

# AWS

Amazon Web Services



The Cloud

# Login to AWS

— — —

`http://aws.amazon.com`

S3

# S3

— — —

- <https://s3.console.aws.amazon.com>

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web.



**Storage**

S3

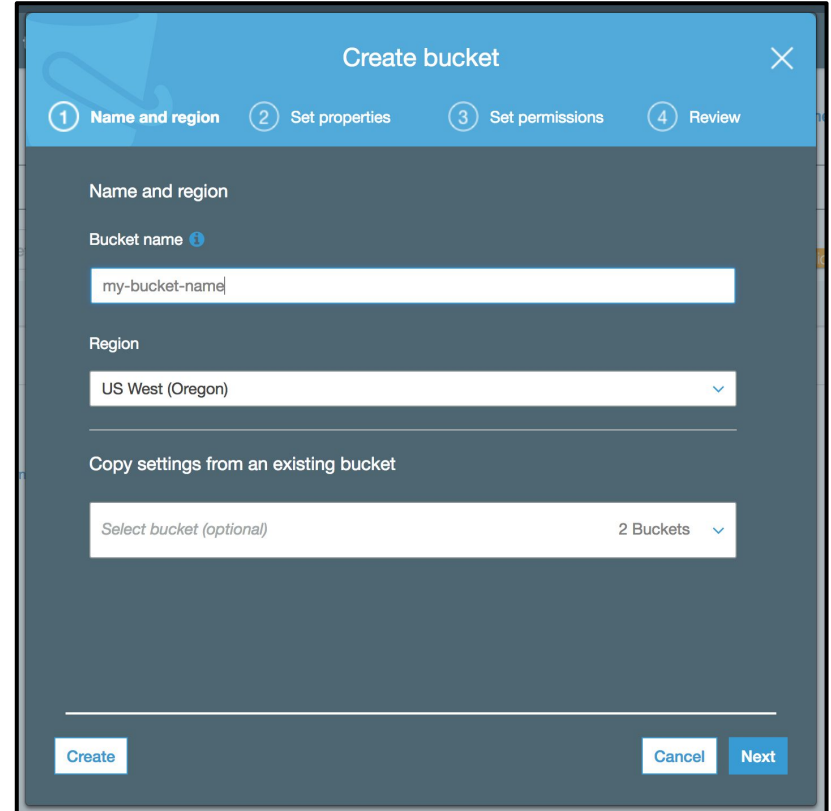
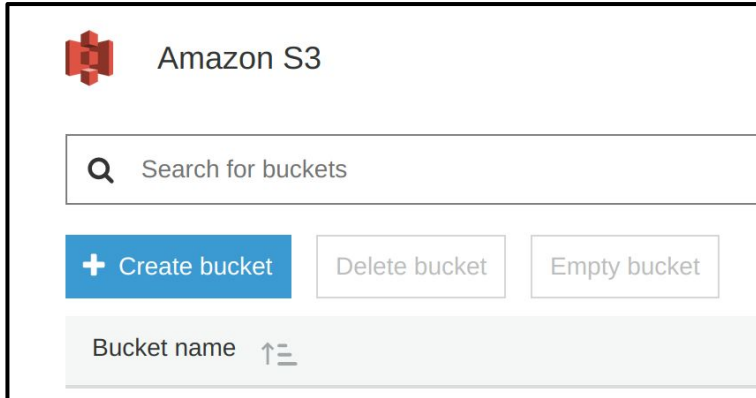
EFS

Glacier

Storage Gateway

# Create a bucket

1. Login to AWS
2. Go to S3
3. Click "Create bucket"
4. Enter a "Bucket name"
5. Click "Create"



# To make your bucket publicly available (optional)

Overview

Properties

Permissions

Management

Access Control List

Bucket Policy

CORS configuration

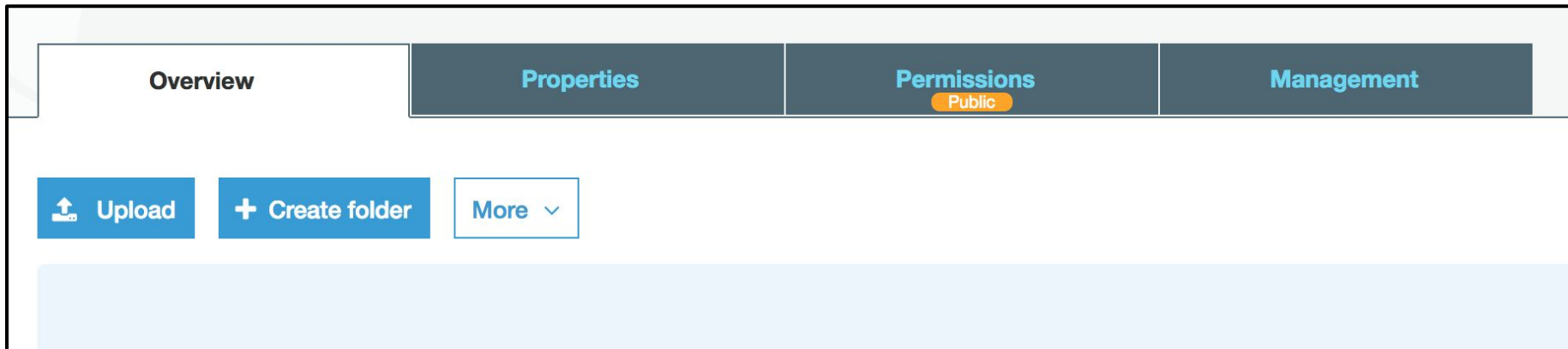
## Bucket policy editor

ARN: arn:aws:s3:::my-bucket-name1

Type to add a new policy or edit an existing policy in the text area below.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::my-bucket-name1/*"
10    }
11  ]
12 }
```

# Manually create folders and upload files





# Create Credentials - 1 (IAM page)

The screenshot shows the AWS IAM console interface. A green arrow points from the 'Users' link in the left-hand navigation menu to the main content area. Another green arrow points from the 'Welcome to Identity and Access Management' header to a dropdown menu on the right. This menu contains the following options: 'My Account', 'My Organization', 'My Billing Dashboard', 'My Security Credentials' (which is highlighted with a horizontal line), and 'Sign Out'.

**Search IAM**

**Dashboard**

- Groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

## Welcome to Identity and Access Management

IAM users sign-in link:  
<https://709440151559.signin.aws.amazon.com/console>

### IAM Resources

Users: 1	Roles: 0
Groups: 1	Identity Providers: 0
Customer Managed Policies: 0	

### Security Status

- My Account
- My Organization
- My Billing Dashboard
- My Security Credentials**
- Sign Out

# Create Credentials - 2 (add user)

Add userDelete user

Find users by username or access k

User name ▼

chyld

# Create Credentials - 3 (add user with api access)

## Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[+](#) Add another user

## Select AWS access type

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

Access type\*



**Programmatic access**

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.



**AWS Management Console access**

Enables a **password** that allows users to sign-in to the AWS Management Console.

\* Required

[Cancel](#)

[Next: Permissions](#)

# Create Credentials - 4 (create an admin group)

## Create group



Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name






Create policy

Refresh

Filter: Policy type

Search

Showing 325 results


	Policy name	Type	Attachments	Description
<input checked="" type="checkbox"/>	 AdministratorAccess	Job function	1	Provides full access to AWS services and resources.
<input type="checkbox"/>	 AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	 AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to related AWS Servi...
<input type="checkbox"/>	 AlexaForBusinessGatewayExecution	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	 AlexaForBusinessReadOnlyAccess	AWS managed	0	Provide read only access to AlexaForBusiness services

Cancel

Create group

# Create Credentials - 5 (view public and secret user key)

 Download .csv

		User	Access key ID	Secret access key
▶		user3	AKIAJB5CD53XIP4VE7CQ	***** <a href="#">Show</a>

# Create Credentials - 6 (add keys to file)

— — —

1. Create ~/.aws directory
2. Create config file
3. Create credentials file

```
#-----:~/.aws // 2 // chyld@Chylds-MacBook-Pro
[47]: l
total 16
drwxr-xr-x  4 chyld  staff   128B Mar 26 10:52 .
drwxr-xr-x+ 35 chyld  staff   1.1K Mar 26 11:20 ..
-rw-r--r--  1 chyld  staff    28B Mar 26 10:51 config
-rw-r--r--  1 chyld  staff   117B Mar 26 10:50 credentials
```

# Create Credentials - 7 (config file)

---

```
#-----:::  
~/aws // 2 // chylid@Chylids-MacBook-Pro  
[49]: cat config  
[default]  
region=us-west-1
```

# Create Credentials - 8 (credentials file)

---

```
#-----:::  
~/aws // 2 // chylid@Chylids-MacBook-Pro  
[51]: cat credentials  
[default]  
aws_access_key_id = AKIAIG5Y20RJQI4UFBLA  
aws_secret_access_key = lqeT2vnpQbYu4VkAsUJ1CDUhn2WI8L
```



# Access your bucket from Python

— — —

- `$ conda install boto3`
- <https://boto3.readthedocs.io/en/latest/>
- <https://boto3.readthedocs.io/en/latest/guide/quickstart.html>

# Reading and Writing to S3 from Python

— — —

```
import boto3
```

```
s3 = boto3.resource('s3')
```

```
# get all buckets
for bucket in s3.buckets.all():
    print(bucket.name)
```

```
chyl-d-hdd-01
chyl-d-temp1
my-bucket-name1
```

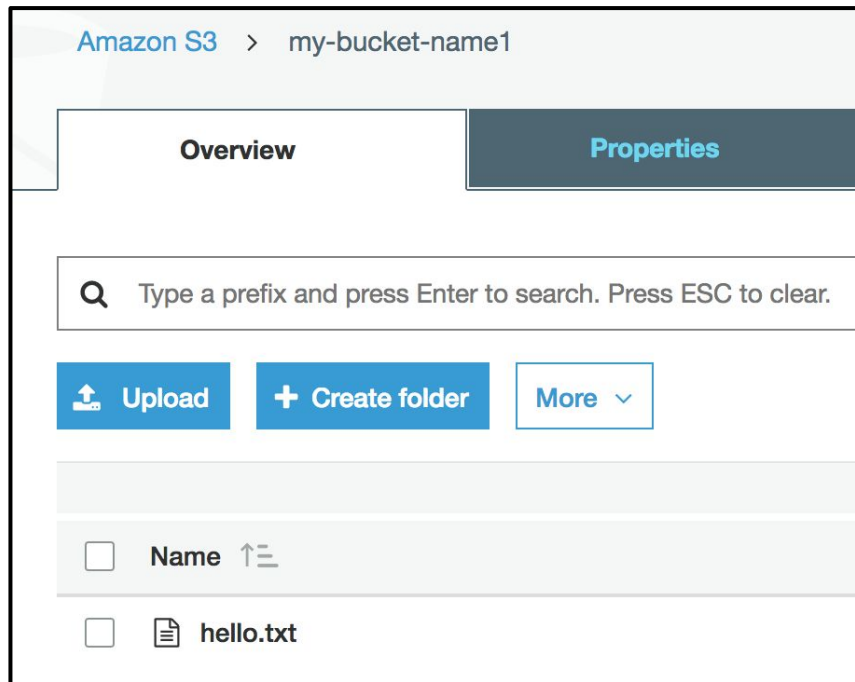
```
# upload file
data = open('hello.txt', 'rb')
s3.Bucket('my-bucket-name1').put_object(Key='hello.txt', Body=data)
```

```
s3.Object(bucket_name='my-bucket-name1', key='hello.txt')
```

```
# download file
s3.Bucket('my-bucket-name1').download_file('hello.txt', 'new-hello.txt')
```

# View uploaded files

— — —



EC2

# EC2

— — —

- <https://console.aws.amazon.com/ec2>

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.



## Compute

EC2

Lightsail ↗

Elastic Container Service

Lambda

Batch

Elastic Beanstalk

# Create IAM Role - Part 1

— — —

Search IAM

Dashboard

Groups

Users

**Roles**

Policies

Identity providers

Account settings

Credential report

Create roleDelete role


Q Search

Role name ▼	Description
-------------	-------------

# Create IAM Role - Part 2

## Select type of trusted entity

**AWS service**  
EC2, Lambda and others

**Another AWS account**  
Belonging to you or 3rd party

**Web identity**  
Cognito or any OpenID provider

**SAML 2.0 federation**  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

## Choose the service that will use this role

### EC2

Allows EC2 instances to call AWS services on your behalf.

### Lambda

Allows Lambda functions to call AWS services on your behalf.

API Gateway	Config	ElastiCache	Kinesis	SMS
AppSync	DMS	Elastic Beanstalk	Lambda	SNS
Application Auto Scaling	Data Pipeline	Elastic Container Service	Lex	SWF
Auto Scaling	DeepLens	Elastic Transcoder	Machine Learning	SageMaker
Batch	Directory Service	ElasticLoadBalancing	MediaConvert	Service Catalog
CloudFormation	DynamoDB	Glue	OpsWorks	Step Functions
CloudHSM	EC2	Greengrass	RDS	Storage Gateway
CloudWatch Events	EC2 - Fleet	GuardDuty	Redshift	
CodeBuild	EKS	Inspector	Rekognition	

\* Required

Cancel

Next: Permissions

# Create IAM Role - Part 3

## Attach permissions policies

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





Create policy

Refresh

Filter: Policy type ▾

Q s3

Showing 4 results

		Policy name ▾	Attachments ▾	Description
<input type="checkbox"/>	▶	 AmazonDMSRedshiftS3Role	0	Provides access to manage S3 settings for Redshift endpoin...
<input checked="" type="checkbox"/>	▶	 AmazonS3FullAccess	0	Provides full access to all buckets via the AWS Management...
<input type="checkbox"/>	▶	 AmazonS3ReadOnlyAccess	0	Provides read only access to all buckets via the AWS Manag...
<input type="checkbox"/>	▶	 QuickSightAccessForS3StorageManagement...	0	Policy used by QuickSight team to access customer data pr...



# Create IAM Role - Part 4

## Review

---

Provide the required information below and review this role before you create it.

**Role name\***

access-s3-from-ec2

Use alphanumeric and '+,=,.-\_' characters. Maximum 64 characters.

**Role description**

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+,=,.-\_' characters.

**Trusted entities**

AWS service: ec2.amazonaws.com

**Policies**



AmazonS3FullAccess 

# Create IAM Role - Part 5

Search IAM

Dashboard

Groups

Users

**Roles**

Policies

Identity providers

Account settings

Credential report

Encryption keys



The role **access-s3-from-ec2** has been created.

Create role

Delete role



Search

Role name ▼

Description



**access-s3-from-ec2**

Allows EC2 instances to call AWS services on your behalf.

# Create an EC2 machine

## EC2 Dashboard

Events

Tags

Reports

Limits

### INSTANCES

Instances

Launch Templates

Spot Requests

Reserved Instances

Dedicated Hosts

Scheduled Instances

### IMAGES

AMIs

Bundle Tasks

### ELASTIC BLOCK STORE

Volumes

Snapshots

## Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances

0 Dedicated Hosts

0 Volumes

2 Key Pairs

0 Placement Groups

0 Elastic IPs

0 Snapshots

0 Load Balancers

6 Security Groups

## Create Instance

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

**Launch Instance**

Note: Your instances will launch in the US West (Oregon) region

## Service Health

### Service Status:



US West (Oregon):

This service is operating normally



## Scheduled Events

### US West (Oregon):

No events

# Check your region

— — —

- Use N. California as the region to start your EC2 instance.
- Create an Instance.



Chyld Medford ▾

N. California ▾

Support ▾

## Create Instance

---

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

Launch Instance



# Choose a Machine Image

— — —

## Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)



**Ubuntu Server 16.04 LTS (HVM), SSD Volume Type** - ami-07585467

Free tier eligible

Ubuntu Server 16.04 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

Select

64-bit

# Choose Memory, # CPUs

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes

[Cancel](#)[Previous](#)[Review and Launch](#)[Next: Configure Instance Details](#)

# Networking and IAM Role selection

## 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 lower prices, or request On-Demand instances to pay for the instance by the hour. For more information, see [Amazon EC2 Instance Types](#).

Number of instances	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="text" value="vpc-d9dbc3bf"/> <a href="#">Create new VPC</a>	
Subnet	<input type="text" value="subnet-04e5c262   Public subnet   us-west-2a"/> <a href="#">Create new subnet</a> 251 IP Addresses available	
Auto-assign Public IP	<input type="text" value="Enable"/>	
Placement group	<input type="checkbox"/> Add instance to placement group.	
IAM role	<input type="text" value="access-s3-from-ec2"/> <a href="#">Create new IAM role</a>	
Shutdown behavior	<input type="text" value="Stop"/>	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	
Tenancy	<input type="text" value="Shared - Run a shared hardware instance"/> <a href="#">Additional charges will apply for dedicated tenancy.</a>	

# Set HDD size

## 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 ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-0fc155f7d651fba81	<input type="text" value="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.

Cancel

Previous

Review and Launch

Next: Add Tags



# Create Security Group

## 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 name:

Description:

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>	Description <small>i</small>
SSH <small>⌵</small>	TCP	22	Custom <small>⌵</small> 0.0.0.0/0	e.g. SSH for Admin Desktop <small>✕</small>
Custom TCP <small>⌵</small>	TCP	8888	Custom <small>⌵</small> 0.0.0.0/0	e.g. SSH for Admin Desktop <small>✕</small>

Add Rule



### Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel

Previous

Review and Launch

# Launch Instance

## Step 7: Review Instance Launch

### ▼ AMI Details

[Edit AMI](#)**Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-07585467****Free tier  
eligible**Ubuntu Server 16.04 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

[Edit instance type](#)

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

### ▼ Security Groups

[Edit security groups](#)**Security group name**

launch-wizard-1

**Description**

launch-wizard-1 created 2018-03-26T12:14:06.599-07:00

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	0.0.0.0/0	
Custom TCP Rule	TCP	8888	0.0.0.0/0	

### ► Instance Details

[Edit instance details](#)[Cancel](#)[Previous](#)[Launch](#)

# Download keys and launch instance

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](#).

Create a new key pair



Key pair name

my-keys

Download Key Pair



You have to download the **private key file** (\*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

# View your instance; Get IP address

- EC2 Dashboard
- Events
- Tags
- Reports
- Limits
- INSTANCES
  - Instances**
  - Launch Templates
  - Spot Requests
  - Reserved Instances
  - Dedicated Hosts
- IMAGES
  - AMIs
  - Bundle Tasks
- ELASTIC BLOCK STORE
  - Volumes
  - Snapshots
- NETWORK & SECURITY
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces

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	Public DNS (IPv4)	IPv4 Public IP
		i-0148f5eb64b9e659e	t2.micro	us-west-1a	running	Initializing	None		54.193.64.42

**Instance:** i-0148f5eb64b9e659e **Public IP:** 54.193.64.42

Description

Status Checks

Monitoring

Tags

Instance ID	i-0148f5eb64b9e659e	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	54.193.64.42
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-30-0-90.us-west-1.compute.internal
Availability zone	us-west-1a	Private IPs	172.30.0.90
Security groups	launch-wizard-1 . <a href="#">view inbound rules</a>	Secondary private IPs	
Scheduled events	<a href="#">No scheduled events</a>	VPC ID	vpc-24149643
AMI ID	ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20180126 (ami-07585467)	Subnet ID	subnet-fdc7a7a6
Platform	-	Network interfaces	eth0
IAM role	-	Source/dest. check	True
Key pair name	my-keys	T2 Unlimited	Disabled
ClassicLink	-	Owner	709440151559



# Change permissions of keys file

```
#-----:::  
~/Downloads // 5 // chyld@Chylds-MacBook-Pro  
[7]: chmod 400 my-keys.pem
```

```
#-----:::  
~/Downloads // 5 // chyld@Chylds-MacBook-Pro  
[8]: ls -al my-keys.pem  
-r-----@ 1 chyld  staff  1692 Mar 26 12:16 my-keys.pem
```

# Login to AWS

```
#-----:::
~/Downloads // 5 // chylD@ChylDs-MacBook-Pro
[10]: ssh -i my-keys.pem ubuntu@54.193.64.42
The authenticity of host '54.193.64.42 (54.193.64.42)' can't be established.
ECDSA key fingerprint is SHA256:MWdEZ291SWbWU1s0juojogY0LyaegQ2jDzXz60+fzHI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '54.193.64.42' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-1049-aws x86_64)

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

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

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

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-172-30-0-90:~$
```

# Download miniconda

— — —

- <https://conda.io/miniconda.html>
- `$ wget https://repo.continuum.io/miniconda/Miniconda3-latest-Linux-x86_64.sh`

```
ubuntu@ip-172-30-0-90:~$ wget https://repo.continuum.io/miniconda/Miniconda3-latest-Linux-x86_64.sh
--2018-03-26 19:28:05-- https://repo.continuum.io/miniconda/Miniconda3-latest-Linux-x86_64.sh
Resolving repo.continuum.io (repo.continuum.io)... 104.16.18.10, 104.16.19.10, 2400:cb00:2048:1::6810:130a, ...
Connecting to repo.continuum.io (repo.continuum.io)|104.16.18.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 58304693 (56M) [application/x-sh]
Saving to: 'Miniconda3-latest-Linux-x86_64.sh'
```

```
Miniconda3-latest-Linux-x86_64.sh 100%[=====>] 55.60M 2.76MB/s in 20s
```

```
2018-03-26 19:28:25 (2.74 MB/s) - 'Miniconda3-latest-Linux-x86_64.sh' saved [58304693/58304693]
```

# Install miniconda

— — —

- `$ bash Miniconda3-latest-Linux-x86_64.sh`
- `<use default path>`
- `yes, add to PATH`

```
ubuntu@ip-172-30-0-90:~$ conda --version
conda 4.4.10
ubuntu@ip-172-30-0-90:~$
```



# Install Python libraries

— — —

```
$ conda install pandas numpy matplotlib scikit-learn scipy
```

```
$ conda install -c conda-forge jupyterlab
```

```
# start jupyter
```

```
$ jupyter lab --no-browser --ip=0.0.0.0 --port=8888 --NotebookApp.token=''
```

# Copy files from S3 to EC2

— — —

```
Downloads pip install awscli
```

```
Downloads aws s3 cp s3://my-bucket/main.py .
```

```
Downloads aws s3 cp master.py s3://my-bucket/master.py
```

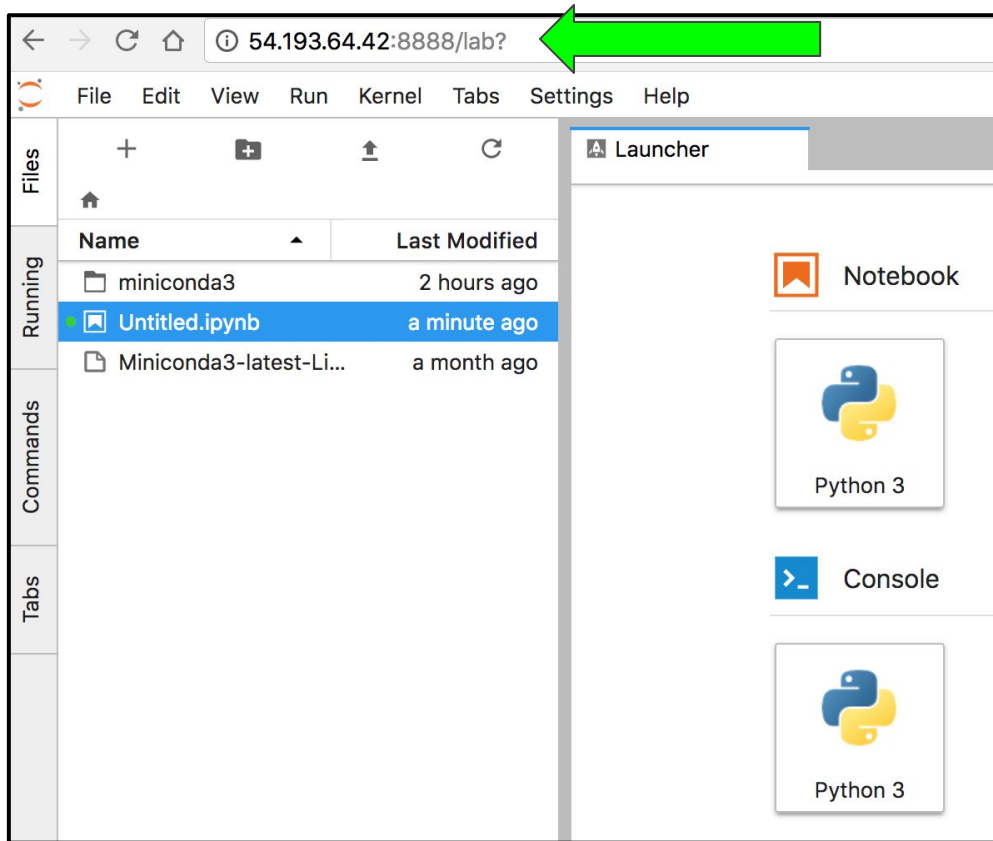
# Start Jupyter Lab

— — —

```
ubuntu@ip-172-30-0-90:~$ jupyter lab --no-browser --ip=0.0.0.0 --port=8888 --NotebookApp.token=''
[W 21:40:22.579 LabApp] All authentication is disabled. Anyone who can connect to this server will be able to run code.
[I 21:40:22.589 LabApp] JupyterLab beta preview extension loaded from /home/ubuntu/miniconda3/lib/python3.6/site-packages/jupyterlab
[I 21:40:22.589 LabApp] JupyterLab application directory is /home/ubuntu/miniconda3/share/jupyter/lab
[I 21:40:22.593 LabApp] Serving notebooks from local directory: /home/ubuntu
[I 21:40:22.593 LabApp] 0 active kernels
[I 21:40:22.594 LabApp] The Jupyter Notebook is running at:
[I 21:40:22.594 LabApp] http://0.0.0.0:8888/
[I 21:40:22.594 LabApp] Use Control-C to stop this server and shut down all kernels (twice to skip confirmation).
```

# Use Jupyter Notebook on AWS EC2

1. Open browser
2. Use IP address of EC2
3. Use 8888 for port number
4. Enjoy!



# Finished with your EC2 instance?

- Terminate if you don't need it anymore
- Stop if you only want to pause the use of the machine - and not get charged (disk space usage costs still apply)

