Launching & Connecting to an AWS Instance

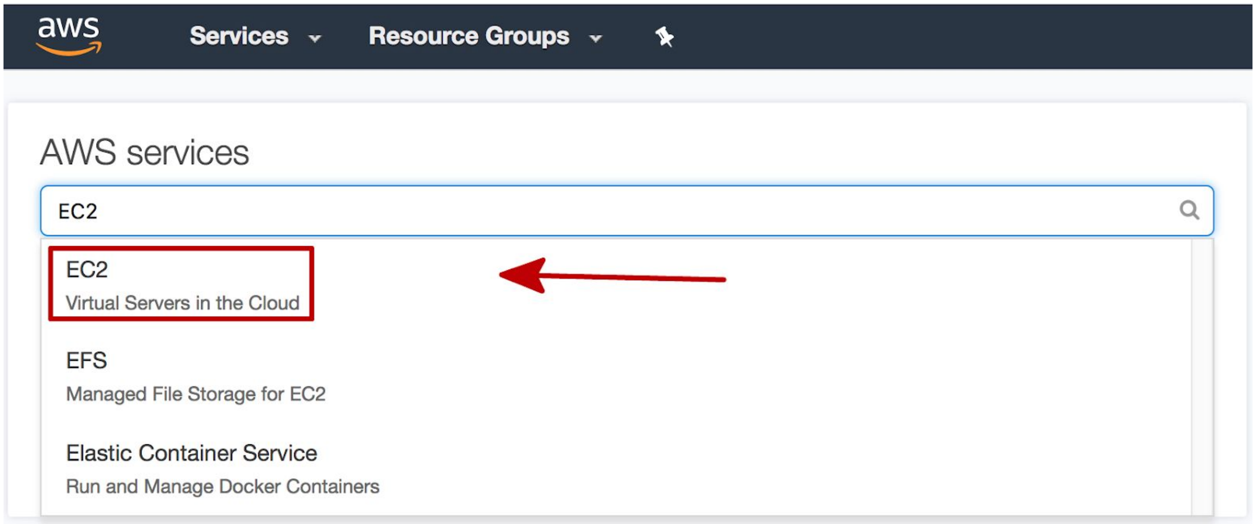
Author: www.github.com/BryanBo-Cao
Fri June 22, 2018

Local computer environment: macOS Sierra version 10.12.6

Launching an Instance in AWS

Click aws

Search “EC2” in the search bar and select “EC2”.



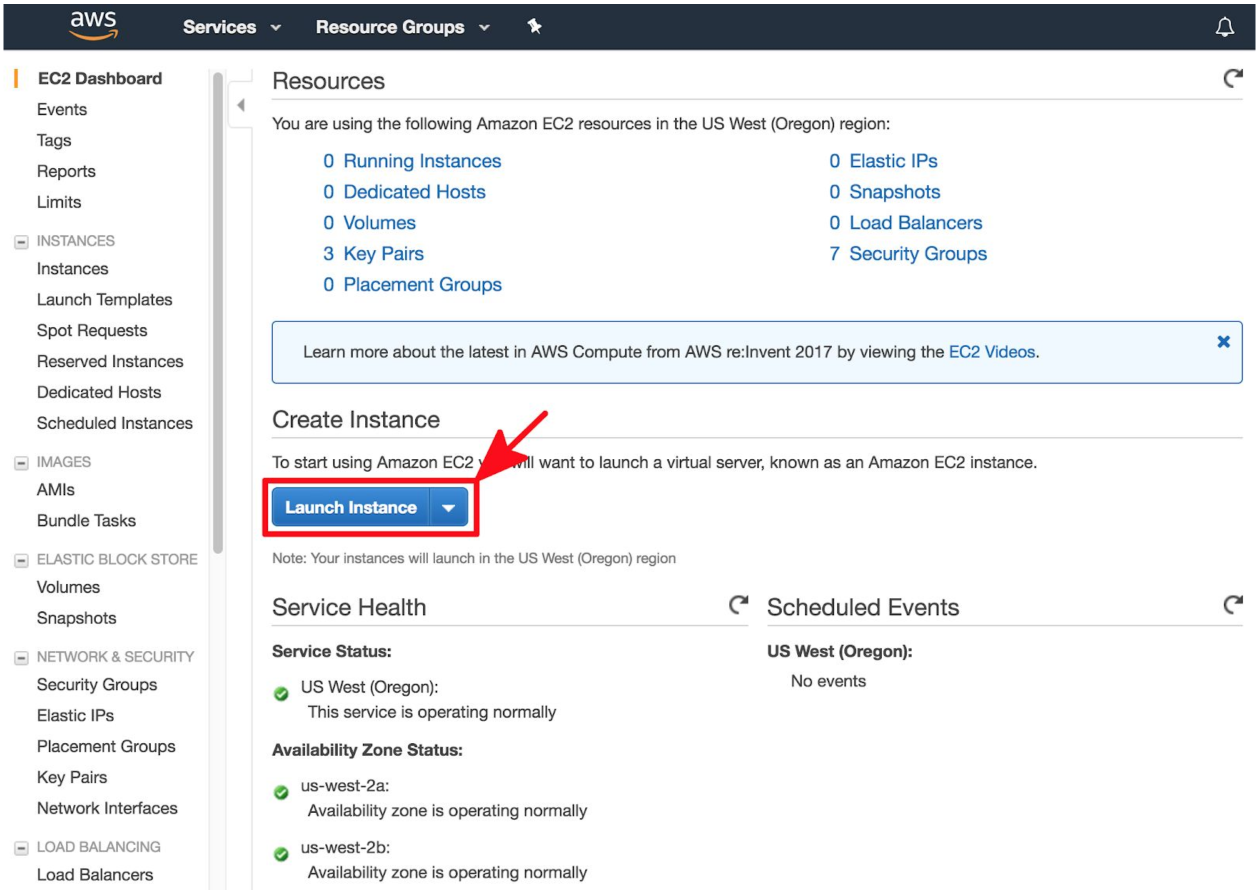
AWS services

EC2

EC2
Virtual Servers in the Cloud

EFS
Managed File Storage for EC2

Elastic Container Service
Run and Manage Docker Containers



Resources

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

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
3 Key Pairs	7 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

Create Instance

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

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

Service Health

Service Status:

US West (Oregon):
This service is operating normally

Availability Zone Status:

us-west-2a:
Availability zone is operating normally

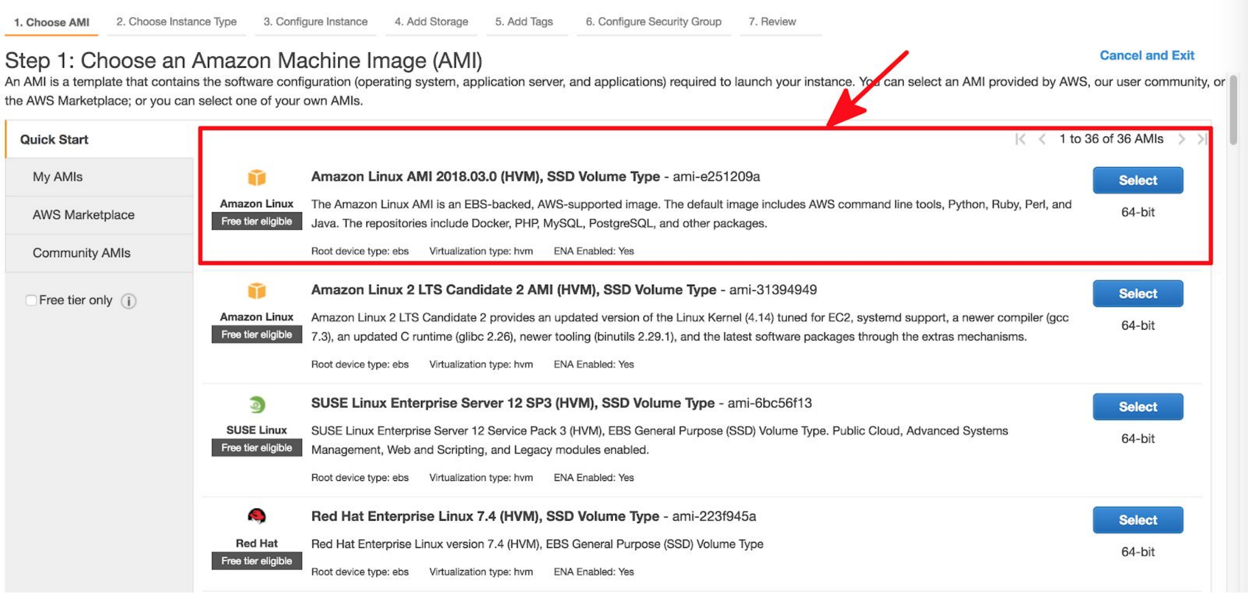
us-west-2b:
Availability zone is operating normally

Scheduled Events

US West (Oregon):

No events

You may choose an image depending on your needs.



Step 1: Choose an Amazon Machine Image (AMI)

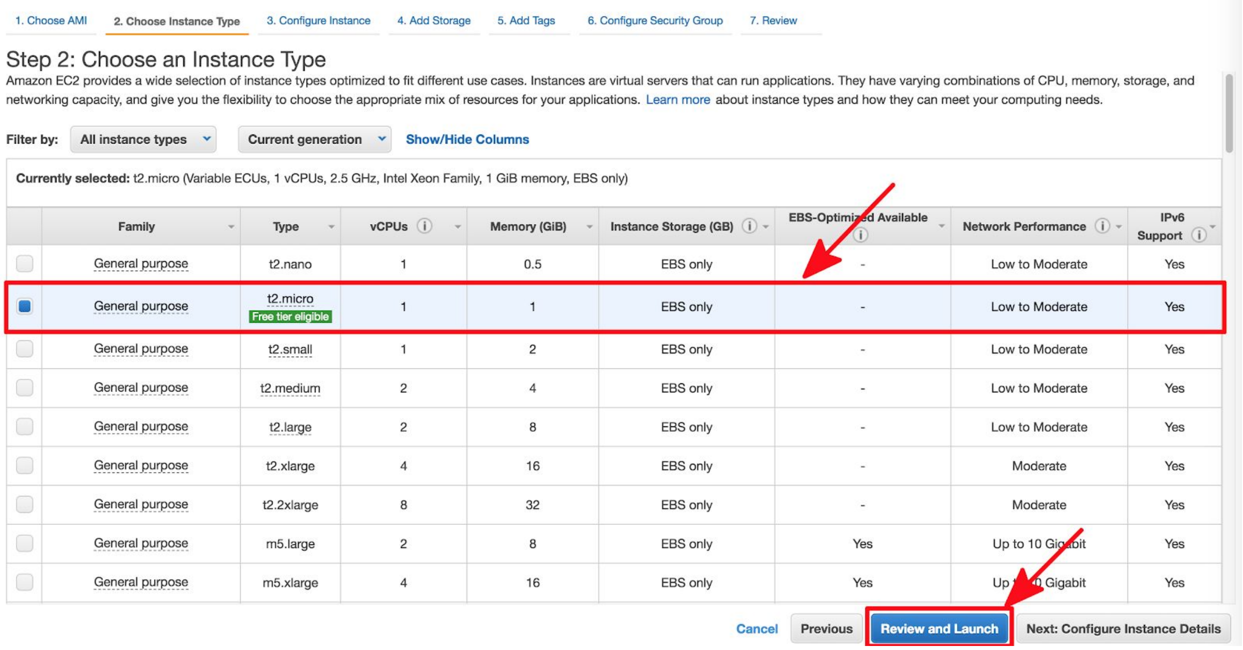
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-e251209a
Amazon Linux — Free tier eligible — 64-bit
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

Amazon Linux 2 LTS Candidate 2 AMI (HVM), SSD Volume Type - ami-31394949
Amazon Linux — Free tier eligible — 64-bit
Amazon Linux 2 LTS Candidate 2 provides an updated version of the Linux Kernel (4.14) tuned for EC2, systemd support, a newer compiler (gcc 7.3), an updated C runtime (glibc 2.26), newer tooling (binutils 2.29.1), and the latest software packages through the extras mechanisms.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-6bc56f13
SUSE Linux — Free tier eligible — 64-bit
SUSE Linux Enterprise Server 12 Service Pack 3 (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

Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type - ami-223f945a
Red Hat — Free tier eligible — 64-bit
Red Hat Enterprise Linux version 7.4 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes



Step 2: Choose an Instance Type

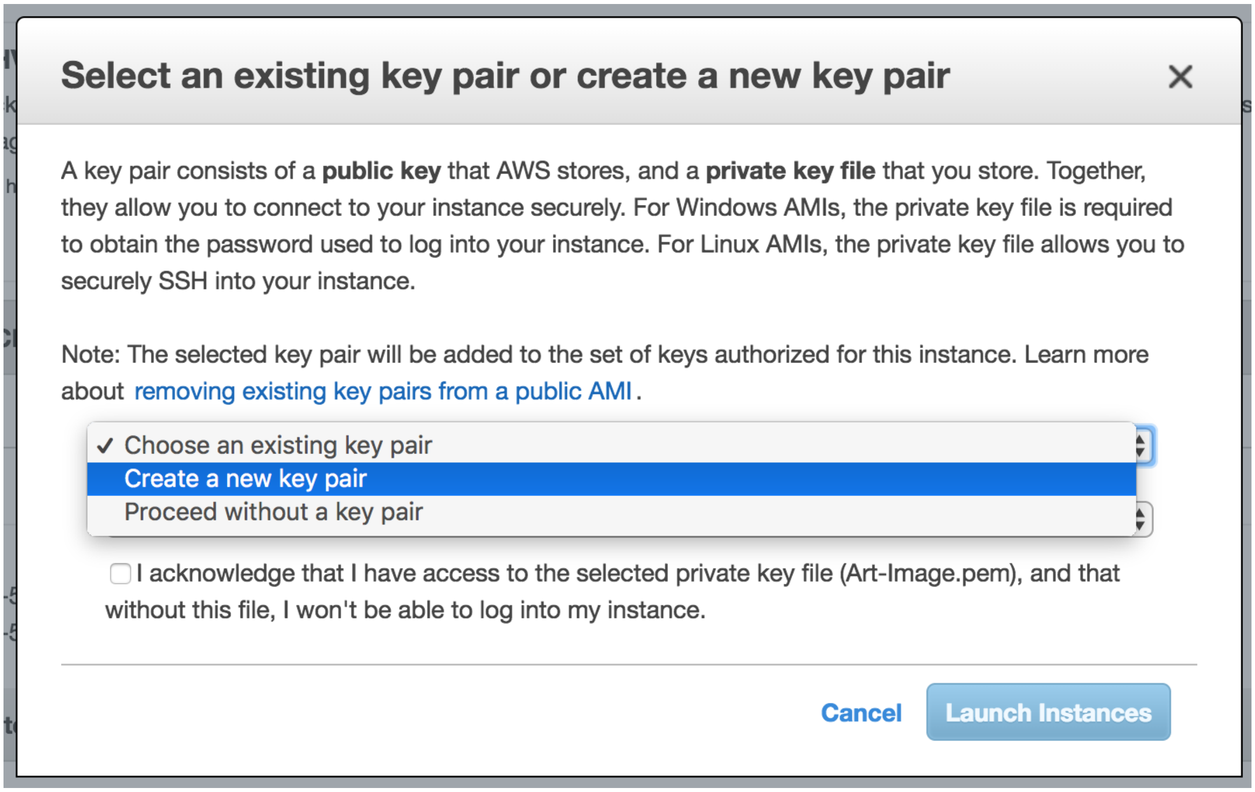
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources 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 (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
□	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes

You may use your existing key pair. Here as an example I create a new key pair.

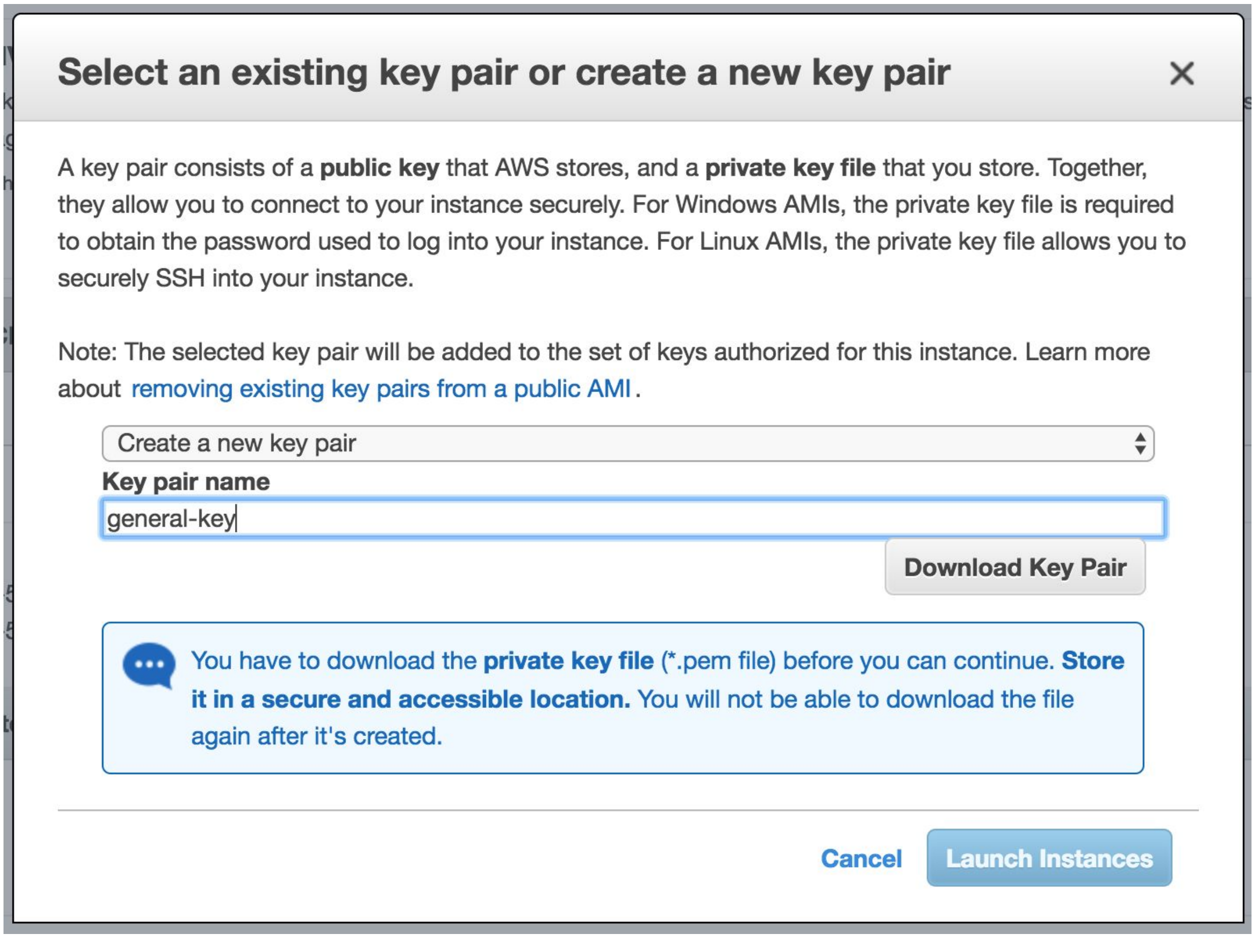

Select an existing key pair or create a new key pair

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 .

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

Set the key pair name as “general-key”, download it and click “Launch Instances”.



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.

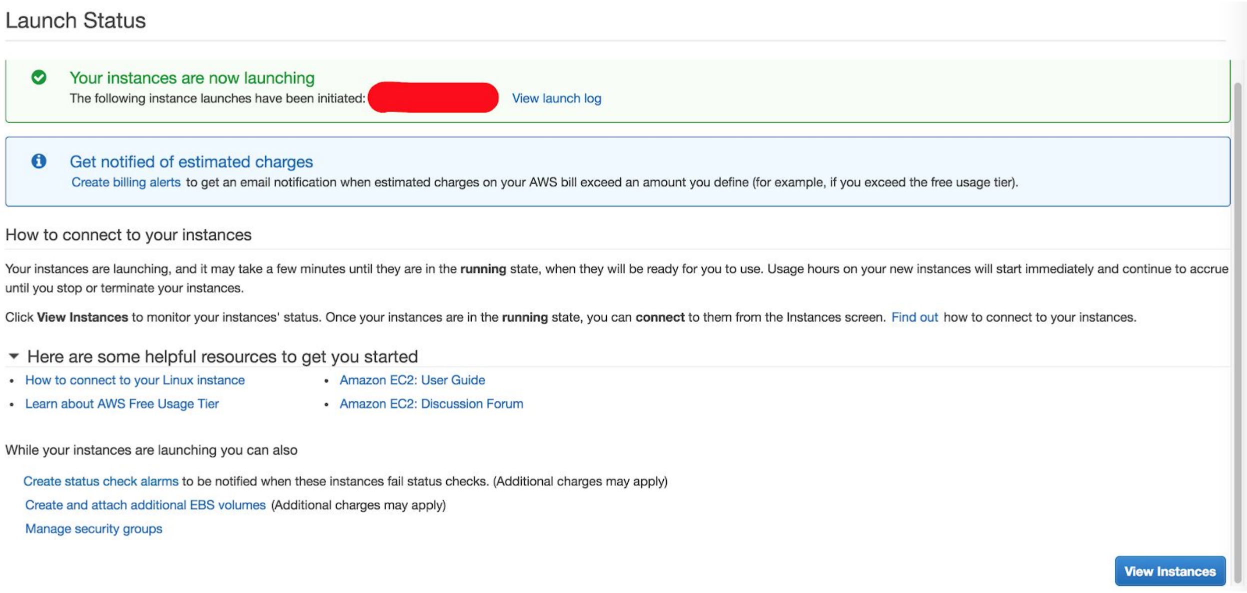
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

general-key

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.



Launch Status

Your instances are now launching
The following instance launches have been initiated: [redacted] View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

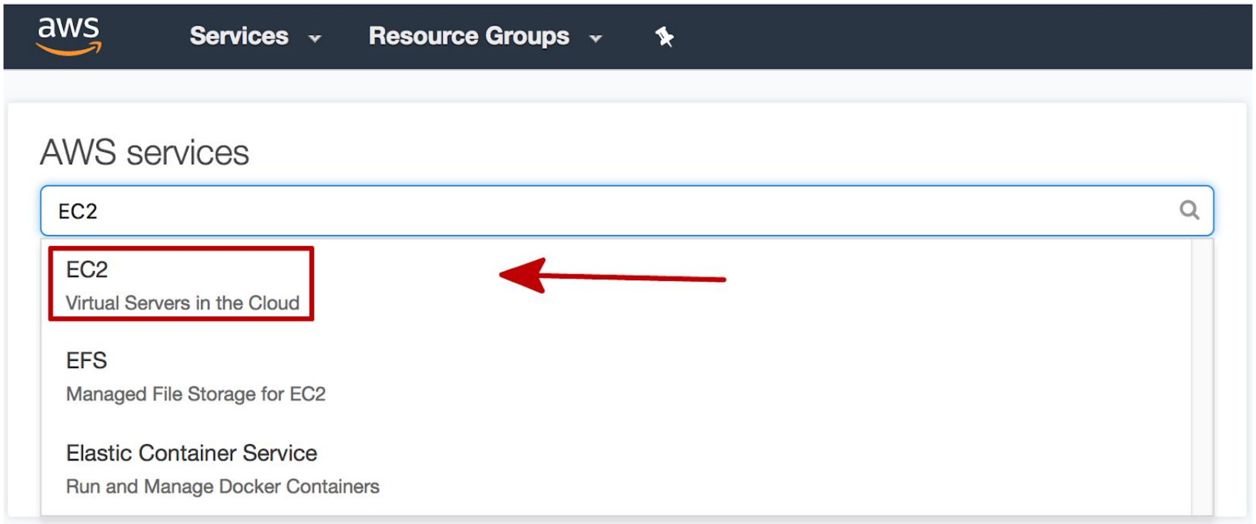
While your instances are launching you can also

Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
Create and attach additional EBS volumes (Additional charges may apply)
Manage security groups

Connecting to an AWS Instance

Click aws

Search “EC2” in the search bar and select “EC2”.



AWS services

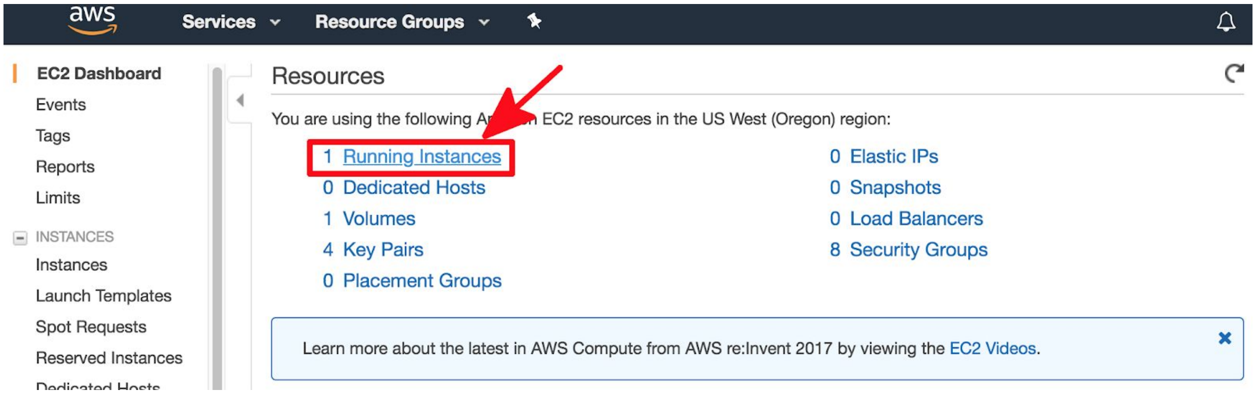
EC2

EC2
Virtual Servers in the Cloud

EFS
Managed File Storage for EC2

Elastic Container Service
Run and Manage Docker Containers

Select “* Running Instances”



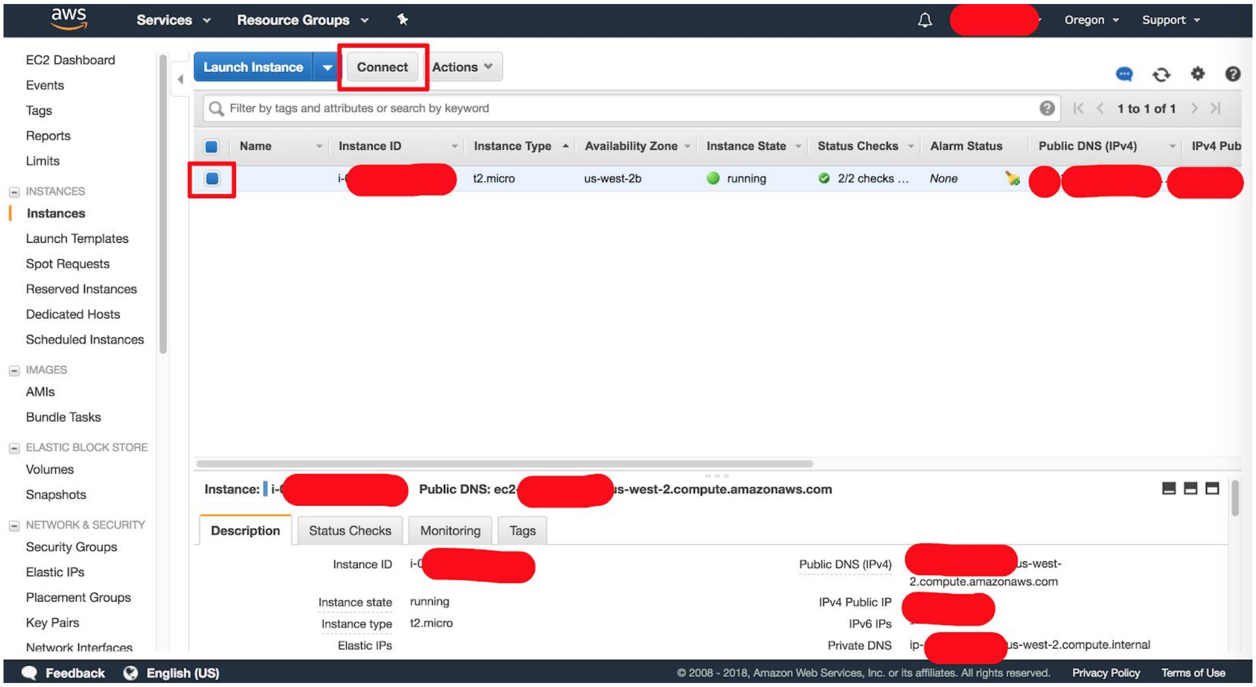
Resources

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

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

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

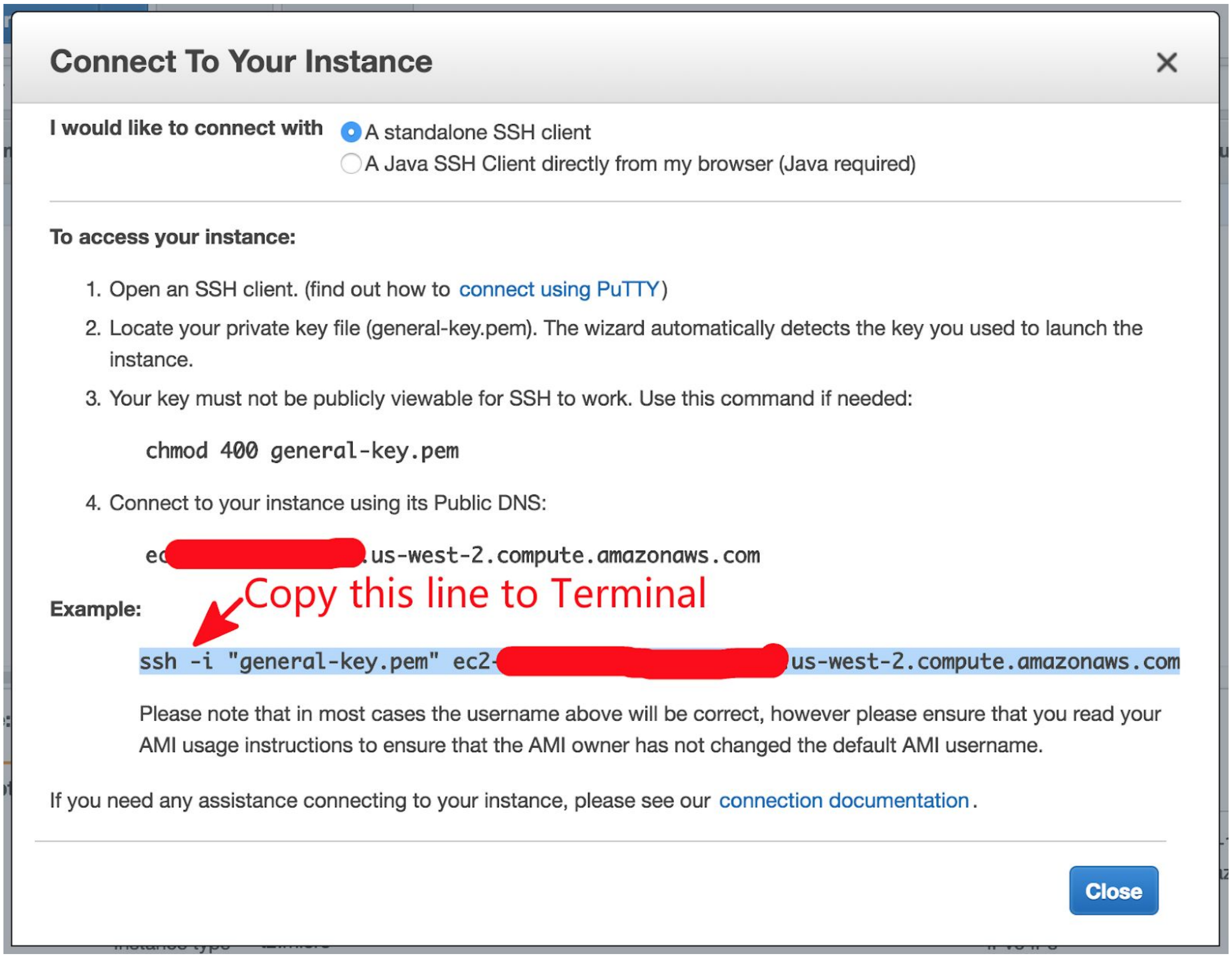
Select the instance that you would like to connect.



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Pub
■		i-[redacted]	t2.micro	us-west-2b	● running	✓ 2/2 checks ...	*None*	[redacted]	[redacted]

Instance: i-[redacted] **Public DNS:** ec2-[redacted]us-west-2.compute.amazonaws.com

Instance ID	i-[redacted]	Public DNS (IPv4)	[redacted]us-west-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	[redacted]
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-[redacted]us-west-2.compute.internal



I would like to connect with ● A standalone SSH client
○ A Java SSH Client directly from my browser (Java required)

To access your instance:

1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (general-key.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 general-key.pem
```

4. Connect to your instance using its Public DNS:

```
ec[redacted].us-west-2.compute.amazonaws.com
```

Example:

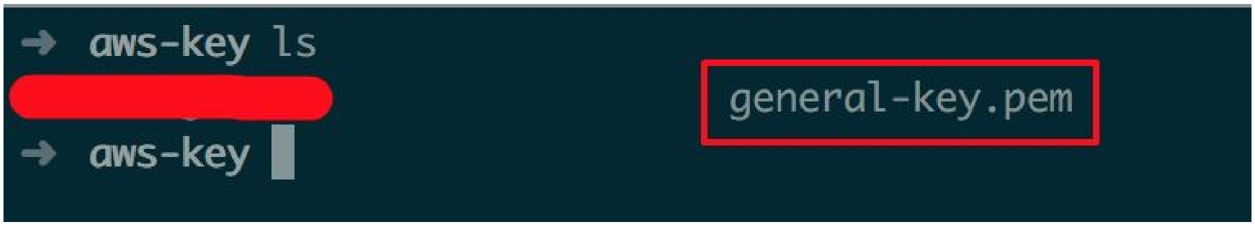
Copy this line to Terminal

```
ssh -i "general-key.pem" ec2-[redacted]us-west-2.compute.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

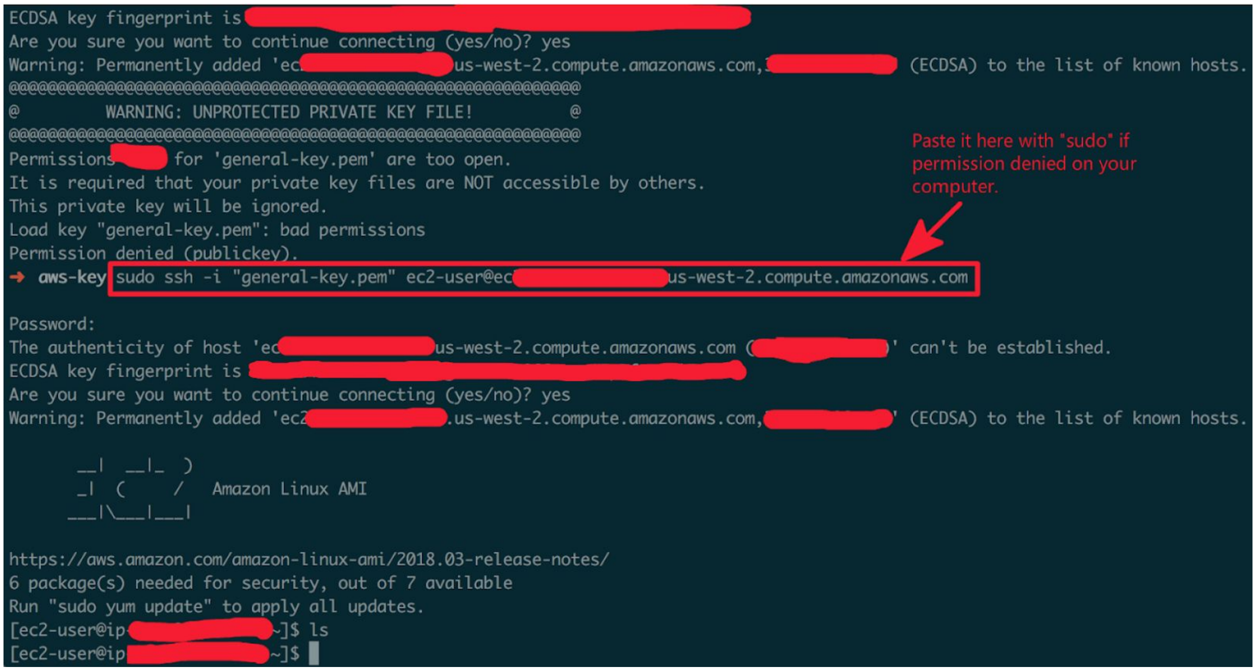
If you need any assistance connecting to your instance, please see our connection documentation.

On the Terminal, before sshing, navigate (cd) to the directory where the key (general-key.pem) that was generated and downloaded.



```
➜ aws-key ls
[redacted]                  general-key.pem
➜ aws-key
```

Copy **ssh -i "general-key.pem" ec2-*.us-west-2.compute.amazonaws.com** to the Terminal.



```
ECDSA key fingerprint is [redacted]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec[redacted]us-west-2.compute.amazonaws.com,[redacted] (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions[redacted] for 'general-key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "general-key.pem": bad permissions
Permission denied (publickey).
➜ aws-key sudo ssh -i "general-key.pem" ec2-user@ec[redacted]us-west-2.compute.amazonaws.com

Password:
The authenticity of host 'ec[redacted]us-west-2.compute.amazonaws.com ([redacted])' can't be established.
ECDSA key fingerprint is [redacted]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2[redacted].us-west-2.compute.amazonaws.com,[redacted]' (ECDSA) to the list of known hosts.

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

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
6 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip[redacted]~]$ ls
[ec2-user@ip[redacted]~]$
```

Paste it here with "sudo" if permission denied on your computer.

If permission denied, append “**sudo**” to the front of the command, which should be **sudo ssh -i "general-key.pem" ec2-*.us-west-2.compute.amazonaws.com**

When you see the Amazon Linux AMI logo on your terminal, it means you have connected to the AWS instance.