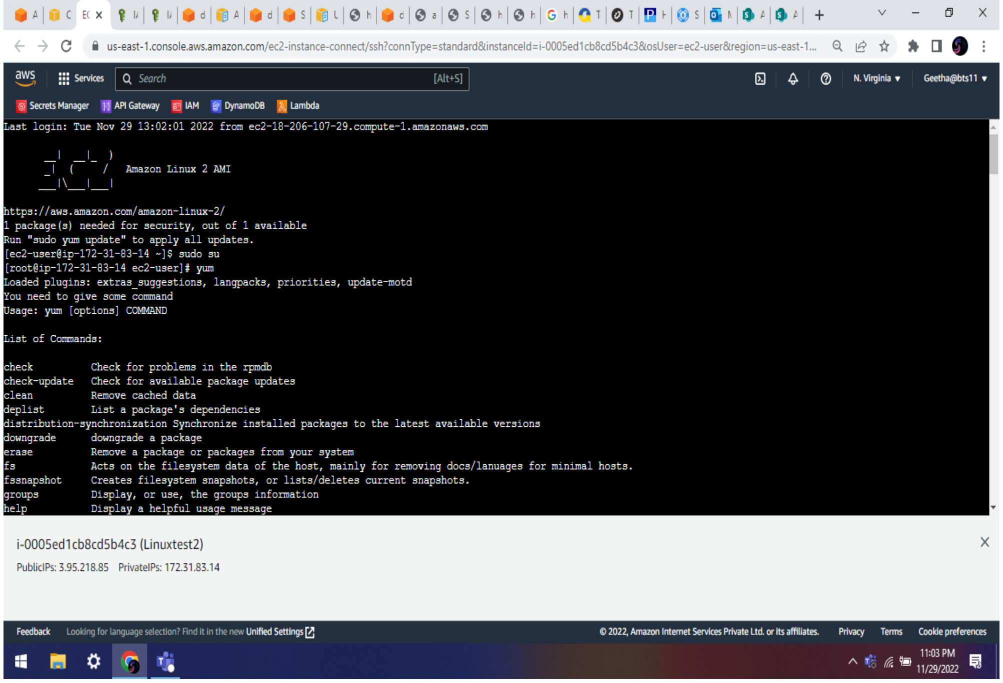
Documentation Amazon Web Services

Linux Commands:

- Change directory
- Move file to another directory
- Command to check contents of a file
- Command for changing permissions to a file
- Copy file from one server(ec2) to another
- Find list of processes running on Linux
- Stopping a process etc.



us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0005ed1cb8cd5b4c3&osUser=ec2-user&region=us-east-1...

```
Last login: Tue Nov 29 13:02:01 2022 from ec2-18-206-107-29.compute-1.amazonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 1 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-83-14 ~]$ sudo su
[root@ip-172-31-83-14 ec2-user]# yum
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
You need to give some command
Usage: yum [options] COMMAND

List of Commands:

check          Check for problems in the rpmdb
check-update   Check for available package updates
clean          Remove cached data
deplist        List a package's dependencies
distribution-synchronization Synchronize installed packages to the latest available versions
downgrade      downgrade a package
erase          Remove a package or packages from your system
fs             Acts on the filesystem data of the host, mainly for removing docs/lanuages for minimal hosts.
fssnapshot     Creates filesystem snapshots, or lists/deletes current snapshots.
groups         Display, or use, the groups information
help           Display a helpful usage message
```

i-0005ed1cb8cd5b4c3 (Linuxtest2)

PublicIPs: 3.95.218.85 PrivateIPs: 172.31.83.14

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
11:03 PM
11/29/2022

Let us consider there are two files named as file1 and file2

And consider the two directories as dir1 and dir2

Changing the directory of the file:

cd dir1 dir2 - where cd refers of changing the directory

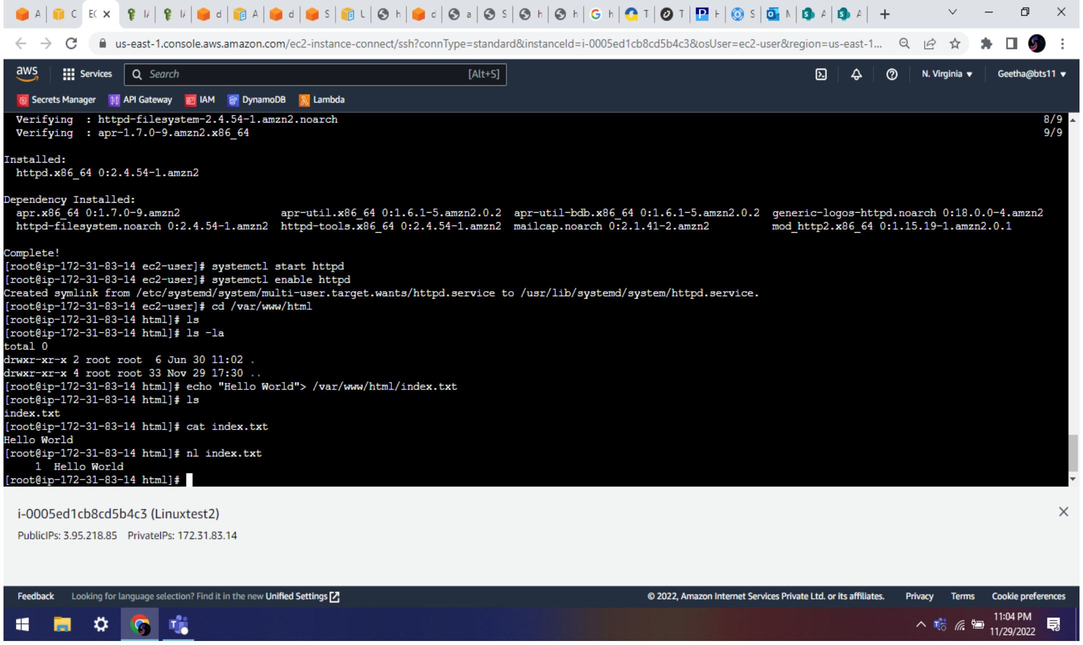
Move file to another directory:

mv file1 dir2 - where mv refers to move

Times New Roman

Check contents of a file:

cat file1 - where cat refers to read the contents inside the file



```
  Verifying  : httpd-filesystem-2.4.54-1.amzn2.noarch                                                                    8/9
  Verifying  : apr-1.7.0-9.amzn2.x86_64                                                                                  9/9

Installed:
  httpd.x86_64 0:2.4.54-1.amzn2

Dependency Installed:
  apr.x86_64 0:1.7.0-9.amzn2                 apr-util.x86_64 0:1.6.1-5.amzn2.0.2  apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2  generic-logos-httpd.noarch 0:18.0.0-4.amzn2
  httpd-filesystem.noarch 0:2.4.54-1.amzn2  httpd-tools.x86_64 0:2.4.54-1.amzn2  mailcap.noarch 0:2.1.41-2.amzn2          mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
[root@ip-172-31-83-14 ec2-user]# systemctl start httpd
[root@ip-172-31-83-14 ec2-user]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-83-14 ec2-user]# cd /var/www/html
[root@ip-172-31-83-14 html]# ls
[root@ip-172-31-83-14 html]# ls -la
total 0
drwxr-xr-x 2 root root  6 Jun 30 11:02 .
drwxr-xr-x 4 root root 33 Nov 29 17:30 ..
[root@ip-172-31-83-14 html]# echo "Hello World"> /var/www/html/index.txt
[root@ip-172-31-83-14 html]# ls
index.txt
[root@ip-172-31-83-14 html]# cat index.txt
Hello World
[root@ip-172-31-83-14 html]# nl index.txt
     1  Hello World
[root@ip-172-31-83-14 html]#
```

i-0005ed1cb8cd5b4c3 (Linuxtest2)

PublicIPs: 3.95.218.85   PrivateIPs: 172.31.83.14

us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0005ed1cb8cd5b4c3&osUser=ec2-user&region=us-east-1...
Services
Search
[Alt+S]
N. Virginia
Geetha@bts11
Secrets Manager
API Gateway
IAM
DynamoDB
Lambda
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
11:04 PM
11/29/2022

Change the permissions of a file:

chmod u=rwx file1 - where r stands for read the file

w stands for write the file

x stands for execute the file

+ is used to add the permission

- is used to remove the permission

Copy file from one server(ec2) to another:

I just needed to replace the Elastic IP with the private IP and configure the security groups properly to allow instances to communicate!

Transferring from Machine A to Machine B

I am running this code on machine A

```
scp -i ~/Path-To-Key-File/AAA.pem /path/file  ec2-user@<Private IP of Machine B>:/path/file
```

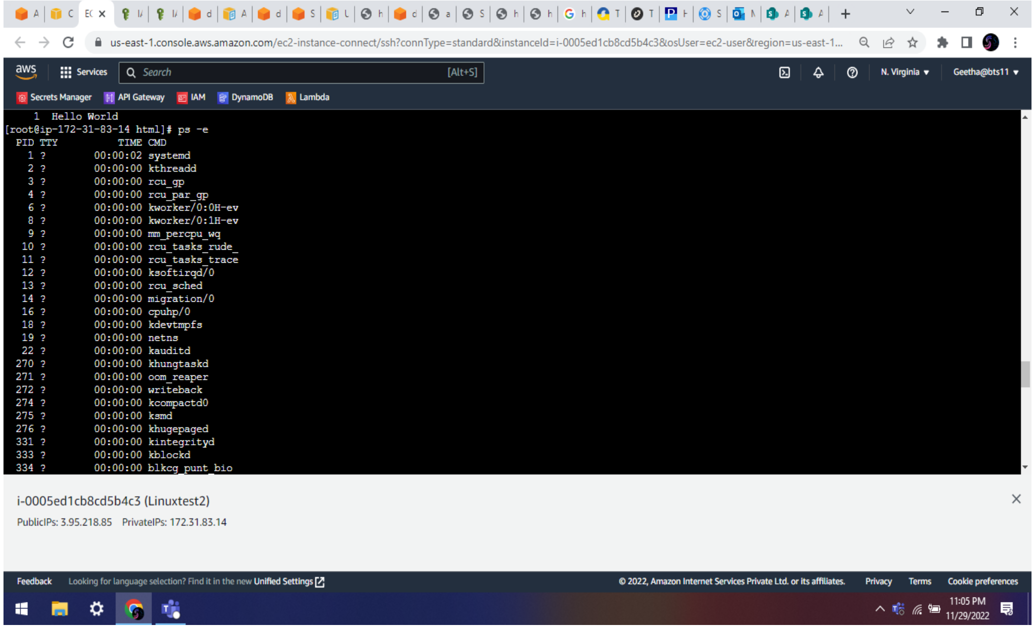
Find list of processes running on linux:

ps - where ps stands for process status and it will display all

running process in task manager

Stopping a process:

ps -e - where ps stands for process status and e stands for end.



us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0005ed1cb8cd5b4c3&osUser=ec2-user&region=us-east-1...
aws
Services
Search
[Alt+S]
N. Virginia
Geetha@bts11
Secrets Manager
API Gateway
IAM
DynamoDB
Lambda

```
    1  Hello World
[root@ip-172-31-83-14 html]# ps -e
  PID TTY          TIME CMD
    1 ?        00:00:02 systemd
    2 ?        00:00:00 kthreadd
    3 ?        00:00:00 rcu_gp
    4 ?        00:00:00 rcu_par_gp
    6 ?        00:00:00 kworker/0:0H-ev
    8 ?        00:00:00 kworker/0:1H-ev
    9 ?        00:00:00 mm_percpu_wq
   10 ?        00:00:00 rcu_tasks_rude_
   11 ?        00:00:00 rcu_tasks_trace
   12 ?        00:00:00 ksoftirqd/0
   13 ?        00:00:00 rcu_sched
   14 ?        00:00:00 migration/0
   16 ?        00:00:00 cpuhp/0
   18 ?        00:00:00 kdevtmpfs
   19 ?        00:00:00 netns
   22 ?        00:00:00 kauditd
  270 ?        00:00:00 khungtaskd
  271 ?        00:00:00 oom_reaper
  272 ?        00:00:00 writeback
  274 ?        00:00:00 kcompactd0
  275 ?        00:00:00 ksmd
  276 ?        00:00:00 khugepaged
  331 ?        00:00:00 kintegrityd
  333 ?        00:00:00 kblockd
  334 ?        00:00:00 blkcg_punt_bio
```

i-0005ed1cb8cd5b4c3 (Linuxtest2)

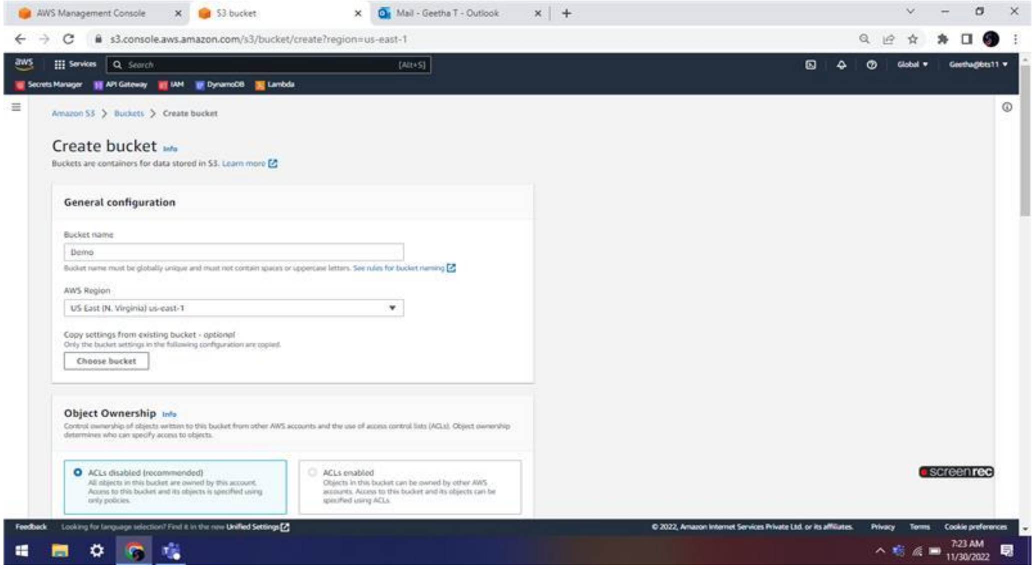
PublicIPs: 3.95.218.85   PrivateIPs: 172.31.83.14

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
11:05 PM
11/29/2022

INDEPENDENT ACTIVITIES:

S3 bucket creation:

1. Sign in to the AWS Management Console and open the Amazon S3 console Choose **Create bucket**.
2. The **Create bucket** wizard opens.
3. In **Bucket name**, enter a DNS-compliant name for your bucket
4. The bucket name must:
    - Be unique across all of Amazon S3.
    - Be between 3 and 63 characters long.
    - Not contain uppercase characters.


AWS Management Console
S3 bucket
Mail - Geetha T - Outlook
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1
Services
Search
[Alt+S]
Secrets Manager
API Gateway
IAM
DynamoDB
Lambda
Global
Geetha@bts11
Amazon S3 > Buckets > Create bucket
screenrec
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
7:23 AM
11/30/2022

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

Demo

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

- Start with a lowercase letter or number.

5. In **Region**, choose the AWS Region where you want the bucket to reside.
6. Under **Object Ownership**, to disable or enable ACLs and control ownership of objects uploaded in your bucket, choose one of the following settings:

7. **ACLs disabled**

   - **Bucket owner enforced** – ACLs are disabled, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect permissions to data in the S3 bucket. The bucket uses policies to define access control.

- To require that all new buckets are created with ACLs disabled by using IAM or AWS Organizations policies,**ACLs enabled**

   - **Bucket owner preferred** – The bucket owner owns and has full control over new objects that other accounts write to the bucket with the `bucket-owner-full-control` canned ACL.

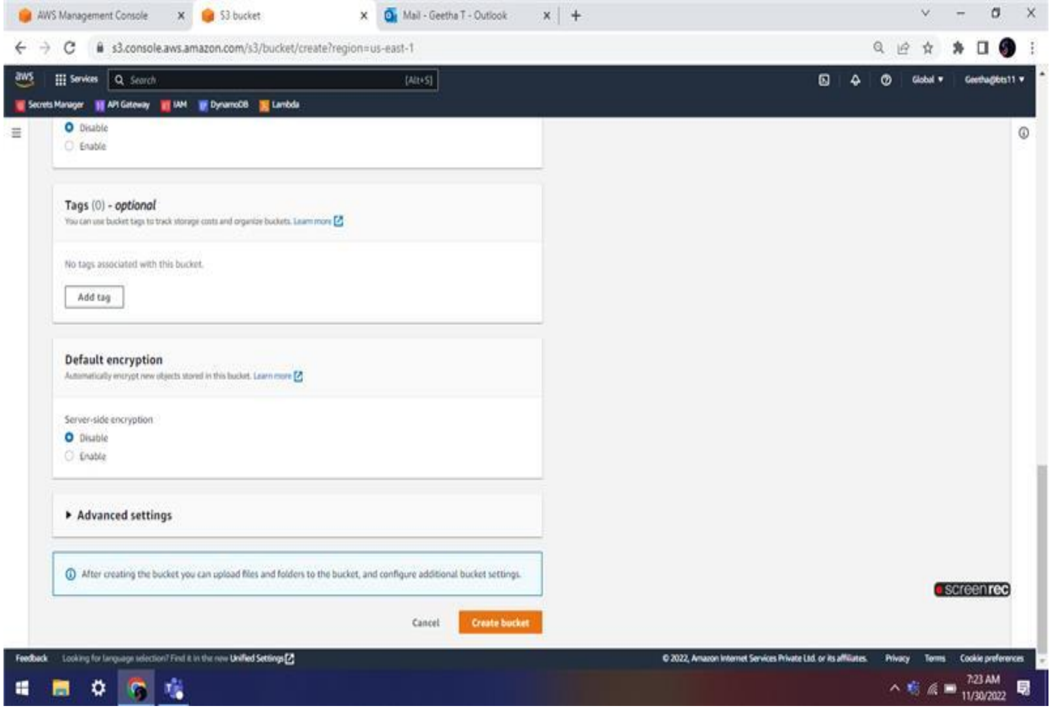
   - If you apply the bucket owner preferred setting, to require all Amazon S3 uploads to include the `bucket-owner-full-control` canned ACL, you can add a bucket policy that only allows object uploads that use this ACL.

   - **Object writer** – The AWS account that uploads an object owns the object, has full control over it, and can grant other users access to it through ACLs.

8. In **Bucket settings for Block Public Access**,I keep all settings enabled unless you know that you need to turn off one or more of them for your use case, such as to host a public website. Block Public Access settings that you enable for the bucket are also enabled for all access points that you create on the bucket.
9. Under **Bucket Versioning**

10. Disable versioning on your bucket.

11. Under **Default encryption**, you can choose to configure your bucket to use server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS KMS keys stored in AWS Key Management Service (AWS KMS) (SSE-KMS).
12. To disable or enable encryption, choose either **Disable** or **Enable**.
13. Choose **Create bucket**.



● Disable
○ Enable

Tags (0) - *optional*

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Default encryption

Automatically encrypt new objects stored in this bucket. Learn more

Server-side encryption

● Disable
○ Enable

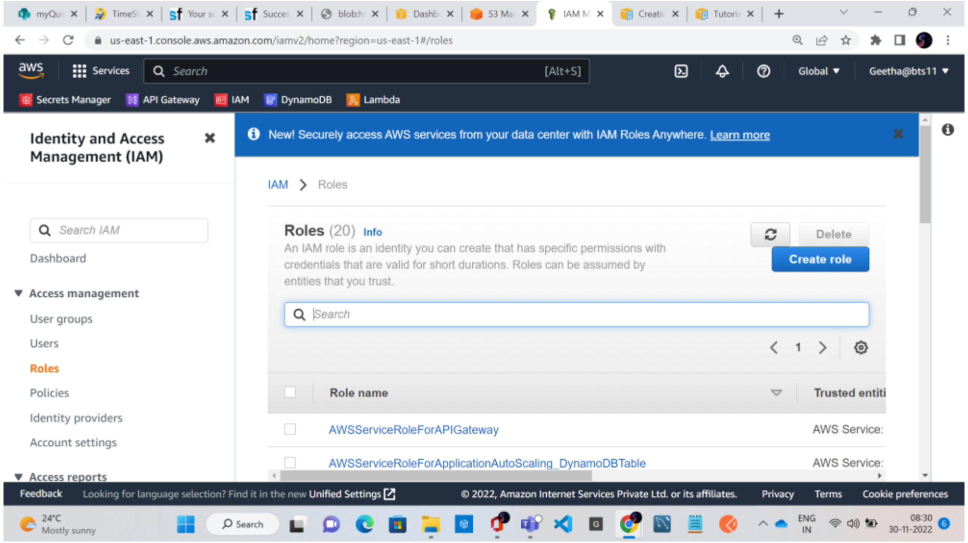
After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel
Create bucket
screenrec
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
7:23 AM
11/30/2022

CREATE IAM ROLE AND GIVE PERMISSION TO READ + PUT OBJECT PERMISSION FOR ONLY ACCESS .CSV FILE:

To create a role (console)

1. Sign in to the AWS Management Console and open the IAM console.
2. In the navigation pane of the console, choose **Roles** and then choose **Create role**.



us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles

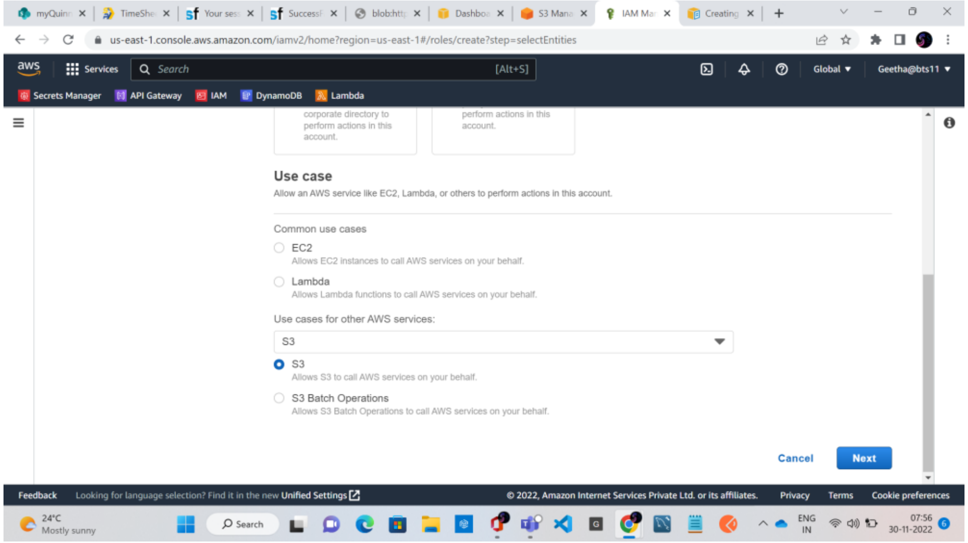
New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more

Roles (20)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entiti
AWSServiceRoleForAPIGateway	AWS Service:
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service:

3. Choose **AWS account** role type.
4. Choose s3 services and Choose **Next**.



us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?step=selectEntities

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

○ EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

S3

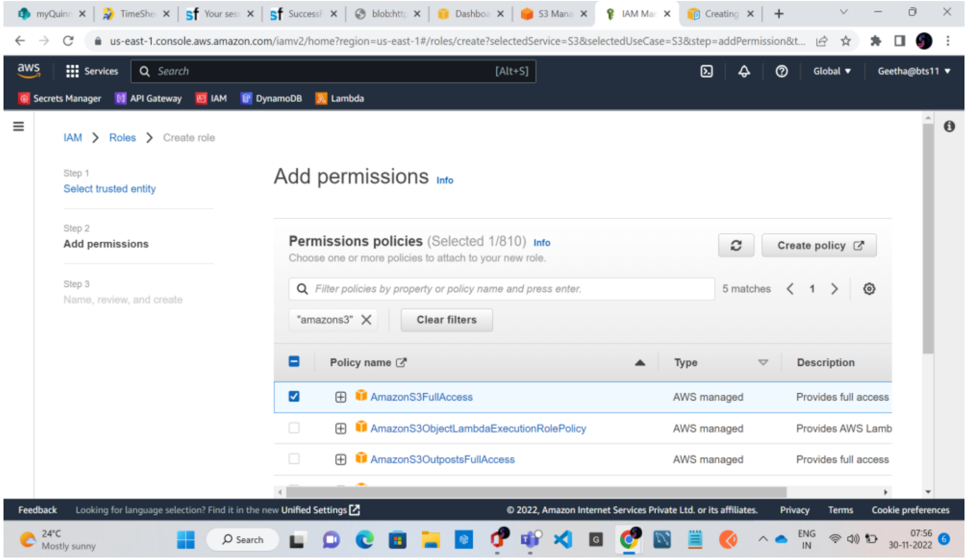
● S3
Allows S3 to call AWS services on your behalf.

○ S3 Batch Operations
Allows S3 Batch Operations to call AWS services on your behalf.

corporate directory to perform actions in this account.
perform actions in this account.
Cancel
Next
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
24°C Mostly sunny
07:56 30-11-2022

5. Choose IAM policies what are the policies we need.

6. Open the **Set permissions boundary** section and choose **Use a permissions boundary to control the maximum role permissions**. Select the policy to use for the permissions boundary.
7. Choose **Next**.
8. For **Role name**, enter a name for your role. Role names must be unique in AWS account.
9. **Add permissions** sections to edit the use cases and permissions for the role.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

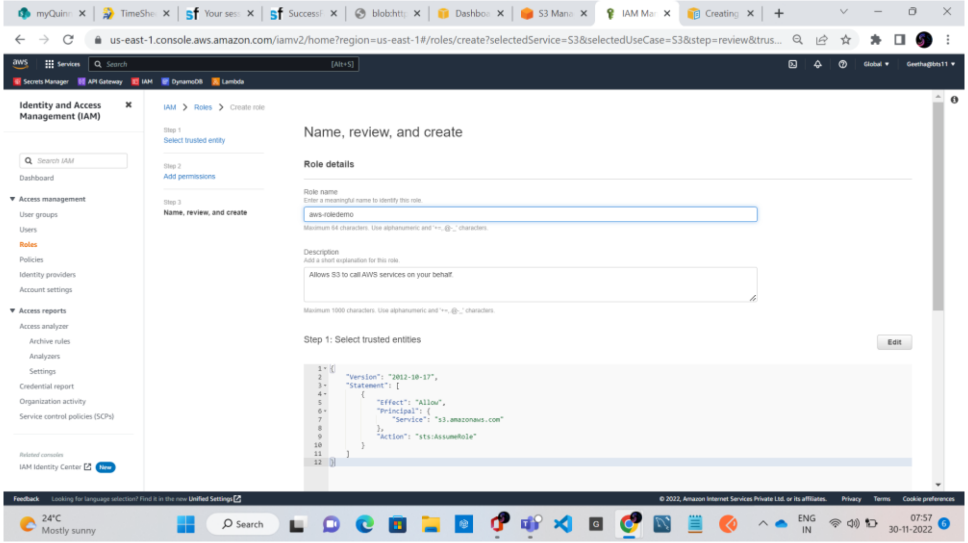
Add permissions Info

Permissions policies (Selected 1/810) Info
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter. 5 matches

"amazons3" Clear filters

	Policy name	Type	Description
☑	AmazonS3FullAccess	AWS managed	Provides full access
□	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	Provides AWS Lamb
□	AmazonS3OutpostsFullAccess	AWS managed	Provides full access



Name, review, and create

Role details

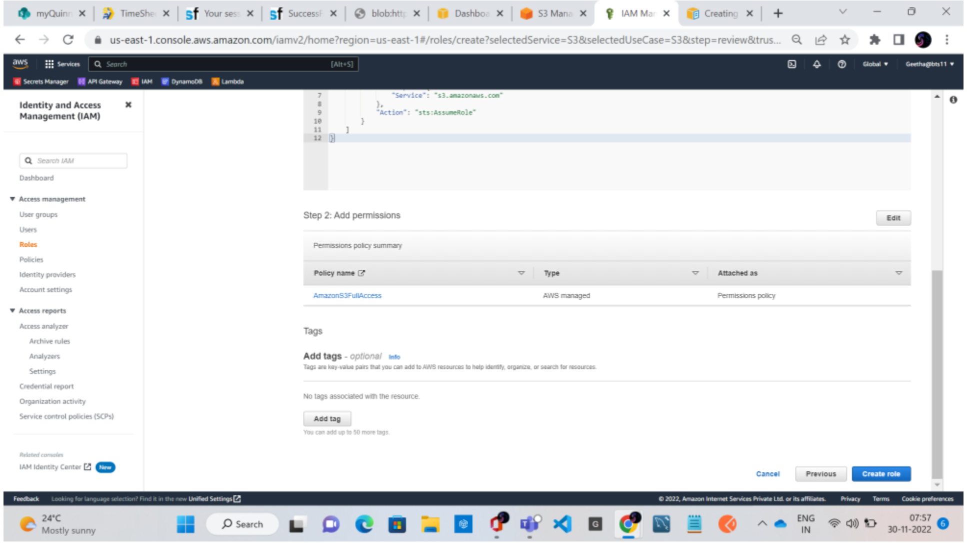
Role name
Enter a meaningful name to identify this role.
aws-roledemo
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows S3 to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

10. Review the role and then choose **Create role.**

11. 

```
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

(Create 2 EC2, create a .txt file in 1st ec2 instance and copy/transfer to 2nd instance using linux command)

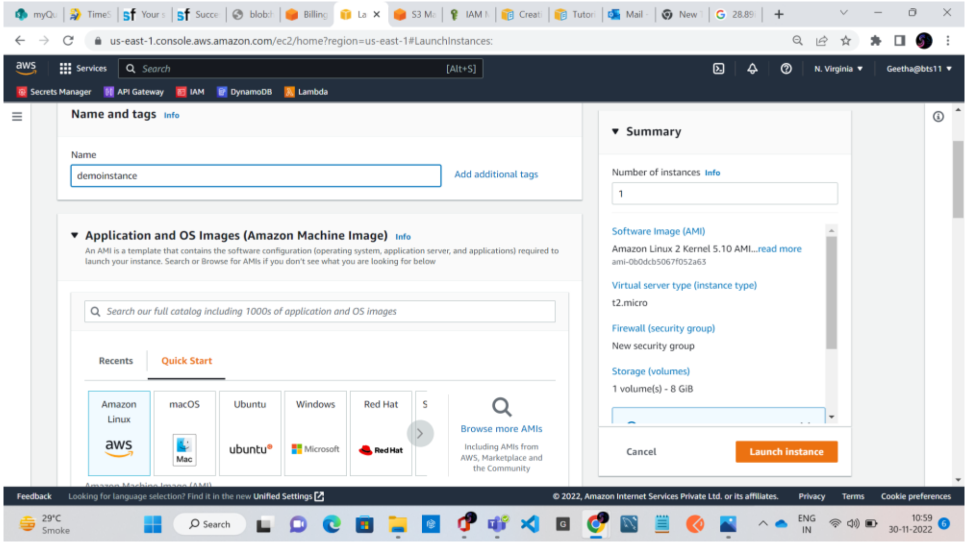
EC2 INSTANCE:

An Amazon EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure.

CREATE EC2 INSTANCE:

To launch an instance

14. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
15. From the EC2 console dashboard, in the **Launch instance** box, choose **Launch instance**, and then choose **Launch instance** from the options that appear.
16. Under **Name and tags**, for **Name**, enter a descriptive name for your instance.
17. Under **Application and OS Images (Amazon Machine Image)**,:
    a. Choose **Quick Start**, and then choose Amazon Linux. This is the operating system (OS) for your instance.
    b. From **Amazon Machine Image (AMI)**, select an HVM version of Amazon Linux 2. Notice that these AMIs are marked **Free tier eligible**. An *Amazon Machine Image (AMI)* is a basic configuration that serves as a template for your instance.
18. Under **Instance type**, from the **Instance type** list, you can select the hardware configuration for your instance. Choose the `t2.micro` instance type, which is selected by default. The `t2.micro` instance type is eligible for the free tier.



Name and tags Info

Name

demoinstance

Add additional tags

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-0b0dcb5067f052a63

Virtual server type (instance type)

t2.micro

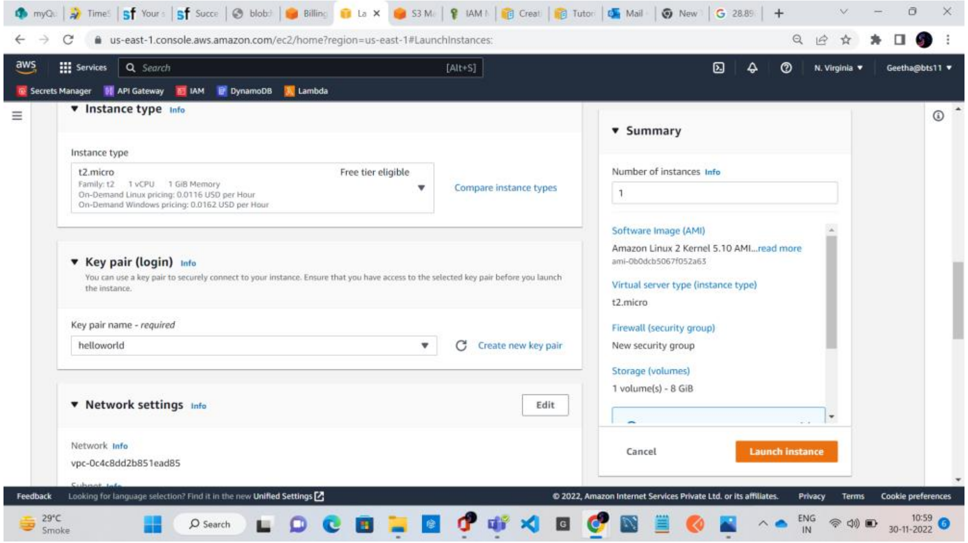
Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel | Launch instance



Instance type Info

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Compare instance types

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

helloworld

Create new key pair

Network settings Info

Edit

Network Info

vpc-0c4c8dd2b851ead85

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-0b0dcb5067f052a63

Virtual server type (instance type)

t2.micro

Firewall (security group)

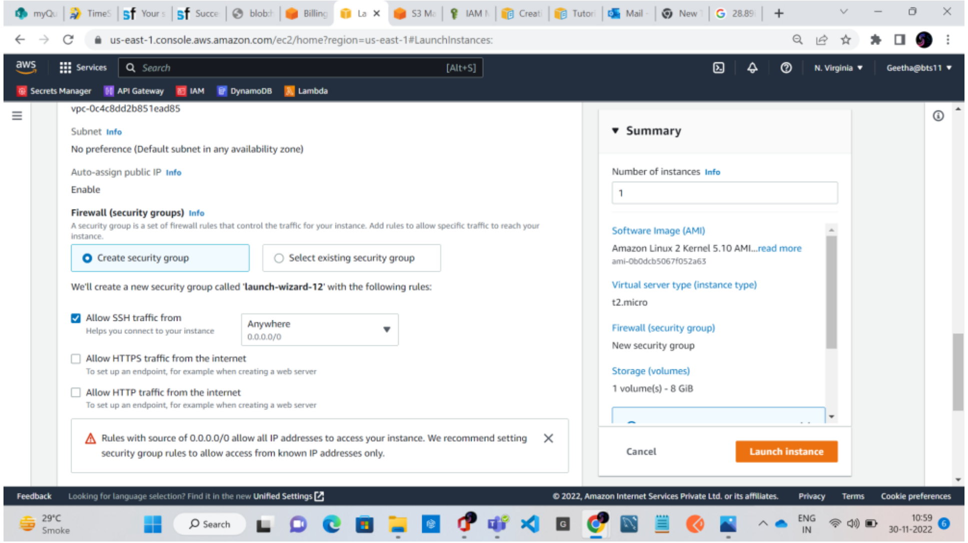
New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel | Launch instance

19. Under **Key pair (login)**, for **Key pair name**, choose the key pair that you created when getting set up.
20. Next to **Network settings**, choose **Edit**. For **Security group name**, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up steps:
    c. Choose **Select existing security group**.
    d. From **Common security groups**, choose your security group from the list of existing security groups.
21. Keep the default selections for the other configuration settings for your instance.
22. Review a summary of your instance configuration in the **Summary** panel, and when you're ready, choose **Launch instance**.



vpc-0c4c8dd2b851ead85

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-12**' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

□ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Summary

Number of instances Info: 1

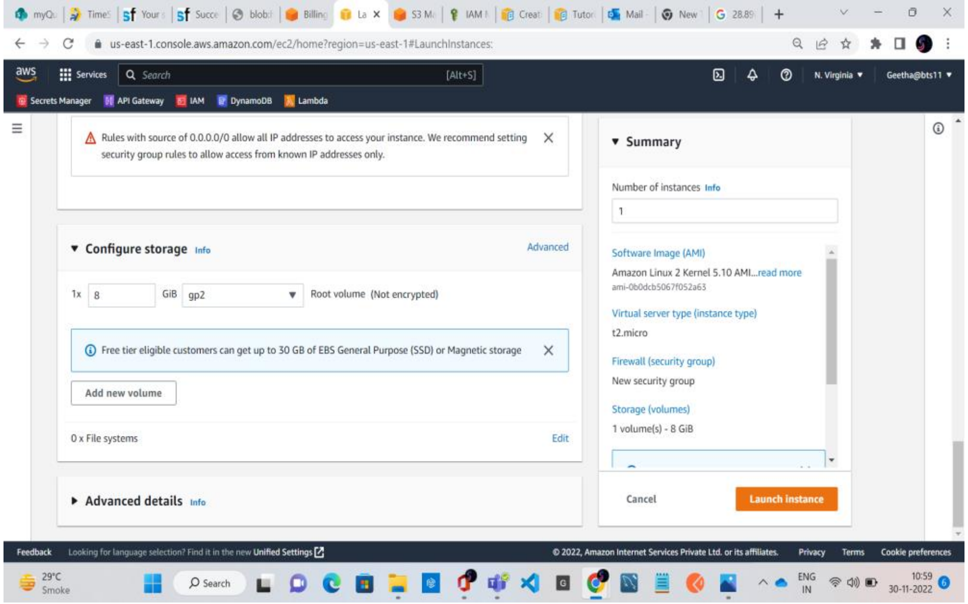
Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0b0dcb5067f052a63

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Cancel
Launch instance
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Smoke
10:59
30-11-2022


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search
[Alt+S]
N. Virginia
Geetha@bts11
Secrets Manager
API Gateway
IAM
DynamoDB
Lambda

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage Info — Advanced

1x 8 GiB gp2 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

0 x File systems — Edit

Advanced details Info

Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0b0dcb5067f052a63

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Cancel
Launch instance
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
29°C
Smoke
10:59
30-11-2022

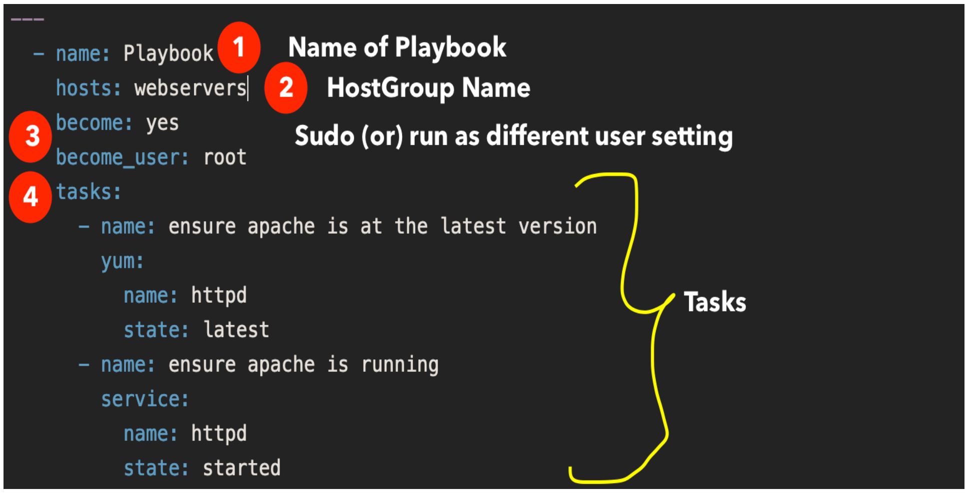
23. A confirmation page lets you know that your instance is launching. Choose **View all instances** to close the confirmation page and return to the console.
24. It can take a few minutes for the instance to be ready for you to connect to it. Check that your instance has passed its status checks; you can view this information in the **Status check** column.

Ansible playbook

Ansible Playbooks are **lists of tasks that automatically execute against hosts**. Groups of hosts form your Ansible inventory. Each module within an Ansible Playbook performs a specific task. Each module contains metadata that determines when and where a task is executed, as well as which user executes it.

Ansible Playbook Example

```
 - name: Playbook
   hosts: webservers
   become: yes
   become_user: root
   tasks:
     - name: ensure apache is at the latest version
       yum:
         name: httpd
         state: latest
     - name: ensure apache is running
       service:
         name: httpd
         state: started
```



```
---
  - name: Playbook
    hosts: webservers
    become: yes
    become_user: root
    tasks:
      - name: ensure apache is at the latest version
        yum:
          name: httpd
          state: latest
      - name: ensure apache is running
        service:
          name: httpd
          state: started
```

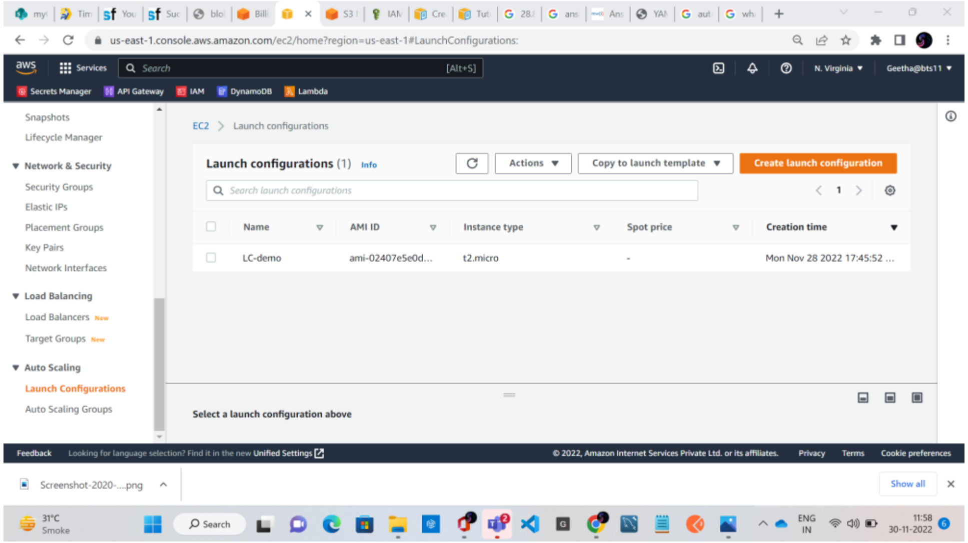
Create an Auto Scaling group using a launch template

AWS AUTO SCALING:

AWS Auto Scaling **monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost**. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes.

Create an Auto Scaling group using a launch template:

25. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/, and choose **Auto Scaling Groups** from the navigation pane.
26. On the navigation bar at the top of the screen, choose the same AWS Region that you used when you created the launch template.
27. Choose **Create an Auto Scaling group**.
28. On the **Choose launch template or configuration** page, do the following:
    e. For **Auto Scaling group name**, enter a name for your Auto Scaling group.
    f. For **Launch template**, choose an existing launch template.
    g. For **Launch template version**, choose whether the Auto Scaling group uses the default, the latest, or a specific version of the launch template when scaling out.
    h. Verify that your launch template supports all of the options that you are planning to use, and then choose **Next**.



	Name	AMI ID	Instance type	Spot price	Creation time
□	LC-demo	ami-02407e5e0d...	t2.micro	-	Mon Nov 28 2022 17:45:52 ...

Select a launch configuration above

29. On the **Choose instance launch options** page, under **Network**, for **VPC**, choose a VPC. The Auto Scaling group must be created in the same VPC as the security group you specified in your launch template.
30. For **Availability Zones and subnets**, choose one or more subnets in the specified VPC. Use subnets in multiple Availability Zones for high availability.

31. If you created a launch template with an instance type specified, then you can continue to the next step to create an Auto Scaling group that uses the instance type in the launch template.
32. Choose **Next** to continue to the next step.
33. We can accept the rest of the defaults, and choose **Skip to review**.
34. Then choose **Next**. On the **Review** page, choose **Create Auto Scaling group**.