

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

КАФЕДРА ІНФОРМАТИКИ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

**ІНСТРУКТИВНО-МЕТОДИЧНІ МАТЕРІАЛИ ДО КОМП'ЮТЕРНОГО
ПРАКТИКУМУ КРЕДИТНОГО МОДУЛЯ**

"Інфраструктура інформаційних систем"

для спеціальності

121 Інженерія програмного забезпечення

Київ, 2024 р.

ЗМІСТ

ПОЯСНЕННЯ ДО ВИКОНАННЯ.....	3
1 КОМПЛЕКС ЛАБОРАТОРНИХ РОБІТ «УПРАВЛІННЯ РЕСУРСАМИ ІНФРАСТРУКТУРИ У ХМАРІ AZURE»	5
1.1 КОНТРОЛЬНІ ПИТАННЯ	6
2 КОМПЛЕКС ЛАБОРАТОРНИХ РОБІТ «ПОБУДОВА ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ ХМАРНИХ ПОСЛУГ AWS, ЩО РЕАЛІЗУЮТЬ ОБЧИСЛЕННЯ, СХОВИЩА ТА МЕРЕЖІ»	10
2.1 ACCESS THE AWS MANAGEMENT CONSOLE	11
2.2 MODULE 1: LAUNCHING AN EC2 INSTANCE AND ATTACHING AN EBS VOLUME.....	11
2.3 MODULE 2: CREATING AN S3 BUCKET	15
2.4 MODULE 3: INTRODUCTION TO IAM.....	17
2.5 MODULE 4: BUILDING THE AMAZON VIRTUAL PRIVATE CLOUD	22
2.6 MODULE 5: INTRODUCTION TO AWS LAMBDA	33
2.7 КОНТРОЛЬНІ ПИТАННЯ	43
3 КОМПЛЕКС ЛАБОРАТОРНИХ РОБІТ «ОСНОВИ СТВОРЕННЯ ВІРТУАЛІЗОВАНИХ СЕРЕДОВИЩ НА БАЗІ ПРОДУКТІВ VMWARE, VIRTUALIZATION 101»	45
4 КОМПЛЕКС ЛАБОРАТОРНИХ РОБІТ «СУЧАСНА МЕРЕЖА NSX ТА ГІПЕРКОНВЕРГЕНТНА ІНФРАСТРУКТУРА VSAN НА БАЗІ VMWARE»	49

Пояснення до виконання

При виконанні лабораторних робіт буде виникати необхідність вводити назви об'єктів та імена (пристроїв, модулів, екземплярів, програм, сертифікатів та ін.) та/або їх параметрів. Замість імен за замовченням студент повинен використовувати імена, що включають його прізвище. Також, необхідно використовувати єдину електронну пошту для реєстрацій при виконанні усіх робіт. Таким чином, буде можливість підтвердити особисте виконання робіт. На рисунках показані декілька прикладів зміни імен за замовченням на персональні (SampleVM, mycontainer, learn-deploy-aci-rg та аналогічні в інших місцях лабораторних робіт підлягають обов'язковій зміні). **За використання імен за замовченням оцінка буде знижена.**

```
az vm create \
--resource-group [sandbox resource group name] \
--location westus \
--name SampleVM \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys \
--verbose
```

```
az container create \
--resource-group learn-deploy-aci-rg \
--name mycontainer \
--image mcr.microsoft.com/azuredocs/aci-helloworld \
--ports 80 \
--dns-name-label $DNS_NAME_LABEL \
--location eastus
```

Azure CLI

```
az group create --name learn-deploy-aci-rg --location eastus
```

Звіт у вигляді одного файлу формується для кожного з чотирьох комплексів робіт окремо і починається з титульного аркушу. У звіті повинен бути зміст. Кожний модуль комплексу лабораторних робіт оформлюється як окремий розділ. Невиконання цієї вимоги призведе до зниження балу.

У звіт заносити знімки екрану з ключовими, послідовними, суттєвими для розуміння роботи кроками, що демонструють логіку виконання і функціональну залежність. Обов'язково треба додавати коментарі до важливих кроків виконання роботи. На більшості знімків потрібно залишати верхню частину з адресним рядком (URI) та іменем користувача входу на портал, де виконується завдання. Знімки екрана не розмивати, щоб текст був читабельним.

Файли звіту виконання лабораторної роботи називайте за таким шаблоном: "ІП-х Прізвище ЛРz", "ІТ-х Прізвище ЛРz" або "ІС-х Прізвище ЛРz", х – номер групи, z – номер комплексу лабораторних робіт (1-4).

При захисті роботи продемонструвати обліковий запис на відповідному порталі (Azure, AWS, VMware) і результати виконання модулів лабораторних робіт.

1 Комплекс лабораторних робіт «Управління ресурсами інфраструктури у хмарі Azure»

Цей комплекс дозволяє студентам навчитися створювати, керувати, захищати та масштабувати ресурси віртуальних машин та контейнерів в Azure.

Для виконання комплексу лабораторних робіт треба увійти на портал <https://docs.microsoft.com/en-us/learn/> за допомогою облікового запису microsoft та перейти за посиланням для виконання модулю. Рекомендується, щоб цей обліковий запис не був пов'язаний з існуючою підпискою Azure.

1. Модуль **Introduction to Azure Virtual Machines** (рис. 1.1). Посилання <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-virtual-machines/>
2. Модуль **Create a Windows virtual machine in Azure**. Посилання <https://docs.microsoft.com/en-us/learn/modules/create-windows-virtual-machine-in-azure/>
3. Модуль **Manage virtual machines with the Azure CLI**. Посилання <https://docs.microsoft.com/en-us/learn/modules/manage-virtual-machines-with-azure-cli/>
4. Модуль **Add and size disks in Azure virtual machines**. Посилання <https://docs.microsoft.com/en-us/learn/modules/add-and-size-disks-in-azure-virtual-machines/>
5. Модуль **Build and run a web application with the MEAN stack on an Azure Linux virtual machine**. Посилання <https://docs.microsoft.com/en-us/learn/modules/build-a-web-app-with-mean-on-a-linux-vm/>
6. Модуль **Manage and control traffic flow in your Azure deployment with routes**. Посилання <https://docs.microsoft.com/en-us/learn/modules/control-network-traffic-flow-with-routes/>
7. Модуль **Manage complex cloud deployments by using advanced JSON ARM template features**. Посилання <https://docs.microsoft.com/en-us/learn/modules/manage-deployments-advanced-arm-template-features/>



900 XP

Introduction to Azure virtual machines

1 hr 7 min • Module • 8 Units

[Feedback](#)[Beginner](#) [Administrator](#) [Developer](#) [Solution Architect](#) [Student](#) [Azure](#) [Azure Virtual Machines](#)

Learn about the decisions you make before creating a virtual machine, the options to create and manage the VM, and the extensions and services you use to manage your VM.

Learning objectives

In this module, you will:

- Compile a checklist for creating a virtual machine
- Describe the options to create and manage virtual machines
- Describe the additional services available to administer virtual machines

[Start >](#) [⊕ Add](#)

Prerequisites

None

This module is part of these learning paths

Рис. 1.1 Портал з першим модулем лабораторної роботи

Практичні дії виконуються у спеціальному середовищі sandbox (рис. 1.2).

This module requires a sandbox to complete. A **sandbox** gives you access to Azure resources. Your Azure subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Due to the impact of the global health pandemic, Azure resources are being prioritized towards health and safety organizations. You may experience some issues when you deploy resources used in the exercises. Please try again or choose a different region. For more information, see Azure blog post - [Update #3: Business continuity with Azure](#).

[Activate sandbox](#)

Рис. 1.2. Сторінка переходу до віртуального середовища виконання лабораторної роботи

Для всіх лабораторних робіт використовувати один обліковий запис. Звіт (єдиний файл) створювати згідно рекомендацій у розділі «Пояснення до виконання».

При захисті роботи продемонструвати обліковий запис на порталі Microsoft і результати проходження модулів лабораторної роботи.

1.1 Контрольні питання

1. С чого складається список підготовчих операцій (checklist) при створенні віртуальної машини (VM) в хмарі?

2. Що в Azure забезпечує приватне підключення між віртуальними машинами Azure та іншими службами Azure?
3. Що потрібно вказати під час налаштування віртуальної мережі в Azure?
4. Що забезпечує безпеку в мережі користувача в Azure?
5. Які етапи інвентаризації потрібно виконати при міграції сервера в хмару?
6. Які рекомендації існують для створення імені віртуального сервера в Azure?
7. Що таке Azure resource? Які є ресурси?
8. Які є особливості розміщення при створення VM?
9. Для чого призначені *VM sizes* в Azure і чим визначається їх вибір користувачем?
10. На які типові навантаження розраховані VM в хмарі Azure?
11. Чи можлива зміна конфігурації VM після її створення? Що відбувається з VM після зміни конфігурації і які помилки можуть при цьому виникати?
12. Як виконується тарифікація під час роботи VM в Azure?
13. Які етапи необхідні для відкриття портів VM?
14. Що таке група безпеки мережі?
15. Що входить до правила групи безпеки мережі?
16. Які правила діють (пріоритет і порядок) вхідного та вихідного трафіку з урахуванням мережевого інтерфейсу і підмережі?
17. Яке останнє правило в групі безпеки мережі?
18. Які є варіанти обміну даними між ресурсами Azure?
19. Які є варіанти з'єднання локальної і хмарної мережі?
20. Яка область видимості адрес віртуальної мережі в хмарі Azure?
21. Команда Azure CLI для створення групи ресурсів.
22. Команда Azure CLI для підключення до Azure.
23. Команда Azure CLI для створення VM в Azure.
24. Що таке VPN-шлюз? Скільки їх потрібно і з яким ресурсом він пов'язаний?
25. Які фактори необхідно врахувати при створенні VPN-шлюза?
26. У чому різниця вивільнення і зупинки VM? Коли застосовується вивільнення?

27. Які передумови зміни розміру диску VM і як цей розмір стає доступним в гостьовій VM?
28. Що таке доступність VM і як вона вимірюється?
29. Що відбувається в разі відмови в роботі VM?
30. Яке призначення ресурсу availability set?
31. У чому різниця Fault Domain і Update Domain?
32. На які диски розповсюджується вплив Fault Domain?
33. Як захистити користувача VM від збоїв на сайті?
34. У чому різниця між технологіями HA та FT?
35. Які є можливості Backup as a Service в Azure?
36. Які ресурси створюються і необхідні для VM?
37. Скільки дисків створюється для VM за замовченням, де вони зберігаються і яке їх призначення?
38. Який максимальний розмір диска доступний для VM?
39. Як можливо мігрувати дані фізичного диска в хмару?
40. Які переваги надає керований (managed) диск?
41. Чи необхідний обліковий запис зберігання для керованого (managed) диску?
42. У чому різниця між RDP і SSH?
43. Яку технологію використовують для підключення локальної мережі до віртуальної мережі Azure?
44. Які зміни можуть бути з публічною адресою VM?
45. Які операції необхідні з диском користувача для VM після його створення?
46. Які є варіанти оплати за виконання обчислень у VM?
47. Що надає обліковий запис сховища і який він може бути?
48. Як пов'язаний обліковий запис сховища з кожним диском з точки зору управління?
49. Як ліцензуються гостьові ОС VM?
50. Що необхідно створити перед створенням VM і чому?
51. Чи можливо одразу відкрити порт при створенні VM?
52. Які адреси надаються VM після її створення?
53. Які є варіанти створення і управління ресурсами в Azure?

- 54.Для чого використовуються шаблони в Azure, як вони оформлені і як їх отримати?
- 55.Де ще, крім порталу Azure, можливо застосувати шаблони?
- 56.Що таке командлети і де вони виконуються?
- 57.Напишіть командлет для створення VM.
- 58.У чому різниця Azure Powershell і Azure CLI?
- 59.Для чого призначені Azure REST API і Azure Client SDK?
- 60.Для чого призначені Azure VM extensions?
- 61.Яке призначення SLA?

2 Комплекс лабораторних робіт «Побудова інфраструктури з використанням хмарних послуг AWS, що реалізують обчислення, сховища та мережі»

Комплекс робіт дозволяє студентам навчитися працювати зі службами, які реалізують інфраструктурні компоненти, а саме з обчисленнями, сховищами та мережами, включаючи Amazon EC2, Elastic Block Store, AWS Lambda і Amazon Virtual Private Cloud (VPC).

Для виконання роботи потрібен обліковий запис AWS Academy. Для його отримання необхідно з початку заповнити анкету.

<https://forms.office.com/r/ZNUHMMiXhF>

Для виконання комплексу лабораторних робіт перейти за посиланням, яке надійде від AWS Academy і зареєструватися на порталі AWS (латинськими літерами) (рис. 2.1).

The screenshot shows the AWS Educate registration form. At the top, the AWS Educate logo is displayed with the text "Apply to join AWS Educate". Below this is a blue banner with the text "Step 2/3: Tell us about yourself". The form contains several input fields: "School or Institution Name" (with a dropdown arrow and a hint to start typing the name), "Country" (with a dropdown arrow), "First Name", "Last Name", "Graduation Month" (with a dropdown arrow), "Graduation Year" (with a dropdown arrow), "Birth Month" (with a dropdown arrow), "Birth Year" (with a dropdown arrow), and "Promo Code (optional)". There are also "Pre" and "En" buttons in the top right corner.

Рис. 2.1. Реєстрація для подальшого виконання лабораторних робіт з AWS

Вказати National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” і термін навчання (graduation month – 07, graduation year – 2025).

Комплекс складається з 5 модулів:

1. Launching an EC2 Instance and attaching an EBS volume;
2. Creating an S3 Bucket;
3. Introduction to IAM;
4. Building the Amazon Virtual Private Cloud (85 хв);
5. Introduction to AWS Lambda (45 хв).

Практичні дії виконуються безпосередньо на порталі AWS Academy у вікні Management Console.

Для всіх лабораторних робіт використовувати один обліковий запис. Зробити скріншоти ключових дій при виконанні кожного модулю лабораторної роботи, та сформулювати звіт згідно рекомендацій у розділі «Пояснення до виконання».

2.1 Access the AWS Management Console

1. To start the lab session, choose **Start Lab** in the upper-right corner of the page.
 - The lab session starts.
 - A timer displays in the upper-right corner of the page and shows the time remaining in the session.

Tip: To refresh the session length at any time, choose **Start Lab** again before the timer reaches 0:00.

2. Before continuing, wait until the lab environment is ready. The environment is ready when the page and the circle icon next to the **AWS** link in the upper-left corner turns green.
3. To connect to the AWS Management Console, choose the **AWS** link in the upper-left corner, above the terminal window.

A new browser tab opens and connects you to the AWS Management Console.

Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with the message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and then choose **Allow pop-ups**.

Note: You are using the console through the lab environment, so you are not incurring any actual costs. However, in the real world, when using a personal or business account to access the console, users incur charges for use of specific AWS services.

2.2 Module 1: Launching an EC2 instance and attaching an EBS volume

Lab overview

In this lab, you create an Amazon Elastic Compute Cloud (Amazon EC2) instance that hosts a simple website and then attach an Amazon Elastic Block Store (Amazon EBS) volume to it. “Yourname” must be changed to student’s first name and last name.

Duration

This lab requires approximately **30 minutes** to complete.

2.2.1 Task 1. Start creating the instance and assign a name

1. Choose the **Services** menu, locate the **Compute** services, and select **EC2**.
2. Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.
3. Name the instance:
 - Give it the name "Web Server 1 Yourname"

Tags help you categorize your AWS resources in different ways; for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags you have assigned to it. Each tag consists of a *key* and a *value*, which you define.

Note: *Name* is simply another tag. The *key* for this tag is *Name*, and the *value* is *Web Server 1 Yourname*.

2.2.2 Task 2. Application and OS Images

7. Choose an AMI from which to create the instance:
 - In the list of available *Quick Start* AMIs, keep the default **Amazon Linux** AMI selected.
 - Also keep the default **Amazon Linux 2023 AMI x86_64 (HVM)** selected.

The type of *Amazon Machine Image (AMI)* you choose determines the Operating System (OS) that will run on the EC2 instance that you launch. In this case, you have chosen Amazon Linux 2023 as the guest OS.

2.2.3 Task 3. Choose an instance type

8. Specify an Instance type:
 - In the *Instance type* panel, keep the default **t2.micro** selected.

The *Instance Type* defines the hardware resources assigned to the instance. This instance type has 1 virtual central processing unit (CPU) and 1 GiB of memory.

2.2.4 Task 4. Choose a key pair

9. Select the key pair to associate with the instance:
 - From the **Key pair name** menu, select **vockey**.

The *vockey* key pair you selected will allow you to connect to this instance via SSH after it has launched. Although you will not need to do that in this lab, it is still required to identify an existing key pair, or create a new one, when you launch an instance.

2.2.5 Task 5. Network settings

10. Next to Network settings, choose **Edit**.
11. Keep the default *VPC* and *subnet* settings. Also keep the **Auto-assign public IP** setting set to **Enable**.

The Network indicates the virtual private cloud (VPC) you want to launch the instance into. You can have multiple networks; for example, one for *development*, a second for *testing*, and a third for *production*.

12. Under *Firewall (security groups)*, keep the default **Create security group** option chosen.

13. Configure a new security group:

- Keep the default selection **Create a new security group**.
- **Security group name:** Clear the text and enter `Web Server of Yourname`
- **Description:** Clear the text and enter `Security group for Yourname's web server`
- Choose **Remove** to remove the default SSH inbound rule.

Note: You will configure a different inbound rule later in this lab.

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.

2.2.6 Task 6. Configure storage

14. In the *Configure storage* section, keep the default settings.

You will launch the Amazon EC2 instance using a default Elastic Block Store (EBS) disk volume. This will be your root volume (also known as a *boot volume*) which will host the Amazon Linux 2023 guest operating system that you specified earlier. It will run on a general purpose SSD (*gp2*) hard drive that is 8 GiB in size. You could alternatively add more storage volumes, however that is not needed in this lab.

2.2.7 Task 7. Advanced details

15. Configure a script to run on the instance when it launches:

- Expand the **Advanced details** panel.
- Scroll to the bottom of the page and then paste the bash script into the **User data** box. It will run automatically when the instance launches for the first time.

Create bash script that runs with root user permissions on the guest OS of the instance. ***Include the script into your report.*** This script must do the following:

- Updates the server
- Installs an Apache web server (httpd)
- Configures the web server to automatically start on boot
- Activates the web server
- Creates a simple webpage `Hello World from Yourname!`

2.2.8 Task 8. Review the instance and launch

16. At the bottom of the **Summary** panel on the right side of the screen choose Launch instance

You will see a Success message.

17. Choose View all instances

The instance will first appear in the *Pending* state, which means it is being launched. The state will then change to *Running*, which indicates that the instance has started booting. It takes a few minutes for the instance to boot.

18. Select the **Web Server 1 Yourname** instance, and review the information in the **Details** tab that displays in the lower pane. Include it into the report.

Notice that the instance has a **Public IPv4 address**. You can use this IP address to communicate with the instance from the internet.

19. Before you continue, wait for your instance to display the following:

- **Instance state:** *Running*
- **Status check:** *2/2 checks passed*

This may take a few minutes. Choose the refresh icon at the top of the page every 30 seconds or so to more quickly become aware of the latest status of the instance.

2.2.9 Task 9. Access your EC2 instance

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

20. From the **Details** tab, copy the **Public IPv4 address** value of your instance to your clipboard.

Note: A *public* address means that the instance can be reached from the internet. Each instance that receives a public IP address is also given an external DNS hostname; for example, `ec2-xxx-xxx-xxx-xxx.compute-1.amazonaws.com`. AWS resolves an external DNS hostname to the *public* IP address of the instance when communication comes from outside its VPC. When communication comes from inside its VPC, the DNS hostname is resolved to the *private* IPv4 address.

21. Open a new tab in your web browser, paste the public IP address you just copied, and press **Enter**. Include results into the report.

The webpage does not load. You must update the security group to be able to access the page.

2.2.10 Task 10. Update the security group

You are not 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. In this task, you update the security group.

22. Return to the **EC2 Management Console** browser tab.
23. In the left navigation pane, under **Network & Security**, choose **Security Groups**.
24. Select the **Web Server of Yourname** security group, which you created when launching your EC2 instance.
25. In the lower pane, choose the **Inbound rules** tab.

2.2.11 Task 11. Create an inbound rule

26. Choose **Edit inbound rules**, and then choose **Add rule**.
27. Configure the following:
 - **Type:** HTTP
 - **Source:** Anywhere-IPv4
 - Choose **Save rules**

The new inbound HTTP rule creates an entry for IPv4 IP (0.0.0.0/0) and IPv6 IP addresses (::/0).

2.2.12 Task 12. Test the rule

28. Return to the tab that you used to try to connect to the web server.
29. Refresh the page.

The page should display the message *Hello World from Yourname!*

2.2.13 Task 13. Attach an EBS volume to your EC2 instance

30. Return to the **EC2 Management Console** browser tab.
31. In the left navigation pane, under **Instances**, choose **Instances**.
32. Select the **Web Server** instance, and in the **Networking** tab below, note the **Availability Zone** in which your instance is running.

The EBS volume you will soon create will need to be in the same Availability Zone.

33. In the left navigation pane, under **Elastic Block Store**, select **Volumes**.
34. Select **Create volume**.
35. For **Size**, enter 1 to create a volume with 1 GiB.
36. For **Availability Zone**, select the same Availability Zone that your EC2 instance is running in.
37. Scroll down and select **Create volume**.

The new volume appears in the volumes list with a state of *available*.

38. Select the new 1 GiB size volume. Then, choose **Actions**, and **Attach volume**.
39. Select the **Instance** drop-down menu, and then select your EC2 instance. The list of instances will automatically populate.
40. Select **Attach volume**.

The state of the volume changes to *in-use*. The new volume is now attached to your EC2 instance.

Lab complete

Log out of the AWS Management Console.

- In the upper-right corner of the page, choose your user name. Your user name begins with **voclabs/user**.
- Choose **Sign out**.

Choose **End Lab** at the top of this page, and then select **Yes** to confirm that you want to end the lab.

2.3 Module 2: Creating an S3 bucket

Lab overview

Follow these steps to create an Amazon Simple Storage Service (Amazon S3) bucket to host a static website.

A *static website* is fixed and displays the same content for each user. In contrast, a *dynamic website* uses advanced programming to provide user interaction and display different content depending on the user's selections. “Yourname” must be changed to student’s first name and last name.

Duration

This lab requires approximately **30 minutes** to complete.

2.3.1 Task 1. Create an S3 bucket

1. Choose the **Services** menu, locate the **Storage** services, and select **S3**.
2. Select **Create bucket** on the right side of the page.
3. For **Bucket name**, enter a unique Domain Name System (DNS)-compliant name for your new bucket.

Follow these naming guidelines:

- The name must be unique across all existing bucket names in Amazon S3.
 - The name must only contain lowercase characters.
 - The name must contain **Yourname**
 - The name must start with a letter or number.
 - The name must be between 3 and 63 characters long.
 - After you create the bucket, you cannot change the name, so choose wisely.
 - Choose a bucket name that reflects the objects in the bucket. This is because the bucket name is visible in the URL that points to the objects that you’re going to put in your bucket.
4. For **Region**, choose the AWS Region where you want the bucket to reside.

Choose a Region close to you to minimize latency and costs, or to address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region.

5. Uncheck the **Block all public access** box because you want to be able to test if the website is working.

A warning message similar to **Turning off block all public access might result in this bucket and the objects within becoming public** appears below the security setting you deselected.

6. Below the warning, check the box next to **I acknowledge that....**
7. Scroll to the bottom of the page, and select **Create bucket**.

Your new bucket appears in the **Buckets** list.

2.3.2 Task 2. Add a bucket policy to make the content publicly available

11. Choose the link for your bucket's name, and then select the **Permissions** tab.
12. In the **Bucket policy** section, choose **Edit**.
13. To grant public read access for your website, create the bucket policy, and paste it in the policy editor.
14. In the policy, use the name of your bucket.
15. Select **Save changes**.

2.3.3 Task 3. Upload an HTML document

In this task, you upload an HTML document to your new bucket.

16. Create index.html with your short description (Name, University, Faculty, Group).
17. Save the index.html file to your local computer.
18. In the console, choose the **Objects** tab.
19. Upload the index.html file to your bucket.
 - Choose **Upload**.
 - Drag and drop the index.html file onto the upload page.
 - As an alternative, choose **Add files**, navigate to the file, and choose **Open**.
20. Expand the **Properties** section.

This section lists the storage classes that are available in Amazon S3. You will learn more about storage classes later, but take a minute to review them now.

Ensure that the **Standard** storage class is selected.

21. At the bottom of the page, choose **Upload**.
22. Choose **Close**.

The index.html file appears in the **Objects** list.

2.3.4 Task 4. Test your website

26. Select the **Properties** tab, and scroll down to the **Static website hosting** section.
27. Choose **Edit**.
28. Select **Enable**.
29. In the **Index document** text box, enter `index.html`
30. Select **Save changes**.
31. Scroll down to the **Static website hosting** section again, and copy the **Bucket website endpoint** URL to your clipboard.
32. Open a new tab in your web browser, paste the URL you just copied, and press **Enter**.

Your webpage should display. You have successfully hosted a static website using an S3 bucket!

Lab complete

Log out of the AWS Management Console.

- In the upper-right corner of the page, choose your user name. Your user name begins with **voclabs/user**.
- Choose **Sign Out**.

Choose **End Lab** at the top of this page, and then select **Yes** to confirm that you want to end the lab.

2.4 Module 3: Introduction to IAM

Lab overview

In this lab, you will explore users, groups, and policies in the AWS Identity and Access Management (IAM) service. “Yourname” must be changed to student’s first name and last name.

Duration

This lab requires approximately **40 minutes** to complete.

2.4.1 Task 1. Explore the users and groups

In this task, you will explore the users and groups that have already been created for you in IAM.

1. First, note the Region that you are in; for example, **N. Virginia**. The Region is displayed in the upper-right corner of the console page.

You might need this information later in the lab.

2. Choose the **Services** menu, locate the **Security, Identity, & Compliance** services, and choose **IAM**.
3. In the navigation pane on the left, choose **Users**.

Create the following IAM users:

- user-1 ;
 - user-2
 - user-3
4. The users are assigned a **Console password** to allow them to access the AWS Management Console. They do not have any permissions and are not a member of any groups.
 5. In the navigation pane on the left, choose **User groups**.

Create the following groups:

- EC2-Admin
 - EC2-Support
 - S3-Support
6. Choose the name of the **EC2-Support** group.

This brings you to the summary page for the **EC2-Support** group.

7. Choose the **Permissions** tab.

Assign the group **EC2-Support** a managed policy called **AmazonEC2ReadOnlyAccess**. Managed policies are prebuilt policies (built either by AWS or by your administrators) that can be attached to IAM users and groups. When the policy is updated, the changes to the policy are immediately applied against all users and groups that are attached to the policy.

8. Under **Policy Name**, choose the link for the **AmazonEC2ReadOnlyAccess** policy.
9. Choose the **{ JSON }** tab.
 - A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to *List* and *Describe* (view) information about Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, Amazon CloudWatch, and Amazon EC2 Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a support role.
 - Statements in an IAM policy have the following basic structure:
 - **Effect** says whether to *Allow* or *Deny* the permissions.
 - **Action** specifies the API calls that can be made against an AWS service (for example, *cloudwatch:ListMetrics*).

- **Resource** defines the scope of entities covered by the policy rule (for example, a specific Amazon Simple Storage Service [Amazon S3] bucket or Amazon EC2 instance; an asterisk [*] means *any resource*).

10. In the navigation pane on the left, choose **User groups**.
11. Choose the name of the **S3-Support** group.
12. Choose the **Permissions** tab.

Assign the group **S3-Support** the **AmazonS3ReadOnlyAccess** policy.

13. Under **Policy Name**, choose the link for the **AmazonS3ReadOnlyAccess** policy.
14. Choose the **{}** **JSON** tab.

This policy has permissions to *Get* and *List* for *all* resources in Amazon S3.

15. In the navigation pane on the left, choose **User groups**.
16. Choose the name of the **EC2-Admin** group.
17. Choose the **Permissions** tab.

This group is different from the other two. Instead of a managed policy, assign the group an *inline policy*, which is a policy assigned to just one user or group. Inline policies are typically used to apply permissions for specific situations.

18. Under **Policy Name**, choose the name of the **EC2-Admin-Policy** policy.
19. Choose the **JSON** tab.

This policy grants permission to *Describe* information about Amazon EC2 instances, and also the ability to *Start* and *Stop* instances.

2.4.2 Business scenario

For the remainder of this lab, you will work with these users and groups to enable permissions that support the following business scenario.

Your company is growing its use of AWS services, and is using many Amazon EC2 instances and Amazon S3 buckets. You want to give access to new staff depending upon their job function, as indicated in the following table:

User	In Group	Permissions
user-1	S3-Support	Read-only access to Amazon S3
user-2	EC2-Support	Read-only access to Amazon EC2
user-3	EC2-Admin	View, Start, and Stop Amazon EC2 instances

2.4.3 Task 2. Add users to groups

You have recently hired *user-1* into a role where they will provide support for Amazon S3. You will add them to the *S3-Support* group so that they inherit the necessary permissions via the attached *AmazonS3ReadOnlyAccess* policy.

Ignore any "not authorized" errors that appear during this task. They are caused by your lab account having limited permissions and will not impact your ability to complete the lab.

Add user-1 to the S3-Support group

26. In the left navigation pane, choose **User groups**.

27. Choose the name of the **S3-Support** group.
28. On the **Users** tab, choose **Add users**.
29. Select **user-1**, and choose **Add users**.

On the **Users** tab, notice that *user-1* has been added to the group.

Add user-2 to the EC2-Support group

You have hired *user-2* into a role where they will provide support for Amazon EC2. You will add them to the *EC2-Support* group so that they inherit the necessary permissions via the attached *AmazonEC2ReadOnlyAccess* policy.

30. Use what you learned from the previous steps to add *user-2* to the *EC2-Support* group.

user-2 should now be part of the *EC2-Support* group.

Add user-3 to the EC2-Admin group

You have hired *user-3* as your Amazon EC2 administrator to manage your EC2 instances. You will add them to the *EC2-Admin* group so that they inherit the necessary permissions via the attached *EC2-Admin-Policy*.

31. Use what you learned from the previous steps to add *user-3* to the *EC2-Admin* group.

user-3 should now be part of the *EC2-Admin* group.

32. In the navigation pane on the left, choose **User groups**.

Each group should have a **1** in the **Users** column. This indicates the number of users in each group.

If you do not have a **1** for the **Users** column for a group, revisit the previous steps to ensure that each user is assigned to a group, as shown in the table in the **Business scenario** section.

2.4.4 Task 3. Sign in and test users

In this task, you will test the permissions of each IAM user in the console.

Get the console sign-in URL

33. In the navigation pane on the left, choose **Dashboard**.

Notice the **Sign-in URL for IAM users in this account** section at the top of the page. The sign-in URL looks similar to the following:

<https://123456789012.signin.aws.amazon.com/console>

This link can be used to sign in to the AWS account that you are currently using.

34. Copy the sign-in link to a text editor.

Test user-1 permissions

35. Open a private or incognito window in your browser.

36. Paste the sign-in link into the private browser, and press ENTER.

You will now sign-in as *user-1*, who has been hired as your Amazon S3 storage support staff.

37. Sign in with the following credentials:

- **IAM user name:** `user-1`
- **Password:** `Lab-Password1`

38. Choose the **Services** menu, and choose **S3**.

39. Choose the name of one of your buckets, and browse the contents.

Because this user is part of the *S3-Support* group in IAM, they have permissions to view a list of Amazon S3 buckets and their contents.

Now, test whether the user has access to Amazon EC2.

40. Choose the **Services** menu, and choose **EC2**.

41. In the left navigation pane, choose **Instances**.

You cannot see any instances. Instead, an error message says *you are not authorized to perform this operation*. This user has not been assigned any permissions to use Amazon EC2.

You will now sign in as *user-2*, who has been hired as your Amazon EC2 support person.

42. First, sign out *user-1* from the console:

- In the upper-right corner of the page, choose **user-1**.
- Choose **Sign Out**.

Test user-2 permissions

43. Paste the sign-in link into the private browser again, and press ENTER.

44. Sign in with the following credentials:

- **IAM user name:** `user-2`
- **Password:** `Lab-Password2`

45. Choose the **Services** menu, and choose **EC2**.

46. In the navigation pane on the left, choose **Instances**.

- You are now able to see an EC2 instance. However, you cannot make any changes to Amazon EC2 resources because you have read-only permissions.
- If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, **N. Virginia**).

47. Select the EC2 instance.

48. Choose the **Instance state** menu, and then choose **Stop instance**.

49. To confirm that you want to stop the instance, choose **Stop**.

An error message appears and says that *You are not authorized to perform this operation*. This demonstrates that the policy only allows you to view information without making changes.

Next, check if *user-2* can access Amazon S3.

50. Choose the **Services** menu, and choose **S3**.

An error message says *You don't have permissions to list buckets* because *user-2* does not have permissions to use Amazon S3.

You will now sign-in as *user-3*, who has been hired as your Amazon EC2 administrator.

51. First, sign out *user-2* from the console:
 - In the upper-right corner of the page, choose **user-2**.
 - Choose **Sign Out**.

Test user-3 permissions

52. Paste the sign-in link into the private browser again, and press ENTER.
53. Sign in with the following credentials:
 - **IAM user name:** *user-3*
 - **Password:** *Lab-Password3*
54. Choose the **Services** menu, and choose **EC2**.
55. In the navigation pane on the left, choose **Instances**.
 - An EC2 instance is listed. As an Amazon EC2 Administrator, this user should have permissions to *Stop* the EC2 instance.
 - If you cannot see an EC2 instance, then your Region might be incorrect. In the upper-right corner of the page, choose the Region name, and then choose the Region that you were in at the beginning of the lab (for example, **N. Virginia**).
56. Select the EC2 instance.
57. Choose the **Instance state** menu, and then choose **Stop instance**.
58. To confirm that you want to stop the instance, choose **Stop**.

This time, the action is successful because *user-3* has permissions to stop EC2 instances. The **Instance state** changes to *Stopping* and starts to shut down.

59. Close your private browser window.

2.4.5 Lab complete

Log out of the AWS Management Console.

- In the upper-right corner of the page, choose your user name. Your user name begins with **voclabs/user**.
- Choose **Sign Out**.

Choose **End Lab** at the top of this page, and then select **Yes** to confirm that you want to end the lab.

2.5 Module 4: Building the Amazon Virtual Private Cloud

In this lab, you will create a basic virtual private cloud (VPC) without using the VPC Wizard. The VPC that you build will include a web server and an Amazon RDS database. Once you have created both, you will connect your address book application running on your web server to your Amazon RDS for MySQL instance. Once you have successfully configured your address book application with your RDS instance, you will be able to add and remove contacts from the address book.

Topics covered

In this lab you will manually:

- Create an Amazon Virtual Private Cloud (VPC)
- Create a public and private subnets
- Create an Internet gateway
- Create a Route Table and added a route to the Internet
- Create a security group for your web server to only allow HTTP traffic to your web server
- Create a security group for your MySQL RDS instance to only allow MySQL traffic from your public subnets
- Deploy a web server and a MySQL RDS instance
- Configure your application to connect to your MySQL RDS instance

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

2.5.1 Create a VPC

In this task, you will create a base VPC.

A virtual private cloud is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC by modifying its IP address range, create subnets, and configure route tables, network gateways, and security settings.

3. In the **AWS Management Console**, on the **Services** menu, click **VPC**.

If you see **New VPC Experience** at the top-left of your screen, ensure **New VPC Experience** is selected. This lab is designed to use the new VPC Console.

4. In the left navigation pane, click **Your VPCs**.
5. Click **Create VPC** then configure:
 - **Name tag:** *"Your Last Name" VPC*
 - **IPv4 CIDR block:** *10.x.0.0/16*
 - Click **Create VPC**,

where "Your Last Name" is yours and x is a variant number.

2.5.2 Create Your Public Subnets

In this task, you will create two public subnets. Each subnet will reside in a separate availability group. Later in the lab, you will launch your web server into one of the public subnets.

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.

Create Your First Public Subnet

6. In the left navigation pane, click **Subnets**.
7. Click **Create subnet** then configure:
 - **VPC ID:** *"Your Last Name" VPC*
 - **Subnet name:** *Public 1 "Your Last Name"*
 - **Availability Zone:** Select the *first* AZ in the list
 - **IPv4 CIDR block:** *10.x.1.0/24*
 - Click **Create subnet**
8. Select **Public 1 "Your Last Name"**.
9. In the **Actions** menu, select **Modify auto-assign IP settings**, then configure:
 - Select **Enable auto-assign public IPv4 address**
 - Click **Save**

Enable auto-assign public IPv4 address provides a public IPv4 address for all instances launched into the selected subnet.

Create Your Second Public Subnet

10. Click **Create subnet** then configure:
 - **VPC ID:** *"Your Last Name" VPC*
 - **Subnet name:** *Public 2 "Your Last Name"*
 - **Availability Zone:** Select the *second* AZ in the list
 - **IPv4 CIDR block:** *10.x.2.0/24*
 - Click **Create subnet**
11. Select **Public 2 "Your Last Name"**.
12. In the **Actions** menu, select **Modify auto-assign IP settings**, then configure:
 - Select **Enable auto-assign public IPv4 address**
 - Click **Save**

Even though your subnets are labeled **Public 1 "Your Last Name"** and **Public 2 "Your Last Name"**, they are not yet public subnets. A public subnet must have an Internet Gateway, which you will attach in the next task.

2.5.3 Create an Internet Gateway

In this task, you will create an Internet gateway so that traffic can access your web server.

An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

An Internet gateway serves two purposes: to provide a target in your VPC route tables for Internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

13. In the left navigation pane, click **Internet Gateways**.

14. Click **Create internet gateway** then configure:

- **Name tag:** *"Your Last Name" IG*
- Click **Create internet gateway**

15. In the **Actions** menu, select **Attach to VPC**, then configure:

- **Available VPCs:** *"Your Last Name" VPC*
- Click **Attach internet gateway**

This will attach the Internet gateway to your VPC. Even though you created an Internet gateway and attached it to your VPC, you still have to tell instances within your public subnet how to get to the Internet.

2.5.4 Create a Route Table, Add Routes, And Associate Public Subnets

In this task, you will:

- Create a route table for internet-bound traffic;
- Add a route to the route table to direct Internet-bound traffic to your Internet gateway;
- Associate your public subnets with your route table.

A route table contains a set of rules, called routes, that are used to determine where network traffic is directed. Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

To use an Internet gateway, your subnet's route table must contain a route that directs Internet-bound traffic to the Internet gateway. You can scope the route to all destinations not explicitly known to the route table (0.0.0.0/0 for IPv4 or ::/0 for IPv6), or you can scope the route to a narrower range of IP addresses; for example, the public IPv4 addresses of your company's public endpoints outside of AWS, or the Elastic IP addresses of other Amazon EC2 instances outside your VPC. If your subnet is

associated with a route table that has a route to an Internet gateway, it's known as a public subnet.

16. In the left navigation pane, click **Route Tables**.

There is currently one default route table associated with the VPC, “**Your Last Name**” VPC. This routes traffic locally. You will now create an additional Route Table to route public traffic to your Internet Gateway.

17. Click **Create route table**.

18. Under **Route table settings** section then configure:

- **Name - optional:** *Public Route Table*
- **VPC:** “*Your Last Name*” VPC
- Click **Create route table**

19. Click the **Routes** tab in the lower half of the page.

Notice that there is one route in your route table that allows traffic within the 10.0.0.0/16 network to flow within the network, but it does not route traffic outside of the network. You will now add a new route to enable public traffic.

20. Click **Edit routes**

21. Click **Add route** then configure:

- **Destination:** 0.0.0.0/0
- **Target:** Select **Internet Gateway** in the drop down and then select the displayed **Internet Gateway id**
- Click **Save changes**

22. Click the **Subnet associations** tab.

23. Under section **Explicit subnet associations**, click **Edit subnet associations**

24. Select **Public 1 “Your Last Name”** and **Public 2 “Your Last Name”**.

25. Click **Save associations**

The two subnets are now *public* because they connect to the Internet via the Internet Gateway.

2.5.5 Create a Security Group for your Web Server

In this task, you will add a security group so that users can access your web server via HTTP.

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC could be assigned to a different

set of security groups. If you do not specify a particular group at launch time, the instance is automatically assigned to the default security group for the VPC.

26. In the left navigation pane, click **Security Groups**.

27. Click **Create security group** then configure:

- **Security group name:** *Web server “Your Last Name”*
- **Description:** *“Your Last Name” Web Server Security Group*
- **VPC:** *“Your Last Name” VPC*

28. Under **Inbound rules**

- Click **Add rule**
- **Type:** HTTP
- **Source:** *Anywhere*

29. At the bottom of the screen, click **Create security group**

In the next task you will launch your web server into one of your public subnets.

2.5.6 Launch a Web Server in your Public Subnet

In this task, you will launch a web server that runs an address book application. Later in the lab, you will connect your address book application to a Amazon RDS for MySQL instance.

30. On the **Services** menu, click **EC2**.

If you see **New EC2 Experience** at the top-left of your screen, ensure **New EC2 Experience** is selected. This lab is designed to use the new EC2 Console.

31. Click **Launch instance** > **Launch instance**.

32. On **Step 1**, click **Select** next to **Amazon Linux 2 AMI**.

You will launch a t2.micro instance. This instance type has 1 vCPU and 1 GiB of memory.

33. On **Step 2**, click **Next: Configure Instance Details**

34. On **Step 3**, configure:

- **Network:** *“Your Last Name” VPC*
- Expand **Advanced Details** (at the bottom of the page)
- Copy and paste this script into the **User data** text box:

```
#!/bin/bash -ex
yum -y update
yum -y install httpd php mysql php-mysql
chkconfig httpd on
```

```
service httpd start
cd /var/www/html
wget https://s3-us-west-2.amazonaws.com/us-west-2-aws-training/awsu-spl/spl-13/scripts/app.tgz
tar xvfz app.tgz
chown apache:root /var/www/html/rds.conf.php
```

This script is run the first time the instance is launched. It installs a web server on your EC2 instance, and runs an app that can be configured to point to your MySQL RDS instance. After you configure your RDS instance, it will present an address book that you can edit.

Ознайомитись зі складом параметрів конфігурування параметрів ВМ (стадія 3).

35. Click **Next: Add Storage** (За замовченням)

36. On **Step 4**, click **Next: Add Tags**

37. On **Step 5**, click **Add Tag** then configure:

- **Key:** *Name*
- **Value:** *"Your Last Name" Web Server*

38. Click **Next: Configure Security Group**

39. Configure the following:

- Click **Select an existing security group**
- Select *"Your Last Name" Web Server*
- Click **Review and Launch**

40. At the **Warning** screen, click **Continue**

41. On **Step 7**, review the settings, then click **Launch**

42. On the **Select an existing key pair or create a new key pair** window, configure the following:

- Select **Proceed without a key pair**
- Select **I acknowledge that...**
- Click **Launch Instances**

43. Click **View Instances**

This brings you to the **Instances** window where you can watch your web server launch and view its details.

44. Wait for your web server to fully launch. It should display the following:

- **Instance State:** running

You can click the refresh icon to refresh your instances status.

45. Your instance should be selected if not, select it.


46. Copy the **Public IPv4 address** address of the instance to your clipboard.

47. Open a new web browser tab and paste the IP address into the browser.

48. Press **Enter** to go the web page.

If you receive an error, please wait 60 seconds and refresh the page to try again. It can take a couple of minutes for the EC2 instance to boot and run the script that installs software.

An application should appear ()

A screenshot of a web application interface. At the top left is the AWS logo. Below it, there are four input fields labeled 'Endpoint', 'Database', 'Username', and 'Password'. Each field is a white rectangle with a light gray border. Below the 'Password' field is a 'Submit' button, which is a small white rectangle with a light gray border and the text 'Submit' in the center.

Currently, you do not have a database. Once you create your RDS instance, you will be able to connect it to your web server.

2.5.7 Create Private Subnets for your MySQL Server

To deploy your RDS database, your VPC must have at least one subnet in at least two Availability Zones in the region where you want to deploy your DB instance. In this task, you will create two private subnets for your Amazon RDS instance.

Create Your First Private Subnet

49. In the **AWS Management Console**, on the **Services** menu, click **VPC**.

50. In the left navigation pane, click **Subnets**.

51. Click **Create subnet** then configure:

- **VPC:** *“Your Last Name” VPC*
- **Subnet name:** *Private 1 “Your Last Name”*
- **Availability Zone:** Select the *first* AZ in the list
- **IPv4 CIDR block:** 10.x.3.0/24
- Click **Create subnet**

Create Your Second Private Subnet

52. Click **Create subnet** then configure:

- **VPC:** *“Your Last Name” VPC*
- **Subnet name:** *Private 2 “Your Last Name”*
- **Availability Zone:** Select the second AZ in the list
- **IPv4 CIDR block:** 10.x.4.0/24
- Click **Create subnet**

2.5.8 Create a Security Group for your Database Server

Now that your private subnets are configured, you will want to secure the types of traffic that can access your MySQL database. In this task, you will create a security group to only allow MySQL traffic from your Web server.

53. In the left navigation pane, click **Security Groups**.

54. Copy the **Security group ID** value of your *Web server* security group and paste it into your text editor.

Next you will create a security group that will allow your *Web server* to communicate with your database.

55. Click **Create security group** then configure:

- **Security group name:** *Database “Your Last Name”*
- **Description:** *“Your Last Name” Database Security Group*
- **VPC:** *“Your Last Name” VPC*

56. Under **Inbound rules**

- Click **Add rule**
- **Type:** MySQL/Aurora
- **Source:**
 - *Custom*
 - Paste the web server security group ID that you copied to your text editor

57. At the bottom of the screen, click **Create security group**

This will allow your web server to communicate with the database.

2.5.9 Create a Database Subnet Group

Amazon RDS instances require a database subnet group. In this task, you will create a database subnet group.

A DB subnet group is a collection of subnets (typically private) that you create in a VPC and that you then designate for your DB instances. Each DB subnet group should have subnets in at least two Availability Zones in a given region. When creating a DB instance in a VPC, you must select a DB subnet group.

58. On the **Services** menu, click **RDS**.

59. In the left navigation pane, click **Subnet groups**.

60. Click **Create DB Subnet Group** then configure:

- **Name:** *"Your Last Name" Subnet Group*
- **Description:** *"Your Last Name" Subnet Group*
- **VPC:** *"Your Last Name" VPC*

Add Your Private Subnets

61. In the **Add subnets** section, configure the following:

- **Availability zone:** Select the first and second Availability Zones in the list.

62. In the **Subnets** section, select:

- *10.x.3.0/24*
- *10.x.4.0/24*

63. At the bottom of the screen, click **Create**

2.5.10 Create an Amazon RDS Database

You are now ready to launch an Amazon RDS database running MySQL.

64. In the left navigation pane, click **Databases**.

65. Click **Create database** then configure:

- **Engine options:** *MySQL*
- **Version:** *MySQL 5.7.31*

It is very important to select version 5.7.31. This lab requires it for the application.

66. In the *Templates* section, select **Dev/Test**.

67. In the **Settings** section, configure:

- **DB instance identifier:** *"Your Last Name"DB*
- **Master username:** admin
- **Master password:** lab-password
- **Confirm password:** lab-password

68. In the **DB instance class** section, configure:

- **DB instance class:** *Burstable classes*
- Select **db.t2.small**

69. In the **Storage** section, de-select **Enable storage autoscaling**

70. In the **Connectivity** section, configure:

- **Virtual Private Cloud (VPC)** “*Your Last Name*” VPC
- **Publicly access:** *No*
- **Existing VPC security groups:**
 - Add the **Database** security group
 - Remove the **default** security group

71. In the **Additional configuration** section, click **Additional configuration**, then configure:

- **Initial database name:** “*Your Last Name*”DB
- De-select **Enable automatic backups** This will turn off backups, which will launch the database a little bit quicker for your lab.
- De-select **Enable Enhanced monitoring**
- De-select **Enable auto minor version upgrade**

72. At the bottom of the screen, click **Create database**

73. Click refresh every 60 seconds until the instance has a status of **available**.

You have deployed a MySQL database.

2.5.11 Connect Your Address Book Application to Your Database

In this task, you will connect the address book application (in your Public subnet) to your database (in your Private subnet).

Obtain Your MySQL Database Endpoint

Before you can connect your address book application to your database, you need to know the *endpoint* of the RDS instance. This is the address of your RDS instance.

74. Click your **mydb** instance.

75. In the **Connectivity & security** section, copy the **Endpoint** to your clipboard.

Your RDS endpoint should look similar to:

mydb.ciljcs3yv1rb.us-west-2.rds.amazonaws.com

Connect to Your Database

76. Return to the browser tab that is displaying your web server, then configure:

- **Endpoint:** Paste your MySQL endpoint
- **Database:** “*Your Last Name*”DB
- **Username:** sdmin
- **Password:** lab-password
- Click **Submit**

Once connected, you should see an address book with two entries.

You have successfully connected your address book application to your database.

77. Try adding and then removing a contact from the address book.



The screenshot shows a web application titled "Address Book". It features a table with columns: Last name, First name, Phone, Email, and Admin. There are two rows of contact data. Above the table is a link "Add Contact". Each row in the table has "Edit" and "Remove" links in the Admin column.

Last name	First name	Phone	Email	Admin
				Add Contact
Doe	Jane	010-110-1101	janed@someotheraddress.org	Edit Remove
Johnson	Roberto	123-456-7890	roberto@someaddress.com	Edit Remove

The address book information is saved in the Amazon RDS for MySQL database.

2.5.12 Conclusion

Додаткові посилання.

VPC

Introduction

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

Route

Tables

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

Security

Groups

for

Your

VPC

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

Internet

Gateways

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Internet_Gateway.html

2.6 Module 5: Introduction to AWS Lambda

The lab provides a basic explanation of AWS Lambda. It will demonstrate the steps required to get started to create a Lambda function in an event-driven environment.

AWS Lambda is a compute service that runs your code in response to events and automatically manages the compute resources for you, making it easy to build applications that respond quickly to new information. AWS Lambda starts running your code within milliseconds of an event such as an image upload, in-app activity, website click, or output from a connected device. You can also use AWS Lambda to create new back-end services where compute resources are automatically triggered based on custom requests.

By the end of this lab you will be able to:

- Create an AWS Lambda function;
- Configure an Amazon S3 bucket as a Lambda Event Source;

- Trigger a Lambda function by uploading an object to Amazon S3;
- Monitor AWS Lambda S3 functions through Amazon CloudWatch Log.

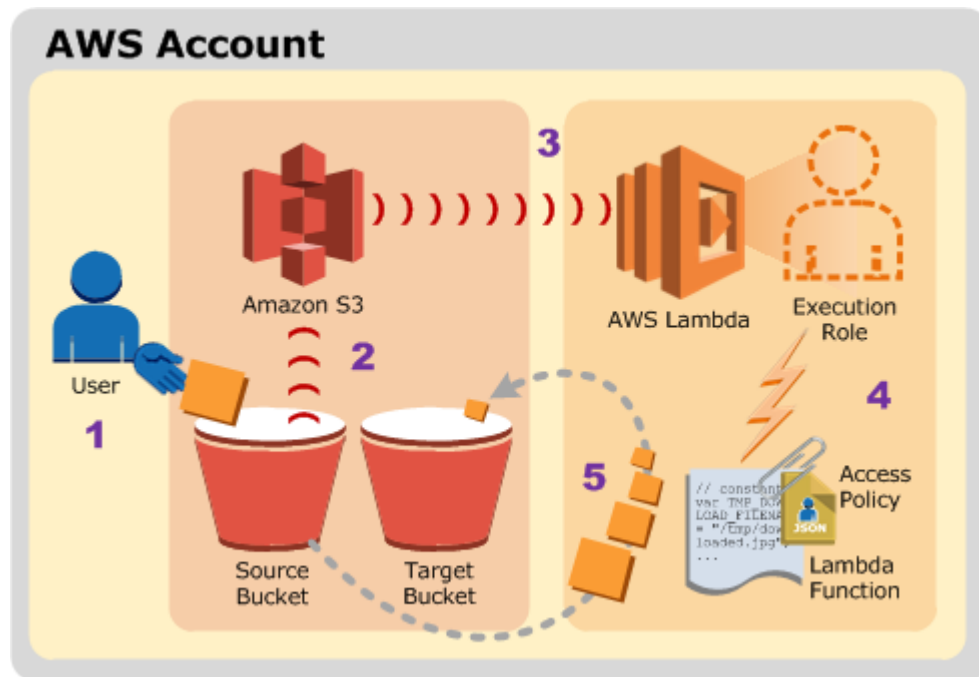
Prerequisites:

Familiarity with Amazon S3 would be beneficial.

2.6.1 Scenario

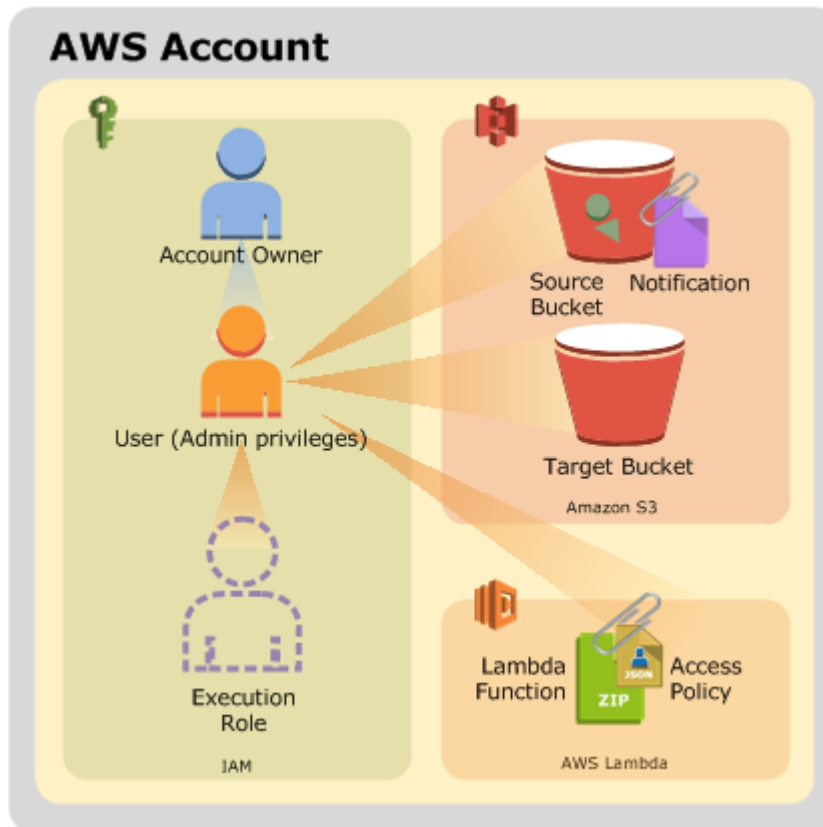
This lab demonstrates AWS Lambda by creating a serverless image thumbnail application.

The following diagram illustrates the application flow:



- 1 A user uploads an object to the source bucket in Amazon S3 (object-created event).
- 2 Amazon S3 detects the object-created event.
- 3 Amazon S3 publishes the object-created event to AWS Lambda by invoking the Lambda function and passing event data as a function parameter.
- 4 AWS Lambda executes the Lambda function.
- 5 From the event data it receives, the Lambda function knows the source bucket name and object key name. The Lambda function reads the object and creates a thumbnail using graphics libraries, then saves the thumbnail to the target bucket.

Upon completing this tutorial, you will have the following resources in your account:



The steps in this lab will show you how to create the Amazon S3 buckets and the Lambda function. You will then test the service by uploading images for resizing.

2.6.2 Create the Amazon S3 Buckets

In this task, you will create two Amazon S3 buckets -- one for input and one for output.

In the AWS Management Console, on the Services menu, click S3.

If you see a message at the top of the screen that says We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console., click Switch to the new console.

In the AWS Management Console, on the Services menu, click S3.

Click Create bucket and then configure:

Amazon S3 buckets require unique names, so you will add a random number to the bucket name such as images-xyz.

1. Bucket name: images-xyz

Replace xyz with a number of your student ticket

- Copy the name of your bucket to a text editor
 - Click **Create bucket**
4. Scroll to the bottom of the screen to click **Create bucket** leaving the rest of the options as default.

6. You will now create another bucket for output. Click **Create bucket** with similar steps as the previous bucket, now configure:

- Bucket name: Paste the name of your images bucket
- At the end of the bucket name, append *-resized*
- Click **Create bucket**

Do not change the Region.

You should now have buckets named similar to: images-xyz images-xyz-resized

8. You will now upload a picture for testing purposes.

- Choose the photo of your student ticket with high resolution (1280 x 853 or more).
- Save it locally using filename HappyFace.jpg.

10. In the S3 Management Console, click the images- bucket. (Not the -resized bucket)

11. Click Upload

12. In the Upload window, click Add files

13. Browse to and select the HappyFace.jpg picture you downloaded.

14. Click Upload

Later in this lab you will invoke the Lambda function manually by passing sample event data to the function. The sample data will refer to this HappyFace.jpg image.

2.6.3 Create an AWS Lambda Function

In this task, you will create an AWS Lambda function that reads the photo from Amazon S3, resizes the photo and then stores the new photo in Amazon S3.

- On the **Services** menu, click Lambda.

Do not change the Region. (In case of errors, you can use US West (Oregon) for this lab.)

11. Click **Create function**

Blueprints are code templates for writing Lambda functions. Blueprints are provided for standard Lambda triggers such as creating Alexa skills and processing Amazon Kinesis Firehose streams. This lab provides you with a pre-written Lambda function, so you will Author from scratch.

- Choose Author from scratch
- In the Create function window, configure:

13. Function name: *"Your Last Name"*
14. Runtime: Python 3.7
15. Expand Change default execution role
16. Execution role: Select Use an existing role
17. Existing role: Choose lambda-execution-role

Make sure to select Python 3.7 under Other supported runtime. If you select Python 3.8 from Latest supported list, the code will fail.

This role grants permission to the Lambda function to access Amazon S3 to read and write the images.

- Click **Create function**

A page will be displayed with your function configuration.

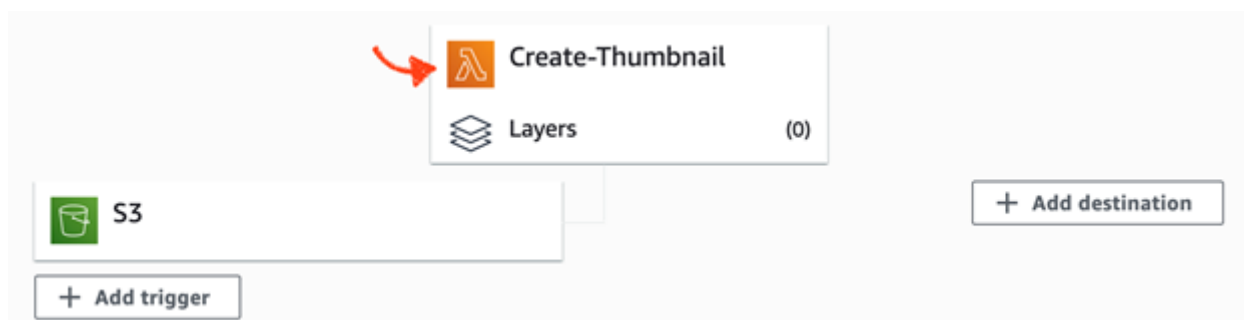
AWS Lambda functions can be triggered automatically by activities such as data being received by Amazon Kinesis or data being updated in an Amazon DynamoDB database. For this lab, you will trigger the Lambda function whenever a new object is created in your Amazon S3 bucket.

15. Click **Add trigger** then configure:

- Select a trigger: S3
- Bucket: Select your images- bucket (e.g. images-xyz)
- Event type: All object create events
- For Recursive invocation, Select I acknowledge that ...

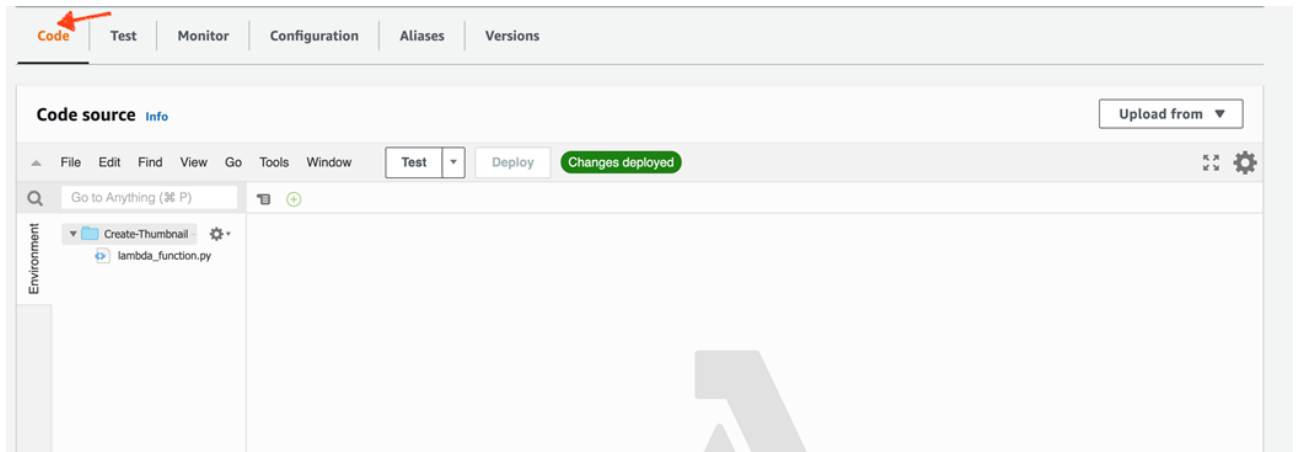
16. Scroll to the bottom of the screen, then click **Add**

17. Expand Function overview and click Create-Thumbnail at the top of the diagram (as shown below):



You will now configure the Lambda function.

- Click Code as shown below:



- Configure the following settings (and ignore any settings that aren't listed):

17. Click Upload from menu and select Amazon S3 location

18. Amazon S3 link URL: Copy and paste this URL into the field:

<https://s3-us-west-2.amazonaws.com/us-west-2-aws-training/awsu-spl/spl-88/2.3.15.prod/scripts/CreateThumbnail.zip>

19. Click **Save**

The CreateThumbnail.zip file contains the following Lambda function:

This code is showing what is in the Zip file.

```
import boto3
import os
import sys
import uuid
from PIL import Image
import PIL.Image

s3_client = boto3.client('s3')

def resize_image(image_path, resized_path):
    with Image.open(image_path) as image:
        image.thumbnail((128, 128))
        image.save(resized_path)

def handler(event, context):
    for record in event['Records']:
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']
        download_path = '/tmp/{}'.format(uuid.uuid4(), key)
        upload_path = '/tmp/resized-{}'.format(key)
```

```
s3_client.download_file(bucket, key, download_path)
resize_image(download_path, upload_path)
s3_client.upload_file(upload_path, '{}-resized'.format(bucket), key)
```

- Examine the above code. It is performing the following steps:

20. Receives an Event, which contains the name of the incoming object (Bucket, Key)

21. Downloads the image to local storage

22. Resizes the image using the Pillow library

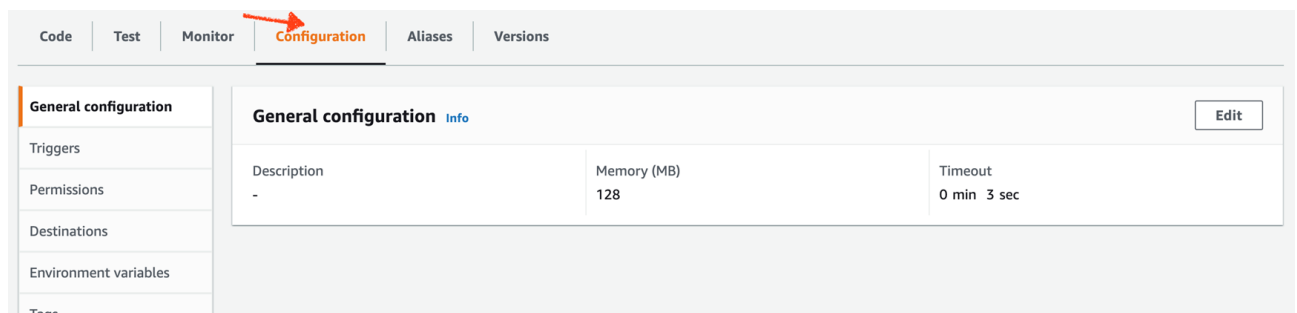
23. Uploads the resized image to the -resized bucket

22. In the Runtime settings section, click [Edit](#)

- Handler enter: CreateThumbnail.handler
- Click [Save](#)

Make sure you set the Handler field to the above value, otherwise the Lambda function will not be found.

26. Click Configuration as shown below:



28. Click General configuration, click [Edit](#)

- Description enter: Create a thumbnail-sized image of “*Your Last Name*”

You will leave the other settings as default, but here is a brief explanation of these settings:

29. Memory defines the resources that will be allocated to your function. Increasing memory also increases CPU allocated to the function.

30. Timeout sets the maximum duration for function execution.

31. Click [Save](#)

Your Lambda function has now been configured.

2.6.4 Test Your Function

In this task, you will test your Lambda function. This is done by simulating an event with the same information normally sent from Amazon S3 when a new object is uploaded.

- Click Test
- In the Test event section, click New event and then configure:

30.Template: Amazon S3 Put

31.Name: Upload

A sample template will be displayed that shows the event data sent to a Lambda function when it is triggered by an upload into Amazon S3. You will need to edit the bucket name so that it uses the bucket you created earlier.

31.Replace example-bucket with the name of your images bucket (e.g. images-xyz) that you copied to your text editor.

Be sure to replace example-bucket in both locations.

```

1 {
2   "Records": [
3     {
4       "eventVersion": "2.0",
5       "eventSource": "aws:s3",
6       "awsRegion": "us-west-2",
7       "eventTime": "1970-01-01T00:00:00.000Z",
8       "eventName": "ObjectCreated:Put",
9       "userIdentity": {
10        "principalId": "EXAMPLE"
11      },
12      "requestParameters": {
13        "sourceIPAddress": "127.0.0.1"
14      },
15      "responseElements": {
16        "x-amz-request-id": "EXAMPLE123456789",
17        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/mnopqrstuvwxyzABCDEFGH"
18      },
19      "s3": {
20        "s3SchemaVersion": "1.0",
21        "configurationId": "testConfigRule",
22        "bucket": {
23          "name": "images-234531245234",
24          "ownerIdentity": {
25            "principalId": "EXAMPLE"
26          },
27          "arn": "arn:aws:s3:::images-234531245234"
28        },
29        "object": {
30          "key": "test/key",

```

33.Replace test/key with the name of the picture that you uploaded. This should be **HappyFace.jpg**


```
1 {  
2   "Records": [  
3     {  
4       "eventVersion": "2.0",  
5       "eventSource": "aws:s3",  
6       "awsRegion": "us-west-2",  
7       "eventTime": "1970-01-01T00:00:00.000Z",  
8       "eventName": "ObjectCreated:Put",  
9       "userIdentity": {  
10        "principalId": "EXAMPLE"  
11      },  
12      "requestParameters": {  
13        "sourceIPAddress": "127.0.0.1"  
14      },  
15      "responseElements": {  
16        "x-amz-request-id": "EXAMPLE123456789",  
17        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/mnopqrstuvwxyzABCDEFGH"  
18      },  
19      "s3": {  
20        "s3SchemaVersion": "1.0",  
21        "configurationId": "testConfigRule",  
22        "bucket": {  
23          "name": "images-234531245234",  
24          "ownerIdentity": {  
25            "principalId": "EXAMPLE"  
26          },  
27          "arn": "arn:aws:s3:::images-234531245234"  
28        },  
29        "object": {  
30          "key": "HappyFace.jpg",
```

35. Click **Test**

AWS Lambda will now trigger your function, using HappyFace.jpg as the input image.

Towards the top of the page you should see the message: Execution result: succeeded

Result returned by your function will show as null.

If your test did not succeed, the error message will explain the cause of failure.

For example, a Forbidden message means that the image was not found possibly due to an incorrect bucket name. Review the previous steps to confirm that you have configured the function correctly.

- Click Details to expand it (towards the top of the screen).

You will be shown information including:

- 38. Execution duration
- 39. Resources configured
- 40. Maximum memory used
- 41. Log output

You can now view the resized image that was stored in Amazon S3.

- On the **Services** menu, click S3.
- Click the name of your **-resized** bucket (which is the second bucket you created), then:

40. Select HappyFace.jpg

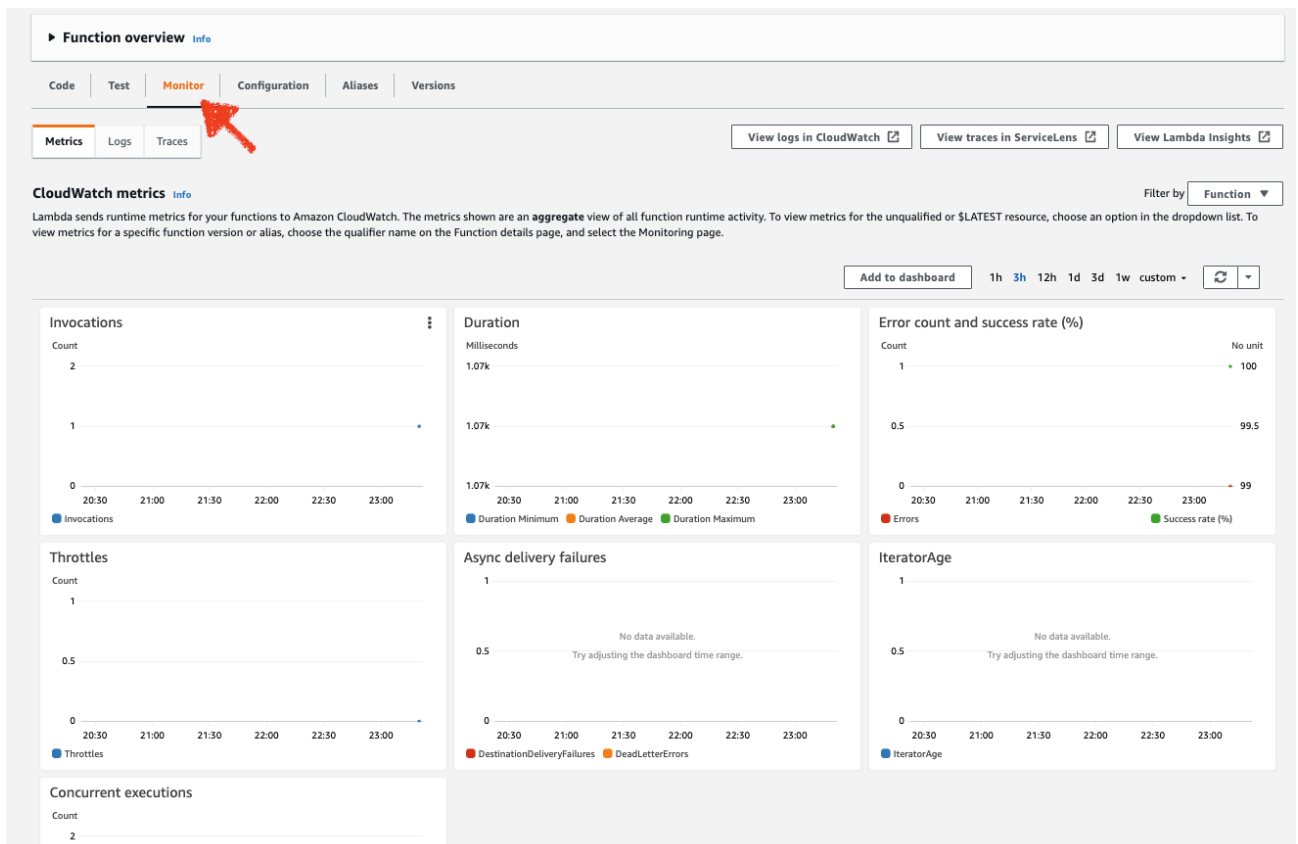
41. Click Actions menu and select Open (If the image does not open, disable your pop-up blocker.)

The image should now be a smaller thumbnail of the original image.

2.6.5 Monitoring and Logging

You can monitor AWS Lambda functions to identify problems and view log files to assist in debugging.

- On the **Services** menu, click Lambda.
- Click your Create-Thumbnail function.
- Click the Monitor tab as shown below:



The console displays graphs showing:

43. Invocations: The number of times that the function was invoked.

44. Duration: The average, minimum, and maximum execution times.

45. Error count and success rate (%): The number of errors and the percentage of executions that completed without error.

46. Throttles: When too many functions are invoked simultaneously, they will be throttled. The default is 1000 concurrent executions.

47. Async delivery failures: The number of errors that occurred when Lambda attempted to write to a destination or dead-letter queue.

48. Iterator Age: Measures the age of the last record processed from streaming triggers (Amazon Kinesis and Amazon DynamoDB Streams).

49. Concurrent executions: The number of function instances that are processing events.

Log messages from Lambda functions are retained in Amazon CloudWatch Logs.

- Click [View logs in CloudWatch](#)
- Click the Log Stream that appears.
- Expand each message to view the log message details.

The Event Data includes the Request Id, the duration (in milliseconds), the billed duration (rounded up to the nearest 100 ms, the Memory Size of the function and the Maximum Memory that the function used. In addition, any logging messages or print statements from the functions are displayed in the logs. This assists in debugging Lambda functions.

2.6.6 Conclusion

AWS Lambda documentation <https://aws.amazon.com/documentation/lambda/>

2.7 Контрольні питання

Що таке S3, призначення?

Яка модель надання хмарних послуг використовується S3 та EBS?
<https://aws.amazon.com/what-is/iaas/>

Для чого використовується S3 Versioning?

Для чого використовується S3 Snapshot?

Яка файлова система використовується у сховищі S3?

Яка команда призначена для копіювання файлу в кошик?

Яка команда призначена для перегляду кошика?

Чи використовується VM в першому модулі? Для чого?

Що таке S3, призначення?

Що таке EC2, призначення?

Якого типу сховище надає сервіс EBS та сервіс S3?

Що таке IOPS?

Чим IOPS відрізняється від Throughput?

Для чого використовується EBS Versioning?

Чи використовували ви VM в модулі VPC?

Для чого використовується Internet Gateway?

Чи використовували ви у VPC для БД окрему VM?

В чому перевага AWS Lambda? Яка модель надання хмарних послуг?

Яка модель надання хмарних послуг використовується EC2?

Як тарифікується робота AWS Lambda?

3 Комплекс лабораторних робіт «Основи створення віртуалізованих середовищ на базі продуктів VMware, Virtualization 101»

Для виконання комплексу лабораторних робіт треба перейти за посиланням і зареєструватися на порталі (рис. 3.1) <https://www.vmwarelearningplatform.com/HOL/catalogs/catalog/1212>
Знайти на порталі (рис. 3.2) лабораторну роботу Virtualization 101 (таблиця 3.1) і виконати модулі в її складі.

Рис. 3.1. Реєстрація на порталі "Hands-on Labs Online portal"

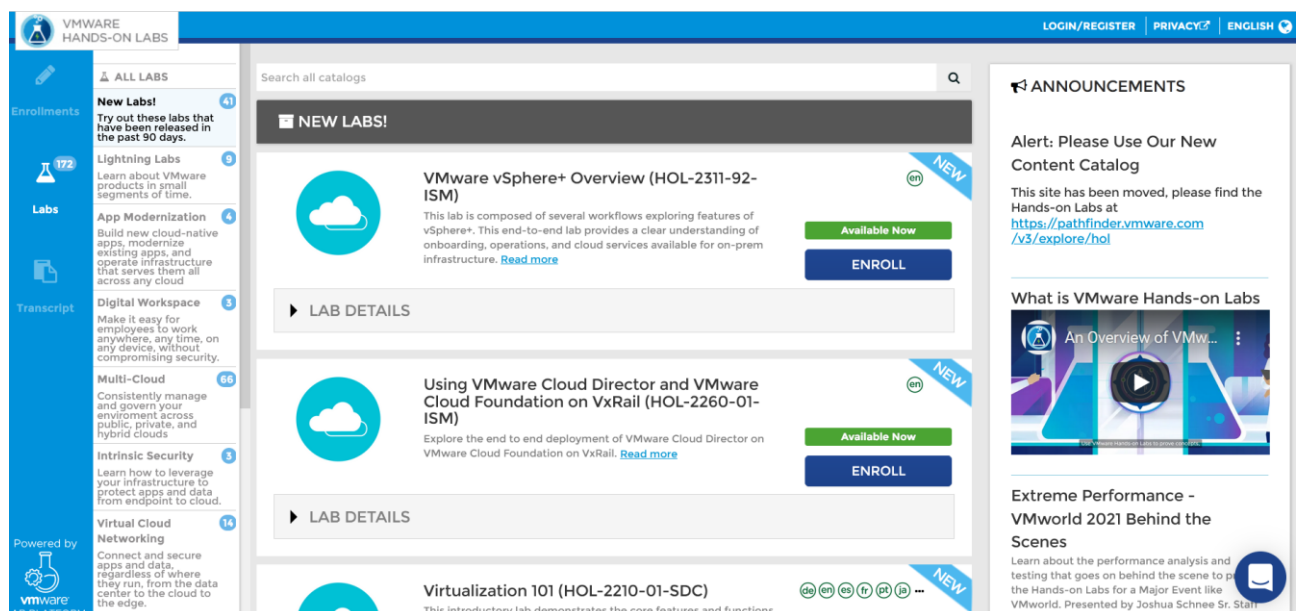


Рис. 3.2. Початкова сторінка portalу "Hands-on Labs Online portal"

У звіт вносити основні, суттєві для розуміння роботи, етапи виконання згідно рекомендацій у розділі «Пояснення до виконання».

Таблиця 3.1. Перелік лабораторних, що входять у комплекс

№	Код	Назва	Рівень	Час, хв.
1.	HOL-2410-01-SDC	Virtualization 101	Beginning	180

Таблиця 3.2 містить зміст роботи HOL-2210-01-SDC (модулі).

Таблиця 3.2. Зміст роботи HOL-2410-01-SDC

#	Virtualization 101	Час, хв.	Рівень
1	Introduction to Management with vCenter Server	60	B
2	Introduction to vSphere Networking And Security	60	B
3	Introduction to vSphere Storage	60	B

Початок роботи з віртуальним середовищем лабораторної роботи «Virtualization 101» показаний на рис. 3.3.

HOL-2410-01-SDC

Virtualization 101 (HOL-2410-01-SDC)

This introductory lab demonstrates the core features and functions of vSphere and vCenter. This is an excellent place to begin your experience with VMware vSphere.

This lab is available in [English](#), [简体中文](#), [日本語](#), [한국어](#), [Français](#), [Deutsch](#), [Português](#), [Español](#)

Lab Modules

#	HOL-2410-01-SDC	Time	Level
1	Introduction to Management with vCenter Server	60	B
2	Introduction to vSphere Networking and Security	60	B
3	Introduction to vSphere Storage	60	B

A **Module Time** can be either 15, 30, 45 or 60 Minutes in Length.
A **Module Level** can be either Beginning or Advanced.

[Close](#)

[Available Now](#)

[ENROLL](#)

[LAB DETAILS](#)

Рис. 3.3. Навігація по лабораторних роботах

При першому вході в лабораторну роботу рекомендується ознайомитися з елементами віртуального середовища (рис. 3.4)

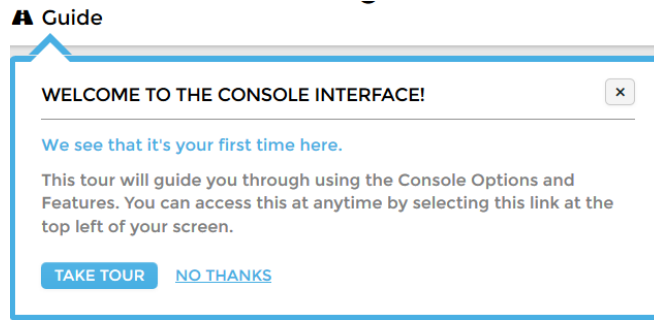


Рис. 3.4. Елементи віртуального середовища порталу "Hands-on Labs Online portal"

Виконати дії, вказані у покроковому керівництві у правій частині екрану (рис. 3.5), зробити скріншоти ключових дій при виконанні кожного модулю лабораторної роботи з комплексу, та сформуванати звіт згідно рекомендацій у розділі «Пояснення до виконання». Керівництво для виконання роботи також доступне у вигляді PDF http://docs.hol.vmware.com/HOL-2024/hol-2410-01-sdc_pdf_en.pdf.

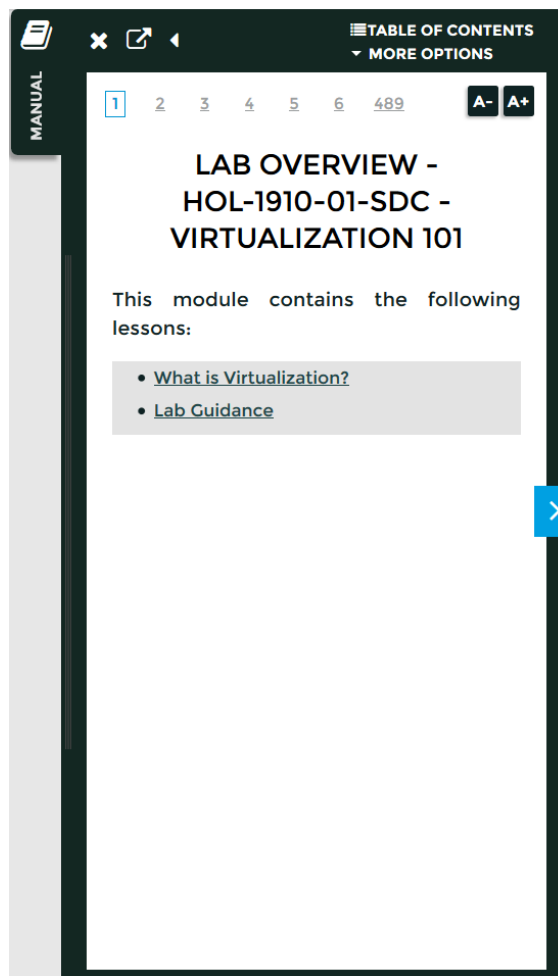


Рис. 3.5. Покрокові інструкції для виконання лабораторної роботи

Наприклад, лабораторна робота «Virtualization 101» містить три модулі: Introduction to Management with vCenter Server, Introduction to vSphere Networking And Security, An Introduction to vSphere Storage. У кожному модулі є окреме, незалежне від інших модулів завдання для виконання.

Після проходження лабораторної роботи результати відображаються в розділі досягнень (рис. 3.6).



Рис. 3.6. Перелік виконаних лабораторних робіт на порталі

4 Комплекс лабораторних робіт «Сучасна мережа NSX та гіперконвергентна інфраструктура vSAN на базі VMware»

Знайти на порталі (рис. 3.2) лабораторні роботи (таблиця 4.1), і виконати їх, фіксуючи основні етапи виконання у звіт згідно рекомендацій у розділі «Пояснення до виконання».

Таблиця 4.1. Перелік лабораторних, що входять у комплекс

№	Код	Назва	Рівень	Час, хв.
1.	HOL-2425-01-NET	VMware NSX - Networking Fundamentals	Beginning, Intermediate	90
2.	HOL-2409-91-HCI	VMware vSAN - Quick Start with ESA	Beginning	30

Таблиця 4.2 містить перелік модулів до виконання.

Таблиця 4.2 Зміст роботи HOL-2425-01-NET

№	VMware NSX - Networking Fundamentals	Час, хв.	Рівень
1	Introduction to the NSX Network and Security Virtualization Platform	15	B
2	NSX Manager, Transport Nodes and Inventory Components	30	B
3	NSX Segments	15	I
4	NSX Routing	30	I
5	NSX Network Address Translation	30	I
6	NSX Distributed Firewall (DFW)	15	B
7	NSX Gateway Firewall	15	B

Робота VMware vSAN - Quick Start with ESA містить два модулі.

При першому вході у лабораторну роботу рекомендується ознайомитися з елементами віртуального середовища (рис. 4.1).

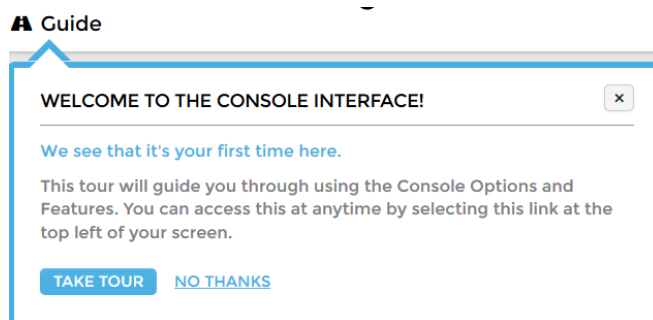


Рис. 4.1. Елементи віртуального середовища порталу "Hands-on Labs Online portal"

Виконати дії, вказані в покроковому керівництві в правій частині екрану, зробити скріншоти ключових дій при виконанні кожного модулю лабораторної

роботи з комплексу, та сформувати звіт згідно рекомендацій у розділі «Пояснення до виконання».

Топології мережі на знімках екрану вказати розбірливо. Імена за замовченням кластерів, шлюзів повинні бути змінені.

Керівництво для виконання робіт також доступне у вигляді PDF
http://docs.hol.vmware.com/HOL-2024/hol-2425-01-net_pdf_en.pdf та
http://docs.hol.vmware.com/HOL-2024/hol-2409-91-hci_pdf_en.pdf.

Кожний модуль має окреме, незалежне від інших модулів завдання для виконання.