



Guide-Setup EC2 server on Amazon Web Services

Web Application Development COP3834

Professor Navarro


Watch tutorial on setting up EC2 Virtual Machine

Step 1: Launch Management Console

From the AWS Management Console, Launch a virtual machine

<https://us-east-2.console.aws.amazon.com/ec2/v2/home?#LaunchInstanceWizard:>

Select Amazon Linux 2 AMI (Free tier eligible)



Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0443305dabd4be2bc (64-bit x86) / ami-0806cc3ac665

Amazon Linux
Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and

Boot device type: ebs Virtualization type: hvm EMI Enabled: Yes

Select Instance Type t2.micro, 1vCPU, 1GiB, EBS only

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 appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

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

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)
<input type="checkbox"/>	t2	t2.nano	1	0.5
<input checked="" type="checkbox"/>	t2	t2.micro Free tier eligible	1	1

Press **Next: Configure Instance Details**

Next: Configure Instance Details

Press **Next: Add Storage** at Step 3

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch m

Cancel

Previous

Review and Launch

Next: Add Storage

On Step 4, change Size to 10 GiB

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) ⓘ
Root	/dev/xvda	snap-074ce2aabf60fabaf	10	General Purpose SSD (gp2) ▼	100 / 3000	N/A
Add New Volume						

Then press **Next: Add Tags**

Next: Add Tags

On Step 5, click **Add Tag** button to create meta data tag for your server instance.

Key will be Name

Value will be: prod-web-abcd {the last 4 letters will be the first letter of the first name of each group member.} In the example below, the Production Web server is part of the group that belongs to Robert, Watkins, Bell, and Yasmine.

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 ⓘ
Name	prod-web-rwby	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

After adding Key pair, press Next: Configure Security Group button

Next: Configure Security Group

Step 6: Update description to SSH for dev and admin

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 ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
SSH	TCP	22	Custom 0.0.0.0/0	SSH for dev and admin

Add Rule

Cancel

Previous

Review and Launch

Press Review and Launch button

Review your settings in Step 7 then press Launch button

Step 7: Review Instance Launch

Cancel

Previous

Launch

At the prompt to “Select an existing key pair or create new key pair”, select Create a new Key pair

Name it prod-web-abc-access (no spaces). Replace abc to match your server name. Press Download Key Pair button and store the file on your hard disk. Share with your team mate.

Download 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](#).

Create a new key pair



Key pair name

prod-web-rwby-access

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

After you save the key pair, press Launch Instances button.

Launch Instances

Launch Status



Your instances are now launching

The following instance launches have been initiated: I-03505da0776294e6a [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

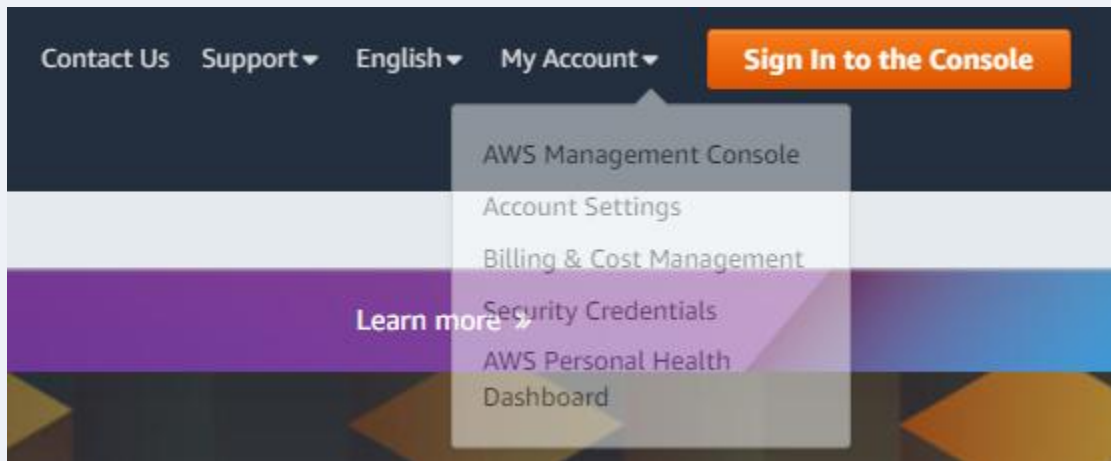
- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

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

View Instances

From aws.amazon.com, select My Account/AWS management Console

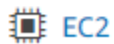


Select EC2 under Recently visited Services or under All services button

AWS Management Console

AWS services

▼ Recently visited services



EC2



Billing

This page shows all of your EC2 resources that are running:

Resources

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	1	Dedicated Hosts	0	Elastic IPs	0
Instances	1	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	2	Snapshots	0
Volumes	1				

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#)

Service health

Region: US East (Ohio)

Status: This service is operating normally

[Service Health Dashboard](#)

Select Instances, then press the Actions button and Connect. As an alternative, you can navigate to <https://console.aws.amazon.com/ec2/>

Instances (1/1) Info

[Filter instances](#)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	prod-web-rwby	i-03505da0776294e6a	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a

[Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

This page will have instructions on using an SSH client as well. Select Connect button at bottom.

Connect to instance [Info](#)

Connect to your instance i-03505da0776294e6a (prod-web-rwby) using any of these options


EC2 Instance Connect

Session Manager


SSH client

EC2 Serial Console

Instance ID


 i-03505da0776294e6a (prod-web-rwby)

Public IP address

 3.144.2.154

User name


Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

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

Cancel

Connect

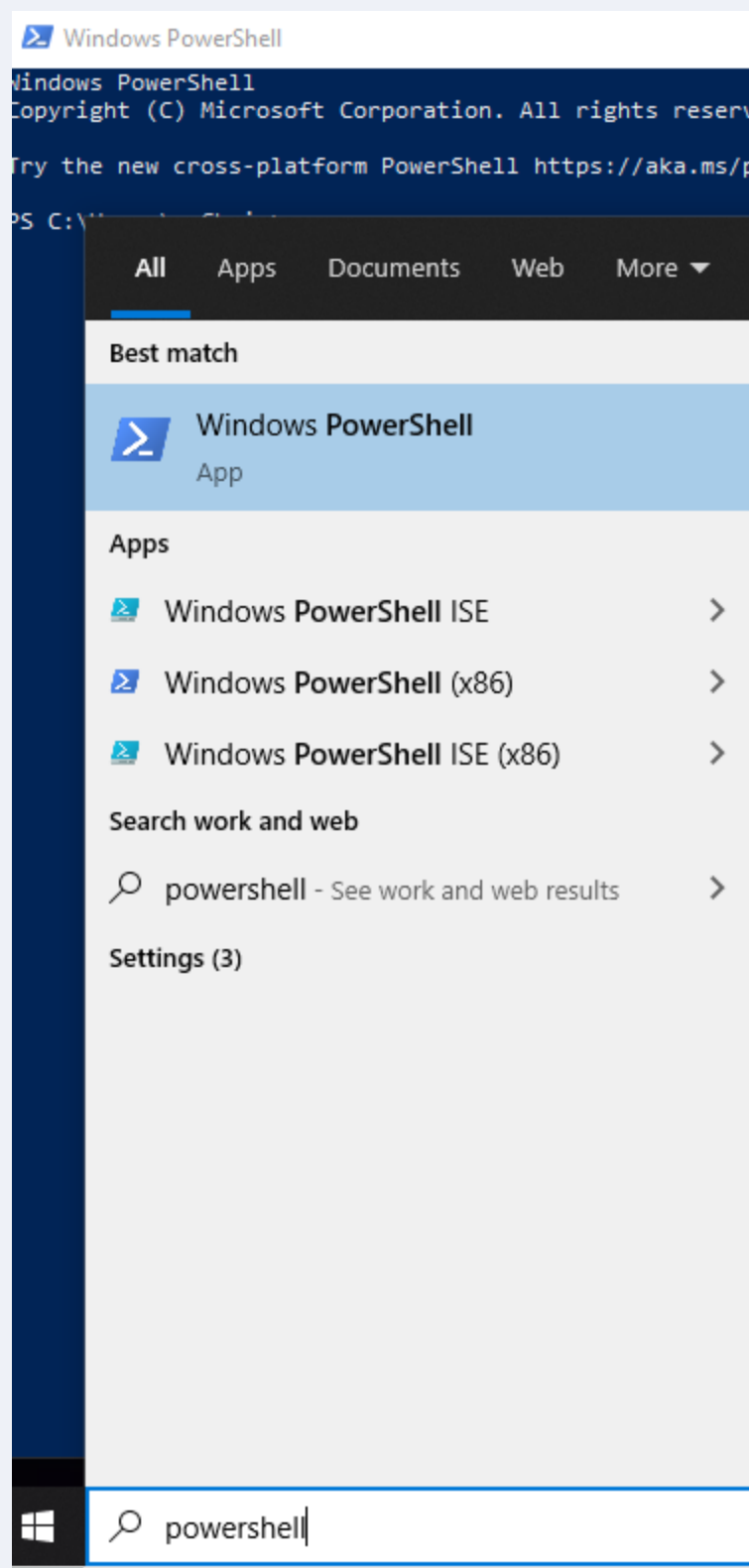
You are now logged in with a browser connection.



```
[ec2-user@ip-172-31-14-199 ~]$ whoami
ec2-user
[ec2-user@ip-172-31-14-199 ~]$
```

Using ssh connection is preferred. If on Windows, I recommend using putty client at <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

Open powershell in windows



Navigate to the path of your pm file and change the permissions to read only for user on Windows and type the commands below


```

> Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\vmChris> cd c:\
PS C:\> ls

    Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          12/7/2019   4:14 AM                PerfLogs
d-r---           8/12/2021  12:47 PM                Program Files
d-r---           8/8/2021   1:56 PM                Program Files (x86)
d-----          8/8/2021   1:50 PM                Python39
d-r---           7/27/2021  10:37 PM                Users
d-----          8/8/2021   1:50 PM                Windows
d-----          7/27/2021  10:43 PM                Windows.old
-ar---           8/11/2021  11:04 PM            1704 prod-web-rwby-access - Copy.pem
-ar---           8/11/2021  11:04 PM            1704 prod-web-rwby-access.pem

PS C:\> icacls.exe prod-web-rwby-access.pem /reset
processed file: prod-web-rwby-access.pem
Successfully processed 1 files; Failed processing 0 files
PS C:\> icacls.exe prod-web-rwby-access.pem /grant:r "$($env:username):(r)"
processed file: prod-web-rwby-access.pem
Successfully processed 1 files; Failed processing 0 files
PS C:\> icacls.exe prod-web-rwby-access.pem /inheritance:r
processed file: prod-web-rwby-access.pem
Successfully processed 1 files; Failed processing 0 files
PS C:\>

```

If you are in Linux or mac, simply type `chmod 400 nameOfPemFile`

From windows 10 cmd prompt type the following. Be sure to change your instance name based on your ssh instructions in aws.

```

C:\Users\vmChris> ssh -i "c:\prod-web-rwby-access.pem" ec2-user@ec2-3-144-2-154.us-east-2.compute.amazonaws.com
Last login: Thu Aug 12 16:39:18 2021 from ec2-3-16-146-2.us-east-2.compute.amazonaws.com

 _ | _ | _ )
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
4 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-14-199 ~]$

```

Note: Instructions were taken and modified from Amazon aws documentation (2021)

