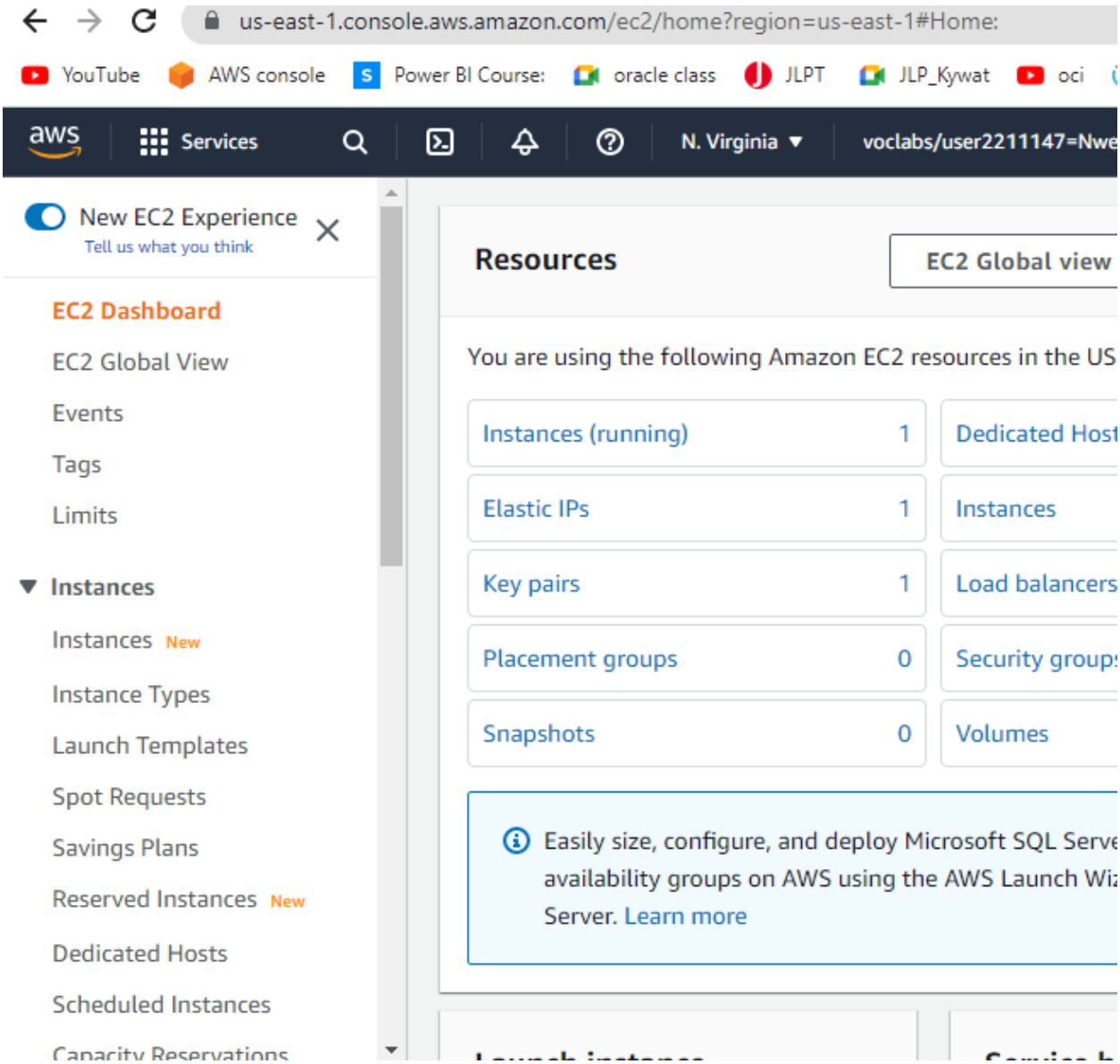
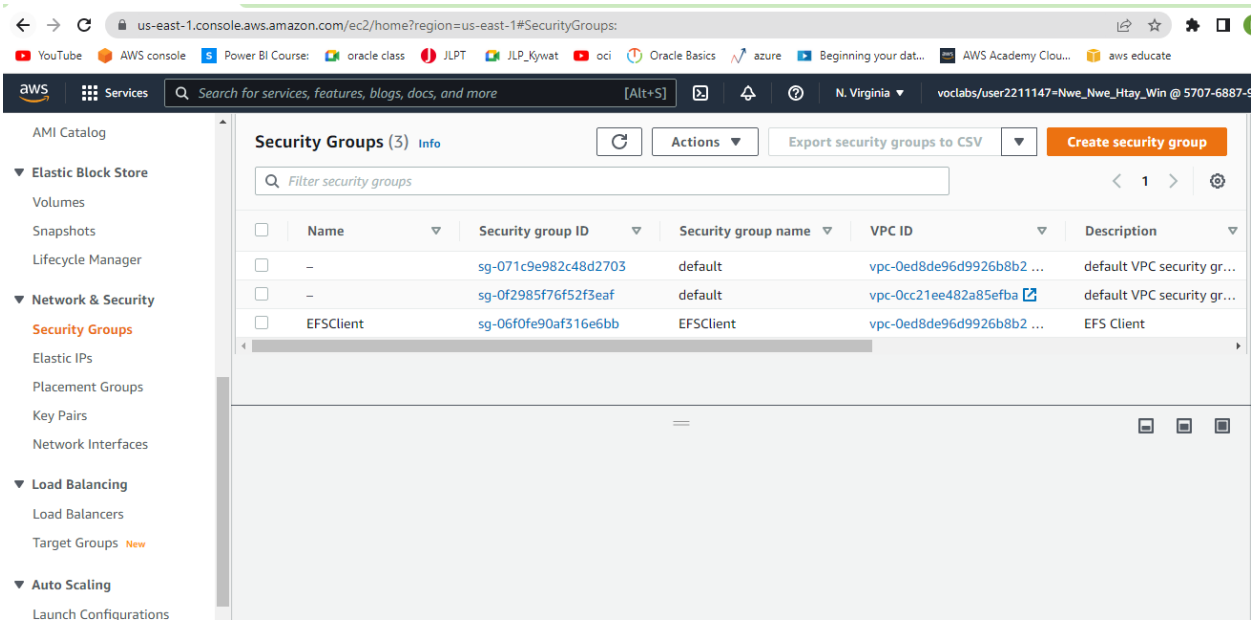
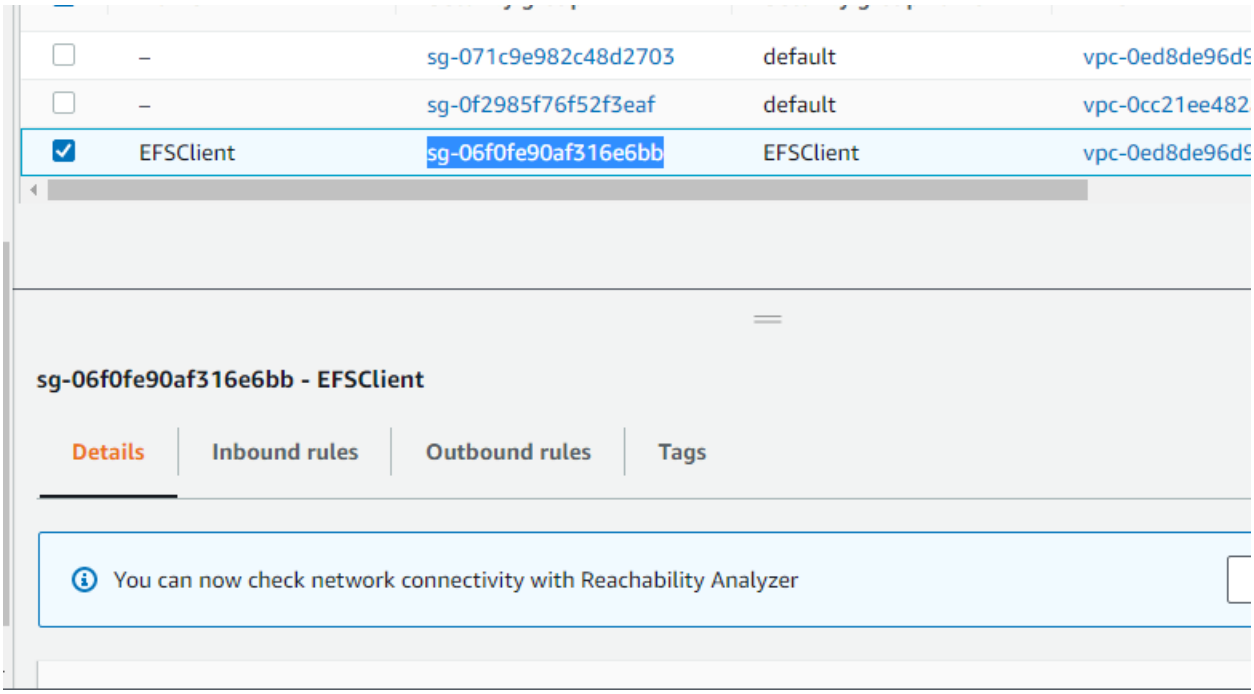


Choose security group


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroups:
YouTube
AWS console
Power BI Course:
oracle class
JLPT
JLP_Kywat
oci
Oracle Basics
azure
Beginning your dat...
AWS Academy Clou...
aws educate
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Target Groups New
Auto Scaling
Launch Configurations
Security Groups (3) Info
Actions
Export security groups to CSV
Create security group
Filter security groups
Name
Security group ID
Security group name
VPC ID
Description
– sg-071c9e982c48d2703 default vpc-0ed8de96d9926b8b2 ... default VPC security gr...
– sg-0f2985f76f52f3eaf default vpc-0cc21ee482a85efba default VPC security gr...
EFSClient sg-06f0fe90af316e6bb EFSClient vpc-0ed8de96d9926b8b2 ... EFS Client


– sg-071c9e982c48d2703 default vpc-0ed8de96d9
– sg-0f2985f76f52f3eaf default vpc-0cc21ee482
EFSClient sg-06f0fe90af316e6bb EFSClient vpc-0ed8de96d9
sg-06f0fe90af316e6bb - EFSClient
Details
Inbound rules
Outbound rules
Tags
You can now check network connectivity with Reachability Analyzer

Basic details

Security group name Info

EFS Mount Target

Name cannot be edited after creation.

Description Info

Inbound NFS access from EFS clients

VPC Info

Lab VPC

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
NFS	TCP	2049	Custom sg-06f0fe90af316e6bb		Delete

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia voclabs/user2211147=Nwe_Nwe_Htay_Win @ 5707-6887-9

New EC2 Experience
Tell us what you think

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

Security group (sg-03cf1b12e3f4f1481 | EFS Mount Target) was created successfully
Details

EC2 > Security Groups > sg-03cf1b12e3f4f1481 - EFS Mount Target

sg-03cf1b12e3f4f1481 - EFS Mount Target

Actions

Details

Security group name	Security group ID	Description	VPC ID
EFS Mount Target	sg-03cf1b12e3f4f1481	Inbound NFS access from EFS clients	vpc-0ed8de96d9926b8b2

Owner	Inbound rules count	Outbound rules count
570768879355	1 Permission entry	1 Permission entry

Inbound rules | Outbound rules | Tags

Elastic File System

File systems
Access points

AWS Backup
AWS DataSync
AWS Transfer

Documentation

Amazon Elastic File System

Scalable, elastic, cloud-native NFS file system

Amazon Elastic File System (Amazon EFS) provides a simple, scalable, elastic file system for general purpose workloads for use with AWS Cloud services and on-premises resources.

Create file system

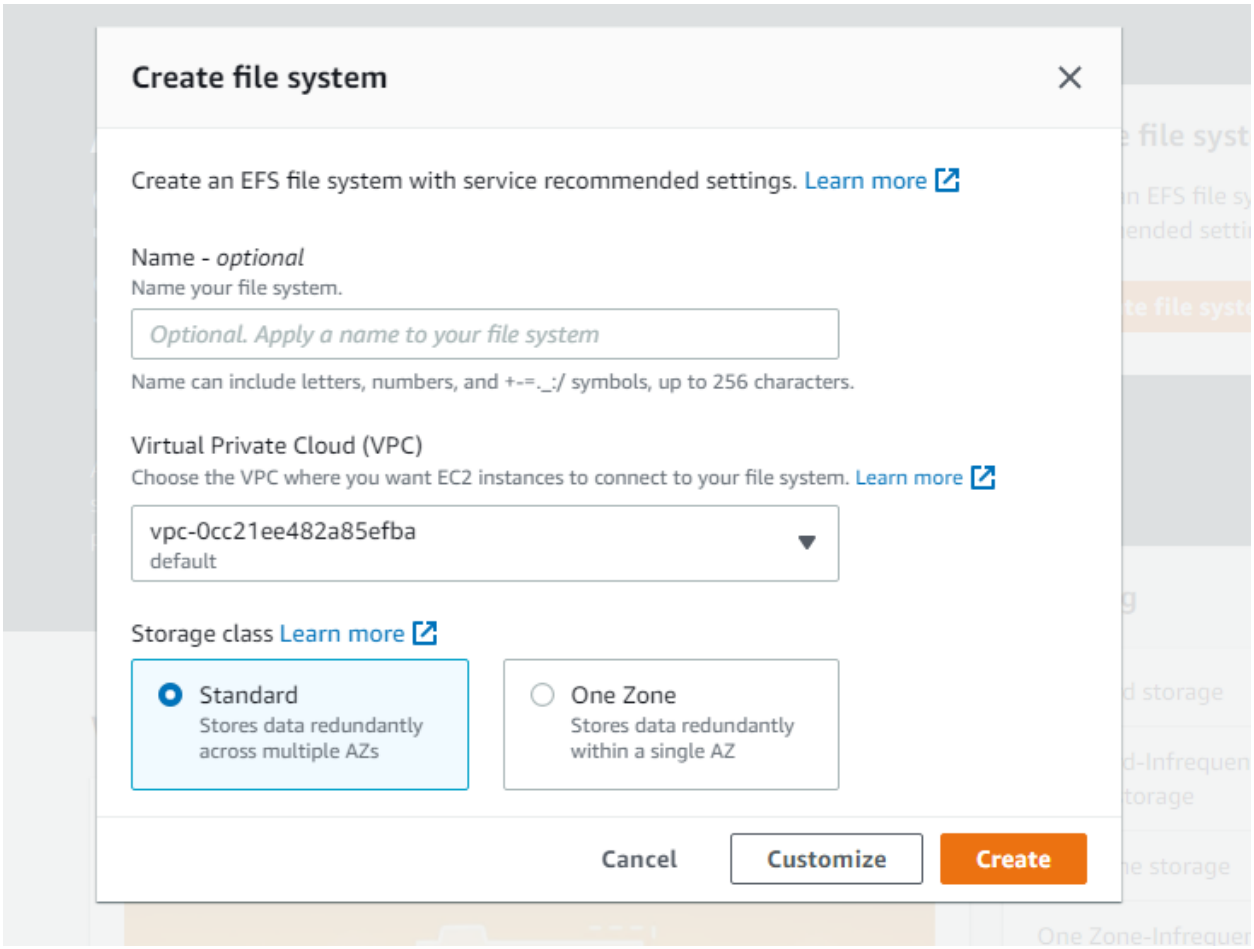
Create an EFS file system with service recommended settings.

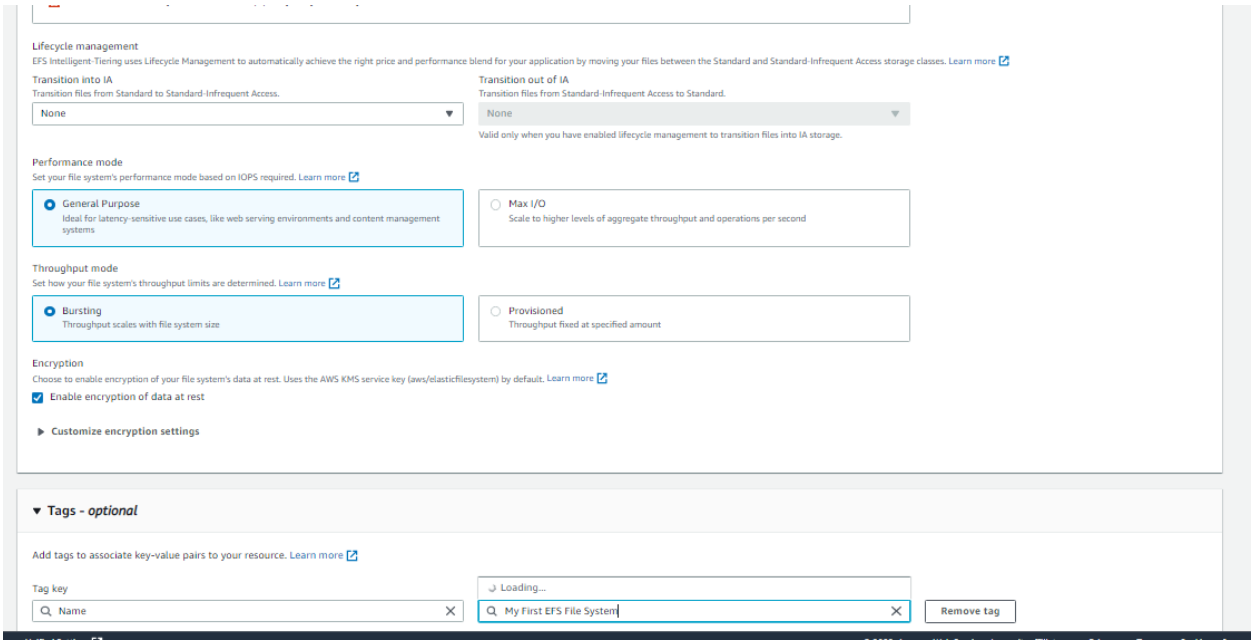
Create file system

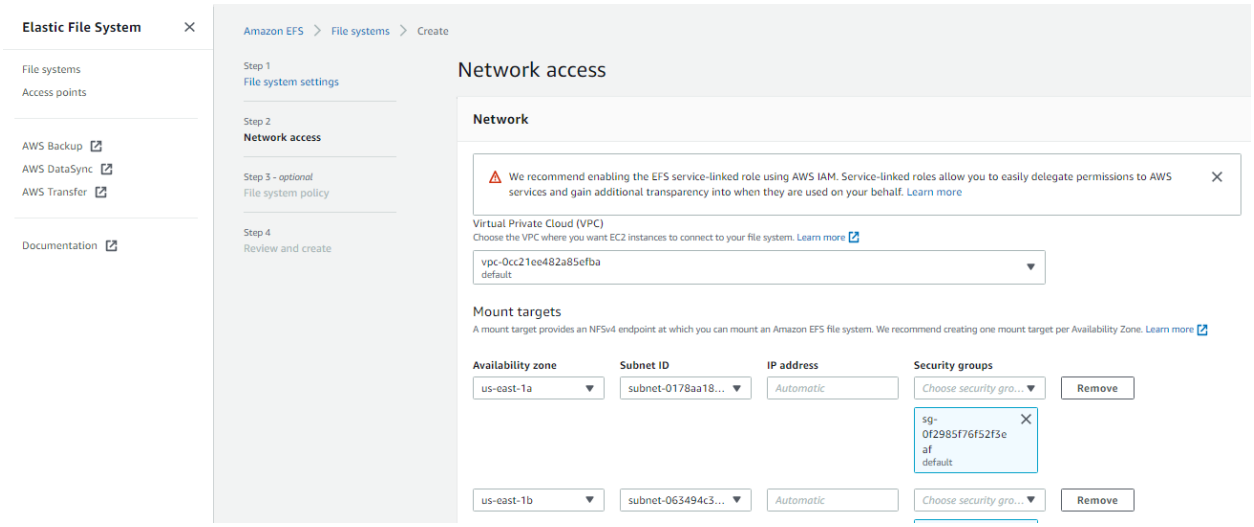
Pricing

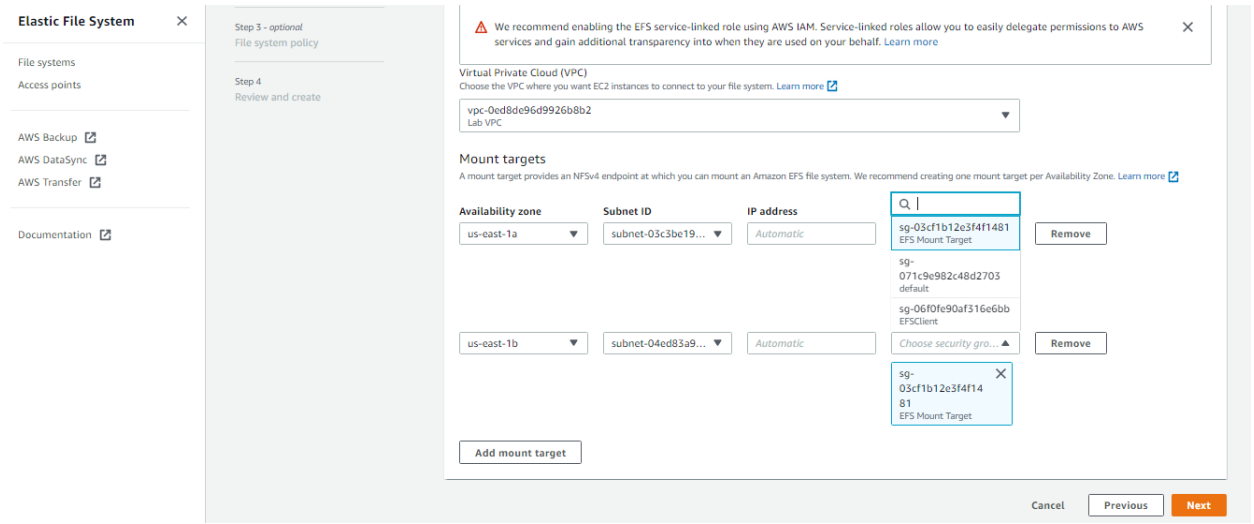
Standard storage	$0.30 per GB
Standard-Infrequent Access storage	$0.025 per GB
One Zone storage	$0.160 per GB

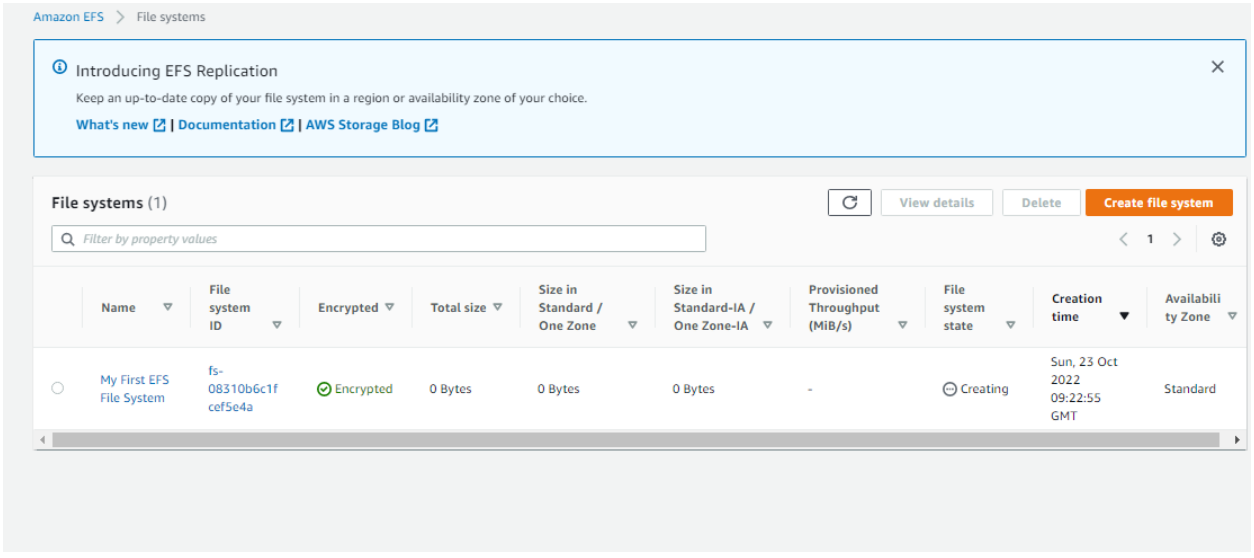
What is Amazon Elastic File System?

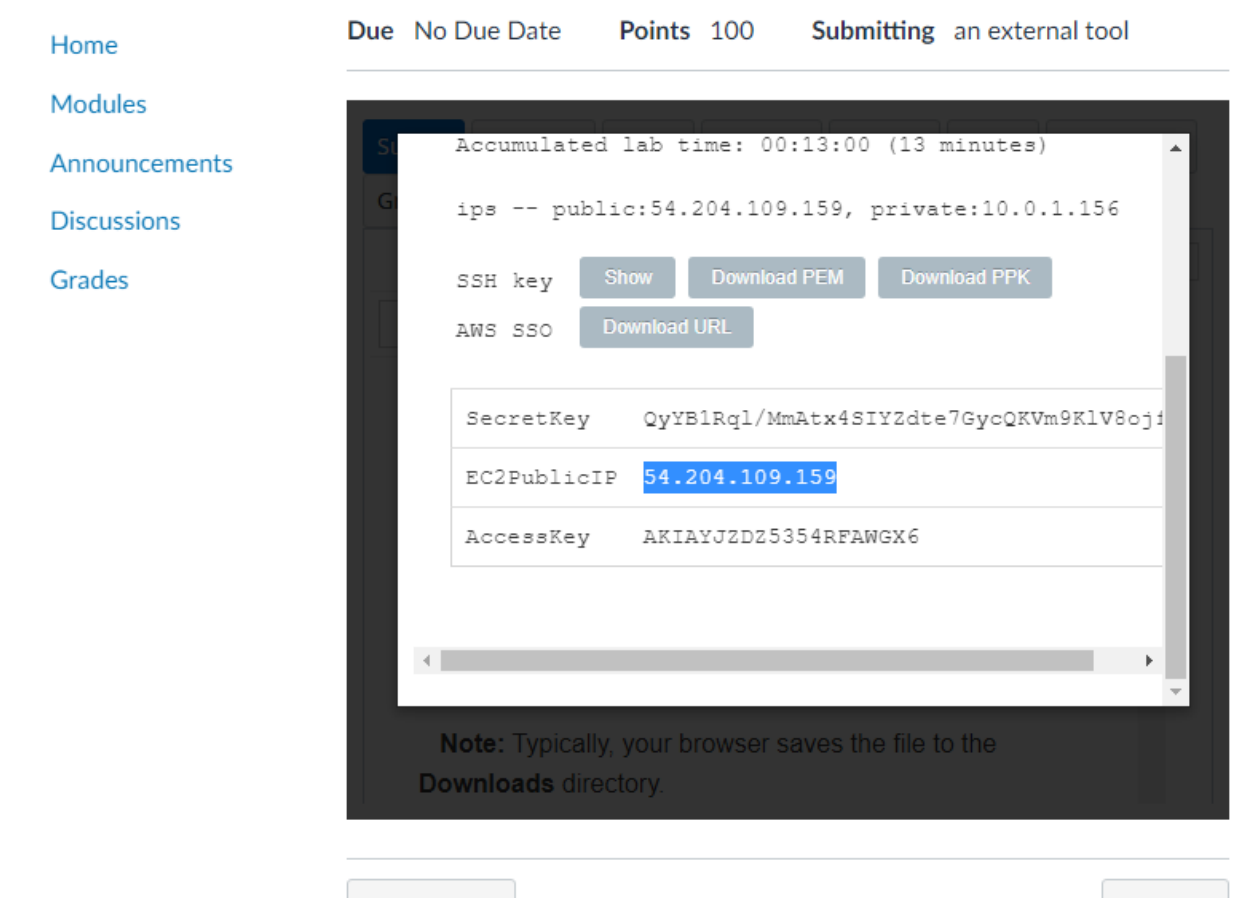

Create file system
Create an EFS file system with service recommended settings. Learn more
Name - optional
Name your file system.
Optional. Apply a name to your file system
Name can include letters, numbers, and +-=._:/ symbols, up to 256 characters.
Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. Learn more
vpc-0cc21ee482a85efba
default
Storage class Learn more
Standard
Stores data redundantly across multiple AZs
One Zone
Stores data redundantly within a single AZ
Cancel
Customize
Create


Lifecycle management
EFS Intelligent-Tiering uses Lifecycle Management to automatically achieve the right price and performance blend for your application by moving your files between the Standard and Standard-Infrequent Access storage classes. Learn more
Transition into IA
Transition files from Standard to Standard-Infrequent Access.
None
Transition out of IA
Transition files from Standard-Infrequent Access to Standard.
None
Valid only when you have enabled lifecycle management to transition files into IA storage.
Performance mode
Set your file system's performance mode based on IOPS required. Learn more
General Purpose
Ideal for latency-sensitive use cases, like web serving environments and content management systems
Max I/O
Scale to higher levels of aggregate throughput and operations per second
Throughput mode
Set how your file system's throughput limits are determined. Learn more
Bursting
Throughput scales with file system size
Provisioned
Throughput fixed at specified amount
Encryption
Choose to enable encryption of your file system's data at rest. Uses the AWS KMS service key (aws/elasticfilesystem) by default. Learn more
Enable encryption of data at rest
Customize encryption settings
Tags - optional
Add tags to associate key-value pairs to your resource. Learn more
Tag key
Name
Loading...
My First EFS File System
Remove tag

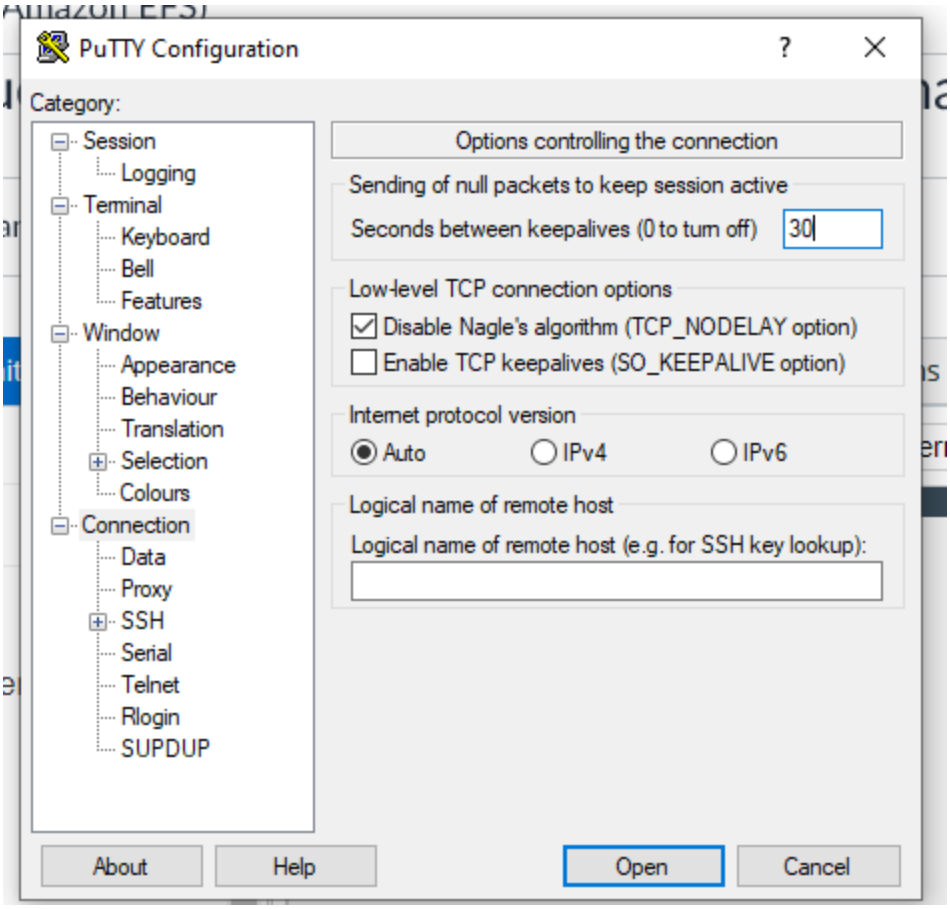

Elastic File System
File systems
Access points
AWS Backup
AWS DataSync
AWS Transfer
Documentation
Amazon EFS > File systems > Create
Step 1
File system settings
Step 2
Network access
Step 3 - optional
File system policy
Step 4
Review and create
Network access
Network
We recommend enabling the EFS service-linked role using AWS IAM. Service-linked roles allow you to easily delegate permissions to AWS services and gain additional transparency into when they are used on your behalf. Learn more
Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. Learn more
vpc-0cc21ee482a85efba
default
Mount targets
A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. Learn more
Availability zone
Subnet ID
IP address
Security groups
us-east-1a
subnet-0178aa18...
Automatic
Choose security gro...
Remove
sg-0f2985f76f52f3eaf
default
us-east-1b
subnet-063494c3...
Automatic
Choose security gro...
Remove

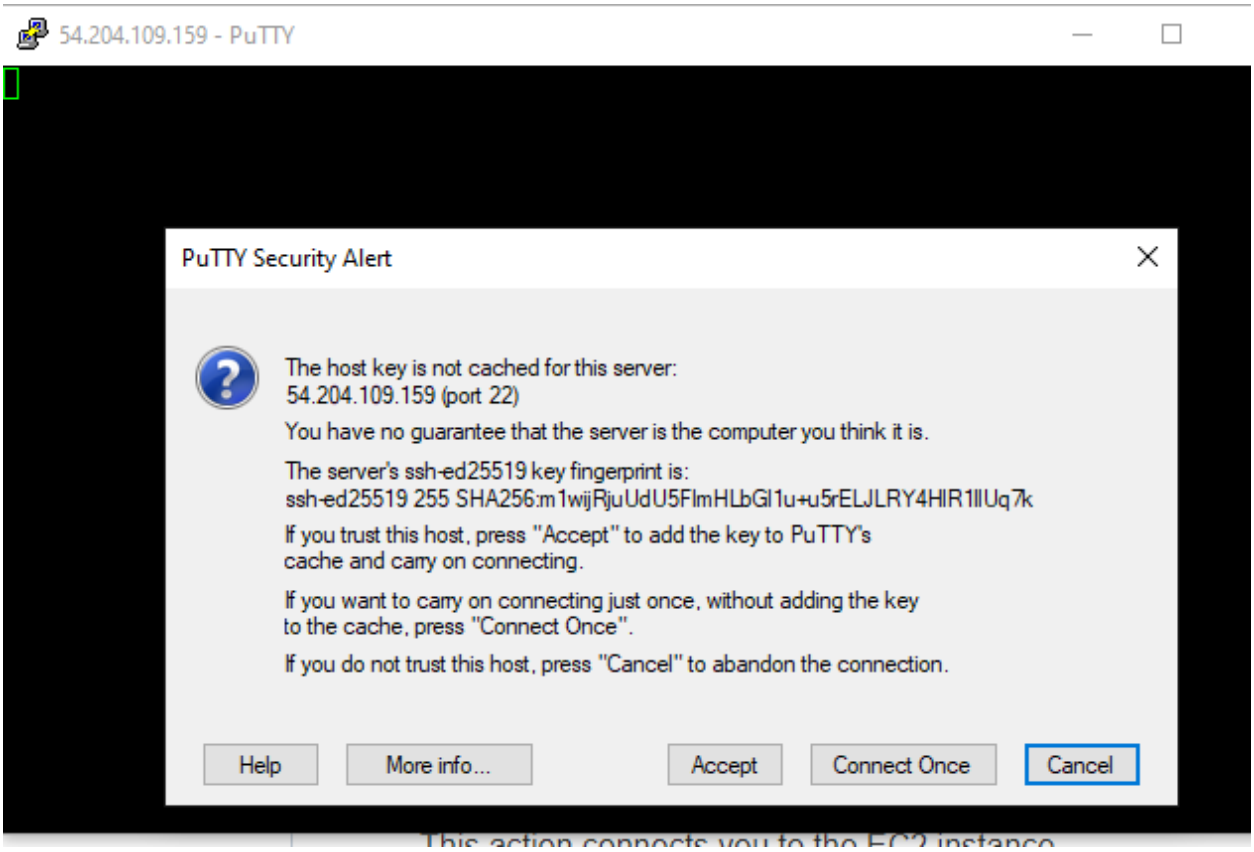

Elastic File System
File systems
Access points
AWS Backup
AWS DataSync
AWS Transfer
Documentation
Step 3 - optional
File system policy
Step 4
Review and create
We recommend enabling the EFS service-linked role using AWS IAM. Service-linked roles allow you to easily delegate permissions to AWS services and gain additional transparency into when they are used on your behalf. Learn more
Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. Learn more
vpc-0ed8de96d9926b8b2
Lab VPC
Mount targets
A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. Learn more
Availability zone
Subnet ID
IP address
us-east-1a
subnet-03c3be19...
Automatic
sg-03cf1b12e3f4f1481
EFS Mount Target
sg-071c9e982c48d2703
default
sg-06f0fe90af316e6bb
EFSClient
Remove
us-east-1b
subnet-04ed83a9...
Automatic
Choose security gro...
Remove
sg-03cf1b12e3f4f14 81
EFS Mount Target
Add mount target
Cancel
Previous
Next

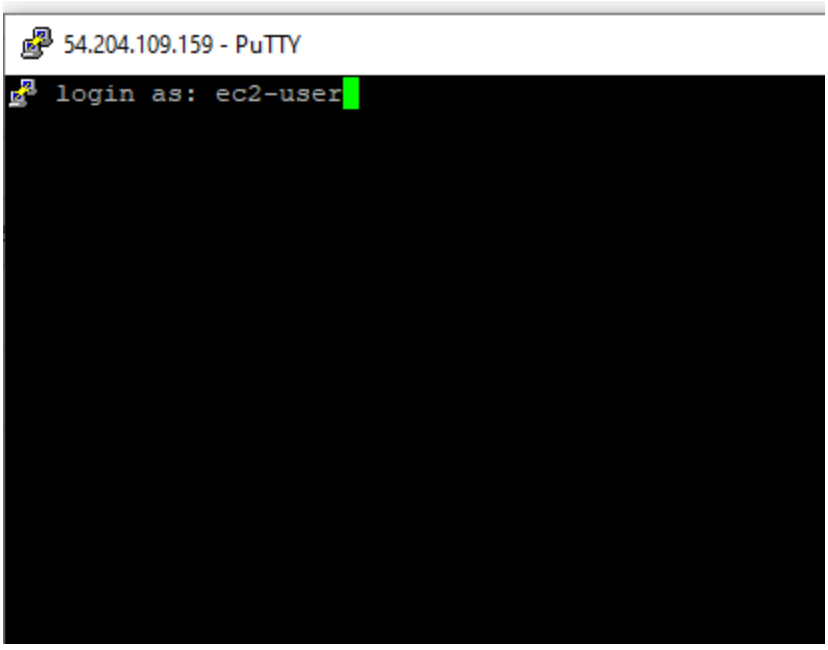

Amazon EFS > File systems
Introducing EFS Replication
Keep an up-to-date copy of your file system in a region or availability zone of your choice.
What's new | Documentation | AWS Storage Blog
File systems (1)
View details
Delete
Create file system
Filter by property values
1
Name
File system ID
Encrypted
Total size
Size in Standard / One Zone
Size in Standard-IA / One Zone-IA
Provisioned Throughput (MiB/s)
File system state
Creation time
Availability Zone
My First EFS File System
fs-08310b6c1fcef5e4a
Encrypted
0 Bytes
0 Bytes
0 Bytes
-
Creating
Sun, 23 Oct 2022 09:22:55 GMT
Standard

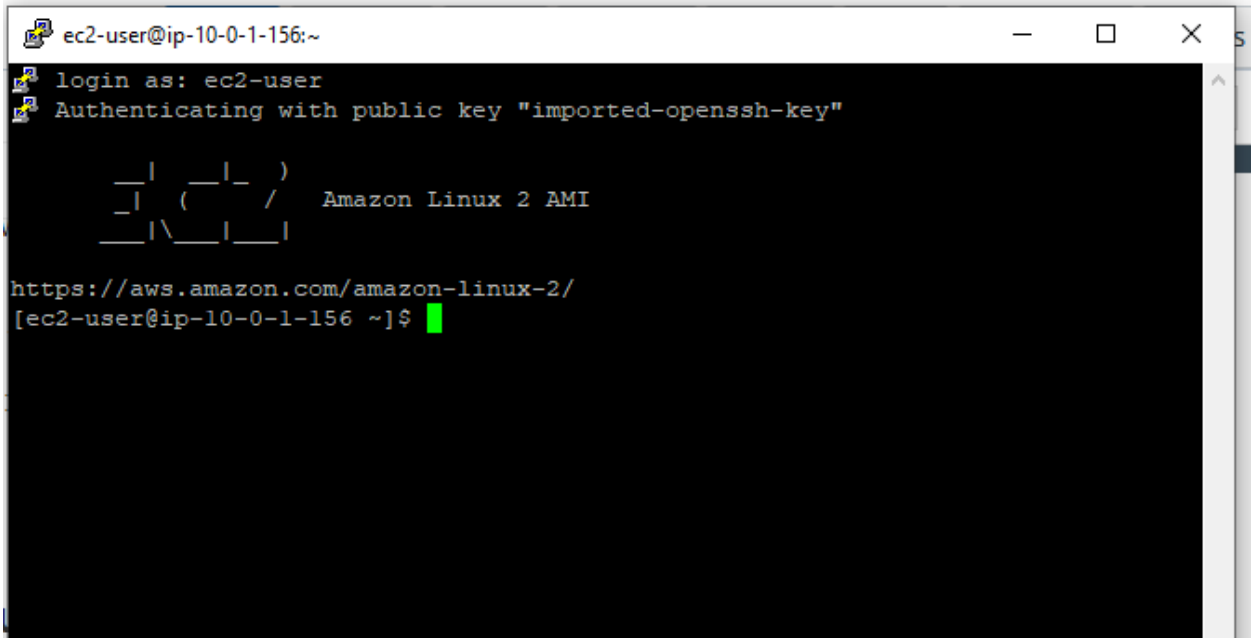


EC3 Public IP and download PPK

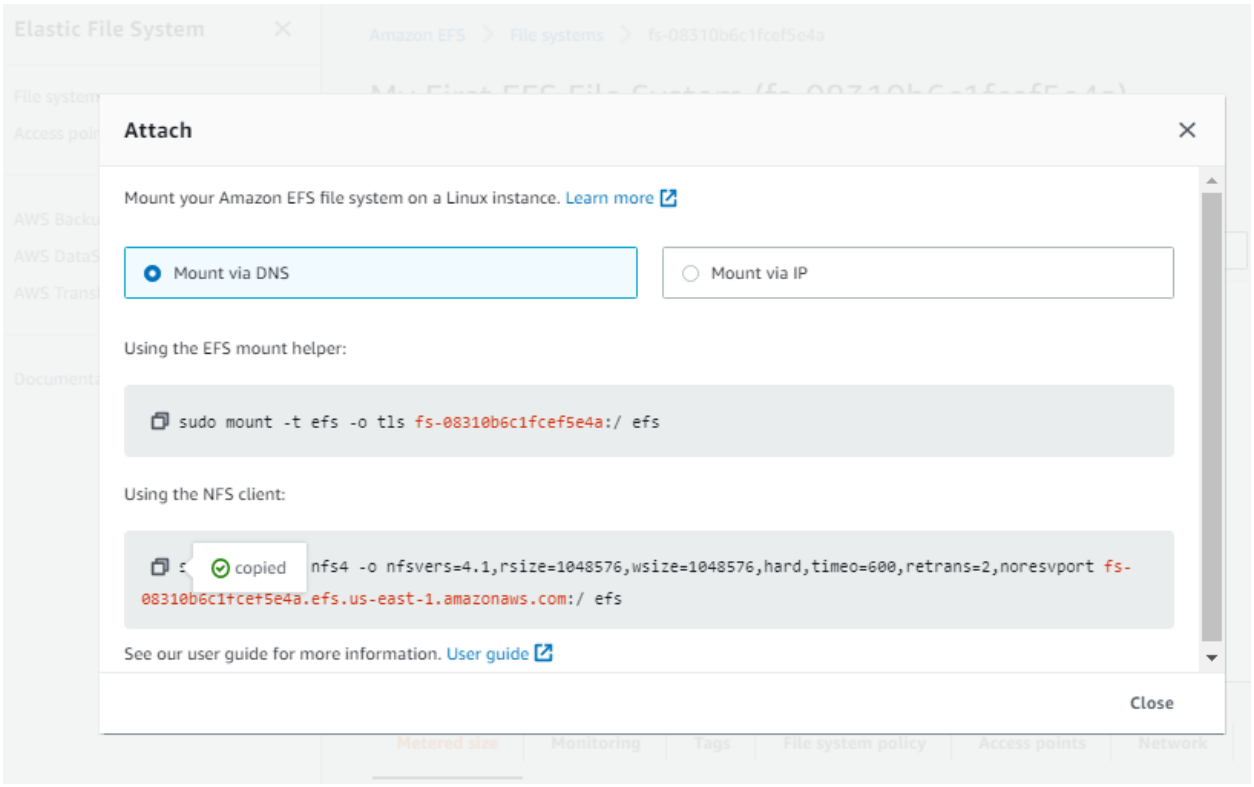

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Options controlling the connection
Sending of null packets to keep session active
Seconds between keepalives (0 to turn off)
30
Low-level TCP connection options
Disable Nagle's algorithm (TCP_NODELAY option)
Enable TCP keepalives (SO_KEEPALIVE option)
Internet protocol version
Auto
IPv4
IPv6
Logical name of remote host
Logical name of remote host (e.g. for SSH key lookup):
About
Help
Open
Cancel

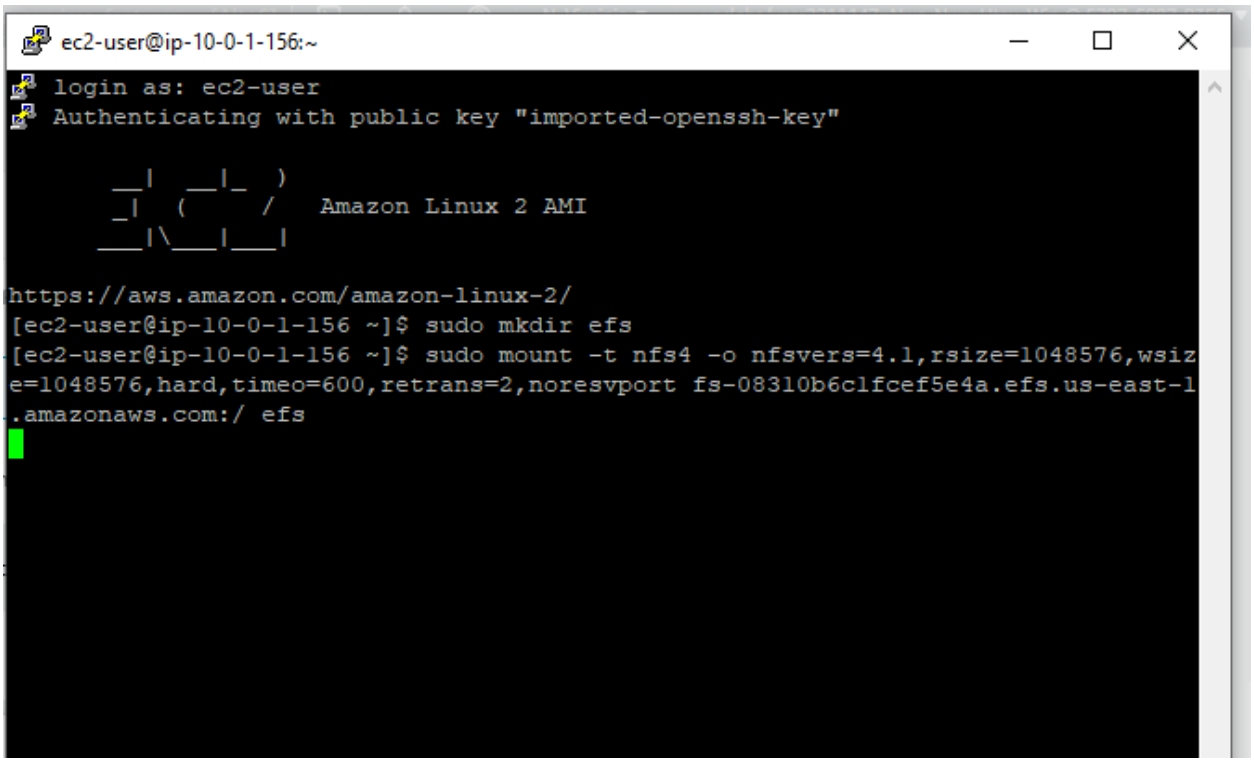

54.204.109.159 - PuTTY
PuTTY Security Alert
The host key is not cached for this server:
54.204.109.159 (port 22)
You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:m1wijRjuUdU5FlmHLbGl1u+u5rELJLRY4HIR1llUq7k
If you trust this host, press "Accept" to add the key to PuTTY's
cache and carry on connecting.
If you want to carry on connecting just once, without adding the key
to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
Help
More info...
Accept
Connect Once
Cancel

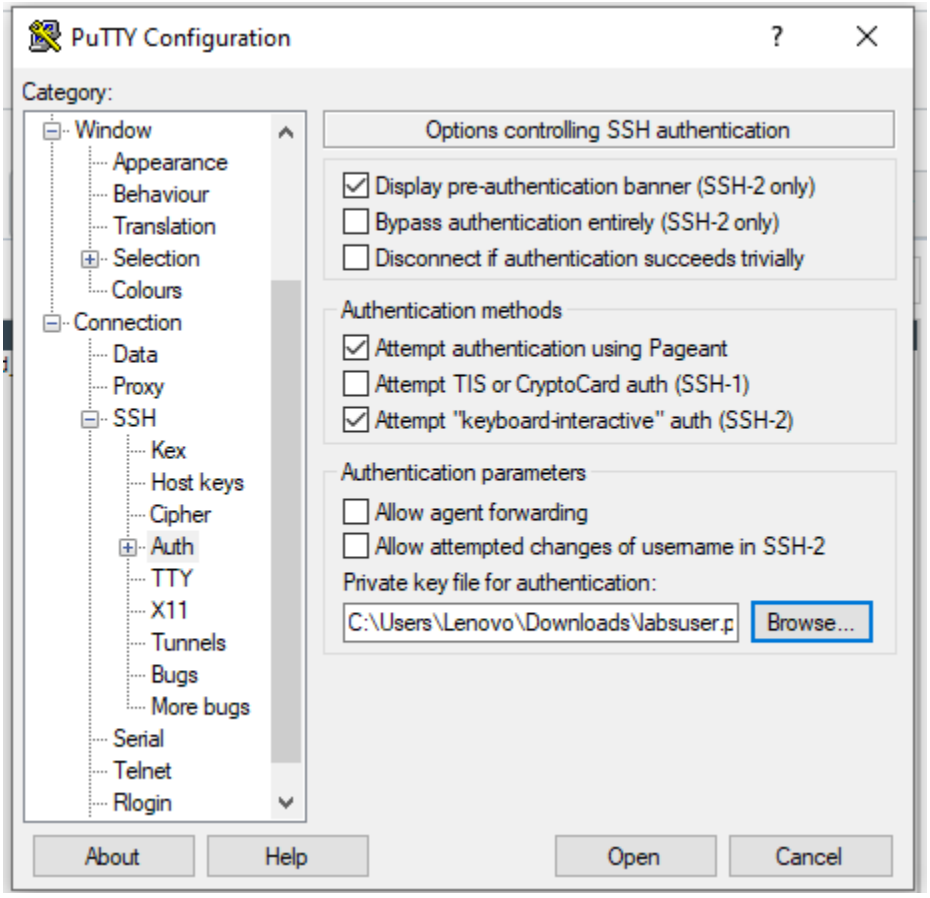

54.204.109.159 - PuTTY
login as: ec2-user

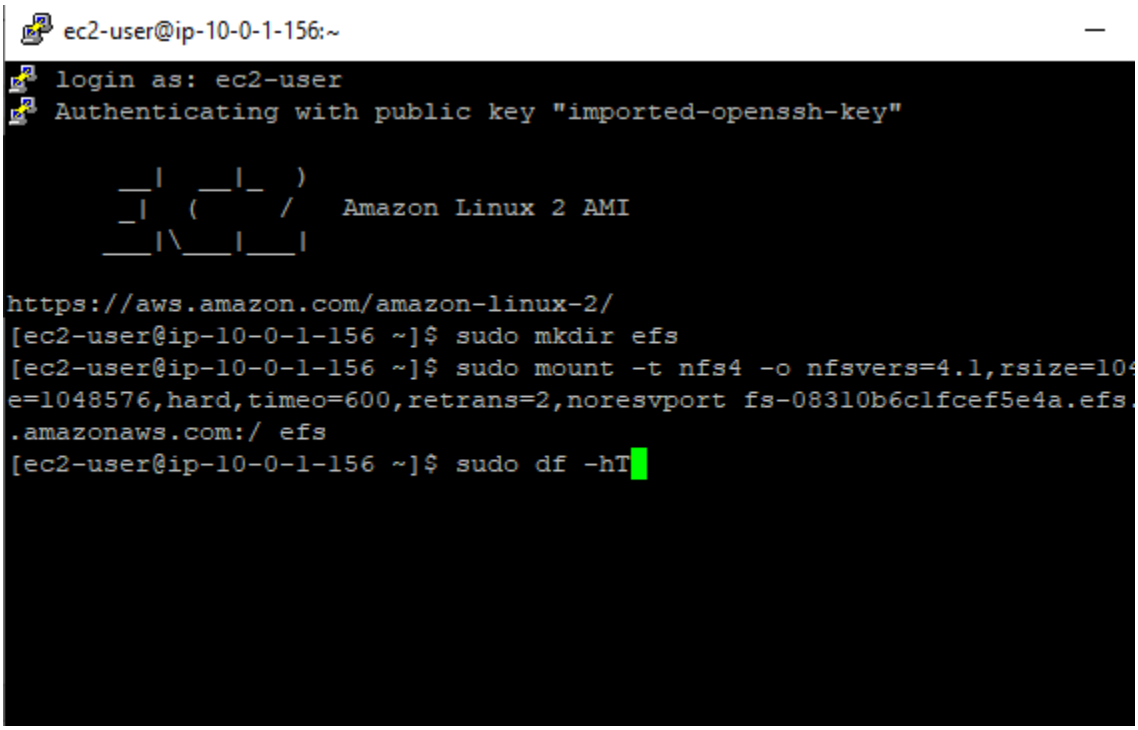

ec2-user@ip-10-0-1-156:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/   Amazon Linux 2 AMI
___|___|___|
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-156 ~]$

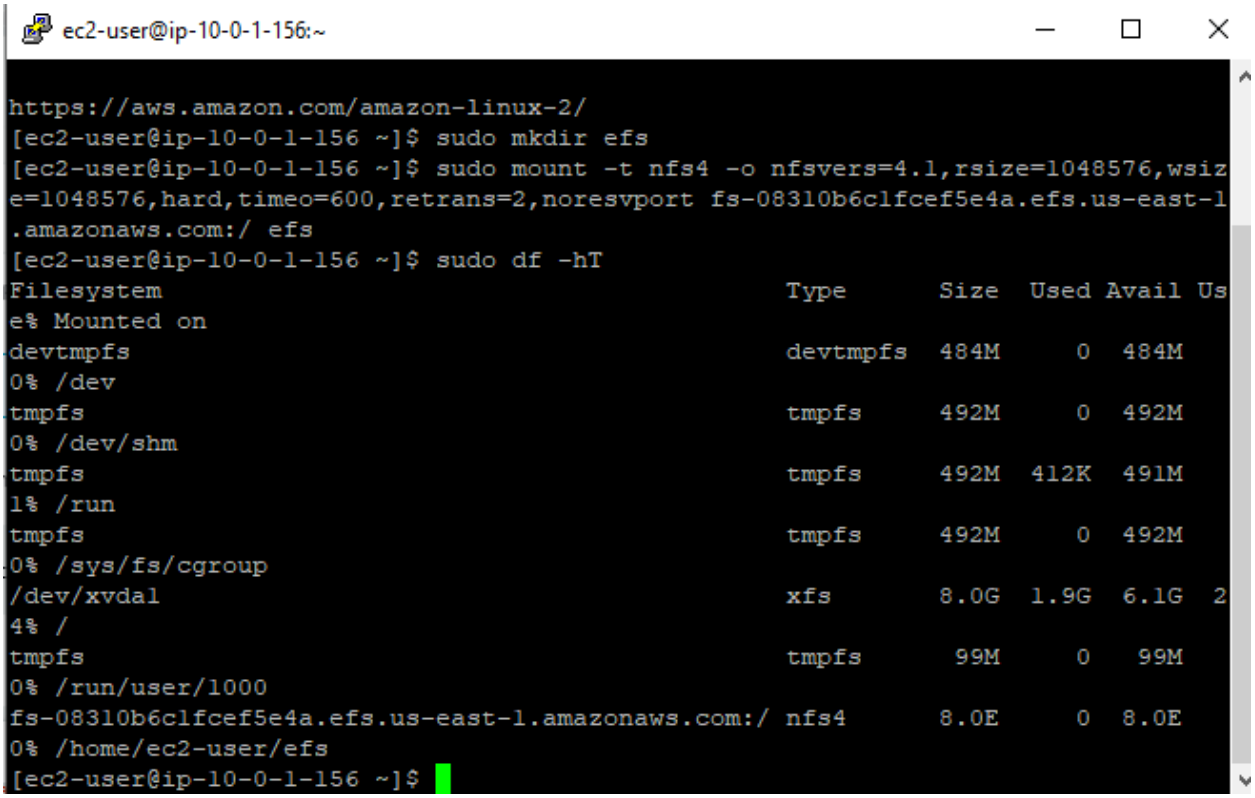
ec2-user@ip-10-0-1-156:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/   Amazon Linux 2 AMI
___|___|___|
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-156 ~]$ sudo mkdir efs
[ec2-user@ip-10-0-1-156 ~]$

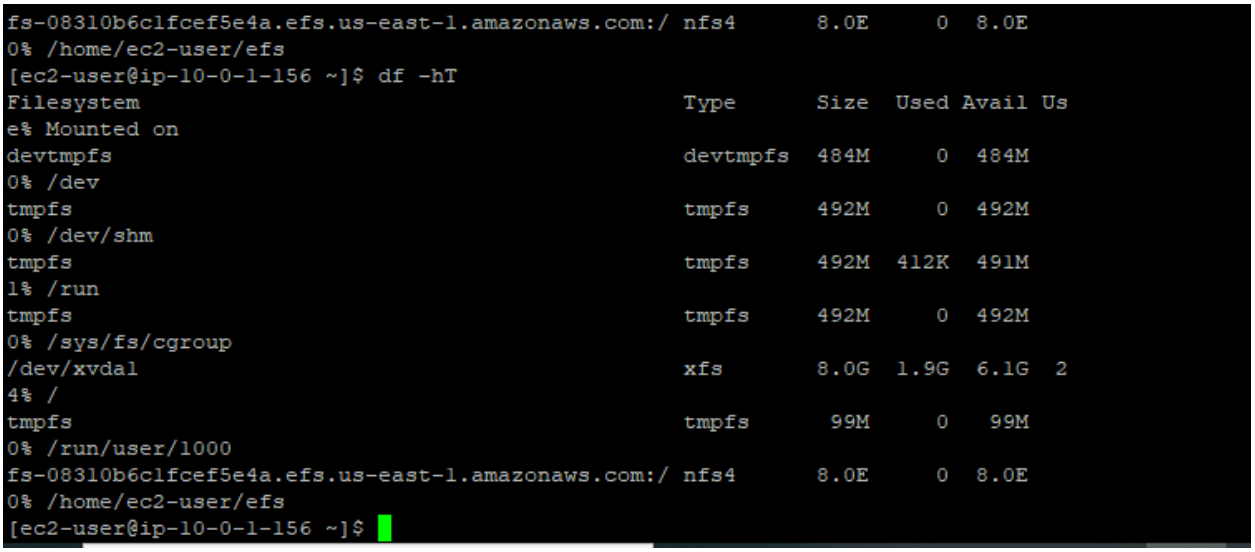

Elastic File System
Attach
Mount your Amazon EFS file system on a Linux instance. Learn more
Mount via DNS
Mount via IP
Using the EFS mount helper:
sudo mount -t efs -o tls fs-08310b6c1fcef5e4a:/ efs
Using the NFS client:
copied
nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-08310b6c1fcef5e4a.efs.us-east-1.amazonaws.com:/ efs
See our user guide for more information. User guide
Close


ec2-user@ip-10-0-1-156:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-156 ~]$ sudo mkdir efs
[ec2-user@ip-10-0-1-156 ~]$ sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsiz
e=1048576,hard,timeo=600,retrans=2,noresvport fs-08310b6c1fcef5e4a.efs.us-east-1
.amazonaws.com:/ efs

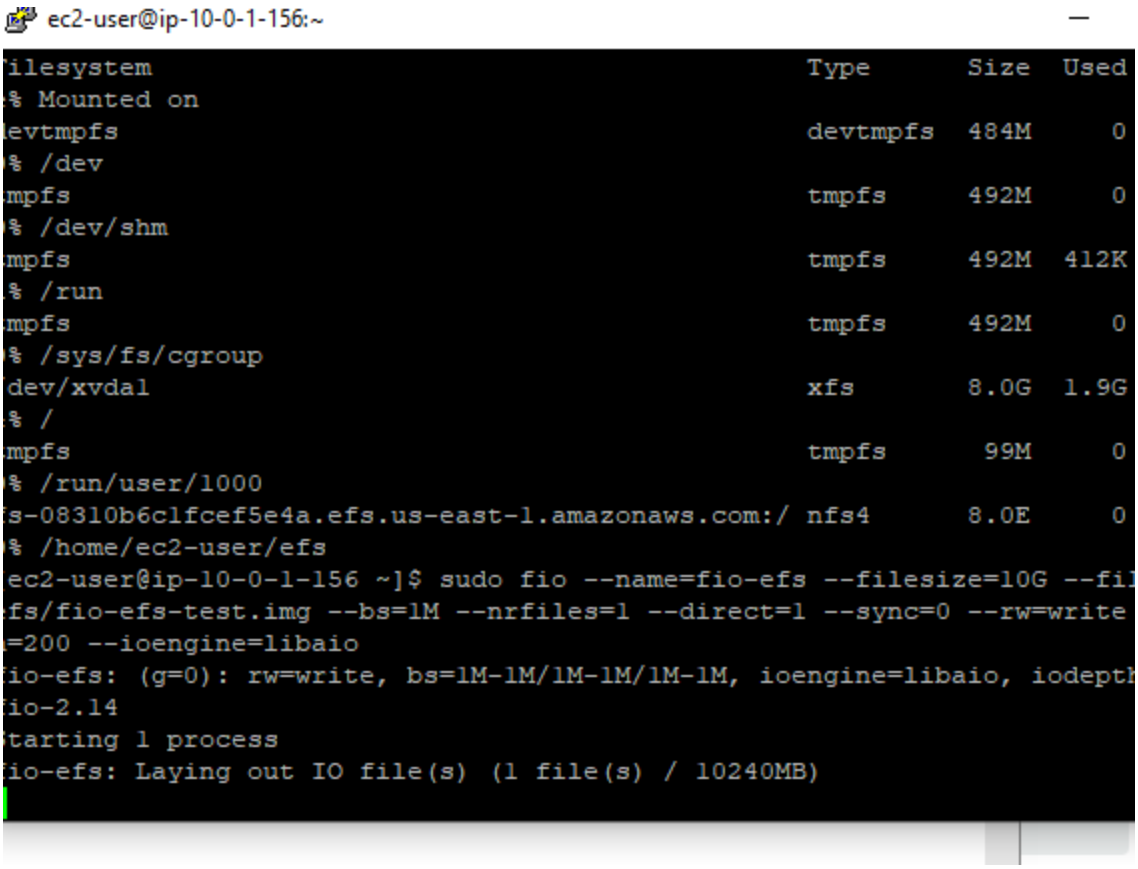

PuTTY Configuration
Category:
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Kex
Host keys
Cipher
Auth
TTY
X11
Tunnels
Bugs
More bugs
Serial
Telnet
Rlogin
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Disconnect if authentication succeeds trivially
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\Users\Lenovo\Downloads\labsuser.p
Browse...
About
Help
Open
Cancel

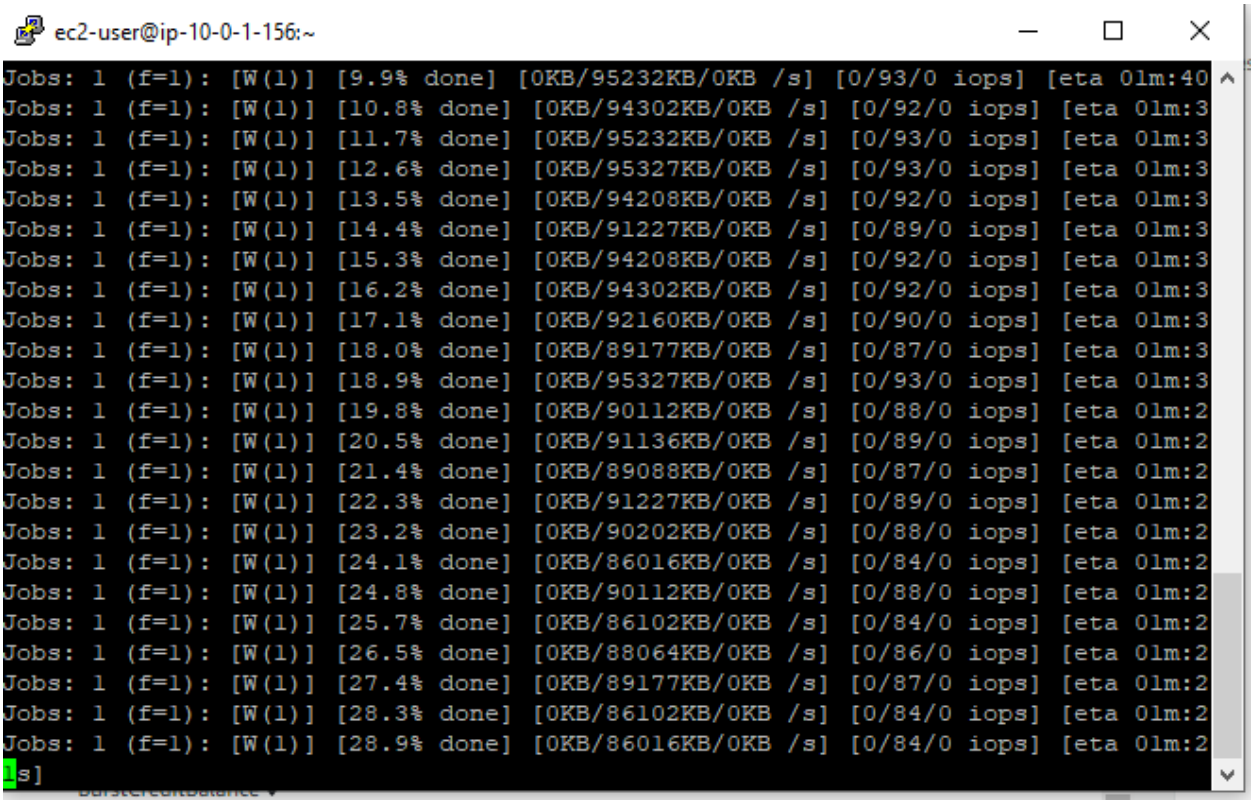

ec2-user@ip-10-0-1-156:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-156 ~]$ sudo mkdir efs
[ec2-user@ip-10-0-1-156 ~]$ sudo mount -t nfs4 -o nfsvers=4.1,rsize=10
e=1048576,hard,timeo=600,retrans=2,noresvport fs-08310b6c1fcef5e4a.efs.
.amazonaws.com:/ efs
[ec2-user@ip-10-0-1-156 ~]$ sudo df -hT

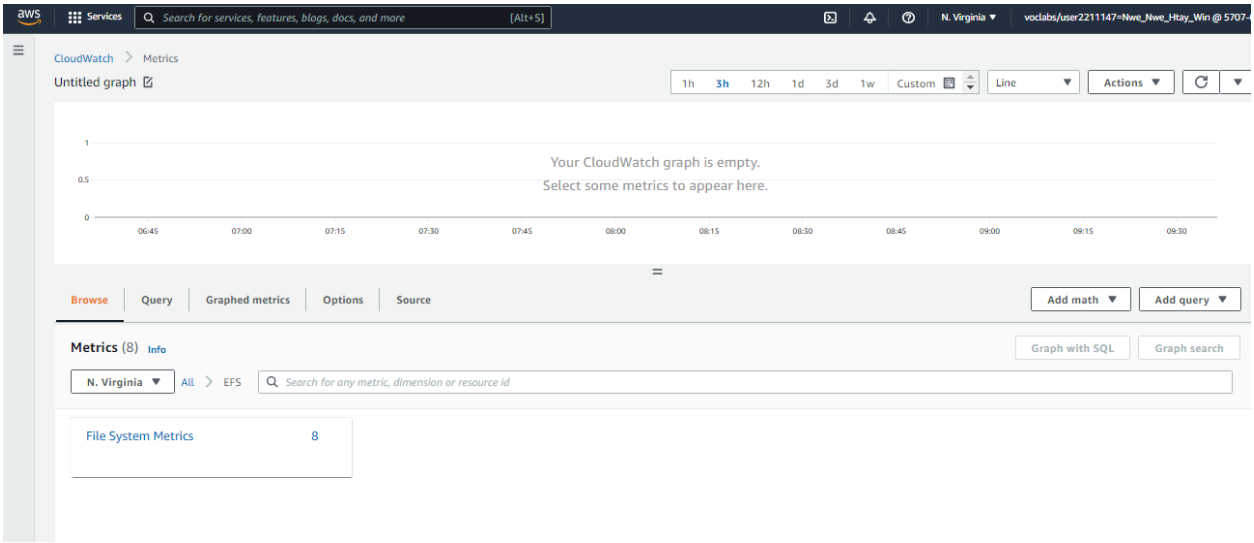


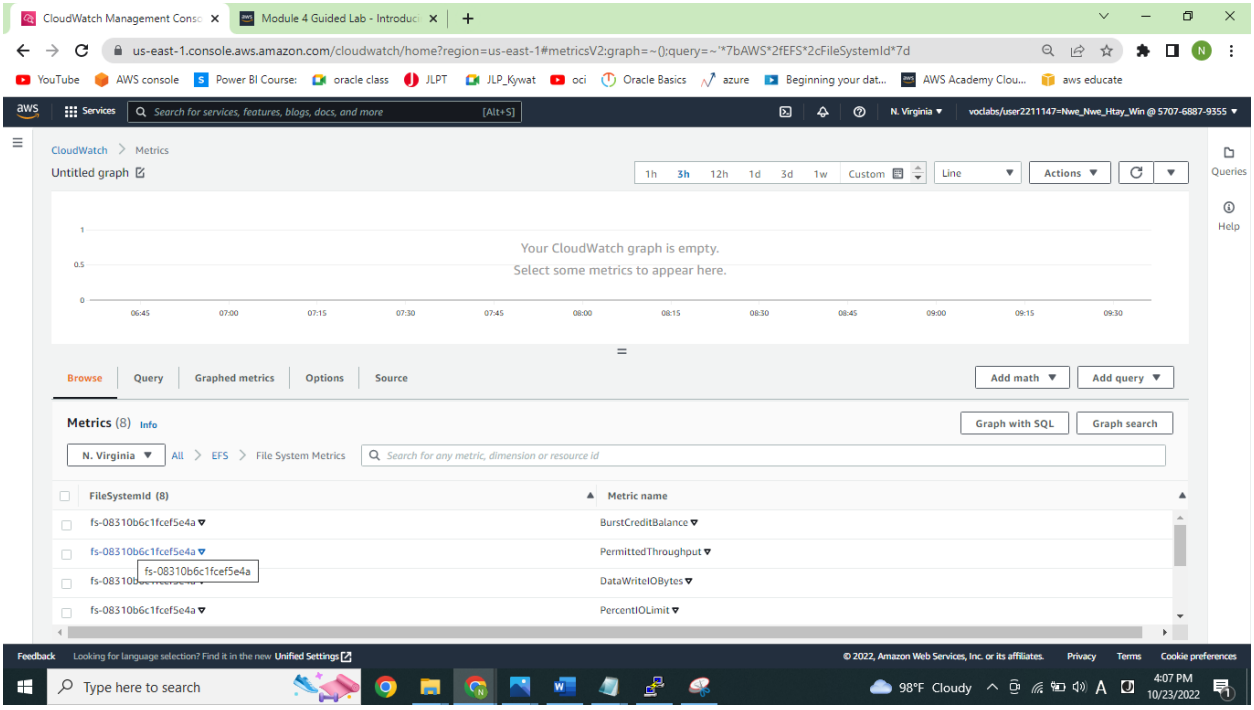



```
sudo fio --name=fio-efs --filesize=10G --filename=./efs/fio-efs-test.img --bs=1M --nrfiles=1 --direct=1 --sync=0 --rw=write --iodepth=200 --ioengine=libaio
```

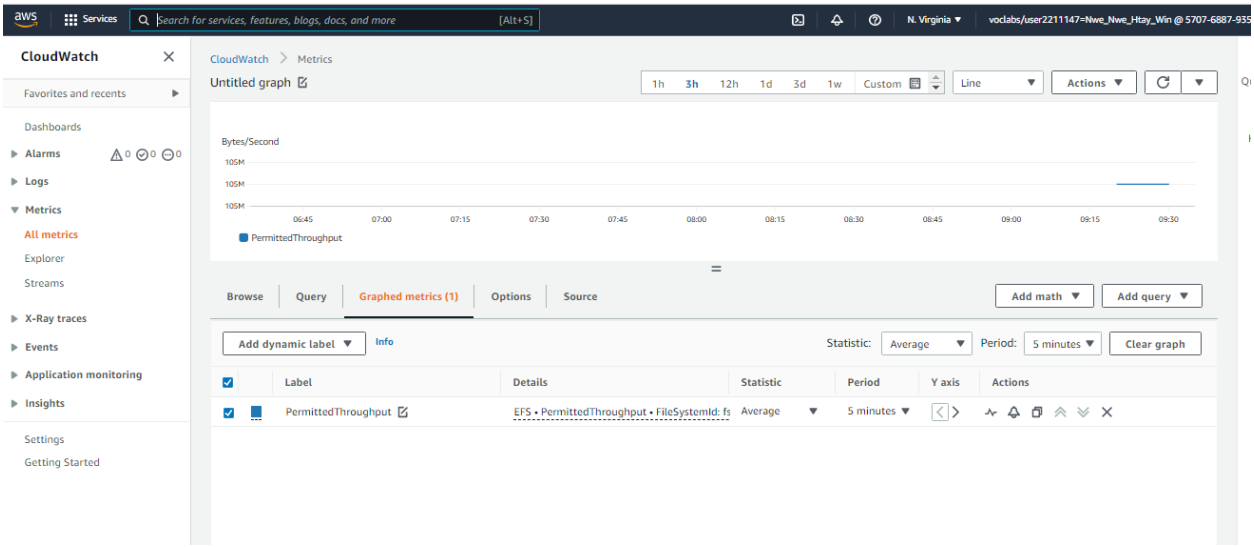

ec2-user@ip-10-0-1-156:~
ilesystem Type Size Used
% Mounted on
evtmpfs devtmpfs 484M 0
% /dev
mpfs tmpfs 492M 0
% /dev/shm
mpfs tmpfs 492M 412K
% /run
mpfs tmpfs 492M 0
% /sys/fs/cgroup
dev/xvda1 xfs 8.0G 1.9G
% /
mpfs tmpfs 99M 0
% /run/user/1000
s-08310b6c1fcef5e4a.efs.us-east-1.amazonaws.com:/ nfs4 8.0E 0
% /home/ec2-user/efs
ec2-user@ip-10-0-1-156 ~]$ sudo fio --name=fio-efs --filesize=10G --fi
fs/fio-efs-test.img --bs=1M --nrfiles=1 --direct=1 --sync=0 --rw=write
=200 --ioengine=libaio
io-efs: (g=0): rw=write, bs=1M-1M/1M-1M/1M-1M, ioengine=libaio, iodept
io-2.14
tarting 1 process
io-efs: Laying out IO file(s) (1 file(s) / 10240MB)


ec2-user@ip-10-0-1-156:~
Jobs: 1 (f=1): [W(1)] [9.9% done] [0KB/95232KB/0KB /s] [0/93/0 iops] [eta 01m:40
Jobs: 1 (f=1): [W(1)] [10.8% done] [0KB/94302KB/0KB /s] [0/92/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [11.7% done] [0KB/95232KB/0KB /s] [0/93/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [12.6% done] [0KB/95327KB/0KB /s] [0/93/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [13.5% done] [0KB/94208KB/0KB /s] [0/92/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [14.4% done] [0KB/91227KB/0KB /s] [0/89/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [15.3% done] [0KB/94208KB/0KB /s] [0/92/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [16.2% done] [0KB/94302KB/0KB /s] [0/92/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [17.1% done] [0KB/92160KB/0KB /s] [0/90/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [18.0% done] [0KB/89177KB/0KB /s] [0/87/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [18.9% done] [0KB/95327KB/0KB /s] [0/93/0 iops] [eta 01m:3
Jobs: 1 (f=1): [W(1)] [19.8% done] [0KB/90112KB/0KB /s] [0/88/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [20.5% done] [0KB/91136KB/0KB /s] [0/89/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [21.4% done] [0KB/89088KB/0KB /s] [0/87/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [22.3% done] [0KB/91227KB/0KB /s] [0/89/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [23.2% done] [0KB/90202KB/0KB /s] [0/88/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [24.1% done] [0KB/86016KB/0KB /s] [0/84/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [24.8% done] [0KB/90112KB/0KB /s] [0/88/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [25.7% done] [0KB/86102KB/0KB /s] [0/84/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [26.5% done] [0KB/88064KB/0KB /s] [0/86/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [27.4% done] [0KB/89177KB/0KB /s] [0/87/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [28.3% done] [0KB/86102KB/0KB /s] [0/84/0 iops] [eta 01m:2
Jobs: 1 (f=1): [W(1)] [28.9% done] [0KB/86016KB/0KB /s] [0/84/0 iops] [eta 01m:2
ls]

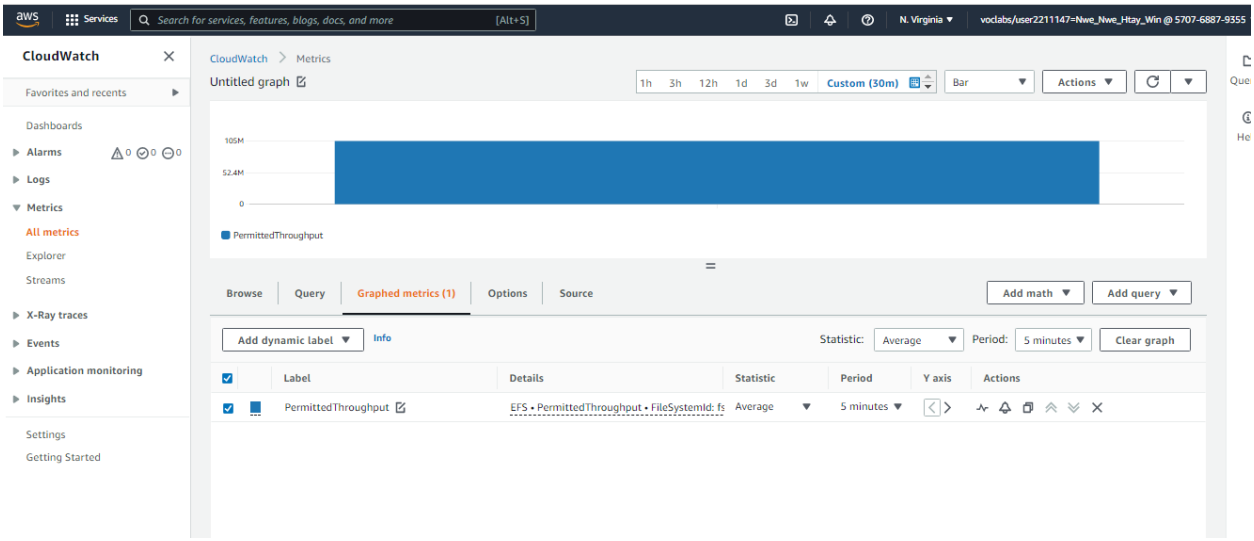




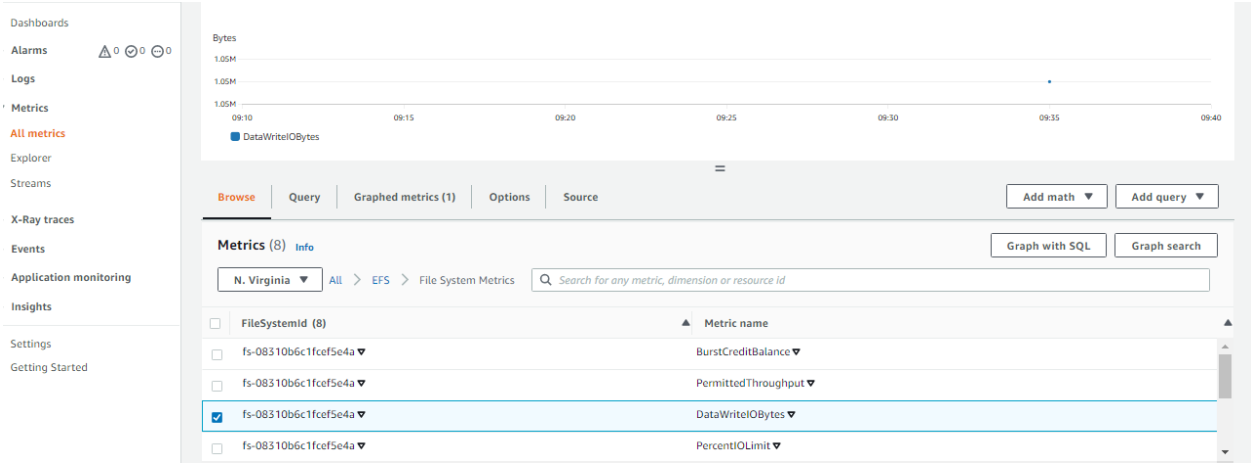
Chooose permitted throughput and refresh the browser from time to time

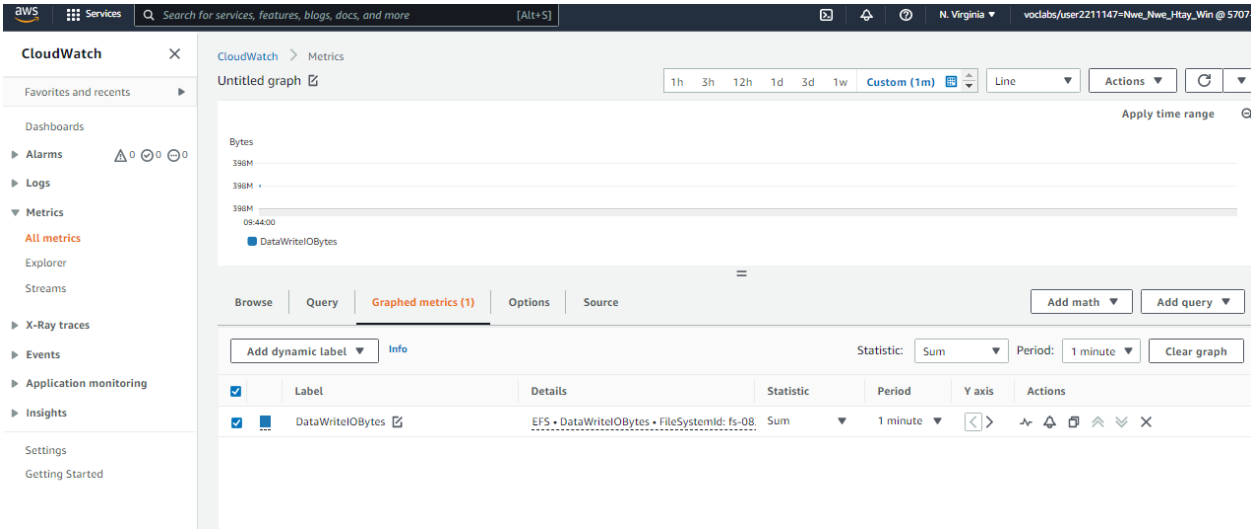


Change the chart type and time period



Scroll around the line and it will show the throughput





Module 4 - Guided Lab: Introducing Amazon Elastic File System (Amazon EFS)

Lab overview and objectives

This lab introduces you to Amazon Elastic File System (Amazon EFS) by using the AWS Management Console.

After completing this lab, you should be able to:

- Log in to the AWS Management Console
- Create an Amazon EFS file system
- Log in to an Amazon Elastic Compute Cloud (Amazon EC2) instance that runs Amazon Linux
- Mount your file system to your EC2 instance
- Examine and monitor the performance of your file system

Duration

This lab requires approximately **20 minutes** to complete.

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch your lab.

   A **Start Lab** panel opens, and it displays the lab status.

   Tip: If you need more time to complete the lab, restart the timer for the environment by choosing the Start Lab button again.

2. Wait until the **Start Lab** panel displays the message *Lab status: ready*, then close the panel by choosing the **X**.
3. At the top of these instructions, choose AWS.

   This action opens the AWS Management Console in a new browser tab. The system automatically logs you in.

   Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with the message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and then choose **Allow pop-ups**.

4. Arrange the **AWS Management Console** tab so that it displays alongside these instructions. Ideally, you will have both browser tabs open at the same time so that you can follow the lab steps more easily.

   Do not change the Region unless specifically instructed to do so.

Task 1: Creating a security group to access your EFS file system

The security group that you associate with a mount target *must allow inbound access for TCP on port 2049 for Network File System (NFS)*. This is the security group that you will now create, configure, and attach to your EFS mount targets.

5. In the **AWS Management Console**, on the **Services** menu, choose **EC2**.
6. In the navigation pane on the left, choose **Security Groups**.
7. Copy the **Security group ID** of the *EFSClient* security group to your text editor.

   The Group ID should look similar to *sg-03727965651b6659b*.

8. Choose **Create security group** then configure:
   - **Security group name:** `EFS Mount Target`
   - **Description:** `Inbound NFS access from EFS clients`
   - **VPC:** *Lab VPC*
9. Under the **Inbound rules** section, choose **Add rule** then configure:
   - **Type:** *NFS*
   - **Source:**
     - *Custom*
     - In the *Custom* box, paste the security group's **Security group ID** that you copied to your text editor
   - Choose **Create security group**.

Task 2: Creating an EFS file system

EFS file systems can be mounted to multiple EC2 instances that run in different Availability Zones in the same Region. These instances use *mount targets* that are created in each *Availability Zone* to mount the file system by using standard NFSv4.1 semantics. You can mount the file system on instances in only one virtual private cloud (VPC) at a time. Both the file system and the VPC must be in the same Region.

10. On the **Services** menu, choose **EFS**.
11. Choose **Create file system**
12. In the **Create file system** window, choose **Customize**
13. On **Step 1**:

- Uncheck Enable automatic backups.
- **Lifecycle management:** Select *None*
- In the **Tags** section, configure:
  - **Key:** `Name`
  - **Value:** `My First EFS File System`

14. Choose **Next**
15. For **VPC**, select *Lab VPC*.
16. Detach the default security group from each *Availability Zone* mount target by choosing the check box on each default security group.
17. Attach the **EFS Mount Target** security group to each *Availability Zone* mount target by:

- Selecting each **Security groups** check box.
- Choosing **EFS Mount Target**.

A mount target is created for each subnet.

Your mount targets should look like the following example. The diagram shows two mount targets in the **Lab VPC** that use the **EFS Mount Target** security group. In this lab, you should be using the Lab VPC.

18. Choose **Next**
19. On **Step 3**, choose **Next**
20. On **Step 4:**

- Review your configuration.
- Choose **Create**

Congratulations! You have created a new EFS file system in your Lab VPC and mount targets in each Lab VPC subnet. In a few seconds, the **File system state** of the file system will change to *Available*, followed by the mount targets 2–3 minutes later.

Proceed to the next step after the **Mount target state** for each mount target changes to *Available*. Choose the screen refresh button after 2–3 minutes to check its progress.

Note: You may need to scroll to the right in the **File systems** pane to find the **File system state**.

Task 3: Connecting to your EC2 instance via SSH

In this task, you will connect to your EC2 instance by using Secure Shell (SSH).

Microsoft Windows users

These instructions are specifically for Microsoft Windows users. If you are using macOS or Linux, skip to the next section.

21. Above these instructions that you are currently reading, choose the Details dropdown menu, and then select Show

    A **Credentials** window opens.

22. Choose the **Download PPK** button and save the **labsuser.ppk** file.

    Note: Typically, your browser saves the file to the **Downloads** directory.

23. Note the **EC2PublicIP** address, if it is displayed.
24. Exit the **Details** panel by choosing the **X**.
25. To use SSH to access the EC2 instance, you must use ***PuTTY***. If you do not have PuTTY installed on your computer, download PuTTY.
26. Open **putty.exe**.
27. To keep the PuTTY session open for a longer period of time, configure the PuTTY timeout:

- Choose **Connection**
- **Seconds between keepalives**: 30

28. Configure your PuTTY session by using the following settings.

- Choose **Session**
- **Host Name (or IP address):** Paste the **EC2PublicIP** for the instance you noted earlier
  - Alternatively, return to the Amazon EC2 console and choose **Instances**
  - Select the instance you want to connect to
  - In the *Description* tab, copy the **IPv4 Public IP** value
- Back in PuTTY, in the **Connection** list, expand **SSH**
- Choose **Auth** (but don't expand it)
- Choose **Browse**
- Browse to the *labsuser.ppk* file that you downloaded, select it, and choose **Open**

- Choose **Open** again

29. To trust and connect to the host, choose **Yes**.
30. When you are prompted with **login as**, enter: `ec2-user`

    This action connects you to the EC2 instance.

31. Microsoft Windows users: Choose this link to skip ahead to the next task.

macOS and Linux users

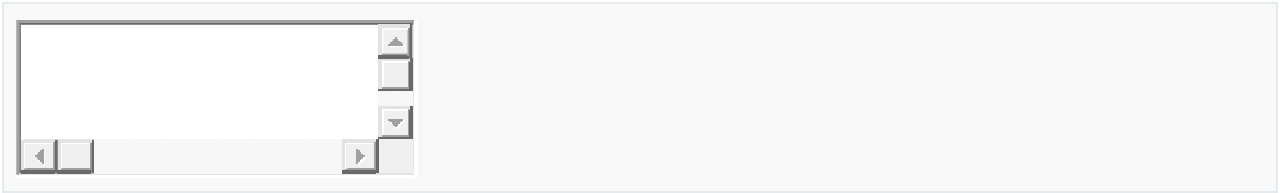
These instructions are specifically for macOS or Linux users. If you are a Windows user, skip ahead to the next task.

32. Above these instructions that you are currently reading, choose the Details dropdown menu, and then select Show

    A **Credentials** window opens.

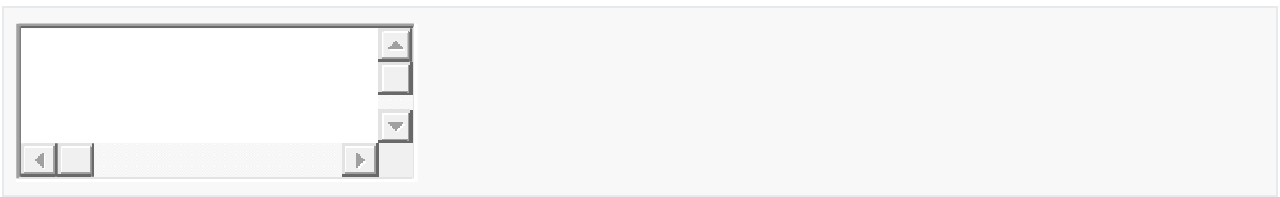
33. Choose the **Download PEM** button and save the **labsuser.pem** file.
34. Note the **EC2PublicIP** address, if it is displayed.
35. Exit the **Details** panel by choosing the **X**.
36. Open a terminal window, and change directory to the directory where the *labsuser.pem* file was downloaded by using the `cd` command.

    For example, if the *labsuser.pem* file was saved to your **Downloads** directory, run this command:



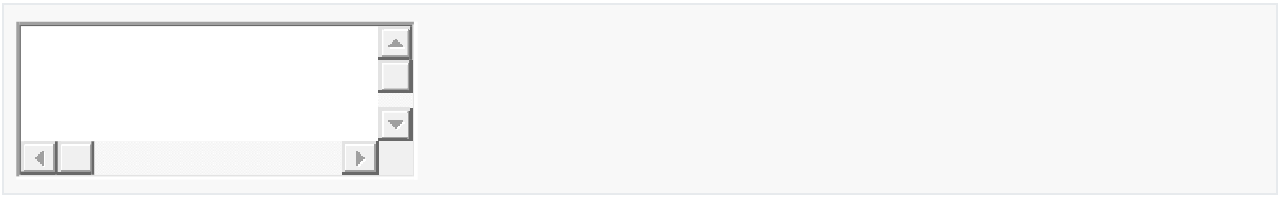
```
cd ~/Downloads
```

37. Change the permissions on the key to be read-only, by running this command:



```
chmod 400 labsuser.pem
```

38. Run the following command (replace **<public-ip>** with the **EC2PublicIP** address that you copied earlier).
    - Alternatively, to find the IP address of the on-premises instance, return to the Amazon EC2 console and select **Instances**
    - Select the instance that you want to connect to
    - In the **Description** tab, copy the **IPv4 Public IP** value



```
ssh -i labsuser.pem ec2-user@<public-ip>
```

39. When you are prompted to allow the first connection to this remote SSH server, enter `yes`.

    Because you are using a key pair for authentication, you are not prompted for a password.

Task 4: Creating a new directory and mounting the EFS file system

Amazon EFS supports the NFSv4.1 and NFSv4.0 protocols when it mounts your file systems on EC2 instances. Though NFSv4.0 is supported, we recommend that you use NFSv4.1. When you mount your EFS file system on your EC2 instance, you must also use an NFS client that supports your chosen NFSv4 protocol. The EC2 instance that was launched as a part of this lab includes an NFSv4.1 client, which is already installed on it.

40. In your SSH session, make a new directory by entering `sudo mkdir efs`
41. Back in the **AWS Management Console**, on the **Services** menu, choose **EFS**.
42. Choose **My First EFS File System**.
43. In the **Amazon EFS Console**, on the top right corner of the page, choose **Attach** to open the Amazon EC2 mount instructions.
44. Copy the entire command in the **Using the NFS client** section.

    The mount command should look similar to this example:

```
sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport fs-bce57914.efs.us-west-2.amazonaws.com:/ efs
```

The provided `sudo mount...` command uses the default Linux mount options.

45. In your Linux SSH session, mount your Amazon EFS file system by:
    - Pasting the command
    - Pressing ENTER

46. Get a full summary of the available and used disk space usage by entering:

    ```
    sudo df -hT
    ```

    This following screenshot is an example of the output from the following *disk filesystem* command:

    ```
    df -hT
    ```

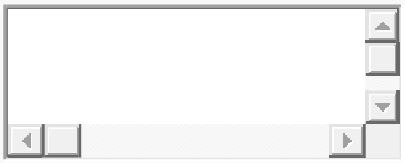
    Notice the *Type* and *Size* of your mounted EFS file system.

Task 5: Examining the performance behavior of your new EFS file system

Examining the performance by using Flexible IO

Flexible IO (fio) is a synthetic I/O benchmarking utility for Linux. It is used to benchmark and test Linux I/O subsystems. During boot, *fio* was automatically installed on your EC2 instance.

47. Examine the write performance characteristics of your file system by entering:



```
sudo fio --name=fio-efs --filesize=10G --filename=./efs/fio-efs-test.img --bs=1M --nrfiles=1 --direct=1 --sync=0 --rw=write --iodepth=200 --ioengine=libaio
```

The `fio` command will take 5–10 minutes to complete. The output should look like the example in the following screenshot. Make sure that you examine the output of your `fio` command, specifically the summary status information for this WRITE test.

Monitoring performance by using Amazon CloudWatch

48. In the **AWS Management Console**, on the **Services** menu, choose **CloudWatch**.
49. In the navigation pane on the left, choose **Metrics**.
50. In the **All metrics** tab, choose **EFS**.
51. Choose **File System Metrics**.
52. Select the row that has the **PermittedThroughput** Metric Name.

You might need to wait 2–3 minutes and refresh the screen several times before all available metrics, including **PermittedThroughput**, calculate and populate.

53. On the graph, choose and drag around the data line. If you do not see the line graph, adjust the time range of the graph to display the period during which you ran the `fio` command.

54. Pause your pointer on the data line in the graph. The value should be *105M*.

The throughput of Amazon EFS scales as the file system grows. File-based workloads are typically spiky. They drive high levels of throughput for short periods of time, and low levels of throughput the rest of the time. Because of this behavior, Amazon EFS is designed to burst to high throughput levels for periods of time. All file systems, regardless of size, can burst to 100 MiB/s of throughput. For more information about performance characteristics of your EFS file system, see the official Amazon Elastic File System documentation.

55. In the **All metrics** tab, *uncheck* the box for **PermittedThroughput**.
56. Select the check box for **DataWriteIOBytes**.

    If you do not see *DataWriteIOBytes* in the list of metrics, use the **File System Metrics** search to find it.

57. Choose the **Graphed metrics** tab.
58. On the **Statistics** column, select **Sum**.
59. On the **Period** column, select **1 Minute**.
60. Pause your pointer on the peak of the line graph. Take this number (in bytes) and divide it by the duration in seconds (60 seconds). The result gives you the write throughput (B/s) of your file system during your test.

The throughput that is available to a file system scales as a file system grows. All file systems deliver a consistent baseline performance of 50 MiB/s per TiB of storage. Also, all file systems (regardless of size) can burst to 100 MiB/s. File systems that are larger than 1T B can burst to 100 MiB/s per TiB of storage. As you add data to your file system, the maximum throughput that is available to the file system scales linearly and automatically with your storage.

File system throughput is shared across all EC2 instances that are connected to a file system. For more information about performance characteristics of your EFS file system, see the official Amazon Elastic File System documentation.

Congratulations! You created an EFS file system, mounted it to an EC2 instance, and ran an I/O benchmark test to examine its performance characteristics.

Submitting your work

61. At the top of these instructions, choose **Submit** to record your progress and when prompted, choose **Yes**.
62. If the results don't display after a couple of minutes, return to the top of these instructions and choose Grades

    Tip: You can submit your work multiple times. After you change your work, choose **Submit** again. Your last submission is what will be recorded for this lab.

63. To find detailed feedback on your work, choose Details followed by **View Submission Report**.

Lab complete

Congratulations! You have completed the lab.

64. Choose End Lab at the top of this page, and then select **Yes** to confirm that you want to end the lab.

    A panel should appear with this message: *DELETE has been initiated... You may close this message box now.*

65. Select the **X** in the top right corner to close the panel.

©2020 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.