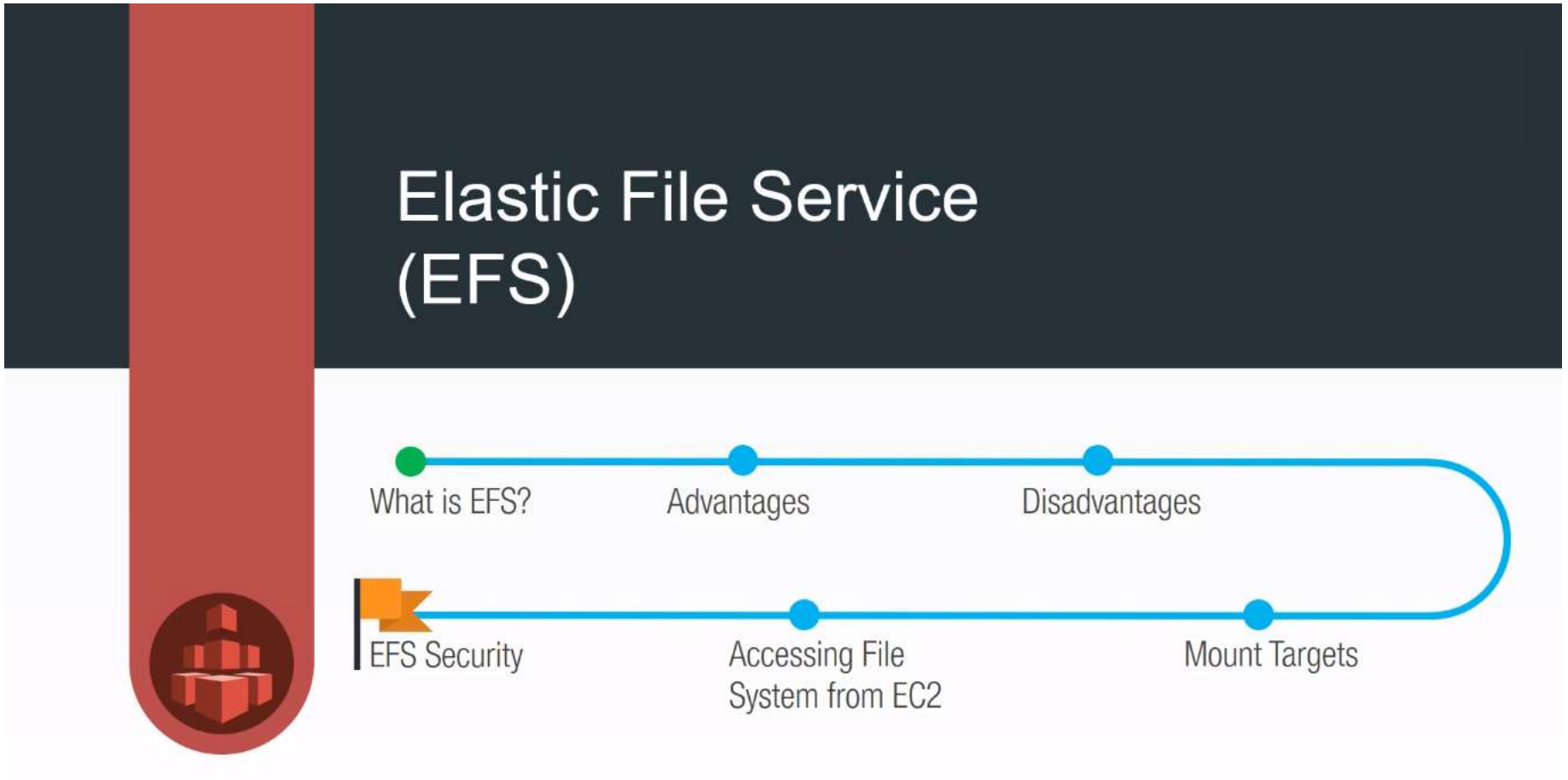
AWS CERTIFIED SOLUTION ARCHITECT

ASSOCIATE

INTRODUCTION

ELASTIC FILE SYSTEM

- Introduction to EFS
- Understanding EFS Architecture
- Deploying EFS
- Attaching it with EC2 instances

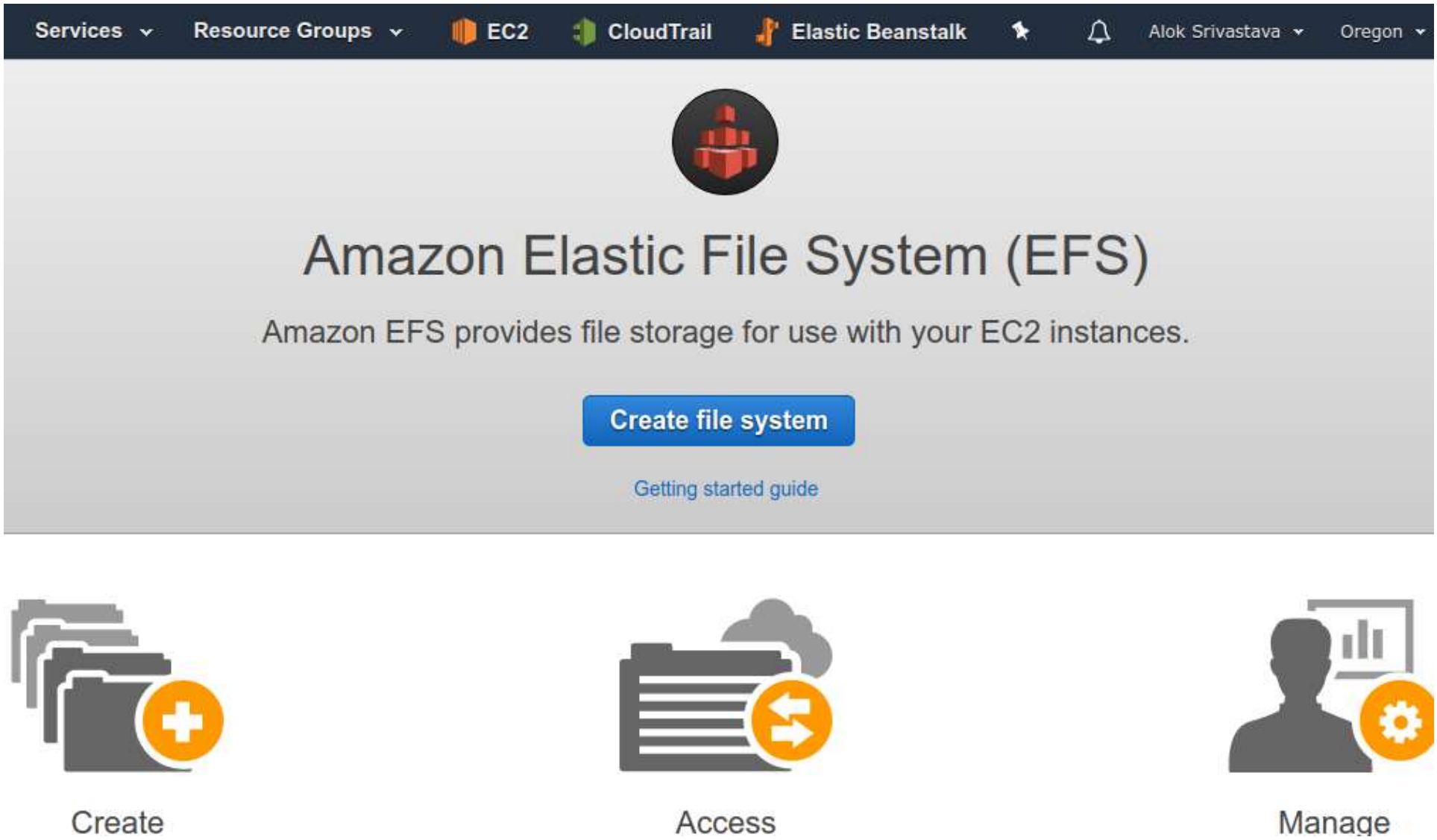

Elastic File Service
(EFS)
What is EFS?
Advantages
Disadvantages
EFS Security
Accessing File
System from EC2
Mount Targets

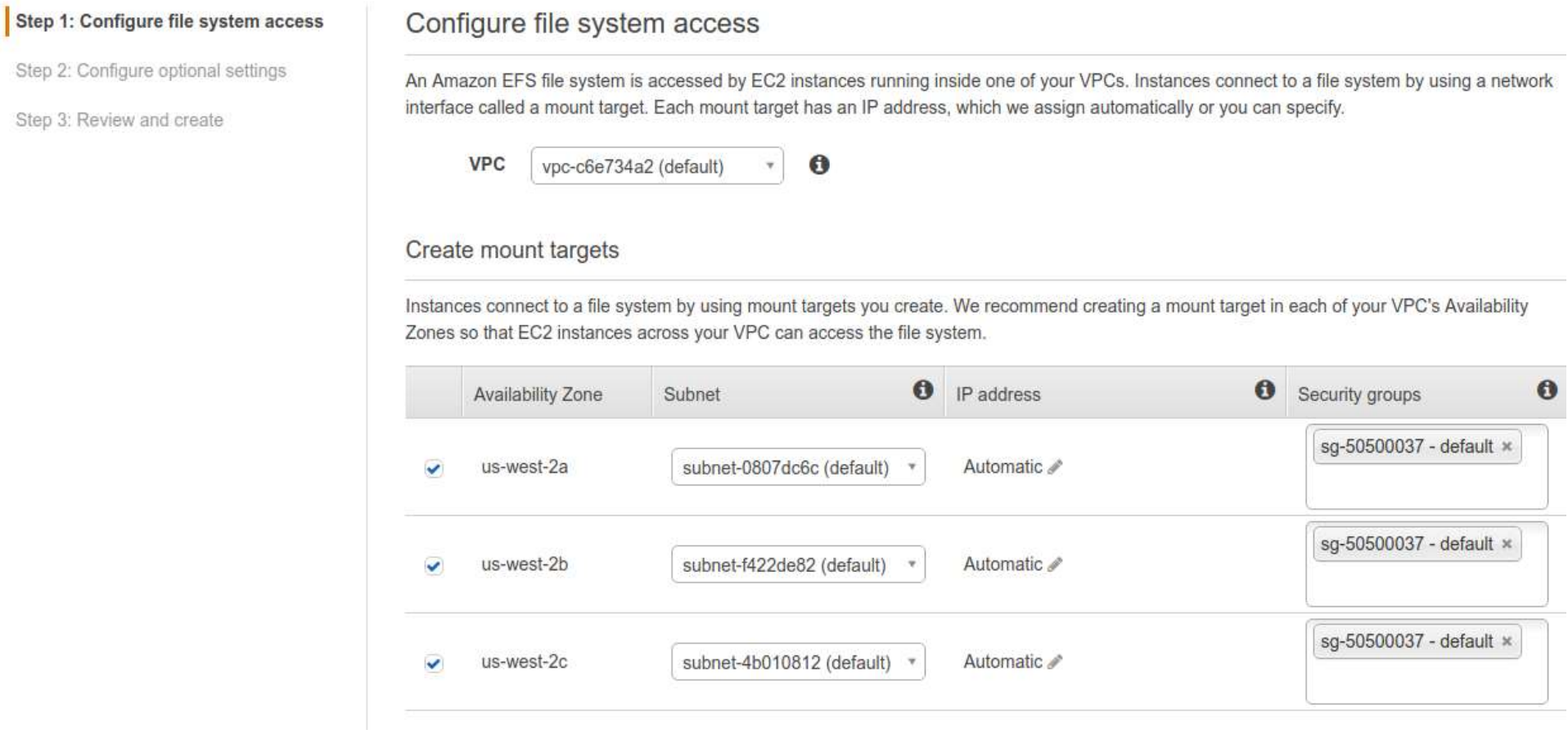
Region Unsupported

EFS is not available in **Asia Pacific (Mumbai)**. Please select another region.

Supported Regions

EU (Ireland)
Asia Pacific (Sydney)
EU (Frankfurt)
US East (N. Virginia)
US East (Ohio)
US West (N. California)
US West (Oregon)


Services
Resource Groups
EC2
CloudTrail
Elastic Beanstalk
Alok Srivastava
Oregon
Amazon Elastic File System (EFS)
Amazon EFS provides file storage for use with your EC2 instances.
Create file system
Getting started guide
Create
Access
Manage


Step 1: Configure file system access
Step 2: Configure optional settings
Step 3: Review and create
Configure file system access
An Amazon EFS file system is accessed by EC2 instances running inside one of your VPCs. Instances connect to a file system by using a network interface called a mount target. Each mount target has an IP address, which we assign automatically or you can specify.
VPC
vpc-c6e734a2 (default)
Create mount targets
Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.
Availability Zone
Subnet
IP address
Security groups
us-west-2a
subnet-0807dc6c (default)
Automatic
sg-50500037 - default
us-west-2b
subnet-f422de82 (default)
Automatic
sg-50500037 - default
us-west-2c
subnet-4b010812 (default)
Automatic
sg-50500037 - default

Key	Value	Remove
Name	efs-test	
Add New Key		

Choose performance mode

We recommend **General Purpose** performance mode for most file systems. **Max I/O** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff of slightly higher latencies for file operations.

- (•) **General Purpose (default)**
- ( ) **Max I/O**

Enable encryption

If you enable encryption for your file system, all data on your file system will be encrypted at rest. You can select a KMS key from your account to protect your file system, or you can provide the ARN of a key from a different account. Encryption of data at rest can only be enabled during file system creation. Encryption of data in transit is configured when mounting your file system. Learn more

Review and create

Review the configuration below before proceeding to create your file system.

File system access

VPC	Availability Zone	Subnet	IP address	Security groups
vpc-c6e734a2 (default)	us-west-2a	subnet-0807dc6c (default)	Automatic	sg-50500037 - default
	us-west-2b	subnet-f422de82 (default)	Automatic	sg-50500037 - default
	us-west-2c	subnet-4b010812 (default)	Automatic	sg-50500037 - default

Optional settings

Tags Name: efs-test
Performance mode General Purpose (default)
Encrypted No

Cancel Previous Create File System

	Name	File system ID	Metered size	Number of mount targets	Creation date
◉ ▾	efs-test	fs-067be7af	6.0 KiB	3	2018-04-21T02:58:21Z

Other details

Owner ID 671609384939
Life cycle state Available
Performance mode General Purpose
Encrypted No

Tags

Manage tags

Name: efs-test

File system access

Manage file system access

DNS name fs-067be7af.efs.us-west-2.amazonaws.com

Amazon EC2 mount instructions
AWS Direct Connect mount instructions

Mount targets

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
	us-west-2a	subnet-0807dc6c (default)	172.31.23.109	fsmt-ba9cf812	eni-a6a33580		Creating

Name: efs-test

Owner ID 671609384939
Life cycle state Available
Performance mode General Purpose
Encrypted No

File system access

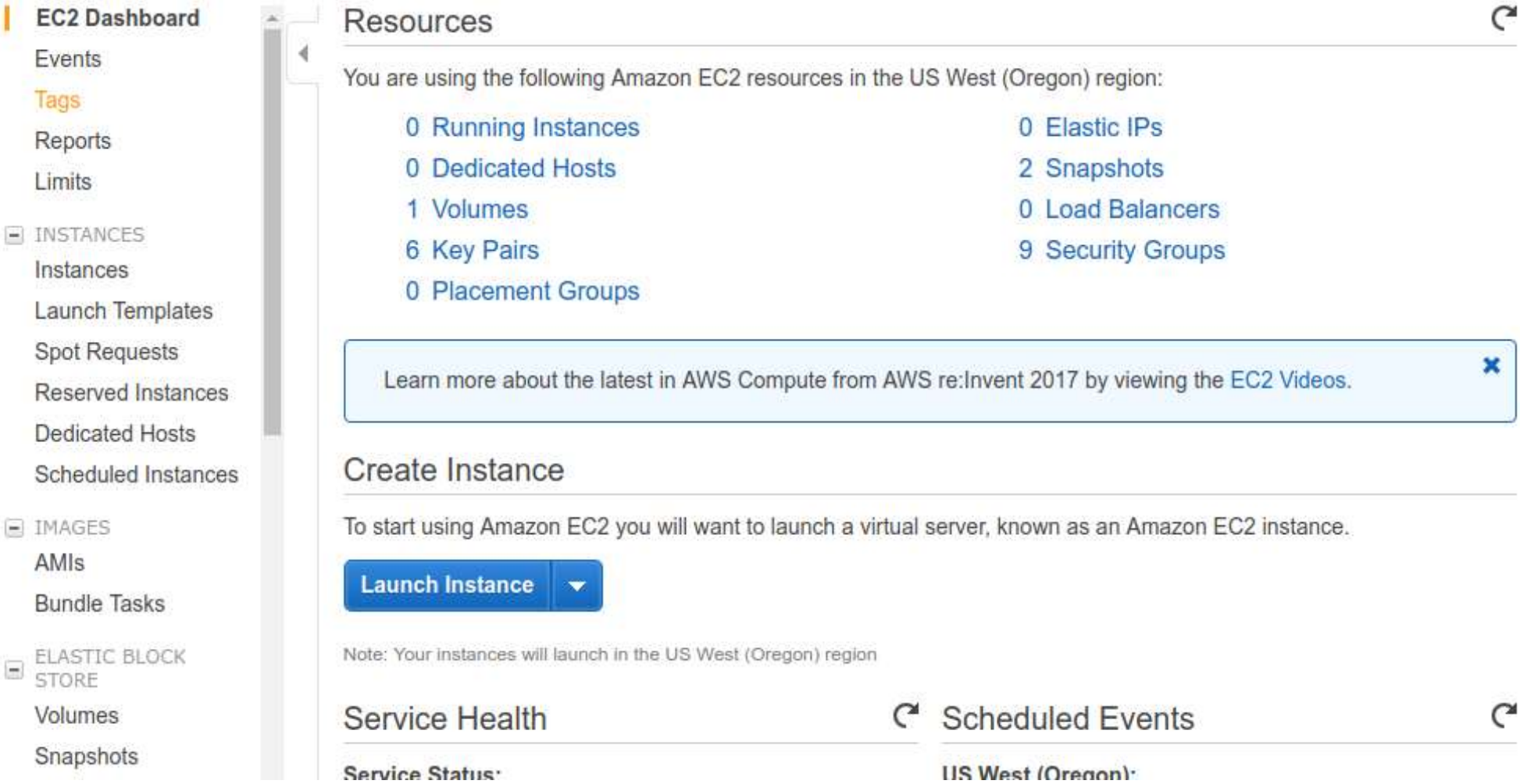
Manage file system access

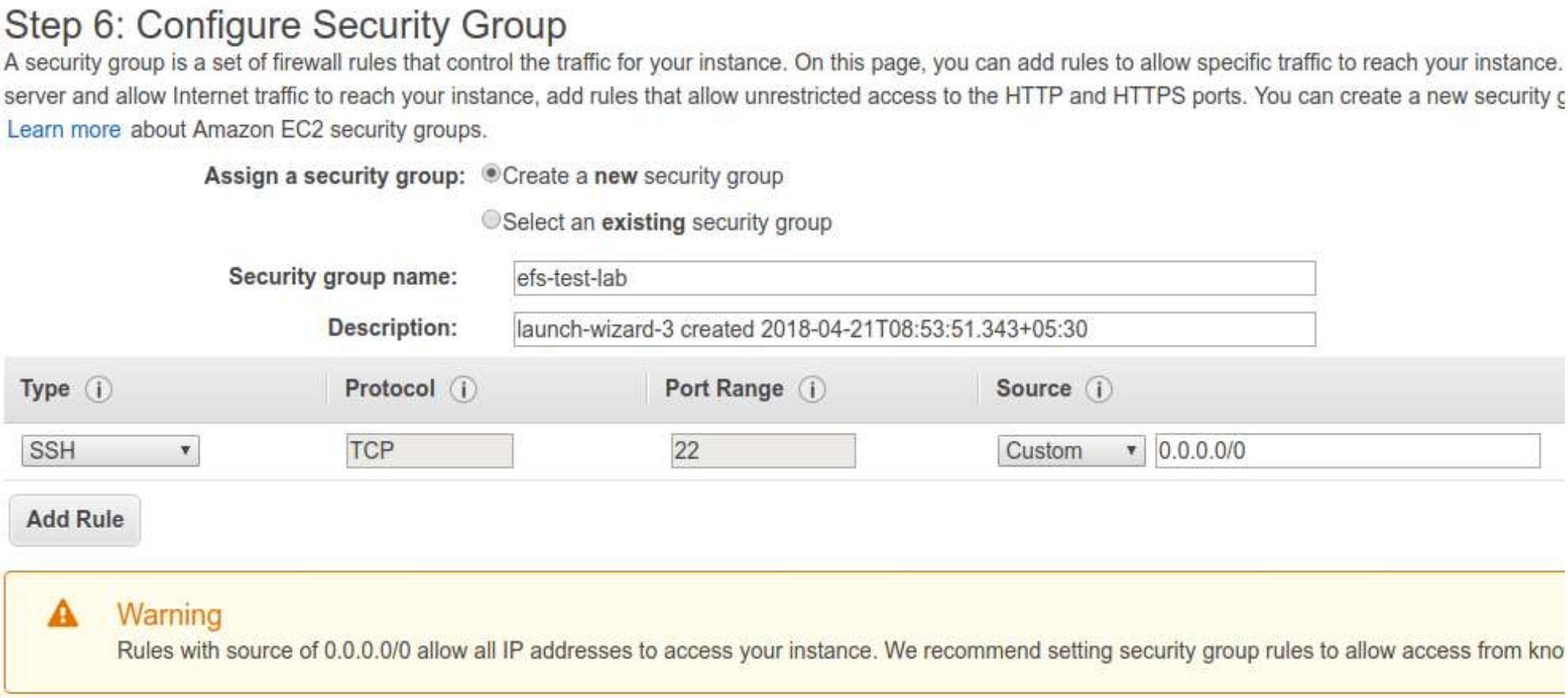
DNS name fs-067be7af.efs.us-west-2.amazonaws.com

Amazon EC2 mount instructions
AWS Direct Connect mount instructions

Mount targets

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
vpc-c6e734a2 (default)	us-west-2a	subnet-0807dc6c (default)	172.31.23.109	fsmt-ba9cf813	eni-a6a33580	sg-50500037 - default	Available
	us-west-2b	subnet-f422de82 (default)	172.31.44.239	fsmt-bc9cf815	eni-7a19e673	sg-50500037 - default	Available


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Resources
You are using the following Amazon EC2 resources in the US West (Oregon) region:
0 Running Instances
0 Dedicated Hosts
1 Volumes
6 Key Pairs
0 Placement Groups
0 Elastic IPs
2 Snapshots
0 Load Balancers
9 Security Groups
Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.
Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
Launch Instance
Note: Your instances will launch in the US West (Oregon) region
Service Health
Service Status:
Scheduled Events
US West (Oregon):


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.
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 g
Learn more about Amazon EC2 security groups.
Assign a security group: Create a new security group
Select an existing security group
Security group name: efs-test-lab
Description: launch-wizard-3 created 2018-04-21T08:53:51.343+05:30
Type
Protocol
Port Range
Source
SSH
TCP
22
Custom
0.0.0.0/0
Add Rule
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from kno

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch proce

⚠ Improve your instances' security. Your security group, efs-test-lab, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.

You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit securit

AMI Details

Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-d874e0a0

Free tier eligible

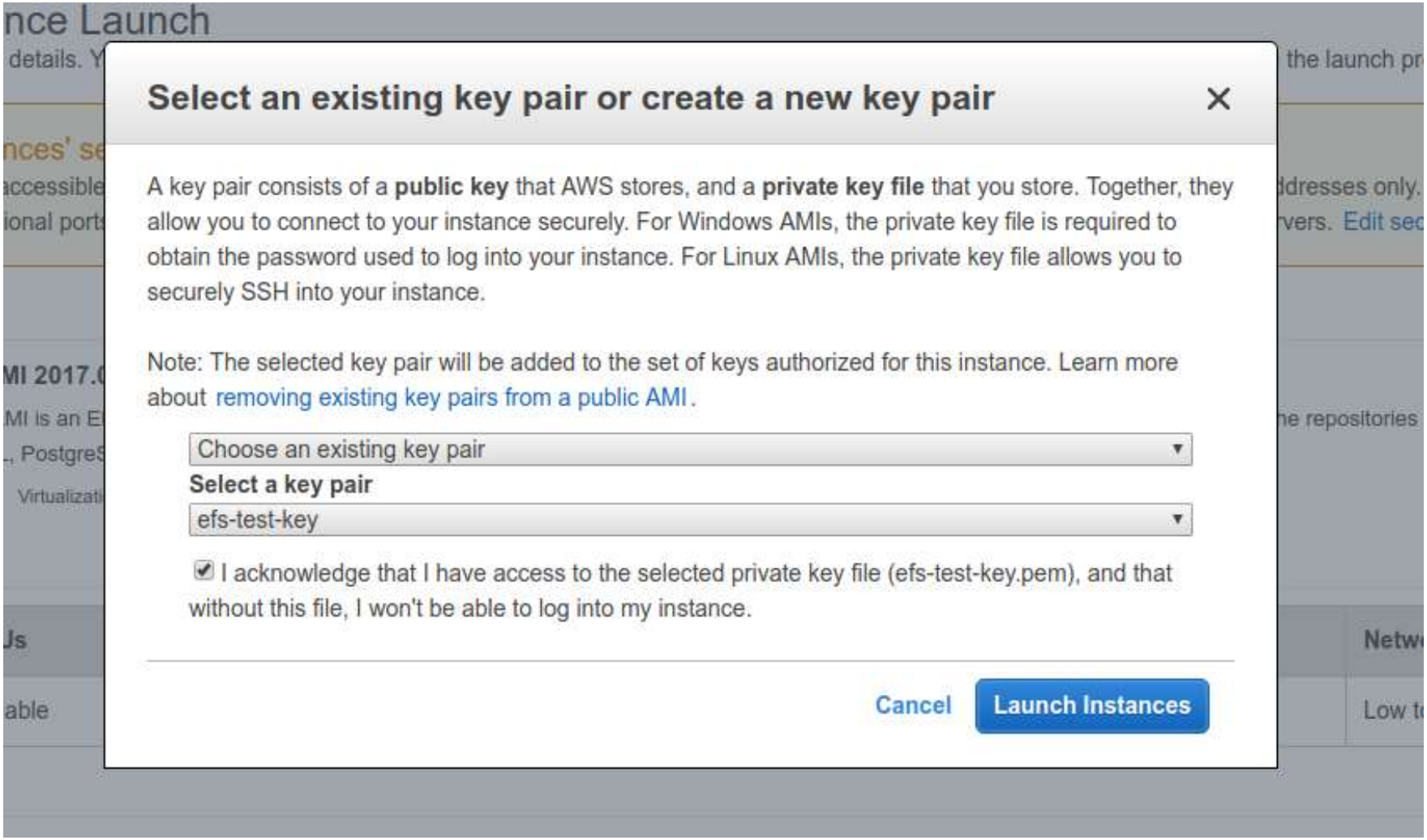
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories incl Docker, PHP, MySQL, PostgreSQL, and other packages.

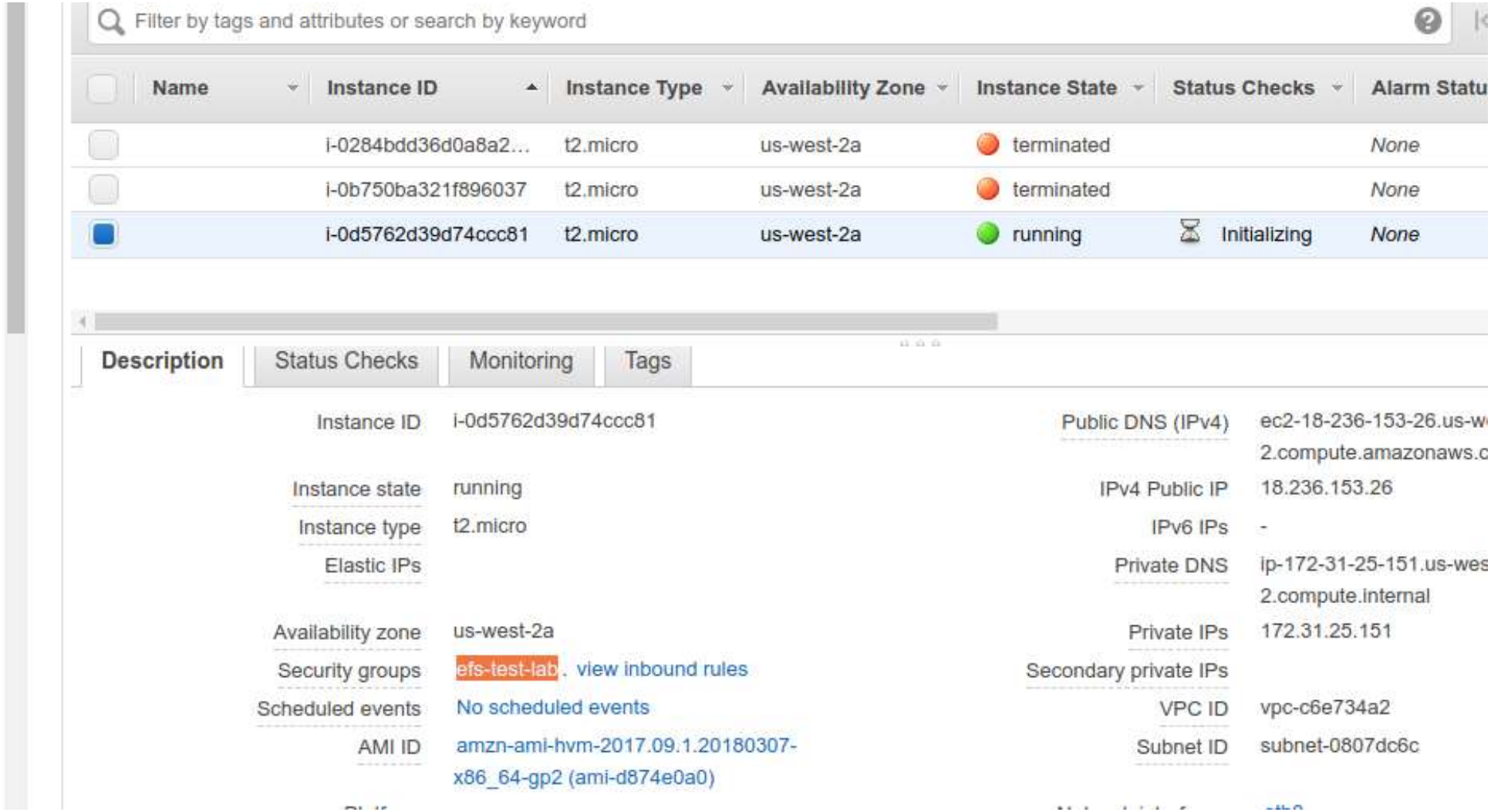
Root Device Type: ebs Virtualization type: hvm

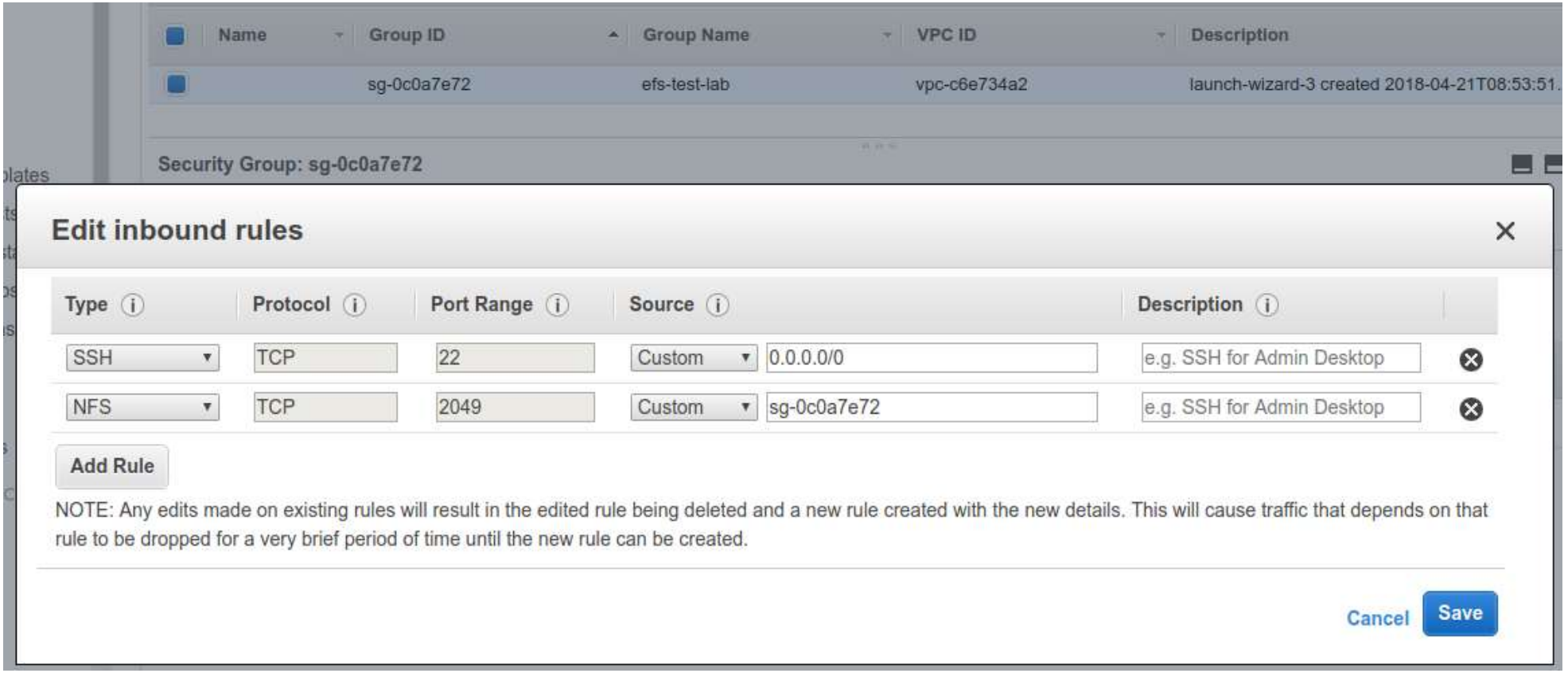
Instance Type

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

Security Groups


nce Launch
details. Y
the launch pr
nces' se
accessible
ional ports
ddresses only.
rvers. Edit sec
MI 2017.0
MI is an E
, PostgreS
Virtualizati
he repositories
Js
Netw
able
Low t
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.
Choose an existing key pair
Select a key pair
efs-test-key
I acknowledge that I have access to the selected private key file (efs-test-key.pem), and that without this file, I won't be able to log into my instance.
Cancel
Launch Instances


Filter by tags and attributes or search by keyword
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Statu
i-0284bdd36d0a8a2...
t2.micro
us-west-2a
terminated
None
i-0b750ba321f896037
t2.micro
us-west-2a
terminated
None
i-0d5762d39d74ccc81
t2.micro
us-west-2a
running
Initializing
None
Description
Status Checks
Monitoring
Tags
Instance ID
i-0d5762d39d74ccc81
Instance state
running
Instance type
t2.micro
Elastic IPs
Availability zone
us-west-2a
Security groups
efs-test-lab. view inbound rules
Scheduled events
No scheduled events
AMI ID
amzn-ami-hvm-2017.09.1.20180307-x86_64-gp2 (ami-d874e0a0)
Public DNS (IPv4)
ec2-18-236-153-26.us-w
2.compute.amazonaws.c
IPv4 Public IP
18.236.153.26
IPv6 IPs
-
Private DNS
ip-172-31-25-151.us-wes
2.compute.internal
Private IPs
172.31.25.151
Secondary private IPs
VPC ID
vpc-c6e734a2
Subnet ID
subnet-0807dc6c


Name
Group ID
Group Name
VPC ID
Description
sg-0c0a7e72
efs-test-lab
vpc-c6e734a2
launch-wizard-3 created 2018-04-21T08:53:51.
Security Group: sg-0c0a7e72
Edit inbound rules
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
NFS
TCP
2049
Custom
sg-0c0a7e72
e.g. SSH for Admin Desktop
Add Rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.
Cancel
Save

efs-test	fs-067be7af	6.0 KiB	3		2018-04-21T02:58:21Z

Other details

Owner ID 671609384939
Life cycle state Available
Performance mode General Purpose
Encrypted No

Tags

Manage tags

Name: efs-test

File system access

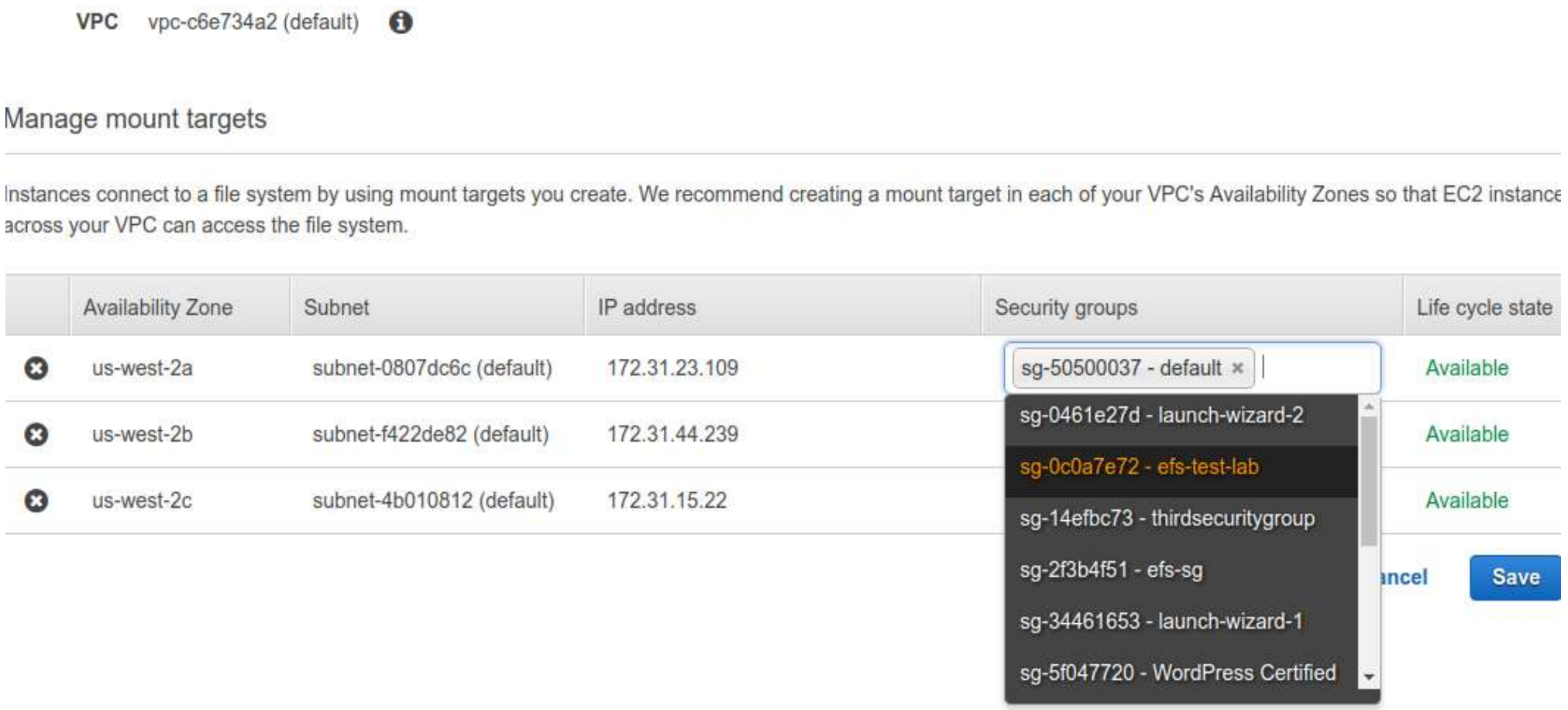
Manage file system access

DNS name fs-067be7af.efs.us-west-2.amazonaws.com

Amazon EC2 mount instructions
AWS Direct Connect mount instructions

Mount targets

VPC	Availability Zone	Subnet	IP address	Mount target ID	Network interface ID	Security groups	Life cycle state
	us-west-2a	subnet-0807dc6c	172.31.23.109	fsmt-	eni-a6a33580	sg-50500037 -	Available


VPC vpc-c6e734a2 (default)
Manage mount targets
Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instance
across your VPC can access the file system.
Availability Zone
Subnet
IP address
Security groups
Life cycle state
us-west-2a
subnet-0807dc6c (default)
172.31.23.109
sg-50500037 - default
Available
us-west-2b
subnet-f422de82 (default)
172.31.44.239
Available
us-west-2c
subnet-4b010812 (default)
172.31.15.22
Available
sg-0461e27d - launch-wizard-2
sg-0c0a7e72 - efs-test-lab
sg-14efbc73 - thirdsecuritygroup
sg-2f3b4f51 - efs-sg
sg-34461653 - launch-wizard-1
sg-5f047720 - WordPress Certified
ncel
Save

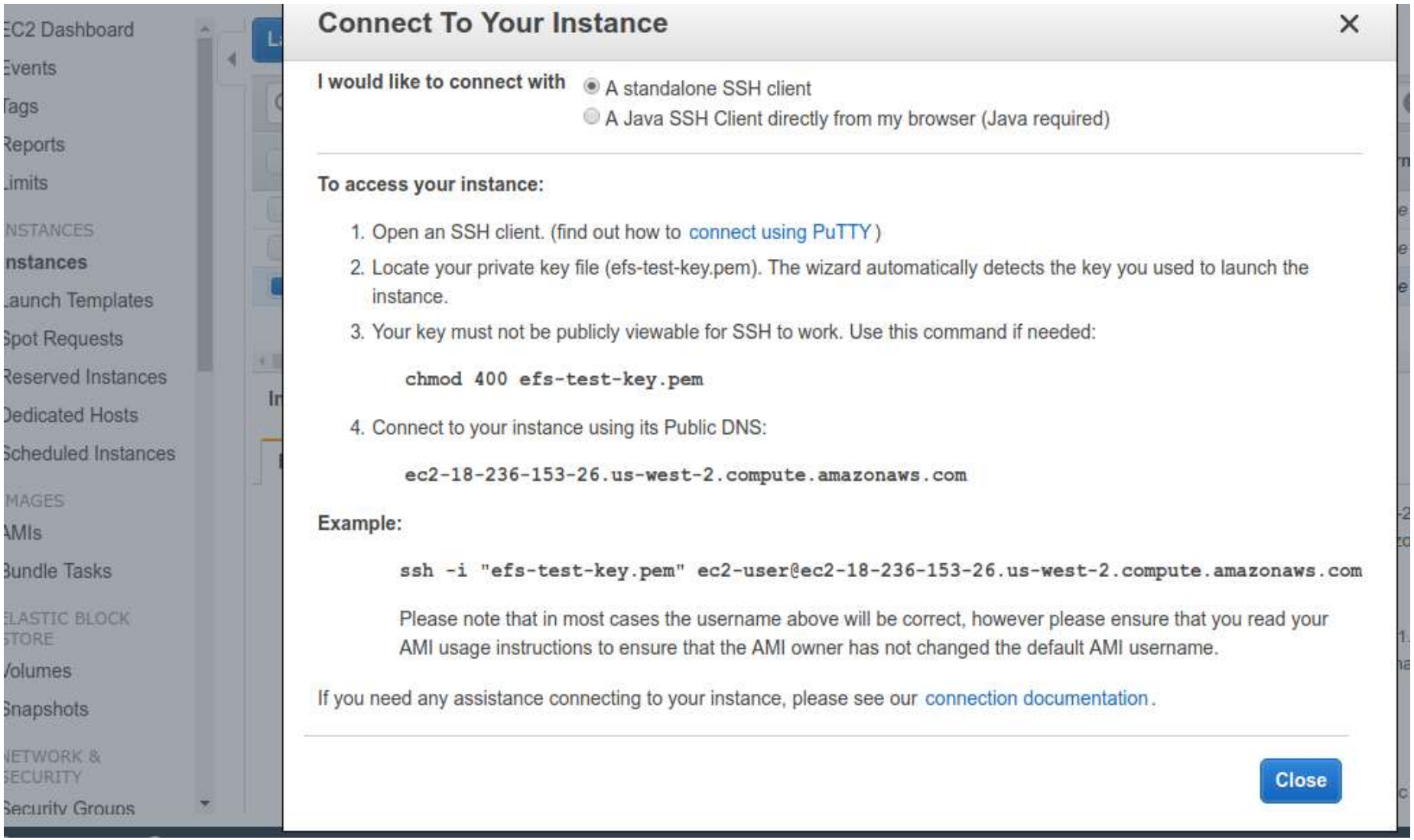
VPC vpc-c6e734a2 (default)

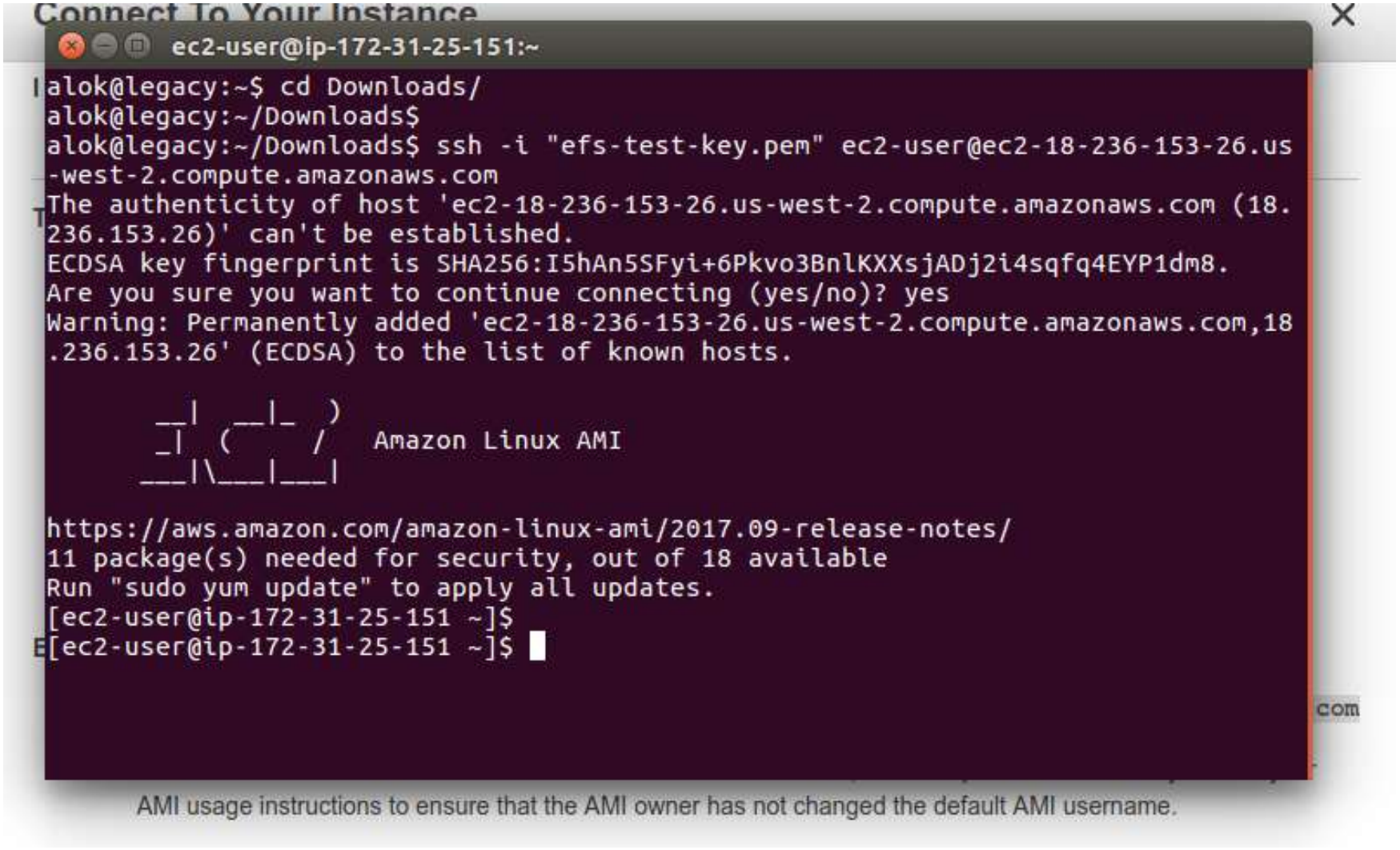
Manage mount targets

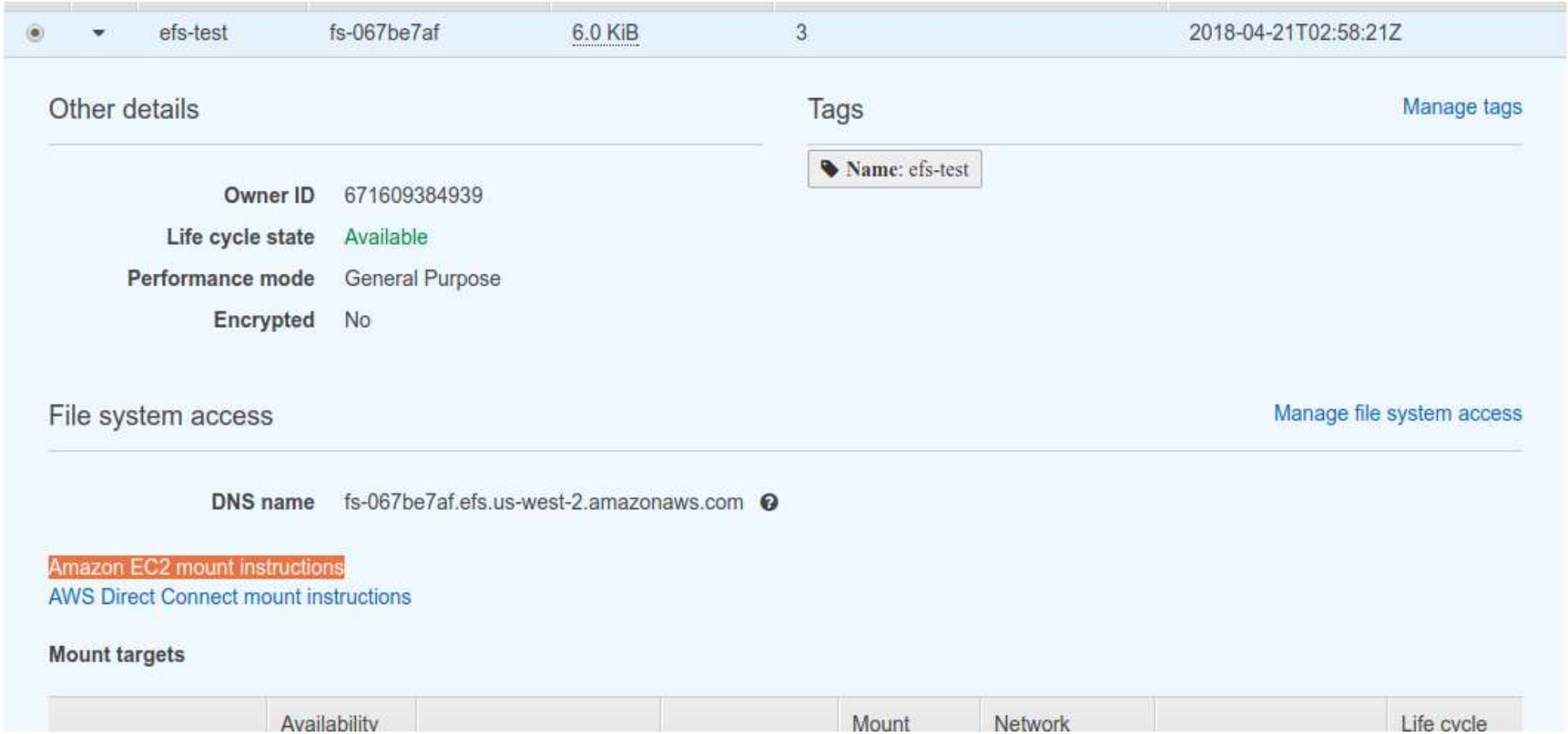
Instances connect to a file system by using mount targets you create. We recommend creating a mount target in each of your VPC's Availability Zones so that EC2 instances across your VPC can access the file system.

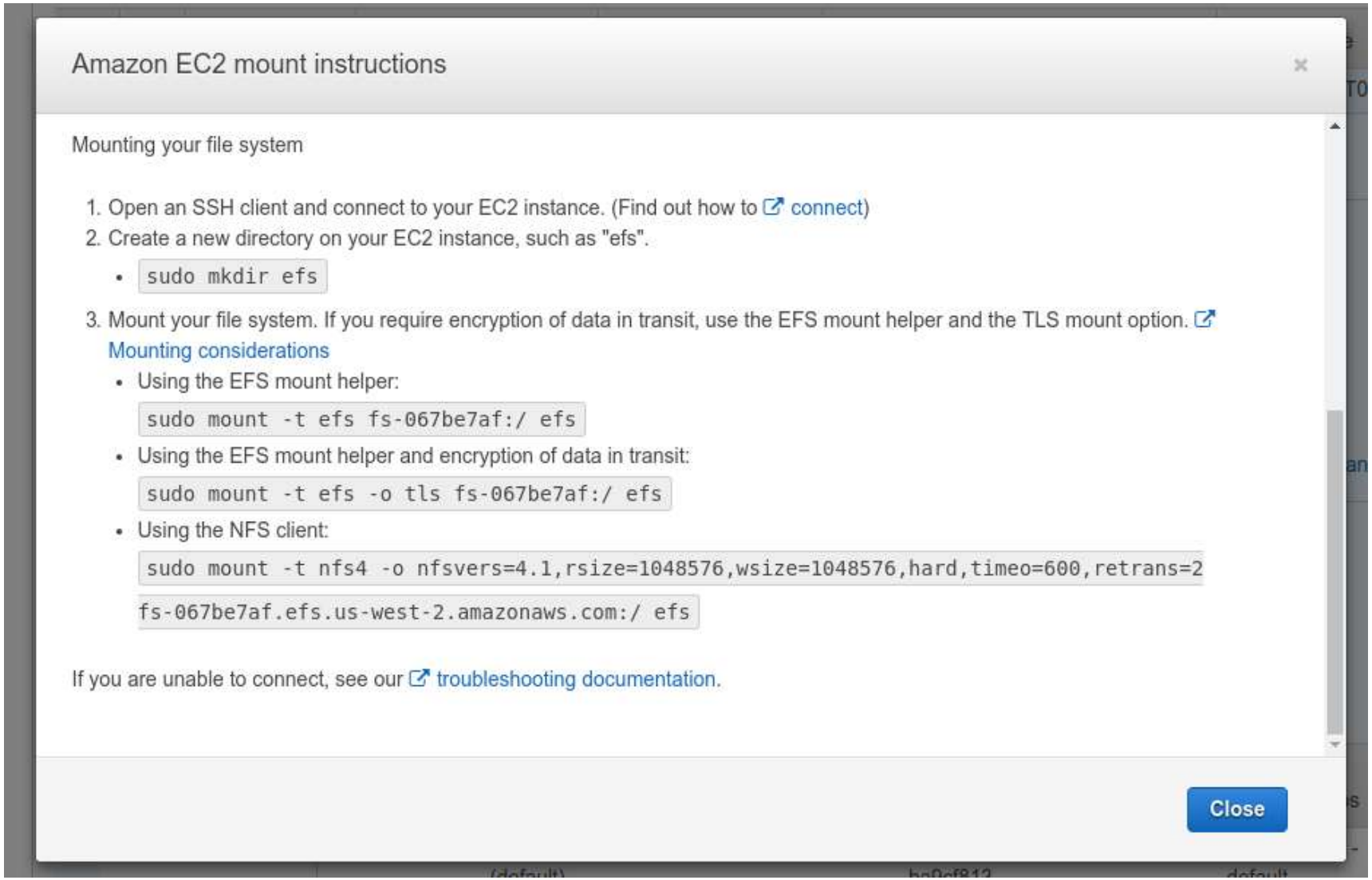
	Availability Zone	Subnet	IP address	Security groups	Life cycle state
⊗	us-west-2a	subnet-0807dc6c (default)	172.31.23.109	sg-0c0a7e72 - efs-test-lab × sg-50500037 - default ×	Available
⊗	us-west-2b	subnet-f422de82 (default)	172.31.44.239	sg-0c0a7e72 - efs-test-lab × sg-50500037 - default ×	Available
⊗	us-west-2c	subnet-4b010812 (default)	172.31.15.22	sg-0c0a7e72 - efs-test-lab × sg-50500037 - default ×	Available

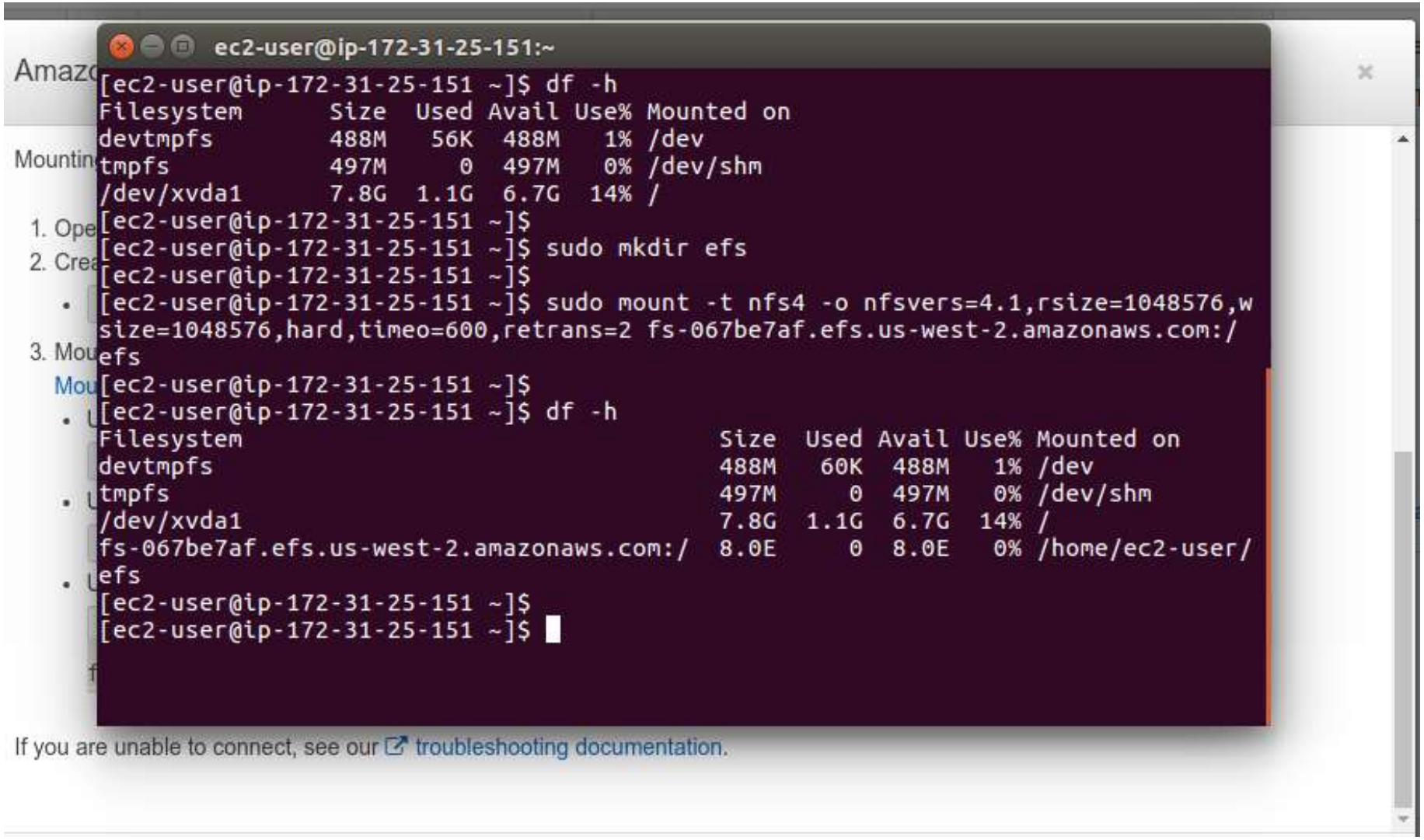
Cancel Save


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
nstances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
MAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Connect To Your Instance
I would like to connect with
A standalone SSH client
A Java SSH Client directly from my browser (Java required)
To access your instance:
1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (efs-test-key.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:
chmod 400 efs-test-key.pem
4. Connect to your instance using its Public DNS:
ec2-18-236-153-26.us-west-2.compute.amazonaws.com
Example:
ssh -i "efs-test-key.pem" ec2-user@ec2-18-236-153-26.us-west-2.compute.amazonaws.com
Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.
If you need any assistance connecting to your instance, please see our connection documentation.
Close


Connect To Your Instance
ec2-user@ip-172-31-25-151:~
alok@legacy:~$ cd Downloads/
alok@legacy:~/Downloads$
alok@legacy:~/Downloads$ ssh -i "efs-test-key.pem" ec2-user@ec2-18-236-153-26.us
-west-2.compute.amazonaws.com
The authenticity of host 'ec2-18-236-153-26.us-west-2.compute.amazonaws.com (18.
236.153.26)' can't be established.
ECDSA key fingerprint is SHA256:I5hAn5SFyi+6Pkvo3BnlKXXsjADj2i4sqfq4EYP1dm8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-18-236-153-26.us-west-2.compute.amazonaws.com,18
.236.153.26' (ECDSA) to the list of known hosts.
__| __|_)
_| (/   Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
11 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-25-151 ~]$
[ec2-user@ip-172-31-25-151 ~]$
com
AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.


efs-test
fs-067be7af
6.0 KiB
3
2018-04-21T02:58:21Z
Other details
Tags
Manage tags
Name: efs-test
Owner ID
671609384939
Life cycle state
Available
Performance mode
General Purpose
Encrypted
No
File system access
Manage file system access
DNS name
fs-067be7af.efs.us-west-2.amazonaws.com
Amazon EC2 mount instructions
AWS Direct Connect mount instructions
Mount targets
Availability
Mount
Network
Life cycle


Amazon EC2 mount instructions
Mounting your file system
1. Open an SSH client and connect to your EC2 instance. (Find out how to connect)
2. Create a new directory on your EC2 instance, such as "efs".
• sudo mkdir efs
3. Mount your file system. If you require encryption of data in transit, use the EFS mount helper and the TLS mount option.
Mounting considerations
• Using the EFS mount helper:
sudo mount -t efs fs-067be7af:/ efs
• Using the EFS mount helper and encryption of data in transit:
sudo mount -t efs -o tls fs-067be7af:/ efs
• Using the NFS client:
sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2
fs-067be7af.efs.us-west-2.amazonaws.com:/ efs
If you are unable to connect, see our troubleshooting documentation.
Close


ec2-user@ip-172-31-25-151:~
[ec2-user@ip-172-31-25-151 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 488M 56K 488M 1% /dev
tmpfs 497M 0 497M 0% /dev/shm
/dev/xvda1 7.8G 1.1G 6.7G 14% /
[ec2-user@ip-172-31-25-151 ~]$
[ec2-user@ip-172-31-25-151 ~]$ sudo mkdir efs
[ec2-user@ip-172-31-25-151 ~]$
[ec2-user@ip-172-31-25-151 ~]$ sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,w
size=1048576,hard,timeo=600,retrans=2 fs-067be7af.efs.us-west-2.amazonaws.com:/
efs
[ec2-user@ip-172-31-25-151 ~]$
[ec2-user@ip-172-31-25-151 ~]$ df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 488M 60K 488M 1% /dev
tmpfs 497M 0 497M 0% /dev/shm
/dev/xvda1 7.8G 1.1G 6.7G 14% /
fs-067be7af.efs.us-west-2.amazonaws.com:/ 8.0E 0 8.0E 0% /home/ec2-user/
efs
[ec2-user@ip-172-31-25-151 ~]$
[ec2-user@ip-172-31-25-151 ~]$
If you are unable to connect, see our troubleshooting documentation.