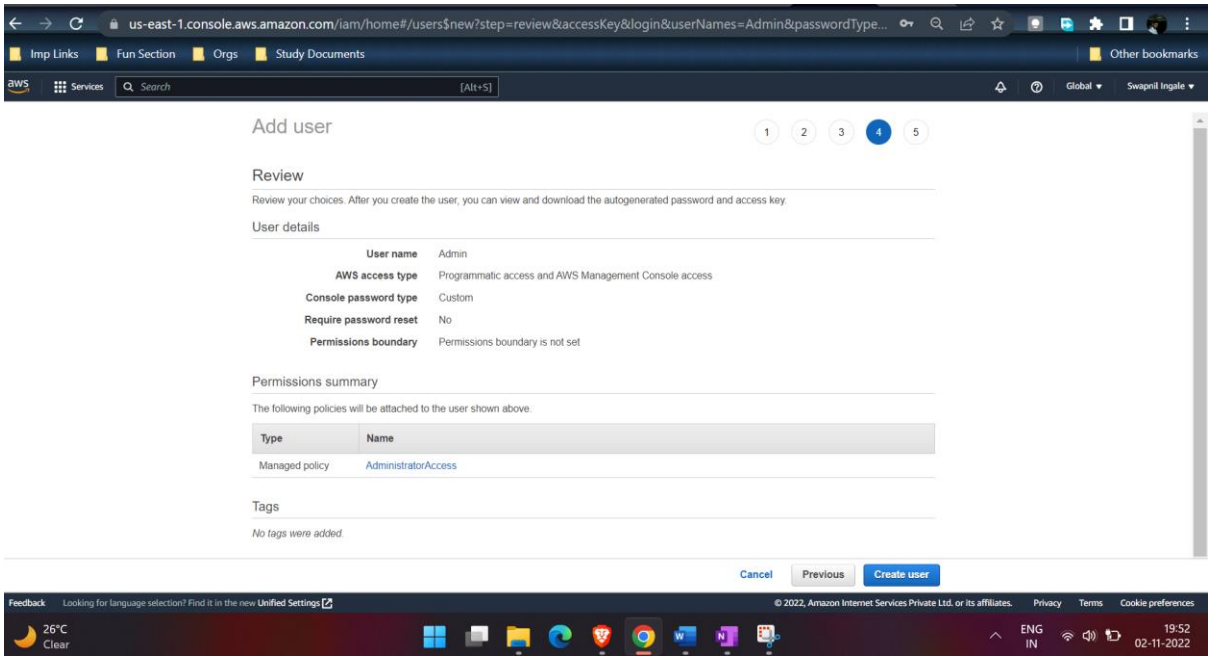
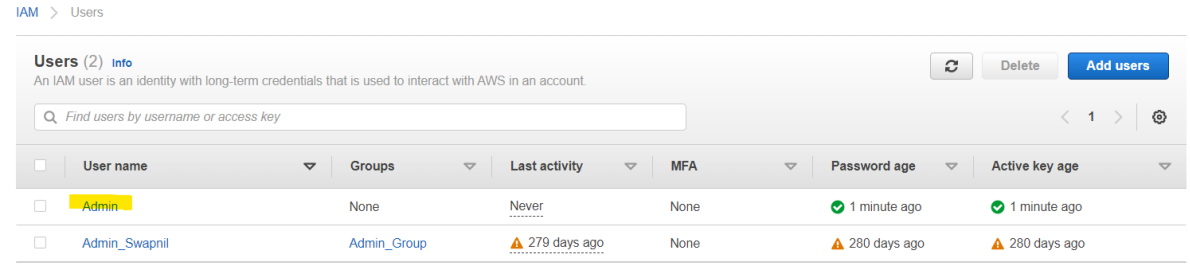
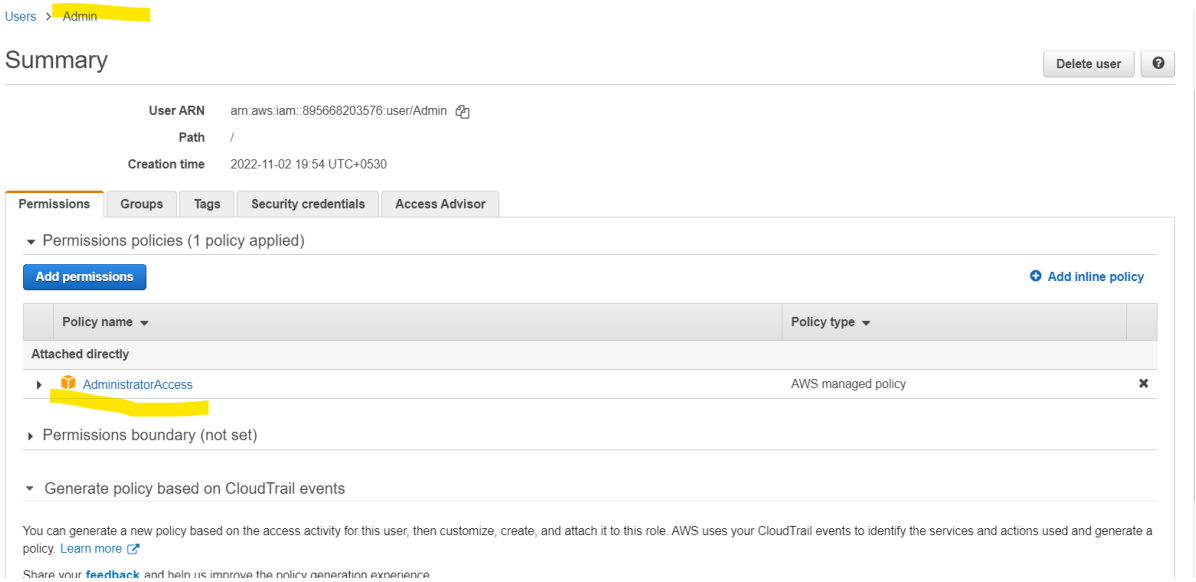
Assignment sheet for IAM

Assignment 1:- Create an IAM user with username of your own wish and grant administrator policy.

➔ **Ans:** Created IAM user “Admin” and provided administrator policy access.





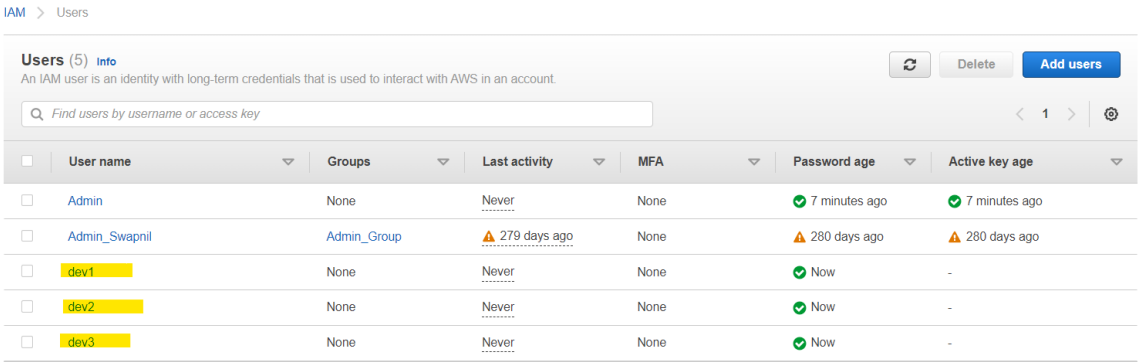


Assignment 2:- Hello students, in this assignment you need to prepare a developers' team of avengers.

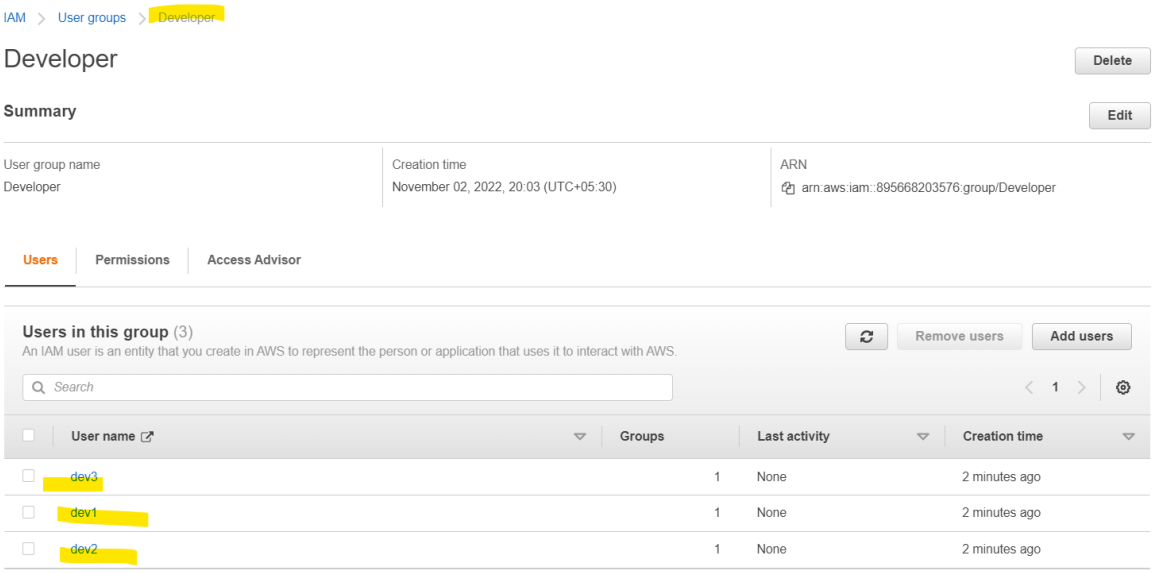
- Create 3 IAM users of avengers and assign them in developer's groups with IAM policy.

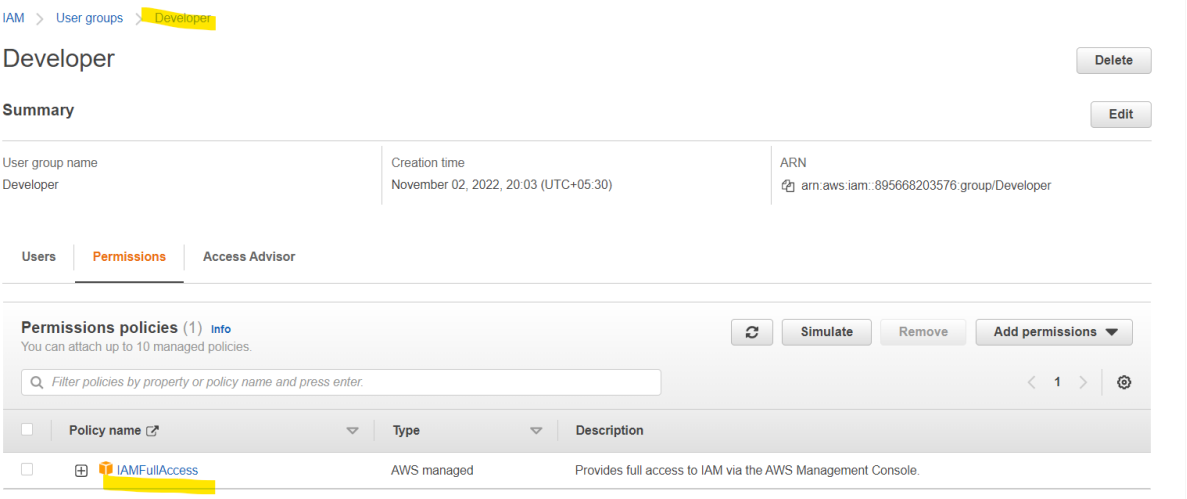
➔ Ans:

Created 3 users dev1, dev2, dev3.



Created group "Developer" with Policy IAMFullAccess and added all 3 users dev1, dev2, dev3 in it.





Assignment 3:- Define a condition in policy for expiration like

```
"DateGreaterThan": {"aws:CurrentTime":
"2020-04-01T00:00:00Z"},
"DateLessThan": {"aws:CurrentTime":
"2020-06-30T23:59:59Z"}
Define the span of 4 months as per your wish
```

➔ **Ans:** Created a Policy with 4 months expiration condition for iam list policies action

Create policy

1 2 3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor | JSON | Import managed policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:ListPolicies",
            "Resource": "*",
            "Condition": {
                "DateGreaterThan": {"aws:CurrentTime": "2022-11-02T00:00:00Z"},
                "DateLessThan": {"aws:CurrentTime": "2023-03-02T23:59:59Z"}
            }
        }
    ]
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Review policy

Name* Test_Expiration_Policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Filter

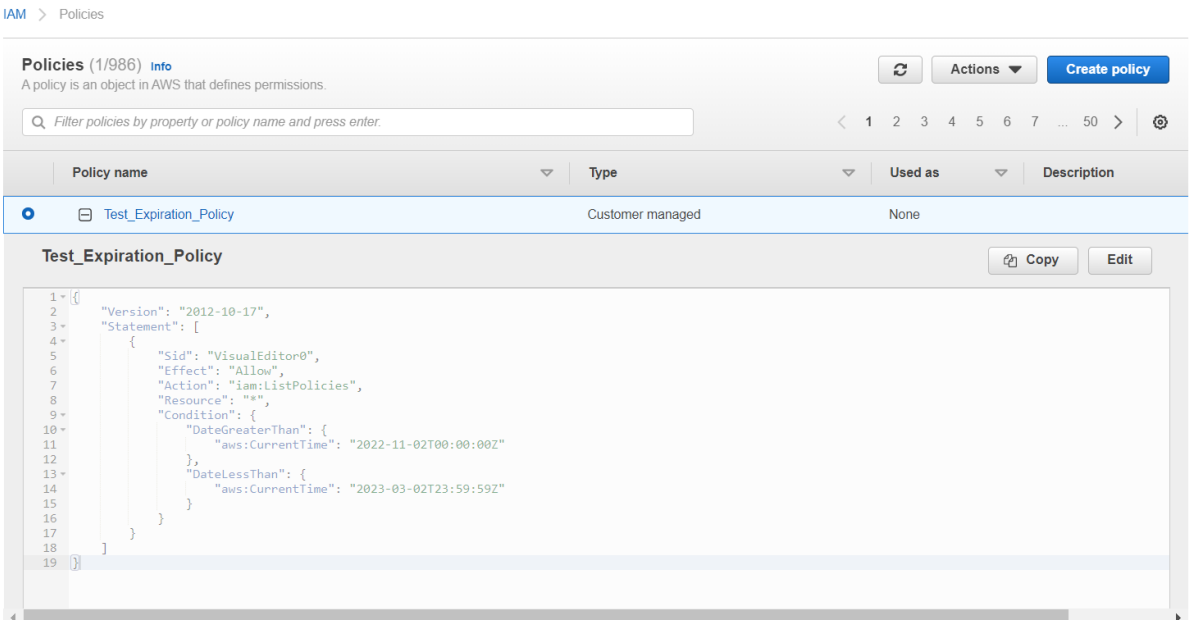
Service	Access level	Resource	Request condition
Allow (1 of 337 services) Show remaining 336			
IAM	**Limited**: List	All resources	Multiple

Tags

Key	Value
No tags associated with the resource.	

* Required

Cancel Previous Create policy



Assignment 3:- Prepare 15 authentic MCQ questions related to IAM.

Q1. IAM stands for

- Internal Application Management
- Internet Access Management
- Identity Access Management
- Internal Access Management

Q2. IAM is

- Global service
- Datacentre specific service
- Regional service
- Depends on CDN

Q3. What are IAM users

- Identities with long-term credentials
- Identities with short-term credentials
- Users with admin access
- Users with view permission only

Q4. IAM Policies are written in which format?

- JASON
- YAML
- Shell
- XML

Q5. What is IAM Policy

- Set of permissions that needs to be attached with AWS resources
- Regional set of rules for AWS accounts
- Criteria for user creation
- Minimum password criteria

Q6. One IAM user cannot be part of more than one group

- True
- False

Q7. What is IAM Role

- Set of permissions to access AWS by relying on temporary security credentials
- Set of permanent permissions to access AWS
- Identification tag
- It is same as access policies

Q8. Which is **NOT CORRCET** option for role-based access control (RBAC)

- Defining IAM roles with permissions that align with job functions
- Permissions based on Experience
- You can audit access by looking at each IAM role and its attached permissions
- Grant access only to the specific service actions and resources required to perform each task

Q9. Which is **NOT CORRCET** option for attribute-based access control (ABAC)

- Set of permissions based on the value of a tag
- Fine-grained permissions to specific resources by requiring the tags on the role or session to match the tags on the resource
- ABAC provides the advantages over the traditional RBAC model
- ABAC requires more complex policies to defined and it is not efficient for quick team growth

Q10. Which is **NOT CORRCET** option for AWS Organizations service control policies (SCPs)

- Service for grouping and centrally managing the AWS accounts that your business owns

- JSON policies that specify the maximum permissions for an organization or organizational unit (OU)
- SCP limits permissions for entities in member accounts, including each AWS account root user. An explicit deny in any of these policies overrides the allow
- SCP specify the minimum permissions for organization

Q11. Which is NOT CORRCET option for Access control lists (ACLs)

- service policies that allow you to control which principals in another account can access a resource
- ACLs cannot be used to control access for a principal within the same account
- ACLs are similar to resource-based policies, although they are the only policy type that does not use the JSON policy document format
- Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs
- None of the above

Q12. Which is **NOT CORRCET** option for Session policies

- Advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user
- Session policies are permanent for user session
- The permissions for a session are the intersection of the identity-based policies for the IAM entity (user or role) used to create the session and the session policies
- PolicyArns parameter to specify up to 10 managed session policies
- Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow

Q13. Which of the following is **NOT CORRECT** for root user

- You cannot attach identity-based policies to the root user, and you cannot set the permissions boundary for the root user
- you can specify the root user as the principal in a resource-based policy or an ACL
- A root user is still the member of an account. If that account is a member of an organization in AWS Organizations, the root user is affected by any SCPs for the account
- Root user can not belong to any policy

Q14.What is the default access when we create a IAM user

- All access is denied by default and requires a policy that grants access
- All access is allowed by default
- Root level is allowed by default for all users
- None of the above

Q15. What is least-privilege permissions

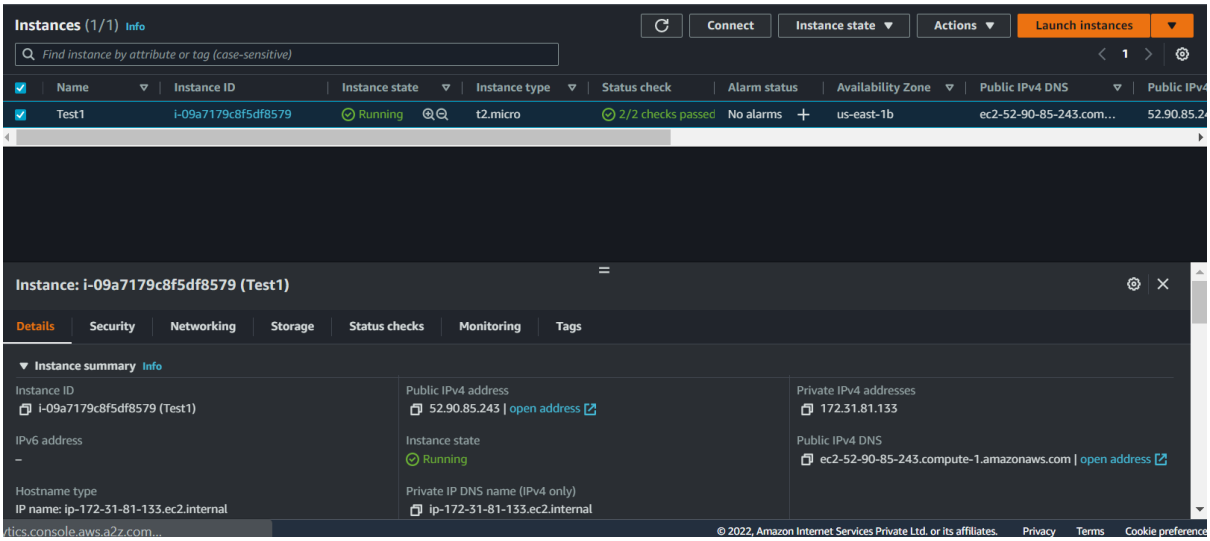
- Only the permissions required with the goal of achieving least-privilege permissions
- Only read permissions for users
- All permissions except delete operation
- None of the above

Q16. Which of the following is **NOT CORRECT** for IAM Access Analyzer

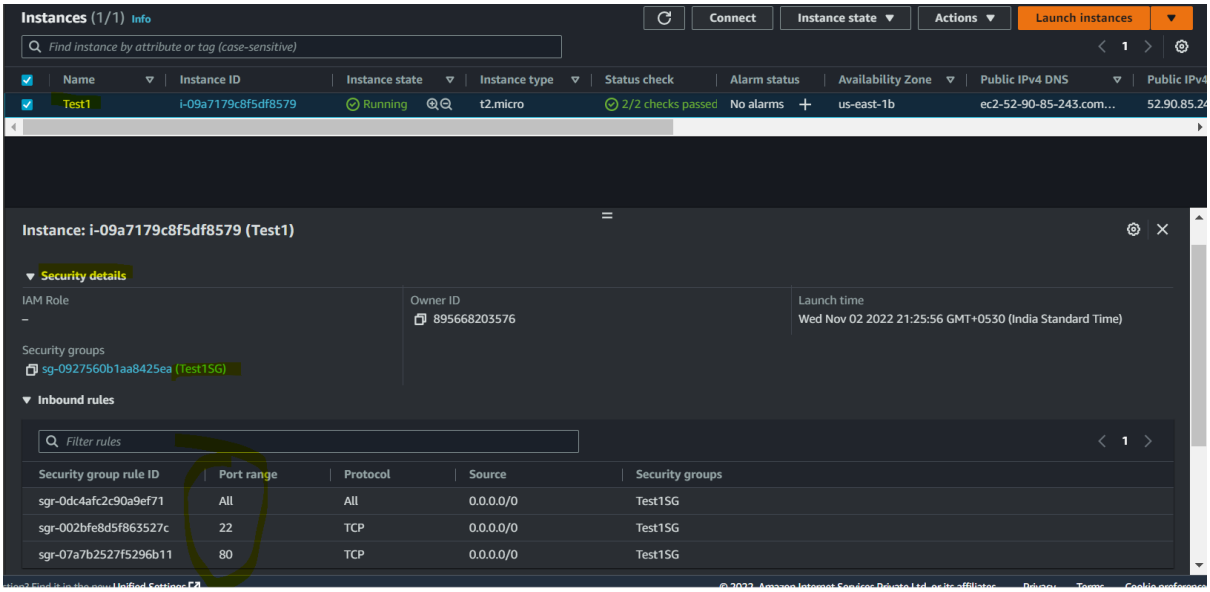
- Achieving least privilege is a continuous cycle to grant the right fine-grained permissions as your requirements evolve. IAM Access Analyzer helps you streamline permissions management in each step of this cycle
- It is Audit service to identify the access for each user and takes actions accordingly
- Policy generation with IAM Access Analyzer generates a fine-grained policy based on the access activity captured in your logs. This means that after you build and run an application, you can generate policies that grant only the required permissions to operate the application
- Policy validation with IAM Access Analyzer uses more than 100 policy checks to guide you to author and validate secure and functional policies. You can use these checks while creating new policies or to validate existing policies
- Public and cross-account findings with IAM Access Analyzer help you verify and refine access allowed by your resource policies from outside your AWS organization or account

Assignment 4:- Launch your Linux instance in IAM and update your machine.

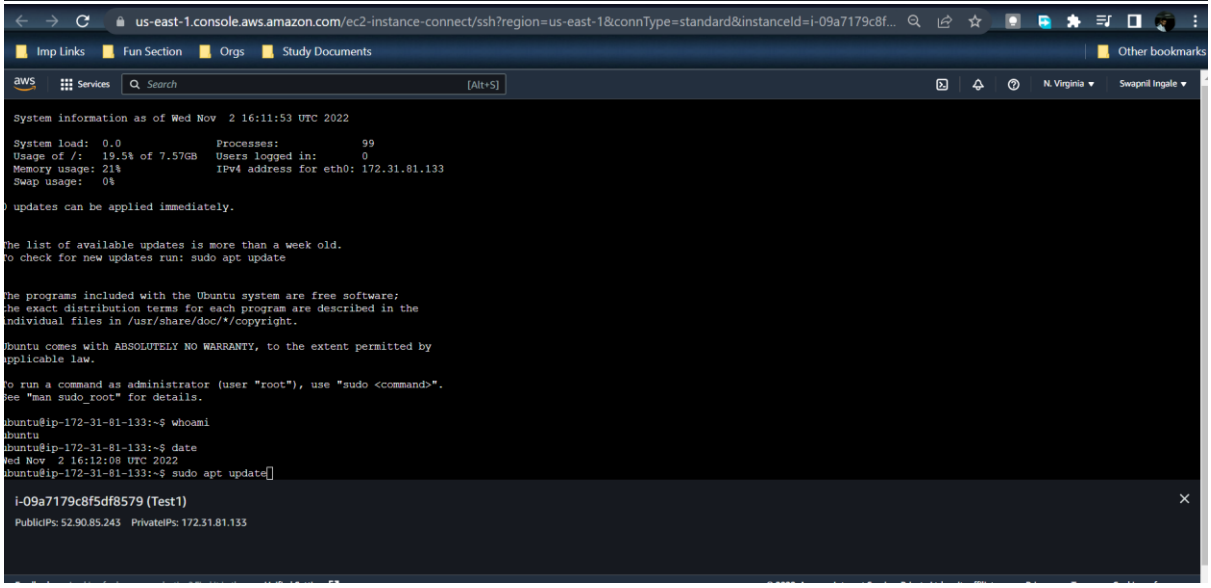
➔ **Ans:** Launched Test1 EC2 instance. Connect to it via EC2 connect option in AWS management console.

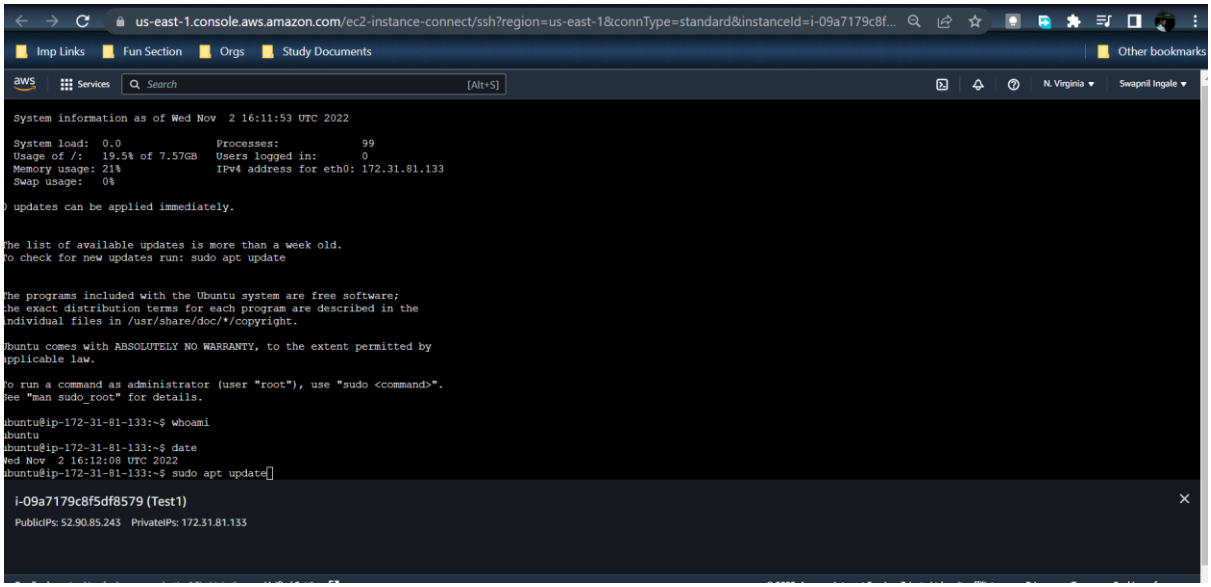


Created Security group “Test1SG” with inbound and outbound rules with allow http, SSH traffic and attached it to EC2 instance “Test1” Connected to instance via AWS GUI option “Connect to instance”



```
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [695 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [159 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [10.8 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [409 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [63.1 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [540 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [743 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [122 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [4404 B]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [13.7 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [4228 B]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [420 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [3008 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [1432 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [272 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [6752 B]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [9360 B]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [356 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [461 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [101 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [372 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [57.4 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [602 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [76.6 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [2408 B]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [4192 B]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [900 B]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [228 B]
Fetched 24.6 MB in 3s (7167 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
77 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-81-133:~$
```




us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-09a7179c8f...
Imp Links
Fun Section
Orgs
Study Documents
Other bookmarks
aws
Services
Search
[Alt+S]
N. Virginia
Swapnil Ingale
System information as of Wed Nov 2 16:11:53 UTC 2022
System load: 0.0
Usage of /: 19.5% of 7.57GB
Memory usage: 21%
Swap usage: 0%
Processes: 99
Users logged in: 0
IPv4 address for eth0: 172.31.81.133
0 updates can be applied immediately.
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-81-133:~$ whoami
ubuntu
ubuntu@ip-172-31-81-133:~$ date
Wed Nov 2 16:12:08 UTC 2022
ubuntu@ip-172-31-81-133:~$ sudo apt update
i-09a7179c8f5df8579 (Test1)
PublicIPs: 52.90.85.243 PrivateIPs: 172.31.81.133