

IT3061 – Massive Data Processing and Cloud Computing

Year 3, Semester 2

Practical Sheet 2



Amazon
EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. EC2 offers many options that enable you to build and run virtually any application.

Launching an EC2 instance

This practical describes the steps of launching a new Linux EC2 instance.

Steps to launch an instance:

Initiate instance launch

Step 1: Choose an Amazon Machine Image (AMI)

Step 2: Choose an Instance Type

Step 3: Configure Instance Details

Step 4: Add Storage

Step 5: Add Tags

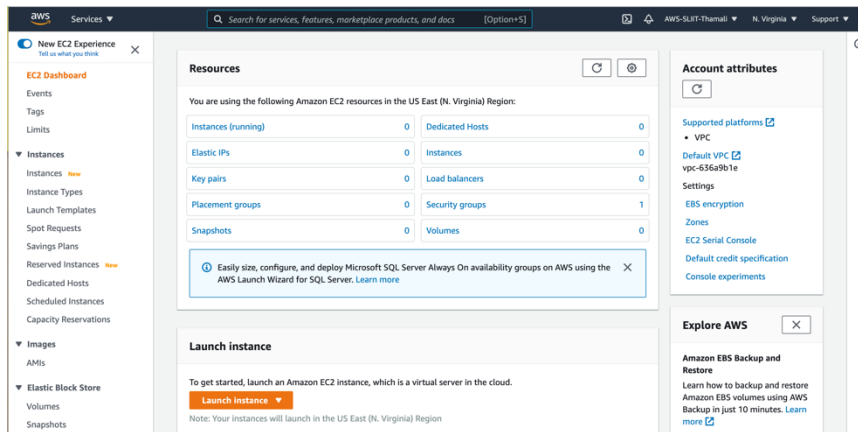
Step 6: Configure Security Group

Step 7: Review Instance Launch and Select Key Pair

- **Initiate instance launch**

Open the AWS Management console.

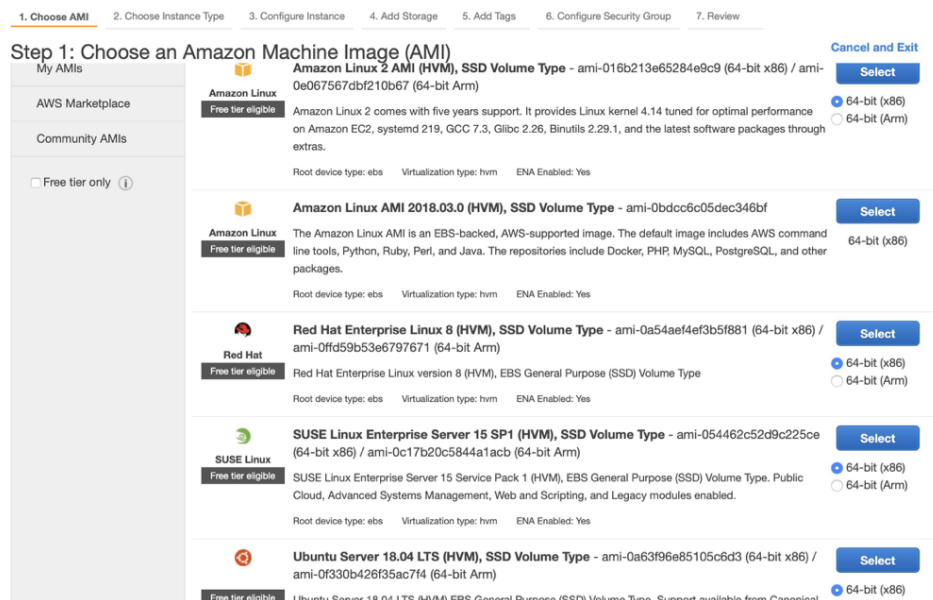
In the navigation bar at the top of the screen, the current Region is displayed. Select a Region for the instance that meets your needs. This choice is important because some Amazon EC2 resources can be shared between regions, while others can't.



From the Amazon EC2 console dashboard, choose **Launch instance**.

- **Step 1: Choose an Amazon Machine Image (AMI)**

Select a pre-configured Amazon Machine Image (AMI) to quickly start a VM. If not, you can create your own AMI using an existing EC2 instance and reuse to create custom instances.



- **Step 2: Choose an Instance Type**

Select the instance type you wish to create. You are able to select a range of instance types with different resource configurations based on your requirement.

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

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

• Step 3: Configure Instance Details

Set network level configurations you need (assign public/private IP, select the network, VPC etc).

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

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-0c05ba5fbaeb63d5c | SLIIT-VPC1 Create new VPC

Subnet subnet-0794813b53cce6e5b | SLIIT-SUBNET-1 | 251 IP Addresses available Create new subnet

Auto-assign Public IP Enable

Placement group ☐ Add instance to placement group

Capacity Reservation Open Create new Capacity Reservation

IAM role None Create new IAM role

Shutdown behavior Stop

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

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring Additional charges apply.

Tenancy Shared - Run a shared hardware instance Additional charges may apply when launching Dedicated instances.

Elastic Inference ☐ Add an Elastic Inference accelerator

Cancel Previous Review and Launch Next: Add Storage

• Step 4: Add Storage

Add storage, change size of storage based on your needs.

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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ①	Device ①	Snapshot ①	Size (GiB) ①	Volume Type ①	IOPS ①	Throughput (MB/s) ①	Delete on Termination ①	Encryption ①
Root	/dev/sda1	snap-021b833c41d050331	8	<div>General Purpose SSD (gp2) Provisioned IOPS SSD (io1) Magnetic (standard)</div>	10 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

- Step 5: Add Tags

Add naming tags to easily and properly identify the resources.

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

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ①	Volumes ①
Name	SLIIT-2020-EC2-1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Purpose	Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

- Step 6: Configure Security Group

Add the security group configurations to determine which protocols, ports and sources you wish to allow.

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

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group
☒ Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-03814fca7cff369e1	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-0a57bd7f9e77355c5	SLIIT-SG-1	To access my EC2 instance remotely	Copy to new

Inbound rules for sg-0a57bd7f9e77355c5 (Selected security groups: sg-0a57bd7f9e77355c5)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	:::0	
SSH	TCP	22	0.0.0.0/0	To allow access fr...
SSH	TCP	22	:::0	To allow access fr...

[Cancel](#) [Previous](#) [Review and Launch](#)

- **Step 7: Review Instance Launch and Select Key Pair**

When you are ready, select the acknowledgment check box, and then choose **Launch Instances**.

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

Step 7: Review Instance Launch

AMI Details [Edit AMI](#)

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0a63f96e85105c6d3

Free tier eligible Ubuntu Server 18.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).
Root Device Type: ebs

Instance Type [Edit instance type](#)

Instance Type EC2 Instance Profile t2.micro Variable Elastic Inference Accelerator

Security Groups [Edit security groups](#)

Security Group ID sg-0a57bd7f9e77355c5

All selected security groups

Type

HTTP

HTTP

SSH

SSH

TCP

TCP

22

22

0.0.0.0/0

:::0

To allow access fr...

To allow access fr...

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key** file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

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

Choose an existing key pair

Select a key pair

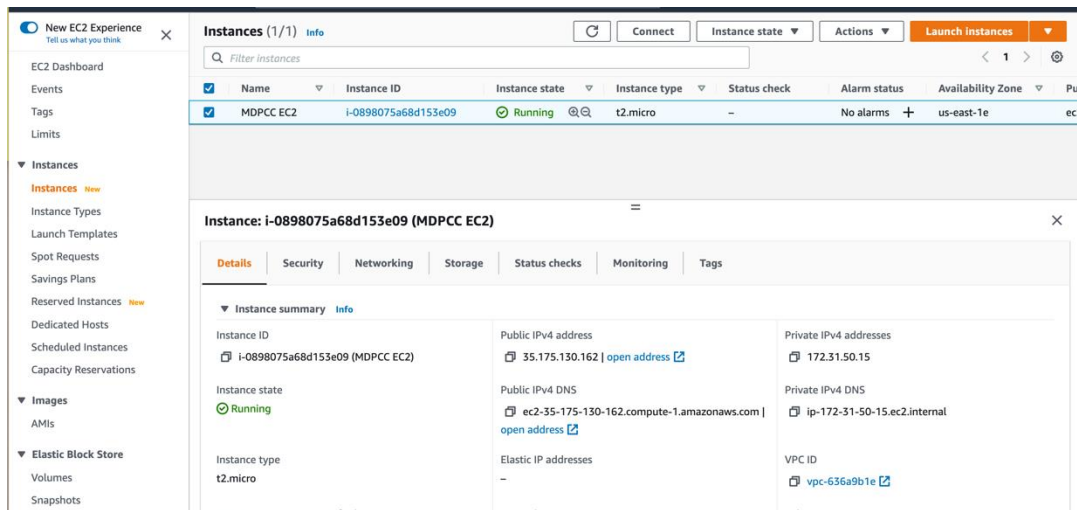
☒ I acknowledge that I have access to the selected private key file (SLIIT-DILAN-2020-07-19.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

[Cancel](#) [Previous](#) [Launch](#)

A confirmation page lets you know that your instance is launching. Choose **View Instances** to close the confirmation page and return to the console.

On the **Instances** page, you can view the status of your instance. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running, and it receives a public DNS name. (If the **Public DNS** column is hidden, choose the **Show/Hide** icon.)



Connect to Amazon EC2 Instance

Now that you have launched your EC2 instance, you can connect to it and use it the way that you'd use a computer sitting in front of you.

Following are the ways of connecting to a Linux instance:

- Connect from Windows using PuTTY
- Connect from Mac or Linux Using an SSH Client
- Connect Using Your Browser

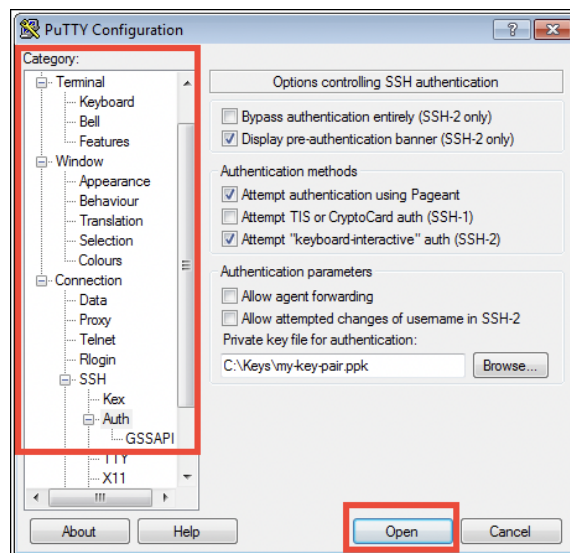
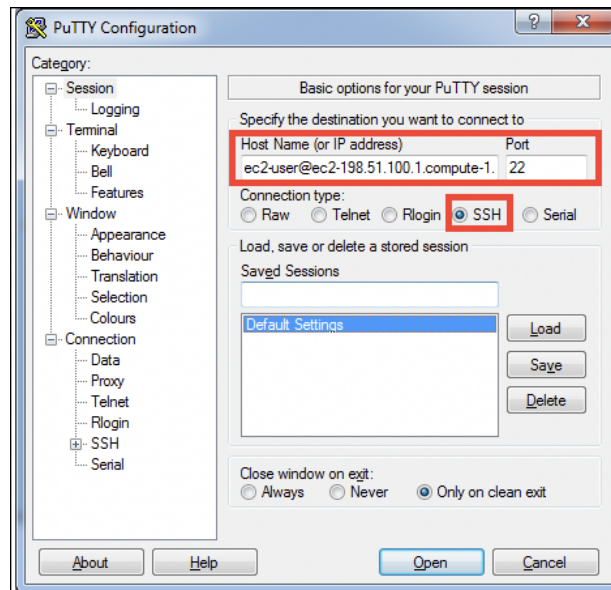
Connect from Windows using PuTTY

PuTTY uses .ppk files instead of .pem files.

To connect using PuTTY

1. On the **Start** menu, choose **All Programs, PuTTY, PuTTY**.
2. In the **Category** pane, choose **Session** and complete the following fields:
 - For **Host Name**, enter **ec2-user@public_dns_name**.
 - For **Connection type**, choose **SSH**.
 - For **Port**, ensure that the value is **22**.

3. In the **Category** pane, choose **Connection, SSH**, and **Auth**. Complete the following:
- Choose **Browse**, select the .ppk file that you generated for your key pair, and then choose **Open**.
 - Choose **Open** to start the PuTTY session.



4. If this is the first time you have connected to this instance, PuTTY displays a security alert dialog box that asks whether you trust the host you are connecting to. Choose **Yes**. A window opens and you are connected to your instance.



Microsoft Azure Virtual Machines is a web service which enables you to Provision Windows and Linux VMs in seconds and reduce costs. Azure virtual machines (VMs) can be created through the Azure portal. This method provides a browser-based user interface to create VMs and their associated resources.

Creating a Windows virtual machine in the Azure portal

This practical describes how to use the Azure portal to deploy a virtual machine (VM) in Azure that runs Windows Server 2019.

Steps

- **Create virtual machine**

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. Enter virtual machines in the search.
3. Under Services, select Virtual machines.
4. In the Virtual machines page, select Create and then Virtual machine. The Create a virtual machine page opens.
5. In the Basics tab, under Project details, make sure the correct subscription is selected and then choose to Create new resource group. Enter myResourceGroup for the name.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Pay-As-You-Go ▼

Resource group * ⓘ

(New) myResourceGroup ▼


Create new

Note - A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal>

6. Under Instance details, enter myVM for the Virtual machine name and choose Windows Server 2019 Datacenter - Gen2 for the Image. Leave the other defaults.


Instance details

Virtual machine name *	①	myVM	✓
Region *	①	(US) East US	▼
Availability options	①	No infrastructure redundancy required	▼
Security type	①	Standard	▼
Image *	①	 Windows Server 2019 Datacenter - Gen2	▼
See all images Configure VM generation			
Size *	①	Standard_E2s_v3 - 2 vcpus, 16 GiB memory (\$27.67/month)	▼
See all sizes			

7. Under Administrator account, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long and meet the defined complexity requirements.

Administrator account			
Username *	①	azureuser	✓
Password *	①	*****	✓
Confirm password *	①	*****	✓

8. Under Inbound port rules, choose Allow selected ports and then select RDP (3389) and HTTP (80) from the drop-down.

Inbound port rules	
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.	
Public inbound ports *	①
<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports	
Select inbound ports *	HTTP (80), RDP (3389) ▼
 This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.	

9. Leave the remaining defaults and then select the Review + create button at the bottom of the page.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing ☐ Windows Server license? * ⓘ

[Review Azure hybrid benefit compliance](#)

Review + create

< Previous

Next : Disks >

10. After validation runs, select the Create button at the bottom of the page.

11. After deployment is complete, select Go to resource.

^ Next steps

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

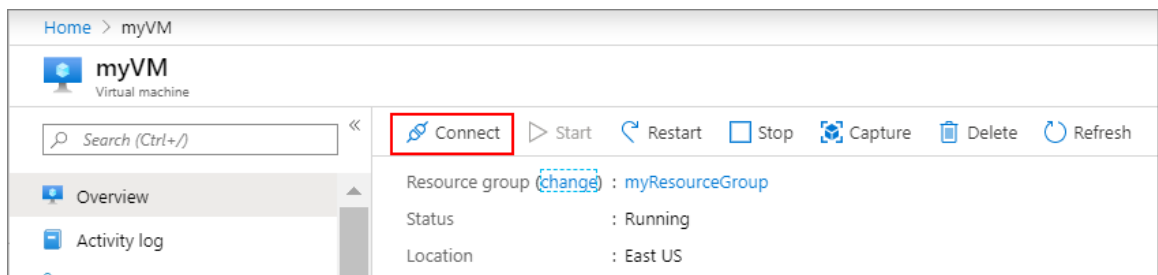
[Run a script inside the virtual machine](#) Recommended

Go to resource

Create another VM

- **Connect to virtual machine** - Create a remote desktop connection to the virtual machine.

1. On the overview page for your virtual machine, select the Connect > RDP.



2. In the Connect with RDP page, keep the default options to connect by IP address, over port 3389, and click Download RDP file.
3. Open the downloaded RDP file and click Connect when prompted.

4. In the Windows Security window, select More choices and then Use a different account. Type the username as localhost\username, enter the password you created for the virtual machine, and then click OK.
5. You may receive a certificate warning during the sign-in process. Click Yes or Continue to create the connection.

References

1. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html
2. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal>