

## AWS LAB

Create my Virtual Private Cloud (VPC) to produce customized network.

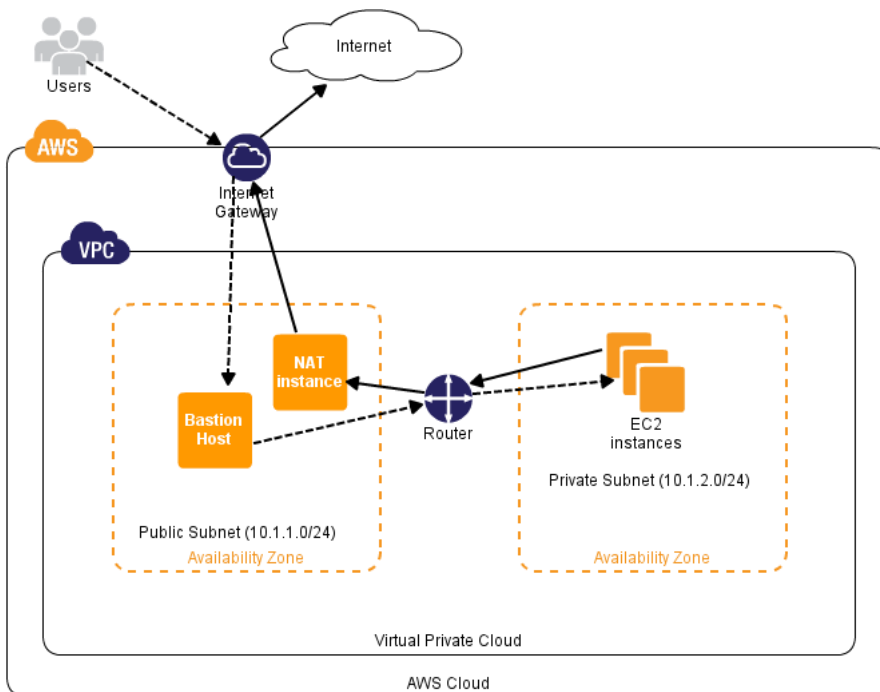
VPC will contain a Public Subnet and a Private Subnet, each subnet with 1 EC2 instance

Purpose: ping to google.com from the EC2 located in the Private Subnet

For this, a NAT instance configured in the public subnet is needed.

Private subnet traffic should be routed through the NAT instance for Internet access.

The IGW allows communication between instances in my VPC and Internet



Same figure with only one Availability zone

## AWS Console

- VPC -> Start VPC Wizard

Select VPC Configuration: VPC with Public and Private Subnets, in the same ZA

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block: 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block  
☐ Amazon provided IPv6 CIDR block

VPC name: ManuLab VPC

Public subnet's IPv4 CIDR: 10.0.0.0/24 (251 IP addresses available)

Availability Zone: eu-west-1a

Public subnet name: Public subnet

Private subnet's IPv4 CIDR: 10.0.1.0/24 (251 IP addresses available)

Availability Zone: eu-west-1a

Private subnet name: Private subnet

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT instance (Instance rates apply).

Instance type: t2.nano

Key pair name: soyris

Service endpoints

Add Endpoint

Enable DNS hostnames: ☒ Yes ☐ No

Hardware tenancy: Default

Running NAT Instance (This may take a few minutes)...

At this step, we have Manu\_VPC Lab created with the 2 Subnets: one Public, one Private

Create Subnet Subnet Actions

Search Subnets and their projects

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Route Table
		subnet-8590a2de	available	vpc-1d1dc17b	172.31.32.0/20	4091		eu-west-1c	rtb-3cca2845
		subnet-de65a196	available	vpc-d81cc0be   RosettaHUB VPC	172.30.1.0/24	250		eu-west-1b	rtb-20c92b59
		subnet-bc6da9f4	available	vpc-1d1dc17b	172.31.16.0/20	4091		eu-west-1b	rtb-3cca2845
		subnet-f49aa8af	available	vpc-d81cc0be   RosettaHUB VPC	172.30.2.0/24	250		eu-west-1c	rtb-20c92b59
		subnet-600cfd06	available	vpc-1d1dc17b	172.31.0.0/20	4091		eu-west-1a	rtb-3cca2845
	Private subnet	subnet-6950e10f	available	vpc-d797e7b1   ManuLab VPC	10.0.3.0/24	250		eu-west-1a	rtb-b2e575cb   Pri...
		subnet-c304f5a5	available	vpc-d81cc0be   RosettaHUB VPC	172.30.0.0/24	250		eu-west-1a	rtb-20c92b59
	Public subnet	subnet-bd57e6db	available	vpc-d797e7b1   ManuLab VPC	10.0.1.0/24	250		eu-west-1a	rtb-1fe57566

- Route Table configuration

[Create Route Table](#)
[Delete Route Table](#)
[Set As Main Table](#)

Search Route Tables and their associated VPCs

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associated	Main	VPC
<input checked="" type="checkbox"/>	Private Route Table	rtb-b2e575cb	1 Subnet	Yes	vpc-d797e7b1   ManuLab VPC
<input type="checkbox"/>	Public Route Table	rtb-1fe57566	1 Subnet	No	vpc-d797e7b1   ManuLab VPC
<input type="checkbox"/>		rtb-3cca2845	0 Subnets	Yes	vpc-1d1dc17b
<input type="checkbox"/>		rtb-20c92b59	0 Subnets	Yes	vpc-d81cc0be   RosettaHUB VPC

---

rtb-b2e575cb | Private Route Table

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Route Propagation](#)
[Tags](#)

[Edit](#)

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	eni-a57cf186 / i-04fcfaac1582aa2a5	Active	No

- Create my VPC security group, and set IP address I am connecting from:

[Create Security Group](#)
[Security Group Actions](#)

Filter: All security groups Search Security Groups and their associated VPCs

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input checked="" type="checkbox"/>	WebSecurityGroup	sg-04ee8179	WebSecurityGroup	vpc-d797e7b1   ManuLab VPC	Enable Internet Access
<input type="checkbox"/>		sg-08c86472	default	vpc-1d1dc17b	default VPC security group
<input type="checkbox"/>		sg-1bca6661	vpc-d81cc0be-securit...	vpc-d81cc0be   RosettaHUB...	RosettaHUB Master security group
<input type="checkbox"/>		sg-1bf05c61	vpc-d81cc0be-securit...	vpc-d81cc0be   RosettaHUB...	RosettaHUB Slave security group
<input type="checkbox"/>		sg-6bf45811	vpc-d81cc0be-securit...	vpc-d81cc0be   RosettaHUB...	RosettaHUB security group
<input type="checkbox"/>		sg-6ec86414	vpc-d81cc0be-securit...	vpc-d81cc0be   RosettaHUB...	RosettaHUB Efs security group
<input type="checkbox"/>		sg-d5cf63af	default	vpc-d81cc0be   RosettaHUB...	default VPC security group
<input type="checkbox"/>		sg-fee88783	default	vpc-d797e7b1   ManuLab VPC	default VPC security group

---

sg-04ee8179 | WebSecurityGroup

[Summary](#)
[Inbound Rules](#)
[Outbound Rules](#)
[Tags](#)

[Edit](#)

Type	Protocol	Port Range	Source	Description
RDP (3389)	TCP (6)	3389	109.210.64.103/32	

- Launch Instances**

Service menu -> EC2 -> Launch Instance

## Microsoft Windows Server 2016 Base

Free tier eligible

Root device type: ebsVirtualization type: hvmENA Enabled: Yes

**Ubuntu Server 16.04 LTS (HVM), SSD Volume Type** - ami-58d7e821

Select

Ubuntu Server 16.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

64-bit

Free tier eligible

Root device type: ebsVirtualization type: hvmENA Enabled: Yes

**Are you launching a database instance? Try Amazon RDS.**

Hide

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora**, **MariaDB**, **MySQL**, **Oracle**, **PostgreSQL**, and **SQL Server** databases on AWS. **Aurora** is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. [Learn more about RDS](#)

Launch a database using RDS

Windows

Free tier eligible

Root device type: ebsVirtualization type: hvmENA Enabled: Yes

**Microsoft Windows Server 2016 Base** - ami-094c7bf0

Select

Microsoft Windows 2016 Datacenter edition. [English]

64-bit

Free tier eligible

Root device type: ebsVirtualization type: hvmENA Enabled: Yes

**Deep Learning AMI (Ubuntu) Version 9.0** - ami-da586ea3

Select

Comes with latest binaries of deep learning frameworks pre-installed in separate virtual environments: MXNet, TensorFlow, Caffe, Caffe2, PyTorch, Keras, Chainer, Theano and CNTK. Fully-configured with NVIDIA CUDA, cuDNN and NCCL as well as Intel MKL-DNN

64-bit

## Choose T2.micro type

### 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 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)
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only
<input checked="" type="checkbox"/>	General purpose	<b>t2.micro</b> Free tier eligible	1	1	EBS only
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only

## 1<sup>st</sup> Instance in the Public Subnet

### 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 it

Number of instances

1

Launch into Auto Scaling Group

Purchasing option

☐ Request Spot instances

Network

vpc-d797e7b1 | ManuLab VPC

Create new VPC

Subnet

subnet-bd57e6db | Public subnet | eu-west-1a

Create new subnet

250 IP Addresses available

Auto-assign Public IP

Use subnet setting (Disable)

Placement group

☐ Add instance to placement group.

Domain join directory

None

Create new directory

IAM role

None

Create new IAM role

Shutdown behavior

Stop

## Select existing security group

### Step 6: Configure Security Group

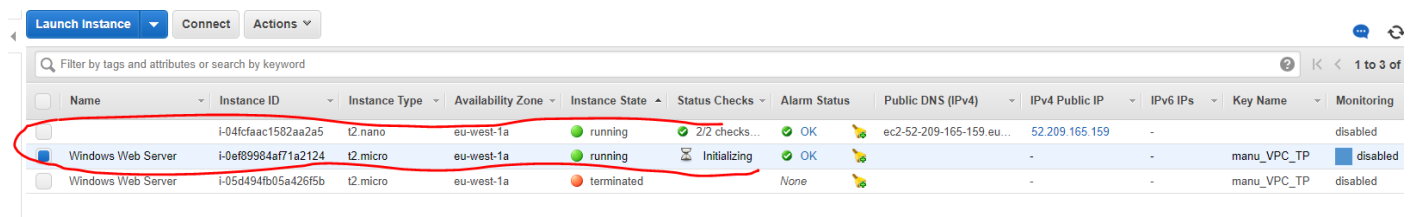
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and HTTP and HTTPS ports. You can create a new security group or select from an existing 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
<input type="checkbox"/> sg-fee88783	default	default VPC security group
<input checked="" type="checkbox"/> sg-04ee8179	WebSecurityGroup	Enable Internet Access

I have now my 2 instances, inside my public Subnet:

- Windows Web Server , created by myself (Microsoft Windows Server)
- Nat Instance, created automatically by Wizard VPC



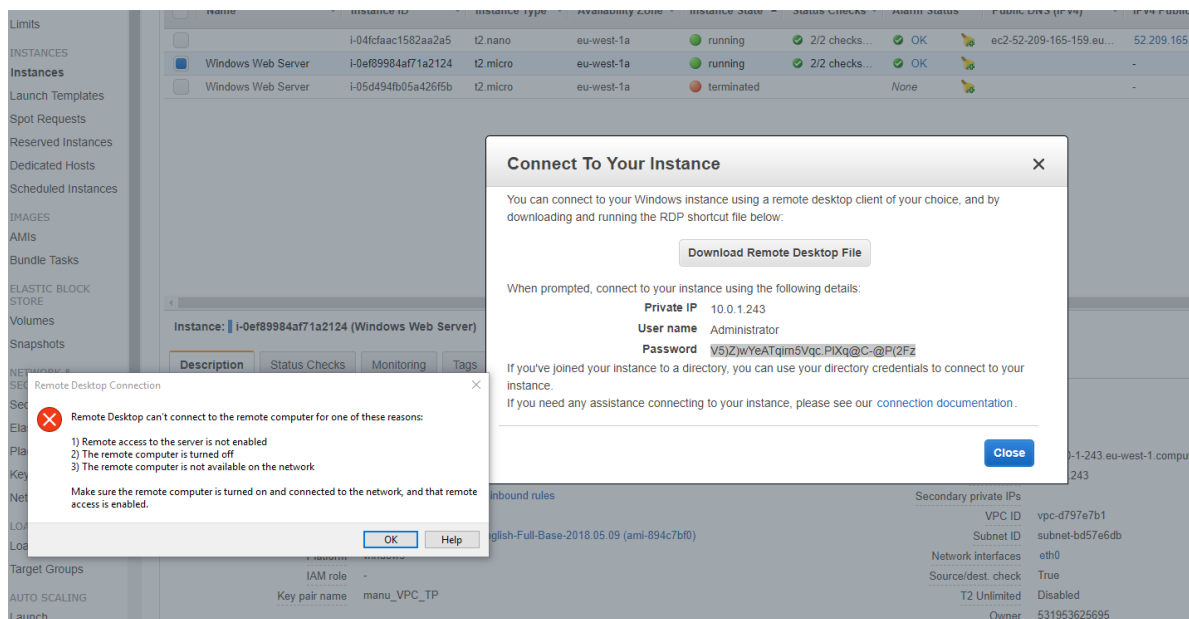
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Monitoring
	i-04fcfaac1582aa2a5	t2.nano	eu-west-1a	running	2/2 checks...	OK	ec2-52-209-165-159.eu...	52.209.165.159	-		disabled
Windows Web Server	i-0ef89984af71a2124	t2.micro	eu-west-1a	initializing	2/2 checks...	OK	-	-	-	manu_VPC_TP	disabled
Windows Web Server	i-05d494fb05a426f5b	t2.micro	eu-west-1a	terminated		None	-	-	-	manu_VPC_TP	disabled

- Try to connect to the Instance

I am not able and I do not understand ...

I check the route table, security group ..., where my IP address from where I am connecting is set ...

No idea what' wrong



The screenshot shows the AWS Management Console with a 'Connect To Your Instance' dialog box open. The dialog box provides details for connecting to the 'Windows Web Server' instance (i-0ef89984af71a2124) using Remote Desktop Protocol (RDP). The details include the Private IP (10.0.1.243), User name (Administrator), and Password (V5)ZjwYeATqm5Vqc.PiXq@C-@P(2Fz). Below the details, there is a 'Download Remote Desktop File' button and a 'Close' button.

Overlaid on the dialog box is a 'Remote Desktop Connection' error message. The message states: 'Remote Desktop can't connect to the remote computer for one of these reasons: 1) Remote access to the server is not enabled 2) The remote computer is turned off 3) The remote computer is not available on the network'. It also includes a note: 'Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.' There are 'OK' and 'Help' buttons at the bottom of the error message.