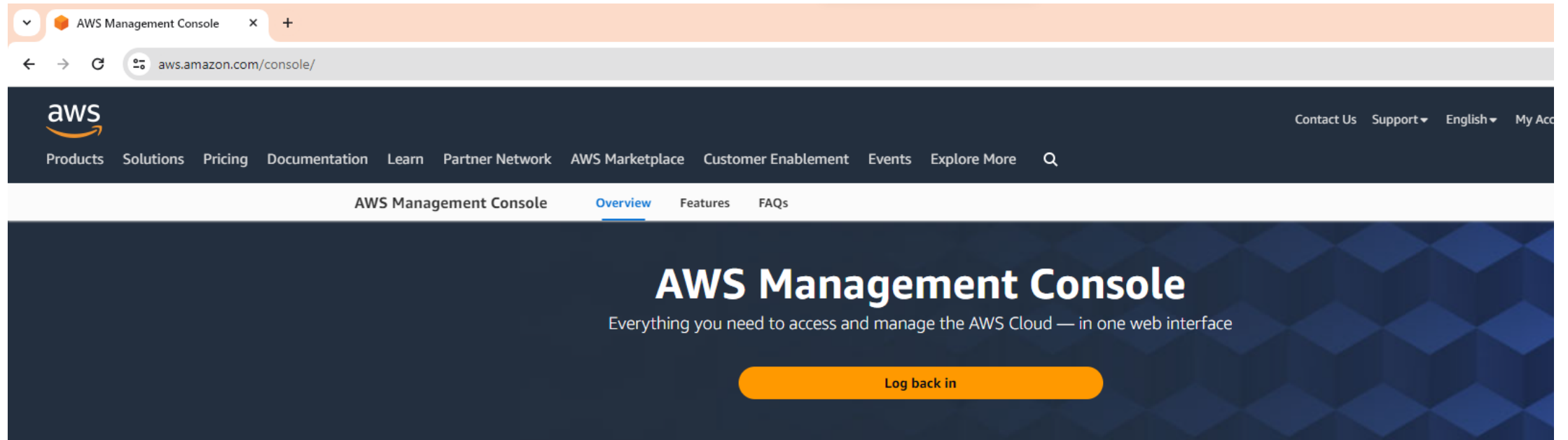


EFS

EFS – Elastic File System

- It is a managed NFS – Network File System
- Can be mounted to many EC2 instances
- Can be added to different availability zone AZ's
- Will support only to Linux not windows
- Can enable KMS for encryption
- Storage class – File Storage
- Provides a simple serverless and elastic file system that lets to share file data without provisioning or managing storage

Login - AWS





Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

username@example.com

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

— New to AWS? —

Create a new AWS account

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Root user sign in ⓘ

Email: tkpradeep.it@gmail.com

Password

[Forgot password?](#)

Sign in

[Sign in to a different account](#)

[Create a new AWS account](#)

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: tkpradeep.it@gmail.com

MFA code

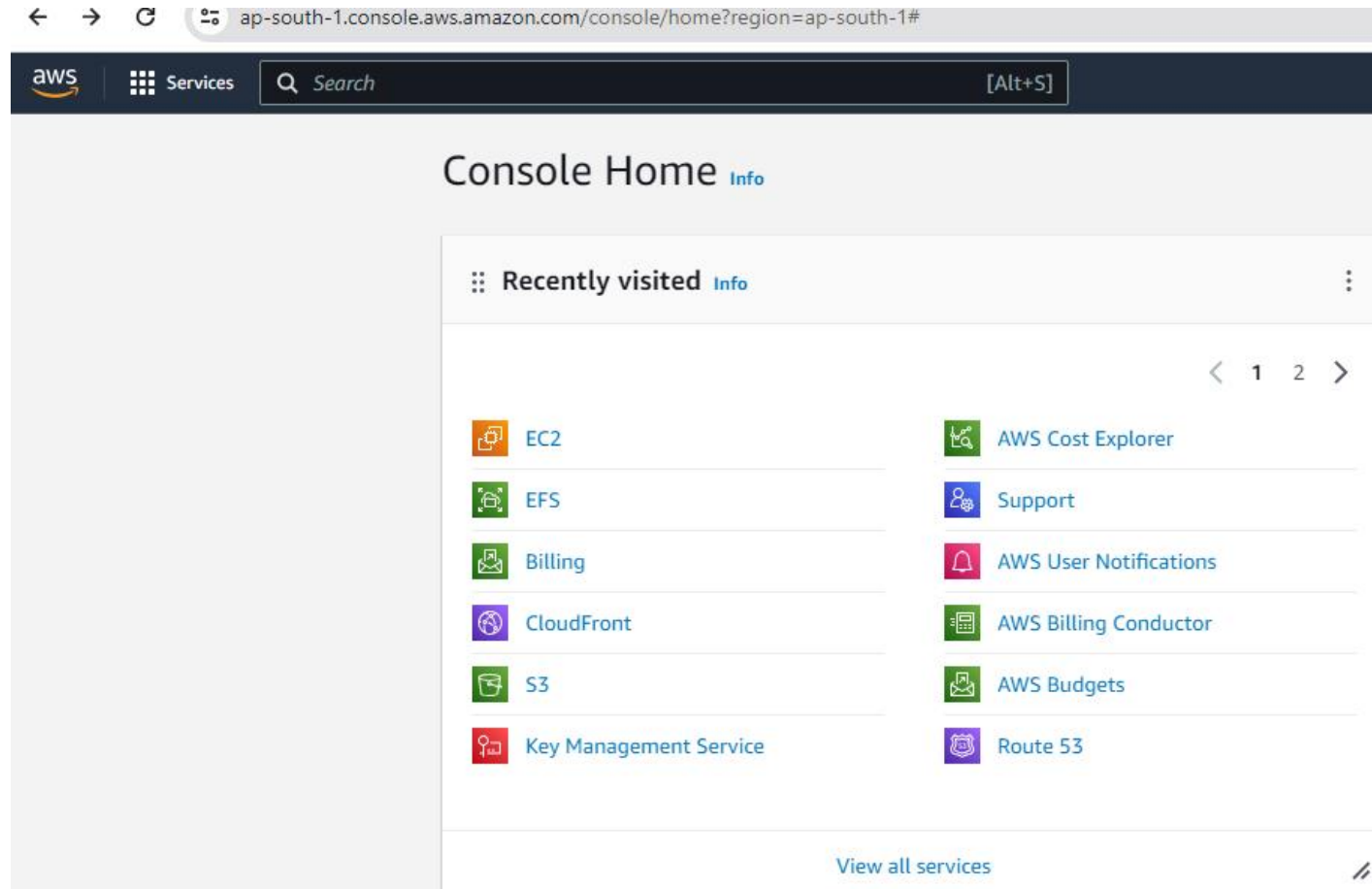
Submit

[Troubleshoot MFA](#)

[Cancel](#)

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Go to search – EC2 – Create a Security Policy



awsServicesSearch

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Load balancers

Snapshots

Launch instance

Migrate a server

Scheduled events

Asia Pacific (Mumbai)

No scheduled events

Migrate a server

Use AWS Application Migration Service to simplify migration from physical, virtual, and cloud infrastructure.

Quick ID filter

Enter a resource ID

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a security group, you must specify a VPC.

Basic details

Security group name

EFS-Demo

Name cannot be edited after creation.

Description

SSH

VPC

vpc-0977d5115de8f3149 (Default)

Inbound rules

Create a policy by adding inbound rule ssh.

Inbound rules

Type

Protocol

Port range

Source

Description - optional

SSH

TCP

22

Anywhere...



0.0.0.0/0

Delete

Add rule

Go to EFS – Create a EFS – add the security policy created

Elastic File System ✕
File systems
Access points
AWS Backup [↗](#)
AWS DataSync [↗](#)
AWS Transfer [↗](#)

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 recommended settings.
Create file system

Create file system ✕

Create an EFS file system with recommended settings. [Learn more](#) [↗](#)

Name - optional
Name 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.

vpc-0977d5115de8f3149
default ▼

Cancel

Customize

Create

Select – Customize – Defaults

≡

[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

File system settings

General

Name - *optional*
Name your file system.

Storage class [Learn more](#)

☒ Standard
Stores data redundantly across multiple AZs

☐ One Zone
Stores data redundantly within a single AZ

Automatic backups

Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. [Learn more](#)

☒ Enable automatic backups

Lifecycle management

Automatically save money as access patterns change by moving files into the Standard-Infrequent Access (IA) storage class. [Learn more](#)

Transition into IA
Transition files from Standard to Standard-Infrequent Access.

Transition out of IA
Transition files from Standard-Infrequent Access to Standard.

30 day(s) since last access

None

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

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

Performance settings

Throughput mode

Choose a method for your file system's throughput limits. [Learn more](#)

☒ **Enhanced**
Provides more flexibility and higher throughput levels for workloads with a range of performance requirements.

☐ **Bursting**
Provides throughput that scales with the amount of storage for workloads with basic performance requirements.

☒ **Elastic (Recommended)**
Use this mode for workloads with unpredictable I/O. With Elastic mode, your throughput scales automatically and you only pay for what you use.

☐ **Provisioned**
Use this mode if you can estimate your workload's throughput requirements. With Provisioned mode, you configure your file system's throughput and pay for throughput provisioned.

▼ Additional settings

Performance mode

Set your file system's performance mode based on IOPS required. File systems using Elastic throughput mode only support General Purpose performance mode. [Learn more](#)

☒ **General Purpose (Recommended)**
Ideal for a variety of diverse workloads, including high performance and latency-sensitive applications

☐ **Max I/O**
Designed for highly parallelized workloads that can tolerate higher latencies

► Tags optional

Cancel

Next

Delete the security policy - existing

Network access

Network

Virtual Private Cloud (VPC) [Learn more](#)

Choose the VPC where you want EC2 instances to connect to your file system.

vpc-0977d5115de8f3149
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

ap-south-1a

subnet-0c6e3a4115137b12a

Automatic

Choose security groups

Remove

ap-south-1b

subnet-02ff94ad2cbee5bda

Automatic

Choose security groups

Remove

ap-south-1c

subnet-0fdc211e469dcf676

Automatic

Choose security groups

Remove

Add mount target

You can only create one mount target per Availability Zone.

Attach the security policy created : EFS-Demo

Network access

Network

Virtual Private Cloud (VPC) [Learn more](#)

Choose the VPC where you want EC2 instances to connect to your file system.

vpc-0977d5115de8f3149
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	
ap-south-1a	subnet-0c6e3a4115137b12a	Automatic	<div>Choose security groups</div> <div>sg-04e200b67a653a212 ✕ EFS-Demo</div>	<div>Remove</div>
ap-south-1b	subnet-02ff94ad2cbee5bda	Automatic	<div>Choose security groups</div> <div>sg-04e200b67a653a212 ✕ EFS-Demo</div>	<div>Remove</div>
ap-south-1c	subnet-0fdc211e469dcf676	Automatic	<div>Choose security groups</div> <div>sg-04e200b67a653a212 ✕ EFS-Demo</div>	<div>Remove</div>

Add mount target

You can only create one mount target per Availability Zone.

Cancel

Previous

Next

Defaults – file system policy

[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

File system policy - *optional*

Policy options

Select one or more of these common policy options, or create a custom policy using the editor. [Learn more](#)

- ☐ Prevent root access by default*
- ☐ Enforce read-only access by default*
- ☐ Prevent anonymous access
- ☐ Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

► **Grant additional permissions**

Policy editor {JSON}

Clear

1 |

Manual changes will prevent the use of the policy options on the left until the editor is cleared.

Cancel

Previous

Next

Step 1
File system settings

Step 2
Network access

Step 3 - optional
File system policy

Step 4
Review and create

Review and create

Step 1: File system settings

Edit

File system		
Field	Value	Is editable?
Name	EFS_Demo_1	Yes
Performance mode	General Purpose	No
Throughput mode	Elastic	Yes
Encrypted	Yes	No
KMS Key ID	-	No
Lifecycle management	Transition into IA: 30 day(s) since last access Transition out of IA: None	Yes
Automatic backup	Yes	Yes

Step 3: File system policy

Edit

File system policy

1

Cancel

Previous

Create

EFS - created

Elastic File System

File systems

Access points

AWS Backup

AWS DataSync

AWS Transfer

Documentation

File system (fs-0b6fd72986f69fed2) is creating.

Amazon EFS

 > File systems

File systems (1)

Filter by property values

View details

Delete

Create file system

	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
	EFS_Demo_1	fs-0b6fd72986f69fed2	Encrypted	0 Bytes	0 Bytes	0 Bytes	-	Creating	Fri, 03 Nov 2023 05:44:51 GMT	Standard

Create 2 EC2 Instance – Amazon Linux – Add the EFS File in Storage – Select the same security policy of EC2 Instance A

[EC2](#) > [Instances](#) > Launch an instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Q following the simple steps below.

Name and tags

Name

EFS-InstanceA

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application applications) required to launch your instance. Search or Browse for AMIs if you don't see w below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Li

SUS

Instance type

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true

Free tier eligible

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0724 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

All generations

Compare instance types

Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Proceed without a key pair (Not recommended)

Default value

Create new key pair

Network settings

Network

vpc-0977d5115de8f3149 | Default

Subnet

subnet-02ff94ad2cbee5bda | my-subnet-2

Auto-assign public IP

Enable

Storage (volumes)

EBS Volumes

Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp3))

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

File systems

EFS

FSx

Shared file system 1

Remove

File system

fs-0b6fd72986f69fed2

Name: EFS_Demo_1 Availability: Regional

Mount point

/mnt/efs/fs1

Add shared file system

Create new shared file system

4 remaining (Up to 5 file systems maximum).

Automatically create and attach security groups

To enable access to the file system, the required security groups will be automatically created and attached to this instance and the selected file system. To manually manage the security groups, clear the checkbox. Learn more.

Automatically mount shared file system by attaching required user data script

Automatically mount your file system by updating your user data to install efs-utils. If you would like to manually mount your file system, clear the checkbox.

Successfully – Created 2 different instances

The screenshot displays the AWS Management Console's 'Instances' page. The left-hand navigation pane includes links for 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Instances' (which is expanded to show 'Instances', 'Instance Types', 'Launch Templates', and 'Spot Requests'), 'Instance Types', 'Launch Templates', and 'Spot Requests'. The main content area is titled 'Instances (2)' and features a search bar with the placeholder text 'Find Instance by attribute or tag (case-sensitive)'. Above the instance list, there are buttons for 'Refresh', 'Connect', 'Instance state', 'Actions', and a prominent orange 'Launch instances' button. The instance list itself is a table with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4 ... , Elastic IP, and IP. Two instances are listed: 'EFS-InstanceA' with ID 'i-0d3aaa23fe758bb43' and 'EFS-InstanceB' with ID 'i-0ea2476f0cb22e0e4'. Both are in a 'Running' state, using 't2.micro' instance type, and are in the 'ap-south-1b' availability zone. Their status checks are 'Initializing'. The table also shows their respective Public IPv4 DNS addresses, Public IPv4 addresses, and Elastic IP addresses.

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IP
<input type="checkbox"/>	EFS-InstanceA	i-0d3aaa23fe758bb43	Running	t2.micro	Initializing	No alarms	ap-south-1b	ec2-43-204-215-216.ap...	43.204.215.216	-	-
<input type="checkbox"/>	EFS-InstanceB	i-0ea2476f0cb22e0e4	Running	t2.micro	Initializing	No alarms	ap-south-1b	ec2-65-1-3-140.ap-sout...	65.1.3.140	-	-

How to confirm to check with EC2 Instances connected with EFS file?

EC2 Dashboard × EC2 Global View Events

▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
▼ Images
AMIs

EC2 > Instances > i-0d3aaa23fe758bb43

Instance summary for i-0d3aaa23fe758bb43 (EFS-InstanceA) Info

Updated less than a minute ago

Buttons: Refresh, Connect, Instance state, Actions

Instance ID i-0d3aaa23fe758bb43 (EFS-InstanceA)	Public IPv4 address 43.204.215.216 open address	Private IPv4 addresses 172.31.25.228
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-43-204-215-216.ap-south-1.compute.amazonaws.com open address
Hostname type IP name: ip-172-31-25-228.ap-south-1.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-25-228.ap-south-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 43.204.215.216 [Public IP]	VPC ID vpc-0977d5115de8f3149 (Default) open	
IAM Role	Subnet ID	Auto Scaling Group name

Select an EC2 Instance – Connect – EC2 Instance Connect – Click on connect

EC2 > Instances > i-0d3aaa23fe758bb43 > Connect to instance

Connect to instance Info

Connect to your instance i-0d3aaa23fe758bb43 (EFS-InstanceA) using any of these options

Buttons: EC2 Instance Connect, Session Manager, SSH client, EC2 serial console

Instance ID
i-0d3aaa23fe758bb43 (EFS-InstanceA)

Connection Type

☒ Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

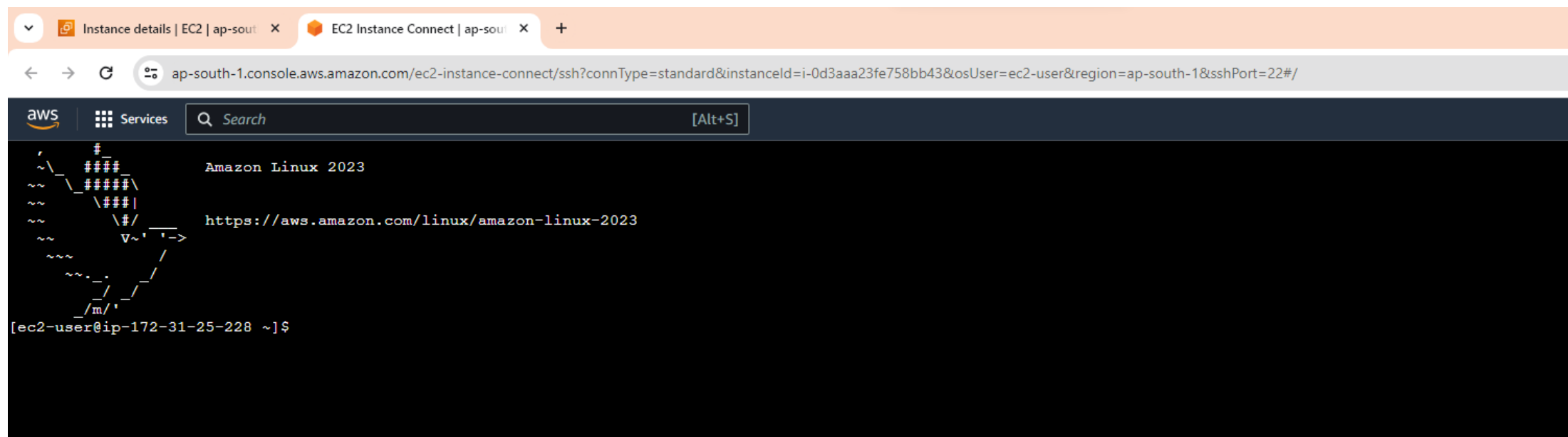
☐ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Public IP address
43.204.215.216

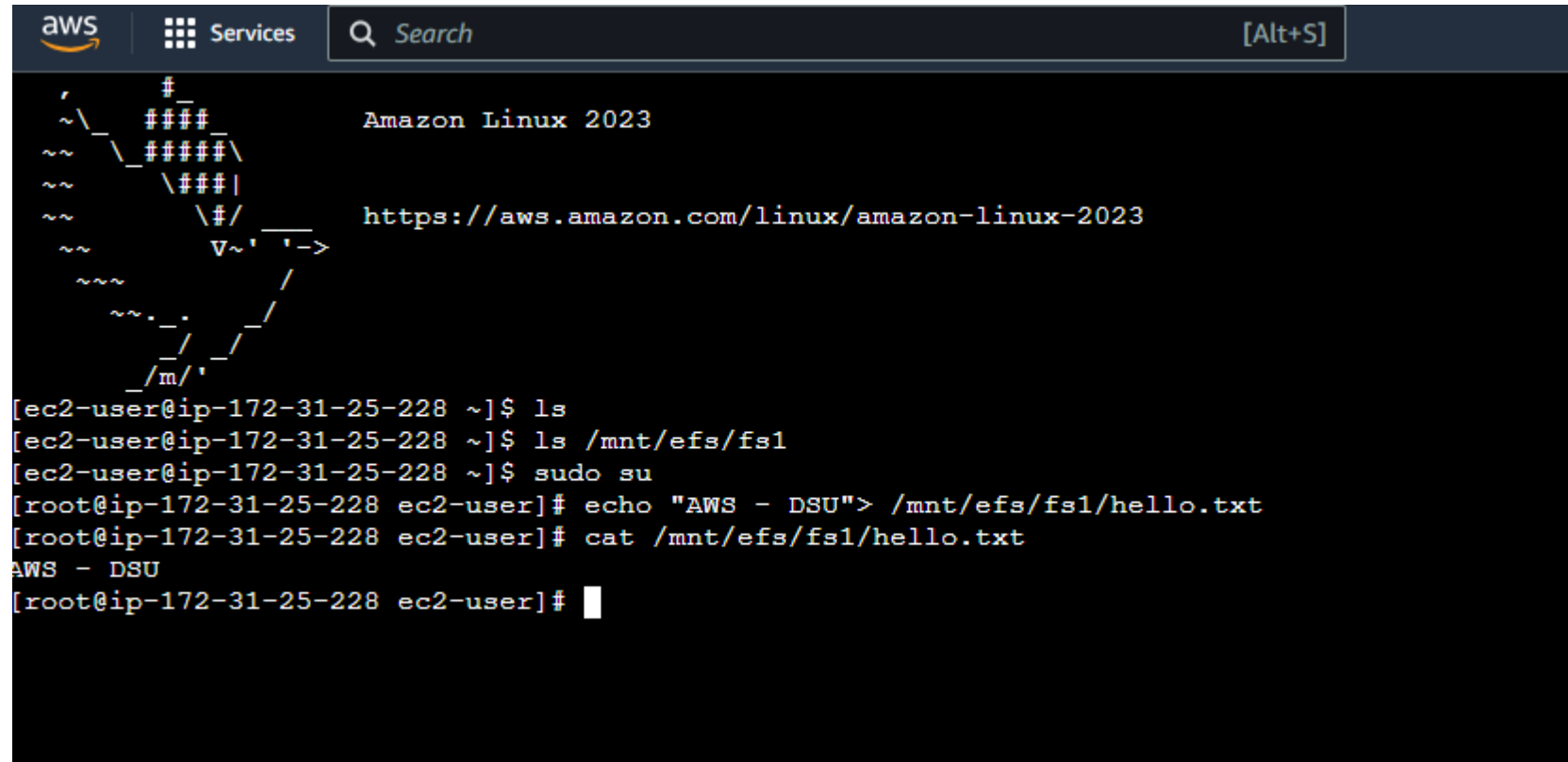
User name
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.
ec2-user

Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Buttons: Cancel, Connect



Create a file using unix commands, and cat the output

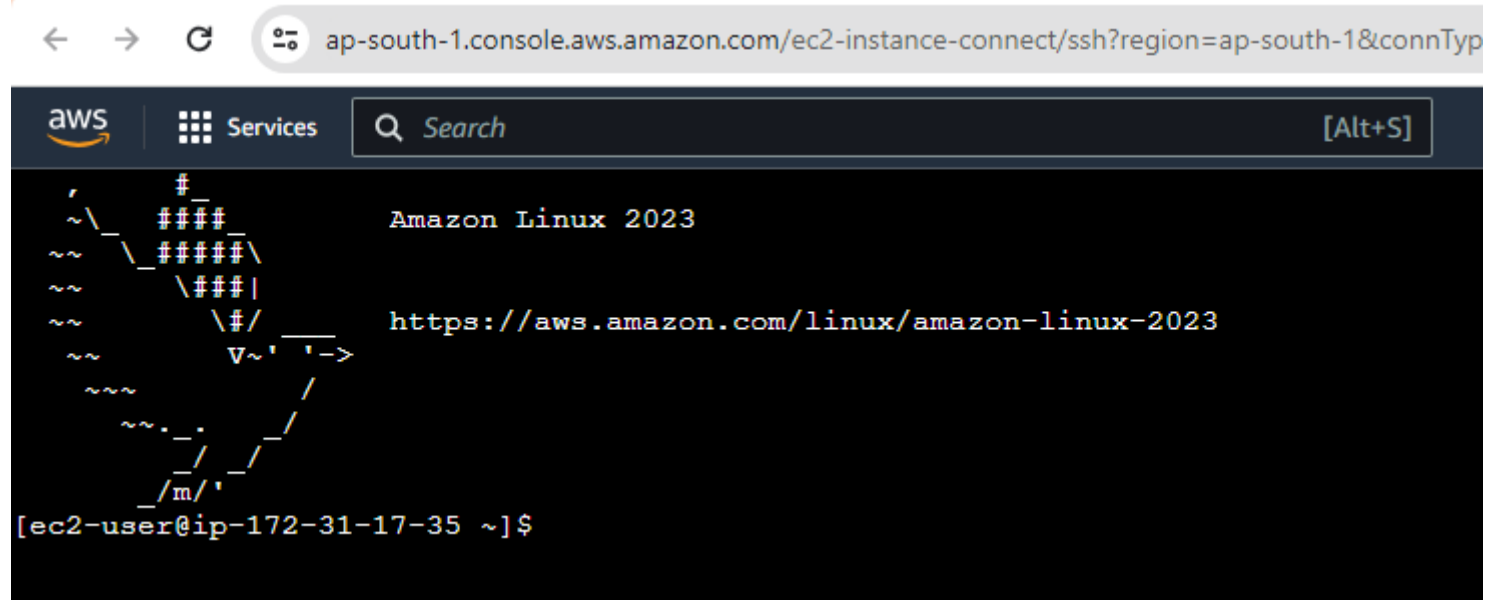


```
aws Services Search [Alt+S]

#
##### Amazon Linux 2023
#####\
\###|
\#/ https://aws.amazon.com/linux/amazon-linux-2023
V~' '->
~~~
~~.-.
-/m/'

[ec2-user@ip-172-31-25-228 ~]$ ls
[ec2-user@ip-172-31-25-228 ~]$ ls /mnt/efs/fs1
[ec2-user@ip-172-31-25-228 ~]$ sudo su
[root@ip-172-31-25-228 ec2-user]# echo "AWS - DSU" > /mnt/efs/fs1/hello.txt
[root@ip-172-31-25-228 ec2-user]# cat /mnt/efs/fs1/hello.txt
AWS - DSU
[root@ip-172-31-25-228 ec2-user]#
```

Open the second EC2 Instance – to check the EFS shared among the instances



The screenshot shows a web browser window with the address bar displaying `ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connTyp`. The browser window shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and a '[Alt+S]' button. The main content area is a terminal window for an Amazon Linux 2023 instance. The terminal output shows the AWS logo, the text 'Amazon Linux 2023', and the URL `https://aws.amazon.com/linux/amazon-linux-2023`. The terminal prompt is `[ec2-user@ip-172-31-17-35 ~]$`.

Now can observe the file created in ec2 instanceA will appear in another ec2 instanceB

[illegible]

Can try to connect using putty, AWS cli ...etc

- Thank you...