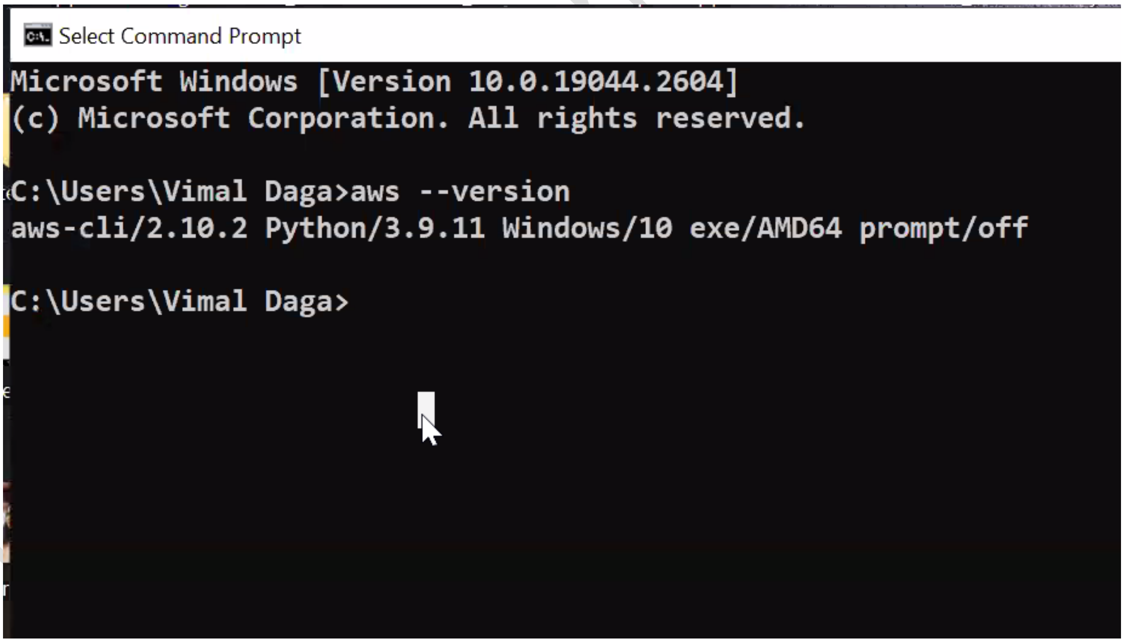
AWS Session 12

8-3-2023

- Three ways to use AWS :
  1. **WebUI** (Console/Portal)
  2. **CLI** – Command line interface(makes things easy/simpler, automate, use script)
  3. **API** (mobile application)
- To create own commands we can use CLI.

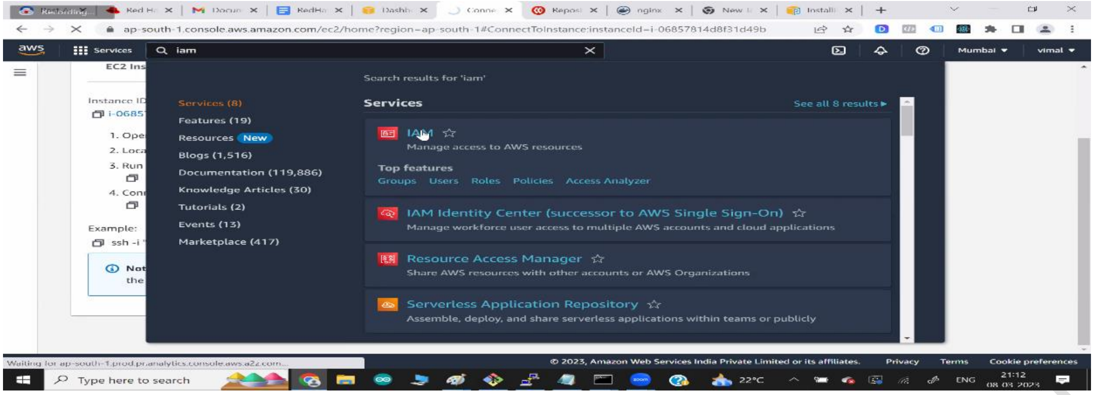
- **PRACTICAL- Launching Instance through CLI**
  In Command Prompt
  To check aws version: **aws --version**



```
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vimal Daga>aws --version
aws-cli/2.10.2 Python/3.9.11 Windows/10 exe/AMD64 prompt/off

C:\Users\Vimal Daga>
```

To login: **aws configure**

- In one single system we can access multiple accounts can be made.
  Before that we will create user in IAM.



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-06857814d8f31d49b

Search results for 'iam'

IAM ☆
Manage access to AWS resources

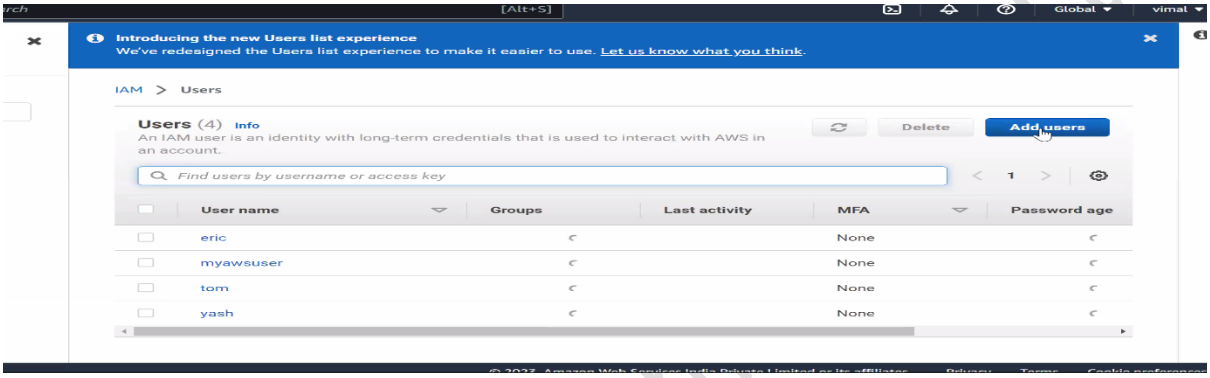
Top features

IAM Identity Center (successor to AWS Single Sign-On) ☆
Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations

Serverless Application Repository ☆
Assemble, deploy, and share serverless applications within teams or publicly

- Now add users.



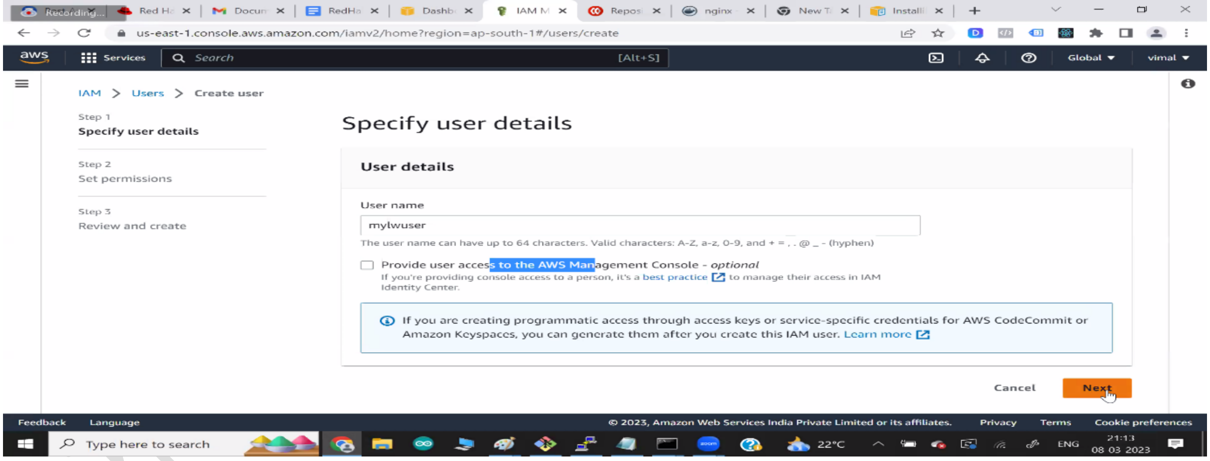
Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

Users (4) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age
□	eric			None	
□	myawsuser			None	
□	tom			None	
□	yash			None	

- Give user details.



us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create

Specify user details

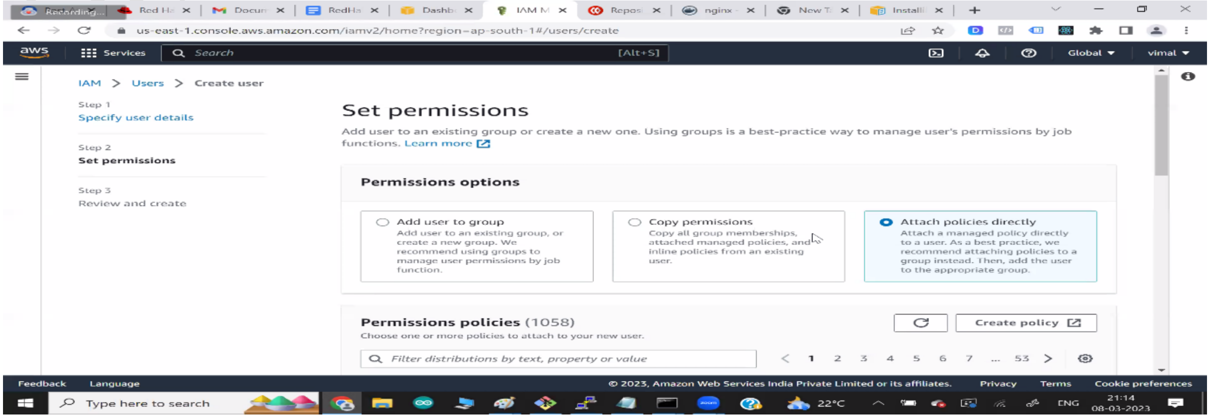
User details

User name
mylwuser

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more



us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

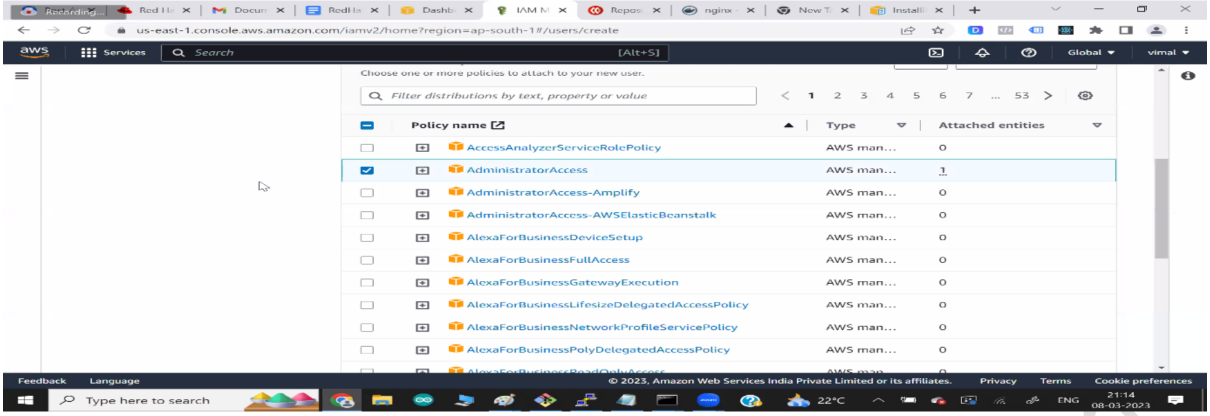
○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1058)
Choose one or more policies to attach to your new user.

Filter distributions by text, property or value



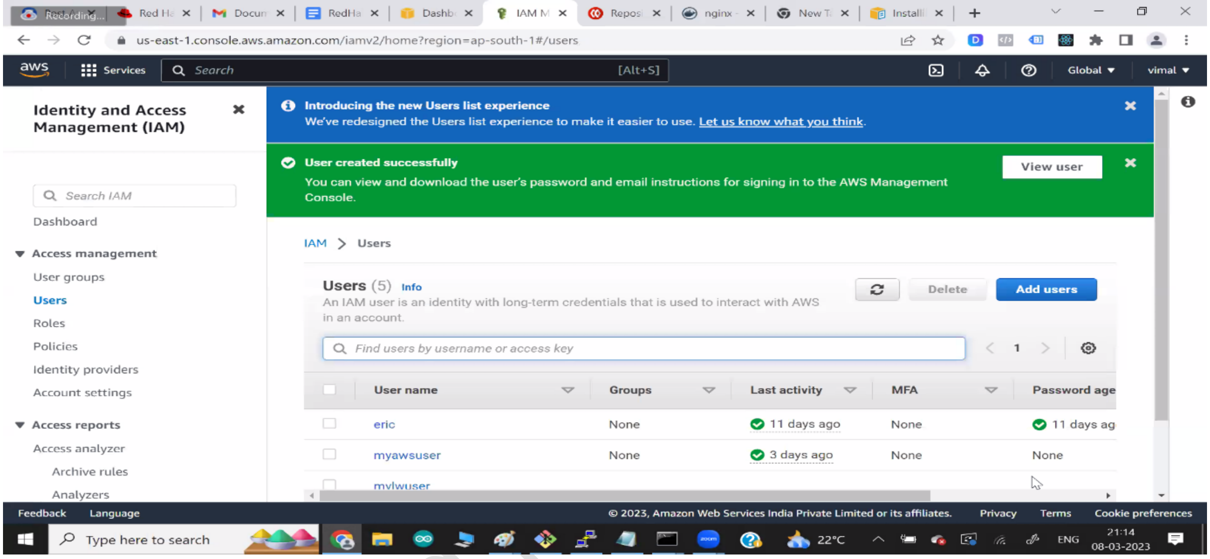
us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create

Choose one or more policies to attach to your new user.

Filter distributions by text, property or value

	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS man...	0
☑	AdministratorAccess	AWS man...	1
□	AdministratorAccess-Amplify	AWS man...	0
□	AdministratorAccess-AWSElasticBeanstalk	AWS man...	0
□	AlexaForBusinessDeviceSetup	AWS man...	0
□	AlexaForBusinessFullAccess	AWS man...	0
□	AlexaForBusinessGatewayExecution	AWS man...	0
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS man...	0
□	AlexaForBusinessNetworkProfileServicePolicy	AWS man...	0
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS man...	0

- After giving details click on craete the user named mylwuser will be created.



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

Identity and Access Management (IAM)

Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

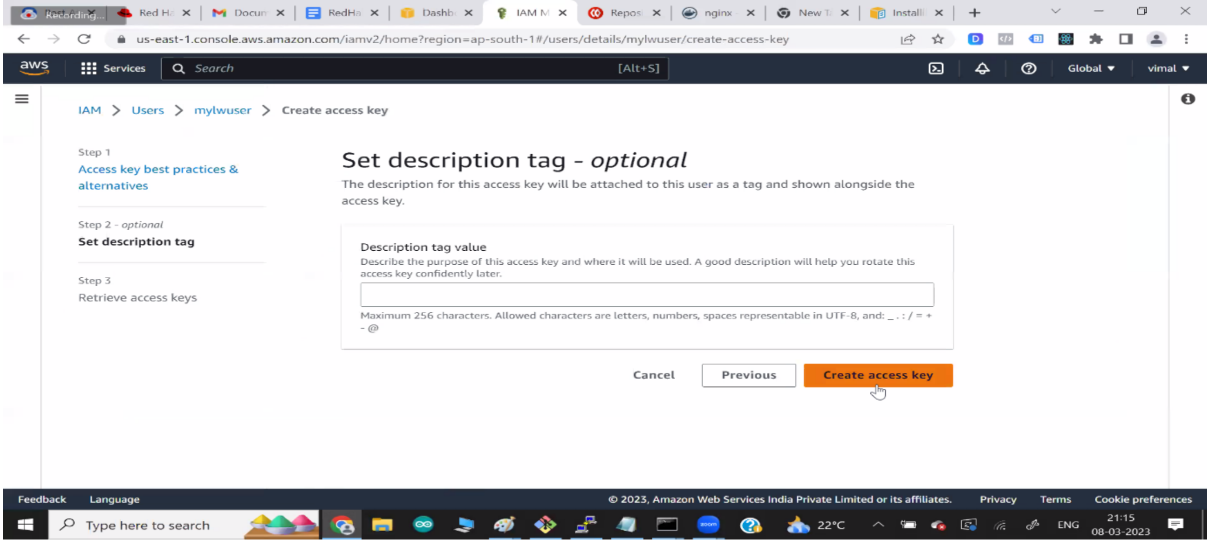
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users

Users (5) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age
□	eric	None	✓ 11 days ago	None	✓ 11 days ag
□	myawsuser	None	✓ 3 days ago	None	None
□	mylwuser				



us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/mylwuser/create-access-key

IAM > Users > mylwuser > Create access key

Step 1
Access key best practices & alternatives

Step 2 - *optional*
Set description tag

Step 3
Retrieve access keys

Set description tag - *optional*

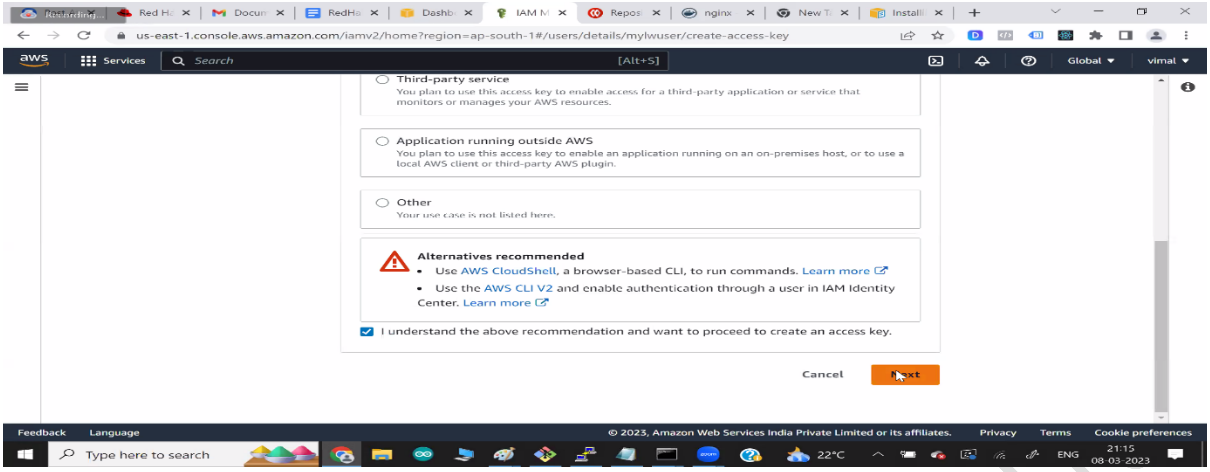
The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel | Previous | Create access key

[AWS]


us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/mylwuser/create-access-key
Services
Search
[Alt+S]
Global
vimal
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C
ENG
21:15
08-03-2023

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

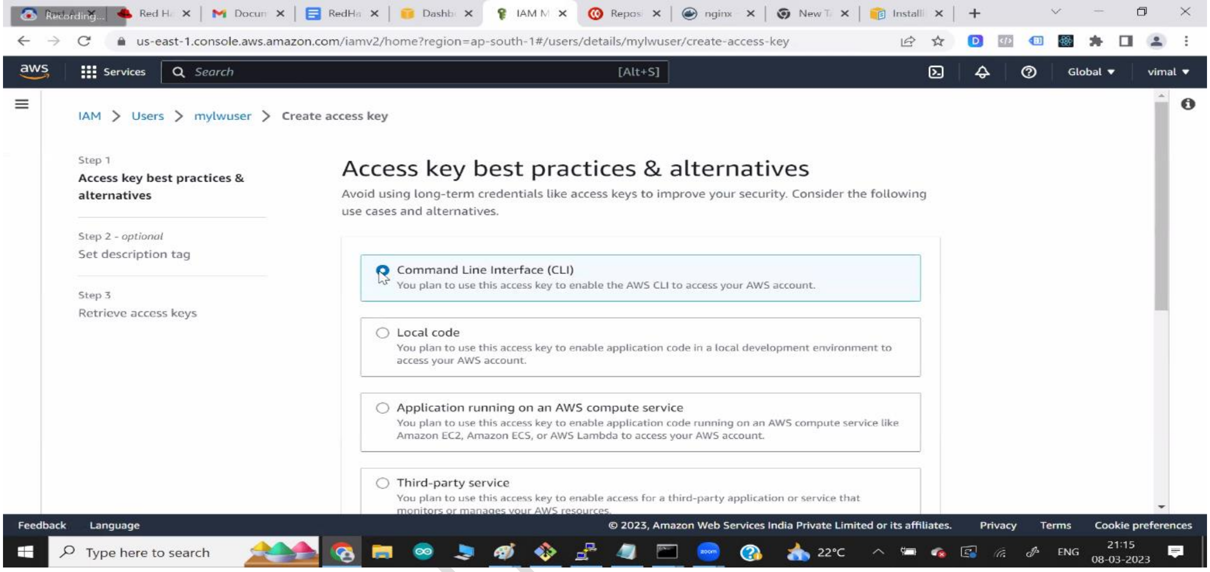
○ Application running outside AWS
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

○ Other
Your use case is not listed here.

Alternatives recommended

- Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
- Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more

☑ I understand the above recommendation and want to proceed to create an access key.


us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/mylwuser/create-access-key
Services
Search
[Alt+S]
Global
vimal
IAM > Users > mylwuser > Create access key
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C
ENG
21:15
08-03-2023

Step 1
Access key best practices & alternatives

Step 2 - *optional*
Set description tag

Step 3
Retrieve access keys

Access key best practices & alternatives

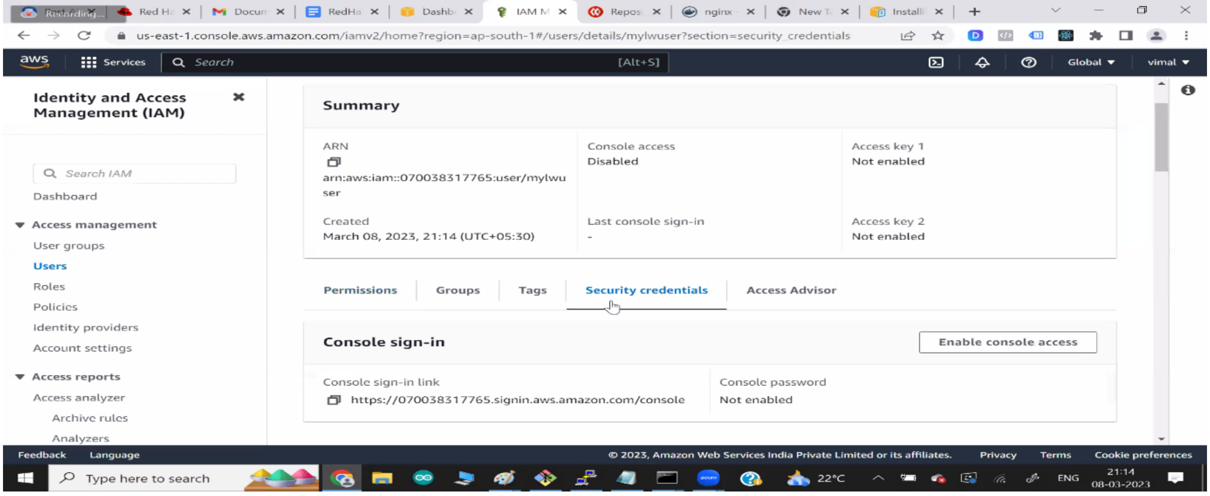
Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

● Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

○ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.



Summary

ARN
arn:aws:iam::070038317765:user/mylwuser

Console access
Disabled

Access key 1
Not enabled

Created
March 08, 2023, 21:14 (UTC+05:30)

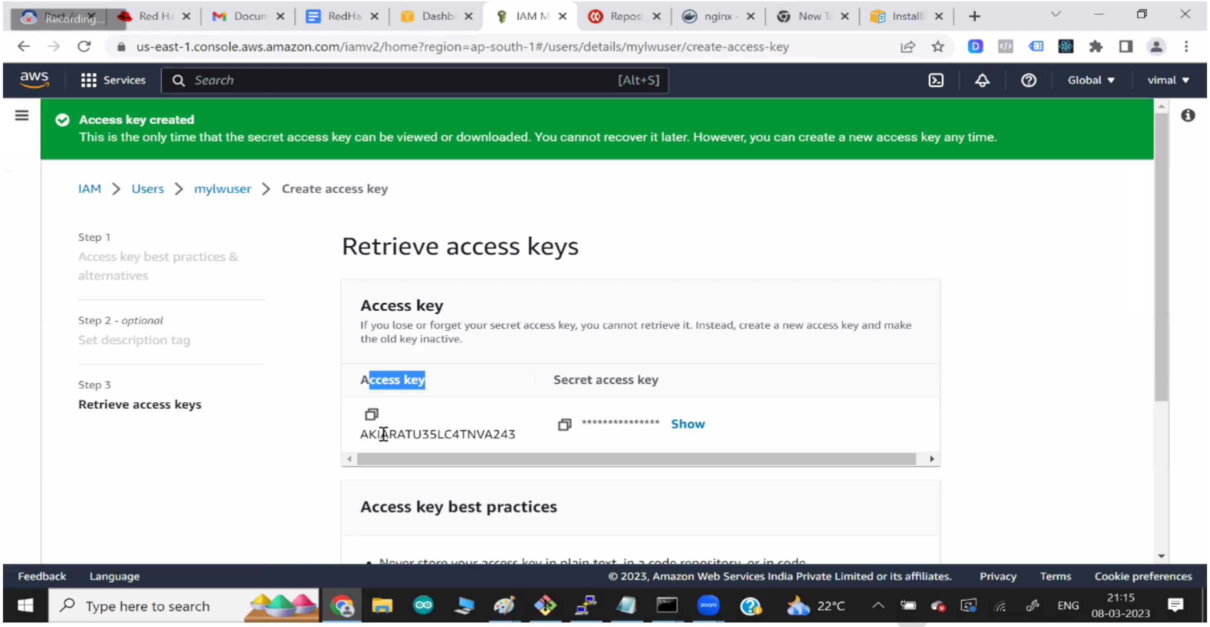
Last console sign-in
-

Access key 2
Not enabled

Console sign-in

Console sign-in link
https://070038317765.signin.aws.amazon.com/console

Console password
Not enabled



us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/mylwuser/create-access-key

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > mylwuser > Create access key

Step 1
Access key best practices & alternatives

Step 2 - *optional*
Set description tag

Step 3
Retrieve access keys

Retrieve access keys

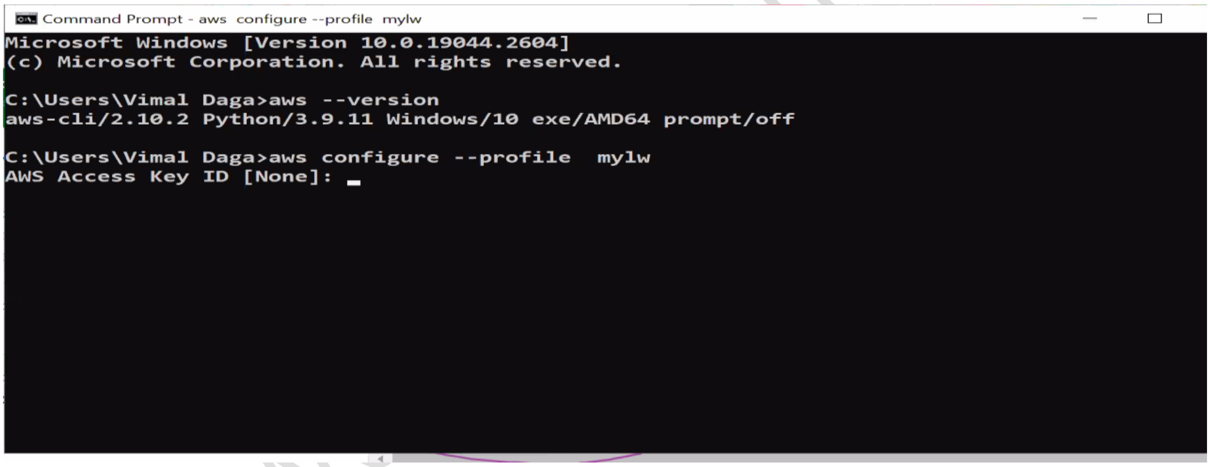
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIARATU35LC4TNVA243	*************** Show

Access key best practices

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

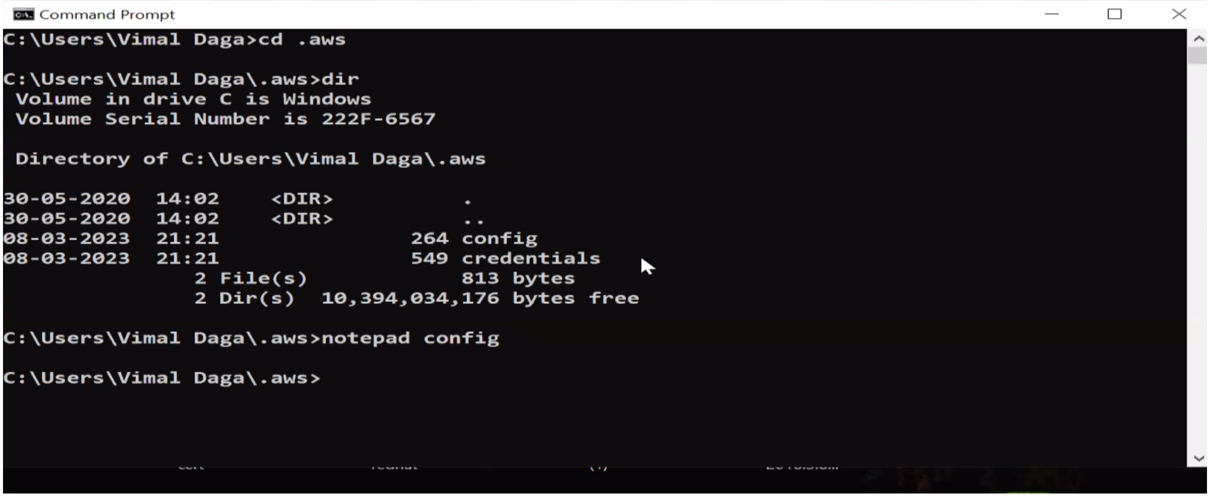
- Now in CLI to configure we will write the command **aws configure --profile mylw**



Command Prompt - aws configure --profile mylw

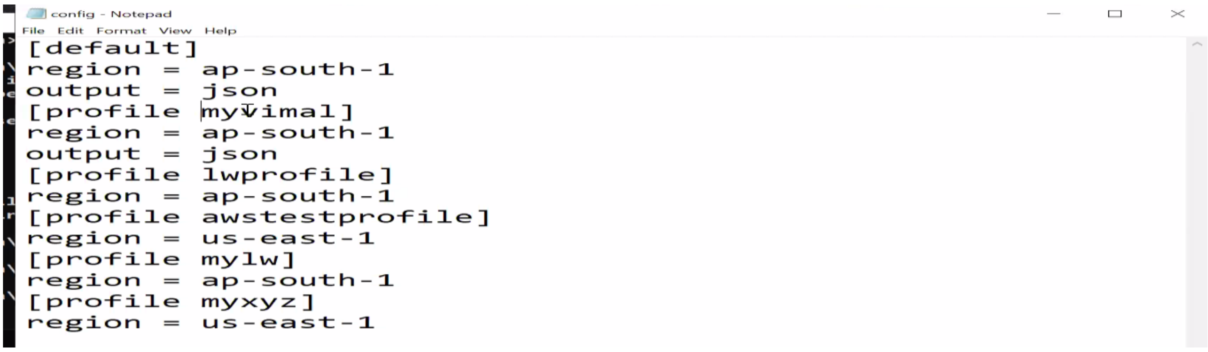
```
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vimal Daga>aws --version
aws-cli/2.10.2 Python/3.9.11 Windows/10 exe/AMD64 prompt/off

C:\Users\Vimal Daga>aws configure --profile  mylw
AWS Access Key ID [None]: _
```

- Add the details in the required field like give access key and secret key. Also give region in our case region: ap-south-1.

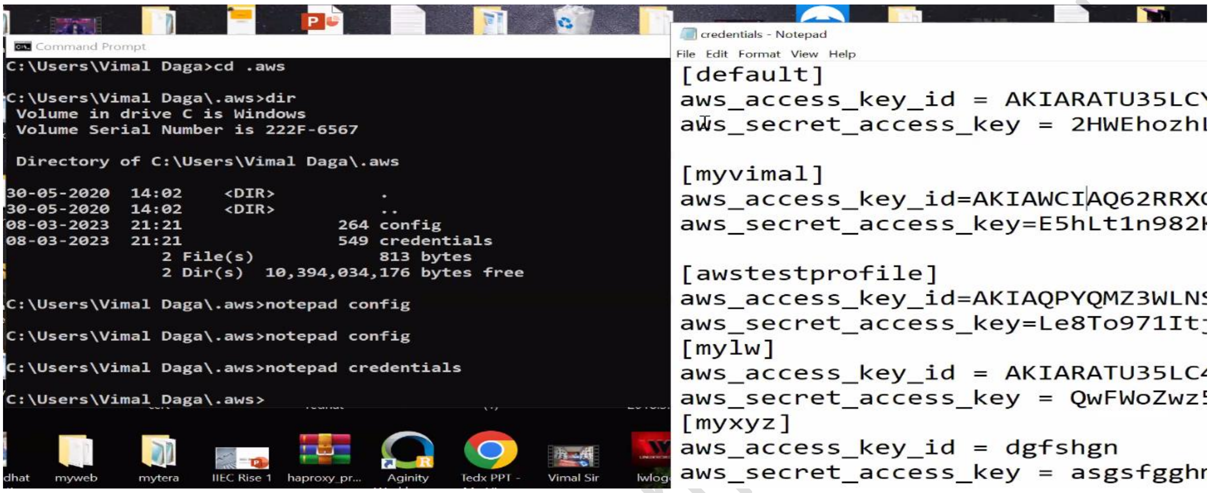


Command Prompt

```
C:\Users\Vimal Daga>cd .aws

C:\Users\Vimal Daga\.aws>dir
 Volume in drive C is Windows
 Volume Serial Number is 222F-6567

 Directory of C:\Users\Vimal Daga\.aws

30-05-2020  14:02    <DIR>          .
30-05-2020  14:02    <DIR>          ..
08-03-2023  21:21               264 config
08-03-2023  21:21               549 credentials
               2 File(s)            813 bytes
               2 Dir(s)  10,394,034,176 bytes free

C:\Users\Vimal Daga\.aws>notepad config

C:\Users\Vimal Daga\.aws>
```



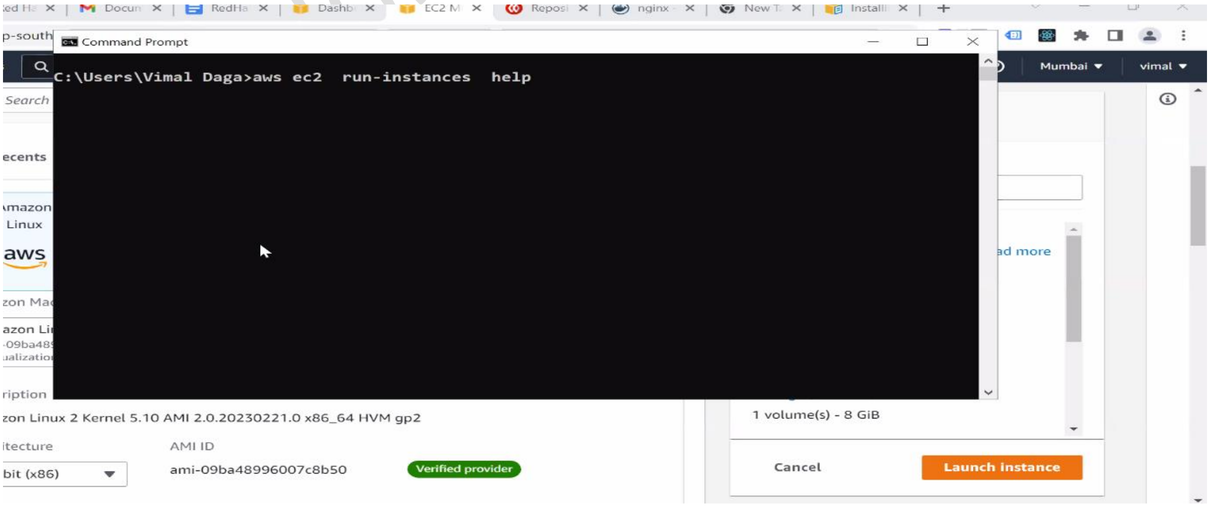
```
[default]
region = ap-south-1
output = json
[profile myvimal]
region = ap-south-1
output = json
[profile lwprofile]
region = ap-south-1
[profile awstestprofile]
region = us-east-1
[profile mylw]
region = ap-south-1
[profile myxyz]
region = us-east-1
```



```
C:\Users\Vimal Daga>cd .aws

C:\Users\Vimal Daga\.aws>dir
 Volume in drive C is Windows
 Volume Serial Number is 222F-6567

 Directory of C:\Users\Vimal Daga\.aws

30-05-2020  14:02    <DIR>          .
30-05-2020  14:02    <DIR>          ..
08-03-2023  21:21               264 config
08-03-2023  21:21               549 credentials
               2 File(s)            813 bytes
               2 Dir(s)  10,394,034,176 bytes free

C:\Users\Vimal Daga\.aws>notepad config

C:\Users\Vimal Daga\.aws>notepad config

C:\Users\Vimal Daga\.aws>notepad credentials

C:\Users\Vimal Daga\.aws>
```

```
[default]
aws_access_key_id = AKIARATU35LCY
aws_secret_access_key = 2HWEhozhl

[myvimal]
aws_access_key_id=AKIAWCIAQ62RRX
aws_secret_access_key=E5hLt1n982

[awstestprofile]
aws_access_key_id=AKIAQPYQMZ3WLN
aws_secret_access_key=Le8To971It
[mylw]
aws_access_key_id = AKIARATU35LC
aws_secret_access_key = QwFWoZwz
[myxyz]
aws_access_key_id = dgfshgn
aws_secret_access_key = asgsfgghr
```

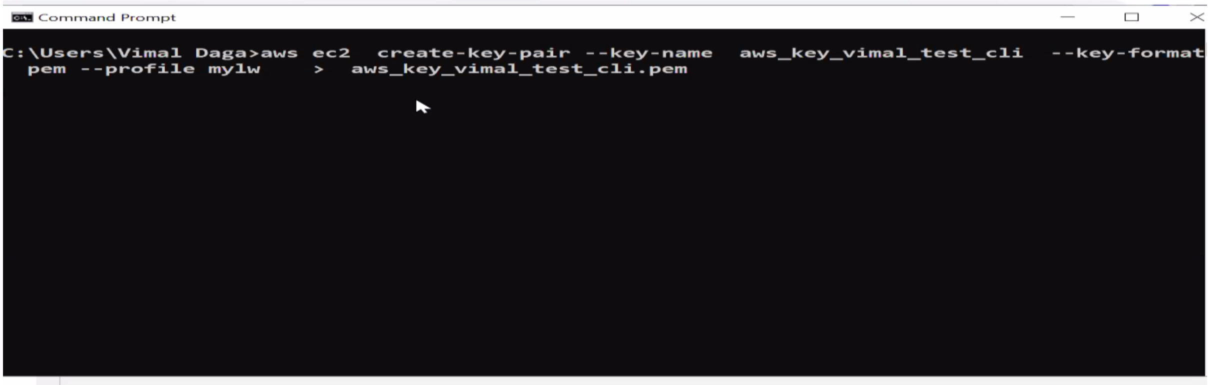
- aws –help command shows all services which aws supports.
- Subcommands is the other facility which we want to give to that particular service.
- Synopsis contains the options that a particular service contains.
- Now to use any service like ec2 we will use help to search other features inside that. Command- **aws ec2 run-instances help**



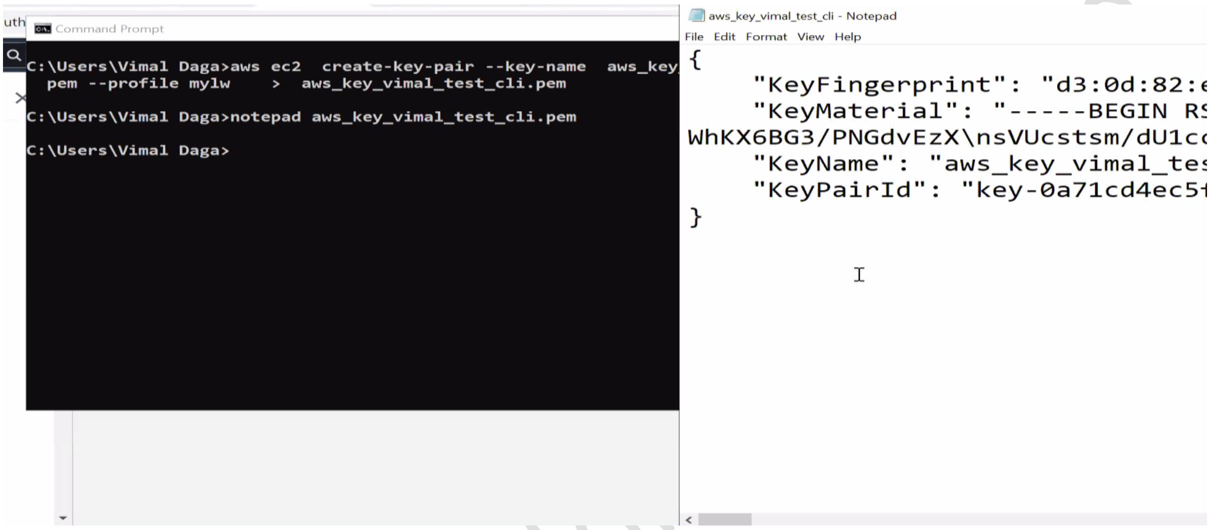
```
C:\Users\Vimal Daga>aws ec2  run-instances  help
```

To create key use command: **aws ec2 create-key-pair --key-name key_name_cli --key-format pem --profile profile_name > file.pem**

Note : here > file.pem is the file in which key details will be stored.



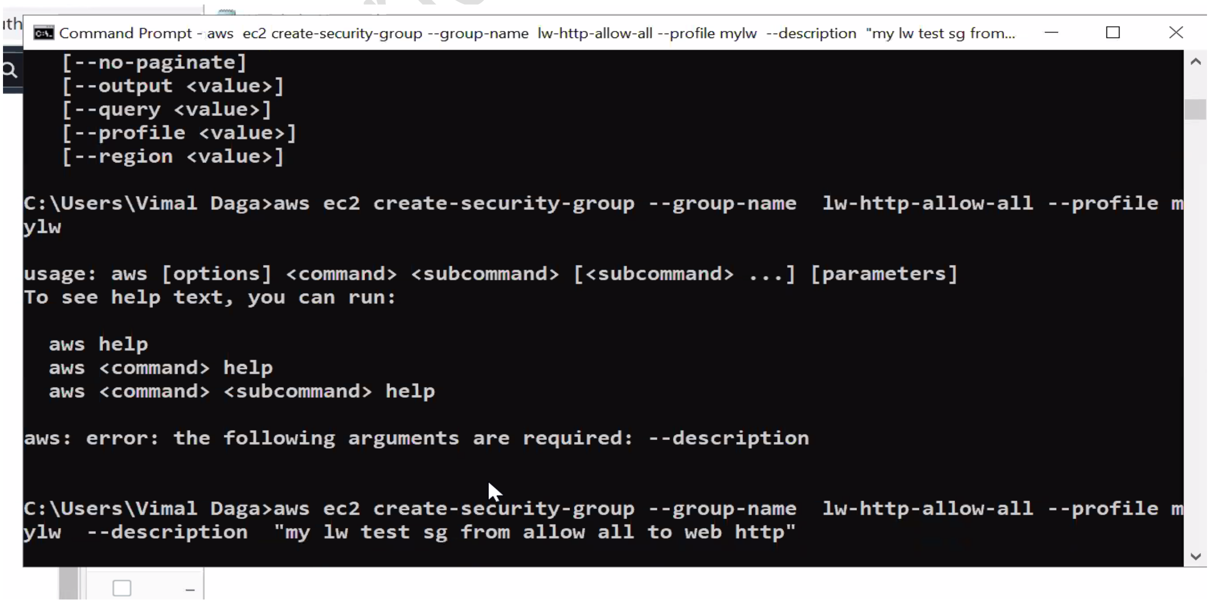
```
C:\Users\Vimal Daga>aws ec2  create-key-pair --key-name  aws_key_vimal_test_cli  --key-format
 pem --profile mylw    >  aws_key_vimal_test_cli.pem
```



```
C:\Users\Vimal Daga>aws ec2  create-key-pair --key-name  aws_key
 pem --profile mylw    >  aws_key_vimal_test_cli.pem

C:\Users\Vimal Daga>notepad aws_key_vimal_test_cli.pem

C:\Users\Vimal Daga>
```

```
{
    "KeyFingerprint": "d3:0d:82:
    "KeyMaterial": "-----BEGIN R
WhKX6BG3/PNGdvEzX\nsVUcstsm/dU1c
    "KeyName": "aws_key_vimal_te
    "KeyPairId": "key-0a71cd4ec5
}
```

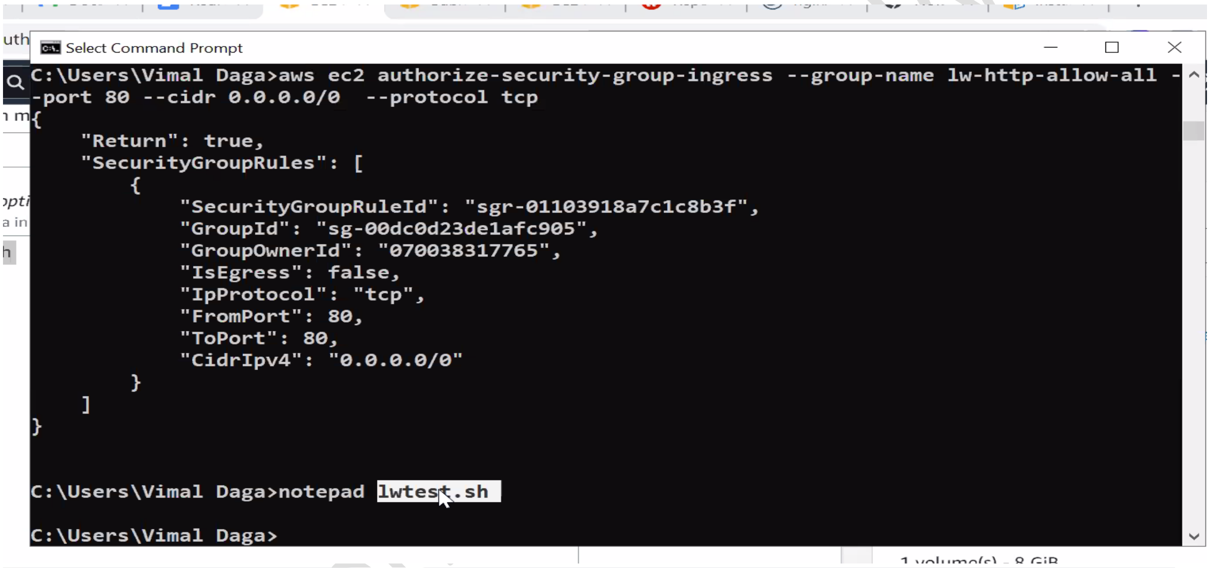
- We can also check in AWS Console screen by goining in key pairs in network and security.


Command Prompt - aws ec2 create-security-group --group-name lw-http-allow-all --profile mylw --description "my lw test sg from...

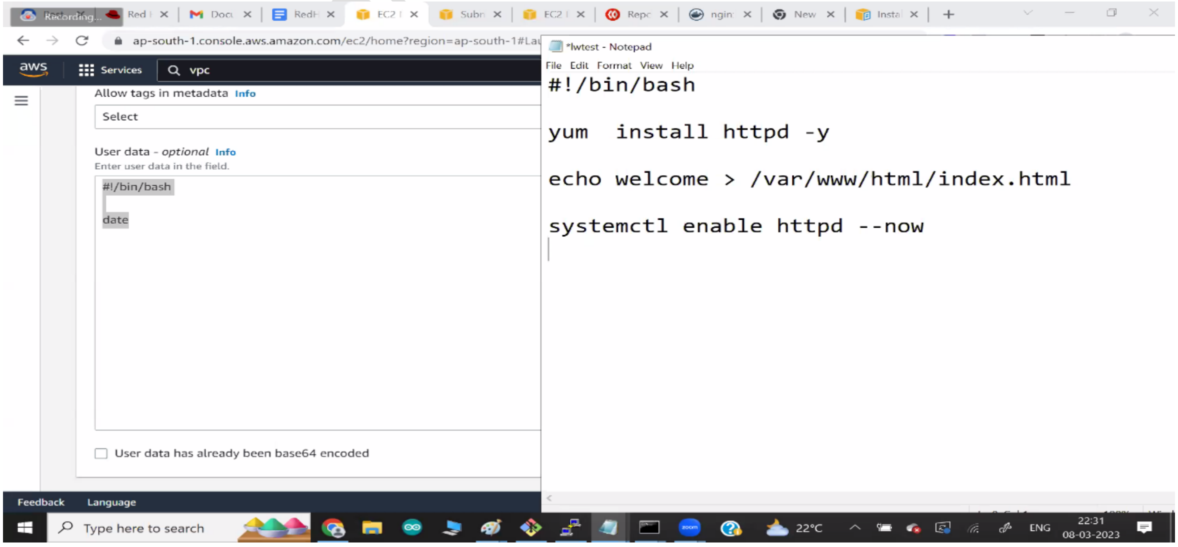
```
   [--no-paginate]
   [--output <value>]
   [--query <value>]
   [--profile <value>]
   [--region <value>]

C:\Users\Vimal Daga>aws ec2 create-security-group --group-name  lw-http-allow-all --profile m
ylw

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help

aws: error: the following arguments are required: --description


C:\Users\Vimal Daga>aws ec2 create-security-group --group-name  lw-http-allow-all --profile m
ylw  --description  "my lw test sg from allow all to web http"
```

aws ec2 create-security-group --group-name group_name --profile mylw --description “describe”

- Every OS/AMI gives AMI ID So whenever we launch instance, internally AWS use ID called ami-ID.
- Every availability zone belongs to different subnet(The way through which we select own Avalability zone).
- Webserver works on the protocol called HTTP which works on port=80. Allowing this is a rule.
- Anybody from internet denoted by IP 0.0.0.0/0 defines any IP in the world. Also referred as as source.
- Anything coming from internet to webserver it is called Inbound/Ingress.
- Group is more like a firewall, by default blocks everything.
- Cidr – Whenever we create a rule and in rule we give protocol and we give source, this way of giving the range is called CIDR.



```
C:\Users\Vimal Daga>aws ec2 authorize-security-group-ingress --group-name lw-http-allow-all --port 80 --cidr 0.0.0.0/0  --protocol tcp
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-01103918a7c1c8b3f",
            "GroupId": "sg-00dc0d23de1afc905",
            "GroupOwnerId": "070038317765",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
            "CidrIpv4": "0.0.0.0/0"
        }
    ]
}

C:\Users\Vimal Daga>notepad lwtest.sh

C:\Users\Vimal Daga>
```


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#La
aws
Services
vpc
*lwtest - Notepad
File Edit Format View Help
Feedback
Language
Type here to search
22°C
ENG
22:31
08-03-2023

Allow tags in metadata Info

Select

User data - optional Info

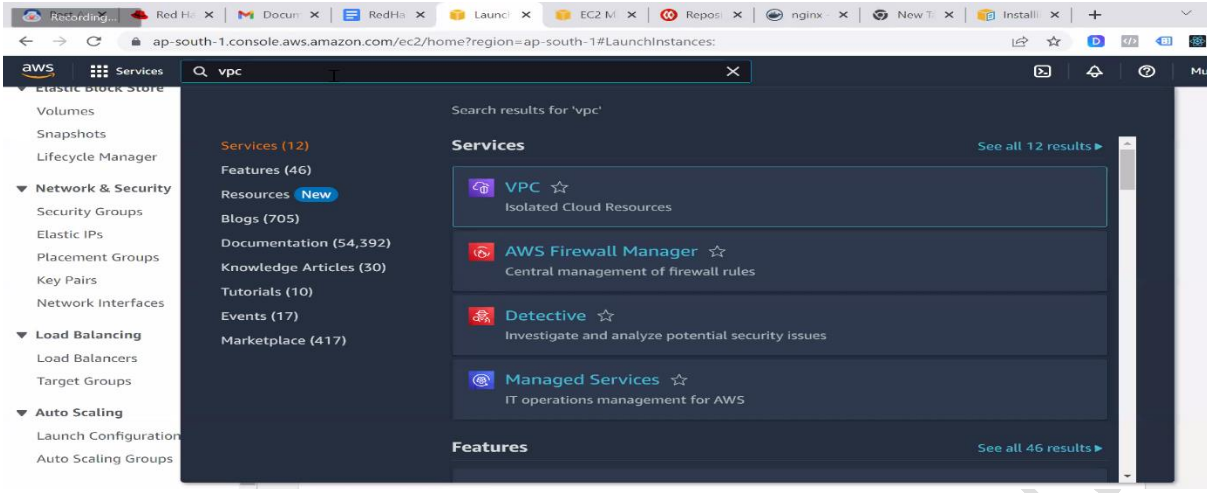
Enter user data in the field.

```
#!/bin/bash

date
```

□ User data has already been base64 encoded

```
#!/bin/bash

yum  install httpd -y

echo welcome > /var/www/html/index.html

systemctl enable httpd --now
```

- To know the security group Use VPC service and then choose subnets and choose subnet id.



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

Search: vpc

- Volumes
- Snapshots
- Lifecycle Manager
- Network & Security
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces
- Load Balancing
  - Load Balancers
  - Target Groups
- Auto Scaling
  - Launch Configurations
  - Auto Scaling Groups

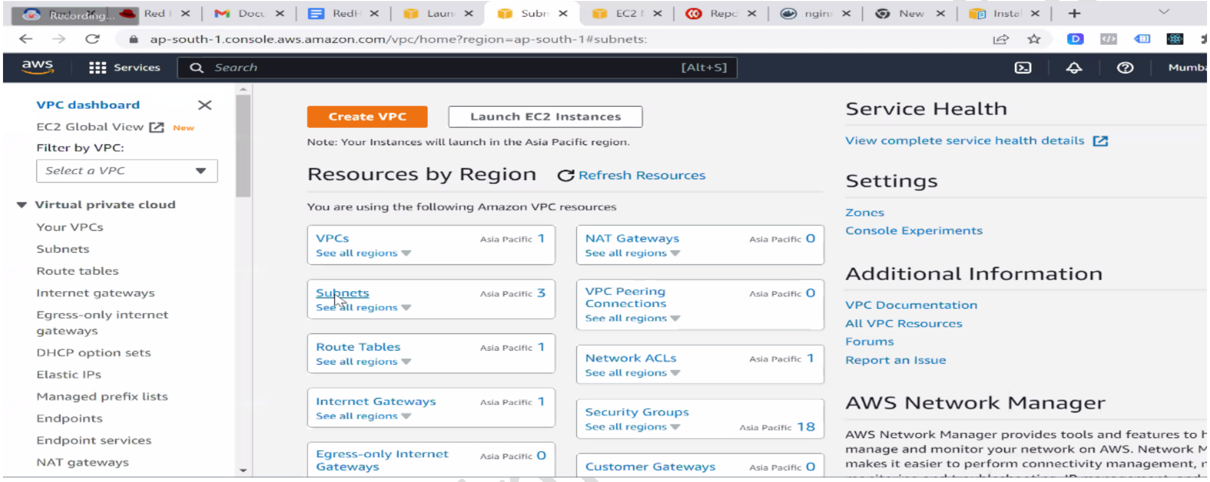
Search results for 'vpc'

- Services (12)
- Features (46)
- Resources New
- Blogs (705)
- Documentation (54,392)
- Knowledge Articles (30)
- Tutorials (10)
- Events (17)
- Marketplace (417)

Services — See all 12 results ▸

- VPC ☆ — Isolated Cloud Resources
- AWS Firewall Manager ☆ — Central management of firewall rules
- Detective ☆ — Investigate and analyze potential security issues
- Managed Services ☆ — IT operations management for AWS

Features — See all 46 results ▸



ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#subnets:

- VPC dashboard
- EC2 Global View New
- Filter by VPC: Select a VPC
- Virtual private cloud
  - Your VPCs
  - Subnets
  - Route tables
  - Internet gateways
  - Egress-only internet gateways
  - DHCP option sets
  - Elastic IPs
  - Managed prefix lists
  - Endpoints
  - Endpoint services
  - NAT gateways

Create VPC | Launch EC2 Instances

Note: Your Instances will launch in the Asia Pacific region.

Resources by Region — Refresh Resources

You are using the following Amazon VPC resources

Resource	Region	Count	Resource	Region	Count
VPCs	Asia Pacific	1	NAT Gateways	Asia Pacific	0
Subnets	Asia Pacific	3	VPC Peering Connections	Asia Pacific	0
Route Tables	Asia Pacific	1	Network ACLs	Asia Pacific	1
Internet Gateways	Asia Pacific	1	Security Groups	Asia Pacific	18
Egress-only Internet Gateways	Asia Pacific	0	Customer Gateways	Asia Pacific	0

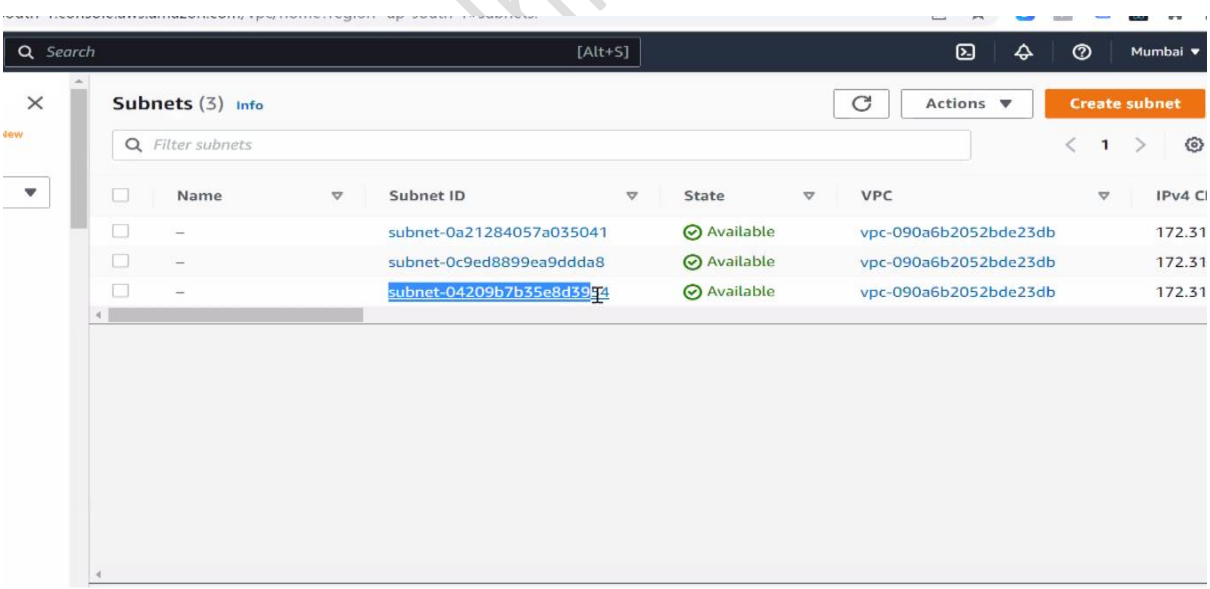
Service Health — View complete service health details

Settings — Zones, Console Experiments

Additional Information — VPC Documentation, All VPC Resources, Forums, Report an Issue

AWS Network Manager

AWS Network Manager provides tools and features to h manage and monitor your network on AWS. Network M makes it easier to perform connectivity management, r

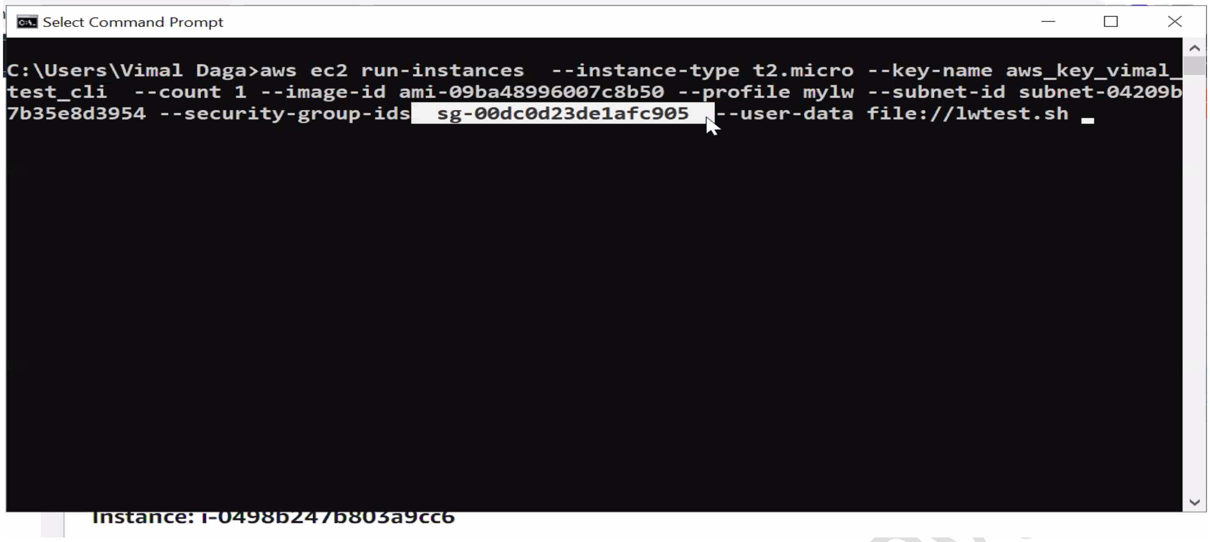


Subnets (3) Info — Actions — Create subnet

Name	Subnet ID	State	VPC	IPv4 CI
–	subnet-0a21284057a035041	Available	vpc-090a6b2052bde23db	172.31
–	subnet-0c9ed8899ea9ddda8	Available	vpc-090a6b2052bde23db	172.31
–	subnet-04209b7b35e8d39f4	Available	vpc-090a6b2052bde23db	172.31

To create instance use command –

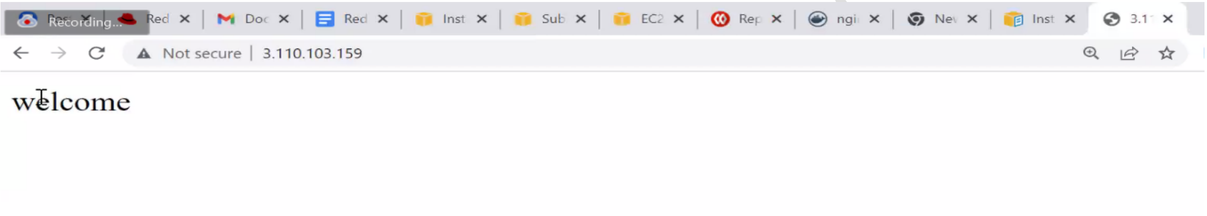
aws ec2 run-instances --instance-type t2.micro --key-name key_name --count 1--image-id image_id --profile profile_name --subnet-id subnet_id --security-group-ids security_group --user-data file://file.sh



```
C:\Users\Vimal Daga>aws ec2 run-instances  --instance-type t2.micro --key-name aws_key_vimal_
test_cli  --count 1 --image-id ami-09ba48996007c8b50 --profile mylw --subnet-id subnet-04209b
7b35e8d3954 --security-group-ids  sg-00dc0d23de1afc905  --user-data file://lwtest.sh
```

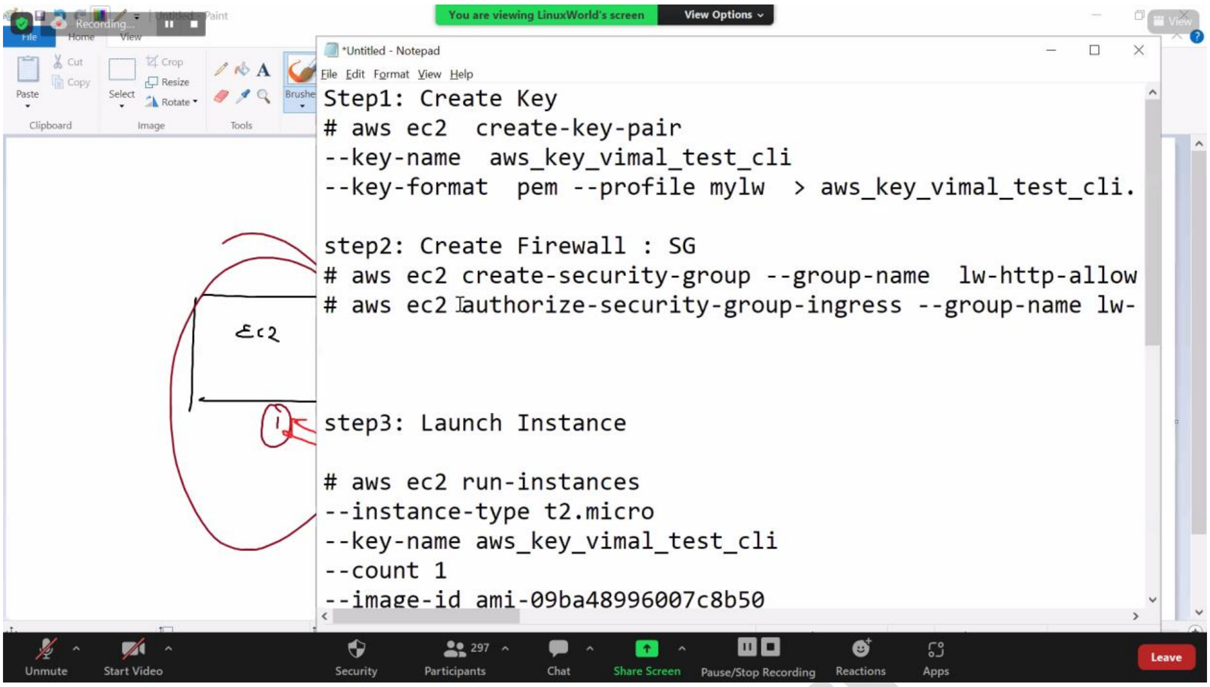
Instance: i-0498b247b803a9cc6

- To check copy the IP of the instance and check in browser.

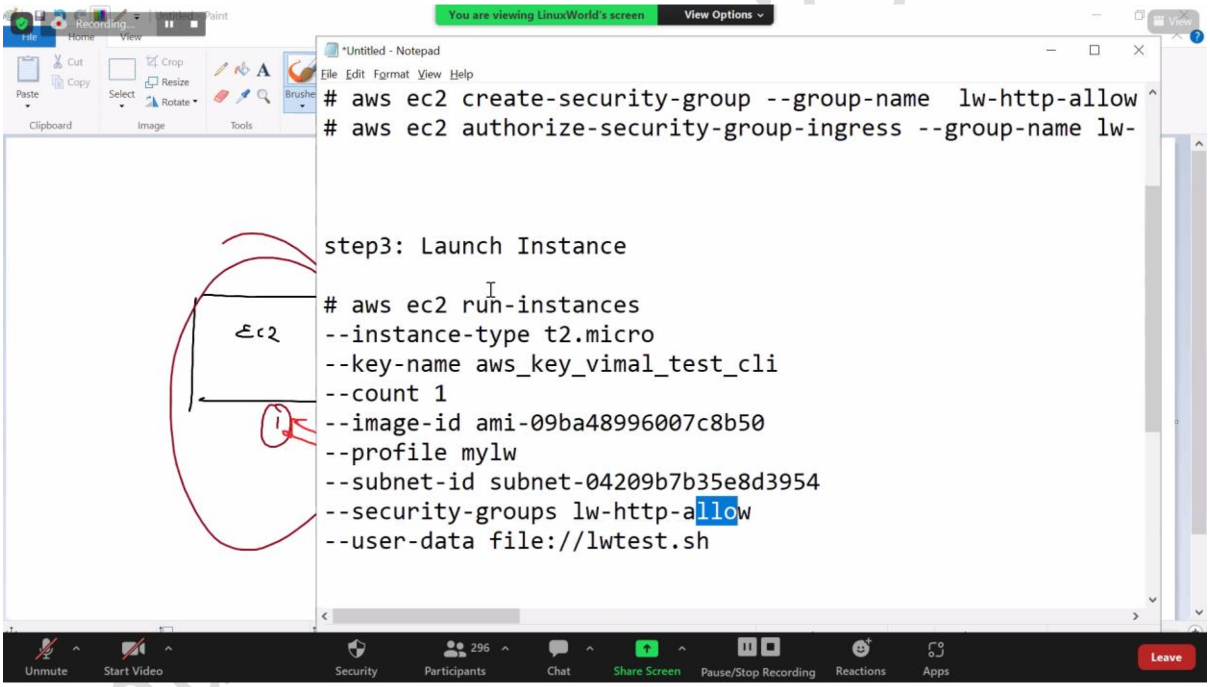


3.110.103.159

welcome



```
Step1: Create Key
# aws ec2  create-key-pair
--key-name  aws_key_vimal_test_cli
--key-format  pem --profile mylw  > aws_key_vimal_test_cli.

step2: Create Firewall : SG
# aws ec2 create-security-group --group-name  lw-http-allow
# aws ec2 authorize-security-group-ingress --group-name lw-



step3: Launch Instance

# aws ec2 run-instances
--instance-type t2.micro
--key-name aws_key_vimal_test_cli
--count 1
--image-id ami-09ba48996007c8b50
```



```
# aws ec2 create-security-group --group-name  lw-http-allow
# aws ec2 authorize-security-group-ingress --group-name lw-



step3: Launch Instance

# aws ec2 run-instances
--instance-type t2.micro
--key-name aws_key_vimal_test_cli
--count 1
--image-id ami-09ba48996007c8b50
--profile mylw
--subnet-id subnet-04209b7b35e8d3954
--security-groups lw-http-allow
--user-data file://lwtest.sh
```