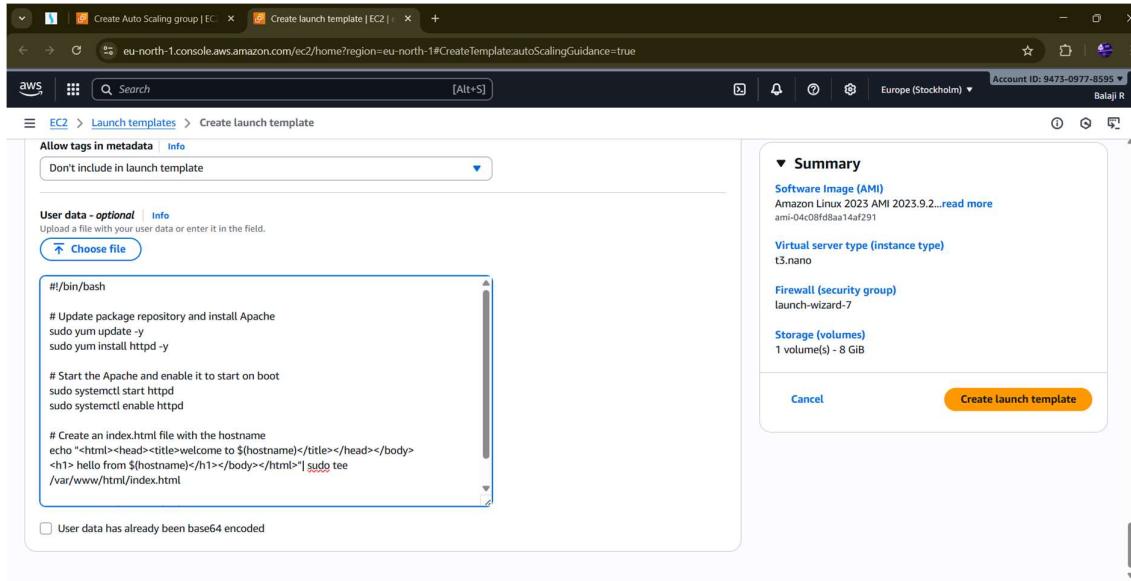
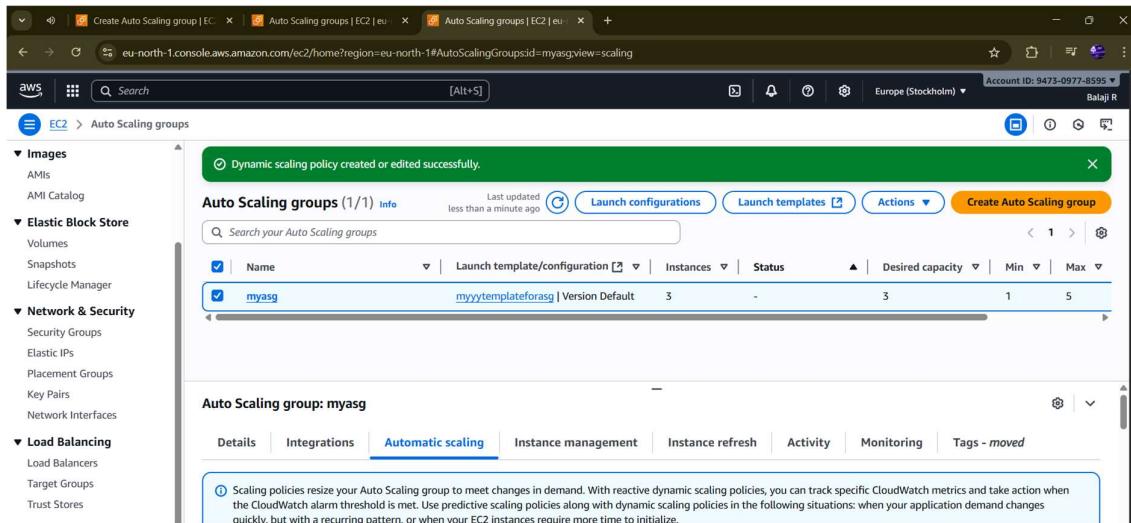


AUTO SCALING GROUPS

First we need to create launch teamplate and select os,key pair,sgp and u see the advance settings in last click and scroll down in user data paste the format



Go to auto scaling groups and select the template then type the desired capacity ex desired cap 3 in minimum 1 and maximum 10 and create the asg



Now you see the 3 instance in ec2 instances

The screenshot shows the AWS EC2 Instances page. The left sidebar has sections for Dashboard, AWS Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main area is titled 'Instances (3) Info' and contains a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP. The table lists three instances: i-0449a785ef8fffc4e0, i-00570aa5051327d02, and i-0b1ab64f99b0de87a, all in the 'Running' state. Below the table is a section titled 'Select an instance'.

Now connect the instance and copy the public ip address and paste in incognito u see the output for the user data we done.

The screenshot shows a browser window with the URL 'welcome to ip-172-31-33-191.eu-north-1.compute.internal'. The page content is 'hello from ip-172-31-33-191.eu-north-1.compute.internal'. The browser toolbar includes icons for CloudShell, Feedback, and various applications like File Explorer, Edge, and Google Chrome. The status bar at the bottom right shows 'ENG IN 09:13 10-10-2025'.

Setting password for instance

Connect the instance and type: **nano /etc/ssh/sshd_config** search for password authentication and type yes , save and exit

Passwd ec2-user give password re type password now restart – systemctl restart sshd

```
[root@ip-172-31-44-102 ec2-user]# nano /etc/ssh/sshd_config
[root@ip-172-31-44-102 ec2-user]# passwd ec2-user
Changing password for user ec2-user.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-172-31-44-102 ec2-user]# systemctl restart sshd
[root@ip-172-31-44-102 ec2-user]# systemctl restart sshd
[root@ip-172-31-44-102 ec2-user]# 
```

i-050db4838b0417fce (password and ssh)
PublicIPs: 51.205.3.147 PrivateIPs: 172.31.44.102

Now in gitbash type: **ssh ec2-user@public ip**

type yes now type the password ur instance will appear in gitbash

```
[ec2-user@ip-172-31-44-102 ~]
[ec2-user@ip-172-31-44-102 ~]$ ssh ec2-user@51.20.53.147
The authenticity of host '51.20.53.147' ('51.20.53.147') can't be established.
ED25519 key fingerprint is SHA256:UQ0BjLhhjhWn1hwduNgDfDwqdeZ6Tq1OJQHCUwD.
This key is not known by any other name.
Are you sure you want to continue connecting (yes/no/[Fingerprint])? y
Please type 'yes' or 'no' or the fingerprint: yes
warning: Permanently added '51.20.53.147' (ED25519) to the list of known hosts.
[ec2-user@51.20.53.147 ~]$ 
```

changing the port number

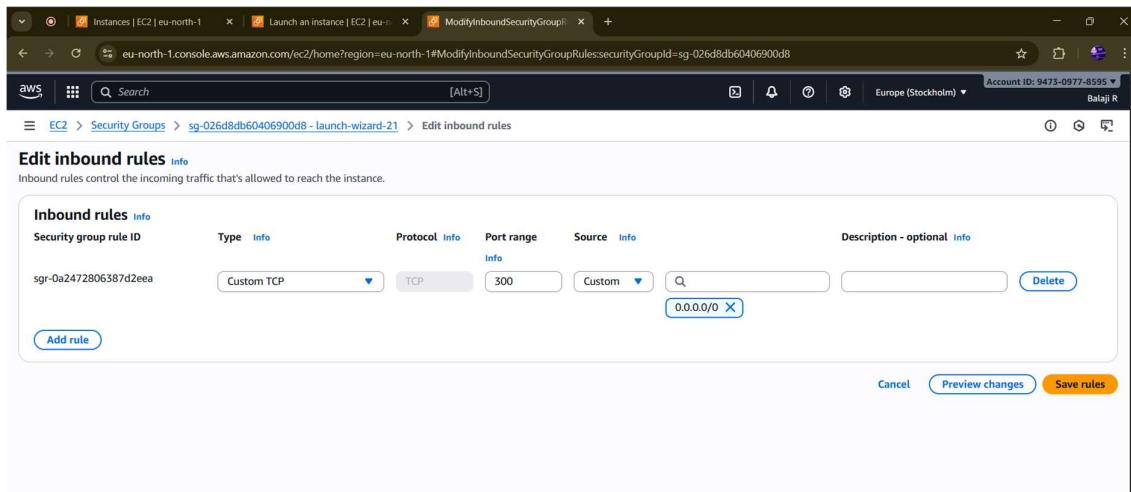
Type sudo su and nano /etc/ssh/sshd_config and search for portnumber remove the # and change 22 to 300 number is ur wish and save and exit go to instance security group and remove the ssh 22 and add custom tcp 300 and restart sshd and go to gitbash

The screenshot shows a terminal window titled "eu-north-1.console.aws.amazon.com/ec2-2018-09-18T14:45:15Z". It displays the following command sequence:

```
[ec2-user@ip-172-31-32-97 ~]$ sudo su
[ec2-user@ip-172-31-32-97 ec2-user]# nano /etc/ssh/sshd_config
[ec2-user@ip-172-31-32-97 ec2-user]# systemctl restart sshd
[ec2-user@ip-172-31-32-97 ec2-user]#
```

Below the terminal, the instance details are shown:

i-0b58b8134ad0c21bf (sshhh)
Public IPs: 16.171.148.228 Private IPs: 172.31.32.97



Now type the command ssh -l key.pem ec2-user@ip -p 300 and you see the output

```
ec2-user@ip-172-31-32-97:~  
balaj@LAPTOP-0EA0V7R5 MINGW64 ~  
$ cd Downloads  
balaj@LAPTOP-0EA0V7R5 MINGW64 ~/Downloads  
$ ssh -i bala.pem ec2-user@16.171.148.228  
ssh: connect to host 16.171.148.228 port 22: Connection refused  
balaj@LAPTOP-0EA0V7R5 MINGW64 ~/Downloads  
$ ssh -i bala.pem ec2-user@16.171.148.228 -p 300  
ssh: connect to host 16.171.148.228 port 300: Connection timed out  
balaj@LAPTOP-0EA0V7R5 MINGW64 ~/Downloads  
$ ssh -i bala.pem ec2-user@16.171.148.228 -p 300  
The authenticity of host '[16.171.148.228]:300' ([16.171.148.228]:300) can't be  
established.  
ED25519 key fingerprint is SHA256:GtLOH2xiyJSiopIU97ZzJWk0hgtwjb1BYAFG+epQ0R4.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[16.171.148.228]:300' (ED25519) to the list of known  
hosts.  
, #  
~\_\_ #####_ Amazon Linux 2023  
~~ \_\#\#\#\_\_  
~~ \#\#\#|  
~~ \#/ , __ https://aws.amazon.com/linux/amazon-linux-2023  
~~ V~, ' -> /  
~~ . , /  
~/m/ , /  
Last login: Fri Oct 10 08:21:56 2025 from 13.48.4.203  
[ec2-user@ip-172-31-32-97 ~]$ |
```