

CCNP ROUTING AND SWITCHING



AWS EC2 Instance

Brennen

2/21/2022

Task 1: Launch Your Amazon EC2 Instance

1. Choose EC2 from the AWS Management Console on the Services menu
2. Launch Instance from the Instance button in the top left
3. Choose the Amazon Linux 2 AMI and Select it.
4. Choose a t2.micro instance and choose next: configure instance details in the bottom right
5. Select Lab VPC and protect against accidental termination

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 [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP

Hostname type

DNS Hostname ☐ Enable IP name IPv4 (A record) DNS requests
☒ Enable resource-based IPv4 (A record) DNS requests
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group ☐ Add instance to placement group

Capacity Reservation

Domain join directory [Create new directory](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☒ [Protect against accidental termination](#)

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy [Additional charges will apply for dedicated tenancy.](#)

Elastic Inference ☐ Add an Elastic Inference accelerator
[Additional charges apply.](#)

Credit specification ☐ Unlimited
[Additional charges may apply](#)

File systems [Create new file system](#)

6. Expand advance details on the bottom and paste the command into the user data field:

```
#!/bin/bash
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
```

This command installs a web server, configures it, activates and creates a web page.

▼ Advanced Details

Enclave ☐ Enable

Metadata accessible ☐ Enabled

Metadata version ☐ V1 and V2 (token optional)

Metadata token response hop limit ☐ 1

Allow tags in metadata ☐ Disabled

User data ☒ As text ☐ As file ☐ Input is already base64 encoded

```
#/bin/bash
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo "<html><h1>Hello From Your Web Servers/h1></html>" > /var/www/html/index.html
```

Cancel Previous Review and Launch Next: Add Storage

7. You do not have to worry about adding storage, choose next: add tags
8. Select Add Tag and configure a key of Name and Value of Web Server, then click next.

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

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 <input type="checkbox"/>	Volumes <input type="checkbox"/>	Network Interfaces <input type="checkbox"/>
Name	Web Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

9. Configure the security group with a name of Web Server security group and a description of Security group for my web server. Remove SSH access for security. Then click review and launch

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	e.g. SSH for Admin Desktop

10. Select Launch, choose proceed without a key pair. Click the necessary popups and launch the instance, then view it.

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. Amazon EC2 supports ED25519 and RSA key pair types.

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](#).

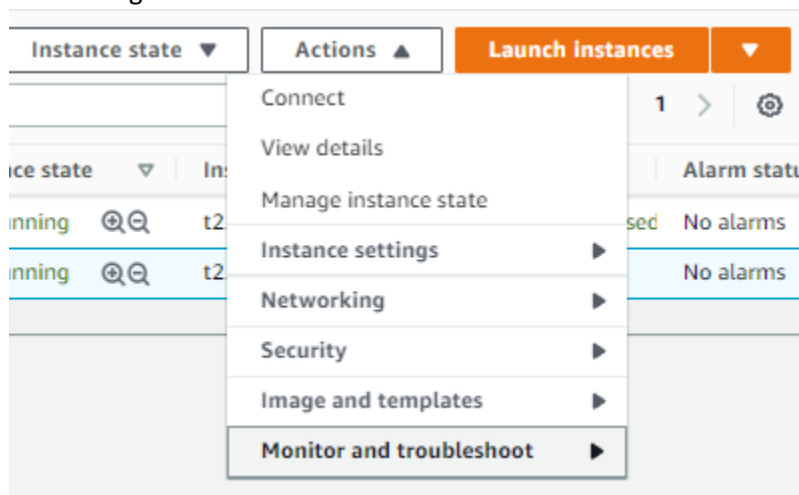
☒ Proceed without a key pair

☒ I acknowledge that without a key pair, I can connect to this instance only by using EC2 Instance Connect or if I know the password built into the AMI. Note that EC2 Instance Connect is only supported on Amazon Linux 2 and Ubuntu. [Learn more](#).

11. The instance will initially be pending but once the state changes to running, you know the EC2 instance is working.

Task 2: Monitor Your Instance

12. Choose the Status Checks Tab by clicking on the instance and selecting the 5th tab that appears, then the 6th Monitoring tab then in the actions menu select Monitor and troubleshoot, retrieve the system log.



13. Look at the output and choose cancel

Get system log [Info](#)

Review system log for instance i-0cc3b91bd2589ef2d as of Thu Feb 17 2022 08:59:01 GMT-0800 (Pacific Standard Time)



Copy log

Download

```
[ 30.557016] cloud-init[3246]: Complete.
[ 30.609138] cloud-init[3246]: Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/
[ 31.093104] xfs filesystem being remounted at /tmp supports timestamps until 2038 (0x7fffffff)
[ 31.111047] xfs filesystem being remounted at /var/tmp supports timestamps until 2038 (0x7fffffff)
[ 30.905775] cloud-init[3246]: ci-info: no authorized ssh keys fingerprints found for user ec2-user.
ci-info: no authorized ssh keys fingerprints found for user ec2-user.
<14>Feb 17 16:55:55 ec2:
<14>Feb 17 16:55:55 ec2: #####
<14>Feb 17 16:55:55 ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
<14>Feb 17 16:55:55 ec2: 256 SHA256:s/Nc/hgu9AhnJjYK10Ya2Iqfodin0CsrHoLeaSMHZMk no comment (ECDSA)
<14>Feb 17 16:55:55 ec2: 256 SHA256:ZjWCLhFCy0ncXjsyUuB95KNkMKieC3sBjFECdn8HlWc no comment (ED25519)
<14>Feb 17 16:55:55 ec2: 2048 SHA256:d0a+yP1BQYMNNDLjJtGCIYTTBeN6UKhK0lSwMibaG0 no comment (RSA)
<14>Feb 17 16:55:55 ec2: -----END SSH HOST KEY FINGERPRINTS-----
<14>Feb 17 16:55:55 ec2: #####
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBL/y+12Xyu5tWAn333qVn8N/28wdGW3JC78ip3aCjg9REfIKQda0Ey8vd/A/
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFGZ31lhGSnjCMEmD71tW7E2mmKGCwboTaxTFCwvi3gJ
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDHbSUCUVbOWBOAdMSH7yrj8rX/YoaQtZSIKqMLOsXSLDnQTPPYkUpwTn+TfCRHgwTc02PYnuJ3F7KLUE2woKIqSpw8Za
-----END SSH HOST KEY KEYS-----
[ 31.125207] cloud-init[3246]: Cloud-init v. 19.3-44.amzn2 finished at Thu, 17 Feb 2022 16:55:56 +0000. Datasource DataSourceEc2.
```

14. In the Actions menu select Monitor and troubleshoot then get a screenshot. Then click cancel.

Get instance screenshot [Info](#)

i-0cc3b91bd2589ef2d (Web Server) on 2022-02-17 at T08:59:30.973 -08:00



```
Amazon Linux 2
Kernel 5.10.96-90.460.amzn2.x86_64 on an x86_64

ip-10-0-1-124 login: [ 31.093104] xfs filesystem being remounted at /tmp supports timestamps until 2038 (0x7fffffff)
[ 31.111047] xfs filesystem being remounted at /var/tmp supports timestamps until 2038 (0x7fffffff)
_
```

For boot or networking issues, use the EC2 serial console for troubleshooting. Choose the **Connect** button to start a session.

Connect

Cancel

Task 3: Update Your Security Group and Access the Web Server

15. Choose the Details tab after clicking the instance
16. Copy the IPV4 Public IP of the instance
17. Open a new tab and paste the ip address
18. You won't be able to access the web server so return to the EC2 Management Console.
19. On the left, choose security groups
20. Choose Inbound rules, edit inbound rules and configure:

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Inbound rule 1
Delete

Security group rule ID
-

Type [Info](#)
HTTP

Protocol [Info](#)
TCP

Port range [Info](#)
80

Source type [Info](#)
Anywhere-IPv4

Source [Info](#)
0.0.0.0/0 X

Description - optional [Info](#)

Add rule

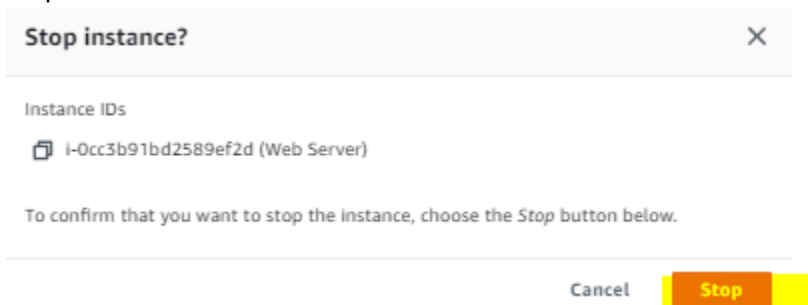
Cancel
Preview changes
Save rules

21. The webpage should now display:

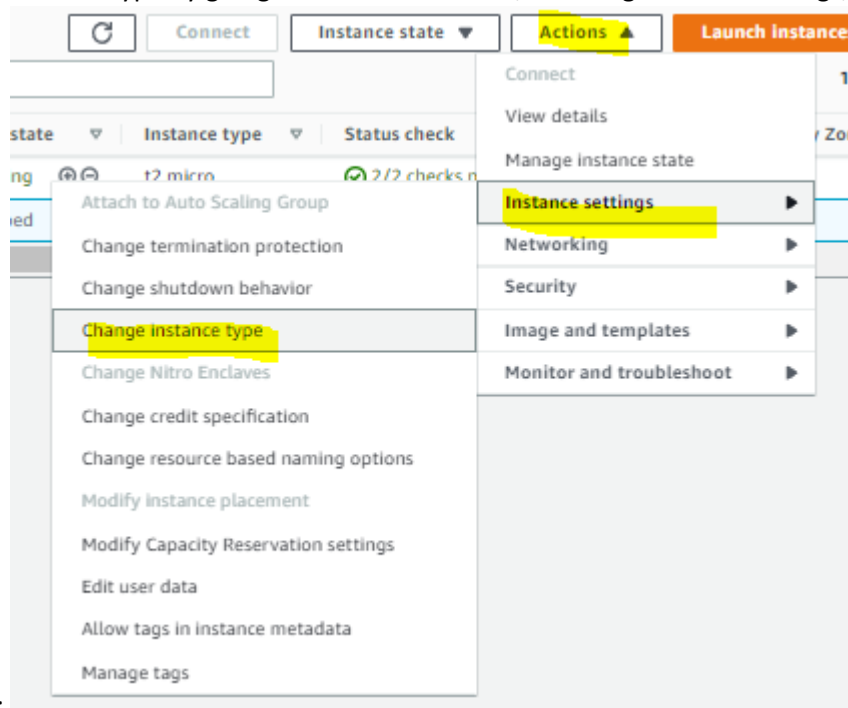


Task 4: Resize Your Instance: Instance Type and EBS Volume

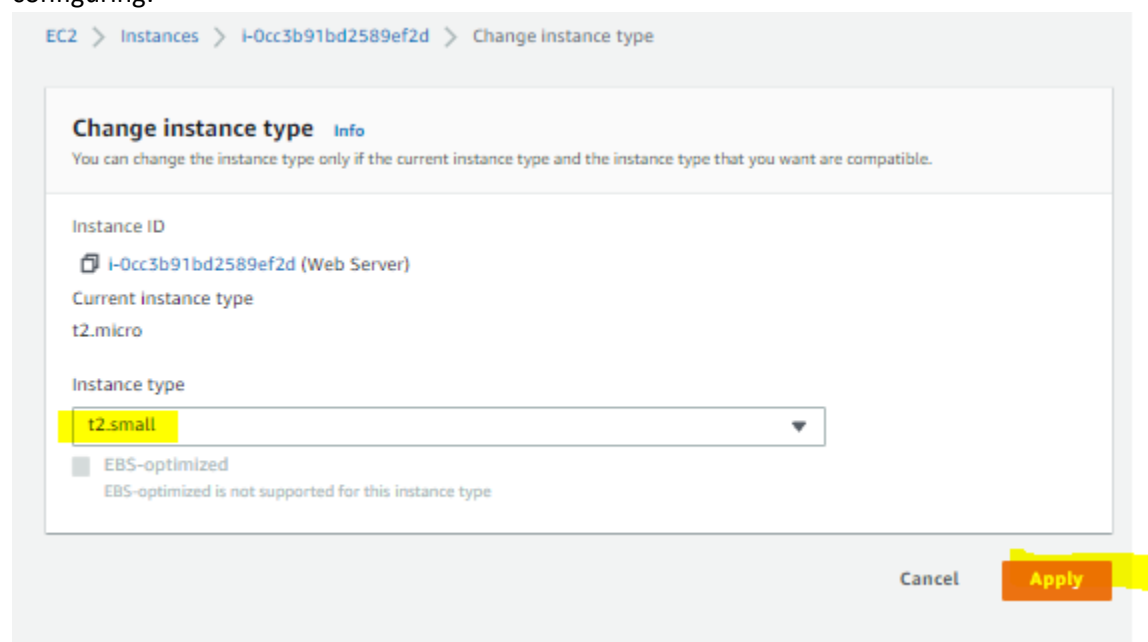
22. Stop the instance to resize it. Select Instances from the left and in the Instance State menu Stop instance.



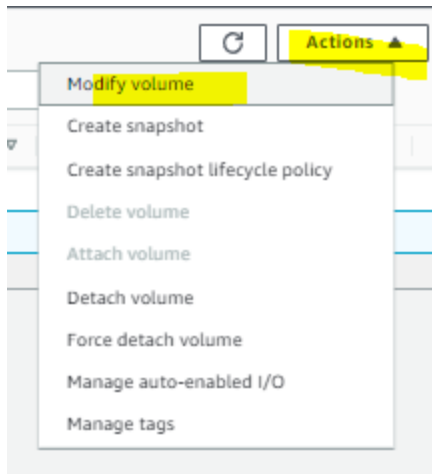
23. Change the instance type by going to the actions menu, selecting instance settings, changing the type, then



configuring:



24. Resize the volume from the left volumes tab.



25. Change disk volume to 10 GiB and choose modify and yes.

EC2 > Volumes > vol-0766f50791385896f > Modify volume

Modify volume Info

Modify the type, size, and performance of an EBS volume.

Volume details

Volume ID
vol-0766f50791385896f (Web Server)

Volume type Info
General Purpose SSD (gp2)

Size (GiB) Info
10
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS Info
100/3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Cancel **Modify**

26. Restart the Instance by clicking on Instances, Start Instance from the instance menu and start.

Instance type changed successfully

Successfully started i-0cc3b91bd2589ef2d

Instances (1/2) Info

Search

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pub
<input type="checkbox"/>	Bastion Host	i-04b926a11d3ed6825	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-
<input checked="" type="checkbox"/>	Web Server	i-0cc3b91bd2589ef2d	Pending	t2.small	-	No alarms +	us-east-1a	-

Task 5: Explore EC2 Limits

27. Choose limits from the left and select running instances from the drop down list.

Task 6: Test Termination Protection

28. DO this by selecting Instances again, and from the instance state menu try to terminate the instance. It should fail and give this message:

Failed to terminate an Instance: The instance 'i-0cc3b91bd2589ef2d' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.

29. In the actions menu select instance setting and turn off termination protection, save it and try to terminate it again, it should work this time.

EC2 > Instances > i-0cc3b91bd2589ef2d > Change termination protection

Change termination protection [Info](#)

Enable termination protection to prevent your instance from being accidentally terminated.

Instance ID
i-0cc3b91bd2589ef2d (Web Server)

Termination protection
☐ Enable

Termination protection disabled.
The instance is no longer protected against accidental termination. If the instance is terminated, data stored on ephemeral storage is lost.

Cancel **Save**

Successfully terminated i-0cc3b91bd2589ef2d