

AMAZON WEB SERVICES (AWS) CRASH COURSE

Izar Lab — August 2020

Jana Biermann, PhD
jb4424@cumc.columbia.edu

Overview

1. AWS introduction
2. Launching an instance
3. SSH into your instance
4. Update instance and install AWS CLI
5. Creating, attaching and mounting a volume
6. Set an alarm for your instance
7. Shut down your instance
8. Elastic Block Store (EBS) vs Simple Storage Service (S3)
9. Additional points

What is AWS?



- AWS is a **secure cloud platform** that offers a **broad set of global cloud-based products**.
- AWS provides you with **on-demand access** to compute, storage, network, database, and other IT resources and management tools.
- AWS offers **flexibility**.
- You **pay only for the individual services you need**, for **as long as you use them**.
- AWS services **work together** like building blocks.

© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

5

AWS Global Infrastructure

- The **AWS Global Infrastructure** is designed and built to deliver a **flexible, reliable, scalable, and secure** cloud computing environment with high-quality **global network performance**.
- This map shows the current **AWS Regions** and more that are coming soon.

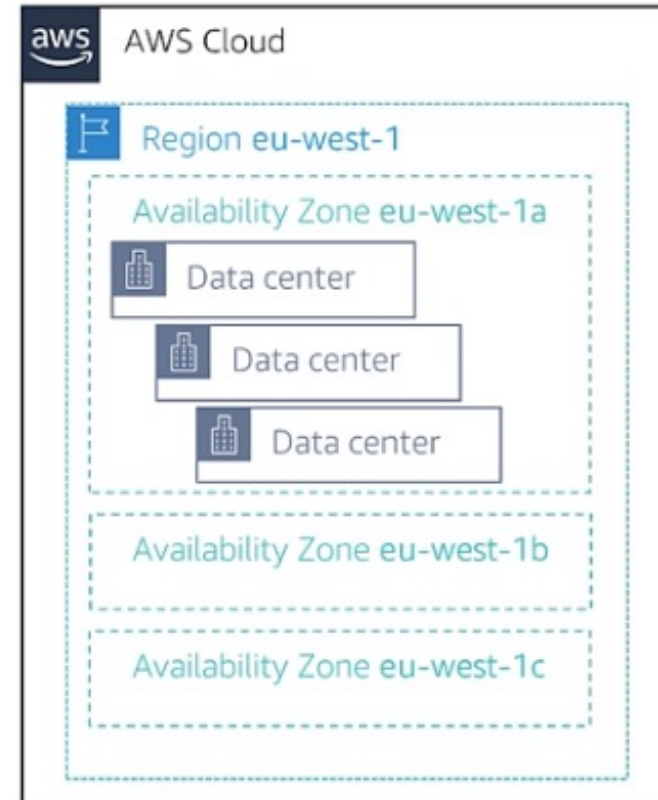


© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

10

Availability Zones

- Each **Region** has multiple Availability Zones.
- Each **Availability Zone** is a fully isolated partition of the AWS infrastructure.
 - There are currently 69 Availability Zones worldwide
 - Availability Zones consist of discrete **data centers**
 - They are designed for fault isolation
 - They are interconnected with other Availability Zones by using high-speed private networking
 - You choose your Availability Zones.
 - **AWS recommends replicating data and resources across Availability Zones for resiliency.**



- ❖ You need to stay within the region us-east-2 (Ohio)
- ❖ Availability Zones can be freely chosen

Sign in

<https://us-east-2.signin.aws.amazon.com>



Sign in as IAM user

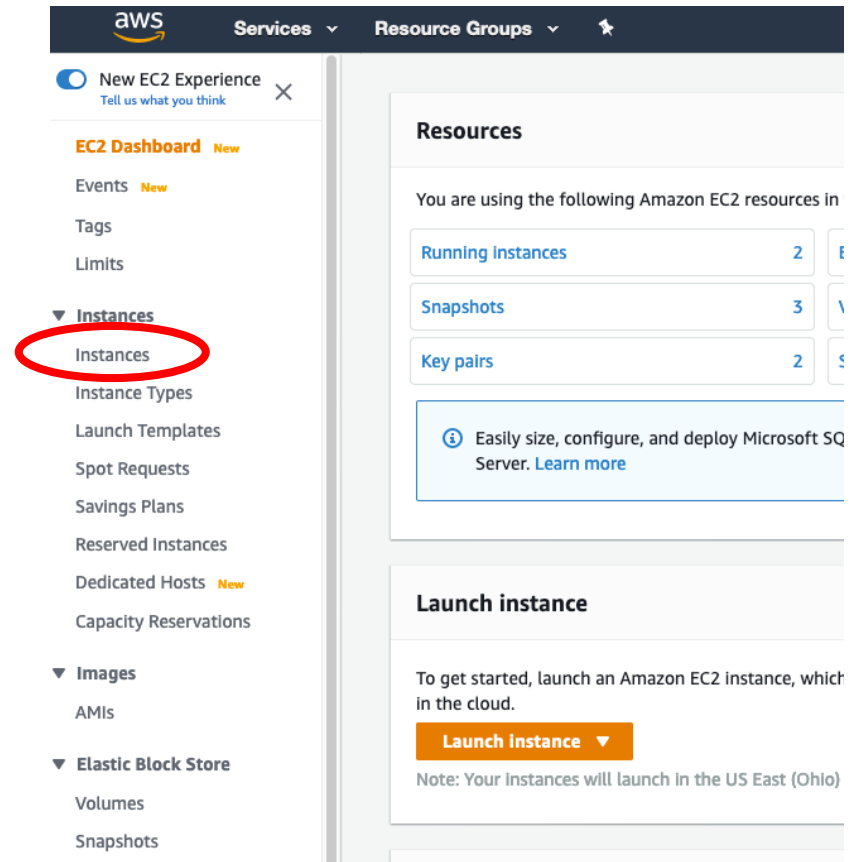
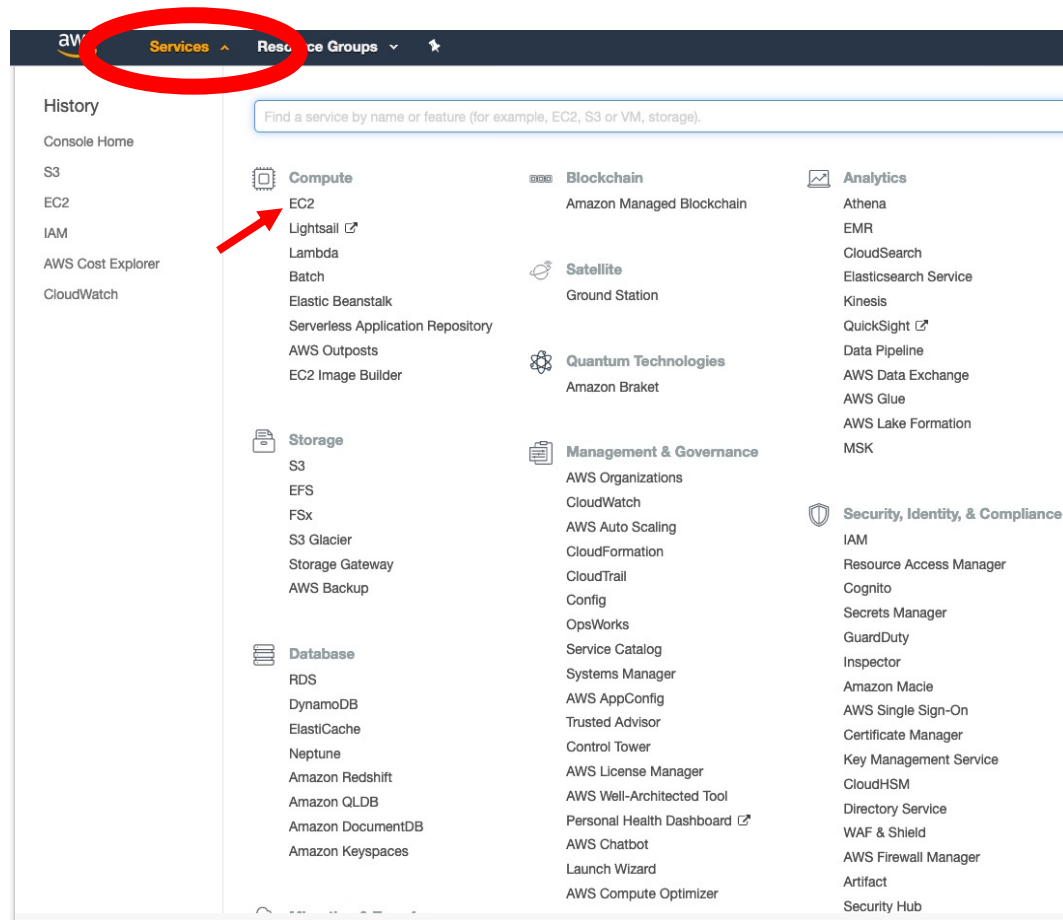
Account ID (12 digits) or account alias

IAM user name

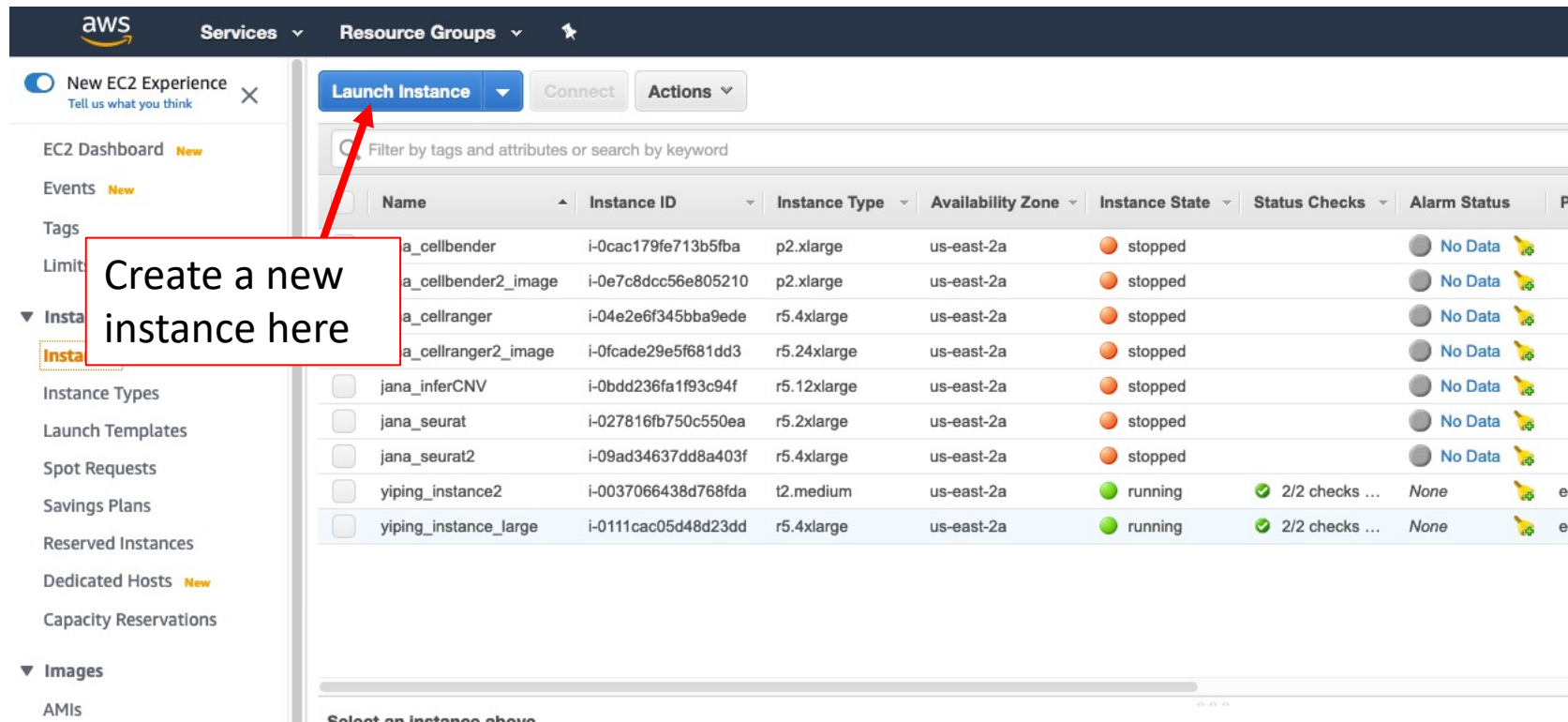
Password

☒ Remember this account

Navigate to instances



Launching an instance



aws Services Resource Groups

New EC2 Experience Tell us what you think

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	
a_cellbender	i-0cac179fe713b5fba	p2.xlarge	us-east-2a	stopped		No Data	
a_cellbender2_image	i-0e7c8dcc56e805210	p2.xlarge	us-east-2a	stopped		No Data	
a_cellranger	i-04e2e6f345bba9ede	r5.4xlarge	us-east-2a	stopped		No Data	
a_cellranger2_image	i-0fcade29e5f681dd3	r5.24xlarge	us-east-2a	stopped		No Data	
jana_inferCNV	i-0bdd236fa1f93c94f	r5.12xlarge	us-east-2a	stopped		No Data	
jana_seurat	i-027816fb750c550ea	r5.2xlarge	us-east-2a	stopped		No Data	
jana_seurat2	i-09ad34637dd8a403f	r5.4xlarge	us-east-2a	stopped		No Data	
yiping_instance2	i-0037066438d768fda	t2.medium	us-east-2a	running	2/2 checks ...	None	ec
yiping_instance_large	i-0111cac05d48d23dd	r5.4xlarge	us-east-2a	running	2/2 checks ...	None	ec

Create a new instance here

- ❖ Name your instances and volumes starting with your name
- ❖ E.g. 'yiping_instance_large'

Launching an instance — Step 1

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Q Search for an AMI by entering a search term e.g. "Windows"

Search by Systems Manager parameter


Quick Start

My AMIs

AWS Marketplace

Community AMIs

☐ Free tier only ⓘ




Amazon Linux

Free tier eligible

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-07c8bc5c1ce9598c3 (64-bit x86) / ami-09a67037138f86e67 (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes




Amazon Linux

Free tier eligible

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-02b0c55eeae6d5096

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

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes




Red Hat

Free tier eligible

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a54aef4ef3b5f881 (64-bit x86) / ami-0ffd59b53e6797671 (64-bit Arm)

Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes




SUSE Linux

Free tier eligible

SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-03f4c416f489586a3 (64-bit x86) / ami-0d24f1c1ba96d2803 (64-bit Arm)

SUSE Linux Enterprise Server 15 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Ubuntu

Free tier eligible

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0bbe28eb2173f6167 (64-bit x86) / ami-04adf33460efc8798 (64-bit Arm)

Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

Select

☐ 64-bit (x86)

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

1 to 40 of 40 AMIs

You will probably want Ubuntu

Launching an instance — Step 2

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. To choose the appropriate mix of resources for your applications, [learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only

What's your use case?

aws training and certification

Instance type details

General Purpose Compute Optimized Memory Optimized Accelerated Computing Storage Optimized

Instance Types	a1, m4, m5, t2, t3	c4, c5	r4, r5, x1, z1	f1, g3, g4, p2, p3	d2, h1, i3
Use Case	Broad	High performance	In-memory databases	Machine learning	Distributed file systems

- ❖ Choose an instance based on use case
- ❖ Check the instance prices at <https://aws.amazon.com/ec2/pricing/on-demand/>
- ❖ Inform yourself about the properties of different instances in the 'Instance Types' menu
- ❖ Keep the economics in mind

© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws Services Resource Groups

New EC2 Experience Tell us what you think

EC2 Dashboard New

Events New

Tags

Limits

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts New

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Resources

You are using the following Amazon EC2 resources in:

Running Instances 2

Snapshots 3

Key pairs 2

Easily size, configure, and deploy Microsoft SQL Server. [Learn more](#)

Launch instance

To get started, launch an Amazon EC2 instance, which in the cloud.

Launch Instance

Note: Your instances will launch in the US East (Ohio)

Launching an instance — Step 3

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

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

Number of Instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<div>vpc-5ead7935 (default) </div>	Create new VPC
Subnet	<div>No preference (default subnet in any Availability Zone)</div>	Create new subnet
Auto-assign Public IP	<div>Use subnet setting (Enable)</div>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<div>Open</div>	
IAM role	<div>None </div>	Create new IAM role
Shutdown behavior	<div>Stop</div>	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	<div>Shared - Run a shared hardware instance</div> Additional charges will apply for dedicated tenancy.	
Elastic Inference	<input type="checkbox"/> Add an Elastic Inference accelerator Additional charges apply.	
T2/T3 Unlimited	<input type="checkbox"/> Enable Additional charges may apply	

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Launching an instance — Step 4

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

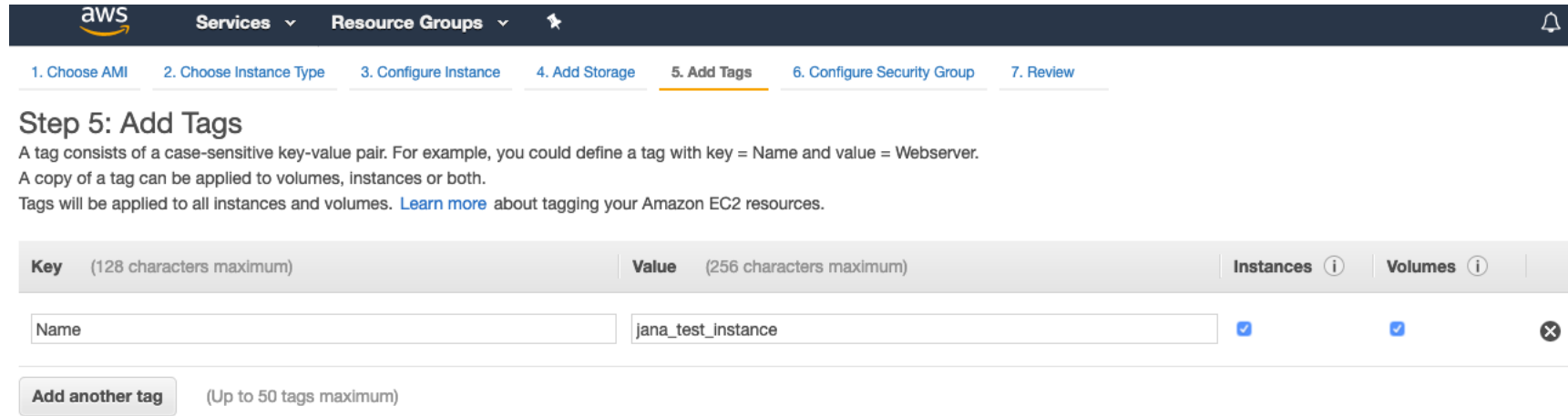
Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/sda1	snap-0cd98f931a8fffac8	8	General Purpose SSD (gp2) ⌵	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted ▼

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

- ❖ Choose the size of the root volume
- ❖ The size can also be changed later in the 'Volumes' menu (only to increase it and it takes some time)
- ❖ You can add additional volumes to your instance (need to be attached and then mounted)
- ❖ This type of storage is expensive
- ❖ For long-term storage use S3 and download the data to your instance whenever needed

Launching an instance — Step 5



Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
Name	jana_test_instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

- ❖ Name your instances and volumes starting with your name
- ❖ E.g. 'yiping_instance_large'

Launching an instance — Step 6

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a **new** security group
☒ Select an **existing** security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-e9c01990	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-01bb301cd3293a98b	launch-wizard-1	launch-wizard-1 created 2020-04-03T19:24:25.538-04:00	Copy to new
<input type="checkbox"/> sg-09f744ffee14e8cb7	launch-wizard-2	launch-wizard-2 created 2020-07-13T19:42:26.434-04:00	Copy to new
<input type="checkbox"/> sg-0a5fce4b0bbfa5621	launch-wizard-3	launch-wizard-3 created 2020-08-05T14:19:09.148-04:00	Copy to new

- ❖ Create a new security group if you don't have one
- ❖ Allow traffic only from your IP address
- ❖ Don't create a new security group every time you launch a new instance
- ❖ Don't allow all traffic

Launching an instance — Step 7

aws

Services

Resource Groups

★

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

6. Configure Security Group

7. Review

Step 7: Review Instance Launch

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

⚠️ Improve your instances' security. Your security group, launch-wizard-1, is open to the world.

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

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

▼ AMI Details

🔗

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0bbe28eb2173f6167

Free tier eligible

Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root Device Type: ebs Virtualization type: hvm

▼ Instance Type

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

▼ Security Groups

Security Group ID	Name	Description
sg-01bb301cd3293a98b	launch-wizard-1	launch-wizard-1 created 2020-04-03T19:24:25.538-04:00

All selected security groups inbound rules

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	

► Instance Details

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

jana_key

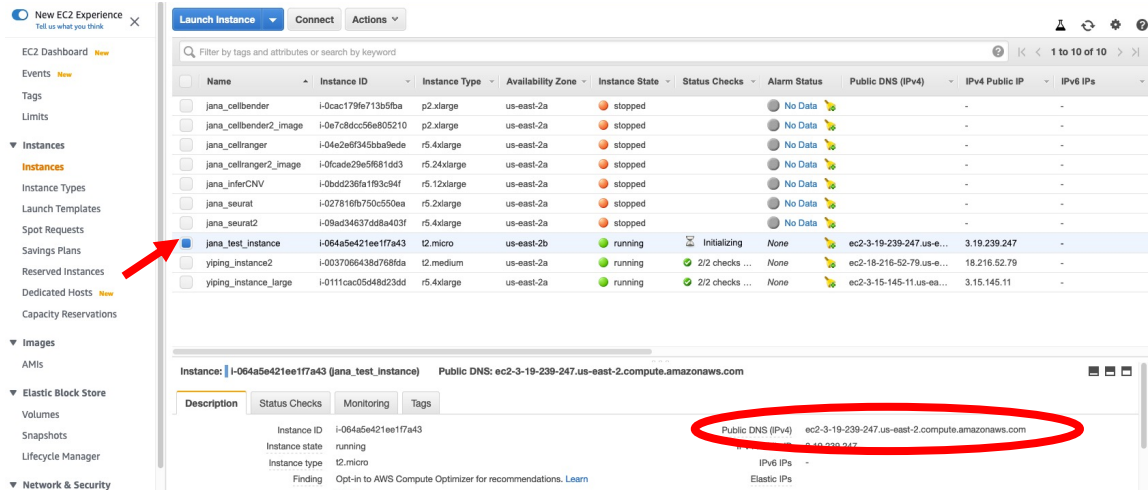
☒ I acknowledge that I have access to the selected private key file (jana_key.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

❖ Review your settings and launch your instance using your AWS key

SSH into your instance



```
jana@MDHO-N012:~$ sshfs -o IdentityFile=[REDACTED].pem ubuntu@ec2-3-19-239-247.us-east-2.compute.amazonaws.com:/home/ubuntu/ ~/AWS
The authenticity of host 'ec2-3-19-239-247.us-east-2.compute.amazonaws.com (3.19.239.247)' can't be established.
ECDSA key fingerprint is [REDACTED].
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
jane@MDHO-N012:~$ ssh -Y -i [REDACTED].pem ubuntu@ec2-3-19-239-247.us-east-2.compute.amazonaws.com
Warning: No xauth data; using fake authentication data for X11 forwarding.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.3.0-1032-aws x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:      https://ubuntu.com/advantage
```

System information as of Wed Aug 12 17:50:57 UTC 2020

```
System load:  0.0      Processes:      93
Usage of /:   14.6% of 7.69GB   Users logged in:  0
Memory usage: 18%      IP address for eth0: 172.31.31.85
Swap usage:   0%
```

```
0 packages can be updated.
0 updates are security updates.
```

```
/usr/bin/xauth: file /home/ubuntu/.Xauthority does not exist
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
ubuntu@ip-172-31-31-85:~$
```

- ❖ Select your instance and copy the IP address
- ❖ You can mount the instance volume to your MacBook using FUSE for macOS (<https://github.com/osxfuse/osxfuse>)
- ❖ SSH into your instance by specifying the directory of your AWS key and the IP address of the instance
- ❖ `ssh -Y -i xxx.pem ubuntu@ec2-3-19-239-247.us-east-2.compute.amazonaws.com`

Update instance and install AWS CLI

- Update instance with:

```
sudo apt-get update; sudo apt-get upgrade -y
```

- Connect to your AWS account:

```
# install aws command line
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
sudo apt install unzip
unzip awscliv2.zip
sudo ./aws/install

# set up aws s3 access
mkdir ~/.aws
echo "[default]" >> .aws/credentials
echo "aws_access_key_id = your_key_id" >>
.aws/credentials
```

```
echo "aws_secret_access_key = your_access_key" >>
.aws/credentials
```

```
# list all buckets (test if AWSCLI works)
aws s3 ls
```

```
# transfer between instance and S3
aws s3 sync data/ s3://bucket/data/ --exclude "*" --
include "only_files_with_these_terms" --quiet
```

```
# directories have to end with /
# use --dryrun first to be safe
```

Create a volume

The screenshot shows the AWS Management Console interface. In the left-hand navigation pane, the 'Elastic Block Store' section is expanded, and the 'Volumes' link is circled in red. A red arrow points from this 'Volumes' link to the 'Create Volume' button in the top navigation bar. The main content area displays a table of existing volumes with columns for 'Name' and 'Volume ID'. The table lists several volumes, including 'jana_cellbender2_image_root', 'jana_cellbender_root', 'jana_cellranger2_image_root', 'jana_cellranger_root', 'jana_cr_tmp', 'jana_inferCNV_root', 'jana_seurat2_root', 'jana_seurat_root', 'yiping_large_data', and 'yiping_large_root'. Below the table, there is a 'Select a volume above' prompt.

Volumes > Create Volume

Create Volume

Volume Type: General Purpose SSD (gp2) ⓘ

Size (GiB): 1 (Min: 1 GiB, Max: 16384 GiB) ⓘ

IOPS: 100 / 3000 (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS) ⓘ

Availability Zone*: us-east-2a ⓘ

Throughput (MB/s): Not applicable ⓘ

Snapshot ID: Select a snapshot ⓘ

Encryption: ☐ Encrypt this volume

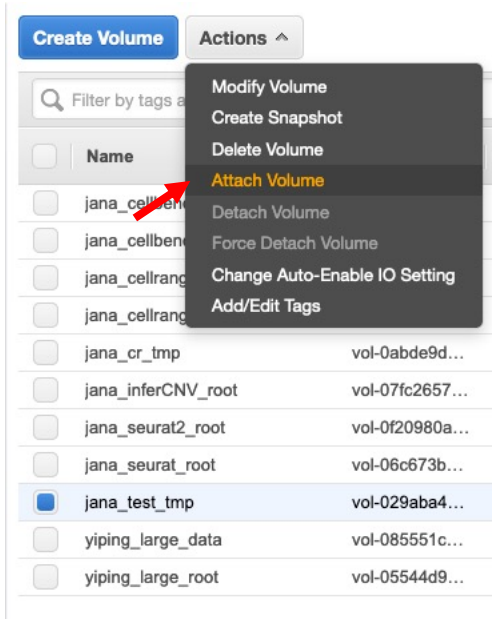
Key (128 characters maximum) Value (256 characters maximum)

Name jana_test_tmp ⓘ

Add Tag 49 remaining (Up to 50 tags maximum)

- ❖ Name your instances and volumes starting with your name
- ❖ E.g. 'yiping_instance_root'

Attach and mount the volume to your instance



Find the name of the volume

lsblk

mkdir data

check if volume has any data (shouldn't be the case when newly created)

sudo file -s /dev/xvdf

Format the volume to ext4 filesystem

sudo mkfs -t ext4 /dev/xvdf

Mount volume

sudo mount /dev/xvdf1 data

Change owner

sudo chown ubuntu:ubuntu vol

Set an alarm for your instance

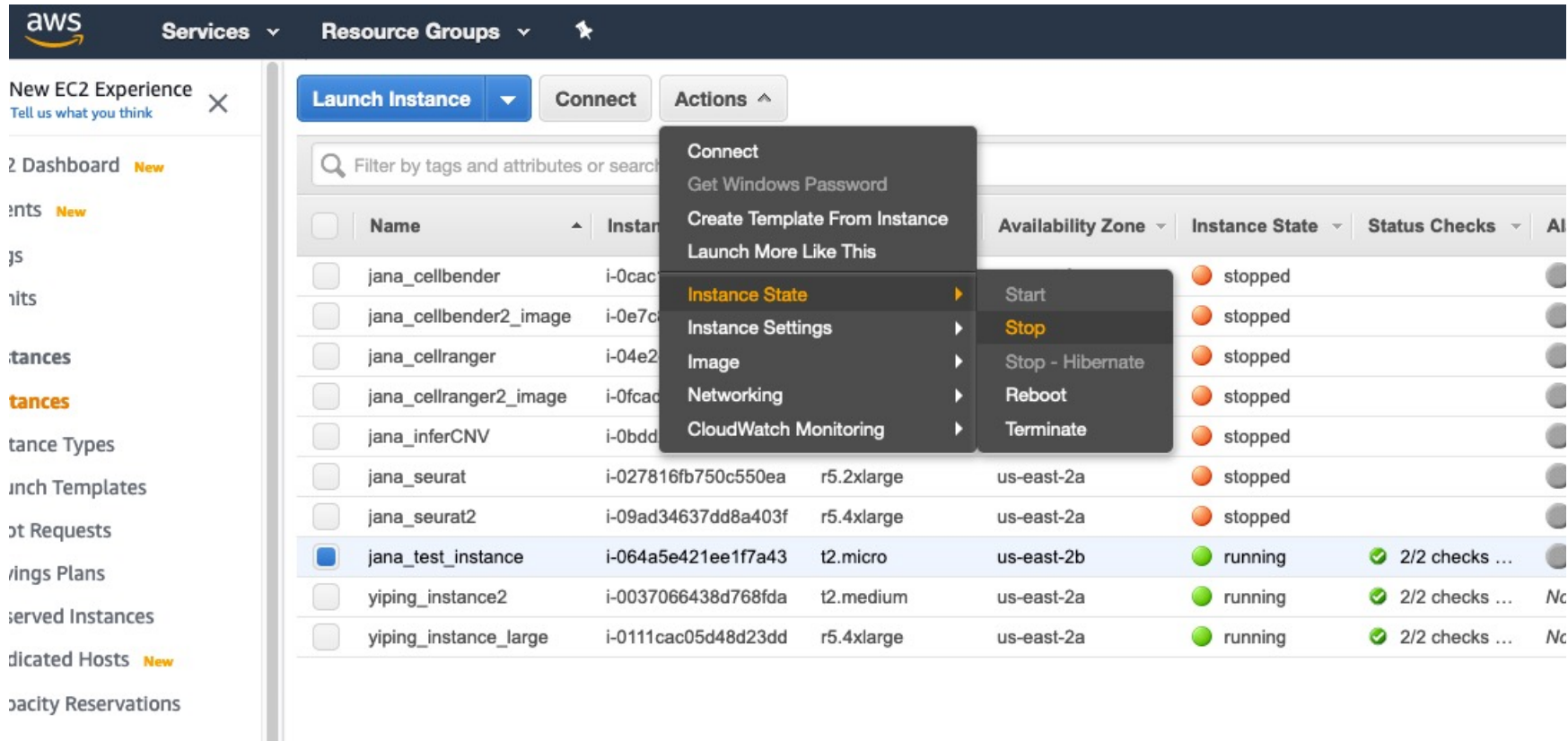
The screenshot shows the AWS Management Console with a list of EC2 instances. The 'jana_test_instance' is selected. The 'Create Alarm' dialog box is open, showing the following configuration:

- Send a notification to:** ☒ Instance_done (j.b4424@cumc.columbia) [create topic](#)
- Take the action:** ☒ Stop this instance [i](#)
☐ Recover this instance [i](#)
☐ Terminate this instance [i](#)
☐ Reboot this instance [i](#)
- Whenever:** Average of CPU Utilization
- Is:** > 0.5 Percent
- For at least:** 2 consecutive period(s) of 15 Minutes
- Name of alarm:** test_alarm

The background shows a table of instances with columns: Name, Instance ID, Instance Type, Availability Zone, Instance State, Status Checks, Alarm Status, Public DNS (IPv4), IPv4 Public IP, and IPv6 IPs. The 'jana_test_instance' is highlighted in blue.

- ❖ Always set alarms for your instances to shut down automatically when they are not used anymore
- ❖ Forgetting to shut down an instance can become expensive
- ❖ Select your instance
- ❖ Select the 'Monitoring' menu
- ❖ Click 'Create Alarm' on the top right
- ❖ You can also create alarms for your volumes

Shut down your instance



The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with links like 'Dashboard', 'Instances', 'Images', etc. The main area displays a table of EC2 instances. The instance 'jana_test_instance' is selected. An 'Actions' dropdown menu is open, showing options like 'Connect', 'Get Windows Password', 'Create Template From Instance', and 'Instance State'. The 'Instance State' sub-menu is further open, showing 'Start', 'Stop' (highlighted), 'Stop - Hibernate', 'Reboot', and 'Terminate'.

Name	Instance ID	Availability Zone	Instance State	Status Checks
jana_cellbender	i-0cac...		stopped	
jana_cellbender2_image	i-0e7c...		stopped	
jana_cellranger	i-04e2...		stopped	
jana_cellranger2_image	i-0fcac...		stopped	
jana_inferCNV	i-0bdd...		stopped	
jana_seurat	i-027816fb750c550ea	us-east-2a	stopped	
jana_seurat2	i-09ad34637dd8a403f	us-east-2a	stopped	
jana_test_instance	i-064a5e421ee1f7a43	us-east-2b	running	2/2 checks ...
yiping_instance2	i-0037066438d768fda	us-east-2a	running	2/2 checks ...
yiping_instance_large	i-0111cac05d48d23dd	us-east-2a	running	2/2 checks ...

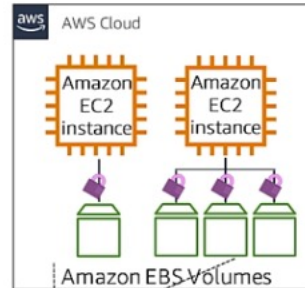
- ❖ Make sure only your instance is selected
- ❖ 'Stop' will shut down the instance until you start it again
- ❖ 'Terminate' will delete the instance (and the associated root volume unless you changed the settings)
- ❖ When instances are stopped, we only pay for the storage of their volume

Elastic Block Store (EBS) vs Simple Storage Service (S3)

Amazon EBS



- Persistent block storage for instances
- Protected through replication
- Different drive types
- Scale up or down in minutes
- Pay for only what you provision
- Snapshot functionality
- Encryption available

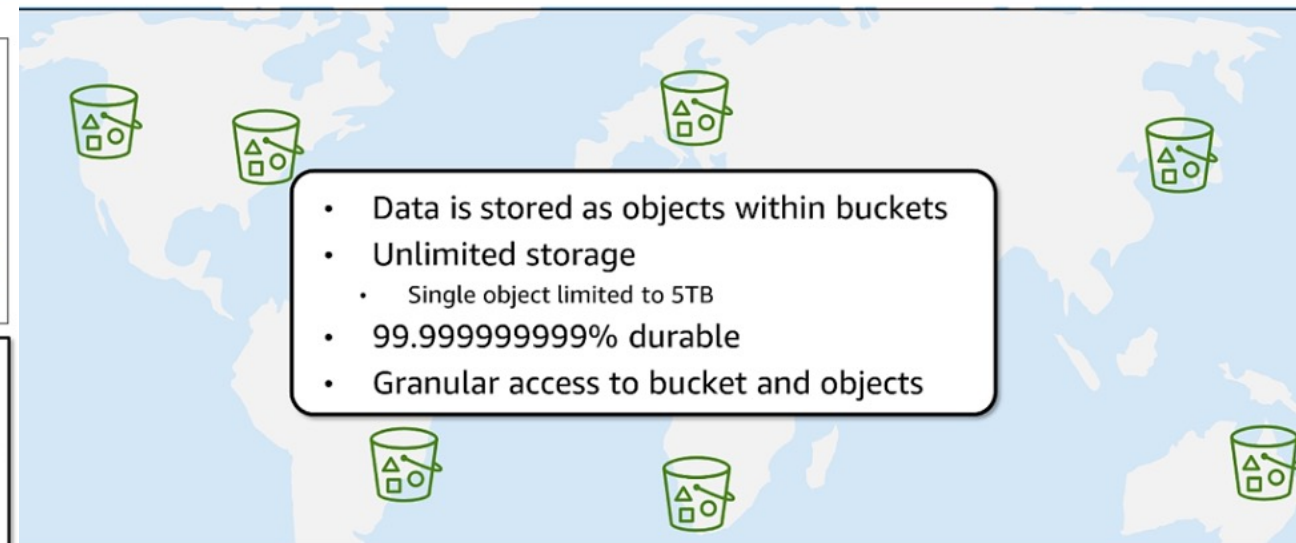


- Solid State Drives (SSD)
- Provisioned IOPS SSD
 - General Purpose SSD
- Hard Disk Drives (HDD)
- Throughput Optimized
 - Cold HDD (sc1) Volume
- Amazon EBS Volumes
- Monday's snapshot
 - Tuesday's snapshot
 - Wednesday's snapshot
 - Thursday's snapshot
 - Friday's snapshot

© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

27

What is Amazon S3?



- Data is stored as objects within buckets
- Unlimited storage
 - Single object limited to 5TB
- 99.999999999% durable
- Granular access to bucket and objects

© 2020 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

26

- ❖ EBS is for short-term storage while you are working with the data
- ❖ S3 is for long-term storage to download to EBS whenever you need to work with the data

Additional points

- You can find your password and key in the credentials file
- Keep the credentials file save in a hidden folder
- S3 is in most cases the only copy of our data so make sure not to delete or alter anything
- Most people in the lab have access to S3 so you can direct them to your analysis output
- Downloading data from AWS is very expensive so please don't download large files but instead analyze them on AWS instances until you reach a smaller format that can be downloaded
- The volume storage associated with instances is also very expensive so try to keep it small and store data on S3
- Please only use your own instances, volumes and images generated with your own key
- If you don't need an instance anymore you can terminate it
- You can check the budget in the 'Cost Explorer' menu and filter for costs generated with your key. This will only include instance-related costs and not the costs generated through S3 and volumes.