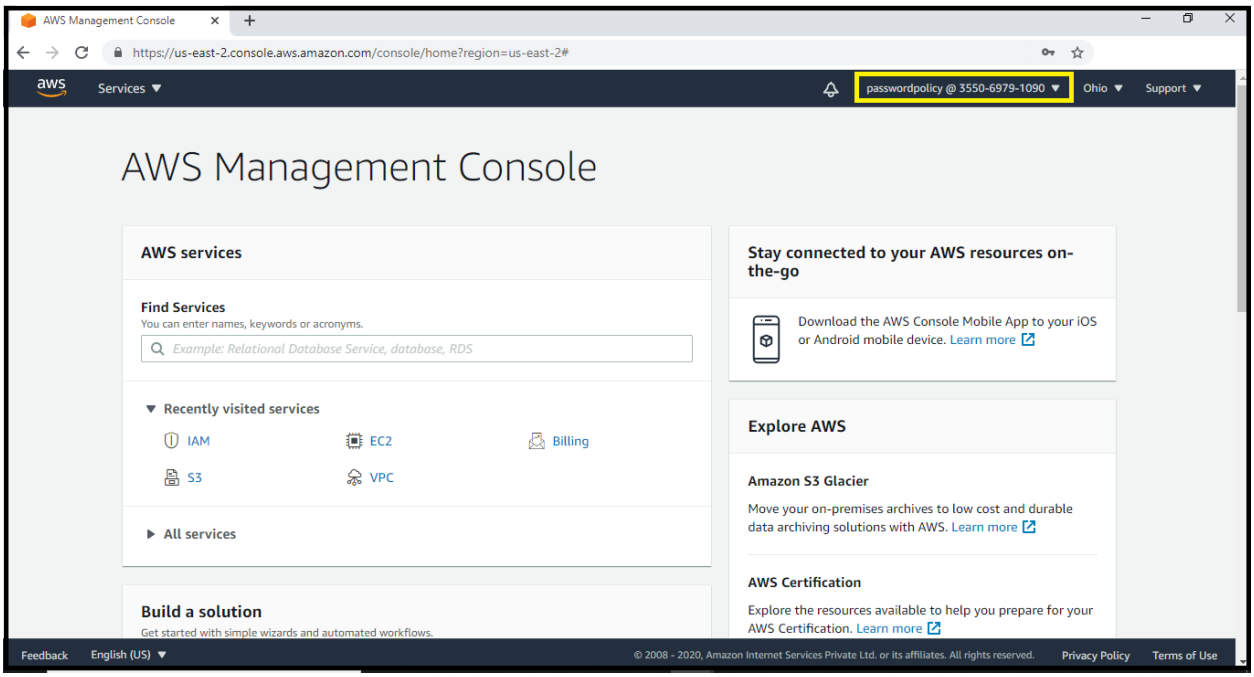


⇨ New **Password Policy** has been created.

Screenshot 10: login as the user and show password incompatibility error



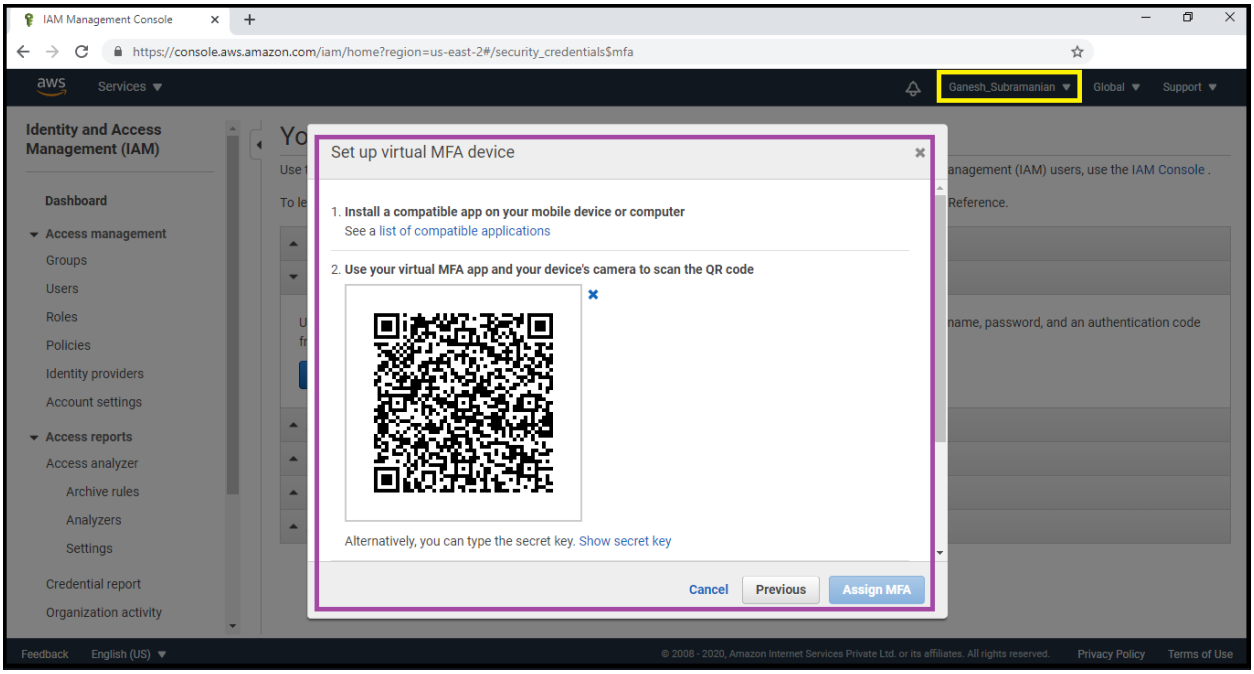
⇨ Password **Incompatibility Error.**



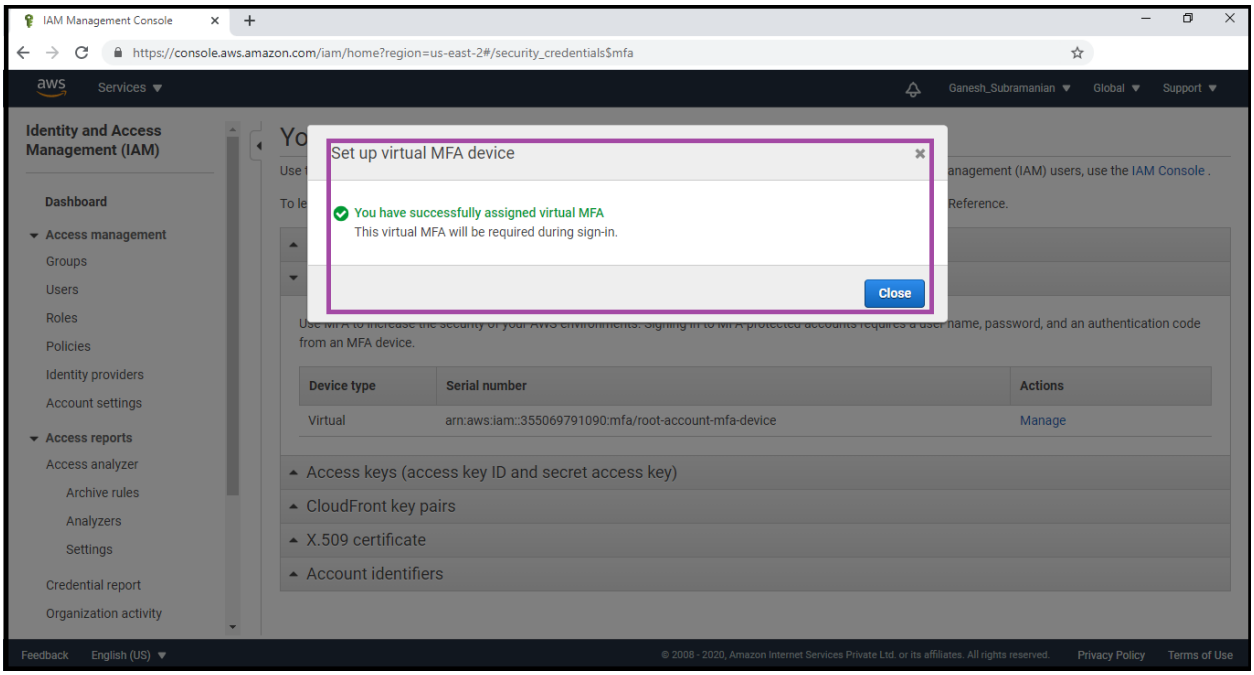
⇨ **Successful login** as a New user "**passwordpolicy**".

Task 9: Enabling MFA and using an MFA device

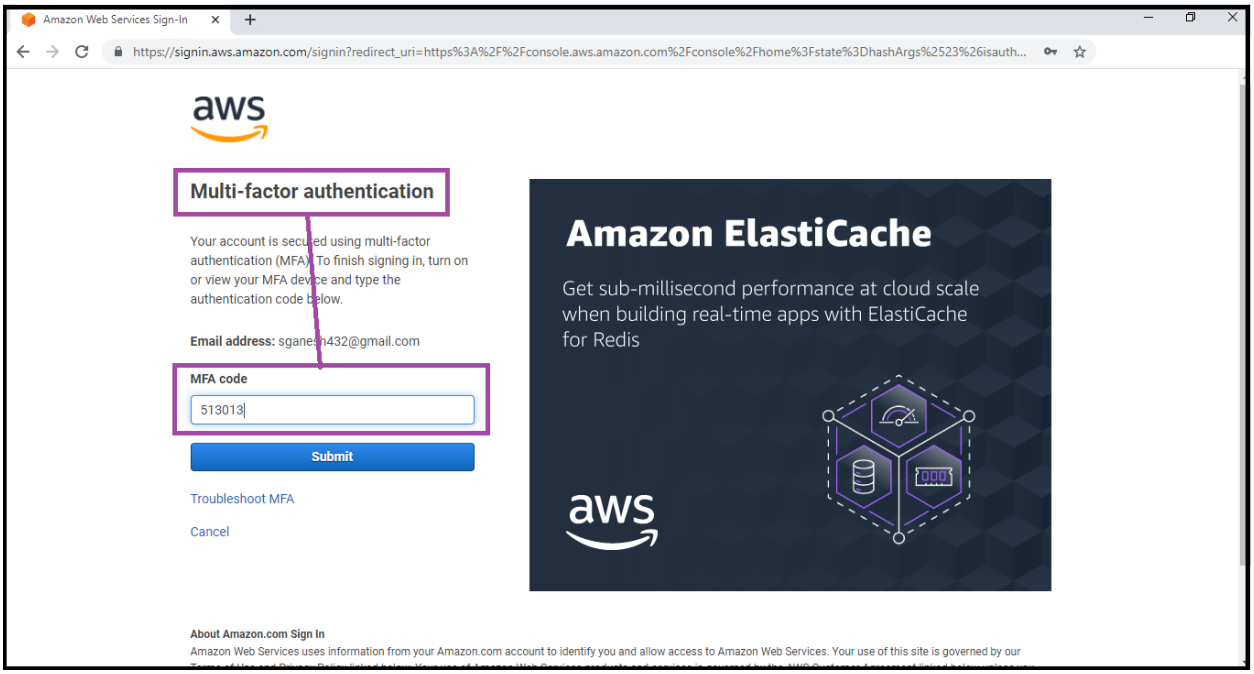
Screenshot 11: Enable MFA



⇨ **MFA** is **Enabled** and QR Code is requested to be Scanned for further process.



Screenshot 12: login screen for MFA



⇨ **MFA Code** is being Prompted during the Login session after Enabling the MFA option.