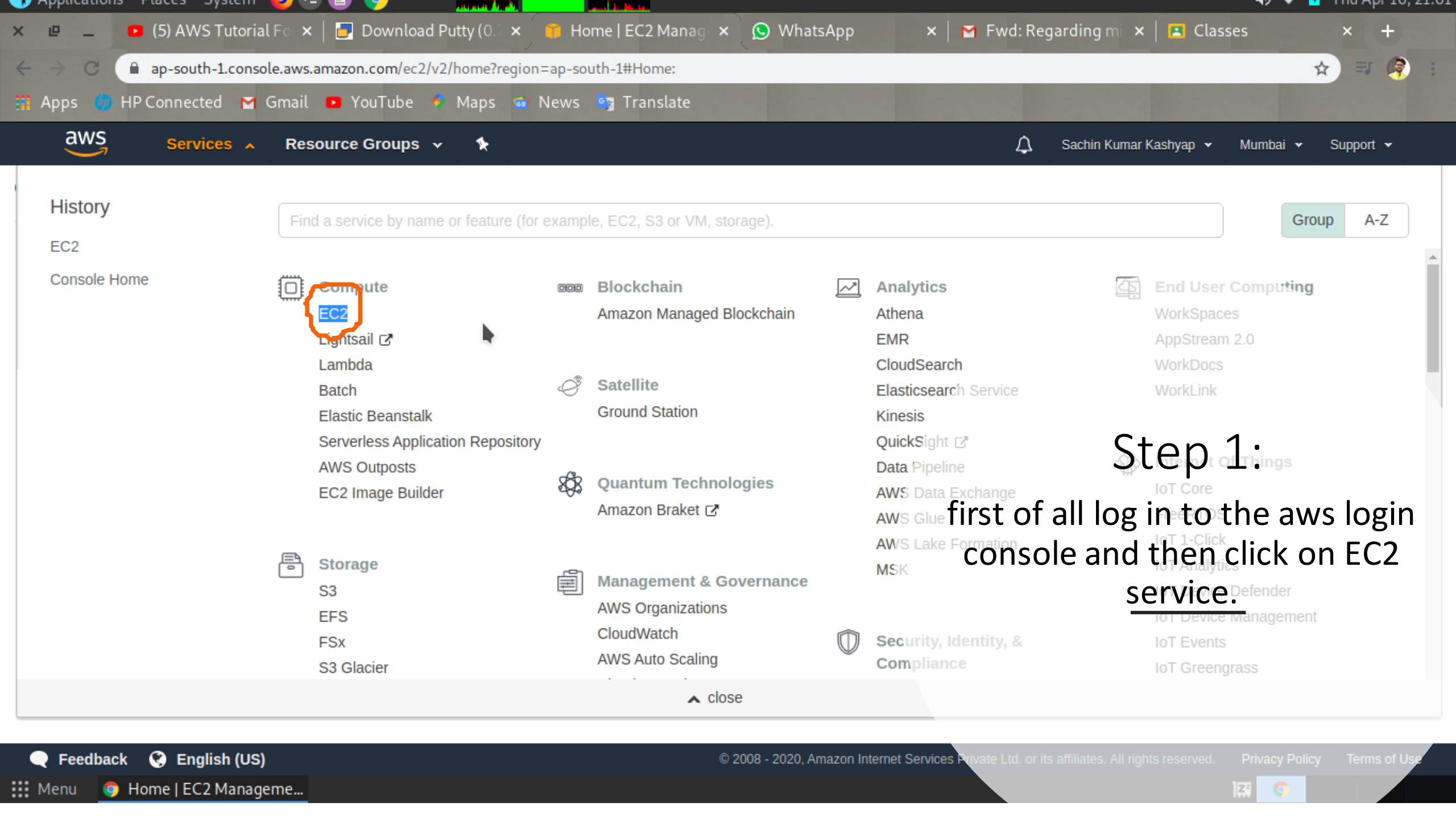


EC2 Service

How to create Amazon machine instance (AMI).



Step 1:
first of all log in to the aws login
console and then click on EC2
service.

aws Services Resource Groups

New EC2 Experience Tell us what you think

EC2 Dashboard New

Events New

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

▼ IMAGES

Running Instances	0	Elastic IPs	0
Dedicated Hosts	0	Snapshots	0
Volumes	2	Load balancers	0
Key pairs	1	Security groups	6
Placement groups	0		

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▲

Launch Instance

Launch Instance from template

Asia Pacific (Mumbai) Region

Scheduled events

Supported platforms

- VPC

Default VPC

vpc-d2b985ba

Console experiments

Settings

Additional information

Getting started guide

Documentation

All EC2 resources

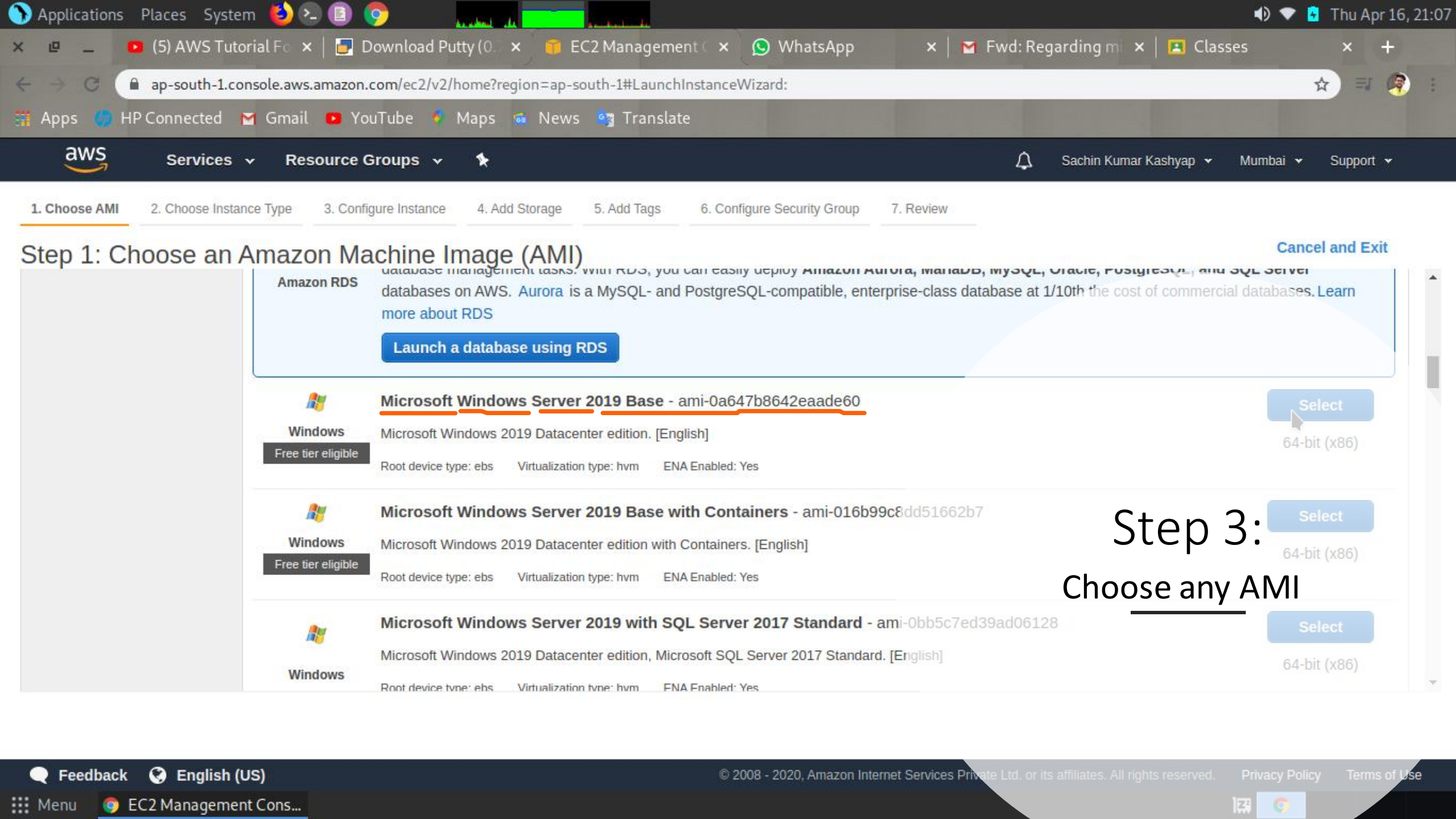
Forums

Pricing

Contact us

Step 2:

Click on Lunch instance



Step 1: Choose an Amazon Machine Image (AMI)

Amazon RDS

database management tasks. With RDS, you can easily deploy Amazon Aurora, MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server databases on AWS. Aurora is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

Launch a database using RDS

Windows

Free tier eligible

Microsoft Windows Server 2019 Base - ami-0a647b8642eaade60

Microsoft Windows 2019 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Windows

Free tier eligible

Microsoft Windows Server 2019 Base with Containers - ami-016b99c8dd51662b7

Microsoft Windows 2019 Datacenter edition with Containers. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Windows

Microsoft Windows Server 2019 with SQL Server 2017 Standard - ami-0bb5c7ed39ad06128

Microsoft Windows 2019 Datacenter edition, Microsoft SQL Server 2017 Standard. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Cancel and Exit

Select

64-bit (x86)

Select

64-bit (x86)

Select

64-bit (x86)

Step 3:
Choose any AMI

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Add Tags
- 6. Configure Security Group
- 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

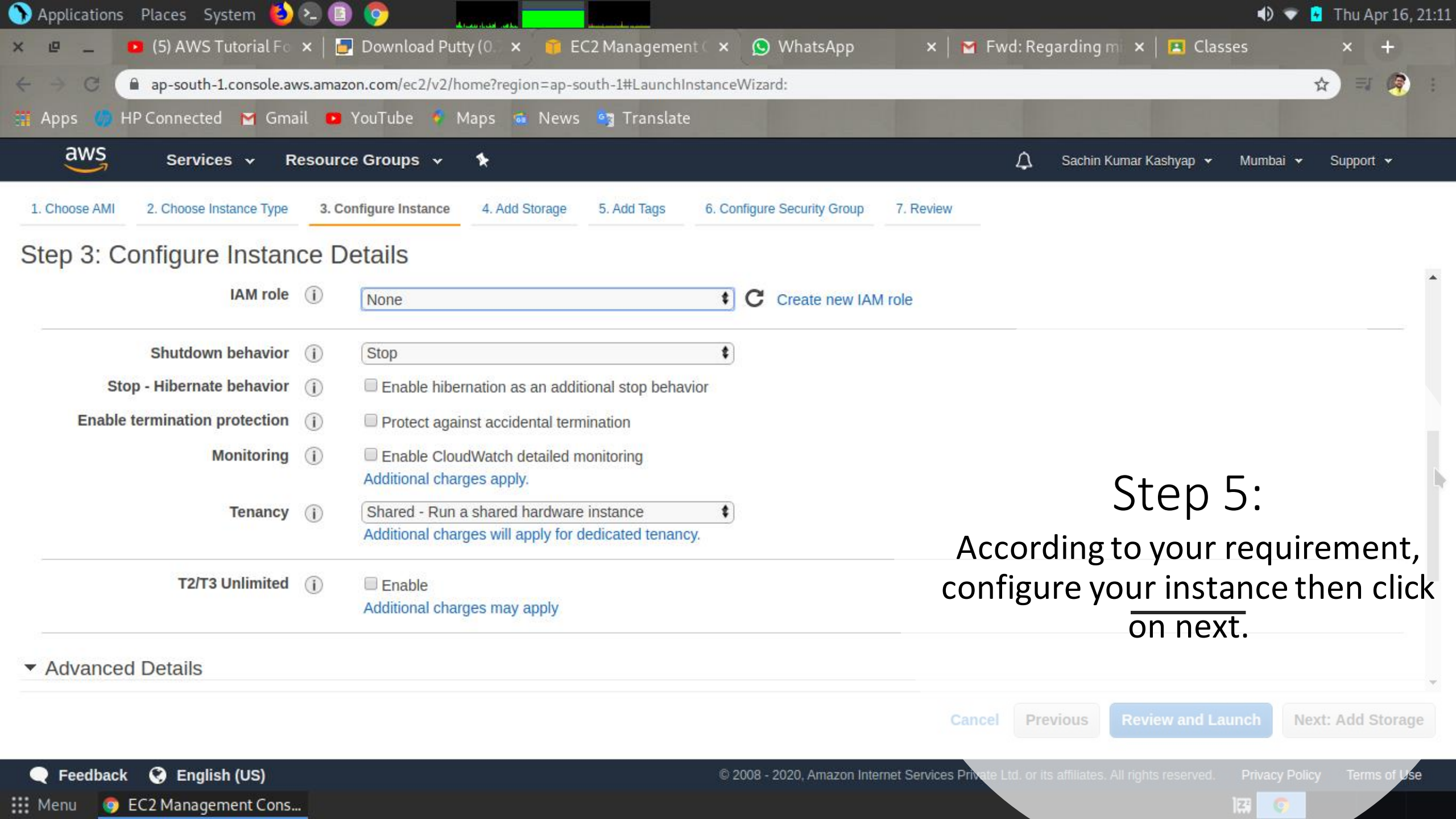
Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

Step 4:
choose any instance type and then click on next.

Cancel Previous Review and Launch Next: Configure Instance Details



Step 3: Configure Instance Details

IAM role ⓘ

None

Create new IAM role

Shutdown behavior ⓘ

Stop

Stop - Hibernate behavior ⓘ

☐ Enable hibernation as an additional stop behavior

Enable termination protection ⓘ

☐ Protect against accidental termination

Monitoring ⓘ

☐ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy ⓘ

Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

T2/T3 Unlimited ⓘ

☐ Enable
Additional charges may apply

Step 5:
According to your requirement,
configure your instance then click
on next.

Advanced Details

Cancel

Previous

Review and Launch

Next: Add Storage

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Add Tags
- 6. Configure Security Group
- 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⁱ	Device ⁱ	Snapshot ⁱ	Size (GiB) ⁱ	Volume Type ⁱ	IOPS ⁱ	Throughput (MB/s) ⁱ	Delete on Termination ⁱ	Encryption ⁱ
Root	/dev/sda1	snap-0680e1e8832053e01	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt ⁱ

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Step 6:
Add new volume if you want
otherwise click on next.

Cancel Previous Review and Launch Next: Add Tags

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Add Tags
- 6. Configure Security Group
- 7. Review

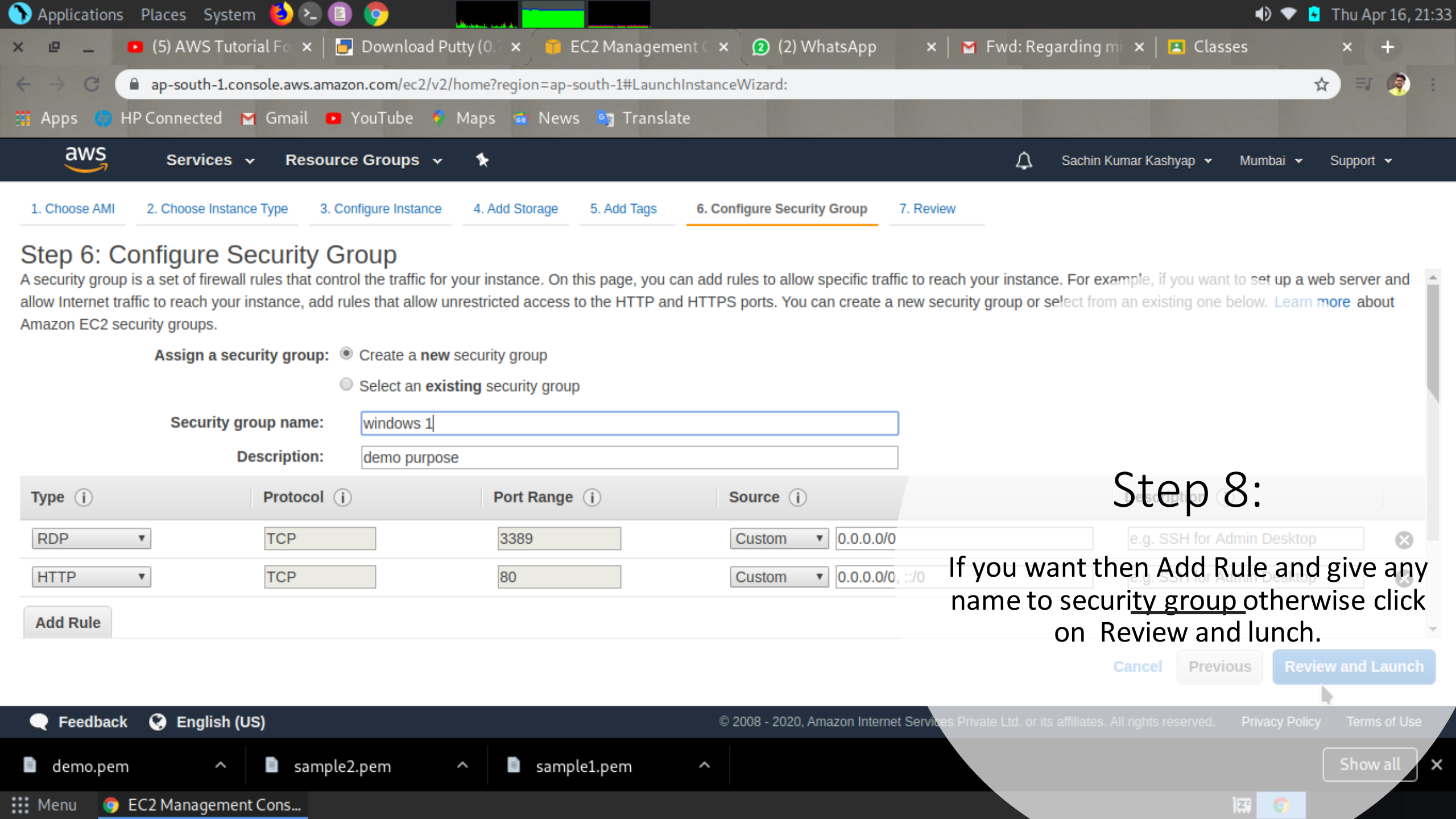
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
sample1	test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

(Up to 50 tags maximum)

Step 7:
Add any tags which you want and then click on next.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:

☒ Create a **new** security group

☐ Select an **existing** security group

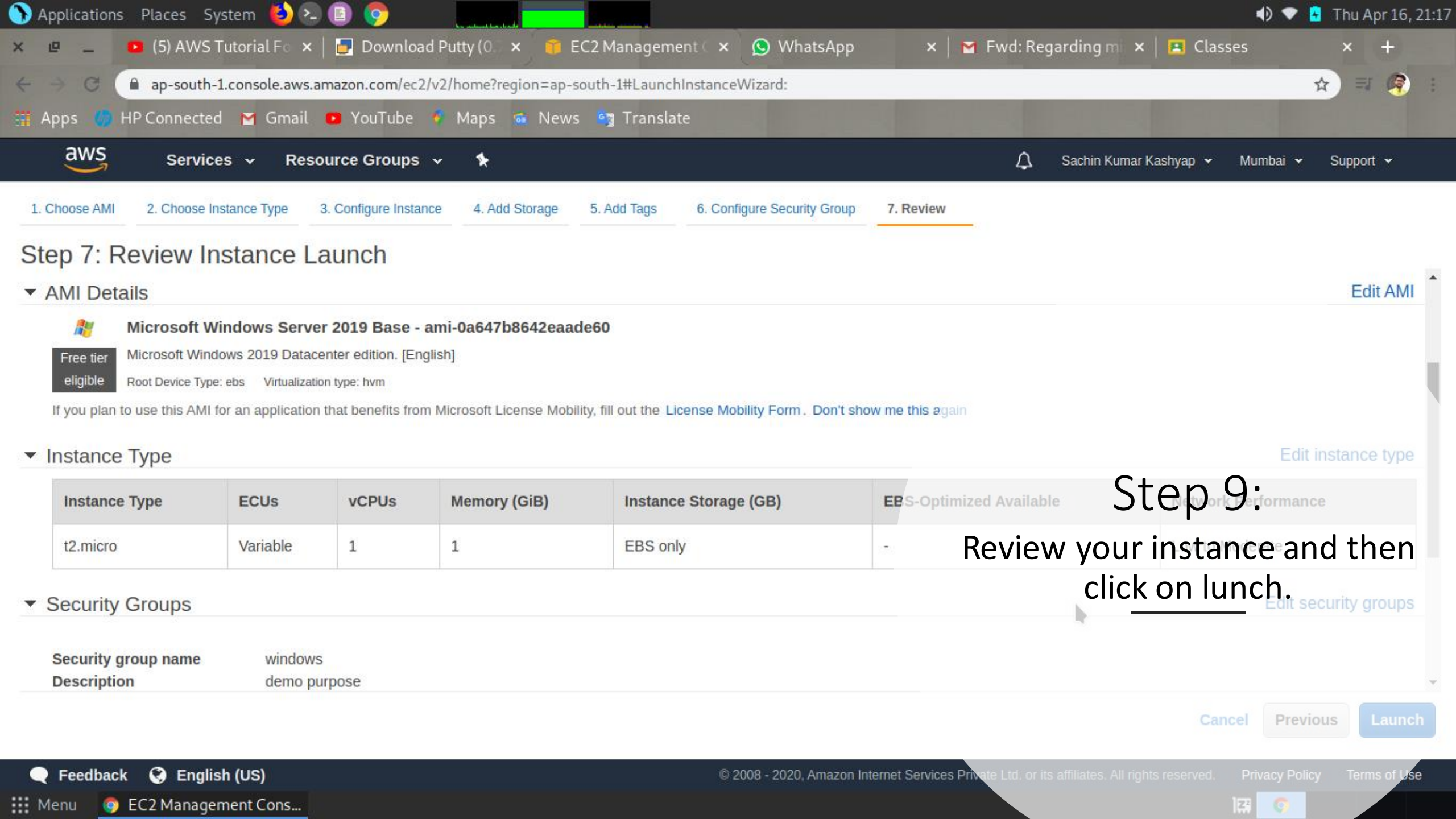
Security group name:

Description:

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Step 8:

If you want then Add Rule and give any name to security_group otherwise click on Review and lunch.



Step 7: Review Instance Launch

AMI Details

[Edit AMI](#)

Microsoft Windows Server 2019 Base - ami-0a647b8642eaade60

Free tier
eligible

Microsoft Windows 2019 Datacenter edition. [English]

Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). [Don't show me this again](#)

Instance Type

[Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Baseline

Security Groups

[Edit security groups](#)

Security group name windows
Description demo purpose

[Cancel](#)[Previous](#)[Launch](#)

1. Choose AMI2. Choose Instance Type3. Configure Instance Details4. Review Instance Launch

Step 7: Review Instance Launch

AMI Details

Microsoft Windows Server 2019 Datacenter

Free tier eligible

Root Device Type: ebs

Virtualization type: x64

If you plan to use this AMI for an application that requires a specific architecture, you must select the appropriate architecture.

Instance Type

Instance Type	ECUs
t2.micro	Variable

Security Groups

Feedback

English (US)

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Create a new key pair

Key pair name

demo

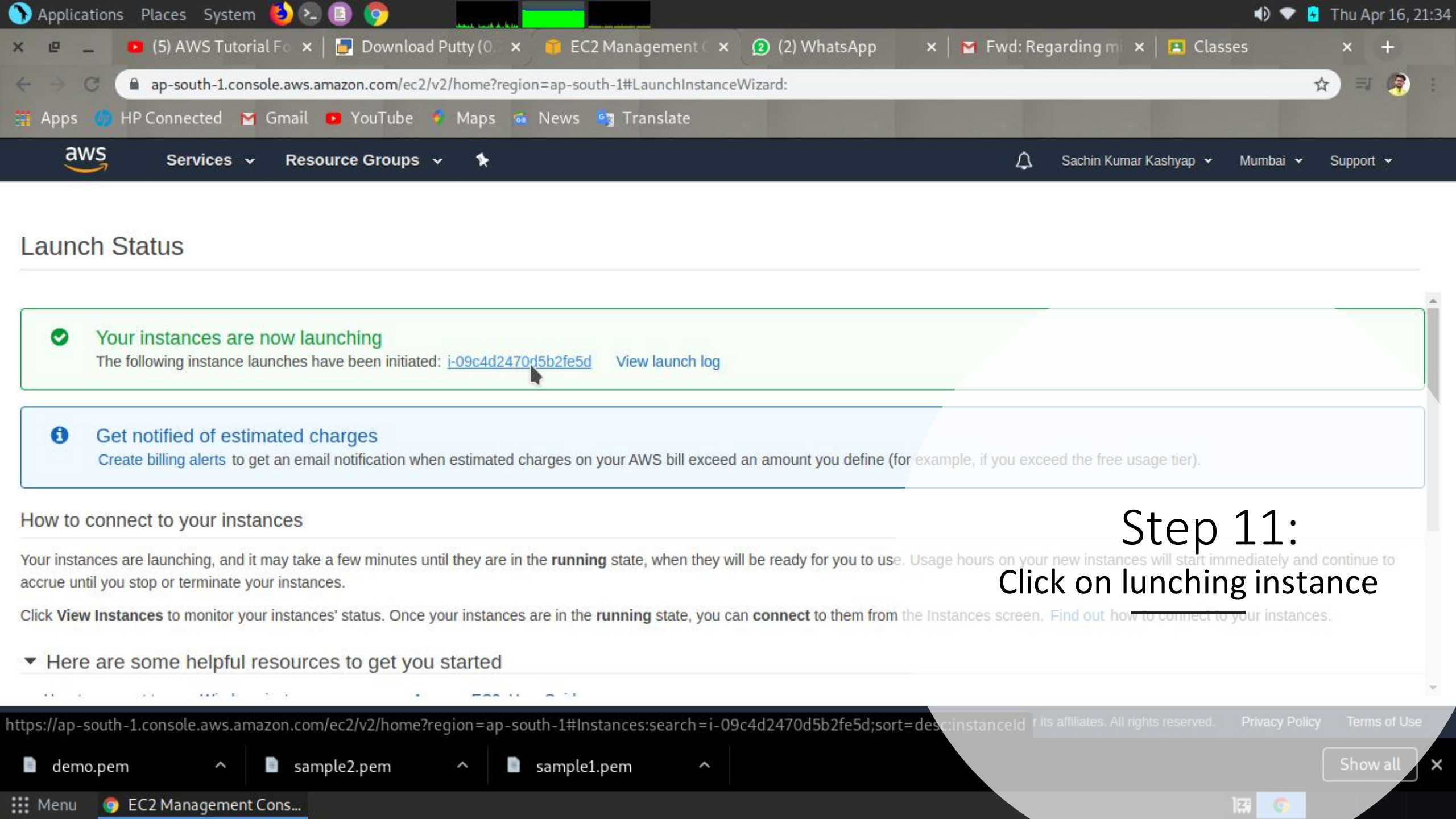
You have to download the **private key file** (*.pem file) before you can continue. [Store it in a secure and accessible location.](#) You will not be able to download the file again after it's created.

Cancel

Launch Instances

Step 10:

Create a key pair and give a name and download key pair at any location and then click on lunch instance.



Launch Status

✓ **Your instances are now launching**
The following instance launches have been initiated: [i-09c4d2470d5b2fe5d](#) [View launch log](#)

i **Get notified of estimated charges**
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

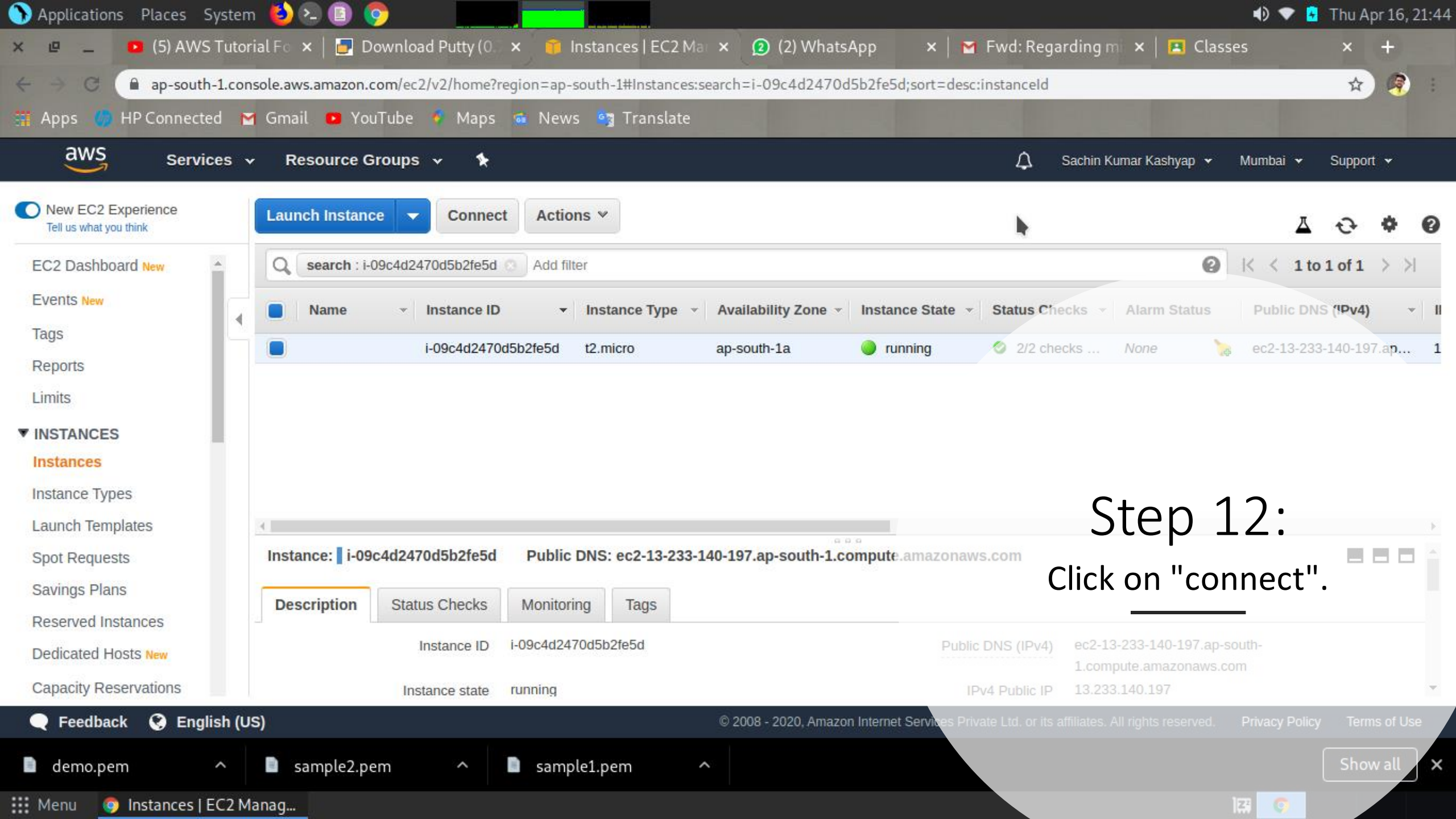
How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

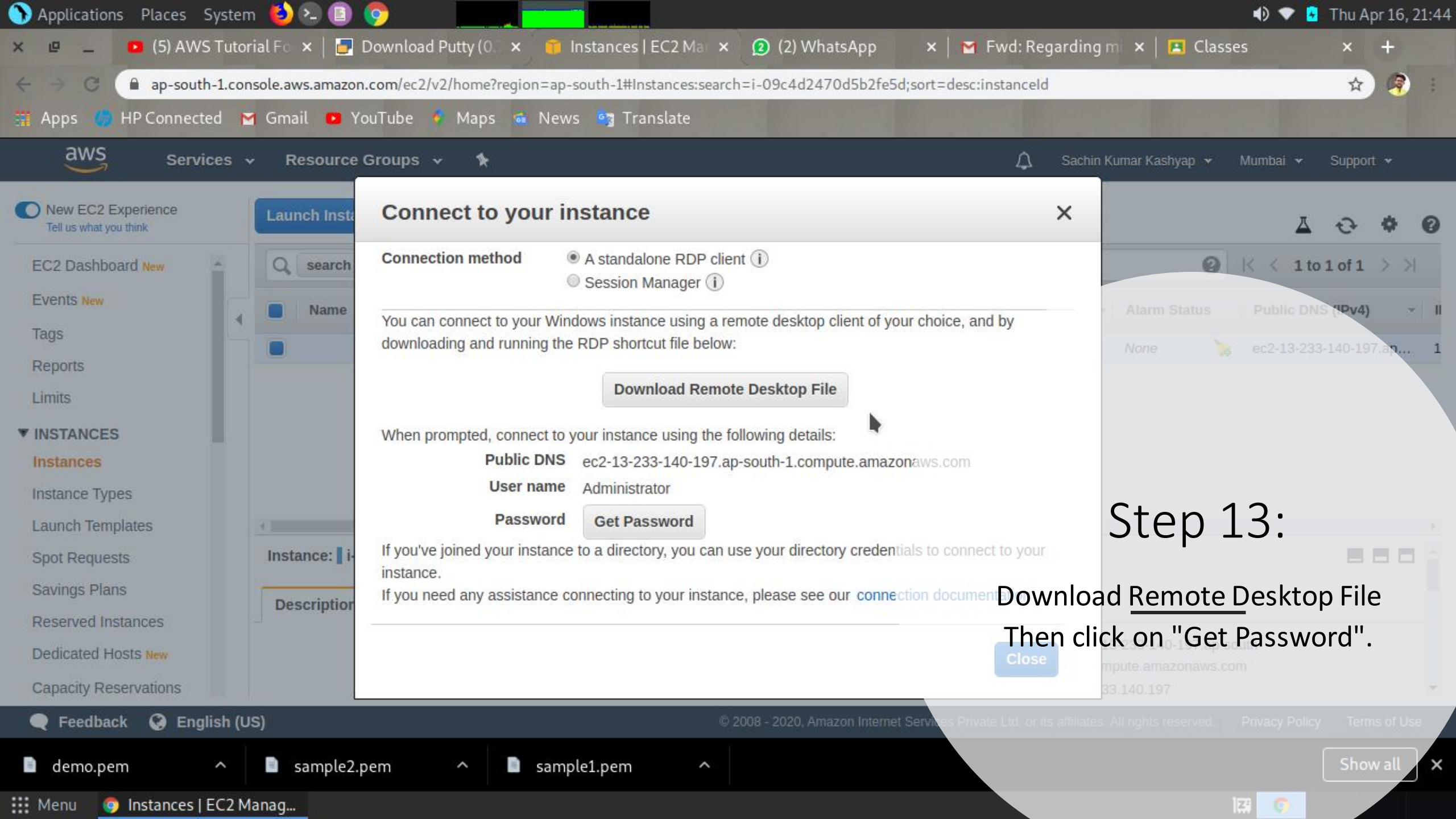
Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

Step 11:
Click on launching instance



Step 12:
Click on "connect".



Connect to your instance

Connection method

- ☒ A standalone RDP client ⓘ
- ☐ Session Manager ⓘ

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download Remote Desktop File](#)

When prompted, connect to your instance using the following details:

Public DNS ec2-13-233-140-197.ap-south-1.compute.amazonaws.com

User name Administrator

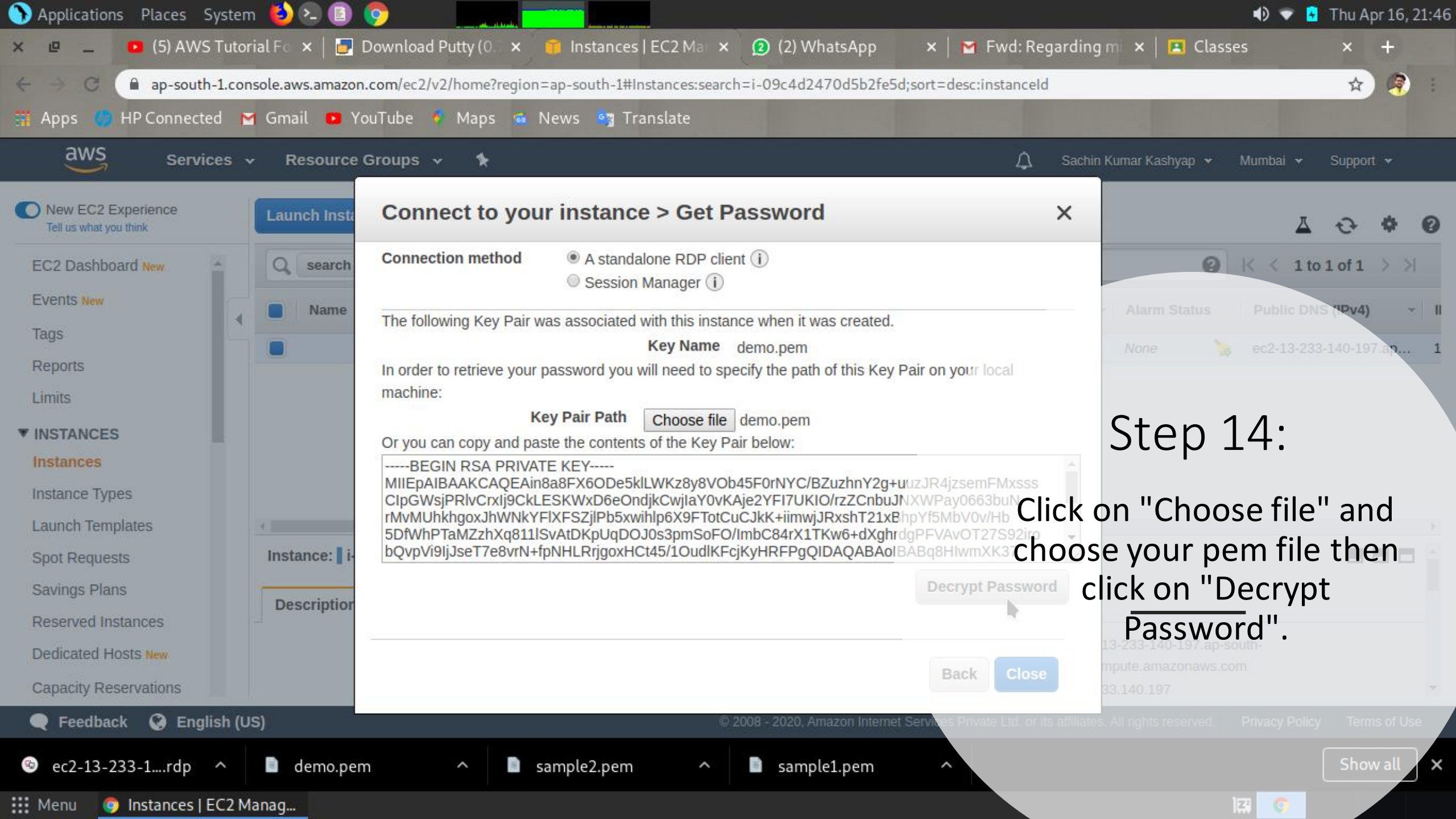
Password [Get Password](#)

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection document](#).

Step 13:
Download Remote Desktop File
Then click on "Get Password".

[Close](#)



Connect to your instance > Get Password

Connection method

- ☒ A standalone RDP client ⓘ
☐ Session Manager ⓘ

The following Key Pair was associated with this instance when it was created.

Key Name demo.pem

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

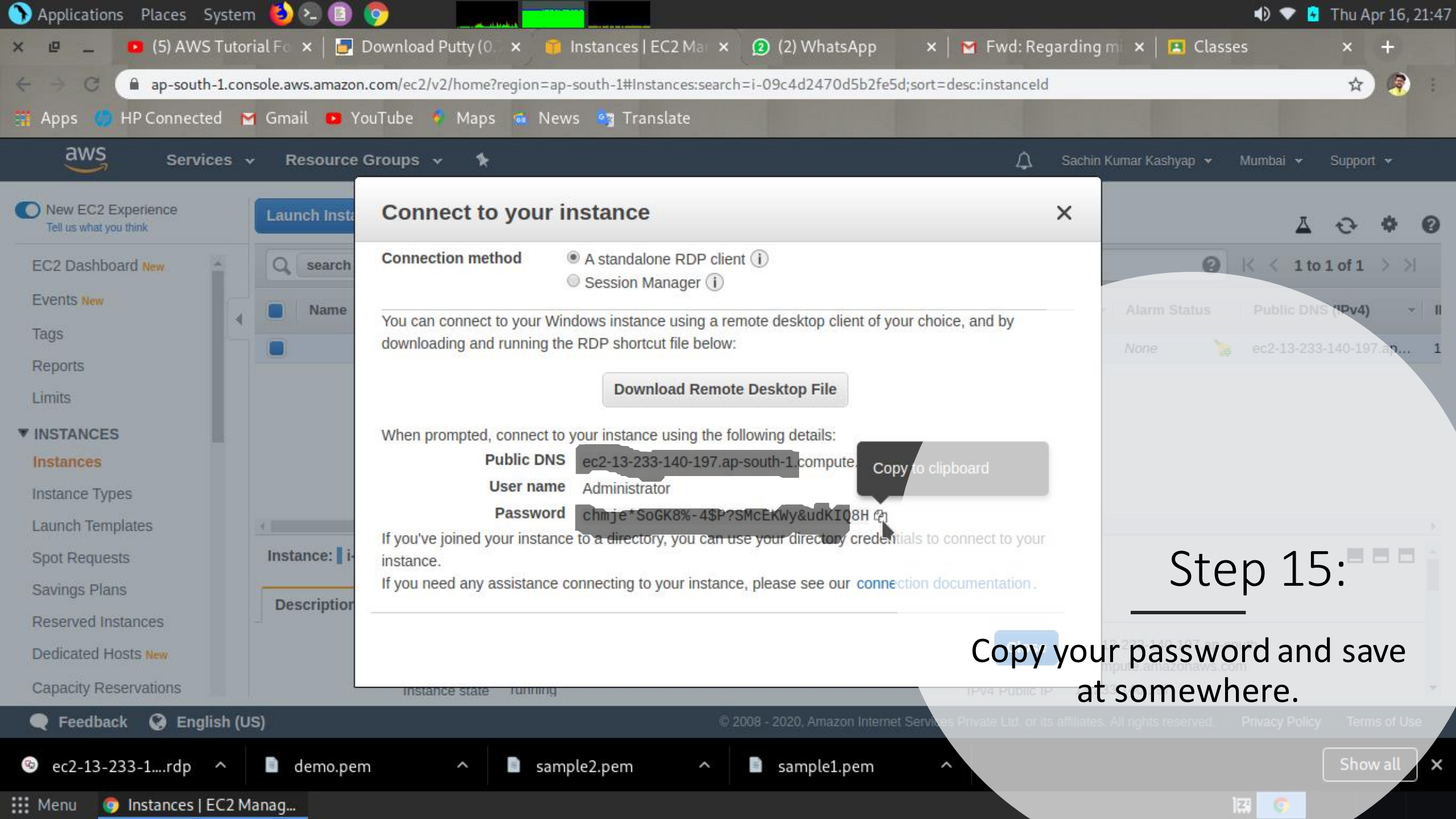
Key Pair Path demo.pem

Or you can copy and paste the contents of the Key Pair below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAin8a8FX6ODE5klLWKz8y8VOB45F0rNYC/BZuzhnY2g+uuzJR4jzsemFMxsss
CipGWsjPRlvCrxlj9CKLESKWxD6eOndjkCwjlaY0vKAje2YFI7UKIO/rzZCnbnJNXWPAY0663buN
rMvMUhkhgoxJhWNkYFIXFSZjlpB5xwihlp6X9FTotCuCJkK+iimwjJRxshT21xBhpYf5MbV0v/Hb
5DfWhPTaMZzhXq811lSvAtDKpUqDOJ0s3pmSoFO/lmbC84rX1TKw6+dXghrdgPFVAvOT27S92irn
bQvpVi9ljJseT7e8vrN+fpNHLRrjgoxHCt45/1OudlKFcjKyHRFPgQIDAQABAolBABq8HlwmXK3
```

Step 14:

Click on "Choose file" and choose your pem file then click on "Decrypt Password".



Connect to your instance

Connection method

- ☒ A standalone RDP client ⓘ
☐ Session Manager ⓘ

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download Remote Desktop File](#)

When prompted, connect to your instance using the following details:

Public DNS ec2-13-233-140-197.ap-south-1.compute

User name Administrator

Password chmje*SoGK8%-4\$P?SMcEKWy&udKI08H 21

[Copy to clipboard](#)

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Step 15:

Copy your password and save at somewhere.



Parrot



Home



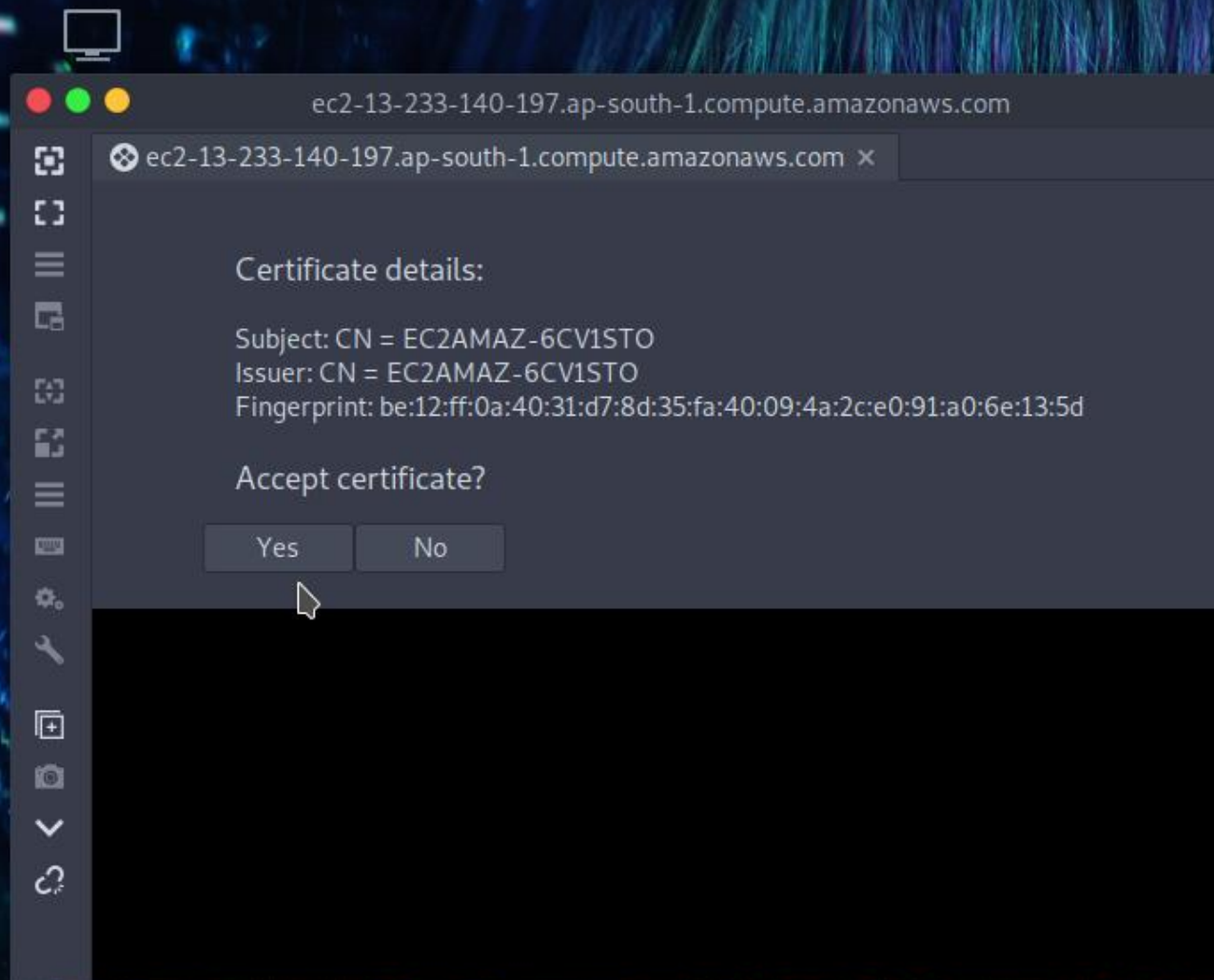
aws



ec2-13-233-140-
197.ap-south-1.
compute.amazonaws...



Step 16:
click on Desktop Remote file



Step 17:
Click on "Yes" to accept
certificate.

ec2-13-233-140-197.ap-south-1.compute.amazonaws.com

ec2-13-233-140-197.ap-south-1.compute.amazonaws.com x

Enter RDP authentication credentials

Username

Password

Domain

Save password ☐

OK Cancel

Step 18

Paste Your password which
you copied in step 15.



Recycle Bin



EC2 Feedback



EC2 Microsoft
Windows G...



6:42 AM
5/2/2020



thanks

Now your AMI is ready.

