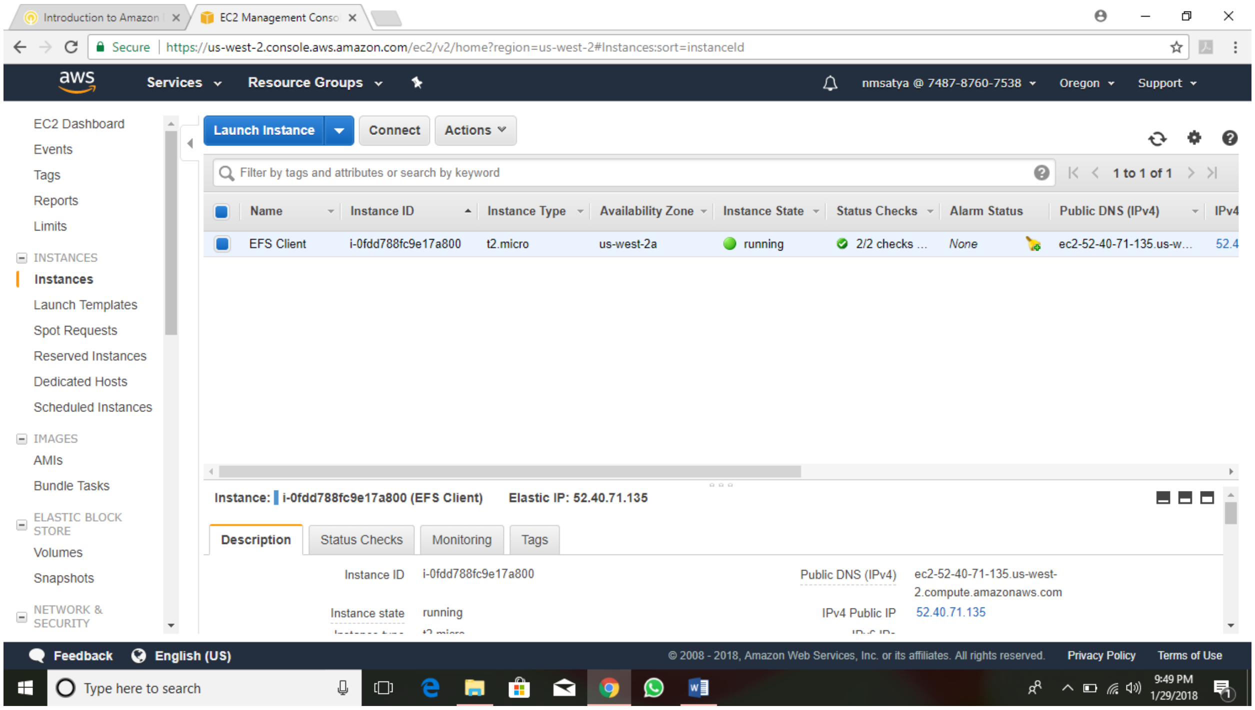
Configure EFS & IAM & Cloud Trail

Logged into AWS Account and create one Linux instance as usual steps



https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:sort=instanceId

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4
EFS Client	i-0fdd788fc9e17a800	t2.micro	us-west-2a	running	2/2 checks ...	None	ec2-52-40-71-135.us-w...	52.4

Instance: i-0fdd788fc9e17a800 (EFS Client) Elastic IP: 52.40.71.135

Instance ID: i-0fdd788fc9e17a800

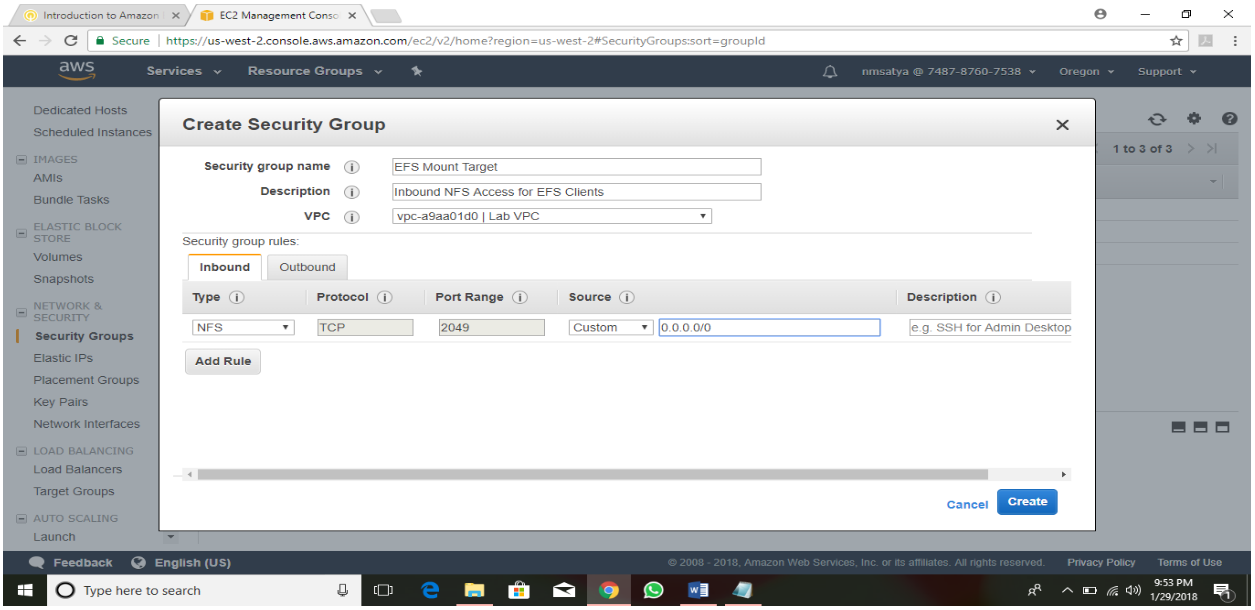
Public DNS (IPv4): ec2-52-40-71-135.us-west-2.compute.amazonaws.com

Instance state: running

IPv4 Public IP: 52.40.71.135

Task-1 – Create a Security Group to Access your Amazon EFS File System

Go the EC2 and select security group and create a new security group.



https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#SecurityGroups:sort=groupId

Create Security Group

Security group name: EFS Mount Target

Description: Inbound NFS Access for EFS Clients

VPC: vpc-a9aa01d0 | Lab VPC

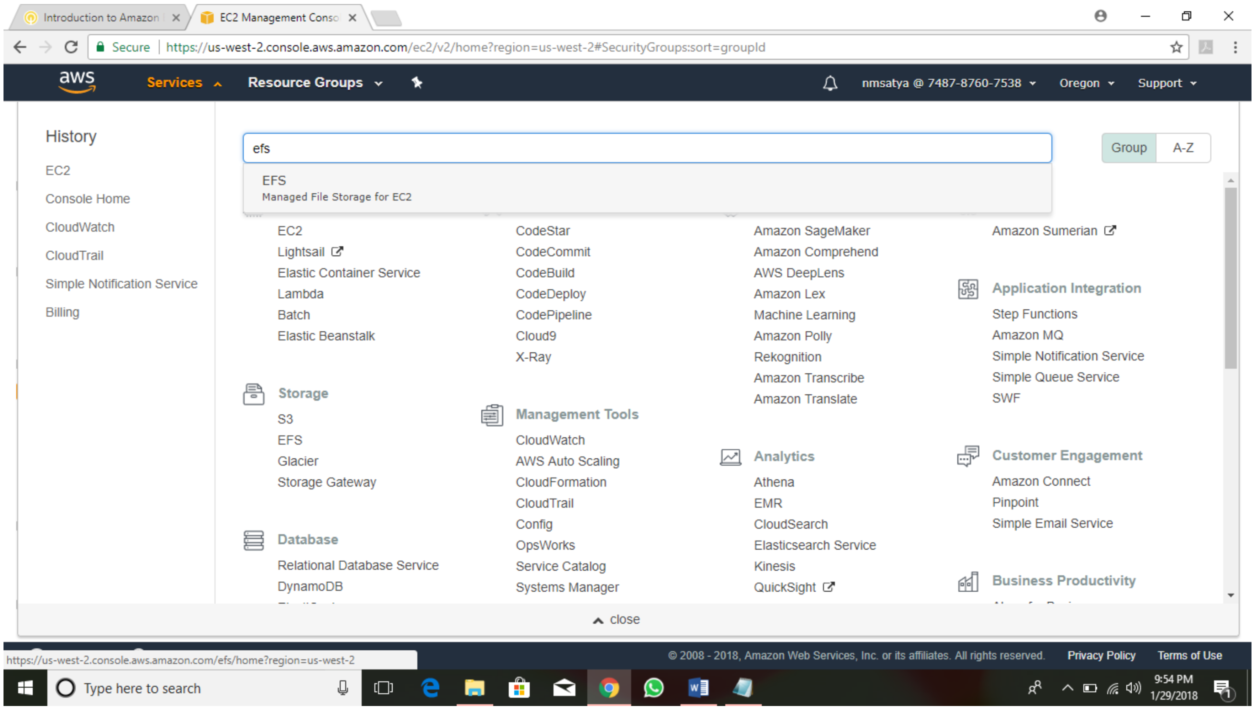
Security group rules:

Inbound

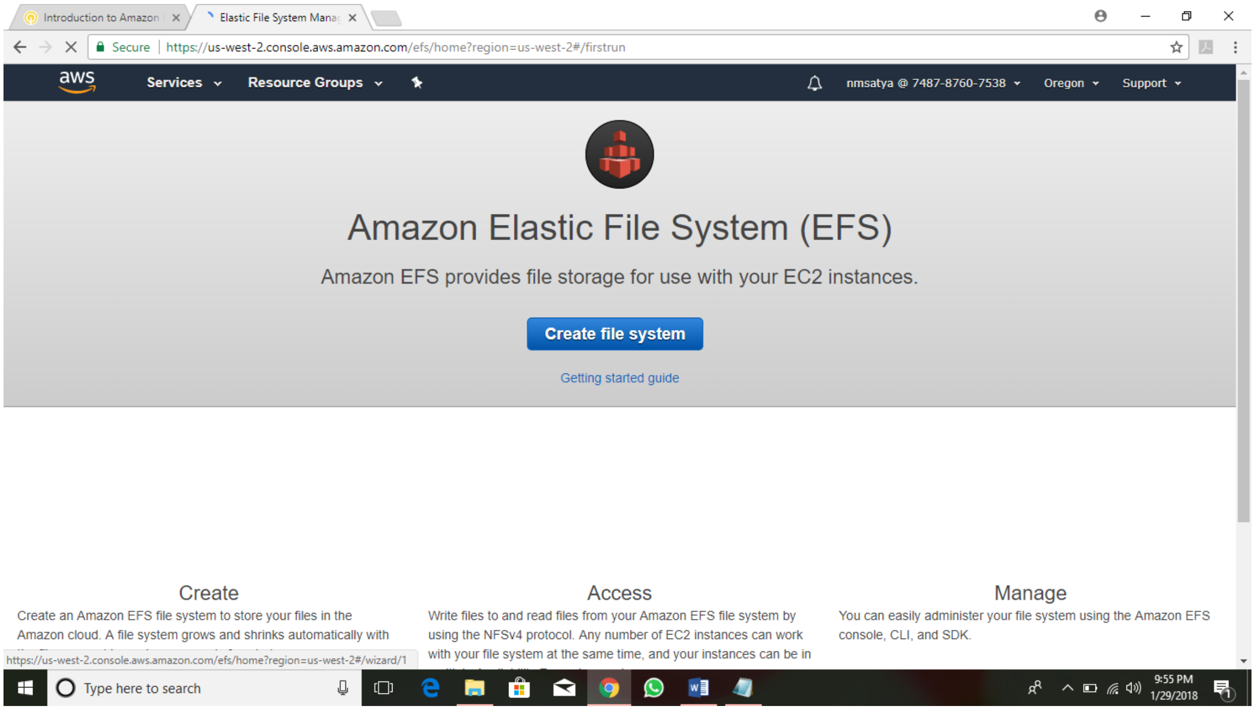
Type	Protocol	Port Range	Source		Description
NFS	TCP	2049	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

Task-2 – Create an Amazon EFS File System

Go to Services and select EFS



Create File System



Amazon Elastic File System (EFS)

Amazon EFS provides file storage for use with your EC2 instances.

Create

Create an Amazon EFS file system to store your files in the Amazon cloud. A file system grows and shrinks automatically with

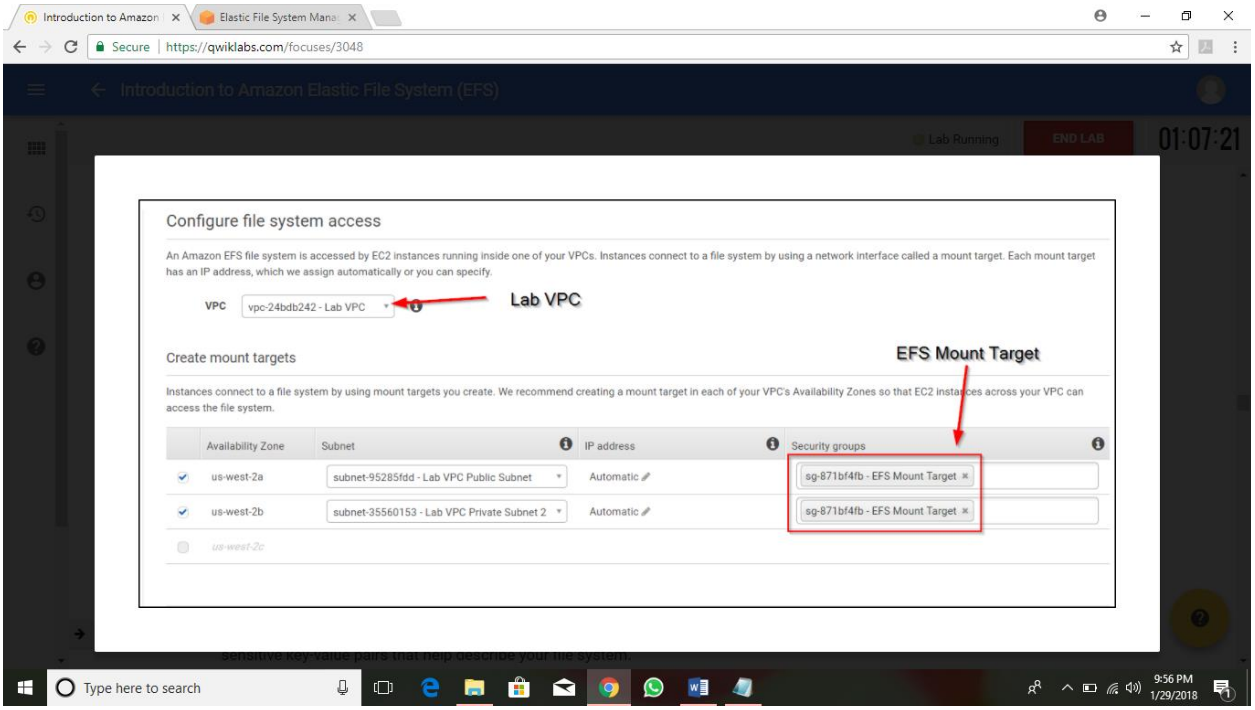
Access

Write files to and read files from your Amazon EFS file system by using the NFSv4 protocol. Any number of EC2 instances can work with your file system at the same time, and your instances can be in

Manage

You can easily administer your file system using the Amazon EFS console, CLI, and SDK.

Select VPC and configure our security group EFS mount Target



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.

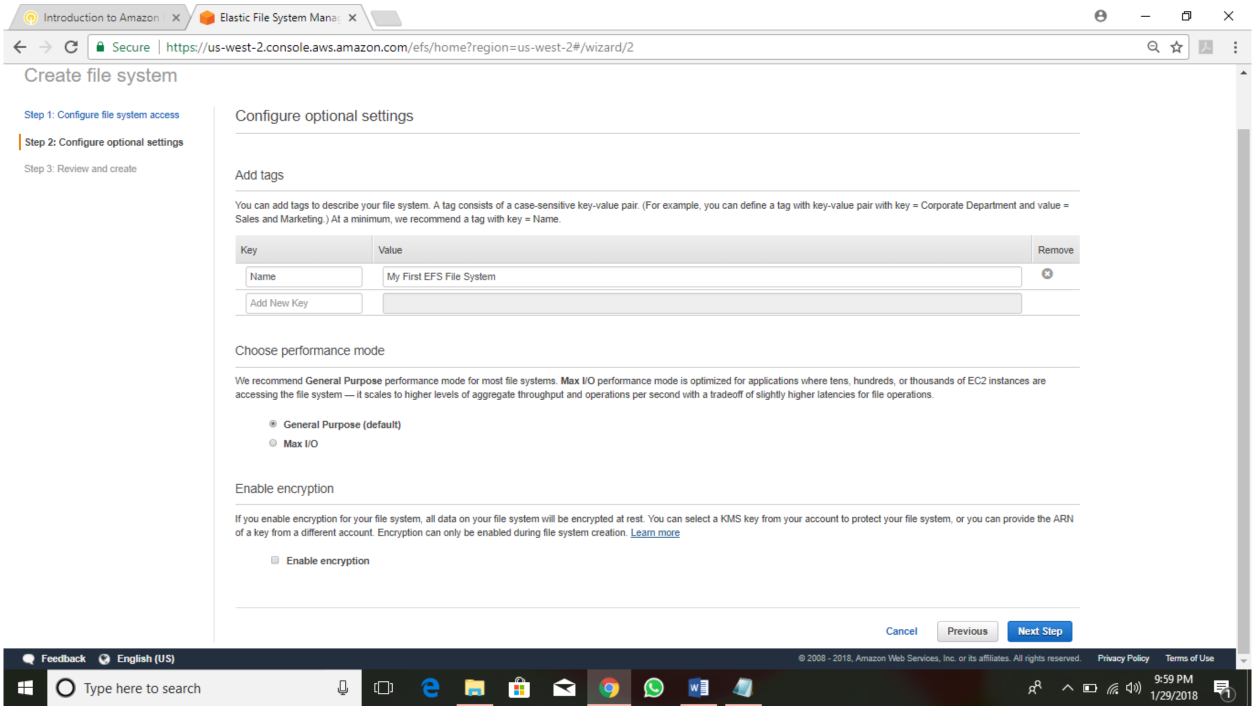
VPC: vpc-24bdb242 - Lab VPC

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-95285fdd - Lab VPC Public Subnet	Automatic	sg-871bf4fb - EFS Mount Target
☑	us-west-2b	subnet-35560153 - Lab VPC Private Subnet 2	Automatic	sg-871bf4fb - EFS Mount Target
□	us-west-2c			

Click Next



Introduction to Amazon
Elastic File System Mana
Secure
https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#/wizard/2
Cancel
Previous
Next Step
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Type here to search
9:59 PM
1/29/2018

Create file system

Step 1: Configure file system access
Step 2: Configure optional settings
Step 3: Review and create

Configure optional settings

Add tags

You can add tags to describe your file system. A tag consists of a case-sensitive key-value pair. (For example, you can define a tag with key-value pair with key = Corporate Department and value = Sales and Marketing.) At a minimum, we recommend a tag with key = Name.

Key	Value	Remove
Name	My First EFS File System	⊗
Add New Key		

Choose performance mode

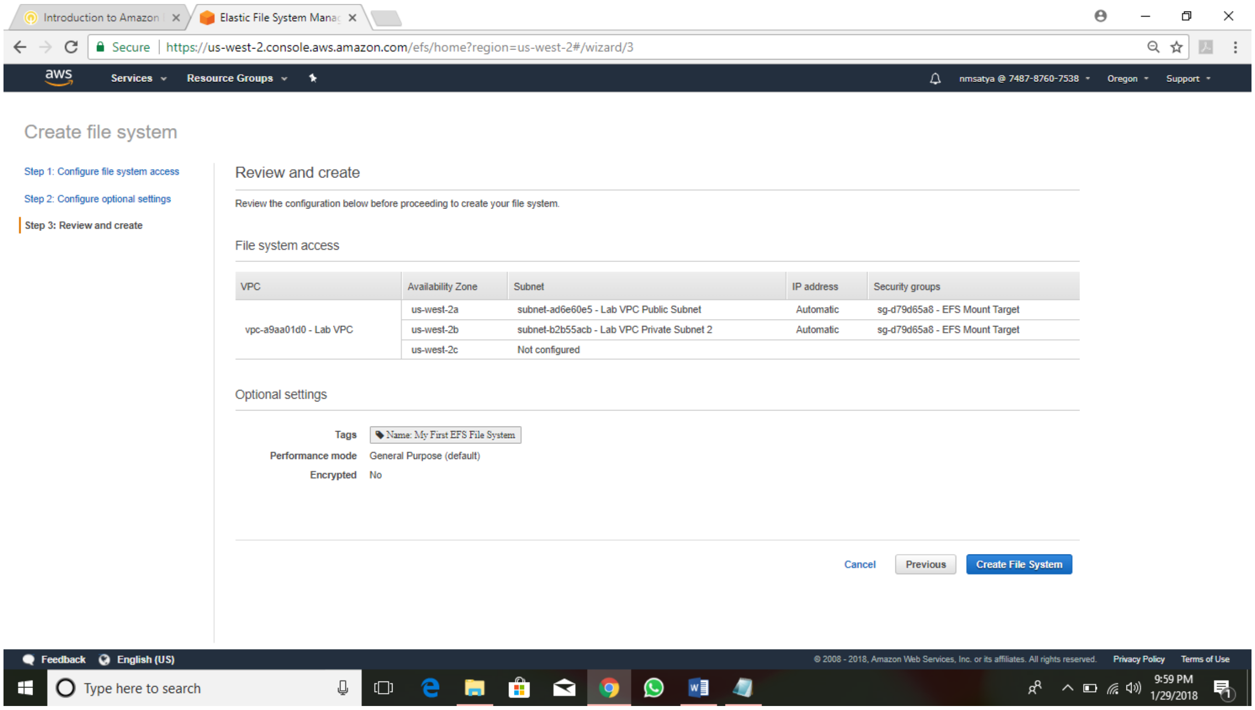
We recommend **General Purpose** performance mode for most file systems. **Max I/O** performance mode is optimized for applications where tens, hundreds, or thousands of EC2 instances are accessing the file system — it scales to higher levels of aggregate throughput and operations per second with a tradeoff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

□ Enable encryption


Introduction to Amazon
Elastic File System Manag
Secure
https://us-west-2.console.aws.amazon.com/efs/home?region=us-west-2#/wizard/3
aws
Services
Resource Groups
nmsatya @ 7487-8760-7538
Oregon
Support

Create file system

Step 1: Configure file system access

Step 2: Configure optional settings

Step 3: Review and create

Review and create

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

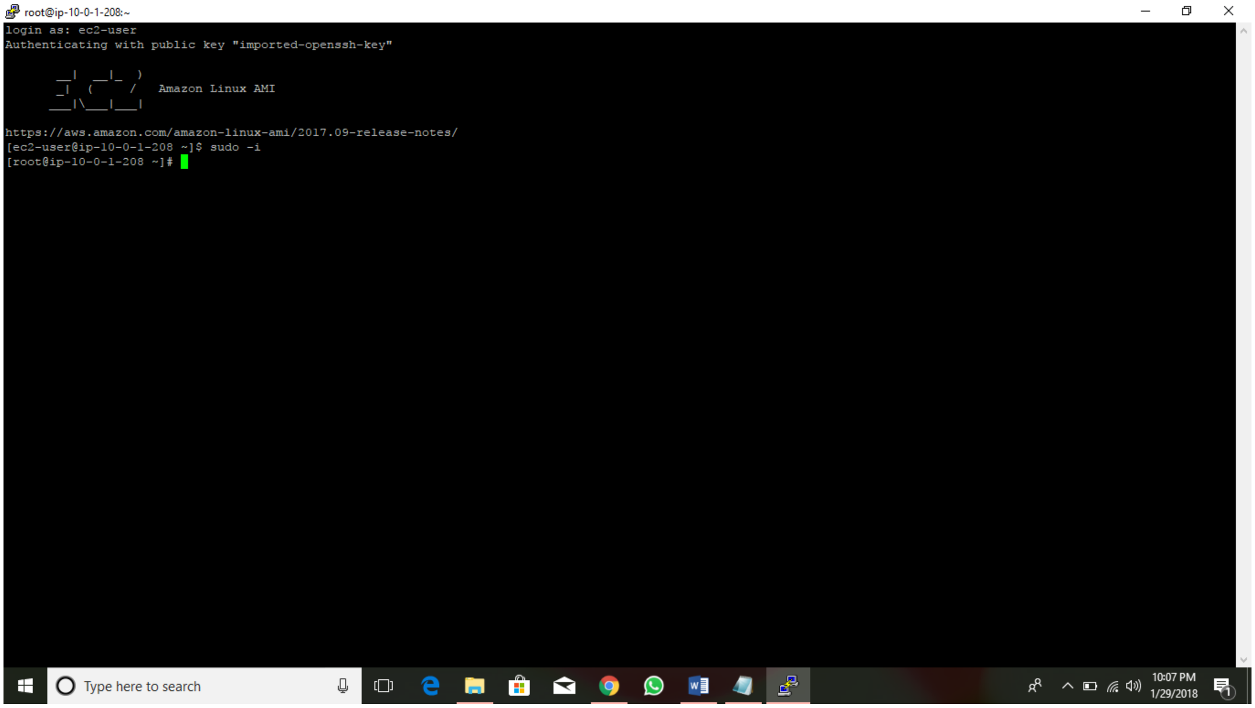
File system access

VPC	Availability Zone	Subnet	IP address	Security groups
vpc-a9aa01d0 - Lab VPC	us-west-2a	subnet-ad6e60e5 - Lab VPC Public Subnet	Automatic	sg-d79d65a8 - EFS Mount Target
	us-west-2b	subnet-b2b55acb - Lab VPC Private Subnet 2	Automatic	sg-d79d65a8 - EFS Mount Target
	us-west-2c	Not configured		

Optional settings

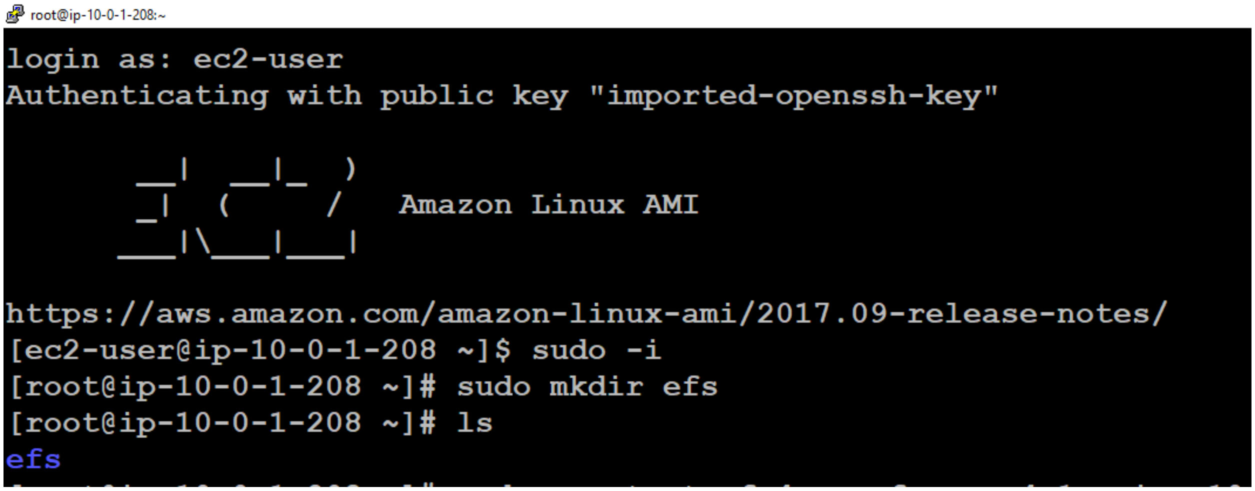
Tags	Name: My First EFS File System
Performance mode	General Purpose (default)
Encrypted	No

Task -3 Connect a Linux instance via putty as-usual

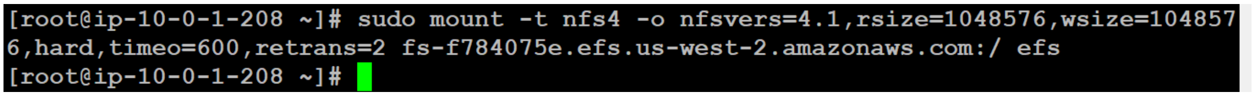


```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-10-0-1-208 ~]$ sudo -i
[root@ip-10-0-1-208 ~]#
```

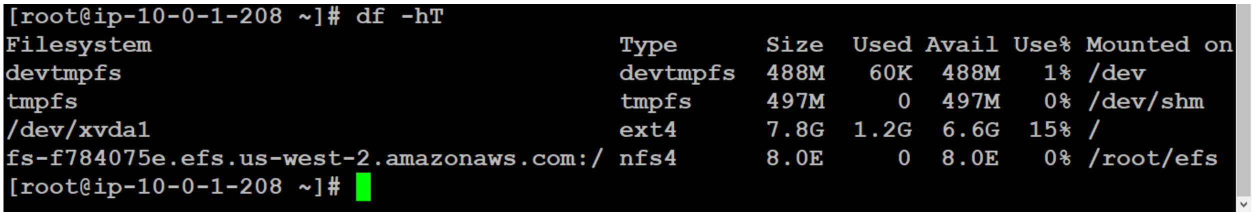
Task -4 Create a New Directory And Mount the EFS File System.



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
[ec2-user@ip-10-0-1-208 ~]$ sudo -i
[root@ip-10-0-1-208 ~]# sudo mkdir efs
[root@ip-10-0-1-208 ~]# ls
efs
```



```
[root@ip-10-0-1-208 ~]# sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=104857
6,hard,timeo=600,retrans=2 fs-f784075e.efs.us-west-2.amazonaws.com:/ efs
[root@ip-10-0-1-208 ~]#
```



```
[root@ip-10-0-1-208 ~]# df -hT
Filesystem                                 Type      Size  Used Avail Use% Mounted on
devtmpfs                                   devtmpfs  488M   60K  488M   1% /dev
tmpfs                                      tmpfs     497M     0  497M   0% /dev/shm
/dev/xvda1                                 ext4      7.8G  1.2G  6.6G  15% /
fs-f784075e.efs.us-west-2.amazonaws.com:/ nfs4      8.0E     0  8.0E   0% /root/efs
[root@ip-10-0-1-208 ~]#
```

Examine The Performance Behavior Of Your New EFS File System

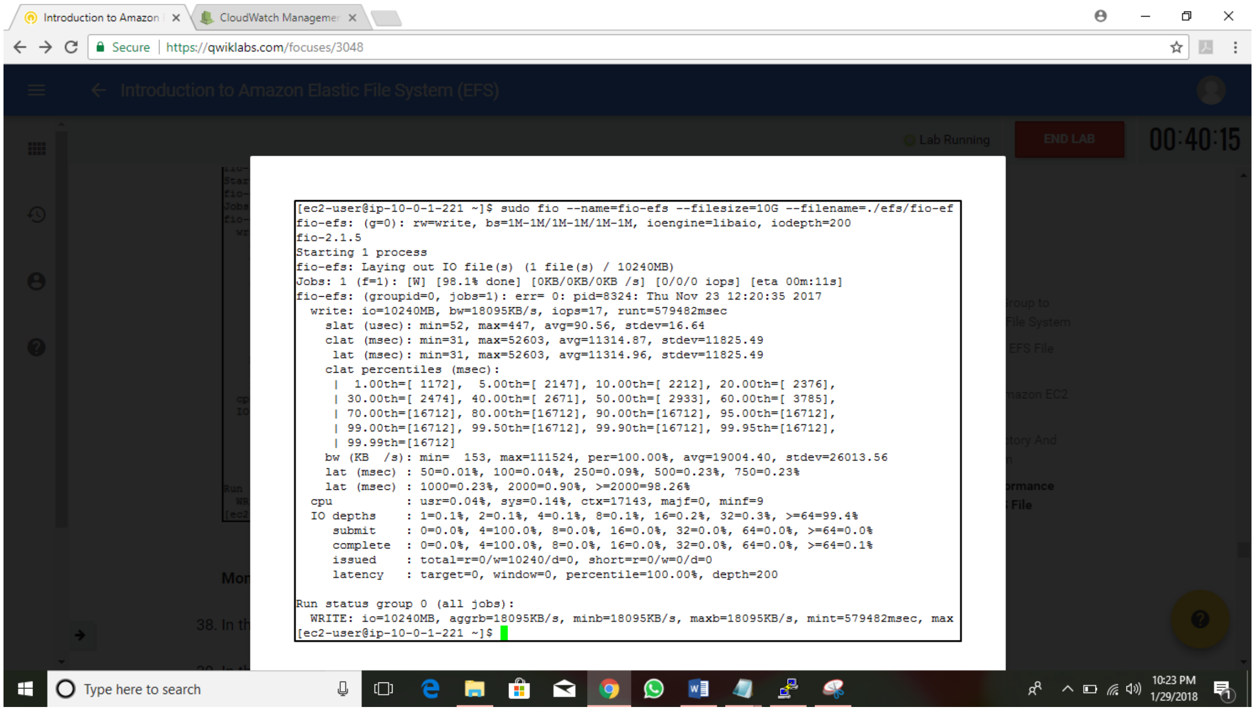
Examine Performance Using Flexible IO

Flexible IO (fio) is a synthetic IO benchmarking utility for Linux which is used to benchmark and test Linux IO subsystems. *Fio* was automatically installed on your EC2 instance during boot.

37. 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 a 3-5 minutes to complete and the output should look something like the screenshot below. Please examine the output of your *fio*command, specifically the summary status information for this WRITE test.



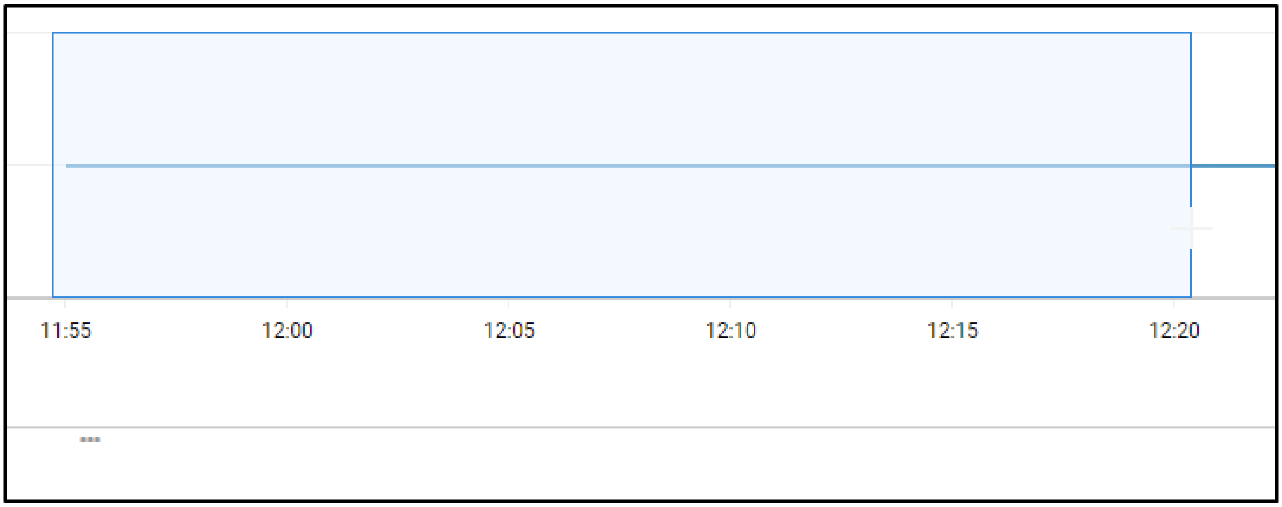
```
[ec2-user@ip-10-0-1-221 ~]$ sudo fio --name=fio-efs --filesize=10G --filename=./efs/fio-ef
fio-efs: (g=0): rw=write, bs=1M-1M/1M-1M/1M-1M, ioengine=libaio, iodepth=200
fio-2.1.5
Starting 1 process
fio-efs: Laying out IO file(s) (1 file(s) / 10240MB)
Jobs: 1 (f=1): [W] [98.1% done] [0KB/0KB/0KB /s] [0/0/0 iops] [eta 00m:11s]
fio-efs: (groupid=0, jobs=1): err= 0: pid=8324: Thu Nov 23 12:20:35 2017
  write: io=10240MB, bw=18095KB/s, iops=17, runt=579482msec
    slat (usec): min=52, max=447, avg=90.56, stdev=16.64
    clat (msec): min=31, max=52603, avg=11314.87, stdev=11825.49
     lat (msec): min=31, max=52603, avg=11314.96, stdev=11825.49
    clat percentiles (msec):
     |  1.00th=[ 1172],  5.00th=[ 2147], 10.00th=[ 2212], 20.00th=[ 2376],
     | 30.00th=[ 2474], 40.00th=[ 2671], 50.00th=[ 2933], 60.00th=[ 3785],
     | 70.00th=[16712], 80.00th=[16712], 90.00th=[16712], 95.00th=[16712],
     | 99.00th=[16712], 99.50th=[16712], 99.90th=[16712], 99.95th=[16712],
     | 99.99th=[16712]
    bw (KB  /s): min=  153, max=111524, per=100.00%, avg=19004.40, stdev=26013.56
    lat (msec) : 50=0.01%, 100=0.04%, 250=0.09%, 500=0.23%, 750=0.23%
    lat (msec) : 1000=0.23%, 2000=0.90%, >=2000=98.26%
  cpu          : usr=0.04%, sys=0.14%, ctx=17143, majf=0, minf=9
  IO depths    : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.2%, 32=0.3%, >=64=99.4%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%, >=64=0.1%
     issued    : total=r=0/w=10240/d=0, short=r=0/w=0/d=0
     latency   : target=0, window=0, percentile=100.00%, depth=200

Run status group 0 (all jobs):
  WRITE: io=10240MB, aggrb=18095KB/s, minb=18095KB/s, maxb=18095KB/s, mint=579482msec, max
[ec2-user@ip-10-0-1-221 ~]$
```

Monitor Performance using Cloud Watch

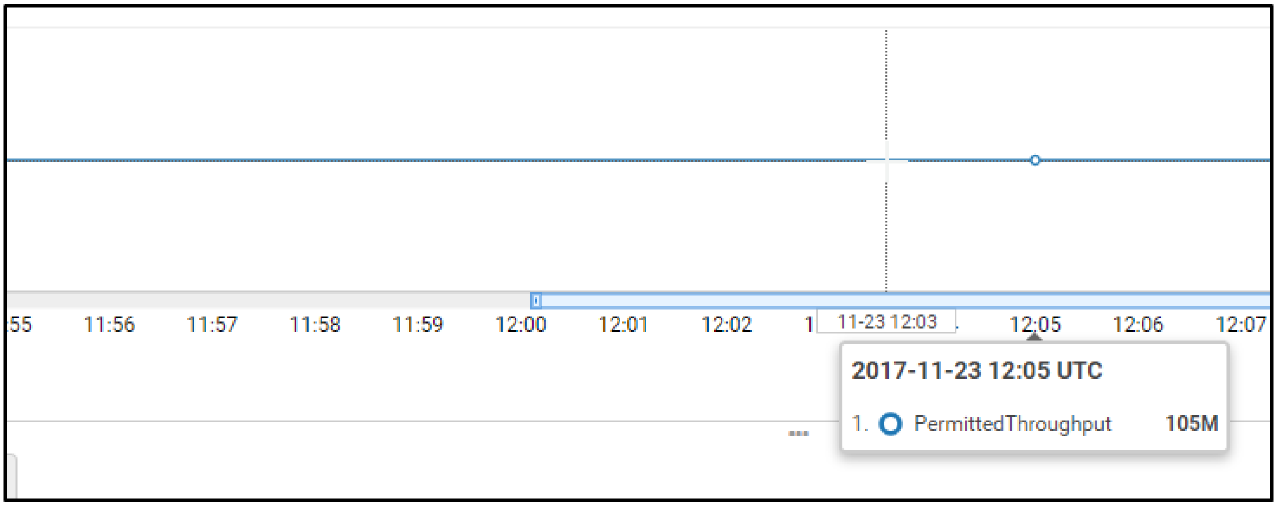
38. In the **AWS Management Console**, on the **Services** menu, click **CloudWatch**.
39. In the navigation pane on the left, click **Metrics**.
40. In the **All metrics** tab, click **EFS**.
41. Click **File System Metrics**.
42. Check the **FileSystemID** for **PermittedThroughput**.

you may need to wait 2-3 minutes and refresh the screen several times for all the available metrics, including **PermittedThroughput**, to calculate and populate.

43. On the graph above, click and drag (up or down) the line just above the elipsis mark **...** to adjust the size of the pane.



44. Hover your mouse over the data line in the graph. The value should be 105M.



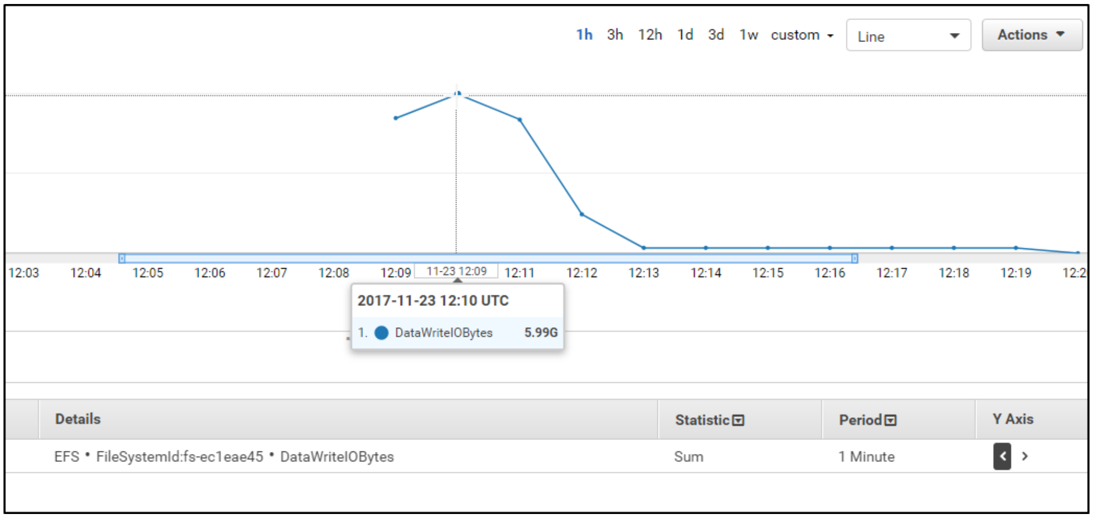
2017-11-23 12:05 UTC

1. ○ PermittedThroughput 105M

Throughput of Amazon EFS scales as the file system grows. Because file-based workloads are typically spiky, driving high levels of throughput for short periods of time and low levels of throughput the rest of the time, 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 http://docs.aws.amazon.com/efs/latest/ug/performance.html.

45. Uncheck the **FileSystemID** for **PermittedThroughput**.
46. Check the **FileSystemID** for **DataWriteIOBytes**.
47. Click the **Graphed metrics** tab.
48. On the **Statistics** column, select **Sum**.

49. On the **Period** column, select **1 Minute**.
50. Hover over the peak of the line graph. Take this number (in bytes) and divide it by the duration in seconds (60 seconds). This will give you the write throughput (B/s) of your file system during your test.



2017-11-23 12:10 UTC
1. ● DataWriteIOBytes 5.99G

Details	Statistic	Period	Y Axis
EFS • FileSystemId:fs-ec1eae45 • DataWriteIOBytes	Sum	1 Minute	‹ ›

The throughput 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 and all file systems (regardless of size) can burst to 100 MiB/s. File systems larger than 1TB can burst to 100 MiB/s per TiB of storage. As you add data to your file system, the maximum throughput available to the file system scales linearly and automatically with your storage.

File system throughput is shared across all Amazon EC2 instances connected to a file system. For example, a 1 TiB file system that can burst to 100 MiB/s of throughput can drive 100 MiB/s from a single Amazon EC2 instance, or 10 Amazon EC2 instances can collectively drive 100 MiB/s. For more information about performance characteristics of your EFS file system.

Cloud Trial - Auditing

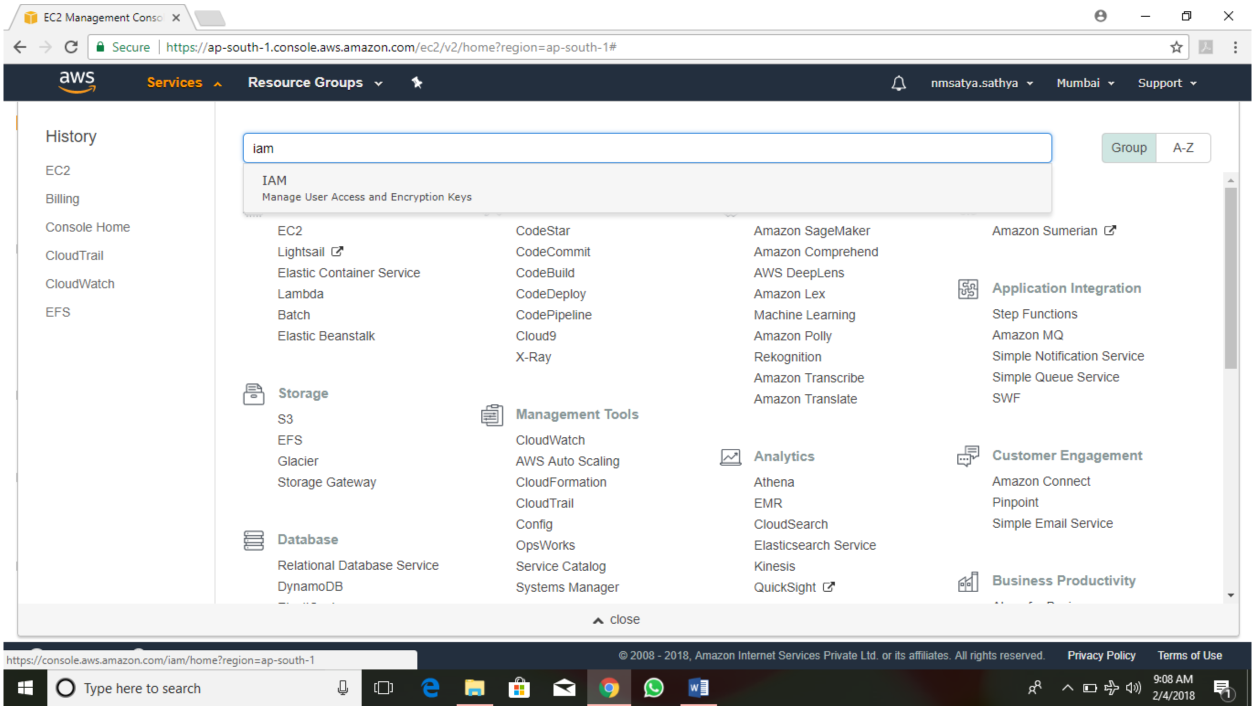
AWS cloud trial to get history of AWS API calls and related events for your account. This history includes calls made with the AWS management console, AWS CLI, AWS SDK's and other AWS services. It is a logging service from AWS.

IAM

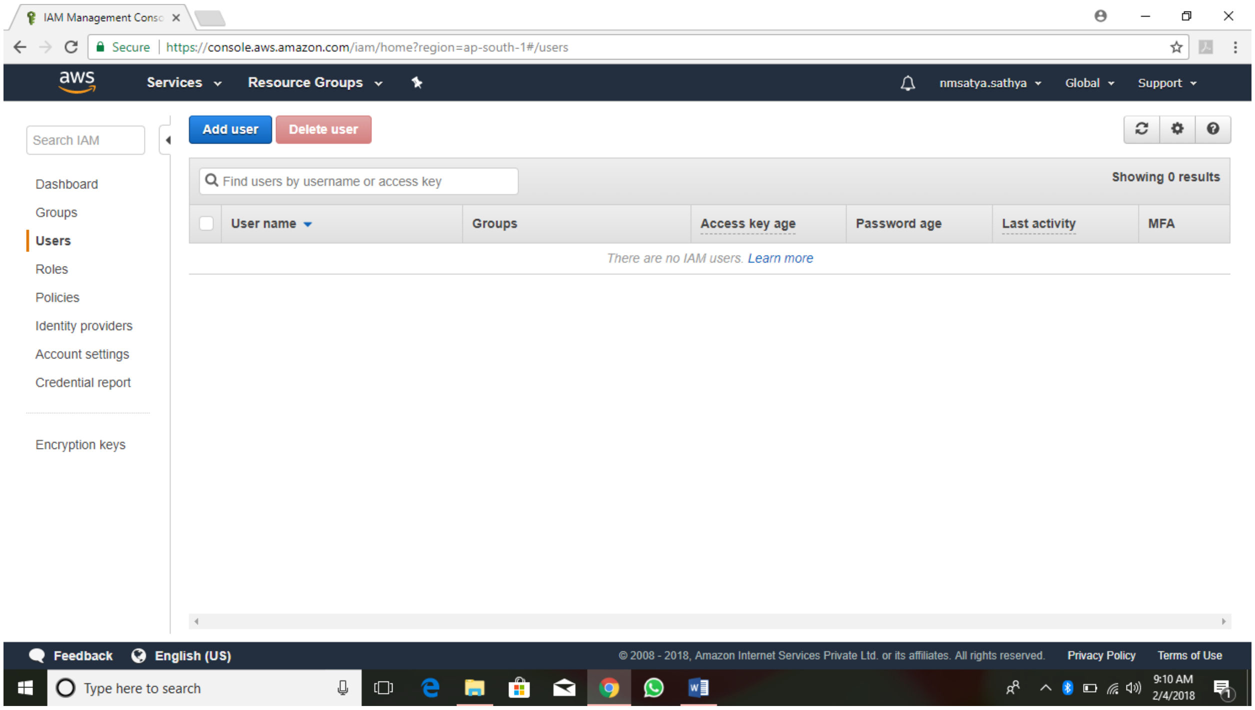
Identity and Access Management

LAB –

Search from console IAM and click



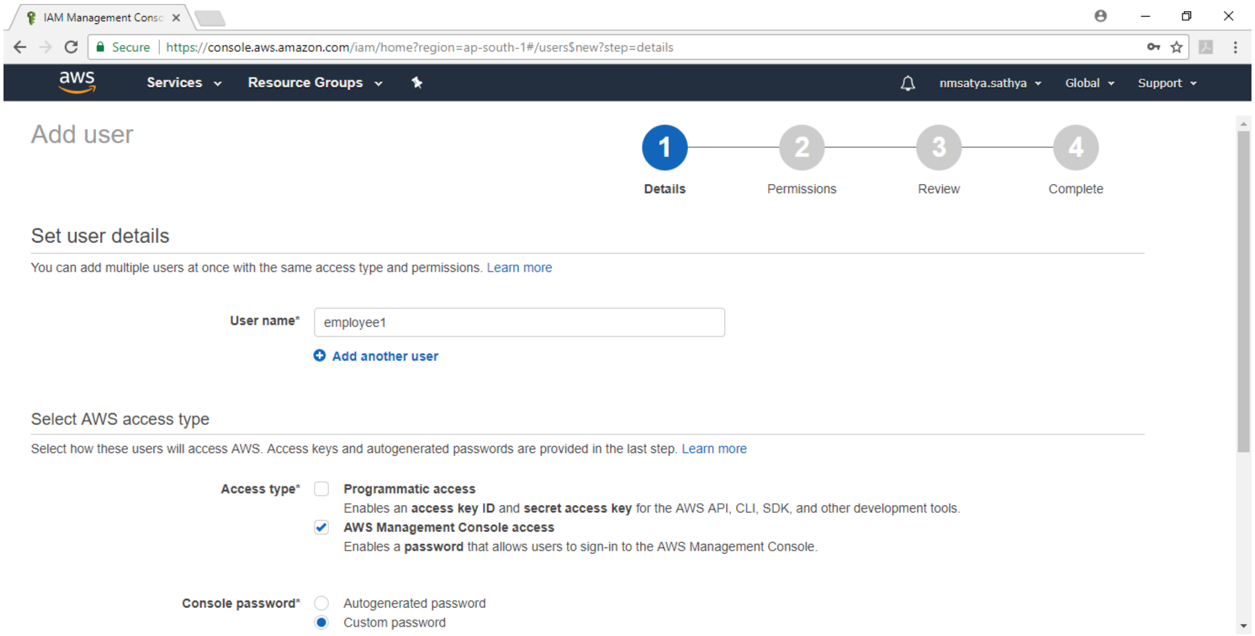
Create a New User



User name	Groups	Access key age	Password age	Last activity	MFA

There are no IAM users. Learn more

Select Access Type – AWS management Console Acess and select custom password



Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

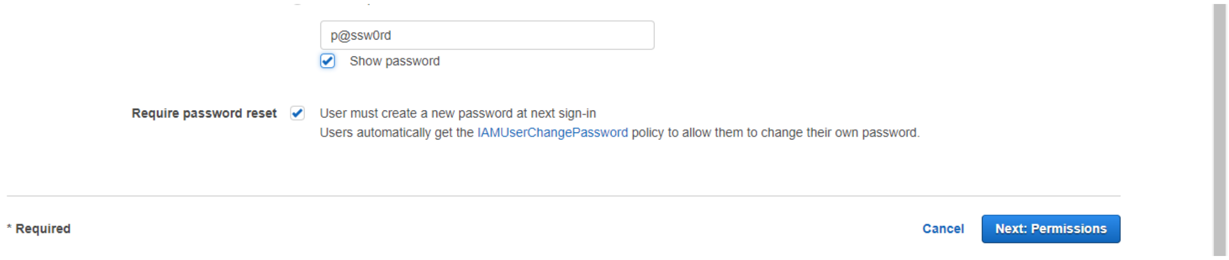
User name* employee1

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

Access type* □ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
☑ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password



p@ssw0rd

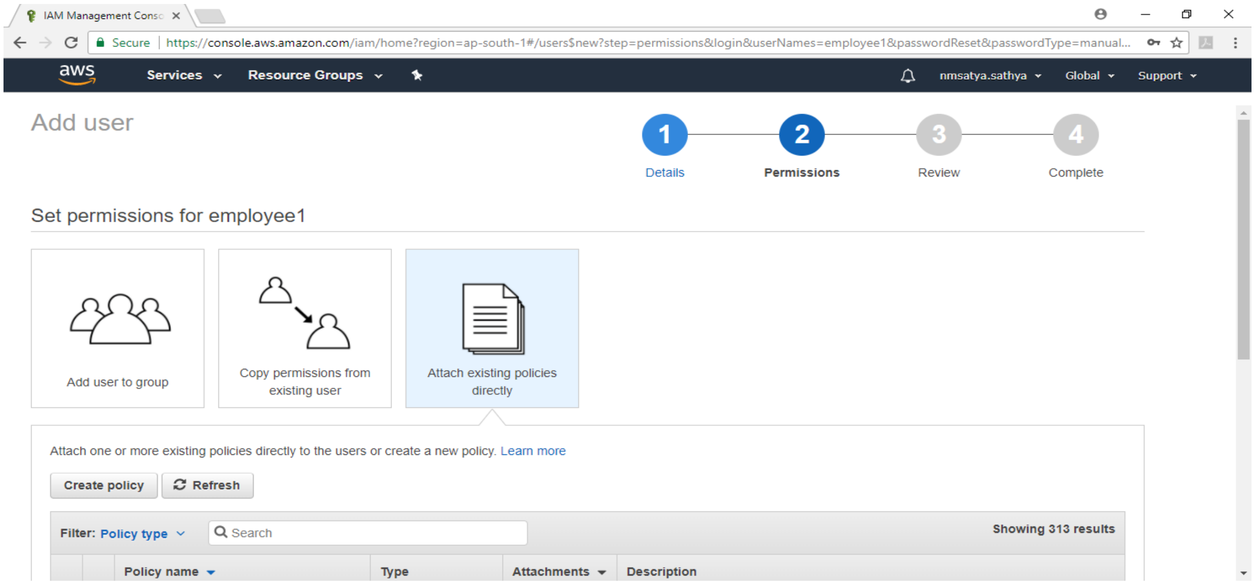
☑ Show password

Require password reset ☑ User must create a new password at next sign-in

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

Go the next option and select attach existing Policies if you want copy permission from existing user in this case let me choose attach existing policies directly



IAM Management Conso

Secure | https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=permissions&login&userNames=employee1&passwordReset&passwordType=manual...

Add user

Set permissions for employee1

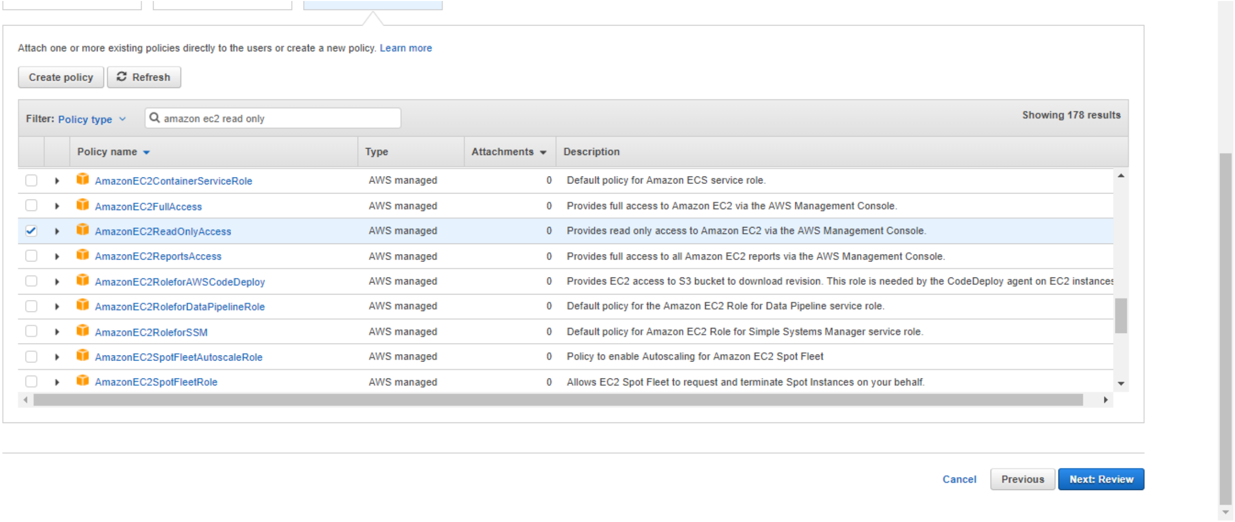
Add user to group
Copy permissions from existing user
Attach existing policies directly

Attach one or more existing policies directly to the users or create a new policy. Learn more

Filter: Policy type Search Showing 313 results

		Policy name	Type	Attachments	Description

Select a role employee1 what can access, I choose AmazonEC2ReadOnlyAccess

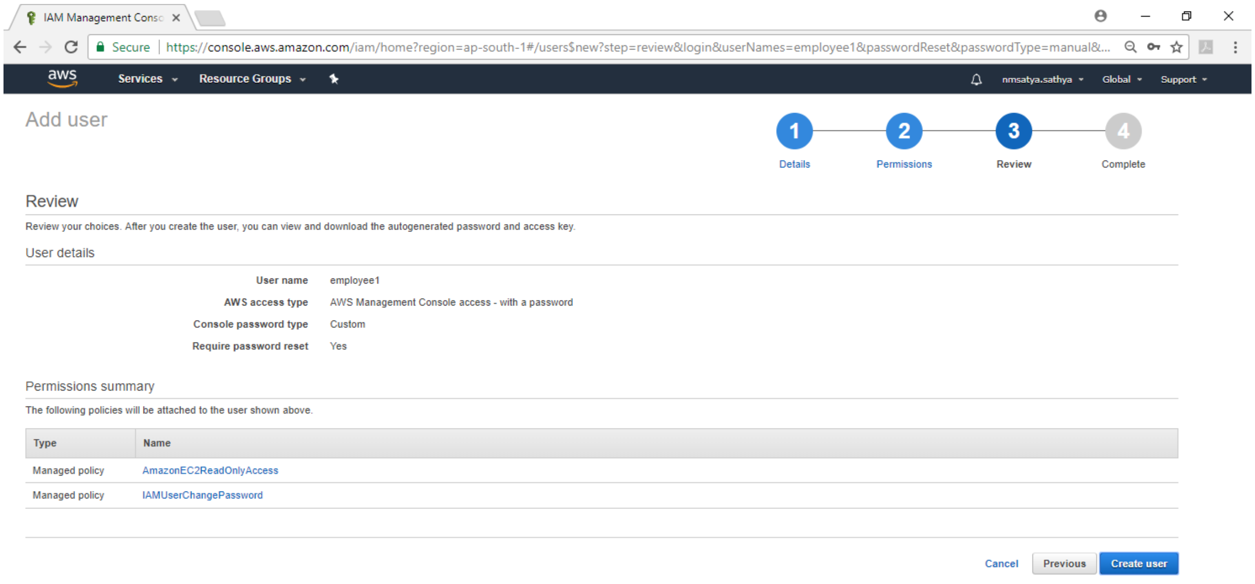


Attach one or more existing policies directly to the users or create a new policy. Learn more

Filter: Policy type amazon ec2 read only Showing 178 results

		Policy name	Type	Attachments	Description
□	▸	AmazonEC2ContainerServiceRole	AWS managed	0	Default policy for Amazon ECS service role.
□	▸	AmazonEC2FullAccess	AWS managed	0	Provides full access to Amazon EC2 via the AWS Management Console.
☑	▸	AmazonEC2ReadOnlyAccess	AWS managed	0	Provides read only access to Amazon EC2 via the AWS Management Console.
□	▸	AmazonEC2ReportsAccess	AWS managed	0	Provides full access to all Amazon EC2 reports via the AWS Management Console.
□	▸	AmazonEC2RoleforAWSCodeDeploy	AWS managed	0	Provides EC2 access to S3 bucket to download revision. This role is needed by the CodeDeploy agent on EC2 instances
□	▸	AmazonEC2RoleforDataPipelineRole	AWS managed	0	Default policy for the Amazon EC2 Role for Data Pipeline service role.
□	▸	AmazonEC2RoleforSSM	AWS managed	0	Default policy for Amazon EC2 Role for Simple Systems Manager service role.
□	▸	AmazonEC2SpotFleetAutoscaleRole	AWS managed	0	Policy to enable Autoscaling for Amazon EC2 Spot Fleet
□	▸	AmazonEC2SpotFleetRole	AWS managed	0	Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

Create a user and finish


IAM Management Conso
Secure
https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=review&login&userNames=employee1&passwordReset&passwordType=manual&...
aws
Services
Resource Groups
nmsatya.sathya
Global
Support

Add user

1 Details
2 Permissions
3 Review
4 Complete

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

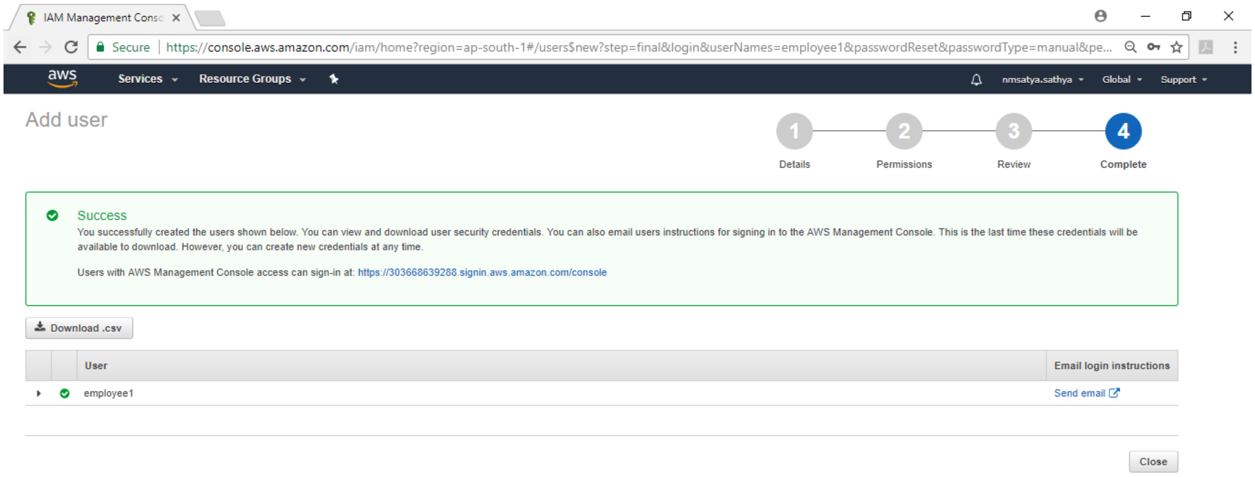
User name	employee1
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	Yes

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonEC2ReadOnlyAccess
Managed policy	IAMUserChangePassword

Once you create a user you can see the URL below screenshot share this url to employee1


IAM Management Conso
Secure
https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=final&login&userNames=employee1&passwordReset&passwordType=manual&pe...
aws
Services
Resource Groups
nmsatya.sathya
Global
Support

Add user

1 Details
2 Permissions
3 Review
4 Complete

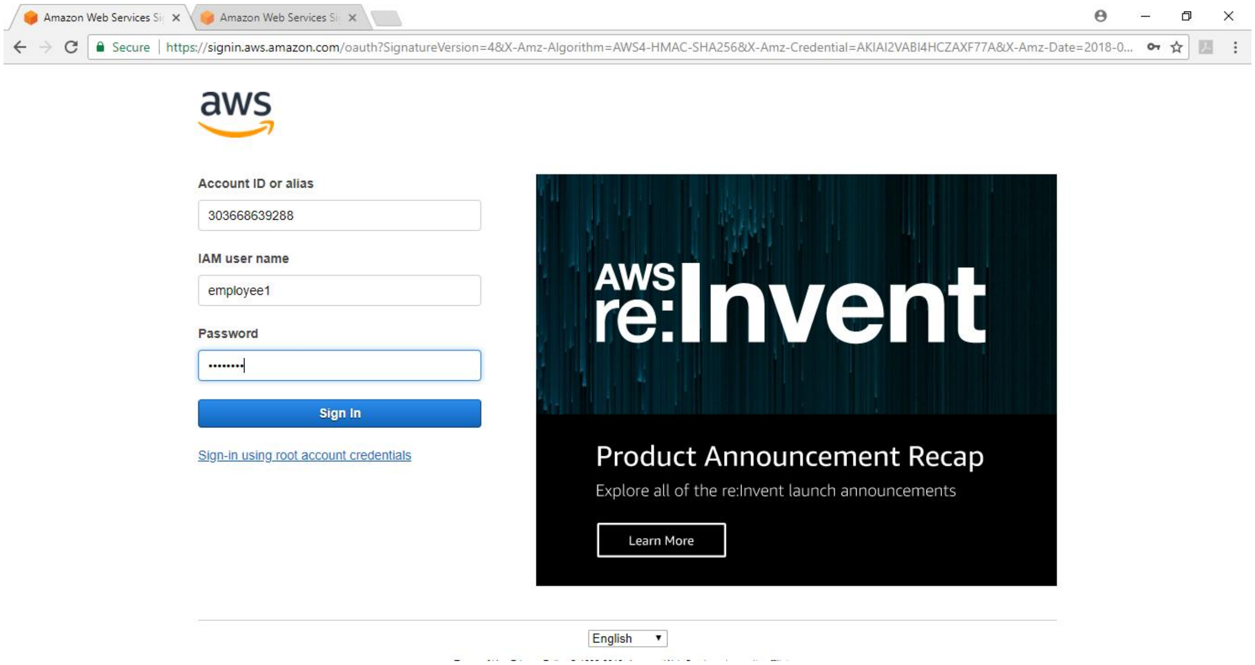
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://303668639288.signin.aws.amazon.com/console

		User	Email login instructions
▸	✓	employee1	Send email

Now employee1 can login and change the password and login


Amazon Web Services Si
Amazon Web Services Si
Secure

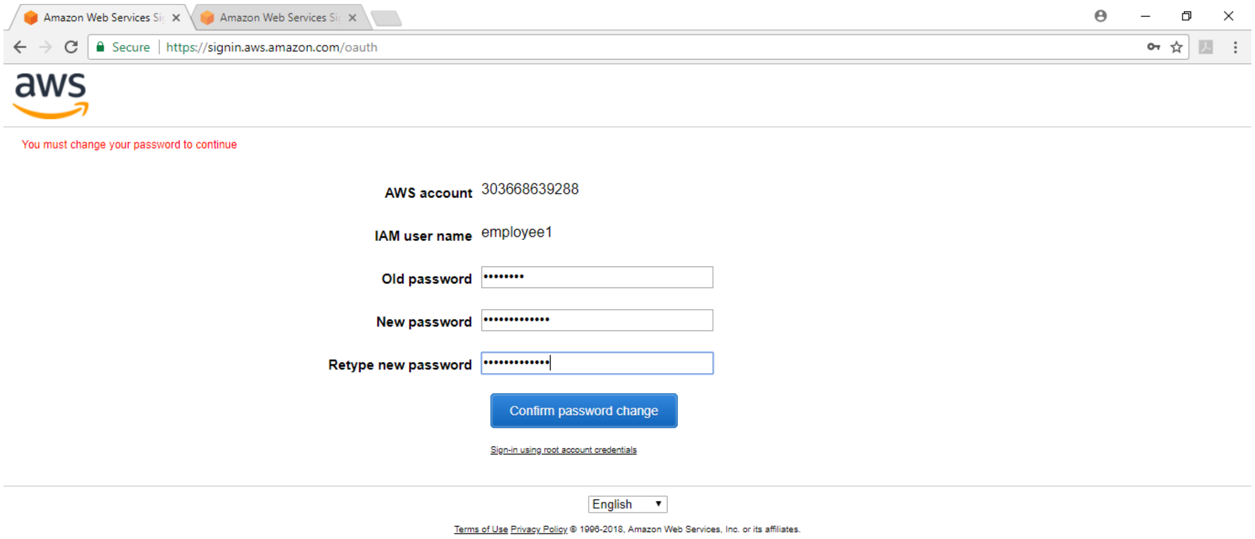
https://signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAI2VABI4HCZAXF77A&X-Amz-Date=2018-0...

Account ID or alias: 303668639288

IAM user name: employee1

Password: ••••••••

Sign In
Sign-in using root account credentials
AWS re:Invent
Product Announcement Recap
Explore all of the re:Invent launch announcements
Learn More
English



https://signin.aws.amazon.com/oauth

You must change your password to continue

AWS account: 303668639288

IAM user name: employee1

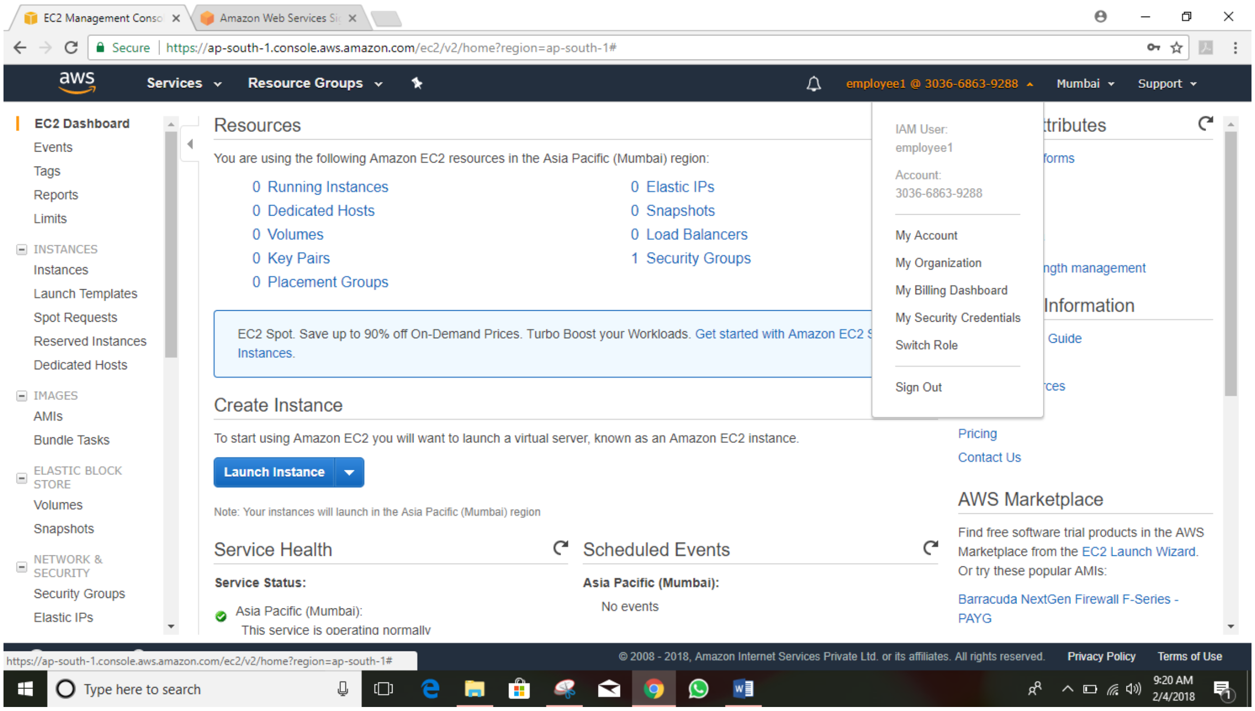
Old password: ••••••••

New password: •••••••••••••

Retype new password: •••••••••••••

Terms of Use Privacy Policy © 1996-2018, Amazon Web Services, Inc. or its affiliates.

After Login see the user account is employee1



Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) region:

0 Running Instances
0 Dedicated Hosts
0 Volumes
0 Key Pairs
0 Placement Groups
0 Elastic IPs
0 Snapshots
0 Load Balancers
1 Security Groups

EC2 Spot. Save up to 90% off On-Demand Prices. Turbo Boost your Workloads. Get started with Amazon EC2 S Instances.

IAM User:
employee1

Account:
3036-6863-9288

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the Asia Pacific (Mumbai) region

Service Health

Service Status:

Asia Pacific (Mumbai):
This service is operating normally

Scheduled Events

Asia Pacific (Mumbai):
No events

AWS Marketplace

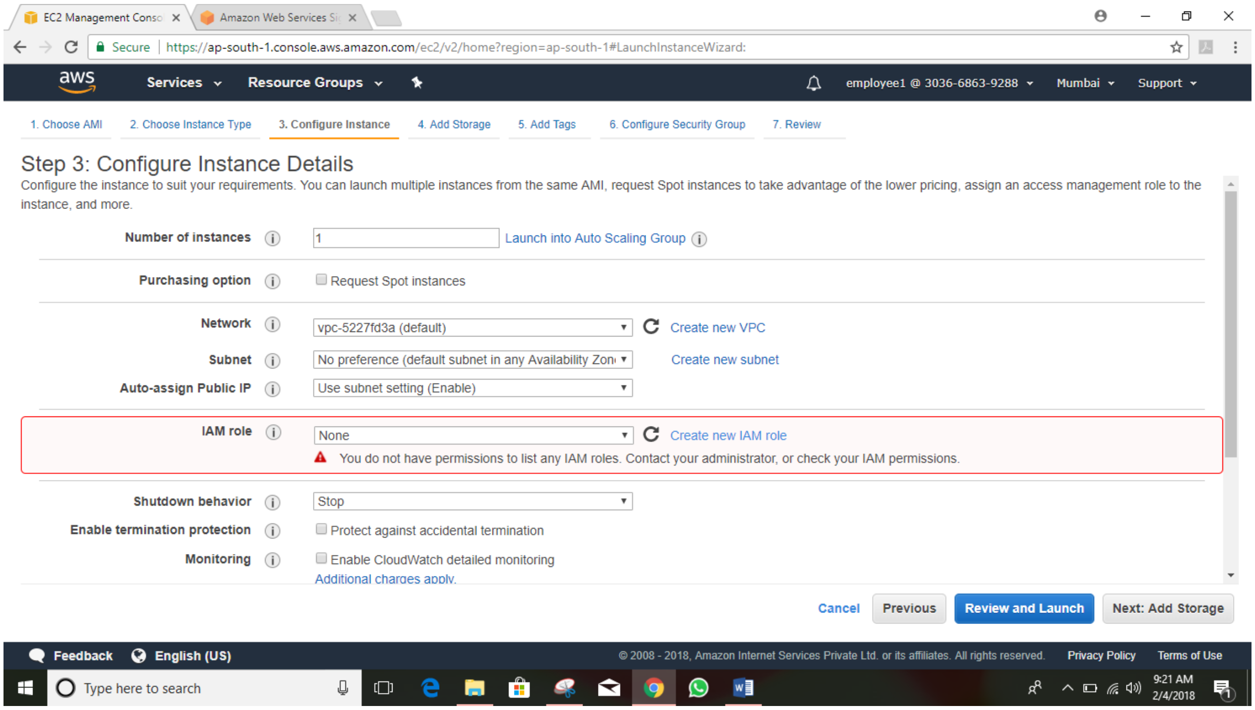
Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard.
Or try these popular AMIs:

Barracuda NextGen Firewall F-Series - PAYG

https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

<u>See the result you cant create any instanse / any other services.</u>



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: □ Request Spot instances

Network: vpc-5227fd3a (default)

Subnet: No preference (default subnet in any Availability Zon

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: None

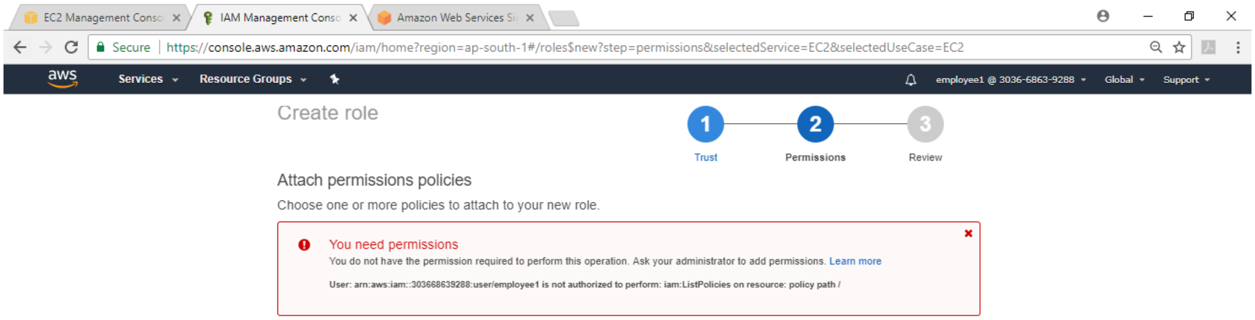
⚠ You do not have permissions to list any IAM roles. Contact your administrator, or check your IAM permissions.

Shutdown behavior: Stop

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.


EC2 Management Conso
IAM Management Conso
Amazon Web Services Si
Secure
https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles$new?step=permissions&selectedService=EC2&selectedUseCase=EC2
aws
Services
Resource Groups
employee1 @ 3036-6863-9288
Global
Support
1
Trust
2
Permissions
3
Review

Create role

Attach permissions policies

Choose one or more policies to attach to your new role.

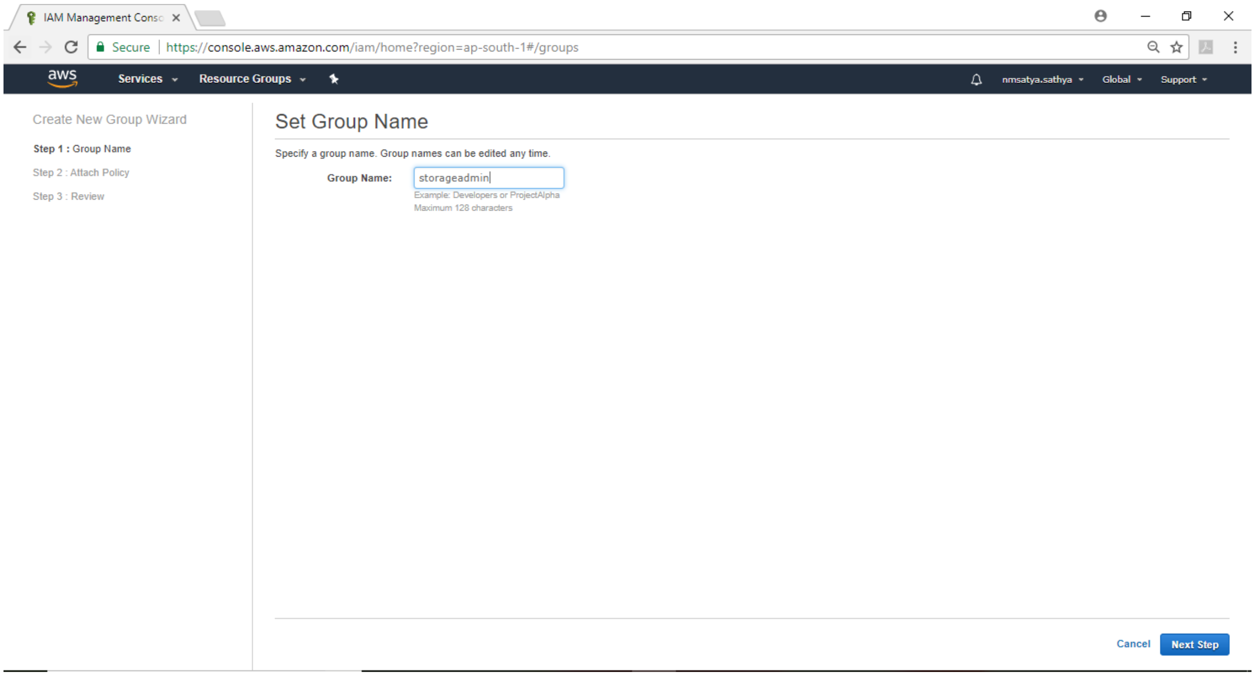
You need permissions

You do not have the permission required to perform this operation. Ask your administrator to add permissions. Learn more

User: arn:aws:iam::303668639288:user/employee1 is not authorized to perform: iam:ListPolicies on resource: policy path /

Now you can Cloud Trial Audit

Create a group from IAM



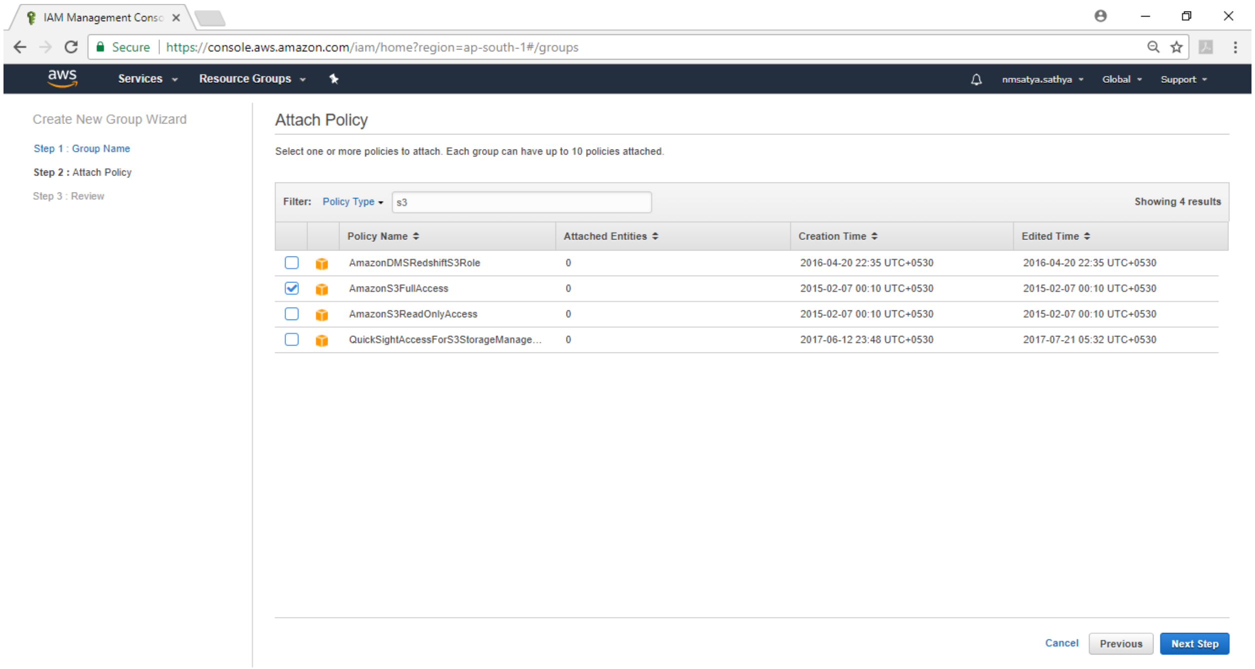
Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: storageadmin

Example: Developers or ProjectAlpha
Maximum 128 characters

Select the AmazonS3FullAccess and next step



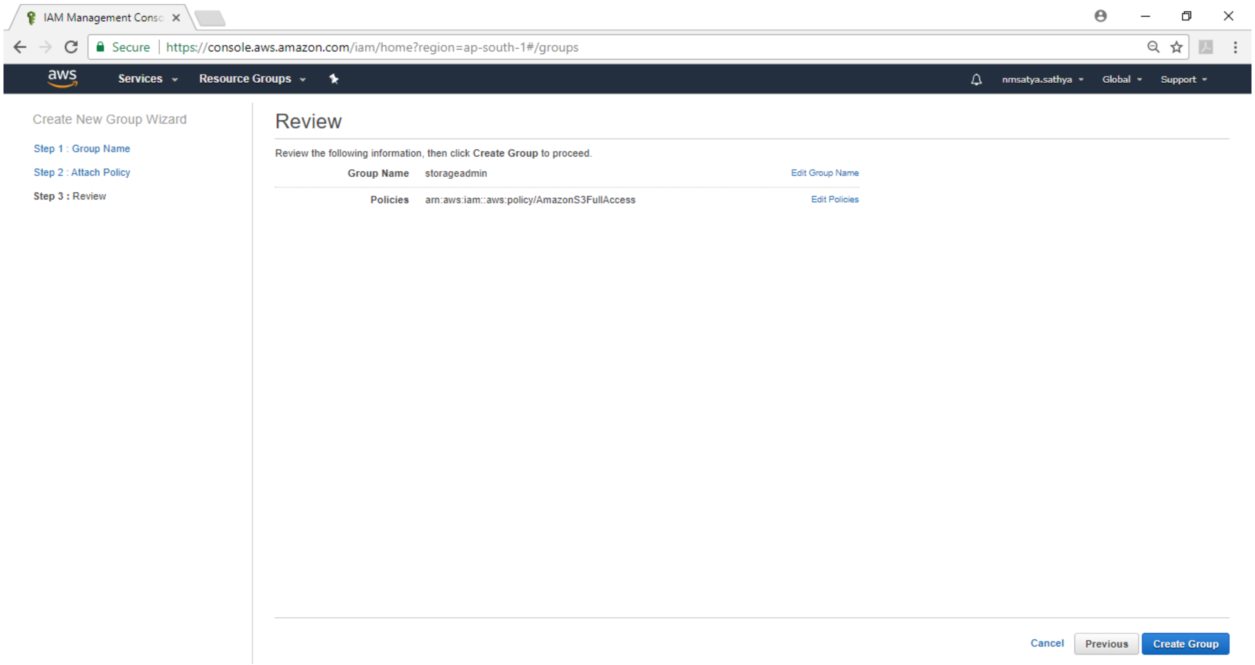
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type s3 Showing 4 results

	Policy Name	Attached Entities	Creation Time	Edited Time
□	AmazonDMSRedshiftS3Role	0	2016-04-20 22:35 UTC+0530	2016-04-20 22:35 UTC+0530
☑	AmazonS3FullAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
□	AmazonS3ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
□	QuickSightAccessForS3StorageManage...	0	2017-06-12 23:48 UTC+0530	2017-07-21 05:32 UTC+0530

Complete the step to create a group



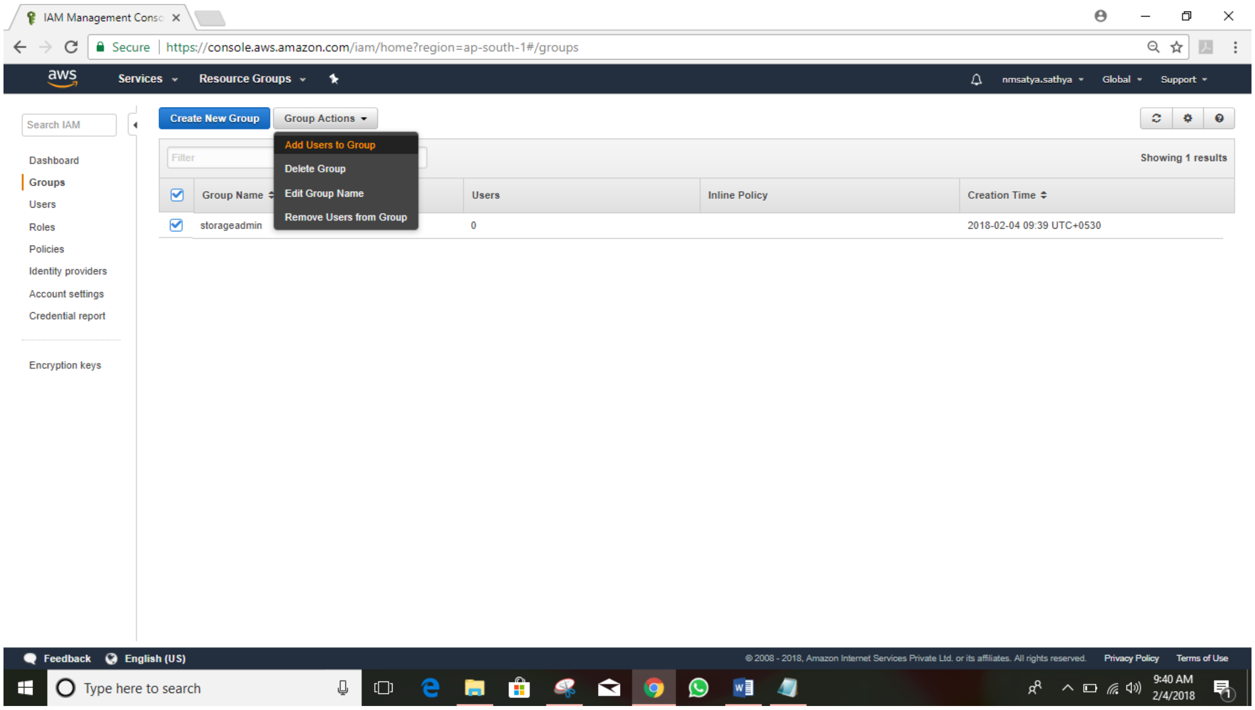
Review

Review the following information, then click **Create Group** to proceed.

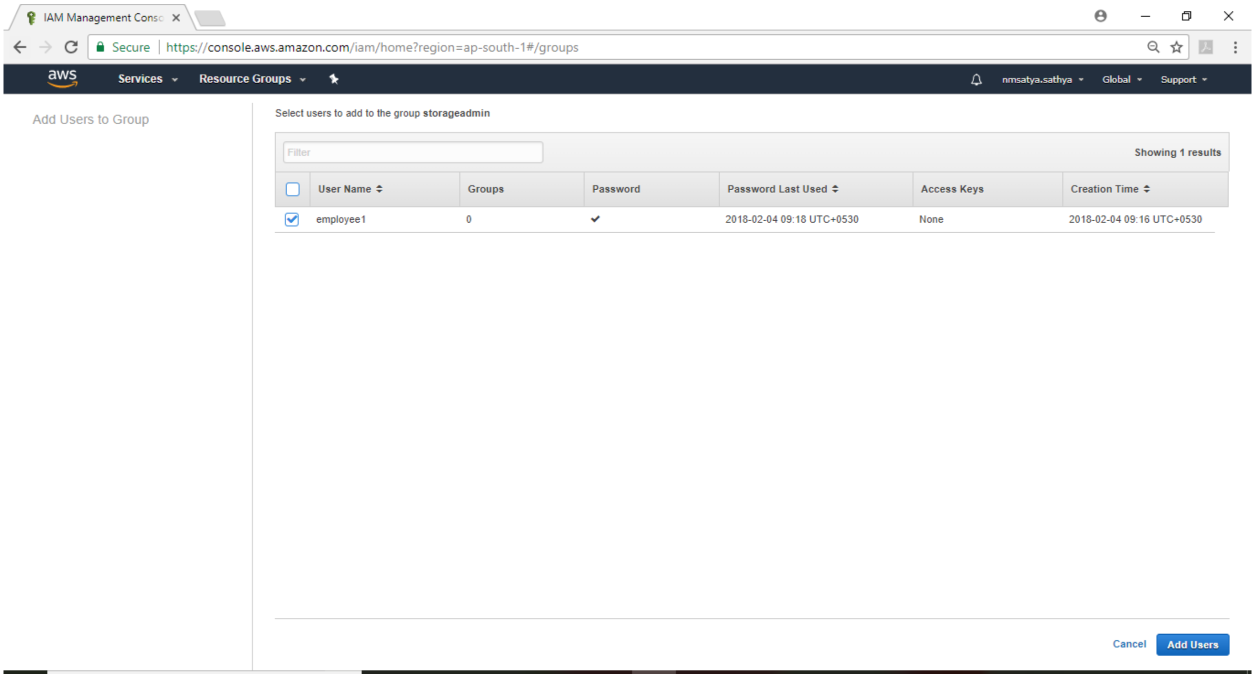
Group Name storageadmin

Policies arn:aws:iam::aws:policy/AmazonS3FullAccess

Click and select storage admin and go to Group Actions and select Add Users to Group



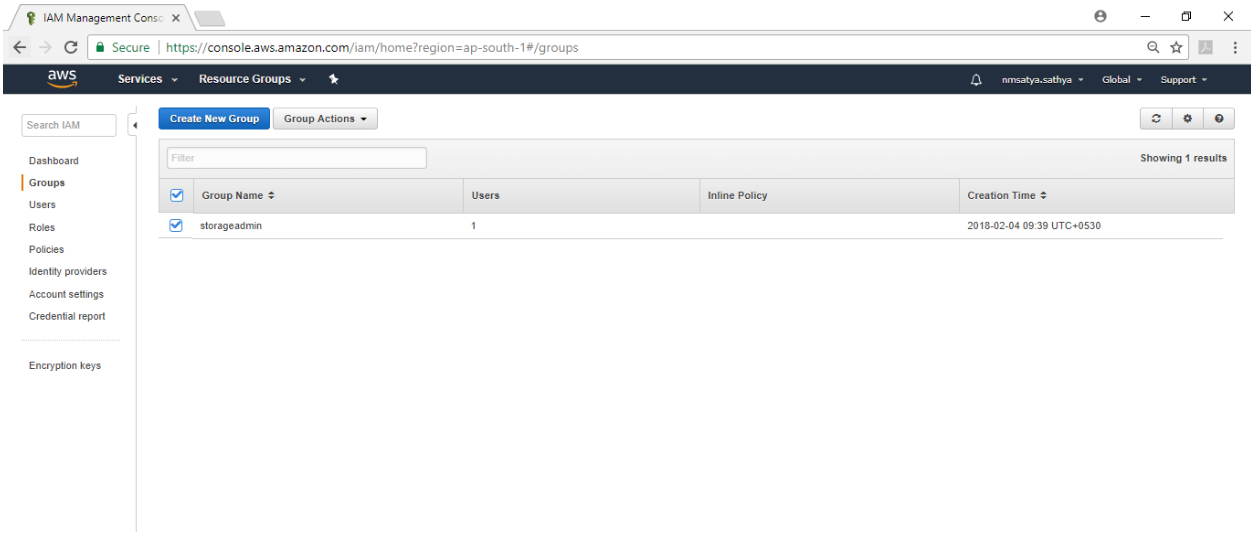
☑	Group Name	Users	Inline Policy	Creation Time
☑	storageadmin	0		2018-02-04 09:39 UTC+0530



Select users to add to the group storageadmin

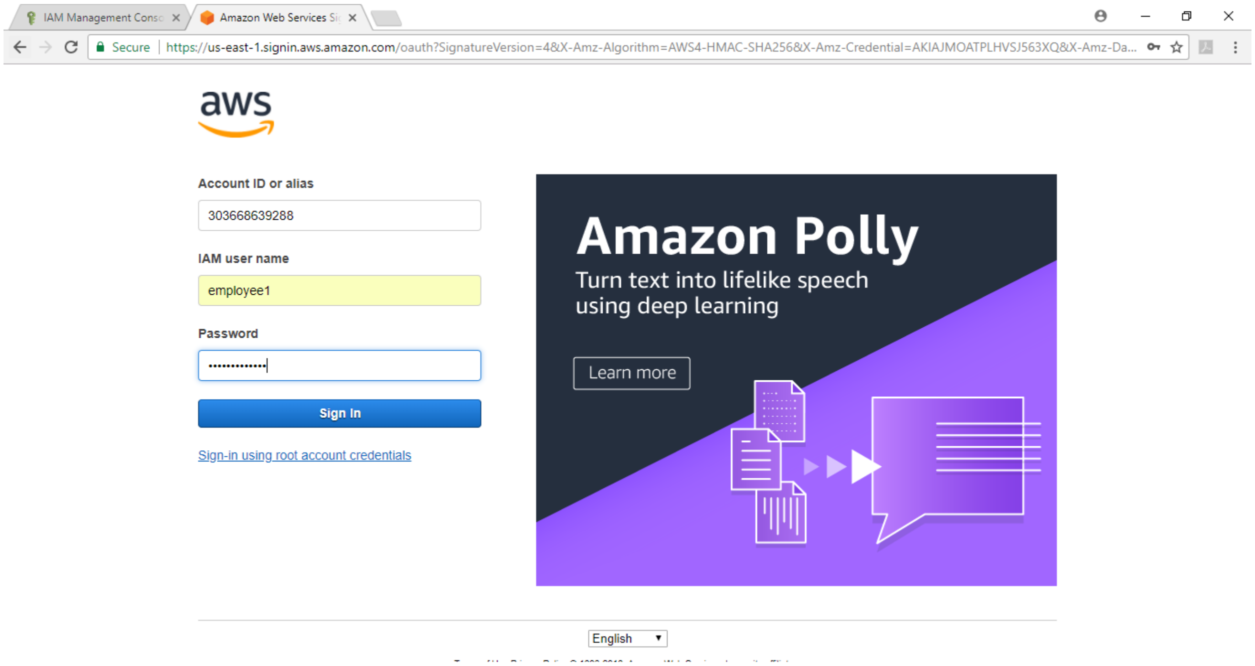
□	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
☑	employee1	0	✓	2018-02-04 09:18 UTC+0530	None	2018-02-04 09:16 UTC+0530

You can see now one users have visible



☑	Group Name	Users	Inline Policy	Creation Time
☑	storageadmin	1		2018-02-04 09:39 UTC+0530

Login again from employee1



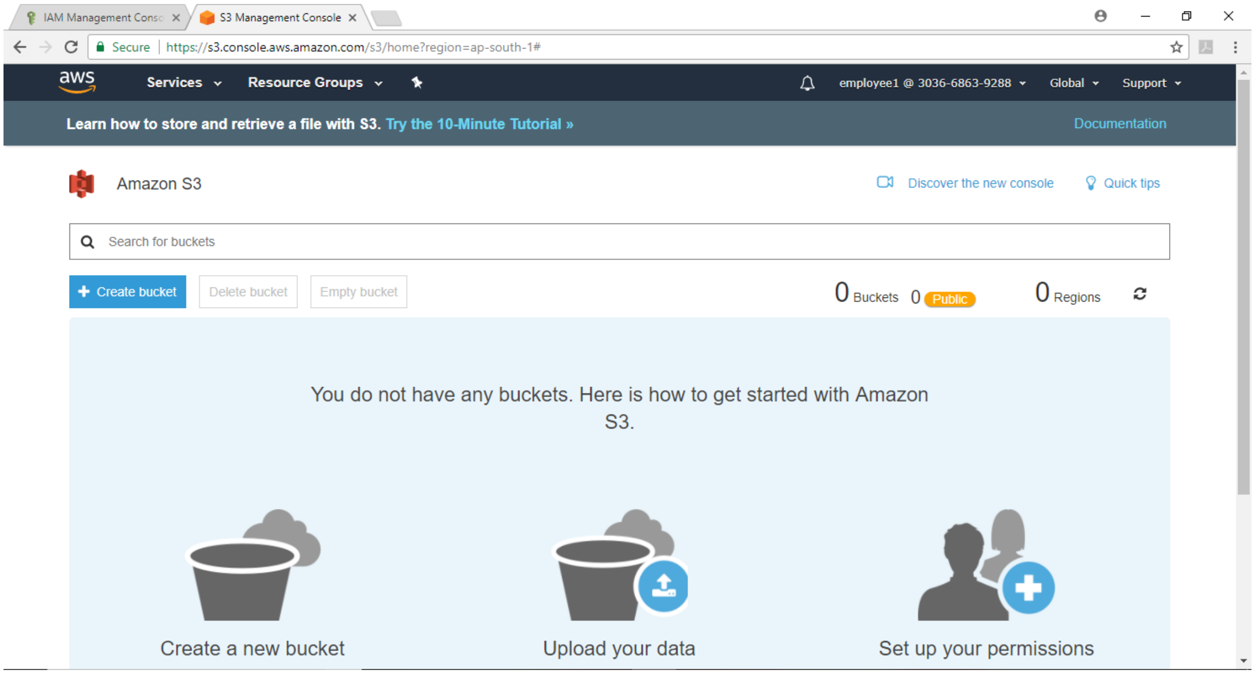
IAM Management Conso
Amazon Web Services Si
Secure
https://us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJMOATPLHVSJ563XQ&X-Amz-Da...
aws
Sign In
Sign-in using root account credentials
Amazon Polly
Turn text into lifelike speech using deep learning
Learn more
English

Account ID or alias
303668639288

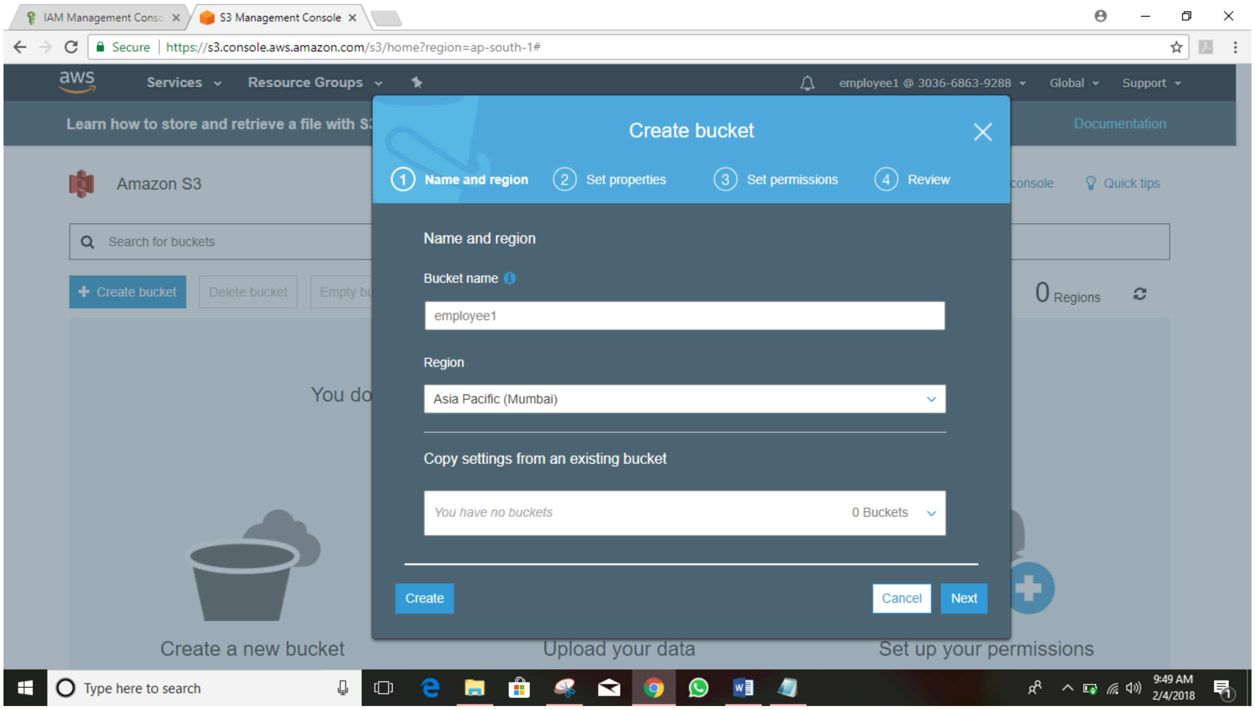
IAM user name
employee1

Password
•••••••••••••

Go to S3 and create a one bucket



You do not have any buckets. Here is how to get started with Amazon S3.



Create bucket

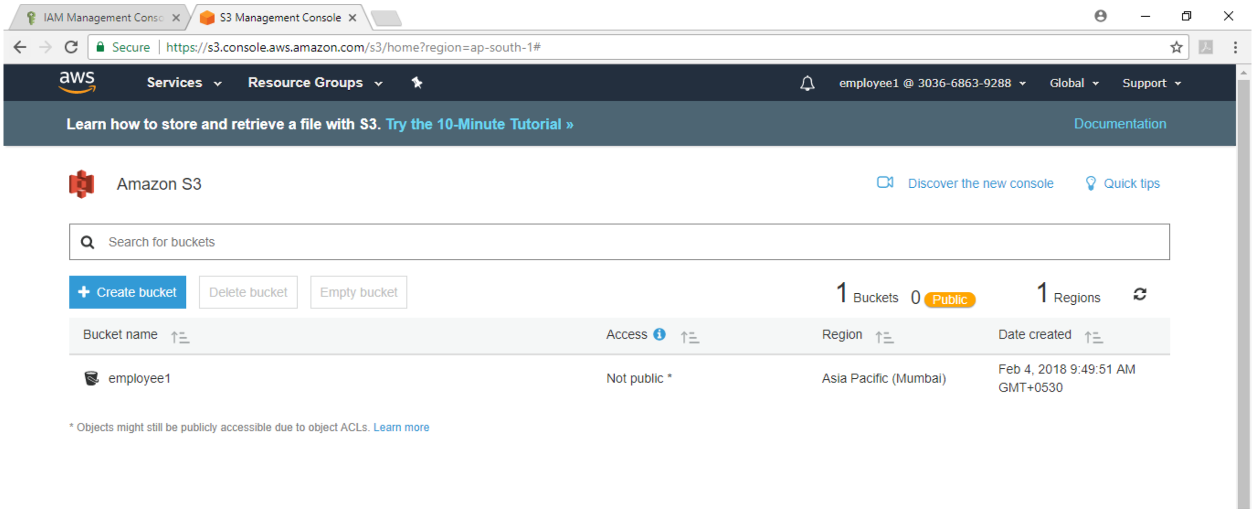
Name and region

Bucket name: employee1

Region: Asia Pacific (Mumbai)

Copy settings from an existing bucket: You have no buckets 0 Buckets

See now bucket are created because of full permission of s3 services given already to employee1 user.

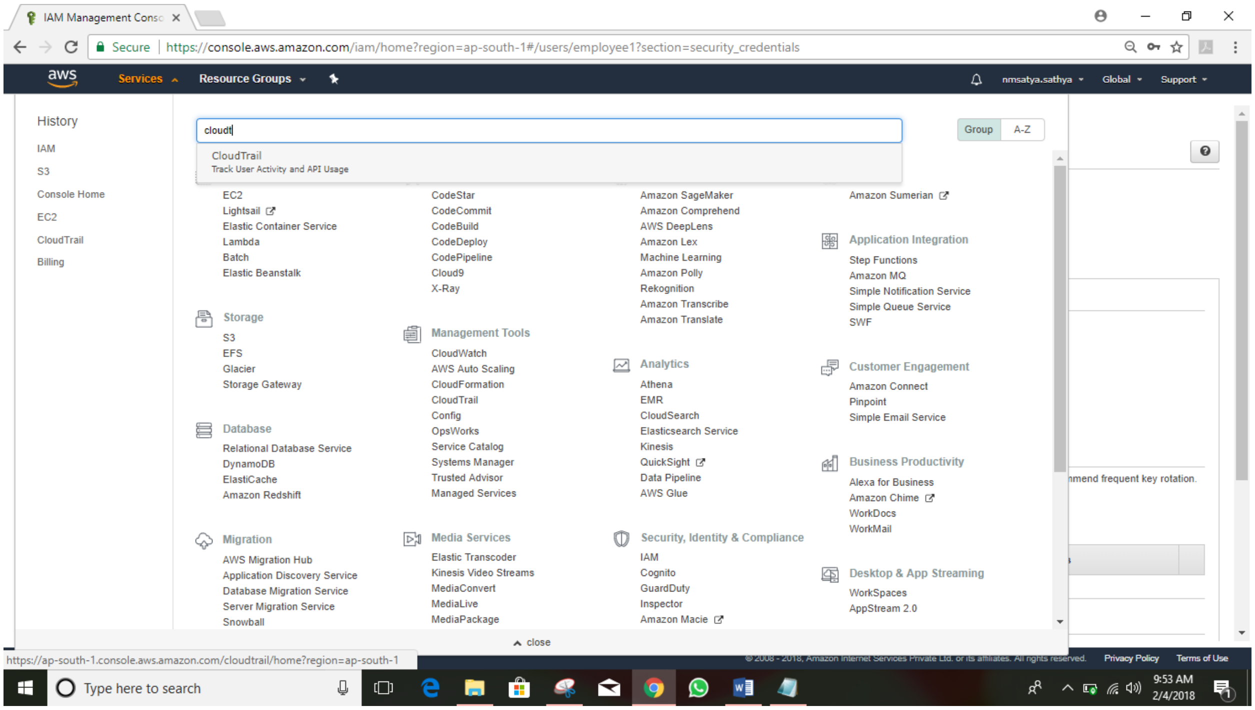


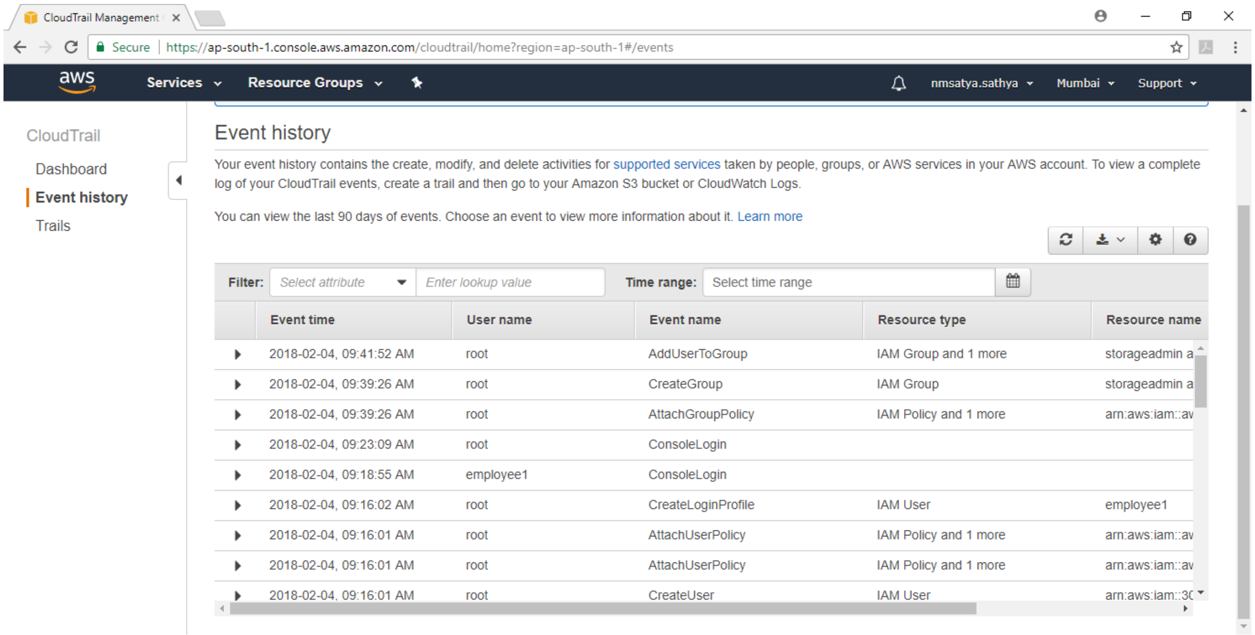
Learn how to store and retrieve a file with S3. Try the 10-Minute Tutorial » Documentation

Bucket name	Access	Region	Date created
employee1	Not public *	Asia Pacific (Mumbai)	Feb 4, 2018 9:49:51 AM GMT+0530

* Objects might still be publicly accessible due to object ACLs. Learn more

Now you can see cloud trail audit from root account for employee1 activity.





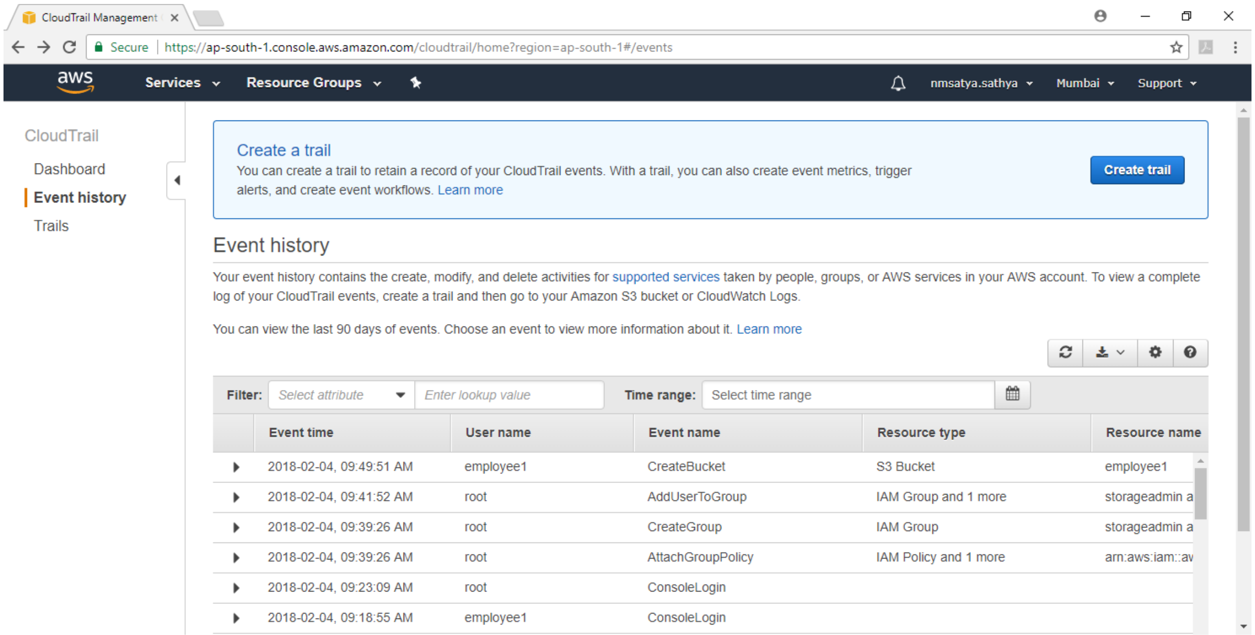
Event history

Your event history contains the create, modify, and delete activities for supported services taken by people, groups, or AWS services in your AWS account. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs.

You can view the last 90 days of events. Choose an event to view more information about it. Learn more

Filter: Select attribute | Enter lookup value | Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
2018-02-04, 09:41:52 AM	root	AddUserToGroup	IAM Group and 1 more	storageadmin a
2018-02-04, 09:39:26 AM	root	CreateGroup	IAM Group	storageadmin a
2018-02-04, 09:39:26 AM	root	AttachGroupPolicy	IAM Policy and 1 more	arn:aws:iam::av
2018-02-04, 09:23:09 AM	root	ConsoleLogin		
2018-02-04, 09:18:55 AM	employee1	ConsoleLogin		
2018-02-04, 09:16:02 AM	root	CreateLoginProfile	IAM User	employee1
2018-02-04, 09:16:01 AM	root	AttachUserPolicy	IAM Policy and 1 more	arn:aws:iam::av
2018-02-04, 09:16:01 AM	root	AttachUserPolicy	IAM Policy and 1 more	arn:aws:iam::av
2018-02-04, 09:16:01 AM	root	CreateUser	IAM User	arn:aws:iam::3C



Create a trail

You can create a trail to retain a record of your CloudTrail events. With a trail, you can also create event metrics, trigger alerts, and create event workflows. Learn more

Event history

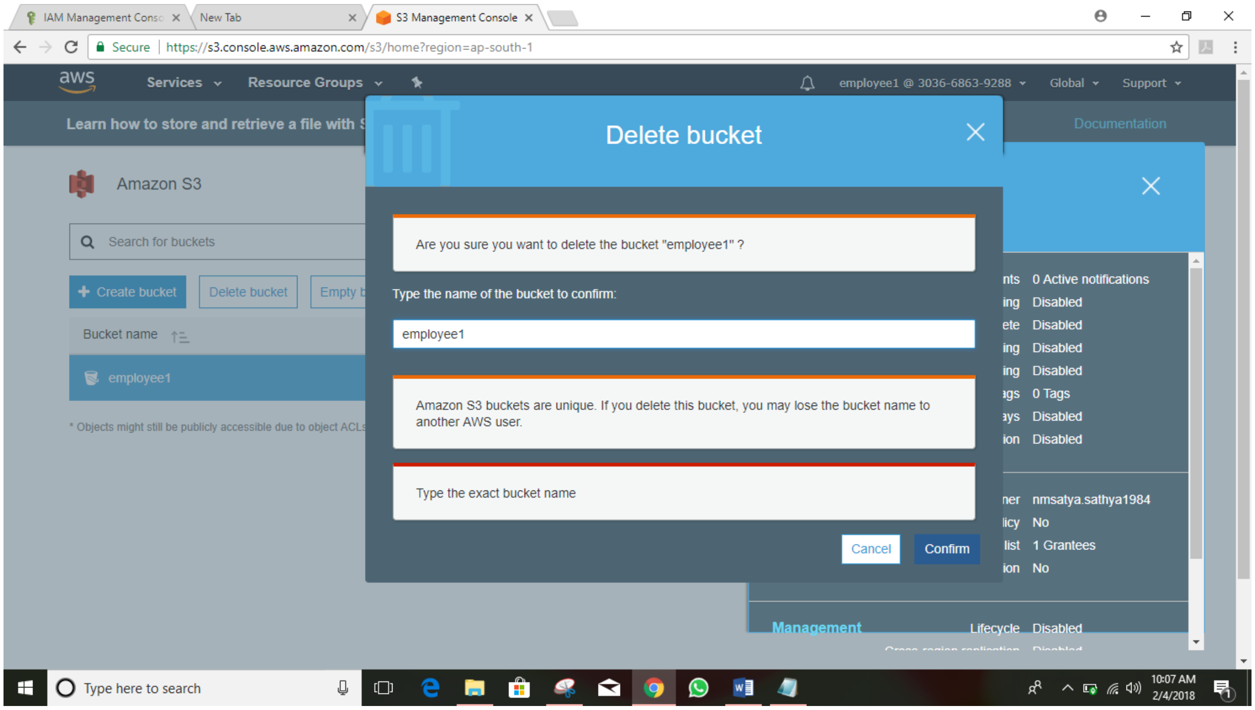
Your event history contains the create, modify, and delete activities for supported services taken by people, groups, or AWS services in your AWS account. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs.

You can view the last 90 days of events. Choose an event to view more information about it. Learn more

Filter: Select attribute | Enter lookup value | Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
2018-02-04, 09:49:51 AM	employee1	CreateBucket	S3 Bucket	employee1
2018-02-04, 09:41:52 AM	root	AddUserToGroup	IAM Group and 1 more	storageadmin a
2018-02-04, 09:39:26 AM	root	CreateGroup	IAM Group	storageadmin a
2018-02-04, 09:39:26 AM	root	AttachGroupPolicy	IAM Policy and 1 more	arn:aws:iam::av
2018-02-04, 09:23:09 AM	root	ConsoleLogin		
2018-02-04, 09:18:55 AM	employee1	ConsoleLogin		

Now you can delete the s3 bucket from employee1 login which is created already.



Delete bucket

Are you sure you want to delete the bucket "employee1" ?

Type the name of the bucket to confirm:

employee1

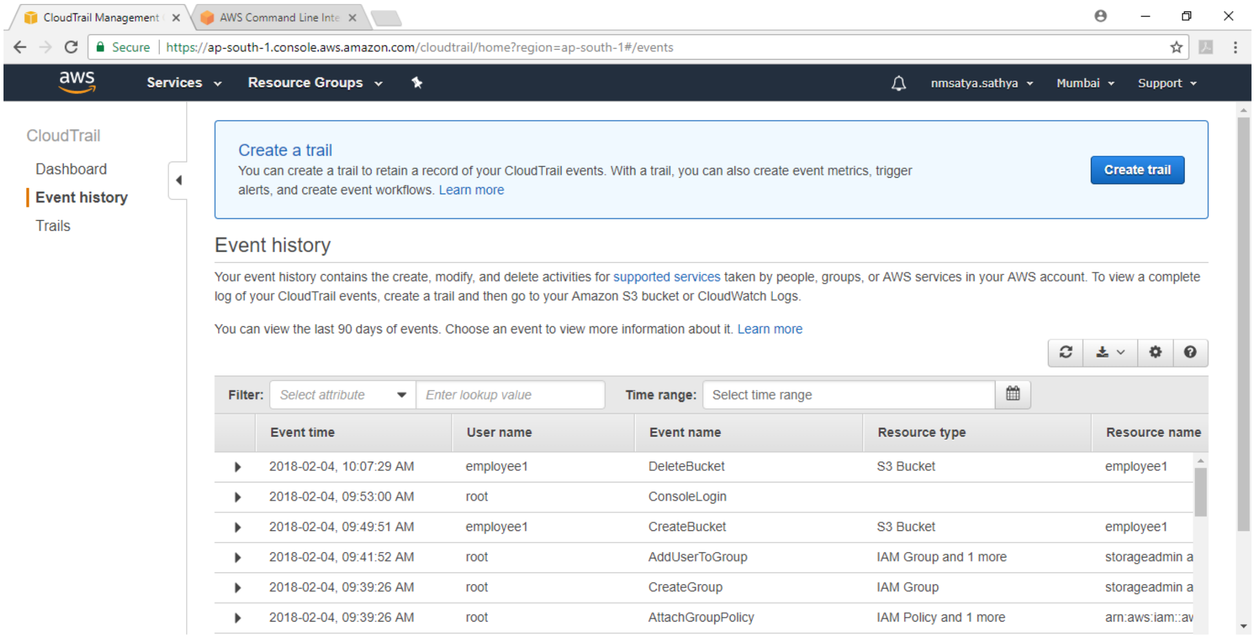
Amazon S3 buckets are unique. If you delete this bucket, you may lose the bucket name to another AWS user.

Type the exact bucket name

Cancel | Confirm

nts	0 Active notifications
ing	Disabled
ete	Disabled
ing	Disabled
ing	Disabled
ags	0 Tags
ays	Disabled
ion	Disabled
ner	nmsatya.sathya1984
licy	No
list	1 Grantees
ion	No
Management Lifecycle	Disabled

Ultimate result is you can see all event viewer (Cloudtrail)



Create a trail

You can create a trail to retain a record of your CloudTrail events. With a trail, you can also create event metrics, trigger alerts, and create event workflows. Learn more

Create trail

Event history

Your event history contains the create, modify, and delete activities for supported services taken by people, groups, or AWS services in your AWS account. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs.

You can view the last 90 days of events. Choose an event to view more information about it. Learn more

Filter: Select attribute | Enter lookup value | Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
2018-02-04, 10:07:29 AM	employee1	DeleteBucket	S3 Bucket	employee1
2018-02-04, 09:53:00 AM	root	ConsoleLogin		
2018-02-04, 09:49:51 AM	employee1	CreateBucket	S3 Bucket	employee1
2018-02-04, 09:41:52 AM	root	AddUserToGroup	IAM Group and 1 more	storageadmin a
2018-02-04, 09:39:26 AM	root	CreateGroup	IAM Group	storageadmin a
2018-02-04, 09:39:26 AM	root	AttachGroupPolicy	IAM Policy and 1 more	arn:aws:iam::av