



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23**

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	01
DOP	24/01/2023
DOS	



AWS (EC2) Installation steps for Linux instance

Please find the AWS account creation steps in the link.

- <https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/>
- https://signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fconsole.aws.amazon.com%2Fsupport%2Fhome%2F%3Fnc2%3Dh_ql_cu%26state%3DhashArgs%2523%26isauthcode%3Dtrue&client_id=arn%3Aaws%3Aiam%3A015428540659%3Auser%2Fsupportcenter&forceMobileApp=0

Requirement – Amazon web service account



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

sudhamsingh_aiml_2020@ltce.in

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](#)

The screenshot shows the AWS sign-in interface on the left and the AWS Services navigation bar on the right. The sign-in page includes fields for email, password, and two-factor authentication, along with links for 'Forgot password?' and 'Create a new AWS account'. The Services navigation bar lists various AWS services under categories like Analytics, Application Integration, AR & VR, AWS Cost Management, Blockchain, Business Applications, Compute, Containers, Customer Enablement, Database, Developer Tools, End User Computing, Front-end Web & Mobile, and Game Development. A 'Recently visited' section shows 'EC2' and 'Console Home'.

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

Step 0 : Login

Step 1 : Open AWS services and select EC2

The screenshot shows the AWS EC2 Management Dashboard. The left sidebar includes links for EC2 Dashboard, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store. The main content area displays 'Resources' with a summary of running instances, auto scaling groups, dedicated hosts, elastic IPs, instances, placement groups, key pairs, security groups, and volumes. It also features sections for 'Launch instance' (with 'Launch instance' and 'Migrate a server' buttons), 'Service health' (showing the region as US East (N. Virginia) and status as 'This service is operating normally'), and 'Explore AWS' (with links for Best Price-Performance with AWS Graviton2, Get Up to 40% Better Price Performance, and a note about T4g instances). The top navigation bar shows the URL as us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home:.

https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



Step 2 : CLICK ON instance (running) in above screen

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store. The main content area has a search bar at the top and a table header for 'Instances Info' with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. Below the header, it says 'No instances' and 'You do not have any instances in this region'. A 'Launch instances' button is visible. The bottom of the page includes a feedback section and links for 2023, Privacy, Terms, and Cookie preferences.

Step 3 : On above screen click on launch Instances

The screenshot shows the 'Launch an instance' page. The left sidebar shows the navigation path: EC2 > Instances > Launch an instance. The main content area has a 'Name and tags' section where 'Name' is set to 'e.g. My Web Server'. Below it is an 'Application and OS Images (Amazon Machine Image)' section with a search bar and a 'Quick Start' tab. Under 'Quick Start', there are tabs for Amazon Linux (selected), macOS, Ubuntu, Windows, Red Hat, and SUSE, along with a 'Browse more AMIs' link. To the right, there's a 'Summary' section with fields for 'Number of instances' (set to 1), 'Software Image (AMI)' (Amazon Linux 2 Kernel 5.10 AMI...), 'Virtual server type (instance type)' (t2.micro), 'Firewall (security group)' (New security group), and 'Storage (volumes)' (1 volume(s) - 8 GiB). A note about the 'Free tier' is shown: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage.' At the bottom are 'Cancel' and 'Launch instance' buttons.



Step 4 : Select **Ubuntu server 22.04** and Select **free tier eligible** and click on button– **Next:configure instance details**

Step 5 : Don't change any setting directly click on button – **Next: Add storage**

Step 6 : Check Volume type: **General purpose SSD (gp 2)** and then click on button – next: **Add Tags**

Step 7 : Need to add key so click on **Add Tag**, In key tab give **any name**, value – **database**

Step 8 : Click on **Create a new key pair**, Insert key pair name anything like – test

Launch an instance [Info](#)

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

Name and tags [Info](#)

Key Info Value Info Resource types [Info](#)

Q sudham X Q database X Select resource ty... ▾ X

Instances X Volumes X

Add tag

49 remaining (Up to 50 tags maximum)

Instance type [Info](#)

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour

Compare instance types

Key pair (login) [Info](#)

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

ccl_sudham [Create new key pair](#)

Network settings [Info](#)

Network [Info](#)
vpc-063362441ac427407

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

Allow SSH traffic from Anywhere
Helps you connect to your instance

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

⚠️ 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 known IP addresses only.

Application and OS Images (Amazon Machine Image) [Info](#)

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

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat S

ubuntu®

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-00874d747dde814fa (64-bit (x86)) / ami-01625be155ee390e9 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-01-15

Architecture AMI ID

64-bit (x86) ami-00874d747dde814fa Verified provider

Create key pair

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name ccl_sudham

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

.pem For use with OpenSSH

.ppk For use with PuTTY

[Cancel](#) [Create key pair](#)

Configure storage [Info](#)

Advanced

1x 8 GiB gp2 Root volume (Not encrypted)

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

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

File systems

Advanced details [Info](#)



Step 9 : Click on Launch Instances

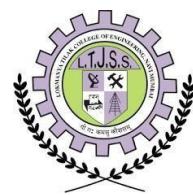
The screenshot shows the AWS EC2 'Launch an instance' wizard. On the left, there's a summary panel with fields for 'Number of instances' (set to 1), 'Software Image (AMI)' (Canonical, Ubuntu, 22.04 LTS), 'Virtual server type (instance type)' (t2.micro), and a note about the free tier. On the right, a success message says 'Successfully initiated launch of instance (i-0b09a1f848101ce25)'. Below it, there are 'Next Steps' like 'Create billing and free tier usage alerts', 'Connect to your instance', and 'Connect an RDS database'. At the bottom, there are 'Cancel' and 'Launch instance' buttons.

Step 10 : You get the msg in green color – click on View Instances

Step 11 : Click on refresh button because we need Status check tab – 2/2 check pass

Step 12 : Select check box which is present at before name DATABASE and click on connect Button

The screenshot shows the AWS EC2 Instances page. It lists one instance named 'sudham' (Instance ID: i-0b09a1f848101ce25) which is 'Running'. The 'Status check' column shows '2/2 checks passed'. The page includes tabs for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The 'Status checks' tab is currently selected. The status bar at the bottom indicates '2023, Amazon Web Services India Private Limited or its affiliates.' and links for Privacy, Terms, and Cookie preferences.



Step 13 : Here you can change the user name if you want – like db_sg1, Step- click on Connect

EC2 > Instances > i-0b09a1f848101ce25 > Connect to instance

Connect to instance Info

Connect to your instance i-0b09a1f848101ce25 (sudham) using any of these options

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID
i-0b09a1f848101ce25 (sudham)

Public IP address
107.23.111.164

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, ubuntu.

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

Cancel **Connect**

Step 14 : Next step perform some **command** on your Ubuntu server-

\$ sudo -i (root login)

apt update (update your system)

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0b09a1f848101ce25&osUser=ubuntu&sshPort=22#/  
AWS Services Search [Alt+S]  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
System information as of Sat Feb 4 16:29:34 UTC 2023  
  
System load: 0.0 Processes: 96  
Usage of /: 19.7% of 7.57GB Users logged in: 0  
Memory usage: 20% IPv4 address for eth0: 172.31.63.91  
Swap usage: 0%  
  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
ubuntu@ip-172-31-63-91:~$
```

i-0b09a1f848101ce25 (sudham)

PublicIPs: 107.23.111.164 PrivateIPs: 172.31.63.91



top (table of processes, which are the running processes in our system and also check usage management)

Press **Ctrl+c** or press **q** for the end top command.

```
ubuntu@ip-172-31-63-91:~# sudo -i
root@ip-172-31-63-91:~# apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8272 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [852 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [189 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [18.2 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [566 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [87.1 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [556 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [797 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [142 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [15.1 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [7988 B]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [2448 B]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [432 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.7 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [9800 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [392 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [19.5 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [13.8 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [392 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [601 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [127 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [8064 B]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [528 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [61.2 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [556 B]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [637 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [87.5 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [11.3 kB]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [4268 B]
Get:41 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [972 B]
Get:42 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [228 B]
Fetched 25.5 MB in 4s (6245 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
29 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-172-31-63-91:~#
```

57_CCL_EXP1 - Google Docs | Connect to instance | EC2 Manager | EC2 Instance Connect

aws Services Search [Alt+S]

top - 16:48:56 up 34 min, 2 users, load average: 0.00, 0.00, 0.00

Tasks: 100 total, 1 running, 99 sleeping, 0 stopped, 0 zombie

%Cpu(s): 0.3 us, 0.0 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st

MiB Mem : 966.2 total, 161.3 free, 209.8 used, 595.1 buff/cache

MiB Swap: 0.0 total, 0.0 free, 0.0 used. 612.1 avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2501	ubuntu	20	0	17300	7980	5596	S	0.3	0.8	0:00.02	sshd
1	root	20	0	101876	12788	8284	S	0.0	1.3	0:05.04	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_flushwg
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-events_highpri
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wg
11	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_tasks_rude
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_tasks_trace
13	root	20	0	0	0	0	S	0.0	0.0	0:00.09	ksoftirqd/0
14	root	20	0	0	0	0	I	0.0	0.0	0:00.45	rcu_sched
15	root	rt	0	0	0	0	S	0.0	0.0	0:00.01	migration/0
16	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/0
18	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kdevtmpfs
20	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	inet_frag_wg
21	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kauditd
22	root	20	0	0	0	0	S	0.0	0.0	0:00.00	khungtaskd
23	root	20	0	0	0	0	S	0.0	0.0	0:00.00	oom_reaper

i-0b09a1f848101ce25 (sudham)

PublicIPs: 107.23.111.164 PrivateIPs: 172.31.63.91

history

vmstat (virtual memory static ,how much memory in the buffer,in the cache, what is in the input,output,systems and the cpu)

df (disk file system)

#df -kh (k-kilobyte h-human readable)

#whatis df (using whatis command take help from system)

57_CCL_EXP1 - Google Docs | Connect to instance | EC2 Manager | EC2 Instance Connect

aws Services Search [Alt+S]

root@ip-172-31-63-91:~# history

1 apt update

2 top

3 history

root@ip-172-31-63-91:~# vmstat

procs	memory	swap	io	system	cpu
r b	swpd free buff cache	si so bi bo	in cs us sy	id wa	st

root@ip-172-31-63-91:~# df

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/root	7941576	1753824	6171368	23%	/
tmpfs	494692	0	494692	0%	/dev/shm
tmpfs	197880	832	197048	1%	/run
tmpfs	5120	0	5120	0%	/run/lock
/dev/xvda15	106858	5329	101529	5%	/boot/efi
tmpfs	98936	4	98932	1%	/run/user/1000

root@ip-172-31-63-91:~# df -kh

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/root	7.6G	1.7G	5.9G	23%	/
tmpfs	484M	0	484M	0%	/dev/shm
tmpfs	194M	832K	193M	1%	/run
tmpfs	5.0M	0	5.0M	0%	/run/lock
/dev/xvda15	105M	5.3M	100M	5%	/boot/efi
tmpfs	97M	4.0K	97M	1%	/run/user/1000

root@ip-172-31-63-91:~# whatis df

df: nothing appropriate.

root@ip-172-31-63-91:~#

i-0b09a1f848101ce25 (sudham)

PublicIPs: 107.23.111.164 PrivateIPs: 172.31.63.91

AIML57_SUDHAM



#df --help (help command)

ctrl + l (clear the screen)

#uname -a (information related to ip, kernel version)

All are Validation steps for checking your EC2 instance working properly or not(check system performance).

```
root@ip-172-31-63-91:~# rmdir test
root@ip-172-31-63-91:~# ls
snap
root@ip-172-31-63-91:~# df --help
Usage: df [OPTION]... [FILE]...
Show information about the file system on which each FILE resides,
or all file systems by default.

Mandatory arguments to long options are mandatory for short options too.
  -a, --all           include pseudo, duplicate, inaccessible file systems
  -B, --block-size=SIZE scale sizes by SIZE before printing them; e.g.,
                       '-BM' prints sizes in units of 1,048,576 bytes;
                       see SIZE format below
  -h, --human-readable print sizes in powers of 1024 (e.g., 1023M)
  -H, --si            print sizes in powers of 1000 (e.g., 1.1G)
  -l, --inodes         limit inode information instead of block usage
  -L, --local          limit listing to local file systems
  -1, --no-sync        do not invoke sync before getting usage info (default)
  --output[=FIELD_LIST] use the output format defined by FIELD_LIST,
                        or print all fields if FIELD_LIST is omitted.
  -P, --portability   use the POSIX output format
  --sync              invoke sync before getting usage info
  --total             elide all entries insignificant to available space,
                     and produce a grand total
  -t, --type=TYPE    limit listing to file systems of type TYPE
  -T, --print-type   print file system type
  -x, --exclude-type=TYPE limit listing to file systems not of type TYPE
  -v                 (ignored)
  --help              display this help and exit
  --version           output version information and exit

Display values are in units of the first available SIZE from --block-size,
and the DF_BLOCK_SIZE, BLOCK_SIZE and BLOCKSIZE environment variables.
Otherwise, units default to 1024 bytes (or 512 if POSIXLY_CORRECT is set).

The SIZE argument is an integer and optional unit (example: 10K is 10*1024).
Units are K,M,G,T,P,E,Z,Y (powers of 1024) or KB,MB,... (powers of 1000).
Binary prefixes can be used, too: KiB=K, MiB=M, and so on.

FIELD_LIST is a comma-separated list of columns to be included. Valid
field names are: 'source', 'fstype', 'itotal', 'iused', 'iavail', 'ipcent',
'size', 'used', 'avail', 'pcent', 'file' and 'target' (see info page).

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Report any translation bugs to <https://translationproject.org/team/>
Full documentation <https://www.gnu.org/software/coreutils/df/>
or available locally via: info '(coreutils) df invocation'
root@ip-172-31-63-91:~#
```

i-0b09a1f848101ce25 (sudham)
Public IPs: 107.23.111.164 Private IPs: 172.31.63.91

mkdir test

ls

cd test

test# touch file1 (create file)

ls

touch file2 file3

ls

rm file1 (remove file)

ls

rm file* (remove all files)

ls

cd ..

ls

rmdir test

ls

mkdir test1 test2 test3

#ls

rmdir test*

ls

Feedback Language

i-0b09a1f848101ce25 (sudham)
Public IPs: 107.23.111.164 Private IPs: 172.31.63.91

Feedback Language

i-0b09a1f848101ce25 (sudham)
Public IPs: 107.23.111.164 Private IPs: 172.31.63.91

Feedback Language

i-0b09a1f848101ce25 (sudham)
Public IPs: 107.23.111.164 Private IPs: 172.31.63.91

Feedback Language

i-0b09a1f848101ce25 (sudham)
Public IPs: 107.23.111.164 Private IPs: 172.31.63.91

Feedback Language



Step 15 : To terminate the instance -

Select the checkbox which is available at the start of your name of instant , then click on **Instant State** Button on the top and select **Terminal Instance**

The screenshot shows the AWS EC2 Instances page. A single instance named "sudham" is listed, showing it is "Running". In the "Actions" dropdown menu, the "Terminate instance" option is highlighted. The instance details page is also visible, showing its public and private IP addresses, instance ID, and other configuration details.

Step 16 : If you want to terminate then this will, and if not the following instance will show as it is !

The screenshot shows the AWS EC2 Instances page again. The same instance "sudham" is listed as "Running". The "Actions" dropdown menu is closed. The instance details page is visible below, showing the same configuration as before.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	3
DOP	
DOS	



AMAZON S3 (BUCKET)

OUTPUT:

STEP 1: Login to AWS console and go to Amazon S3 BUCKET.

The screenshot shows the AWS Management Console homepage. A search bar at the top right contains the query "bucket". Below the search bar, there are two main sections: "Services" and "Features".

- Services:**
 - S3: Scalable Storage in the Cloud (selected)
 - Amazon Braket: Service for exploring, evaluating, and experimenting with quantum computing.
 - Incident Manager: Automated incident response plans in AWS Systems Manager.
 - AWS Budgets: Set Custom Budgets and Receive Alerts.
- Features:**
 - Buckets: S3 feature
 - Logging configuration: Amazon Interactive Video Service feature
 - Enable Macie automated data discovery: Amazon Macie feature
 - S3 on Outposts: AWS Outposts feature

On the right side of the screen, there is a "Welcome to AWS" sidebar with three sections: "Getting started with AWS", "Training and certification", and "What's new with AWS?".

Click on Create Bucket.

The screenshot shows the AWS S3 Management Console. The left sidebar has a "Buckets" section with various options like Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. There is also a "Storage Lens" section with links for Dashboards and AWS Organizations settings.

The main content area displays a green success message: "Successfully deleted bucket 'cc15'". Below this, it says "Amazon S3 > Buckets". It shows an "Account snapshot" with a "Storage lens provides visibility into storage usage and activity trends. Learn more" link and a "View Storage Lens dashboard" button.

The "Buckets (1) Info" section shows a single bucket named "elasticbeanstalk-ap-south-1-793536247045". The table details for this bucket are:

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-793536247045	Asia Pacific (Mumbai) ap-south-1	Objects can be public	January 31, 2023, 10:49:11 (UTC+05:30)

At the bottom right of the main content area, there is a "Create bucket" button.



STEP 2: Give Bucket name & select region for storage.

STEP 3: Keep object ownership setting as ACLs Disabled as by-default.

The screenshot shows the 'Create bucket' page in the AWS S3 console. In the 'General configuration' section, the 'Bucket name' is set to 'cc15' and the 'AWS Region' is set to 'Asia Pacific (Mumbai) ap-south-1'. Under 'Object Ownership', the 'ACLs disabled (recommended)' option is selected, which is highlighted in blue. A note at the bottom states: 'Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the s3:PutBucketOwnershipControls permission.' Below this, there is a warning about upcoming permission changes related to disabling ACLs.

STEP 4: Disable block all public access checkbox.

STEP 5: Select the checkbox for Turning off block all public access might result in this bucket and the objects with in becoming public.

The screenshot shows the 'Block Public Access settings for this bucket' page. Under 'Block public access', the 'Block public access to buckets and objects granted through new access control lists (ACLS)' checkbox is checked. A warning message states: 'Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.' A checkbox labeled 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' is checked. A note at the bottom states: 'Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the s3:PutBucketPublicAccessBlock permission.'



STEP 6: Keep Bucket Versioning as Disabled and add tags if required.

STEP 7: Keep Default encryption Disabled and click on create bucket button.

The screenshot shows the AWS S3 Bucket creation interface. The 'Bucket Versioning' section has 'Disable' selected. The 'Tags (0) - optional' section indicates 'No tags associated with this bucket.' The 'Default encryption' section shows 'Encryption key type: Info' with 'Amazon S3-managed keys (SSE-S3)' selected. The 'Bucket Key' section shows 'Bucket Key' is disabled. At the bottom, a note says 'After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.' The 'Create bucket' button is highlighted in orange.

You can now see the successful creation of your Bucket.

The screenshot shows the AWS S3 Buckets list. A green banner at the top says 'Successfully created bucket "cc15"'. Below it, the 'Buckets' table lists two buckets:

Name	AWS Region	Access	Creation date
cc15	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 7, 2023, 10:50:28 (UTC+05:30)
elasticbeanstalk-ap-south-1-793536247045	Asia Pacific (Mumbai) ap-south-1	Objects can be public	January 31, 2023, 10:49:11 (UTC+05:30)



STEP 8: Now click on the **Bucket** that you have created.

The screenshot shows the AWS S3 Management Console. A green banner at the top indicates that a bucket named "ccl5" has been successfully created. The main area displays an "Account snapshot" and a table of buckets. The table includes columns for Name, AWS Region, Access, and Creation date. The "ccl5" bucket is listed with the following details:

Name	AWS Region	Access	Creation date
ccl5	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 7, 2023, 10:50:28 (UTC+05:30)
elasticbeanstalk-ap-south-1-795536247045	Asia Pacific (Mumbai) ap-south-1	Objects can be public	January 31, 2023, 10:49:11 (UTC+05:30)

STEP 9: You can either **create a folder** here or **upload** an existing file in the Bucket.

The screenshot shows the AWS S3 Management Console for the "ccl5" bucket. The "Objects" tab is selected. The table header includes columns for Name, Type, Last modified, Size, and Storage class. A message at the bottom states "No objects" and "You don't have any objects in this bucket." Below the table is a large "Upload" button.



STEP10: Now click on **upload** button and click on **add files** button browse your local machine and select which file you need to upload on S3 next click on **upload button** at bottom right end.

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more [?]

Drag and drop files and folders you want to upload here, or choose Add files, or Add folder.

Files and folders (0)
All files and folders in this table will be uploaded.

Find by name

No files or folders
You have not chosen any files or folders to upload.

Destination

Destination
s3://cc15

► Destination details
Bucket settings that impact new objects stored in the specified destination.

► Permissions
Grant public access and access to other AWS accounts.

► Properties
Configure object metadata and server-side encryption.

Now you can check the **upload status** screen.

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://cc15	1 file, 15.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 15.0 B)

Name	Folder	Type	Size	Status	Error
INDEX.html	-	text/html	15.0 B	Succeeded	-



Now click on **close** button.

The screen will appear as below

Activities Google Chrome Feb 7 11:32 AM ccl5 - S3 bucket x + s3.console.aws.amazon.com/s3/buckets/ccl5?region=ap-south-1&tab=objects Guest (Update) AWS Services Search [Alt+S] Global sudham2412 Amazon S3 > Buckets > ccl5 ccl5 Info Publicly accessible Objects (2) Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload Find objects by prefix < 1 > Objects Name Type Last modified 1.png png February 7, 2023, 10:55:40 (UTC+05:30) 205.4 KB Standard INDEX.html html February 7, 2023, 11:52:16 (UTC+05:30) 15.0 B Standard Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

STEP 11: Select **Properties** and scroll down to **Static website hosting** option which is Disabled now click on **Edit** option on right side.

Activities Google Chrome Feb 7 10:57 AM ccl5 - S3 bucket x + s3.console.aws.amazon.com/s3/buckets/ccl5?region=ap-south-1&tab=properties Guest (Update) AWS Services Search [Alt+S] Global sudham2412 Amazon S3 > Buckets > ccl5 ccl5 Info Properties Bucket overview AWS Region Asia Pacific (Mumbai) ap-south-1 Amazon Resource Name (ARN) arn:aws:s3:::ccl5 Creation date February 7, 2023, 10:50:28 (UTC+05:30) Bucket Versioning Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more Edit Bucket Versioning Disabled Multi-factor authentication (MFA) delete An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more Disabled Tags (0) You can use bucket tags to track storage costs and organize buckets. Learn more Edit Key Value No tags associated with this resource. Default encryption Info https://s3.console.aws.amazon.com/s3/# © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



Activities Google Chrome

Feb 7 10:58 AM

s3.console.aws.amazon.com/s3/buckets/ccl5-region=ap-south-1&tab=properties

Guest Update

Services Search [Alt+S]

Send notifications to Amazon EventBridge for all events in this bucket
Off

Transfer acceleration
Use an accelerated endpoint for faster data transfers. Learn more [Edit](#)

Transfer acceleration
Disabled

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more [Edit](#)

Object Lock
Disabled

Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support [Edit](#)

Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more [Edit](#)

Requester pays
Disabled

Static website hosting
Use this bucket to host a website or redirect requests. Learn more [Edit](#)

Static website hosting
Disabled

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

STEP 12: Enable the radio button and specify the file name in Index document which you have added in S3.

Activities Google Chrome

Feb 7 10:59 AM

s3.console.aws.amazon.com/s3/bucket/ccl5/property/website/edit?region=ap-south-1

Guest Update

Services Search [Alt+S]

Redirect requests for an object
Redirect requests to another bucket or domain. Learn more [Edit](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access [Edit](#)

Index document
Specify the home or default page of the website.

Error document - optional
This is returned when an error occurs.

Redirection rules - optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more [Edit](#)

Cancel [Save changes](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



Activities Google Chrome

ccl5 - S3 bucket s3.console.aws.amazon.com/s3/bucket/ccl5/property/website/edit?region=ap-south-1

Guest Update

Services Search [Alt+S]

Amazon S3 > Buckets > ccl5 > Edit static website hosting

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Disable

Enable

Hosting type

Host a static website

Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Scroll down and save the changes at bottom right.

Following screen will appear.

Activities Google Chrome

ccl5 - S3 bucket s3.console.aws.amazon.com/s3/buckets/ccl5?region=ap-south-1&tab=properties

Guest Update

Services Search [Alt+S]

Amazon S3 > Buckets > ccl5

ccl5 Info

Properties Objects Permissions Metrics Management Access Points

Bucket overview

AWS Region: Asia Pacific (Mumbai) ap-south-1

Amazon Resource Name (ARN): arnaws3:ccl5

Creation date: February 7, 2023, 10:50:28 (UTC+05:30)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning: Disabled

Multi-factor authentication (MFA) delete: An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key Value

No tags associated with this resource.

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



STEP 13: Click on **Permissions Tab**.

STEP 14: In **bucket policy** click on **Edit option**.

The screenshot shows the AWS S3 Bucket Permissions Overview page for the 'cc15' bucket. The 'Permissions' tab is selected. Under 'Access', it says 'Objects can be public'. In the 'Block public access (bucket settings)' section, there is a note about public access being granted through ACLs, policies, and access point policies. A button labeled 'Edit' is present. Below it, 'Block all public access' is set to 'Off'. There is also a link to 'Individual Block Public Access settings for this bucket'. In the 'Bucket policy' section, it says 'No policy to display.' and has 'Edit' and 'Delete' buttons.

STEP 15: After clicking on edit button paste the following code in **bucket policy**.

The screenshot shows the 'Edit bucket policy' page for the 'cc15' bucket. The 'Policy' section contains the following JSON code:

```
1 ~ |{  
2 ~ "Version": "2012-10-17", "Statement": [  
3 ~ {  
4 ~ "Sid": "PublicReadGetObject", "Effect": "Allow",  
5 ~ "Principal": "*",  
6 ~ "Action": ["  
7 ~ "s3:GetObject"],  
8 ~ "Resource": [ "arn:aws:s3:::cc15/*"  
9 ~ ]}  
10 |}]
```

To the right, there is an 'Edit statement' panel with a 'Select a statement' dropdown and a '+ Add new statement' button.



Scroll down and click on **Save Changes** button.

The screenshot shows the AWS S3 Bucket Policy editor. The main pane displays a JSON policy document:

```
1 - {
2 -   "Version": "2012-10-17", "Statement": [
3 -     {
4 -       "Sid": "PublicReadGetObject", "Effect": "Allow",
5 -       "Principal": "*",
6 -       "Action": [
7 -         "s3:GetObject"
8 -       ],
9 -       "Resource": [
10 -         "arn:aws:s3:::ccl5/*"
11 -       ]
12 -     }
13 -   ]
14 - }
```

Below the JSON is a button labeled "+ Add new statement". The status bar at the bottom indicates "JSON Ln 10, Col 3" and "Security: 0 Errors: 0 Warnings: 0 Suggestions: 0". To the right, a modal window titled "Edit statement" is open, containing the text "Select a statement" and a button "+ Add new statement". At the bottom right of the main editor are "Cancel" and "Save changes" buttons.

The screenshot shows the AWS S3 Bucket Permissions settings page for the "ccl5" bucket. A green banner at the top says "Successfully edited bucket policy." Below it, the "Permissions overview" section shows the "Block public access (bucket settings)" status as "Off". The "Bucket policy" section shows the following JSON policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::ccl5/*"
      ]
    }
  ]
}
```

At the bottom right of the permissions page are "Edit" and "Delete" buttons. The status bar at the bottom indicates "Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences".



STEP 16: Open your html file and click on **Object URL**.

STEP 17: Now for delete files click on **checkbox** of your file and then click on **Delete** Button.

The screenshot shows the AWS S3 console with the 'Objects' page for the 'ccl5' bucket. There are two objects listed:

Name	Type	Last modified	Size	Storage class
1.png	png	February 7, 2023, 10:55:40 (UTC+05:30)	205.4 KB	Standard
INDEX.html	html	February 7, 2023, 11:52:16 (UTC+05:30)	15.0 B	Standard

Write **permanently delete** and click on **delete object button**.

The screenshot shows the AWS S3 console with the 'Delete objects' confirmation dialog. It asks for confirmation to permanently delete 'INDEX.html'. The 'permanently delete' input field contains the text 'permanently delete'.



Now click on **close** button.

The screenshot shows the AWS S3 console interface. At the top, a message says "Successfully deleted objects" with a link to "View details below". Below this, a summary table shows the source as "Source s3://cc15" and the results of the deletion: "Successfully deleted 1 object, 205.4 KB" and "Failed to delete 0 objects". A "Delete objects: status" section follows, with tabs for "Failed to delete" (selected) and "Configuration". Under "Failed to delete (0)", there is a table with columns: Name, Folder, Type, Last modified, Size, and Error. The table is empty, showing "No objects failed to delete." At the bottom right of the main content area is a "Close" button.

STEP 18: Now come to **Amazon S3** tab and select your **bucket** and then click on **delete** button.

The screenshot shows the AWS S3 Management Console. On the left, a sidebar menu includes "Buckets", "Access Points", "Object Lambda Access Points", "Multi-Region Access Points", "Batch Operations", "IAM Access Analyzer for S3", "Block Public Access settings for this account", "Storage Lens", "Dashboards", "AWS Organizations settings", "Feature spotlight", and "AWS Marketplace for S3". The main content area is titled "Amazon S3 > Buckets". It features an "Account snapshot" section with a "View Storage Lens dashboard" button. Below it is a "Buckets (2) info" section with a note that buckets are containers for data stored in S3. A table lists the buckets: "cc15" (selected, highlighted in blue) and "elasticbeanstalk-ap-south-1-795556247045". The table columns are: Name, AWS Region, Access, and Creation date. The "cc15" row shows "Asia Pacific (Mumbai) ap-south-1", "Public", and "February 7, 2023, 10:50:28 (UTC+05:30)". The "elasticbeanstalk" row shows "Asia Pacific (Mumbai) ap-south-1", "Objects can be public", and "January 31, 2023, 10:49:11 (UTC+05:30)". At the top right of the table are buttons for "Copy ARN", "Empty", "Delete", and "Create bucket". At the bottom right of the main content area is a "Close" button.



Activities Google Chrome

ccl5 - S3 bucket s3.console.aws.amazon.com/s3/bucket/ccl5/delete?region=ap-south-1

AWS Services Search [Alt+S]

Amazon S3 > Buckets > ccl5 > Delete bucket

Delete bucket [Info](#)

Delete bucket "ccl5"?

To confirm deletion, enter the name of the bucket in the text input field.

ccl5

Cancel **Delete bucket**

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

You can see that the bucket is **deleted**.

Activities Google Chrome

S3 Management Console s3.console.aws.amazon.com/s3/buckets?region=ap-south-1

AWS Services Search [Alt+S]

Amazon S3 > Buckets

Successfully deleted bucket "ccl5"

View Storage Lens dashboard

Buckets (1) [Info](#)

Buckets are containers for data stored in S3. Learn more [\[?\]](#)

Find buckets by name

Name	AWS Region	Access	Creation date
elasticbeanstalk-ap-south-1-7935536247045	Asia Pacific (Mumbai) ap-south-1	Objects can be public	January 31, 2023, 10:49:11 (UTC+05:30)

Copy ARN Empty Delete Create bucket

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	4
DOP	
DOS	



AMAZON RDS

OUTPUT:

STEP 1: Login to AWS console and search RDS.

STEP 2: Click on to RDS and Create database.



STEP 3: Select standard database.

STEP 4: Select MySQL and MySQL Community edition.

The screenshot shows the AWS RDS Management Console interface. In the top navigation bar, there are tabs for 'Activities', 'Google Chrome', 'WhatsApp', 'RDS Management Console', and 'Cloud Computing Services'. The main content area is titled 'Create database'. Under 'Choose a database creation method', the 'Standard create' option is selected. In the 'Engine options' section, the 'MySQL' engine type is chosen. The right sidebar contains a detailed description of MySQL, mentioning it's the most popular open-source database and listing various features like support for up to 64 TiB, General Purpose, Memory Optimized, and Burstable Performance instance classes, automated backup, and up to 15 read replicas per instance. At the bottom of the page, there are links for 'Feedback', 'Language', and file attachments for 'Exp No-6 S3.pdf' and 'owncloudfin.pdf'.

STEP 5: In Templates select Free tier.

The screenshot shows the AWS RDS Management Console interface. In the top navigation bar, there are tabs for 'Activities', 'Google Chrome', 'WhatsApp', 'RDS Management Console', and 'Cloud Computing Services'. The main content area is titled 'MySQL'. Under 'Known issues/limitations', it says to review the 'Known Issues/limitations' link to learn about potential compatibility issues with specific database versions. In the 'Templates' section, the 'Free tier' template is selected. The right sidebar contains a detailed description of MySQL, mentioning it's the most popular open-source database and listing various features like support for up to 64 TiB, General Purpose, Memory Optimized, and Burstable Performance instance classes, automated backup, and up to 15 read replicas per instance. At the bottom of the page, there are links for 'Feedback', 'Language', and file attachments for 'Exp No-6 S3.pdf' and 'owncloudfin.pdf'.



STEP 6: Mention **database name** (default is database1) and **username** and **password**.

STEP 7: Instance is db.t2.micro .

Rest of things keep default

The screenshot shows the 'Settings' tab of the AWS RDS Management Console. It includes fields for the DB instance identifier ('databaseSudham'), master username ('admin'), master password, and confirm master password. Below these are sections for 'Instance configuration' and 'DB instance class' (set to db.t2.micro). The bottom of the screen shows a file navigation bar with 'Exp No-6 S3.pdf' and 'owncloudfina....pdf'.

The screenshot shows the 'Instance configuration' tab of the AWS RDS Management Console. It includes sections for 'DB instance class' (set to db.t2.micro), 'Storage' (set to General Purpose SSD (gp2)), and 'Storage autoscaling'. The bottom of the screen shows a file navigation bar with 'Exp No-6 S3.pdf' and 'owncloudfina....pdf'.

STEP 8: Select Public Access -Yes.

The screenshot shows the 'Connectivity' tab of the AWS RDS Management Console. It includes sections for 'Compute resource' (set to 'Don't connect to an EC2 compute resource'), 'Virtual private cloud (VPC)' (set to 'Default VPC (vpc-006fa53a4b125ac9a)'), 'DB subnet group' (info), 'Public access' (set to 'Yes'), and 'VPC security group (firewall)' (set to 'Choose existing'). The bottom of the screen shows a file navigation bar with 'Exp No-6 S3.pdf' and 'owncloudfina....pdf'.

The screenshot shows the 'Additional configuration' tab of the AWS RDS Management Console. It includes sections for 'Availability Zone' (info), 'RDS Proxy' (info), 'Certificate authority - optional' (info), 'Database authentication' (options: Password authentication, Password and IAM database authentication, Password and Kerberos authentication), and 'Monitoring'. The bottom of the screen shows a file navigation bar with 'Exp No-6 S3.pdf' and 'owncloudfina....pdf'.



STEP 9: Click on to Create Database.

The screenshot shows the AWS RDS Management Console. In the center, there's a large orange button labeled 'Create database'. To its left, a blue box contains a note: 'You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.' At the bottom right of the main area, there's a small 'MySQL' tab. On the right side of the screen, there's a sidebar titled 'MySQL' with a list of features: 'Supports database size up to 64 TiB.', 'Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.', 'Supports automated backup and point-in-time recovery.', and 'Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.'

STEP 10: It will take some time.

The screenshot shows the AWS RDS Management Console with a message at the top: 'Creating database databasesudham. Your database might take a few minutes to launch.' Below this, there's a note: 'Consider creating a Blue/Green Deployment to minimize downtime during upgrades.' A table lists the database 'databasesudham' with details: Instance: db.t2.micro, Status: Creating. On the right, there's a 'View credential details' button.

STEP 11: Go to google type mysql workbench.

The screenshot shows a Google search results page for 'mysql workbench'. The first result is 'MySQL Workbench', which is described as a unified tool for database architects, developers, and DBAs. The page also mentions MySQL Workbench provides data modeling, SQL development, and more. To the right of the search results, there's a snippet for 'MySQL Workbench' with a thumbnail image of a dolphin and the text: 'MySQL Workbench is a visual database design tool that integrates SQL development, administration, database design, creation and maintenance into a single integrated development environment for the MySQL database system. Wikipedia'.



STEP 12: Click on to download.

The screenshot shows the MySQL.com homepage. The navigation bar includes links for Products, Cloud, Services, Partners, Customers, Why MySQL?, News & Events, and How to Buy. A sub-menu for 'MySQL Enterprise Edition' is open, showing options like Datasheet (PDF), Technical Specification, MySQL Database, MySQL Document Store, and Oracle Enterprise Manager. The main content area features a section for 'MySQL Workbench Enhanced Data Migration' with a 'Download Now' button and a screenshot of the software interface. A brief description states: 'MySQL Workbench is a unified visual tool for database architects, developers, and DBAs. MySQL Workbench provides data modeling, SQL development, and'.

STEP 13: MySQL community download – Microsoft Windows.

The screenshot shows the 'MySQL Community Downloads' page for Microsoft Windows. It features a 'General Availability (GA) Releases' tab selected, showing the 'MySQL Workbench 8.0.32' page. A dropdown menu under 'Select Operating System' is set to 'Microsoft Windows'. The 'Recommended Download' section offers the 'MySQL Installer for Windows' (Windows x86, 32 & 64-bit, MSI Installer MSI), which is highlighted with a blue box and a 'Go to Download Page >' button. Other download options include 'Windows (x86, 64-bit), MSI Installer' (8.0.32, 45.7M). A note at the bottom states: 'Starting with MySQL 8.0 the MySQL Installer package replaces the standalone MSI packages.'

STEP 14: Click on to – No thanks, just download.

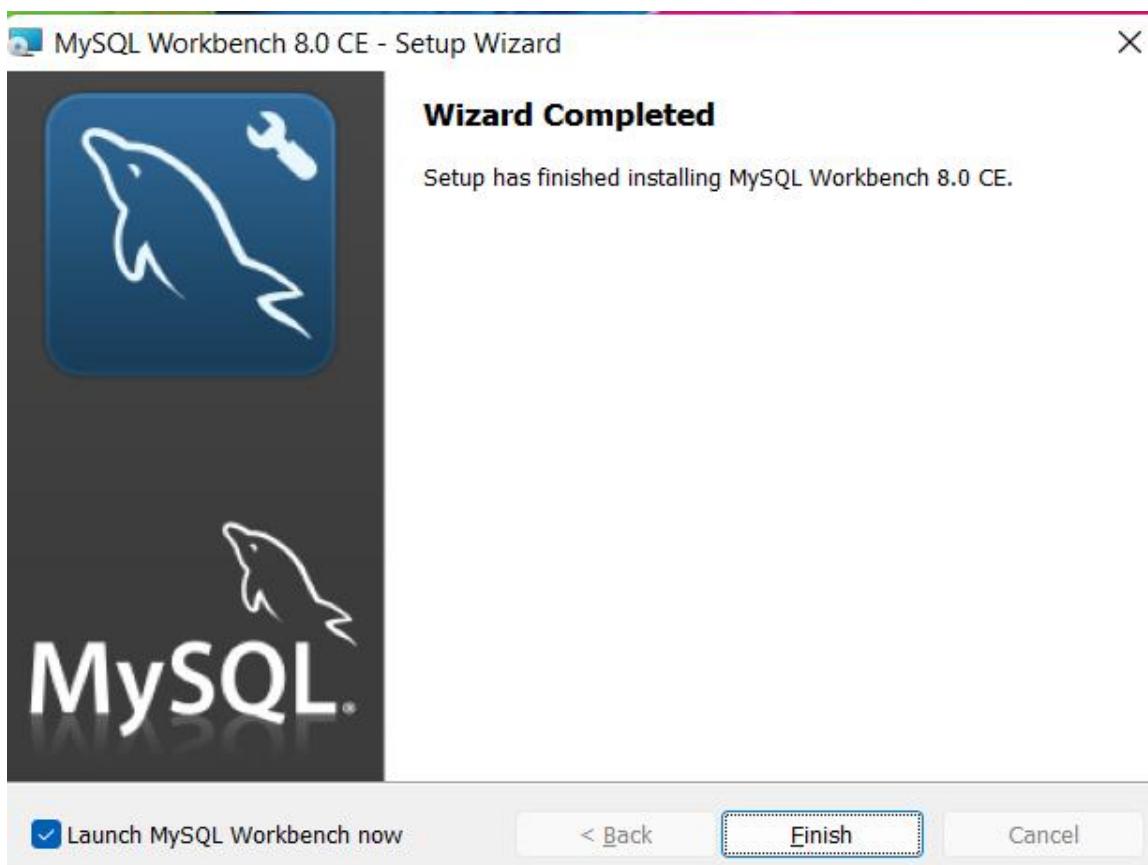
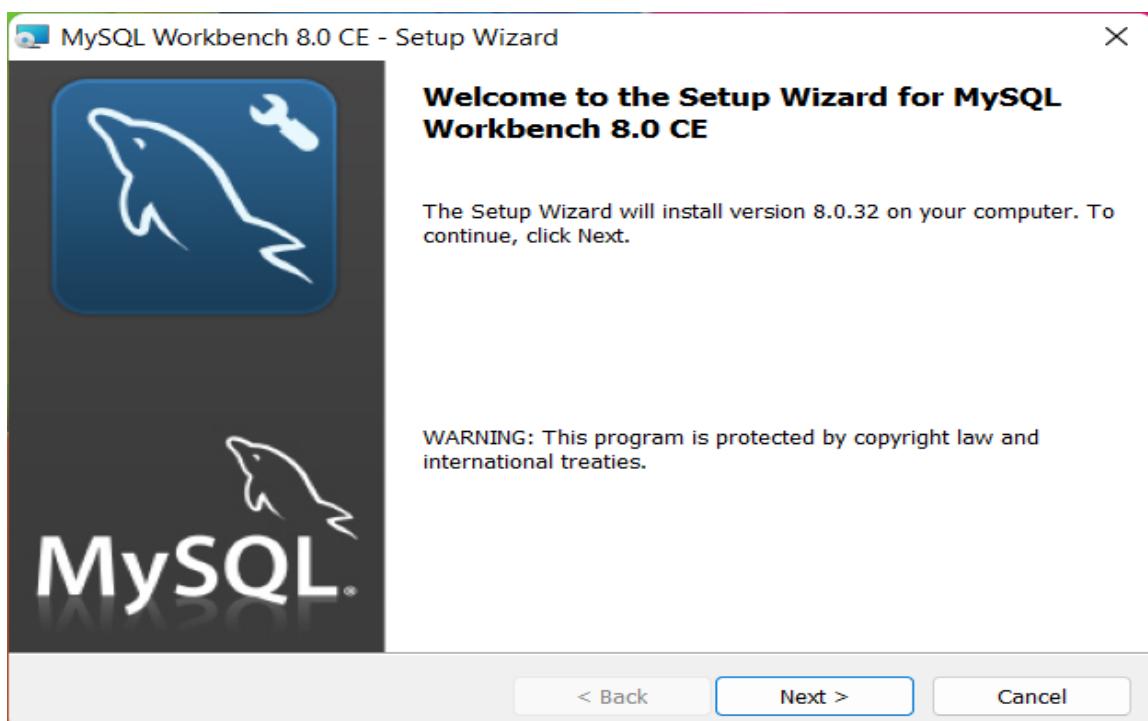
The screenshot shows the same MySQL Community Downloads page for Microsoft Windows, but with a different URL (dev.mysql.com/downloads/file?id=516912). A link at the bottom left reads 'No thanks, just start my download.' Below the main content, there's a box for logging in or signing up for an Oracle Web account, and a note about Oracle SSO authentication.

ORACLE © 2023 Oracle

Privacy / Do Not Sell My Info | Terms of Use | Trademark Policy | Cookie Preferences



STEP 15: Go to downloads of your machine and **install** it with default settings.





Check your database is created and status is available.

Successfully created database databasesudham

RDS > Databases > databasesudham

Summary

DB identifier databasesudham	CPU 6.45%	Status Available	Class db.t2.micro
Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ ap-south-1b

Connectivity & security

Endpoint databasesudham.c8kdtke5vhw.ap-south-1.rds.amazonaws.com	Networking Availability zone ap-south-1b VPC vpc-006fa63a4b125ac9a Subnet group default-vpc-006fa63a4b125ac9a Subnets	Security VPC security groups default (sg-077f2269a9988215b) Active Publicly accessible Yes Certificate authority Info rds-ca-2019
---	--	---

STEP 16: Click on to view credential.

STEP 17: Click on to database.

Consider creating a Blue/Green Deployment to minimize downtime during upgrades

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

DB identifier	Role	Engine	Region & AZ	Size	Status	Actions
databasesudham	Instance	MySQL Community	ap-south-1b	db.t2.micro	Available	1 Action

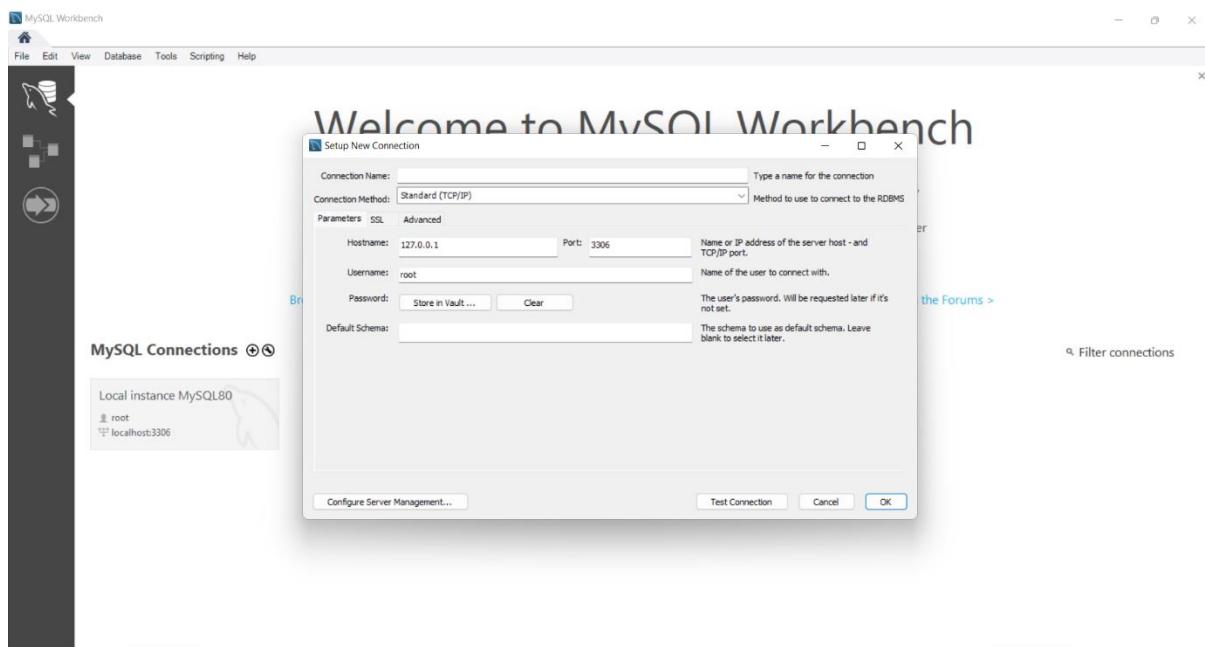
STEP 18: Copy Endpoint.

Connectivity & security

Endpoint databasesudham.c8kdtke5vhw.ap-south-1.rds.amazonaws.com	Networking Availability Zone ap-south-1b VPC vpc-006fa63a4b125ac9a Subnet group default-vpc-006fa63a4b125ac9a Subnets subnet-0a4135f2296078778 subnet-099dca33802577893 subnet-0fe6e6e885db04f1be Network type IPv4	Security VPC security groups default (sg-077f2269a9988215b) Active Publicly accessible Yes Certificate authority Info rds-ca-2019 Certificate authority date August 22, 2024, 22:38 (UTC+05:30) DB instance certificate expiration date August 22, 2024, 22:38 (UTC+05:30)
---	---	--

STEP 19: Go back to **workbench**.

STEP 20: Click on to mysql connection

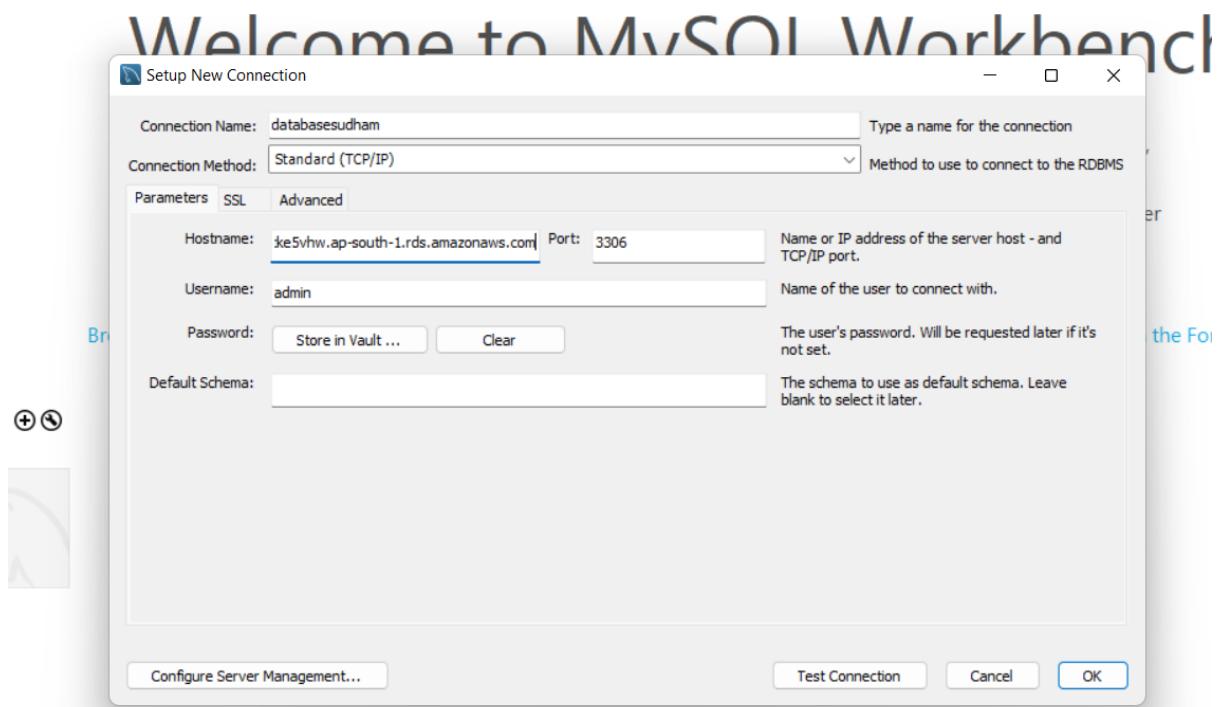


STEP 21: Paste copied endpoint in Hostname

Connection Name: databasesudham

Username: admin

Click on to **Test Connection**.



Enter **admin password**



STEP 22: Go to VPC security group.

The screenshot shows the AWS VPC Security Group details page for a specific endpoint. The endpoint is `databasesudham.c8kdttk5vhw.ap-south-1.rds.amazonaws.com` on port 3306. The VPC is `vpc-006fa63a4b125ac9a`. The security group is `default (sg-077f2269a9988215b)`, which is active. The subnet group is `default-vpc-006fa63a4b125ac9a`, and the subnets are `subnet-0a4135f2296078778`, `subnet-099dca33802577893`, and `subnet-0f6e6e885db04f1be`. The network type is IPv4. The certificate authority is `rds-ca-2019`, and the certificate authority date is August 22, 2024, 22:38 (UTC+05:30). The DB instance certificate expiration date is August 22, 2024, 22:38 (UTC+05:30).

STEP 23: Click on to Inbound rules.

The screenshot shows the AWS Security Groups Inbound rules page for the `sg-077f2269a9988215b - default` security group. There is one inbound rule listed, which can be edited or managed. The page also includes a message about running the Reachability Analyzer and links for managing tags and editing rules.



STEP 24: First select Click on to Edit inbound rule add rule select ipv4 --all traffic (add 0.0.0.0/0) and save Rules
(Important step to add inbound rule)

Inbound rules

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0f68553fbecf7dfdd	All traffic	All	All	Custom	sg-077f2269a9988215b
-	All traffic	All	All	Anywhere	0.0.0.0/0

Add rule Cancel Preview changes Save rules

Inbound security group rules successfully modified on security group (sg-077f2269a9988215b | default)

Name	Security group ID	Security group name	VPC ID	Description	Owner
sg-07990f1e62b5bd05b	launch-wizard-1	vpc-006fa63a4b125ac9a	launch-wizard-1 create...	793536247045	
sg-0393a7f77d5a4726d	launch-wizard-3	vpc-006fa63a4b125ac9a	launch-wizard-3 create...	793536247045	
sg-077f2269a9988215b	default	vpc-006fa63a4b125ac9a	default VPC security gr...	793536247045	
sg-0e47ddbfsae746661	launch-wizard-2	vpc-006fa63a4b125ac9a	launch-wizard-2 create...	793536247045	

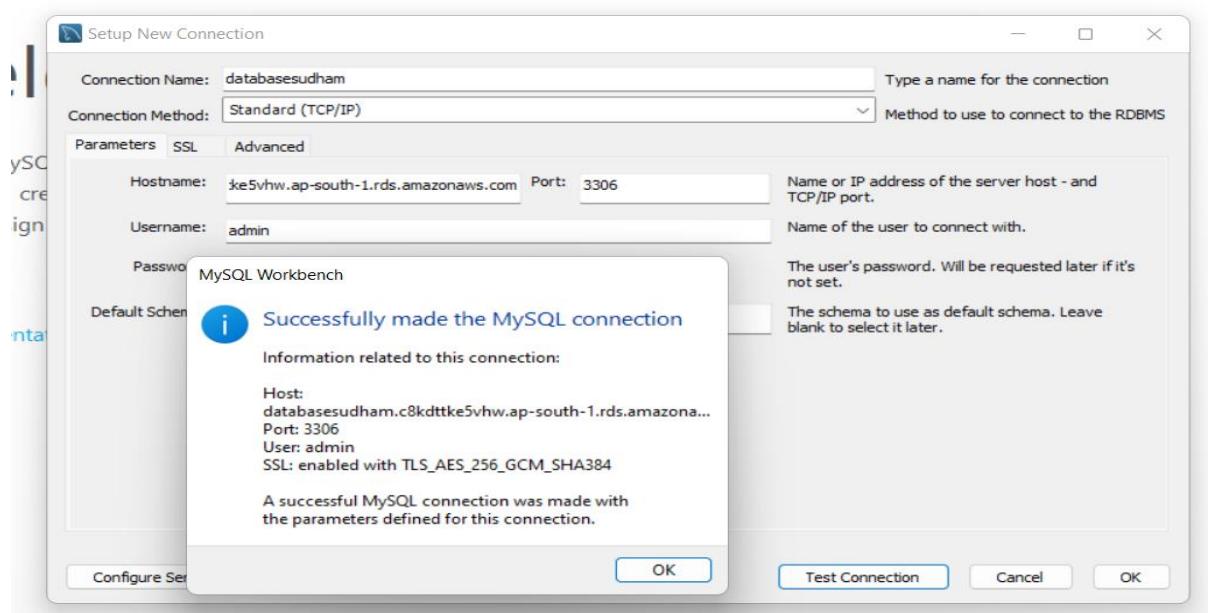
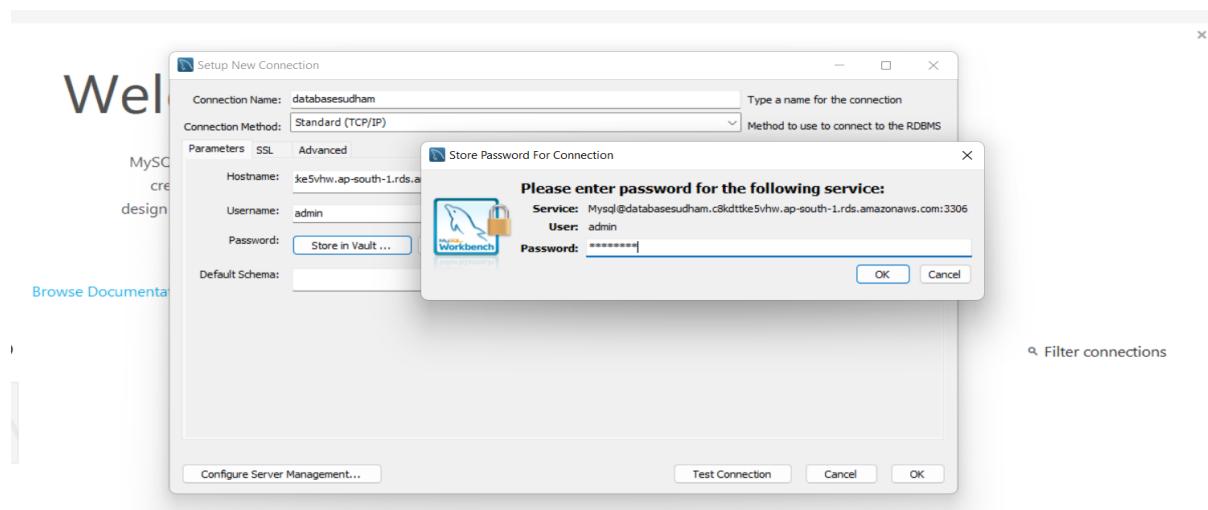
sg-077f2269a9988215b - default

Inbound rules (2)

Run Reachability Analyzer

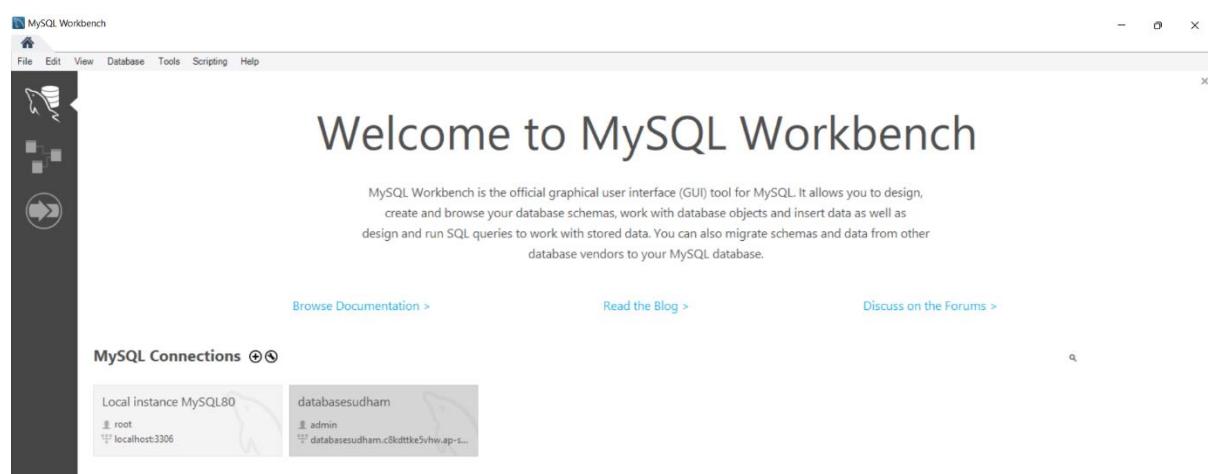


STEP 25: Go to **workbench** (after giving details click on to Test Connection).



Click on **Ok** button

Go to workbench double click on connection (**databasesudham**)





It will get opened.

The screenshot shows the MySQL Workbench interface. The title bar says "MySQL Workbench" and "databasesudham". The left sidebar has sections for MANAGEMENT (Server Status, Client Connections, Users and Privileges, Status and System Variables, Data Export, Data Import/Restore), INSTANCE (Startup / Shutdown, Server Logs, Options File), and PERFORMANCE (Dashboard, Performance Reports, Performance Schema Setup). The main area is titled "Query 1" and contains a toolbar with various icons. Below the toolbar is a text input field with "1" in it. A message in the center says "Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help." At the bottom, there are tabs for "Object Info" and "Session".

STEP 26: Write query and execute

Create database tsec;

Use tsec;

Show tables;

create table student(roll int, name varchar(10), city varchar(10));

Desc student;

insert into student values(1,'sudham','kalyan');

The screenshot shows the MySQL Workbench interface after executing the queries. The "Query 1" window now displays the following SQL code:

```
1 create database tsec;
2 use tsec;
3 create table student( roll int, name varchar(10), city varchar (10));
4 desc student;
5 insert into student values(1,'sudham','kalyan');
6 select * from student;
```

Below the code, the "Result Grid" shows a single row of data:

roll	name	city
1	sudham	kalyan

The "Output" window at the bottom shows the execution log with the following details:

#	Time	Action	Message	Duration / Fetch
1	00:38:34	create database tsec	1 row(s) affected	0.109 sec
2	00:39:01	use tsec	0 row(s) affected	0.110 sec
3	00:41:26	create table student(roll int, name varchar(10), city varchar (10))	0 row(s) affected	0.109 sec
4	00:42:05	desc student	3 row(s) returned	0.094 sec / 0.000 sec
5	00:43:59	insert into student values(1,'sudham','kalyan')	1 row(s) affected	0.094 sec
6	00:44:31	select * from student LIMIT 0, 1000	1 row(s) returned	0.094 sec / 0.000 sec



STEP 27: Now delete the instance (once you have done with it)

Select instance go to action **stop instance** and then **delete instance**.

The screenshot shows the AWS RDS console with the 'Databases' page. On the left, there's a sidebar with various navigation links. The main area displays a table of databases, with one row selected. An 'Actions' dropdown menu is open over the selected database, showing options like 'Stop temporarily', 'Reboot', and 'Delete'. The 'Delete' option is highlighted with a blue border.

The screenshot shows the AWS RDS console with the 'Databases' page. A modal window at the top center says 'Stopping database databasesudham is in progress'. The main area shows the database table again, but the 'Actions' column for the selected database now shows 'Stopping' instead of 'Delete'.

Uncheck create final snapshot.



ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databases:

RDS > Databases

Delete databasesudham instance?

Are you sure you want to Delete the **databasesudham** DB Instance?

Create final snapshot
Determines whether a final DB Snapshot is created before the DB instance is deleted.

Retain automated backups
Determines whether retaining automated backups for 7 days after deletion

I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available.

To confirm deletion, type **delete me** into the field:
delete me

Cancel **Delete**

Databases

Region & AZ: south-1b Size: db.t2.micro Status: Stopping Actions: 1 Action

ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databases:

RDS > Databases

Successfully deleted DB instance databasesudham

Consider creating a Blue/Green Deployment to minimize downtime during upgrades
You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases

No instances found

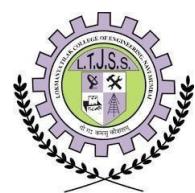
As you can see that DB instance is deleted successfully.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23**

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	05
DOP	28/02/2023
DOS	



SECURITY AS A SERVICE ON AWS

Aim : To study Security as a Service on AWS Security

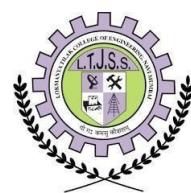
Theory :

Cloud security at AWS is the highest priority. As organizations embrace the scalability and flexibility of the cloud, AWS is helping them evolve security, identity, and compliance into key business enablers. AWS builds security into the core of our cloud infrastructure, and offers foundational services to help organizations meet their unique security requirements in the cloud.

- As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. Security in the cloud is much like security in your on-premises data centers—only without the costs of maintaining facilities and hardware. In the cloud, you don't have to manage physical servers or storage devices. Instead, you use software-based security tools to monitor and protect the flow of information into and out of your cloud resources.
- An advantage of the AWS Cloud is that it allows you to scale and innovate, while maintaining a secure environment and paying only for the services you use. This means that you can have the security you need at a lower cost than in an on-premises environment.
- As an AWS customer you inherit all the best practices of AWS policies, architecture, and operational processes built to satisfy the requirements of our most security-sensitive customers. Get the flexibility and agility you need in security controls.
- The AWS Cloud enables a shared responsibility model. While AWS manages security of the cloud, you are responsible for security in the cloud. This means that you retain control of the security you choose to implement to protect your own content, platform, applications, systems, and networks no differently than you would in an on-site data center.
- AWS provides you with guidance and expertise through online resources, personnel, and partners. AWS provides you with advisories for current issues, plus you have the opportunity to work with AWS when you encounter security issues.
- You get access to hundreds of tools and features to help you to meet your security objectives. AWS provides security-specific tools and features across network security, configuration management, access control, and data encryption.
- Finally, AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals. In the AWS environment, you can take advantage of automated tools for asset inventory and privileged access reporting.

Benefits of AWS security

- **Keep Your data safe —** The AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure AWS data centers.
- **Meet compliance requirements —** AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
- **Save money —**Cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility
- **Scale quickly —** Security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.



Security as a Service on AWS refers to a set of cloud-based security services that are provided by Amazon Web Services (AWS) to help customers secure their applications and data in the cloud.

The screenshot shows the AWS Management Console with the sidebar open, displaying a list of services. The 'Services' button is highlighted. The search bar contains 'Search'. The keyboard shortcut '[Alt+S]' is shown in the top right. The main content area is titled 'Security, Identity, & Compliance' and lists various services:

- AWS Artifact
- AWS Audit Manager
- Certificate Manager
- CloudHSM
- Cognito
- Detective
- Directory Service
- AWS Firewall Manager
- GuardDuty
- IAM
- IAM Identity Center (successor to AWS Single Sign-On)

Amazon Inspector

Continual vulnerability management at scale

Key Management Service

Securely Generate and Manage AWS Encryption Keys

Amazon Macie

Amazon Macie classifies and secures your business-critical content.

AWS Private Certificate Authority

Managed private certificate authority service

Resource Access Manager

Share AWS resources with other accounts or AWS Organizations

Secrets Manager

Easily rotate, manage, and retrieve secrets throughout their lifecycle

Security Hub

AWS Security Hub is AWS's security and compliance center

Security Lake

Automatically centralize all your security data with a few clicks

AWS Signer

Ensuring trust and integrity of your code

Amazon Verified Permissions

Manage, analyze and enforce permissions across your applications

WAF & Shield

Protects Against DDoS Attacks and Malicious Web Traffic



To study Security as a Service on AWS, you can follow the following steps:

- **Learn about the AWS Shared Responsibility Model:** The AWS Shared Responsibility Model is a critical concept to understand when it comes to security on AWS. AWS is responsible for securing the infrastructure that runs the cloud, while the customer is responsible for securing their data and applications in the cloud. Understanding the shared responsibility model is critical to ensuring that you are securing your applications and data appropriately on AWS.
- **Understand the various AWS Security Services:** AWS offers a wide range of security services that can help you secure your applications and data. These services include:
 1. Identity and Access Management (IAM): IAM allows you to manage access to AWS resources securely. You can create users and groups, assign permissions, and use IAM roles to grant temporary access to users or services.
 2. Amazon Inspector: Inspector is an automated security assessment service that helps you test the security of your applications and infrastructure.
 3. Amazon GuardDuty: GuardDuty is a threat detection service that continuously monitors for malicious activity in your AWS account.
 4. AWS WAF: The AWS Web Application Firewall (WAF) helps you protect your web applications from common web exploits and attacks.
 5. Amazon Macie: Macie is a fully managed data security and privacy service that uses machine learning and pattern matching to discover and protect sensitive data.
 6. AWS Certificate Manager: Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources.
- **Study AWS Security Best Practices:** AWS publishes a set of security best practices for all of its services. These best practices include detailed guidance on how to secure your applications and data, and they cover topics such as access management, network security, data encryption, and logging.
- **Review AWS Compliance and Security Reports:** AWS regularly publishes compliance and security reports, such as SOC 2, ISO 27001, and PCI DSS reports. These reports provide independent verification of AWS's compliance with industry-standard security and compliance frameworks.
- **Practice with AWS Security Services:** AWS provides a free tier that allows you to experiment with many of its security services without incurring any costs. Use this opportunity to practice and experiment with AWS security services.
- **Get Certified:** AWS offers several security-related certifications, such as AWS Certified Security – Specialty. These certifications demonstrate your knowledge and expertise in securing applications and data on AWS. Consider getting certified to validate your skills.
- **Stay up-to-date:** AWS is constantly updating and adding new security features and services. Stay up-to-date with these changes by reading AWS blogs, attending webinars, and participating in AWS events.

By following these steps, you can gain a comprehensive understanding of Security as a Service on AWS and become proficient in securing applications and data in the cloud.



8 Securities Case Study

8 Securities uses the following products from AWS as part of its infrastructure:

- **Amazon EC2 Windows instances**— To run the portal, main website, and business intelligence tools
- **Elastic IP Addresses for Amazon EC2**—To bind to domain names, and start and stop instances on demand
- **Amazon EBS**— Used for data storage, for starting and stopping instances, and for having data always available
- **Amazon VPC**— Used for a production network. Roll notes, “As some of our applications are bound to the machine Media Access Control [MAC] address, the key benefit for us is to have static MAC addresses when instances are restarted.”
- **Elastic Load Balancing**— Used for the main website, to load balance across multiple instances

Top 6 AWS Account Security Tools

1. AWS Identity and Access Management (IAM)

AWS IAM is essential for controlling access to your AWS resources. It enables you to create users and roles with permissions to specific resources in your AWS environment. Always assigning least-privilege permissions to these users and roles minimizes the impact of a breach where an attacker has gained access. AWS IAM also has multi-factor authentication and supports single sign-on (SSO) access to further secure and centralize user access.

2. Amazon GuardDuty

Amazon GuardDuty uses machine learning to look for malicious activity in your AWS environments. It combines your CloudTrail event logs, VPC Flow Logs, S3 event logs, and DNS logs to continuously monitor and analyze all activity. GuardDuty identifies issues such as privilege escalation, exposed credentials, and communication with malicious IP addresses and domains. It can also detect when your EC2 instances are serving malware or mining bitcoin.

3. Amazon Macie

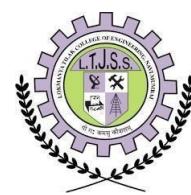
Amazon Macie discovers and protects your sensitive data stored in AWS S3 buckets. It first identifies sensitive data in your buckets, such as personally-identifiable information or personal health information, through discovery jobs. You can schedule these jobs to monitor new data added to your buckets. After it finds sensitive data, Macie continuously evaluates your buckets and alerts you when a bucket is unencrypted, is publicly accessible, or is shared with AWS accounts outside of your organization.

4. AWS Config

AWS Config records and continuously evaluates your AWS resource configuration. This includes keeping a historical record of all changes to your resources, which is useful for compliance with legal requirements and your organization's policies. AWS Config evaluates new and existing resources against rules that validate certain configurations. For example, if all EC2 volumes must be encrypted, AWS Config can detect non-encrypted volumes and send a notification. In addition, it can also execute remediation actions such as encrypting the volume or deleting it.

5. AWS CloudTrail

AWS CloudTrail tracks all activity in your AWS environment. It records all actions a user executes in the AWS console and all API calls as events. You can view and search these events to identify unexpected or unusual requests in your AWS environment.



6. Security Hub

AWS Security Hub combines information from all the above services in a central, unified view. It collects data from all security services from multiple AWS accounts and regions, making it easier to get a complete view of your AWS security posture. In addition, Security Hub supports collecting data from third-party security products. Security Hub is essential to providing your security team with all the information they may need.

Top 4 AWS Application Security Tools

1. Amazon Inspector

Amazon Inspector is a security assessment service for applications deployed on EC2. These assessments include network access, common vulnerabilities and exposures (CVEs), Center for Internet Security (CIS) benchmarks, and common best practices such as disabling root login for SSH and validating system directory permissions on your EC2 instances.

2. AWS Shield

AWS Shield is a fully-managed distributed denial-of-service (DDoS) protection service. Shield is enabled by default as a free standard service with protection against common DDoS attacks against your AWS environment.

3. AWS Web Application Firewall

AWS Web Application Firewall (WAF) monitors and protects applications and APIs built on services such as CloudFront, API Gateway, and AppSync. You can block access to your endpoints based on different criteria such as the source IP address, the request's origin country, values in headers and bodies, and more (i.e, you can enable rate limiting, only allowing a certain number of requests per IP)

4. AWS Secrets Manager

AWS Secrets Manager is a managed service where you can store and retrieve sensitive information such as database credentials, certificates, and tokens. Use fine-grained permissions to specify exact actions an entity can perform on the secrets, such as creating, updating, deleting, or retrieving secrets.

Conclusion : We had successfully studied Security as a Service on AWS Security.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23**

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	06
DOP	
DOS	



IAM - (IDENTITY & ACCESS MANAGEMENT)

Step 1 - Sign in. Sign in as a root user. Provide username and password when prompted. Open the console and search for **IAM** and click on it.

The screenshot shows the AWS Services search results for 'iam'. The 'Services' section on the left lists various services like Features, Resources (New), Blogs, Documentation, Knowledge Articles, Tutorials, Events, and Marketplace. The main search results show 'Search results for 'iam'' with three items: 'IAM' (Manage access to AWS resources), 'IAM Identity Center (successor to AWS Single Sign-On)' (Manage workforce user access to multiple AWS accounts and cloud applications), and 'Resource Access Manager' (Share AWS resources with other accounts or AWS Organizations). A link 'See all 8 results' is also visible.

Step 2 - Select the Users menu. Navigate to the Users screen. You'll find it in the IAM dashboard, under **Identity and Access Management (IAM)** drop-down menu on the left side of the screen. Click on **Users**.

The screenshot shows the IAM dashboard. On the left sidebar, under 'Identity and Access Management (IAM)', the 'Users' option is selected. The main content area displays the 'IAM dashboard' with sections for 'Security recommendations' (including 'Add MFA for root user', 'Root user has no active access keys', and 'Update your access permissions for AWS Billing, Cost Management, and Account consoles'), 'AWS Account' (Account ID: 404055596869, Account Alias: 404055596869, Create), 'Quick Links' (My security credentials, Policy simulator, Web identity federation playground), and 'Tools' (Feedback, Language, Copyright notice, Privacy, Terms, Cookie preferences). The 'IAM resources' section shows counts for User groups (0), Users (0), Roles (8), Policies (0), and Identity providers (0).

Step 3 - Add a user. Click on **Add User** to navigate to a user detail form. Provide all details, such as the username and access type. We use the name **cli-user**, and check the **Programmatic access** box under **Access type**. This option gives the user access to AWS development tools, such as the command line interface used later. Click on **Next: Permissions** to continue.



Screenshot of the AWS IAM Management Console showing the 'Users' page and the 'Create user' wizard.

The 'Users' page displays a table with columns: User name, Groups, Last activity, MFA, Password age, and Active key age. A message at the bottom says "No resources to display".

The 'Create user' wizard is on Step 1: Specify user details. It shows the 'User details' section where the 'User name' is set to "sudham2412". A note says "The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, ., @, _ (hyphen)". An optional checkbox "Provide user access to the AWS Management Console - optional" is checked. A note says "If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center." Below this, there are sections for "Console password" (radio buttons for "Autogenerated password" and "Custom password"), "Show password" (checkbox), and "Users must create a new password at next sign-in (recommended)" (checkbox). A note says "Users automatically get the IAMUserChangePassword policy to allow them to change their own password." A note at the bottom says "If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more".

Step 4 - Set the user permissions. Click **Attach existing policies directly** and then filter the policies by keyword: IAM. For this user, select **IAMFullAccess** from the list of available policies.

The **IAMFullAccess** policy enables this user to create and manage user permissions in AWS. Later, this user will perform AWS IAM operations.

Screenshot of the 'Set permissions' step of the 'Create user' wizard.

The 'Permissions options' section has three radio buttons: "Add user to group" (disabled), "Copy permissions" (disabled), and "Attach policies directly" (selected). A note says "Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group."

The 'Permissions policies (1/1050)' section shows a search bar with "iamfullaccess" and a table with one result: "Policy name: IAMFullAccess" (Type: AWS managed, Attached entities: 0).

The 'Permissions boundary - optional' section is collapsed.



Step 5 - Finish the user setup. We will skip the tags section of user creation and go to the review page. Check details of the username, AWS access type & permissions. Then, click **Create user**.

The screenshot shows the 'Review and create' step of the IAM user creation wizard. It displays the following information:

- User details:** User name: sudham2412. Console password type: Custom password. Require password reset: Yes.
- Permissions summary:** Shows two policies assigned:
 - IAMFullAccess (AWS managed, Permissions policy)
 - IAMUserChangePassword (AWS managed, Permissions policy)
- Tags - optional:** A note stating "Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user." Below it says "No tags associated with the resource." and has a "Add new tag" button.
- Buttons at the bottom:** Cancel, Previous, Create user (highlighted in orange).

Step 6 - At this point, the user cli-user exists, with the chosen policies applied to the account. AWS provides this user an access key ID and secret access key. Download or copy these keys to a secure place to use later.

The screenshot shows the 'Retrieve password' step of the IAM user creation wizard. It displays the following information:

- Console sign-in details:** Console sign-in URL: https://404055596869.signin.aws.amazon.com/console. User name: sudham2412. Console password: ***** (Show button available).
- Buttons at the bottom:** Download .csv file, Return to users list (highlighted in orange).

The screenshot shows the 'Users' list in the AWS IAM console. It displays the following information:

- Users (1) Info:** An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
- Table:** Shows one user entry:

User name	Groups	Last activity	MFA	Password age	Active key age
sudham2412	None	Never	None		
- Buttons at the top right:** Delete, Add users.



Set up AWS user credentials in the CLI

With minimal setup, AWS CLI enables an admin to use their favorite shell or CLI to interact with AWS services. You can choose any Linux distribution or shell. This demonstrates a Bash shell running on an Ubuntu Linux distribution.

1. Install the command line tool. First, install AWS CLI on your system using the following command in Bash terminal : **sudo apt install awscli**

```
Activities Terminal Mar 16 10:54 AM computer@computer-ThinkCentre:~
```

```
(base) computer@computer-ThinkCentre:~$ sudo apt install awscli
[sudo] password for computer:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libevent-core-2.1-7
  libevent-pthreads-2.1-7 libflashrom1 libfdt1-2
  libgstreamer-plugins-bad1.0-0 libjs-highlight.js libl LLVM13 libl LLVM13:i386
  libmecab2 mecab-ipadic mecab-ipadic-utf8 mecab-utils
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  docutils-common groff gsfonts imagemagick imagemagick-6-common
  imagemagick-6.q16 libjxr-tools libjxr0 liblqr-1-0 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 netpbm psutils
  python3-botocore python3-docutils python3-jmespath python3-pyasn1
  python3-pygments python3-roman python3-rsa python3-s3transfer
Suggested packages:
  imagemagick-doc autotrace curl enscript ffmpeg gnuplot grads hp2xx html2ps
  libwmf-bin mplayer povray radiance transfig ufraw-batch inkscape
  docutils-doc fonts-linuxlibertine | ttf-linux-libertine texlive-lang-french
  python-pygments-doc ttf-bitstream-vera
The following NEW packages will be installed:
  awscli docutils-common groff gsfonts imagemagick imagemagick-6-common
  imagemagick-6.q16 libjxr-tools libjxr0 liblqr-1-0 libmagickcore-6.q16-6
  libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 netpbm psutils
  python3-botocore python3-docutils python3-jmespath python3-pyasn1
  python3-pygments python3-roman python3-rsa python3-s3transfer
0 upgraded, 24 newly installed, 0 to remove and 8 not upgraded.
Need to get 18.1 MB of archives.
After this operation, 114 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblqr-1-0 amd64 0.4.2-2.1 [27.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 imagemagick-6-common all 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1 [64.5 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libmagickcore-6.q16-6 amd64 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1 [1,789 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libmagickwand-6.q16-6 amd64 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1 [328 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/universe amd64 groff amd64 1.22.4-8build1 [4,104 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/main amd64 python3-jmespath all 0.10.0-1 [21.7 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy/universe amd64 python3-botocore all 1.23.34+repack-1 [4,508 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy/main amd64 python3-pyasn1 all 0.4.8-1 [50.9 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy/main amd64 docutils-common all 0.17.1+dfsg-2 [117 kB]

Setting up libmagickcore-6.q16-6-extra:amd64 (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
Setting up imagemagick-6.q16 (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
update-alternatives: using /usr/bin/compare-im6.q16 to provide /usr/bin/compare (compare) in auto mode
update-alternatives: using /usr/bin/compare-im6.q16 to provide /usr/bin/compare-im6 (compare-im6) in auto mode
update-alternatives: using /usr/bin/animate-im6.q16 to provide /usr/bin/animate (animate) in auto mode
update-alternatives: using /usr/bin/animate-im6.q16 to provide /usr/bin/animate-im6 (animate-im6) in auto mode
update-alternatives: using /usr/bin/convert-im6.q16 to provide /usr/bin/convert (convert) in auto mode
update-alternatives: using /usr/bin/convert-im6.q16 to provide /usr/bin/convert-im6 (convert-im6) in auto mode
update-alternatives: using /usr/bin/composite-im6.q16 to provide /usr/bin/composite (composite) in auto mode
update-alternatives: using /usr/bin/composite-im6.q16 to provide /usr/bin/composite-im6 (composite-im6) in auto mode
update-alternatives: using /usr/bin/conjure-im6.q16 to provide /usr/bin/conjure (conjure) in auto mode
update-alternatives: using /usr/bin/conjure-im6.q16 to provide /usr/bin/conjure-im6 (conjure-im6) in auto mode
update-alternatives: using /usr/bin/import-im6.q16 to provide /usr/bin/import (import) in auto mode
update-alternatives: using /usr/bin/import-im6.q16 to provide /usr/bin/import-im6 (import-im6) in auto mode
update-alternatives: using /usr/bin/identify-im6.q16 to provide /usr/bin/identify (identify) in auto mode
update-alternatives: using /usr/bin/identify-im6.q16 to provide /usr/bin/identify-im6 (identify-im6) in auto mode
update-alternatives: using /usr/bin/stream-im6.q16 to provide /usr/bin/stream (stream) in auto mode
update-alternatives: using /usr/bin/stream-im6.q16 to provide /usr/bin/stream-im6 (stream-im6) in auto mode
update-alternatives: using /usr/bin/display-im6.q16 to provide /usr/bin/display (display) in auto mode
update-alternatives: using /usr/bin/display-im6.q16 to provide /usr/bin/display-im6 (display-im6) in auto mode
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage (montage) in auto mode
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage-im6 (montage-im6) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify (mogrify) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify-im6 (mogrify-im6) in auto mode
Setting up imagemagick (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for sgml-base (1.30) ...
Setting up python3-docutils (0.17.1+dfsg-2) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Setting up awscli (1.22.34-1) ...
```



Once the setup runs, verify the installation by checking the version : **aws –version**

```
(base) computer@computer-ThinkCentre:~$ aws --version
aws-cli/1.22.34 Python/3.10.6 Linux/5.19.0-35-generic botocore/1.23.34
(base) computer@computer-ThinkCentre:~$
```

2. Configure the user with the keys. Run the **aws configure** command in the shell to quickly set up the access key ID & secret access key obtained from AWS when you created a new user in IAM console.

```
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws configure
AWS Access Key ID [None]: AKIAJXWRV
AWS Secret Access Key [None]: sudham2412
Default region name [ap-south-1]:
Default output format [json]: json
(base) computer@computer-ThinkCentre:~$
```

This step saves your credentials in a local file at path: `~/.aws/credentials` and region and output format configs at path: `~/.aws/config` file.

Now that cli-user with programmatic access is set up, we can use that account to create other users and give them policy-based access through AWS CLI. The next two sections walk through these steps.

Create a user and assign permissions

To create a user using IAM, run the `aws iam create-user` command in AWS CLI with a username:

```
aws iam create-user --user-name sudham2412
```

It creates a new user and shows the user details in the bash console.

```
(base) computer@computer-ThinkCentre:~$ aws iam create-user --user-name sudham2412{
  "User": {
    "Path": "/",
    "UserName": "sudham2412",
    "UserId": "AIDAXWRVBDHII7PCK47BG",
    "Arn": "arn:aws:iam::529465940434:user/sudham2412",
    "CreateDate": "2021-06-21T16:33:28Z"
  }
}
```

```
(base) computer@computer-ThinkCentre:~$
```

Suppose this user needs to manage EC2 services. To grant this new user EC2 admin rights, start by listing which EC2 policies we can grant. Use the command:

```
aws iam list-policies | grep EC2FullAccess
```

Identify the appropriate policy for the user's access level. In this case, it is `AmazonEC2FullAccess`. Pass the Amazon Resource Name (ARN) to the following command in `--policy-arn` parameter:

```
aws iam attach-user-policy --user-name sudham2412 --policy-arn
"arn:aws:iam::aws:policy/AmazonEC2FullAccess"
```

```
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws iam list-policies | grep EC2FullAccess
"PolicyName": "Amazon EC2FullAccess", "Arn": "arn:aws:iam::aws:policy/Amazon EC2FullAccess",
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws iam attach-user-policy --user-name sudham2412 --policy-arn
"arn:aws:iam::aws:policy/Amazon EC2FullAccess"
(base) computer@computer-ThinkCentre:~$
```

Check user details and list user permissions

Once you create the user and attach the appropriate user policy to them, verify that AWS assigned the appropriate policy by checking the user details.

To check the list of IAM users, run: `aws iam list-users`

The following command tells AWS to list all attached policies for a user account:

```
aws iam list-attached-user-policies --user-name sudham2412
```



```
(base) computer@computer-ThinkCentre:~$ ~
(base) computer@computer-ThinkCentre:~$ 
(base) computer@computer-ThinkCentre:~$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "cli-user",
      "UserId": "AIDAXWRVBDHJDOWXYJSI3",
      "Arn": "arn:aws:iam::529465940434:user/cli-user",
      "CreateDate": "2021-06-21T15:48:20Z"
    },
    {
      "Path": "/",
      "UserName": "sudham2412",
      "UserId": "AIDAXWRVBDHJ17PCK47BG",
      "Arn": "arn:aws:iam::529465940434:user/sudham2412", "CreateDate": "2021-06-21T16:33:28Z"
    }
  ]
}
(base) computer@computer-ThinkCentre:~$ aws iam list-attached-user-policies
--user-name sudham2412{
  "AttachedPolicies": [
    {
      "PolicyName": "Amazon EC2FullAccess",
      "PolicyArn": "arn:aws:iam::aws:policy/Amazon EC2FullAccess"
    }
  ]
}
(base) computer@computer-ThinkCentre:~$
```

- Now you can **delete** your users from **IAM - Access Management > Users** > select your username > click on **Delete**

The screenshot shows the AWS IAM 'Users' page. On the left, the navigation menu is expanded to show 'Access management' with 'Users' selected. The main area displays a table with one row for 'sudham2412'. The 'Delete' button is visible at the top right of the table.

User name	Groups	Last activity	MFA	Password age	Active key age
sudham2412	None	Never	None	10 minutes ago	-

- You can see the users you created deleted successfully.

The screenshot shows the same AWS IAM 'Users' page after the user 'sudham2412' has been deleted. A green banner at the top states 'User sudham2412 deleted.' Below it, the table is empty with the message 'No resources to display'.



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23**

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	07
DOP	21/03/2023
DOS	



DOCKER

Step 1 - Go to official website of docker : <https://hub.docker.com/>

Wasm is a fast, light alternative to Linux containers – try it out today with the [Docker+Wasm Beta](#).

Products ▾ Developers ▾ Pricing Blog About Us ▾ Partners ▾

Sign In Get Started

Play with Docker
Hands-on Docker Tutorials for Developers

Don't let app complexity get in the way of opportunity

Learn Docker today and join the millions of developers who use Docker Desktop and Docker Hub to simplify building and sharing world-changing apps

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Docker Desk....exe Cancelled Show all

Step 2 - Create your docker account

Step 3 - Choose for personal use with \$0 and click on Continue with Free

Choose a Plan

Select a plan to get started with Docker

Personal \$0

Includes the Docker essentials and is ideal for individual developers, students, open source communities, and small businesses.

- Docker Desktop
- Unlimited public repositories
- Docker Engine + Kubernetes
- Limited image pulls per day
- Unlimited scoped tokens

Pro \$5 /month

Extends the Docker capabilities and includes pro tools for individual developers who want to accelerate their productivity.

- Everything in Personal, plus:
- Docker Desktop
- Unlimited private repositories
- 5,000 image pulls per day
- 5 concurrent builds
- 300 vulnerability scans

Team \$9 /user/month max 100 users

Ideal for teams and includes capabilities for enhanced collaboration, productivity and security.

- Everything in Pro, plus:
- Hardened Docker Desktop
- Enhanced Container Isolation
- Settings management
- Centralized management
- Image Access Management
- Registry Access Management
- Single Sign-On (SSO)
- SCIM user provisioning
- VDI support
- Purchase via invoice
- Volume Pricing Available

Business \$24 /user/month

Ideal for medium and large businesses who need centralized management and advanced security capabilities.

- Pay annually with an annual subscription

Continue with Free Buy Now Buy Now Buy Now

Step 4 - You have to verify your account from your added gmail account through mail

Your email has been verified!



Step 5 - Creating first repository

Click on **Create a Repository**

Welcome to Docker
Download the desktop application
Download for Windows
Also available for Mac and Linux

Create a Repository
Push container images to a repository on Docker Hub.

Docker Hub Basics
Watch the guide on how to create and push your first image into a Docker Hub repository.

Language-Specific Guides
Learn how to containerize language-specific applications using Docker.

Access the world's largest library of container images

nginx, mongoDB, alpine, node, redis, busybox, ubuntu, python, postgres, httpd

Name it <your-username>/sudham
Set the visibility to private

Repositories / Create

Create repository

Namespace: sudham2412 | Repository Name*: sudham

Visibility

Using 0 of 1 private repositories. [Get more](#)

Public ⓘ
Appears in Docker Hub search results

Private ⓘ
Only visible to you

Pro tip
You can push a new image to this repository using
`docker tag local-image:tagname new-docker push new-repo:tagname`

Make sure to change `tagname` with your desired tag.

Create

Click on **Create**

sudham2412 / sudham

Description

... [Edit](#)

⌚ Last pushed: 23 minutes ago



Now next,

Step 6 - Click on Explore tab to see official and publisher images

The screenshot shows the Docker Hub explore page with a search bar and navigation links for Explore, Repositories, Organizations, and Help. A user profile for 'sudham2412' is visible. The main content displays a list of 1-25 of 10,000 available results, with a dropdown menu set to 'Suggested'. The first few items listed are:

- alpine** (Docker Official Image) - 1B+ stars, 9.8K pulls, updated 10 days ago. Description: A minimal Docker image based on Alpine Linux with a complete package index and onl... Tags: Linux, ARM 64, 386, PowerPC 64 LE, IBM Z, riscv64, x86-64, ARM. Pulls chart: 9,268,526 last week.
- nginx** (Docker Official Image) - 1B+ stars, 10K+ pulls, updated 9 days ago. Description: Official build of Nginx. Tags: Linux, ARM 64, 386, mips64le, PowerPC 64 LE, IBM Z, x86-64, ARM. Pulls chart: 32,868,043 last week.
- busybox** (Docker Official Image) - 1B+ stars, 2.9K pulls, updated 6 days ago. Description: Busybox base image. Tags: Linux, riscv64, IBM Z, x86-64, ARM, ARM 64, 386, mips64le, PowerPC 64 LE. Pulls chart: 12,698,125 last week.
- ubuntu** (Docker Official Image) - 1B+ stars, 10K+ pulls, updated 7 days ago. Description: Ubuntu is a Debian-based Linux operating system based on free software. Tags: Linux, ARM, ARM 64, PowerPC 64 LE, IBM Z, 386, riscv64, x86-64. Pulls chart: 25,915,974 last week.

Here you can click on the docker tab

The screenshot shows the Docker Hub Docker tab with a list of images. The tabs at the top include Docker.pdf, Explore Docker's ..., Install Docker Engine, docker_instructions, and Docker Playgrou. The Docker tab is active. The list of images includes:

- traefik** Updated 5 hours ago. Description: Traefik, The Cloud Native Edge Router. Tags: Linux, Windows, x86-64, ARM, ARM 64, IBM Z. Pulls chart: 1,222,191 last week.
- mariadb** (Docker Official Image) Updated 6 days ago. Description: MariaDB Server is a high performing open source relational database, forked from MyS... Tags: Linux, 386, x86-64, ARM 64, PowerPC 64 LE, IBM Z. Pulls chart: 5,158,020 last week.
- docker** (Docker Official Image) Updated 3 hours ago. Description: Docker in Docker!. Tags: Linux, Windows, ARM, PowerPC 64 LE, IBM Z, x86-64, ARM 64. Pulls chart: 4,007,808 last week.
- rabbitmq** (Docker Official Image) Updated a day ago. Description: RabbitMQ is an open source multi-protocol messaging broker. Tags: Linux, 386, riscv64, x86-64, ARM, ARM 64, PowerPC 64 LE, IBM Z. Pulls chart: 1,607,377 last week.
- hello-world** (Docker Official Image) Updated 7 days ago. Description: Hello World! (an example of minimal Dockerization). Tags: Linux, Windows, mips64le, PowerPC 64 LE, riscv64, IBM Z, x86-64, ARM, ARM 64, 386. Pulls chart: 5,005,679 last week.

You can explore that tab in which various versions of docker's downloads are given.
You can select various platforms, architecture and operating systems



Installing using apt repository on ubuntu

Before you install Docker Engine for the first time on a new host machine, you need to set up the Docker repository. Afterward, you can install and update Docker from the repository.

Set up the repository

Step 1 - Update the apt package index and install packages to allow apt to use a repository over HTTPS:

```
sudo apt-get update  
sudo apt-get install \  
    ca-certificates \  
    curl \  
    gnupg
```

Step 2 - Add Docker's official GPG key:

```
sudo mkdir -m 0755 -p /etc/apt/keyrings  
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o  
/etc/apt/keyrings/docker.gpg
```

Step 3 - Use the following command to set up the repository:

```
echo \  
"deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyrings/docker.gpg]  
https://download.docker.com/linux/ubuntu \  
"$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \  
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

```
(base) computer@computer-ThinCentre:~$ sudo apt-get update  
sudo apt-get install \  
    ca-certificates \  
    curl \  
    gnupg \  
    lsb-release  
Hit:1 https://deb.nodesource.com/node_16.x jammy InRelease  
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease  
Hit:3 https://ppa.launchpadcontent.net/gns3/ppa/ubuntu jammy InRelease  
Get:4 https://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]  
Hit:5 https://dl.google.com/linux/chrome/deb stable InRelease  
Get:6 https://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]  
Get:7 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Fetched 396 kB in 4s (79.7 kB/s)  
Reading package lists... Done  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
lsb-release is already the newest version (11.1.0ubuntu4).  
lsb-release set to manually installed.  
ca-certificates is already the newest version (20210101ubuntu0.22.04.1).  
ca-certificates set to manually installed.  
gnupg is already the newest version (2.2.27-3ubuntu2.1).  
gnupg set to manually installed.  
The following packages were automatically installed and are no longer required:  
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi gyp javascript-common  
libflashrom1 liblfdi1-2 libgstreamer-plugins-bad1.0-0 libjs-events  
libjs-highlight.js libjs-inherits libjs-is-typedarray libjs-psl  
libjs-source-map libjs-sprintf.js libjs-typedarray-to-buffer libnode-dev  
libnode72 libssl-dev libuv1-dev node-abrev node-ansi-regex node-ansi-styles  
node-ansi-styles node-are-we-there-yet node-arrify node-asap node-asynckit  
node-balanced-match node-brace-expansion node-chownr node-clean-yaml-object  
node-color-convert node-color-name node-commander node-core-util-is  
node-decompress-response node-delayed-stream node-delegates node-depd  
node-diff node-encoding node-end-of-stream node-node-err-code  
node-escape-string-regexp node-fancy-log node-foreground-child  
node-fs.realpath node-function-bind node-get-stream node-glob node-growl  
node-has-flag node-has-unicode node-hosted-git-info node-iconv-lite  
node-tferri node-influrnurhash node-indent-string node-inflight node-inherits  
node-tnt node-ip node-ip-regex node-ts-buffer node-is-plain-obj  
node-ts-typedarray node-isarray node-issex node-json-parse-better-errors  
node-jsonparse node-kindof node-lodash-packages node-lowercase-keys  
node-lru-cache node-matches response node-minmatch node-minlist  
node-npm-pass node-queue stream node-negotiator node-npm bundled node-once  
node-osenv node-p-cancelable node-p-map node-path-is-absolute  
node-process-nextick-args node-promise-inflight node-promise-retry  
node-promzard node-pump node-quick-lru node-read node-readable-stream  
node-resolve node-retry node-safe-buffer node-set-blocking node-signal-exit  
node-slash node-slice-ansi node-source-map node-spdx-correct  
node-spdx-exceptions node-spdx-expression-parse node-spdx-license-ids  
node-sprintf.js node-stealthy-require node-string-decoder  
node-supports-color node-text-table node-time-stamp node-tmatch  
node-typedarray-to-buffer node-universalify node-util-deprecate  
node-validate-npm-package-license node-webidl-conversions node-whatwg-fetch  
node-wrapify node-yallist  
Use 'sudo apt autoremove' to remove them.
```



Installing Docker Engine

Step 1 - Update the apt package index : `sudo apt-get update`

Receiving a GPG error when running apt-get update?

Your default umask may be incorrectly configured, preventing detection of the repository public key file. Try granting read permission for the Docker public key file before updating the package index : `sudo chmod a+r /etc/apt/keyrings/docker.gpg`

`sudo apt-get update`

Step 2 - Install Docker Engine, containerd, and Docker Compose.

`sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin`

```
(base) computer@computer-ThinkCentre:~$ sudo apt-get update
Get:1 https://download.docker.com/linux/ubuntu jammy InRelease [48.9 kB]
Get:2 https://download.docker.com/linux/ubuntu jammy/stable amd64 Packages [13.6 kB]
Hit:3 https://deb.nodesource.com/node_16.x jammy InRelease
Hit:4 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:5 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:7 https://ppa.launchpadcontent.net/gns3/ppa/ubuntu jammy InRelease
Get:8 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 398 kB in 4s (106 kB/s)
Reading package lists... Done
(base) computer@computer-ThinkCentre:~$ sudo chmod a+r /etc/apt/keyrings/docker.gpg
sudo apt-get update
Hit:1 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:2 https://deb.nodesource.com/node_16.x jammy InRelease
Hit:3 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:6 https://ppa.launchpadcontent.net/gns3/ppa/ubuntu jammy InRelease
Get:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 336 kB in 2s (217 kB/s)
Reading package lists... Done

(base) computer@computer-ThinkCentre:~$ sudo apt-get update
Hit:1 https://download.docker.com/linux/ubuntu jammy InRelease
Hit:2 https://deb.nodesource.com/node_16.x jammy InRelease
Hit:3 https://dl.google.com/linux/chrome/deb stable InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:5 https://ppa.launchpadcontent.net/gns3/ppa/ubuntu jammy InRelease
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 336 kB in 2s (173 kB/s)
Reading package lists... Done
(base) computer@computer-ThinkCentre:~$ sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
```

Step 3 - Verify that the Docker Engine installation is successful by running the hello-world image : `sudo docker run hello-world`

Step 4 - Check docker version to ensure that its installed successfully : `docker -v`

```
(base) computer@computer-ThinkCentre:~$ sudo docker run hello-world
Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

(base) computer@computer-ThinkCentre:~$ docker -v
Docker version 23.0.1, build a5ee5b1
(base) computer@computer-ThinkCentre:~$
```



Creating containerised docker

Step 1 - Cloning : `git clone https://github.com/docker/Cloning` into 'getting-started'...

Step 2 - Open code : `code ./getting-started/app/`

```
(base) computer@computer-ThinkCentre:~/Documents/AIML/CCL$ git clone https://github.com/docker/getting-started.git
Cloning into 'getting-started'...
remote: Enumerating objects: 957, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 957 (delta 0), reused 1 (delta 0), pack-reused 952
Receiving objects: 100% (957/957), 5.24 MiB | 21.05 MiB/s, done.
Resolving deltas: 100% (541/541), done.
(base) computer@computer-ThinkCentre:~/Documents/AIML/CCL$ code ./getting-started/app/
(base) computer@computer-ThinkCentre:~/Documents/AIML/CCL$
```

Step 3 - Create file : Dockerfile and locate localhost, then enter :

`sudo docker build -t getting-started .`

Type required password of your system

The screenshot shows the Visual Studio Code interface. In the Explorer sidebar, there is a project structure with a folder named 'APP' containing 'spec', 'src', 'Dockerfile', 'package.json', and 'yarn.lock'. The 'Dockerfile' tab is selected, displaying the following content:

```
1 # syntax=docker/dockerfile:1
2
3 FROM node:18-alpine
4 WORKDIR /app
5 COPY .
6 RUN yarn install --production
7 CMD ["node", "src/index.js"]
8 EXPOSE 3000
```

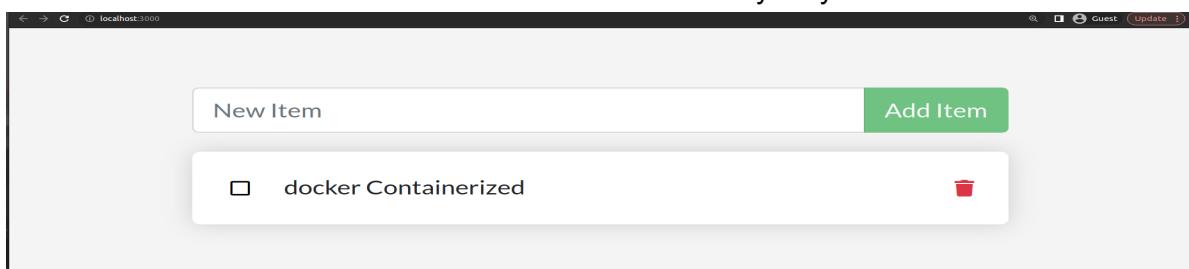
In the Terminal tab, the command `sudo docker build -t getting-started .` is being run. The terminal output shows:

```
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ touch Dockerfile
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ docker build -t getting-started .
ERROR: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/_ping": dial unix /var/run/docker.sock: connect: permission denied
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ sudo docker build -t getting-started .
[sudo] password for computer:
Sorry, try again.
[sudo] password for computer:
[+] Building 19.5s (11/11) FINISHED
=> [internal] load build definition from Dockerfile
=> => transferring dockerfile: 184B
0.0s
```

Step 4 - Getting-started : `sudo docker run -dp 3000:3000 getting-started`

```
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$ sudo docker run -dp 3000:3000
00 ge+-----+
33762
● computer@computer-ThinkCentre:~/Documents/AIML/CCL/getting-started/app$
```

You can see that containerized docker created successfully on your localhost

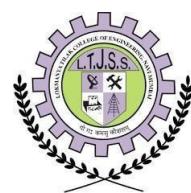




**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)**

**T.E/SEM VI/CBCGS/AIML
Academic Year: 2022-23**

NAME	SINGH SUDHAM DHARMENDRA
BRANCH	CSE-(AI&ML)
ROLL NO.	57
SUBJECT	CLOUD COMPUTING LAB
COURSE CODE	CSL605
PRACTICAL NO.	08
DOP	
DOS	



KUBERNETES

Aim : To study container orchestration using Kubernetes

Theory :

Kubernetes (also known as "K8s") is an open-source container orchestration tool that helps manage and automate the deployment, scaling, and management of containerized applications. Kubernetes was originally developed by Google, and is now maintained by the Cloud Native Computing Foundation (CNCF).

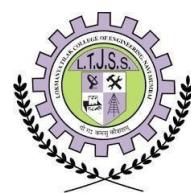
At a high level, Kubernetes works by managing a cluster of nodes (physical or virtual machines) that run containerized applications. A Kubernetes cluster consists of one or more master nodes, which control the cluster and make decisions about scheduling and scaling containers, and one or more worker nodes, which actually run the containers.

Benefits of Kubernetes

Kubernetes is a powerful container orchestration tool that offers a number of benefits to organizations deploying containerized applications:

- Scalability: Kubernetes enables automatic scaling of containers to meet the changing demands of an application. It can automatically add or remove containers based on metrics like CPU and memory utilization.
- High availability: Kubernetes provides a highly available infrastructure for containerized applications by automatically restarting containers that fail, and distributing containers across multiple nodes in a cluster.
- Portability: Kubernetes enables easy deployment of containerized applications across different environments, including on-premises data centers, public clouds, and hybrid environments.
- Resource efficiency: Kubernetes helps optimize the use of computing resources by packing containers efficiently onto nodes in the cluster, and dynamically allocating resources as needed.
- Simplified management: Kubernetes provides a declarative API for defining the desired state of an application, and automatically reconciles the actual state of the application with the desired state. This simplifies management and reduces the risk of configuration errors.
- Ecosystem support: Kubernetes has a large and growing ecosystem of tools and add-ons, such as Helm charts and Operators, which help automate the deployment and management of complex applications on Kubernetes.

Overall, Kubernetes provides a powerful platform for managing containerized applications, with features that help simplify management, improve scalability and availability, and optimize resource utilization.



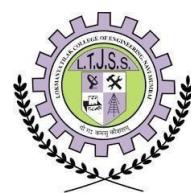
Kubernetes is a powerful tool for managing containerized applications, with a rich set of features that help automate the deployment, scaling, and management of applications at scale. While Kubernetes can be complex to set up and manage, it has become a de facto standard for container orchestration in the cloud-native ecosystem, and is widely used by organizations of all sizes.

Official website : <https://kubernetes.io/>

The screenshot shows a browser window with multiple tabs open, including "11_CCL_EXP8 - Google Docs", "11_CCL_EXP8-kubernetes", "What Is Kubernetes? | Go", "kubernetes documentation", "Learn Kubernetes with M", and "Kubernetes". The main content area is a red banner with the Kubernetes logo and the text: "Legacy k8s.gcr.io container image registry is being redirected to registry.k8s.io. k8s.gcr.io image registry is gradually being redirected to registry.k8s.io (since Monday March 20th). All images available in k8s.gcr.io are available at registry.k8s.io. Please read our announcement for more details." Below the banner, there is a section about Kubernetes, a diagram showing containers grouped into pods which are managed by a controller and run on a node, and sections for "Planet Scale" and "Never Outgrow" with their respective icons and descriptions.

For installation in ubuntu visit : <https://ubuntu.com/kubernetes/install#download>

The screenshot shows the Ubuntu website's "Download" section. It features four main categories: "Ubuntu Desktop", "Ubuntu Server", "Ubuntu for IoT", and "Ubuntu Cloud". Under "Ubuntu Server", there is a "Get Ubuntu Server" button and links for "Mac and Windows", "ARM", "IBM Power", and "s390x". Under "Ubuntu for IoT", there are links for "Raspberry Pi", "Intel IoT platforms", "Intel NUC", "KVM", "Qualcomm Dragonboard 410c", "Intel IEI TANK 870", "AMD-Xilinx Evaluation kits & SOMs", and "RISC-V platforms". The "Ubuntu Cloud" section links to "Amazon AWS, Microsoft Azure, Google Cloud Platform and more..." and "Download cloud images for local development and testing".



Here are some steps you can take to get started:

- Learn the basics of containers: Before diving into Kubernetes, it's important to understand the basics of containers. You can start by reading about Docker, which is one of the most popular containerization tools.
- Set up a Kubernetes cluster: You can set up a Kubernetes cluster locally using tools like Minikube or Kind, or you can use a cloud provider like Google Cloud, Amazon Web Services, or Microsoft Azure to create a Kubernetes cluster.
- Learn the Kubernetes architecture: Kubernetes has a complex architecture, so it's important to understand how all the components fit together. The Kubernetes documentation is a good place to start.
- Practice deploying applications: Once you have a Kubernetes cluster set up, you can practice deploying applications using Kubernetes. Start with a simple application and gradually work your way up to more complex deployments.
- Learn about Kubernetes networking: Kubernetes has its own networking model, so it's important to understand how it works. You can start by reading about Kubernetes Services and Ingress.
- Learn about Kubernetes storage: Kubernetes also has its own storage model, so it's important to understand how to manage storage for your applications. You can start by reading about Kubernetes Volumes.
- Explore Kubernetes ecosystem: Kubernetes has a large ecosystem of tools and add-ons that can help you manage and extend your cluster. Some popular tools include Helm, Prometheus, and Istio.

Overall, learning Kubernetes takes time and practice, but it can be a very rewarding skill to have in today's world of cloud-native applications.

Container orchestration using Kubernetes involves managing a cluster of nodes (physical or virtual machines) that run containerized applications using Kubernetes.

Kubernetes is a popular open-source container orchestration tool that has become a de facto standard for managing containerized applications in cloud computing environments. Kubernetes provides a powerful platform for automating the deployment, scaling, and management of containerized applications, and can be used with a wide range of cloud computing services and platforms.

In cloud computing environments, Kubernetes can be used to manage containerized applications deployed on a range of cloud platforms, including public clouds like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, as well as private clouds and hybrid clouds. Kubernetes can also be used to manage containers on on-premises data centers.



Applications

Kubernetes provides a number of key features that help automate the management of containerized applications:

- Container orchestration: Kubernetes can manage containers at scale, orchestrating the deployment, scaling, and management of containerized applications across multiple nodes in a cluster.
- Service discovery and load balancing: Kubernetes provides a built-in service discovery and load balancing mechanism, enabling containers to find and communicate with other containers in the same application.
- Automatic scaling: Kubernetes can automatically scale containers based on metrics like CPU and memory usage, enabling applications to handle traffic spikes and sudden increases in demand.
- Self-healing: Kubernetes can automatically restart containers that fail, and can detect and replace nodes that become unavailable.
- Rollouts and rollbacks: Kubernetes enables controlled rollouts and rollbacks of containerized applications, allowing organizations to test new versions of applications before deploying them to production.
- Configuration management: Kubernetes provides a declarative API for defining the desired state of an application, and can automatically reconcile the actual state of the application with the desired state. This helps simplify configuration management and reduces the risk of configuration errors.

Conclusion : We had successfully studied container orchestration using Kubernetes