Introduction to Amazon EC2

Lab overview and objectives

This lab provides you with a basic overview of launching, resizing, managing, and monitoring an Amazon Elastic Compute Cloud (Amazon EC2) instance.

Amazon EC2 is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale cloud computing simple and intuitive to use.

With the web service interface of Amazon EC2, you can obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources. You can run application servers, blogs, batch processing, and more on the Amazon computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes so that you can quickly scale capacity both up and down as your computing requirements change.

Amazon EC2 changes the economics of computing so that you pay for only the capacity that you actually use. Amazon EC2 provides developers the tools to build failure-resilient applications and isolate themselves from common failure scenarios.

Objectives

After completing this lab, you will know how to:

- Launch a web server with termination protection enabled
- Monitor Your EC2 instance
- Modify the security group that your web server is using to allow HTTP access
- Resize your EC2 instance to scale
- Explore Amazon EC2 limits
- Test termination protection
- Terminate your EC2 instance

Task 1: Launching your EC2 instance

In this task, you launch an EC2 instance with *termination protection*. Termination protection prevents you from accidentally terminating an EC2 instance. You also deploy your instance with a user data script in order to deploy a simple web server.

5. In the AWS Management Console on the **Services** menu, choose **EC2**.
6. In the left navigation pane, choose **EC2 Dashboard** to ensure that you are on the dashboard page.
7. Choose **Launch instance**, and then select **Launch instance**.

Step 1: Name your EC2 instance

Using tags, you can categorize your AWS resources in different ways (for example, by purpose, owner, or environment). This categorization is useful when you have many resources of the same type. You can quickly

identify a specific resource based on the tags that you have assigned to it. Each tag consists of a key and a value, both of which you define.

When you name your instance, AWS creates a key-value pair. The key for this pair is **Name**, and the value is the name you enter for your EC2 instance.

8. In the **Name and tags** section, for **Name**, enter `Web-Server`
9. Choose the **Add additional tags** link.
10. From the **Resource types** dropdown list, ensure that both **Instances** and **Volumes** are selected.

Step 2: Choose an Amazon Machine Image (AMI)

An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud. An AMI includes the following:

- A template for the root volume for the instance (for example, an operating system or an application server with applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it is launched

The **Quick Start** list contains the most commonly used AMIs. You can also create your own AMI or select an AMI from the AWS Marketplace, an online store where you can sell or buy software that runs on AWS.

11. Locate the **Application and OS Images (Amazon Machine Image)** section. It is just below the **Name and tags** section.
12. In the **AMI Machine Image (AMI)** box, notice that **Amazon Linux 2 AMI** is selected by default. Keep this setting.

Step 3: Choose an instance type

Amazon EC2 provides a wide selection of instance types that are optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more instance sizes so that you can scale your resources to the requirements of your target workload.

In this step, you choose a **t2.micro** instance. This instance type has 1 virtual CPU and 1 GiB of memory.

13. Keep the default instance type, **t2.micro**.

Step 4: Configure a key pair

Amazon EC2 uses public key cryptography to encrypt and decrypt login information. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

In this lab, you do not log in to your instance, so you do not require a key pair.

14. In the **Key pair (login)** section, from the **Key pair name - *required*** dropdown list, choose **Proceed without a key pair**.

Step 5: Configure the network settings

You use this pane to configure networking settings.

The virtual private cloud (VPC) indicates which VPC you want to launch the instance into. You can have multiple VPCs, including different ones for development, testing, and production.

15. In the **Network settings** section, choose **Edit**.
16. From the **VPC - *required*** dropdown list, choose **Lab VPC**.

    The Lab VPC was created using an AWS CloudFormation template during the setup process of your lab. This VPC includes two public subnets in two different Availability Zones.

17. In the **Network settings** section, for **Security group name - *required***, enter `Web Server security group`

    A security group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

    In this lab, you do not log in to your instance using SSH. Removing SSH access improves the security of the instance.

18. To delete the existing SSH rule, next to **Security group rule 1**, choose **Remove**.

Step 6: Add storage

Amazon EC2 stores data on a network-attached virtual disk called Amazon Elastic Block Store (Amazon EBS).

You launch the EC2 instance using a default 8 GiB disk volume. This is your root volume (also known as a boot volume).

19. In the **Configure storage** pane, keep the default storage configuration.

Step 7: Configure advanced details

20. Expand the **Advanced details** pane.

When you no longer require an EC2 instance, you can terminate it, which means that the instance stops, and Amazon EC2 releases the instance's resources. You cannot restart a terminated instance. If you want to prevent your users from accidentally terminating the instance, you can enable termination protection for the instance, which prevents users from terminating instances.

21. From the **Termination protection** dropdown list, choose **Enable**.

When you launch an instance in Amazon EC2, you have the option of passing user data to the instance. These commands can be used to perform common automated configuration tasks and even run scripts after the instance starts.

22. Copy the following commands, and paste them into theIn the **User data** text box.

```
#!/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
```

The script does the following:

- Install an Apache web server (httpd)
- Configure the web server to automatically start on boot
- Activate the Web server
- Create a simple web page

Step 8: Launch an EC2 instance

Now that you have configured your EC2 instance settings, it is time to launch your instance.

23. In the **Summary** section, choose **Launch instance**.
24. Choose **View all instances**

The instance appears in a **Pending** state, which means that it is being launched. It then changes to **Running**, which indicates that the instance has started booting. There will be a short time before you can access the instance.

The instance receives a public Domain Name System (DNS) name that you can use to contact the instance from the Internet.

Next to your **Web-Server**, select the check box. The **Details** tab displays detailed information about your instance.

To view more information in the **Details** tab, drag the window divider upward.

Review the information displayed in the **Details, Security** and **Networking** tabs.

25. Wait for your instance to display the following:

Note: Refresh if needed.

- **Instance State:** Running
- **Status Checks:** 2/2 checks passed

Task 2: Monitoring your instance

Monitoring is an important part of maintaining the reliability, availability, and performance of your EC2 instances and your AWS solutions.

26. Choose the **Status checks** tab.

    With instance status monitoring, you can quickly determine whether Amazon EC2 has detected any problems that might prevent your instances from running applications. Amazon EC2 performs automated checks on every running EC2 instance to identify hardware and software issues.

    Notice that both the **System reachability** and **Instance reachability** checks have passed.

27. Choose the **Monitoring** tab.

    This tab displays Amazon CloudWatch metrics for your instance. Currently, there are not many metrics to display because the instance was recently launched.

    You can chose a graph to see an expanded view.

    Amazon EC2 sends metrics to Amazon CloudWatch for your EC2 instances. Basic (5 minute) monitoring is enabled by default. You can enable detailed (1 minute) monitoring.

28. At the top of the page, choose the **Actions** dropdown menu. Select **Monitor and troubleshoot Get system log**.

    The system log displays the console output of the instance, which is a valuable tool for diagnosing problems. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started. If you do not see a system log, wait a few minutes and then try again.

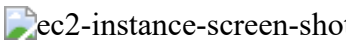
29. Scroll through the output, and note that the HTTP package was installed from the user data that you added when you created the instance. The entries in the system log should be similar to the following example:

```
[   26.760639] cloud-init[3280]: Installed:

[   26.770051] cloud-init[3280]: httpd.x86_64 0:2.4.52-1.amzn2

[   26.777748] cloud-init[3280]: Dependency Installed:

[   26.781750] cloud-init[3280]: apr.x86_64 0:1.7.0-9.amzn2

[   26.793739] cloud-init[3280]: apr-util.x86_64 0:1.6.1-5.amzn2.0.2
```

```
[   26.796595] cloud-init[3280]: apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2
[   26.805964] cloud-init[3280]: generic-logos-httpd.noarch 0:18.0.0-4.amzn2
[   26.817765] cloud-init[3280]: httpd-filesystem.noarch 0:2.4.52-1.amzn2
[   26.829760] cloud-init[3280]: httpd-tools.x86_64 0:2.4.52-1.amzn2
[   26.833753] cloud-init[3280]: mailcap.noarch 0:2.1.41-2.amzn2
[   26.845761] cloud-init[3280]: mod_http2.x86_64 0:1.15.19-1.amzn2.0.1
[   26.849762] cloud-init[3280]: Complete!
```

30. To return to the Amazon EC2 dashboard, choose **Cancel**.
31. With your **Web-Server** selected, choose the **Actions** dropdown menu, and select **Monitor and troubleshoot Get instance screenshot**.

    This option shows you what your EC2 instance console would look like if a screen were attached to it. It is essentially a command line interface.

    If you are unable to reach your instance via SSH or RDP, you can capture a screenshot of your instance and view it as an image. This option provides visibility about the status of the instance and allows for quicker troubleshooting.

32. At the bottom of the page, choose **Cancel**.

Task 3: Updating your security group and accessing the web server

When you launched the EC2 instance, you provided a script that installed a web server and created a simple web page. In this task, you access content from the web server.

33. Select the check box next to the Amazon EC2 **Web-Server** that you created, and then choose the **Details** tab.
34. Copy the **Public IPv4 address** of your instance to your clipboard.
35. In your web browser, open a new tab, paste the IP address that you just copied, and then press Enter.

    Question: Are you able to access your web server? Why not?

    You are not currently able to access your web server because the security group is not permitting inbound traffic on port 80, which is used for HTTP web requests. This is a demonstration of how to use a security group as a firewall to restrict the network traffic that is allowed in and out of an instance.

    To correct this issue, you now update the security group to permit web traffic on port 80.

36. Keep the browser tab open, but return to the **EC2 Management Console** tab.
37. In the left navigation pane, choose **Security Groups**.

38. Next to **Web Server security group**, select the check box.

39. Choose the **Inbound rules** tab.

    The security group currently has no rules.

40. Choose **Edit inbound rules**, and then choose **Add rule** and configure the following options:

    - **Type:** Choose **HTTP**.
    - **Source:** Choose **Anywhere-IPv4**.

    Note: Notice the *"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."* While this is true and common best practice, this lab allows access from any IP address (Anywhere) to simplify both the security group configuration and testing of the website running on your EC2 instance.

41. Choose **Save rules**

42. Return to the web server browser tab with the public IPv4 address that you previously opened, and choose to refresh the page.

    You should see the message **Hello From Your Web Server!**

Task 4: Resizing your instance - instance type and EBS volume

As your needs change, you might find that your instance is over utilized (too small) or under utilized (too large). If so, you can change the instance type. For example, if a t2.micro instance is too small for its workload, you can change it to an m5.medium instance. Similarly, you can change the size of a disk.

Stop your instance

Before you can resize an instance, you must stop it.

When you stop an instance, it is shut down. There is no charge for a stopped EC2 instance, but the storage charge for attached EBS volumes remains.

43. On the **EC2 Management Console**, in the left navigation pane, choose **Instances**.

    The check box next to **Web Server** should already be selected.

44. At the top of the page, select the **Instance state** dropdown menu, and choose **Stop instance**.

45. In the **Stop instance?** pop-up window, choose **Stop**.

    Your instance performs a normal shutdown and then stops running.

46. Wait for the **Instance state** to display **Stopped**.

Change the instance type

47. Select the check box next to your **Web-Server**. From the **Actions** dropdown menu, select **Instance settings Change instance type**, and then configure the following option:

- **Instance type:** Select **t2.nano**.

48. Choose **Apply**.

    When the instance is started again, it is a t2.nano instance.

    Note: You are restricted from using other instance types in this lab.

Resize the EBS volume

49. In the left navigation menu, choose **Volumes**.
50. Select the check box for the one volume that is listed, which is attached to your **Web-Server** instance.
51. In the **Actions** dropdown menu, select **Modify Volume**.

    The disk volume currently has a size of 8 GiB. You now increase the size of this disk.

52. Change the **Size (GiB)** to `10`
53. Choose **Modify**.
54. To confirm and increase the size of the volume, in the **Modify** pop-up window, choose **Modify**

Start the resized instance

You now start the instance again, which now has less memory but more disk space.

55. In left navigation pane, choose **Instances**. Next to your **Web-Server**, select the check box.
56. From the **Instance state** dropdown menu, choose **Start instance**.

Task 5: Exploring EC2 limits

Amazon EC2 provides different resources that you can use. These resources include images, instances, volumes, and snapshots. When you create an AWS account, there are default limits on these resources on a per-Region basis.

57. In the left navigation pane, choose **Limits**.

    Note: There is a limit on the number of instances that you can launch in this Region. When launching an instance, the request must not cause your usage to exceed the current instance limit in that Region.

    You can request an increase for many of these limits.

Task 6: Testing termination protection

You can delete your instance when you no longer need it. This is referred to as terminating your instance. You cannot connect to or restart an instance after it has been terminated.

In this task, you learn how to use termination protection.

58. In left navigation pane, choose **Instances**. Select the check box for your **Web-Server**.

59. At the top of the page in the **Instance state** dropdown menu, choose **Terminate instance**. From the **Terminate instance?** pop-up window, choose **Terminate**.

    Note: At the top of the page, a message says **Failed to terminate an instance: The instance 'i-xxxxxxxxxxx' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.** This message is a safeguard to prevent the accidental termination of an instance. If you really want to terminate the instance, you need to turn off the termination protection.