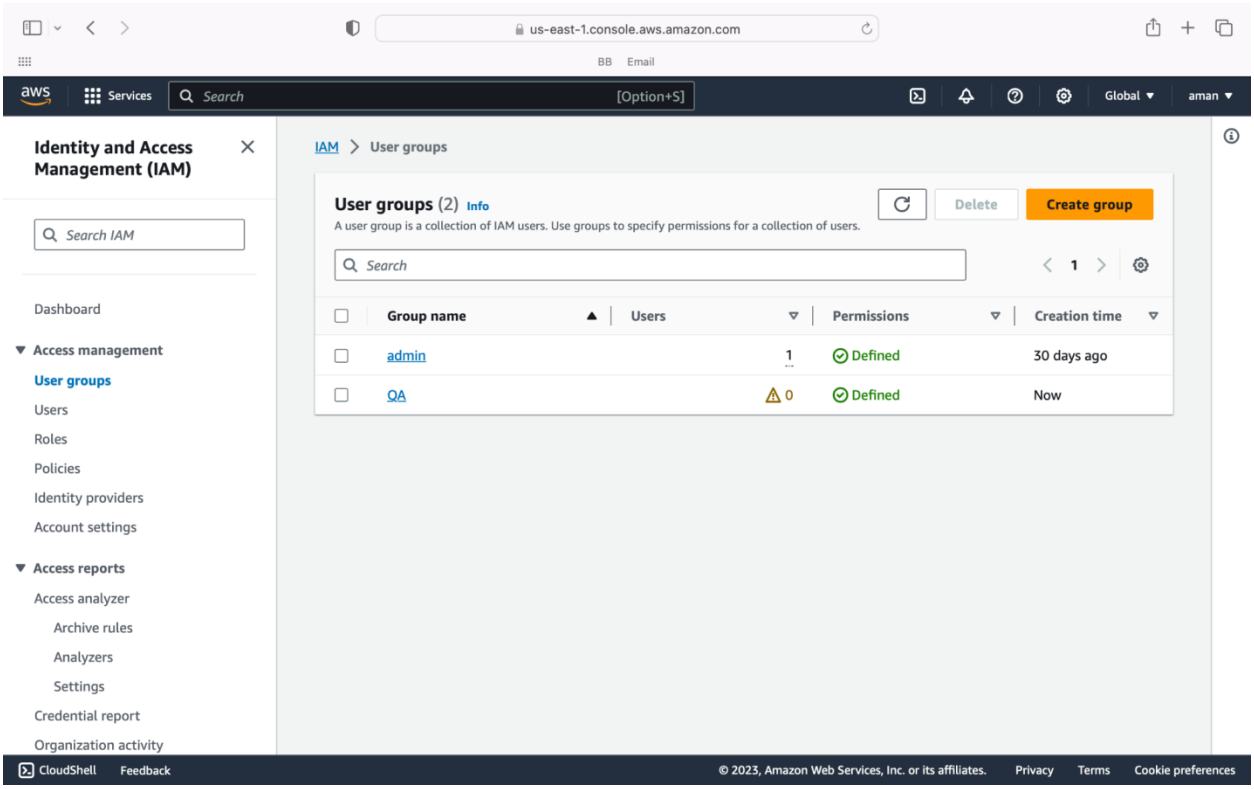
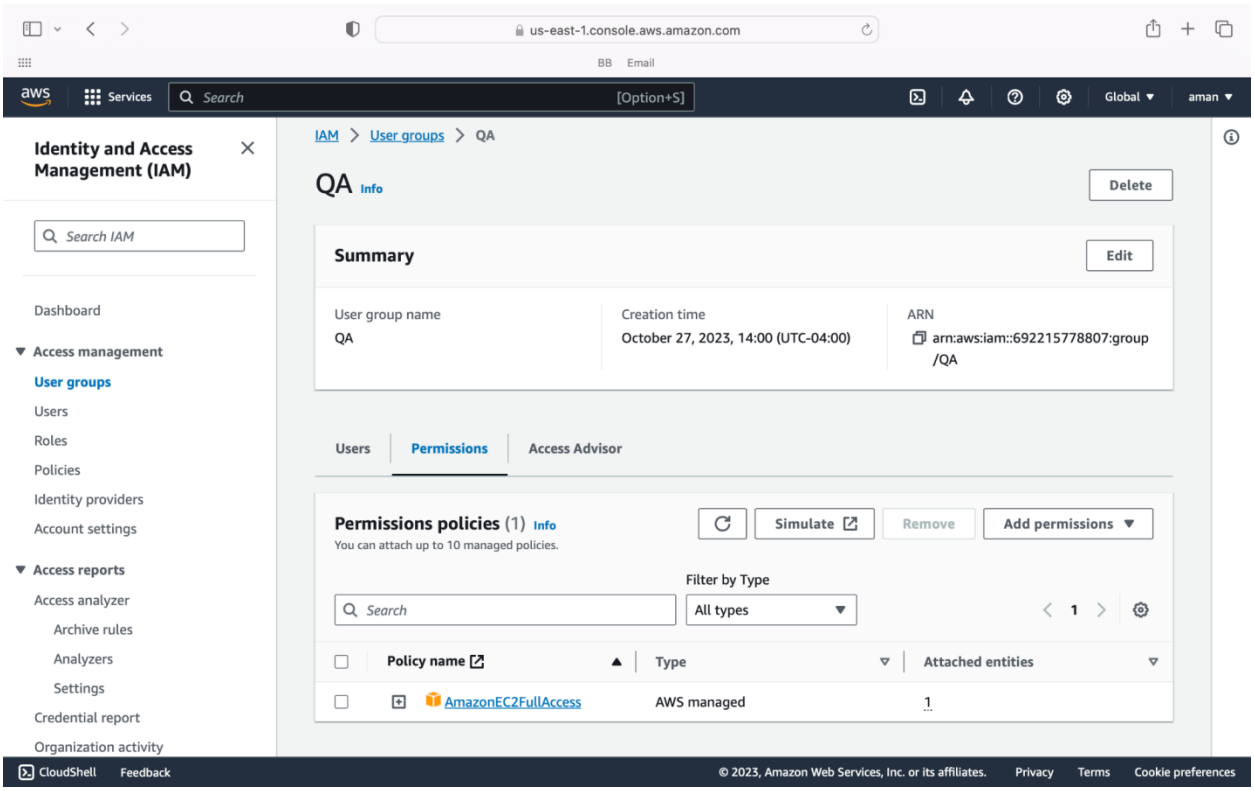
Identity and Access Management

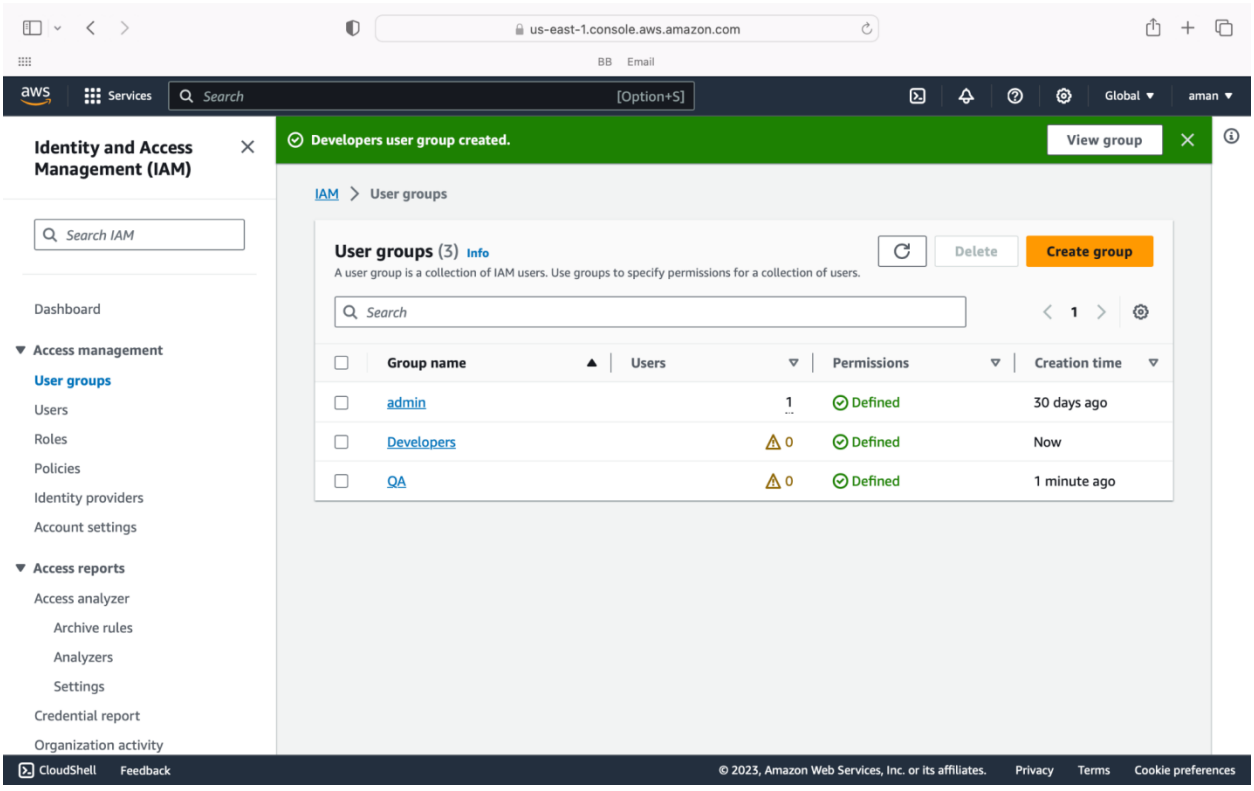
Follow the steps in Section 13 'Security Best Practices', section 'Identity and Access Management', to create a group, create users, and assign the users to a group. Submit a screenshot of step 3, with the new group visible.



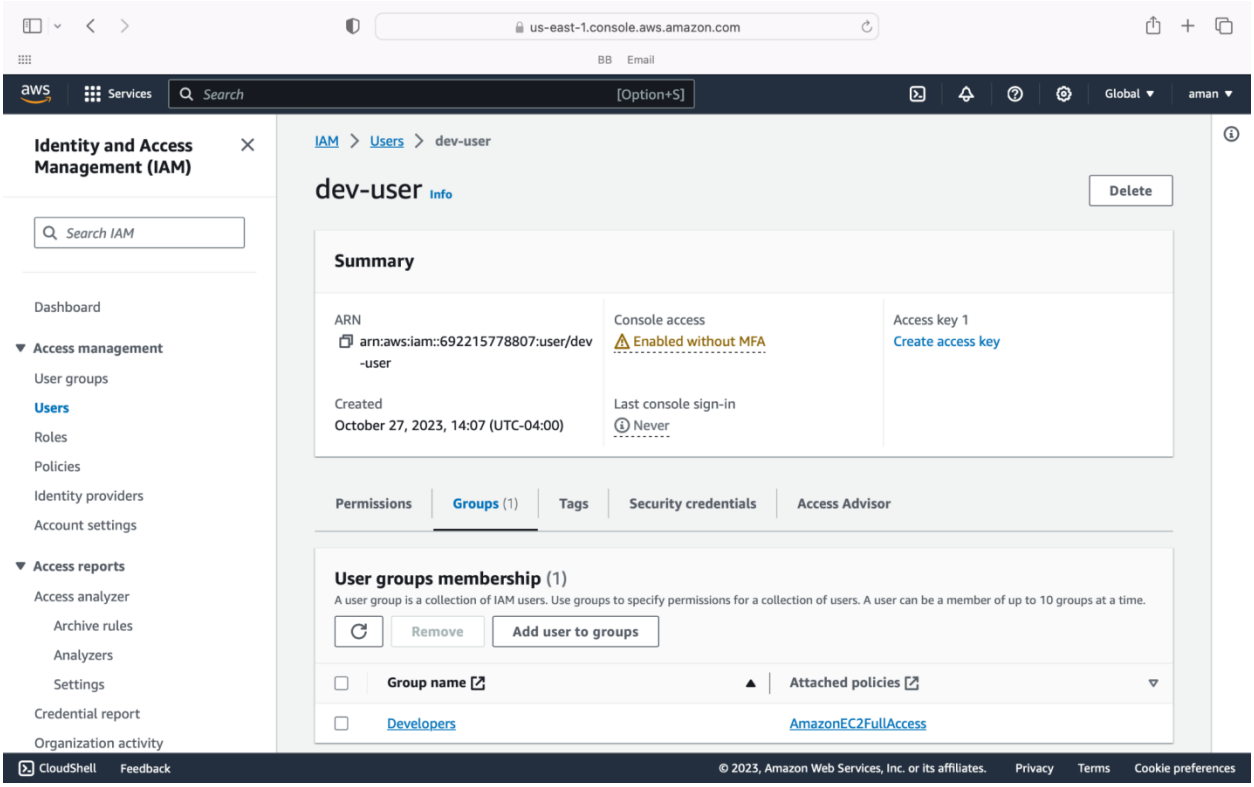
Follow the steps to attach a policy to the group. Submit a screenshot of step 2, with the selected policy visible.



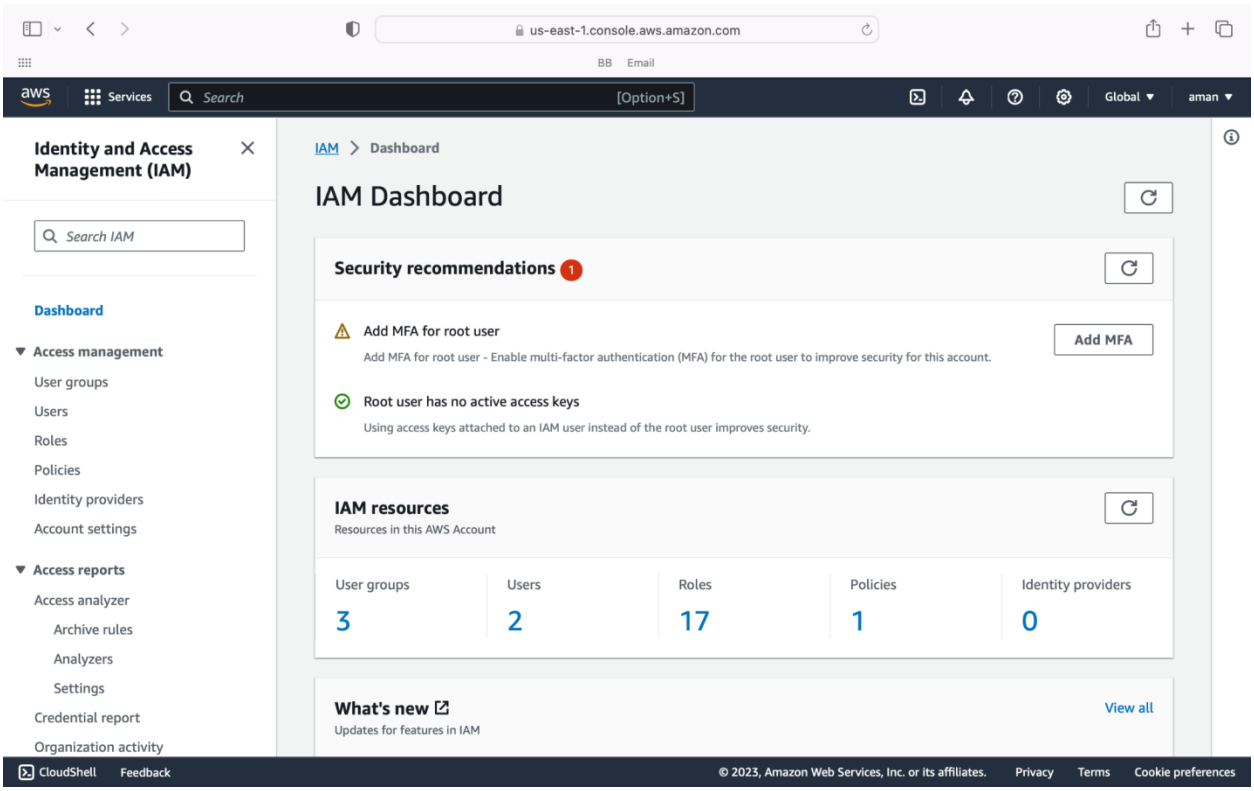
Follow the steps to create the Developers Group. Submit a screenshot of step 5, with the two groups visible.



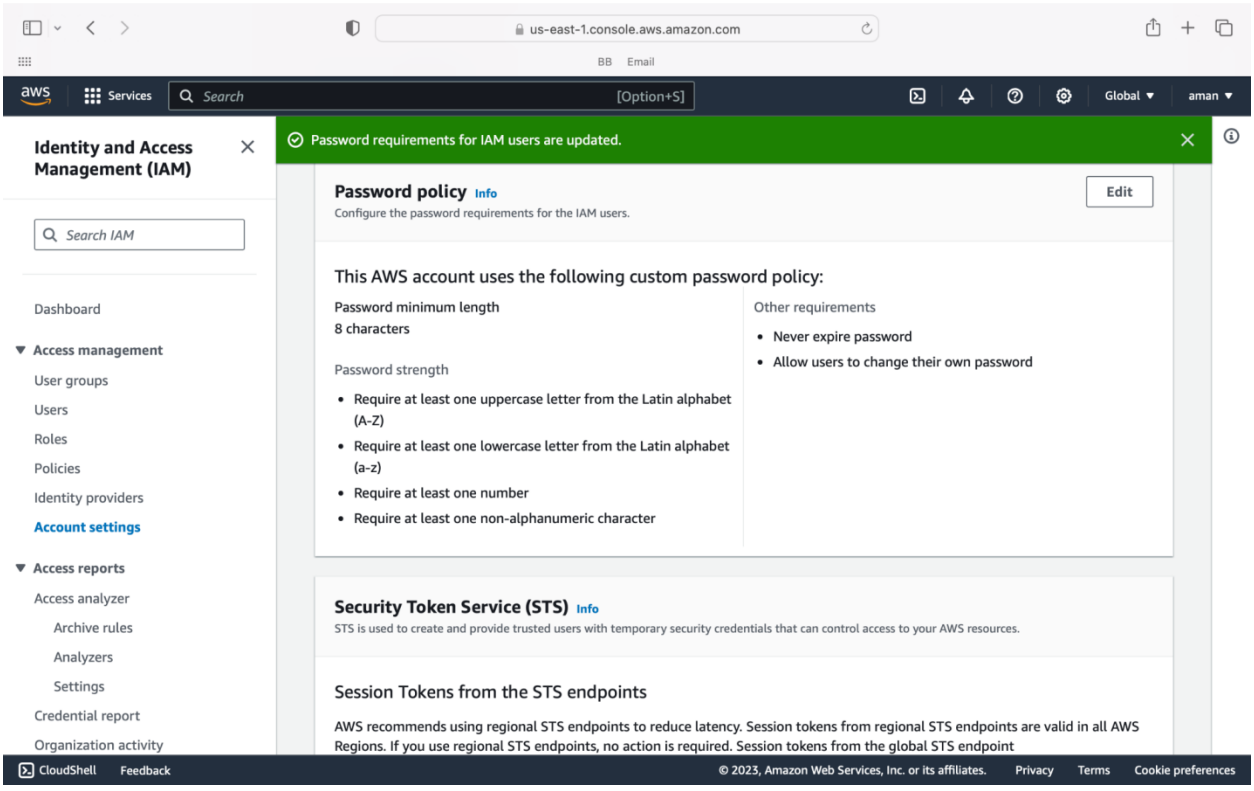
Follow the steps to create a user, and add the user to the Developers Group. Submit a screenshot of step 4 in which the user was successfully created.



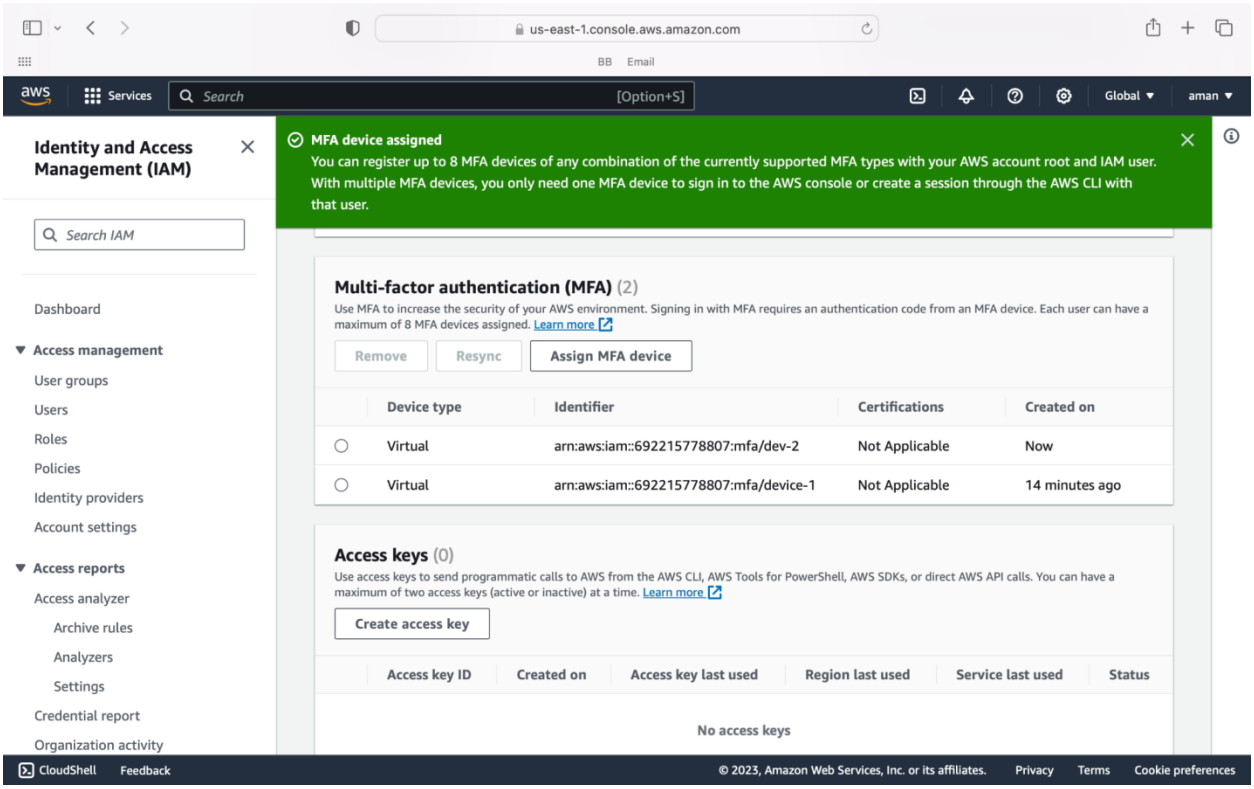
Follow the steps to delete the root access keys. Submit a screenshot of step 4 in which the security status verifies the root access keys were deleted.



Follow the steps to apply an IAM password policy. Submit a screenshot of step 5 in which it verifies a password policy has been successfully set.

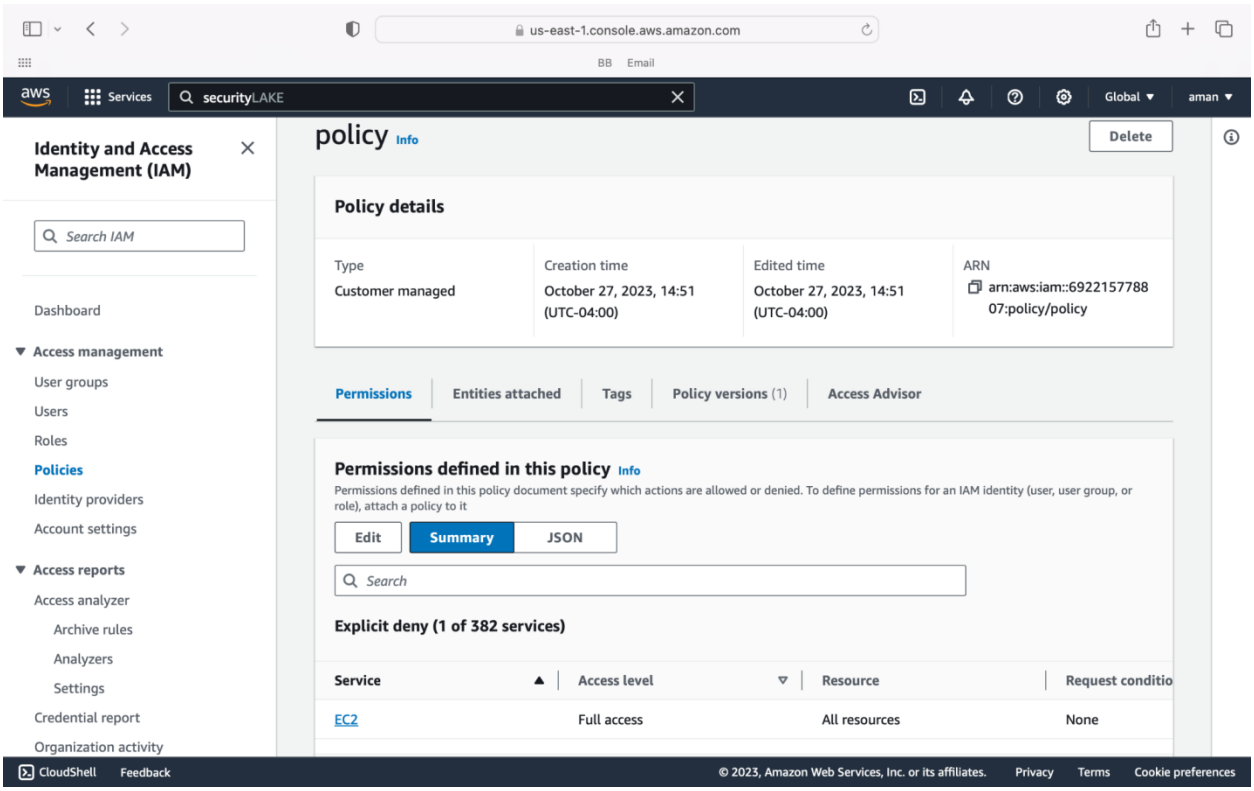


Follow the steps to enable MFA, and try out a virtual MFA Device. Submit a screenshot of step 3, in which the IAM dashboard displays Security Status 5 out of 5.

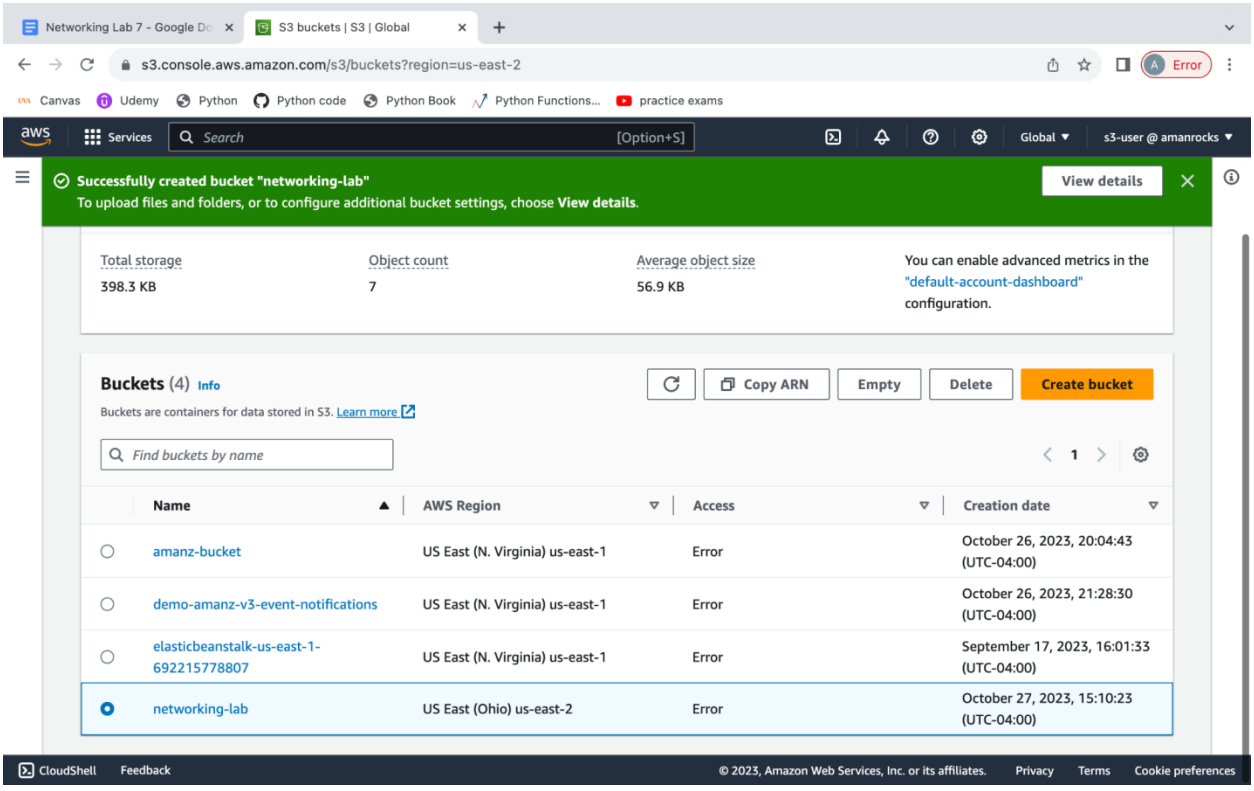


IAM Policies

Follow the steps to create a policy related to S3. Submit a screenshot of step 9, displaying that the policy has been successfully created.

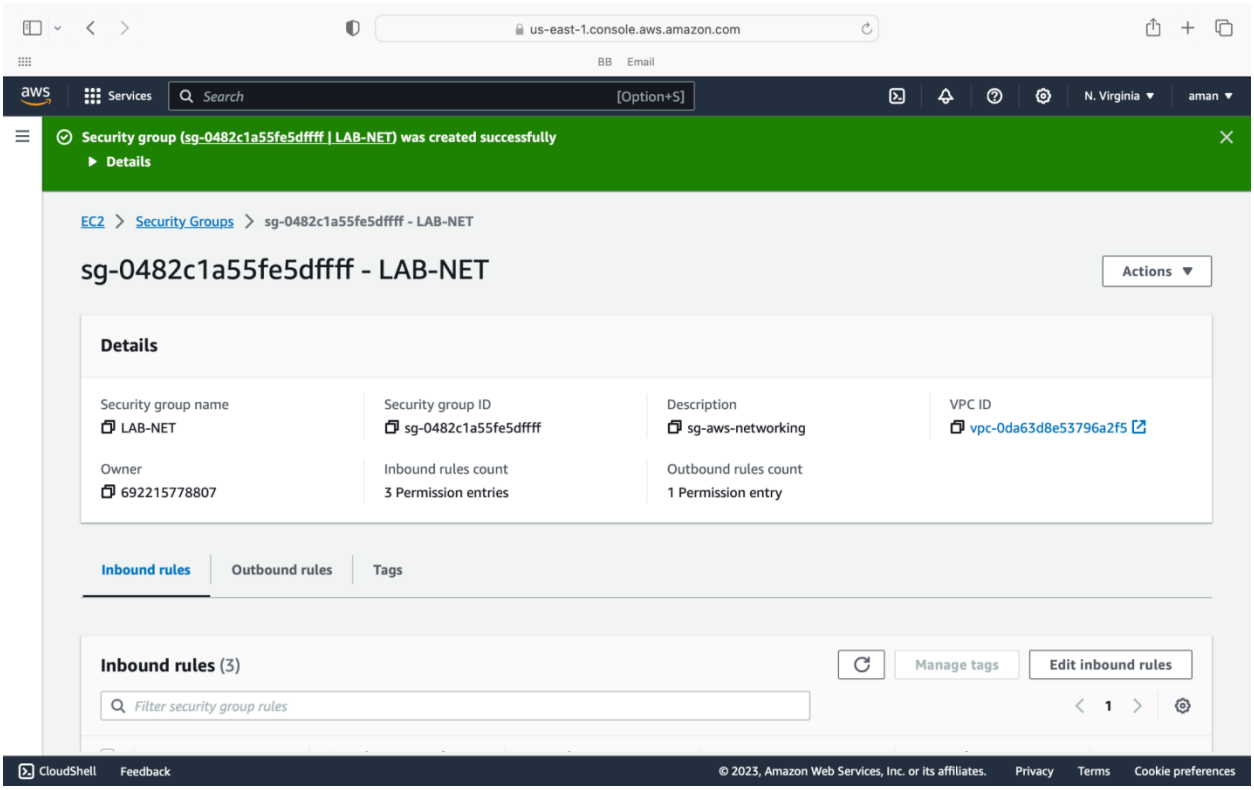


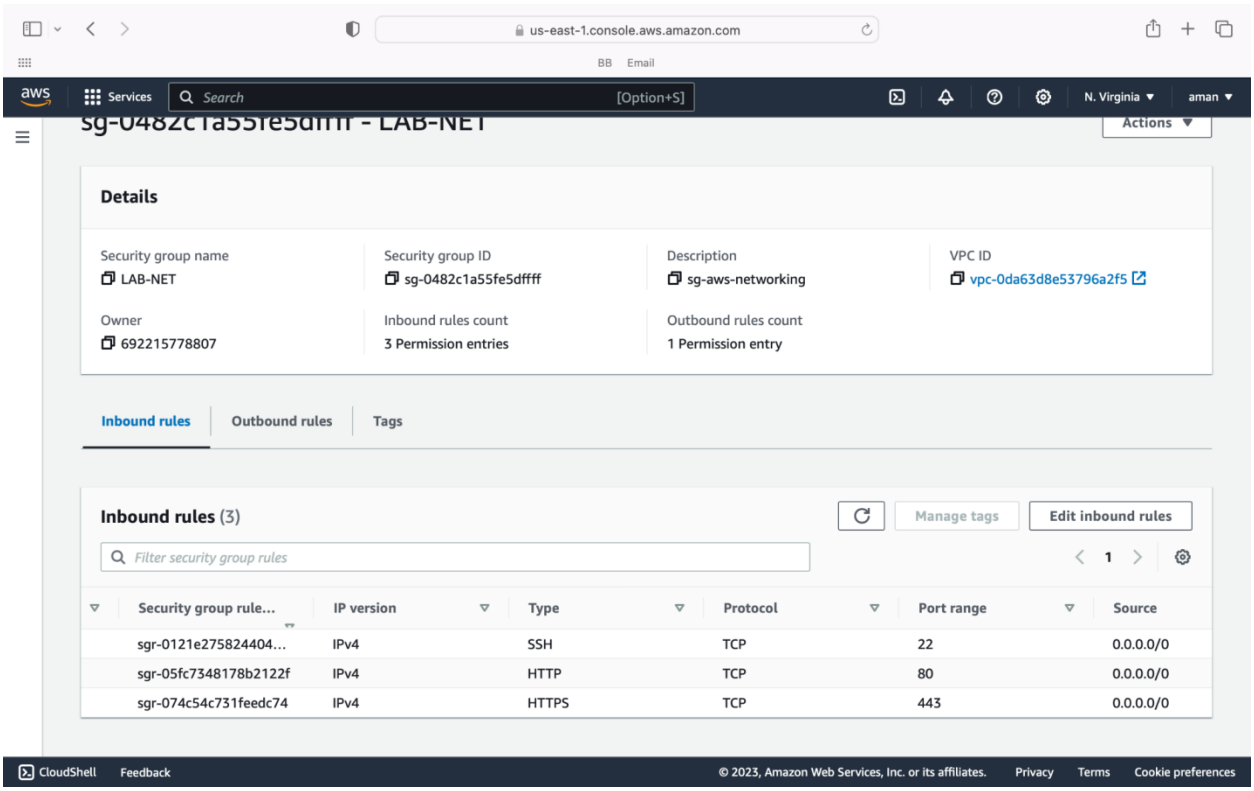
Follow the steps to create a user and assign a policy to it. Submit a screenshot of step 8 in which the user successfully creates a bucket.



Security Groups

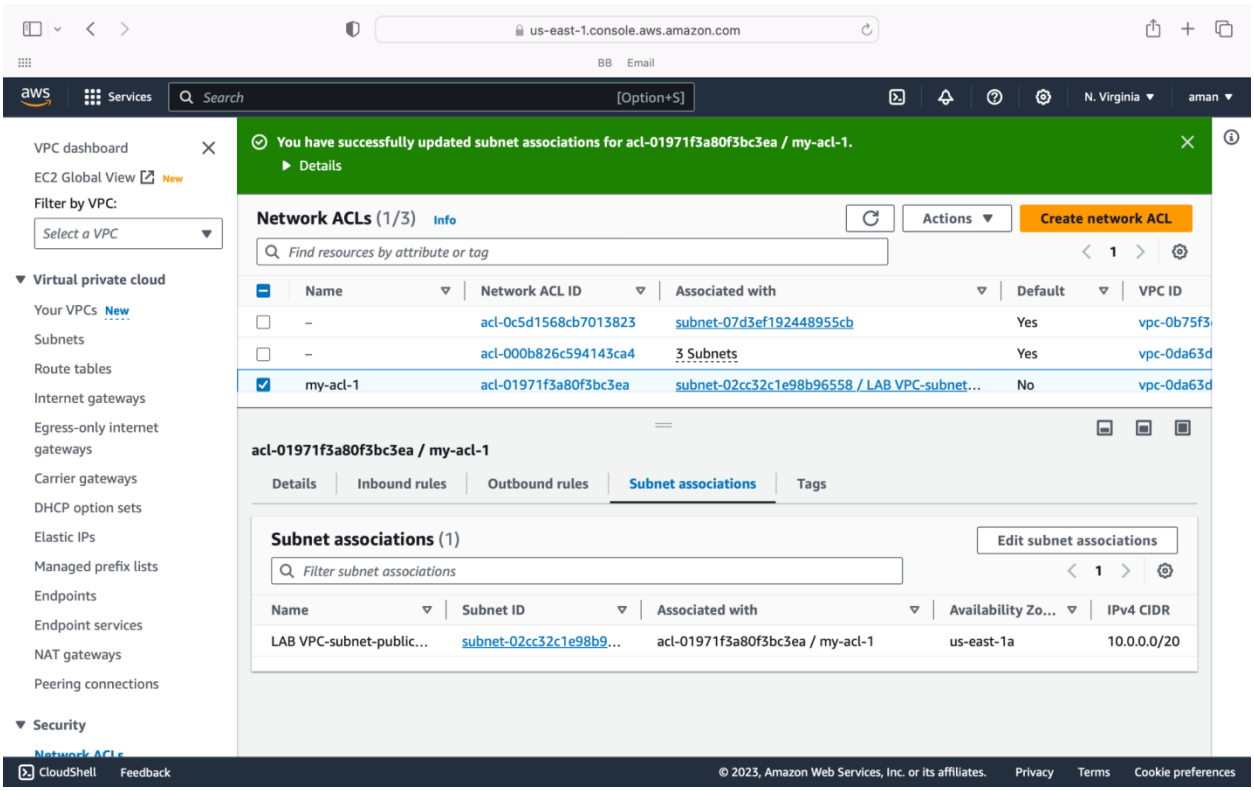
Follow the steps to create a Security Group. Submit a screenshot of step 3 with the new security group visible.





Network ACLs

Follow the steps to view the Network ACLs in the AWS Management Portal, and create a new Network ACL. Submit a screenshot of step 15 in which you verify the Subnet Association of the new Network ACL.


us-east-1.console.aws.amazon.com
BB Email
aws Services Search [Option+S] N. Virginia aman
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
You have successfully updated subnet associations for acl-01971f3a80f3bc3ea / my-acl-1.
Details
Network ACLs (1/3) Info
Actions
Create network ACL
Find resources by attribute or tag
1
Name
Network ACL ID
Associated with
Default
VPC ID
– acl-0c5d1568cb7013823 subnet-07d3ef192448955cb Yes vpc-0b75f3
– acl-000b826c594143ca4 3 Subnets Yes vpc-0da63d
my-acl-1 acl-01971f3a80f3bc3ea subnet-02cc32c1e98b96558 / LAB VPC-subnet... No vpc-0da63d
acl-01971f3a80f3bc3ea / my-acl-1
Details
Inbound rules
Outbound rules
Subnet associations
Tags
Subnet associations (1)
Edit subnet associations
Filter subnet associations
1
Name
Subnet ID
Associated with
Availability Zo...
IPv4 CIDR
LAB VPC-subnet-public... subnet-02cc32c1e98b9... acl-01971f3a80f3bc3ea / my-acl-1 us-east-1a 10.0.0.0/20
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences