

**Session: 202130**



# **Cloud Computing**

**Assessment No.3**

## **AWS Implementation**

Case study

**Submitted by:**

Johan Sebastian Ramirez Vallejo

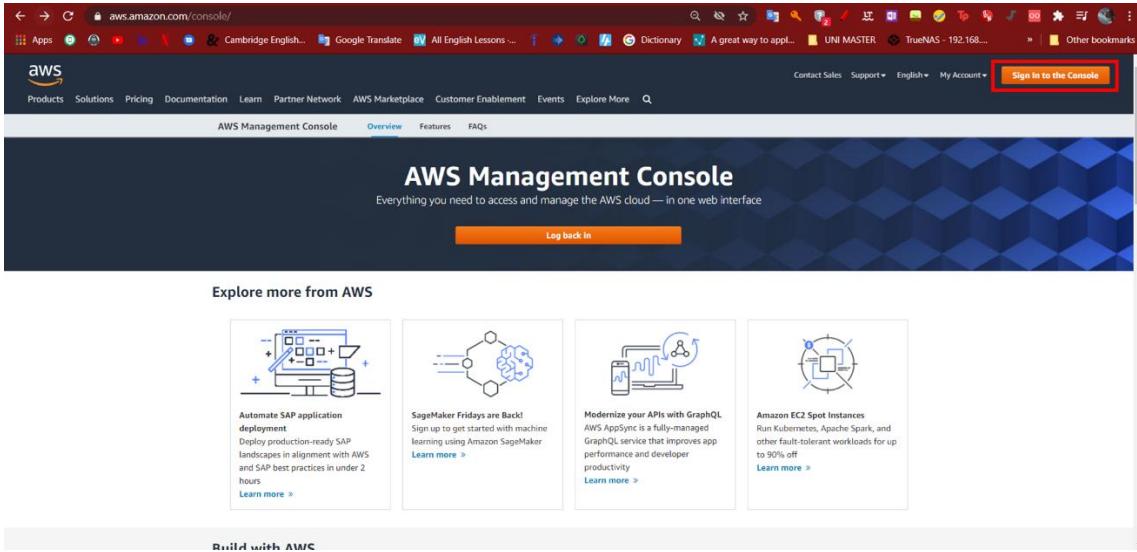
# Contents

<b>1. ACCESS DR ALARMS TO AWS MANAGEMENT CONSOLE .....</b>	<b>3</b>
1.1. STEPS AWS MANAGEMENT CONSOLE .....	3
<b>2. VPC WITH PUBLIC AND PRIVATE SUBNETS AWS .....</b>	<b>4</b>
2.1. CREATE A VPC.....	5
2.2. CREATE PRIVATE AND PUBLIC SUBNETS.....	6
<b>3. SECURITY.....</b>	<b>7</b>
3.1. SECURITY VPC: ROUTE TABLES, INTERNET GATEWAY, VPN GATEWAY AND NAT GATEWAY.....	7
3.1.1. <i>Route tables</i> .....	8
3.1.2. <i>NAT gateway and NAT instances</i> .....	9
3.1.3. <i>Internet gateway</i> .....	13
3.1.4. <i>VPN gateway</i> .....	14
3.1.5. <i>Association between Public and Private subnets, NAT gateway/NAT instance, and Internet gateway</i> .....	14
3.2. SECURITY GROUPS AND NETWORK ACLS .....	20
3.2.1. <i>Security groups</i> .....	20
3.2.2. <i>Network ACLs</i> .....	21
3.3. SECURITY AWS IDENTITY AND ACCESS MANAGEMENT (IAM).....	22
<b>4. A WINDOWS SERVER IN THE PRIVATE SUBNET.....</b>	<b>25</b>
4.1. CREATE A EC2 INSTANCE .....	26
<b>5. DATABASE INSTANCE .....</b>	<b>29</b>
5.1. CREATE DB INSTANCE RDS.....	29
5.2. CREATE EC2 INSTANCE TO CONNECT DB INSTANCE.....	32
5.3. CREATE THE SECOND USER ACCESS. ....	35
<b>6. WORDPRESS INSTANCE .....</b>	<b>36</b>
<b>7. RESOURCES .....</b>	<b>39</b>

# 1. Access DR alarms to AWS management Console

## 1.1. Steps AWS management Console

- Log in <https://aws.amazon.com/console/> web site
  - The account must be setup before to access – This can be done for the consultant that allow the users in DR Alarms access to the platform with administrative access policy.

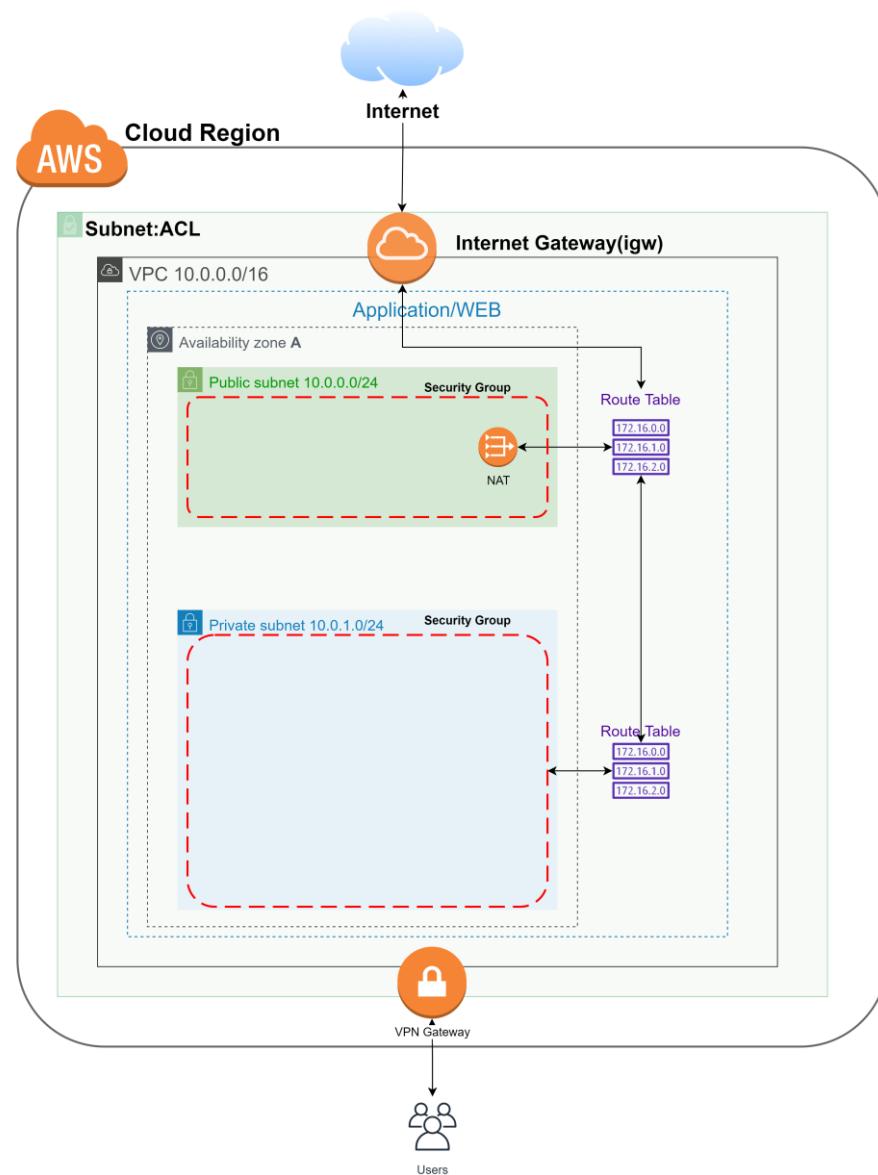


## 2. VPC with public and private subnets AWS

Manage and compute resources to provide services need external network in AWS environment. The VPC with public and private subnets provide the virtual network with the flexibility to run different services for the company, that are in a virtual environment.

**Private subnets** are connected through a NAT gateway located in a **Public subnet** to reach the internet, and **the route tables** interconnect logically subnets, **NAT gateway**, and the **Internet gateway (igw)**.

To secure the VPC are used two layers: **Network ACLs** and **Security groups** that act as Firewalls in this network. The next diagram will show the virtual public network created by DR alarms services.

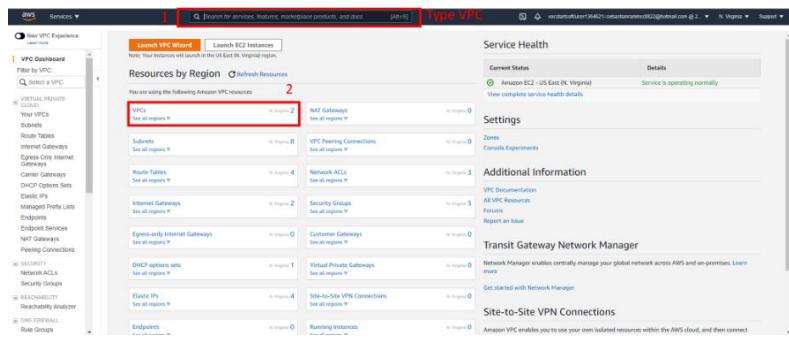


## 2.1. Create a VPC.

The next steps will show how to create a virtual private cloud (VPC) which is a **virtual** network dedicated to AWS account in this case to DR Alarms. It is logically isolated from other virtual networks in the AWS Cloud (Amazon Web Services, 2021k).

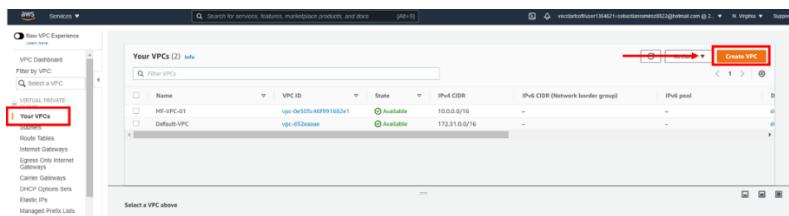
- **Open AWS VPC console**

- Type VPC in the top search bar and select VPC.
- On VPC dashboard click on VPC.



- **Create VPC**

- Click on Create VPC



- **Settings VPC**

- **Name tag** – represents the optional name for the VPC.
- **IPv4 CIDR Block** – represents the IPv4 address **range** for the VPC, this means that the VPC need to be set as a higher legacy class (B) that is represented in CIDR notation 10.0.0.0/16 to see in detail follow next link <https://tools.ietf.org/html/rfc4632> (Society, 2006). This means that 65536 IPs subnets can be created from this **primary** CIDR block.

This screenshot shows the 'Create VPC' configuration page. The 'VPC settings' section contains fields for 'Name tag - optional' (containing 'DRA-VPN-01') and 'IPv4 CIDR block - info' (containing '10.0.0.0/16'). The 'Tags' section at the bottom shows a single tag 'Name' with value 'DRA-VPN-01'. At the bottom right, there is a 'Create VPC' button.

## 2.2. Create Private and Public Subnets

The next steps allow to create the subnets in an availability zone to provide the services (instances), they are interconnected, but logically separate to provide different type of services such us a website in a public subnet or database in a private subnet. The logically difference between them is how they are connected to internet and their security layers.

- **Click on subnets in VPC dashboard on the left hand and click create Subnet.**
  - This step should be done to private and public subnets (repeat for each one).

The screenshot shows the AWS VPC Subnets page. On the left, there's a navigation sidebar with options like 'Subnets' (which is selected and highlighted with a red box). The main area displays a table of subnets with columns: Name, Subnet ID, State, VPC, IPv4 CIDR, IPv6 CIDR, Available IPv4 addresses, and Availability Zone. There are six subnets listed, all in the 'Available' state. The 'Create subnet' button is located at the top right of the table.

- **Setting Public Subnet**

- **VPC ID** – Select the VPC that was created.
- **Subnet name** – Name the subnet how it will be identifier.
- **Availability zone** – Chose the availability zone where the subnets will be located. A good practice is located them in the same zone.
- **IPv4 CIDR Block** – According to the VPC primary CIDR 10.0.0.0/16 it is necessary a CIDR Block inferior so, 10.0.0.0/24 (Public Subnet) and 10.0.1.0/24 (Private Subnet) legacy class (C) means that 256 IPs (Instances) within this subnet can be located (Amazon Web Services, 2021k)
- **Click to create subnet.**

Public Subnet	Private Subnet
<p><b>VPC</b></p> <p>VPC ID: vpc-0fb54469c52d47e1 (DRA-VPC-01)</p> <p>Associated VPC CIDRs: 10.0.0.0/16</p> <p><b>Subnet settings</b></p> <p>Subnet 1 of 1</p> <p>Subnet name: DRA-PublicSubnet-ZA</p> <p>Availability Zone: US East (N. Virginia) / us-east-1a</p> <p>IPv4 CIDR block: 10.0.0.0/24</p> <p>Tags - optional:</p> <p>Key: Name Value: DRA-PublicSubnet-ZA</p> <p>Add new tag</p> <p>Remove</p> <p>Add new subnet</p>	<p><b>VPC</b></p> <p>VPC ID: vpc-0fb54469c52d47e1 (DRA-VPC-01)</p> <p>Associated VPC CIDRs: 10.0.0.0/16</p> <p><b>Subnet settings</b></p> <p>Subnet 1 of 1</p> <p>Subnet name: DRA-PrivateSubnet-ZA</p> <p>Availability Zone: US East (N. Virginia) / us-east-1a</p> <p>IPv4 CIDR block: 10.0.1.0/24</p> <p>Tags - optional:</p> <p>Key: Name Value: DRA-PrivateSubnet-ZA</p> <p>Add new tag</p> <p>Remove</p> <p>Add new subnet</p>

### 3. Security

Security in Amazon is generally managed by controlling data traffic with different practices, including data control by ports and scope of each CIDR block. For example, the rules and data transit between NAT, route table, ACL, security group. But it must also be considered. The permissions granted to users who have access to the instances and the platform. Data assurance can be done through different practices such as Backup, updates, and protection of operating systems from viruses or hackers. Managing security through audits, monitoring, notification, alerts, configurations in the different network's layers and resources are also part of the good practices for security in the cloud.

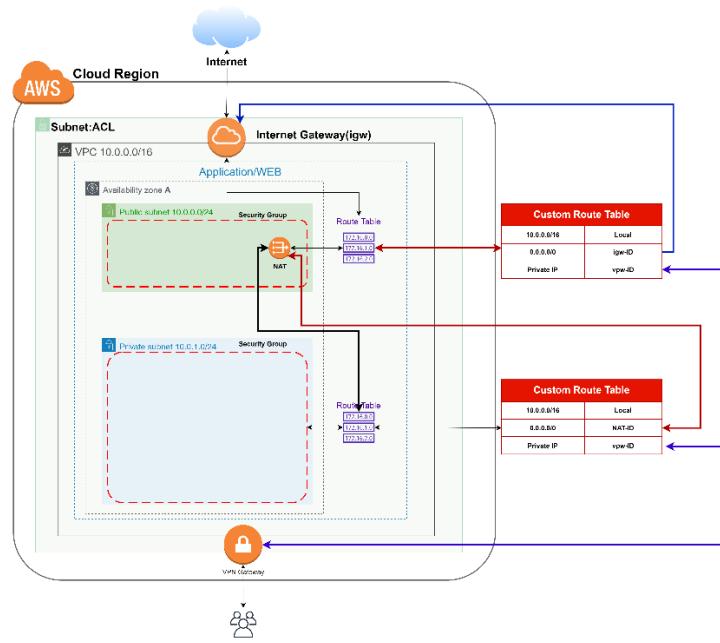
#### 3.1. Security VPC: Route tables, Internet gateway, VPN gateway and NAT gateway

To secure DR Alarms requires route the traffic through different layers to avoid unwanted traffic, this is done closing or opening ports inbound and outbound depending on the service. The **diagram** and following **steps** will show how to create the boundaries between the internet and their **association**, AWS Cloud Region and other VPC within AWS region. the next steps will show every step to set up: Route tables, NAT Gateway, VPN gateway, Internet gateway, Network ACLs, Elastic IPs and security groups. All these configurations will provide the access security of the instances created within VPC.

##### Note:

**NAT gateway:** it is guide to detail step by step in this manual, but it was simulated in the private route table directly to internet gateway because AWS Educate does not allow to create one.

**VPN gateway:** it is required to a secure connection between customer and AWS services, it was taken account in the design for DR Alarms, but AWS Educate account does not allow to create one.



### 3.1.1. Route tables

The route tables are implicit in the VPCs to control where the network traffic is directed. Every Subnet must be associated with a route table, and each route table is implicitly associated with the main route table (Amazon Web Services, 2021i).

- Click on Route tables in the left hand VPC dashboard.
- Create Route table

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under 'Route Tables', there is a red box around the 'Route Tables' link (labeled 1) and the 'Create route table' button (labeled 2). The main pane displays a table of existing route tables:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
rtb-01f08ad71725adee8		-	-	Yes	vpc-0d5e9f76f1659ef1   MF-VPC-1	269021346461
rtb-d20102ac		-	-	Yes	vpc-d32eaaae   Default-VPC	269021346461

Below the table, a specific route table is selected: 'Route Table: rtb-01f08ad71725adee8'. The 'Routes' tab is active. At the bottom of this panel is an 'Edit routes' button.

- Create the route table for Private and public subnet.
- Name Tag – Identification Route table
- VPC – Point the VPC to use the route table.
- Extra tag – optional tag to identify the RT.
- Click to create.

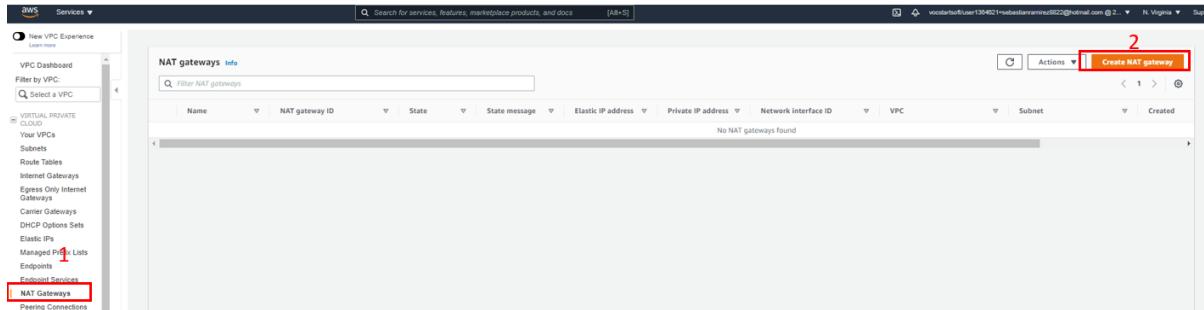
<b>Route Table for the Private Subnet</b>	<p><b>Create route table</b></p> <p>A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.</p> <p>Name tag <input type="text" value="DRA-RT-Private"/> <span style="color: #808080;">(Required)</span></p> <p>VPC* <input type="text" value="vpc-0cf85d469b52d47e1"/> <span style="color: #808080;">(Required)</span></p> <p>Key (128 characters maximum) <input type="text" value="Name"/> Value (256 characters maximum) <input type="text" value="DRA-RT-Private"/></p> <p>Add Tag 49 remaining (Up to 50 tags maximum)</p> <p>* Required <span style="float: right;">Cancel <b>Create</b></span></p>
<b>Route Table for the Public Subnet</b>	<p><b>Create route table</b></p> <p>A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.</p> <p>Name tag <input type="text" value="DRA-RT-Public"/> <span style="color: #808080;">(Required)</span></p> <p>VPC* <input type="text" value="vpc-0cf85d469b52d47e1"/> <span style="color: #808080;">(Required)</span></p> <p>Filter by attributes <input type="text" value="DRA-RT-Private"/> <span style="color: #808080;">(Required)</span></p> <p>Value (256 characters maximum) <input type="text" value="DRA-RT-Public"/></p> <p>Add Tag 49 remaining (Up to 50 tags maximum)</p> <p>* Required <span style="float: right;">Cancel <b>Create</b></span></p>

### 3.1.2. NAT gateway and NAT instances

#### 3.1.2.1. NAT gateway (it is not free)

This gateway supports to connect to the internet from instances within a private subnet security.

- Click on NAT gateway in the VPC dashboard left hand.



#### ■ Create the NAT Gateway

- **Name** – Identification NAT gateway
- **Subnet** – Choose the public subnet, because it is the subnet which is connected directly to the Internet.
- **Elastic IP** – click in Allocate Elastic IP – it is necessary to establish a static IP because a NAT works as an instance in the public subnet that translates the traffic between internet and private subnet (Amazon Web Services, 2021f).
- **Create NAT gateway**

1  
2  
3  
4

### 3.1.2.2. NAT Instance

The NAT instance is a server installed in the public subnet allowing traffic to internet instances from private subnets (Amazon Web Services, 2021g).

- **Create the Security group**
  - Select the ports to allow the traffic and point the inbound rules to the private subnet.
  - **Allow traffic from outbound** – notice that remote control port is not open.

The screenshot shows the 'Create security group' wizard with the following details:

**Basic details**

- Security group name: **nat**
- Description: **ALLOW TRAFFIC PRIVATE SUB THROUGH PUBLIC SUB TO INTERNET**
- VPC: **us-west-2a** (arn:aws:vpc:us-west-2:234567890123456789:subnet-012345678901234567)

**Inbound rules**

Type	Protocol	Port range	Source	Description
HTTP	TCP	80	Custom (16.8.1.0/24)	INBOUND-HTTP TRAFFIC FROM PRIVATE SUBNET
HTTPS	TCP	443	Custom (16.8.1.0/24)	INBOUND-HTTPS TRAFFIC FROM PRIVATE SUBNET
SSH	TCP	22	Custom (16.8.0.0/16)	INBOUND-SSH TRAFFIC TO THE INSTANCE

**Outbound rules**

Type	Protocol	Port range	Destination	Description
HTTP	TCP	80	Custom (0.0.0.0/0)	ALLOW OUTBOUND-HTTP TRAFFIC
HTTPS	TCP	443	Custom (0.0.0.0/0)	ALLOW OUTBOUND-HTTPS TRAFFIC

- **Create the instance.**

- Launch the instance

The screenshot shows the EC2 Instances page with the following interface elements:

- Instances** tab selected.
- Launch Instances** button highlighted with a red box.
- Step 1: Choose an Amazon Machine Image (AMI)** section:
  - Search bar: **nat**
  - Filter results: **1 to 50 of 618 AMIs**
  - Results table:
 

Name	Description	Select
amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-ebs - ami-00a9d4a05375b2783	Amazon Linux AMI 2018.03.0.20181116 x86_64 VPC HVM ebs Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	Select
amzn-ami-vpc-nat-hvm-2017.09.1.20180108-x86_64-ebs - ami-01623d7b	Amazon Linux AMI 2017.09.1.20180108 x86_64 VPC NAT HVM EBS Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	Select
amzn-ami-vpc-nat-2018.03.0.20200716.0-x86_64-ebs - ami-01ef319f39c5aaed	Amazon Linux AMI 2018.03.0.20200716.0 x86_64 VPC NAT HVM EBS Root device type: ebs Virtualization type: hvm ENA Enabled: Yes	Select

## ■ In community AMI call a NAT and select

### 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 families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro	1	1	EBS only	-	Low to Moderate	Yes

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-0f55469b52d47ef1 | DRA-VPC-01 Create new VPC  
Subnet: subnet-09fe65a7782ebd18 | DRA-PublicSubnet-Z Create new subnet  
251 IP Addresses available

Auto-assign Public IP: Enable

Placement group: Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory Create new directory

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 will apply for dedicated tenancy

Elastic Inference: Add an Elastic Inference accelerator Additional charges apply

Credit specification: Unlimited Additional charges may apply

File systems: Add file system Create new file system

Network interfaces:

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-0a9fe651	Auto-assign	Add IP	

Cancel Previous Review and Launch Next: Add Storage

1. Select the VPC
2. Select Public Subnet
3. Select enable and after launch the instance allocate Elastic IP to hold the IP to this Instance

## ■ Next to add storage(leave the default) and Tag the Instance

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	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (Mbps)	Delete on Termination	Encryption
Root	/dev/xvda	097e04bc11ff77ad5	8	Magnetic (Infiniti)	N/A	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/> Not Encrypted

Add New Volume

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 2 IOPS/GiB. Set my root volume to General Purpose (SSD). 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.

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 (0)	Volumes (0)	Network Interfaces (0)
Name	<input type="text" value="DRA-SERVER-PUBLIC-SUBNET"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

- Select the security group that was created – review and launch the instance.

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 security groups.

Select a new security group  Create a new security group  Select an existing security group

Security Group ID	Name	Description	Actions
sg-03162cfebd8d0ff	default	default VPC security group	<a href="#">Copy to new</a>
sg-02f02c1e46940ff	NAT-001	ALLOW TRAFFIC PRIVATE SUB THROUGH PUBLIC SUB TO INTERNET	<a href="#">Copy to new</a>

**Warning**  
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Select the Security group that was created

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	10.0.1.0/24	INBOUND HTTP TRAFFIC
SSH	TCP	22	10.0.0.0/16	INBOUND TRAFFIC FROM INTERNAL
HTTPS	TCP	443	10.0.1.0/24	INBOUND HTTPS TRAFFIC

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

- Setting the NAT instance in the network

- Allocate Elastic IP address (Option is find in the EC2 dashboard left hand) – it is necessary to allocate a static IP in the network to point the instance always to the same address.
- Associate Elastic IP address – Assign the address to the instance.
- Make sure it is locating the IP address in the instance created.
- Make sure you instance can send and receive traffic – Select the instance - go to actions – networking -change source / destination check- Save.

EC2 > Elastic IP address > Allocate Elastic IP address

Allocate Elastic IP address [Info](#)

1

Elastic IP address settings [Info](#)

Allocate a new IP address [Create another](#)

Public IPv4 address pool  Allocation pool of IPv4 addresses [Learn more](#)

Private IPv4 address pool  Allocation pool of IPv4 addresses for your private subnets. This pool must be located in the same VPC as the instance you're creating. [Learn more](#)

Global static IP address [Learn more](#)

Tags - optional [Learn more](#)

Key [Create new key](#) [Import key](#) [Associate key](#) [Delete key](#)

2

EC2 > Elastic IP address > Associate Elastic IP address

Associate Elastic IP address [Info](#)

Elastic IP address: 50.6.117.117 [Info](#)

Pull down action and click associate EIP

Resource type [Learn more](#)

Choose the type of resource with which to associate the Elastic IP address.

Instance  [Select instance](#)

Network interface [Select interface](#)

3

EC2 > Instances > i-05685422f9010932f (NAT-INSTANCE-PS) [Info](#)

Instance summary for i-05685422f9010932f (NAT-INSTANCE-PS)

1

2

3

EC2 > Instances > i-05685422f9010932f > Change source / destination check

Source / destination check [Info](#)

If this is a NAT instance, you must stop source / destination checking. A NAT instance must be able to send and receive traffic when the source or destination is not itself.

Instance ID: i-05685422f9010932f (NAT-INSTANCE-PS)

Network interface [Info](#)

eni-0f814181338694408 (NAT-INSTANCE-PS)

Source / dest checking [Info](#)

Stop [Stop](#)

5

EC2 > Instances > i-05685422f9010932f > Stop

Stop [Stop](#)

4

EC2 Dashboard [New](#)

Instances [New](#)

Instances (1/1) [Info](#)

Filter instances [Clear filters](#)

Instance state: running [Filter instances](#)

Name: NAT-INSTANCE-PS [Filter instances](#)

Instance ID: i-05685422f9010932f

Attach network interface [Edit](#)

Detach network interface [Edit](#)

Change source/destination check [Edit](#)

Disassociate Elastic IP address [Edit](#)

Manage IP addresses [Edit](#)

Connect [Edit](#)

View details [Edit](#)

Manage instance state [Edit](#)

Instance settings [Edit](#)

Networking [Edit](#)

Security [Edit](#)

Image and templates [Edit](#)

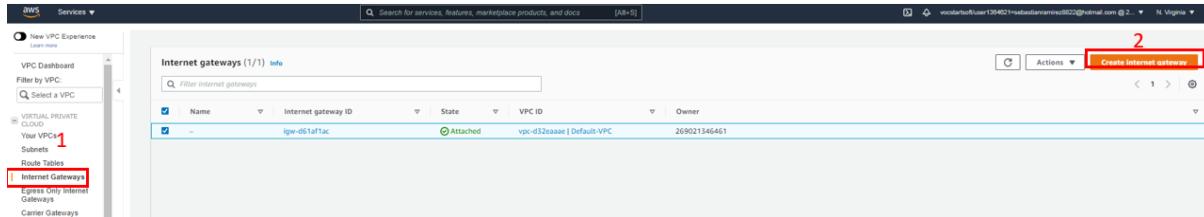
Monitor and troubleshoot [Edit](#)

Launch instances [Edit](#)

### 3.1.3. Internet gateway

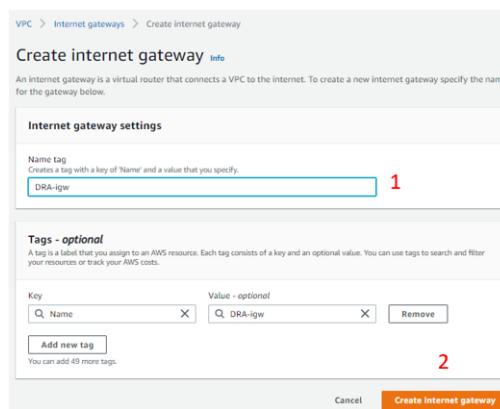
Internet gateways serve two purposes: to point the VPC route tables for internet, and perform network address translation (NAT)(Amazon Web Services, 2021e).

- Click on Internet gateway in the VPC dashboard left hand.



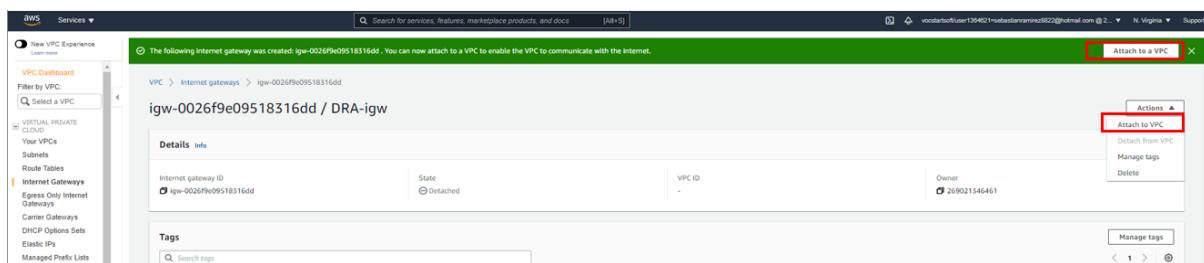
- Create internet gateway.

- Name tag – identification for Internet Gateway



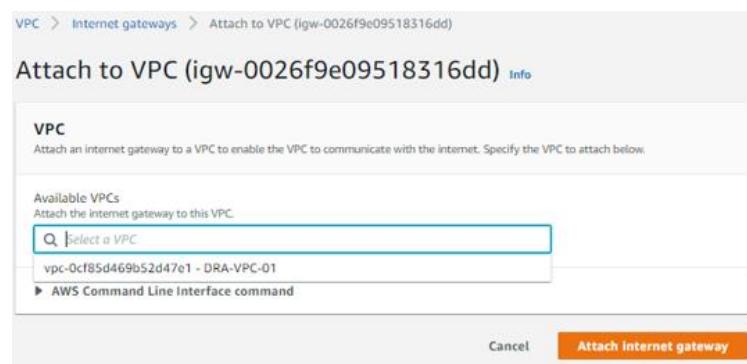
- Attach internet gateway to VPC.

- Find options after creating an Internet gateway to attach to the VPC.



- Select the VPC that was created.

- Attach internet gateway.



### 3.1.4. VPN gateway

- The general concept is a remotely secure connection between on-premises equipment and Staff to the VPCs, this occur though a VPN tunnel that encrypted the data that pass through (Amazon Web Services, 2021c).
- The module can be found in the VPC dashboard left hand / (Center, 2020)

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under 'VPC PRIVATE NETWORKS', 'Customer Gateways' and 'Virtual Private Gateways' are highlighted with a red box. In the center, the 'Site-to-Site VPN Connections' section is also highlighted with a red box. At the bottom right, there is a 'Create VPN Connection' button.

### 3.1.5. Association between Public and Private subnets, NAT gateway/NAT instance, and Internet gateway

#### o Public association

- The public association consist of to connect a route table pointed to the local network and internet network (refer to the diagram), **the VPN connection is simulated**, but it is connected through the route table.
- Click on Route tables in the left hand VPC dashboard.**
  - Select Public RT that was created and **Routes** to edit where must point – Notice that the RT is pointed just to local network as a default configuration.

The screenshot shows the AWS VPC Dashboard. On the left sidebar, 'Route Tables' is highlighted with a red box. In the main area, a route table named 'DRA-RT-Public' is selected. The 'Routes' tab is highlighted with a red box. A specific route entry is highlighted with a red box, showing a destination of '10.0.0.0/16' and a target of 'local'. The 'Edit routes' button is also highlighted with a red box.

- **Click Edit routes** – create the route to traffic data through the Internet gateway that was created above – 0.0.0.0/0, which represents all IPv4 addresses. The target is the internet gateway that's attached to your VPC (Amazon Web Services, 2021i).
- **Select the igw and Save routes.**

## Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-[ igw-0026f9e09518316dd DRA-igw]		No

Add route Cancel **Save routes**

\* Required

- **Subnet Associations – Edit subnet associations** which literally associate the public subnet to the public route table. Notice that the Public RT doe does not have any association. For default this is not associate

Route Tables **1**

**2** DRA-RT-Public

**3** Subnet Associations

**4** Edit subnet associations

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
DRA-RT-Public	rtb-09150e11cb3367132	-	-	No	vpc-0cf85d469b52d47e1   DRA-VPC-01
DRA-RT-Private	rtb-018d087572420f16a	-	-	No	vpc-0cf85d469b52d47e1   DRA-VPC-01
	rtb-d20102ac	-	-	Yes	vpc-d32eaeee   Default-VPC
	rtb-0805caa342274b203	-	-	Yes	vpc-0cf85d469b52d47e1   DRA-VPC-01

- **Select the Public subnet - Save.**

## Edit subnet associations

Route table rtb-09150e11cb3367132 (DRA-RT-Public)				
Associated subnets <b>subnet-0a6fe65a7782ebd18</b>				
<b>1</b> <input checked="" type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	
<b>1</b> <input checked="" type="checkbox"/>	subnet-0ee519a28f5b61c99   DRA-PrivateSubnet-ZA	10.0.1.0/24	-	Main
<b>1</b> <input checked="" type="checkbox"/>	subnet-0a6fe65a7782ebd18   DRA-PublicSubnet-ZA	10.0.0.0/24	-	Main

\* Required Cancel **Save**

**2**

- **Route propagation** – mark yes when the VPN is established.  
Notice there is not any connection with a VPN.

The screenshot shows the AWS VPC Route Tables page. On the left, a sidebar lists various VPC components: Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, Peering Connections, Security Groups, Network ACLs, and Reachability. A red box labeled '1' highlights the 'Route Tables' section. In the main content area, a table lists four route tables:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
DRA-RT-Public	rb-09150e11cb3367132	subnet-0a6fe65a7782ebd18	-	No	vpc-0cf85d469b52d47e1   DRA-VPC-01
DRA-RT-Private	rb-018d087572420f16a	-	-	No	vpc-0cf85d469b52d47e1   DRA-VPC-01
	rb-d20102ac	-	-	Yes	vpc-d32eaaae   Default-VPC
	rb-0805caa342274b203	-	-	Yes	vpc-0cf85d469b52d47e1   DRA-VPC-01

A red box labeled '2' points to the 'Actions' dropdown menu. Below the table, a sub-table for 'Route Table: rb-09150e11cb3367132' shows tabs for Summary, Routes, Subnet Associations, Edge Associations, Route Propagation (which is highlighted with a red box labeled '3'), and Tags. A red box labeled '4' points to the 'Edit route propagation' button. A message box states: "You do not have any virtual private gateways which are allowed to update this route table."

- **Results Association Public subnet**

The screenshot displays two side-by-side AWS VPC configuration pages. The left page shows the 'Public Route' configuration, and the right page shows the 'Public association' configuration.

**Public Route:** This section shows the 'Create route table' and 'Actions' dropdown menus. The main content lists route tables and their associations. A red box highlights the 'Edit routes' button. Below it, a table shows a single route entry:

Destination	Target
10.0.0.0/16	local
0.0.0.0	igw-00269fe095

**Public association:** This section shows the 'Create route table' and 'Actions' dropdown menus. It lists route tables and their associations. A red box highlights the 'Edit subnet associations' button. Below it, a table shows a single association entry:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0a6fe65a7782ebd...	10.0.0.0/24	-

Observe that the route table is pointed to the local network and internet.

### ○ Private association

- The public association consist of to connect a route table pointed to the local network and NAT gateway or NAT instance (refer to the diagram), **the VPN connection is simulated**, but it is connected through the route table.
- Click on Route tables in the left hand VPC dashboard.**
  - Select Private RT that was created and **Routes** to edit where must point – Notice that the RT is pointed just to local network as a default configuration.

The screenshot shows the AWS VPC Dashboard. On the left sidebar, under 'Route Tables' (marked with a red box 1), there are two entries: 'DRA-RT-Public' and 'DRA-RT-Private' (marked with a red box 2). The 'DRA-RT-Private' table is selected. In the main pane, the 'Create route table' button is visible at the top. Below it is a table with columns: Name, Route Table ID, Explicit subnet association, Edge associations, Main, and VPC ID. The 'DRA-RT-Private' row is highlighted. At the bottom of the main pane, there is a 'Route Table: rtb-018d087572420f16a' section with tabs for Summary, Routes (marked with a red box 3), Subnet Associations, Edge Associations, Route Propagation, and Tags. The 'Routes' tab is selected. Below this, the 'Edit routes' button is highlighted with a red box 4. A table shows a single route entry: Destination 10.0.0.0/16, Target local, Status active, and Propagated No. This row is also highlighted with a red box.

- Click Edit routes** – create the route to traffic data through the Internet gateway that was created above – 0.0.0.0/0, which represents all IPv4 addresses. The target is the NAT gateway that was putted in the public subnet.
- Select the NAT gateway/or NAT instance and Save routes.**

### ○ NAT gateway

Edit routes

The screenshot shows the 'Edit routes' interface. It has a table with columns: Destination, Target, Status, and Propagated. There are two rows: one for '10.0.0.0/16' with 'local' as the target and another for '0.0.0.0/0' with an empty target field. The second row has a 'Save routes' button to its right. Below the table, there is an 'Add route' button and a note '\* Required'. A dropdown menu is open over the empty target field for '0.0.0.0/0', listing options: Carrier Gateway, Egress Only Internet Gateway, Gateway Load Balancer Endpoint, Instance, Internet Gateway, NAT Gateway (which is highlighted), Network Interface, and Outpost Local Gateway. At the bottom right of the dropdown are 'Cancel' and 'Save routes' buttons.

## ○ NAT Instance

### Edit routes

The screenshot shows the 'Edit routes' interface for a route table. A modal window is open, listing various targets for a route. The 'Instance' option is highlighted with a red box. Other options include Carrier Gateway, Egress Only Internet Gateway, Gateway Load Balancer Endpoint, Internet Gateway, local, NAT Gateway, and Network Interface.

Route Tables > Edit routes

### Edit routes

The screenshot shows the 'Edit routes' interface for a route table. It contains two route entries:

- Destination: 10.0.0/16, Target: local, Status: active, Propagated: No
- Destination: 0.0.0.0, Target: i-05885d22f9010932f (with a tooltip 'i-05885d22f9010932f NAT-INSTANCE-PS'), Status: active, Propagated: No

A modal window from the previous slide is partially visible at the bottom.

\* Required Cancel Save routes

- **Subnet Associations – Edit subnet associations** which literally associate the public subnet to the public route table. Notice that the Public RT does not have any association. For default this is not associate.

The screenshot shows the AWS VPC Experience interface under the 'Route Tables' section. It displays two route tables:

- DRA-RT-Public (selected)
- DRA-RT-Private

For the DRA-RT-Private route table, there are four entries listed:

- rtb-09150e11cb3367132: subnets associated with rtb-018d087572420f16a
- rtb-018d087572420f16a: main route table
- rtb-d20102ac: main route table
- rtb-0805caa342274b203: main route table

The 'Subnet Associations' tab is selected in the details view for the rtb-018d087572420f16a entry. The message 'You do not have any subnet associations.' is displayed.

- Select the Public subnet – Save.

### Edit subnet associations

Route table rtb-018d087572420f16a (DRA-RT-Private)

Associated subnets subnet-0ee519a28f5b61c99

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0ee519a28f5b61c99   DRA-PrivateSubnet-ZA	10.0.1.0/24	-	Main
subnet-0a6fe65a7782ebd18   DRA-PublicSubnet-ZA	10.0.0.0/24	-	rtb-09150e11cb3367132

\* Required Cancel Save

- Route propagation (To set up a VPN) – mark yes when the VPN is established. Notice there is not any connection with a VPN.

New VPC Experience

VPC Dashboard Filter by VPC: Select a VPC

VIRTUAL PRIVATE CLOUD Your VPCs Subnets

**Route Tables**

- Internet Gateways
- Egress Only Internet Gateways
- Carrier Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

SECURITY

Create route table Actions

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
DRA-RT-Public	rtb-09150e11cb3367132	subnet-0a6fe65a7782ebd18	-	No	vpc-0cf85d469b52d47e1   DRA-VPC-01
<b>DRA-RT-Private</b>	<b>rtb-018d087572420f16a</b>	-	-	No	<b>vpc-0cf85d469b52d47e1   DRA-VPC-01</b>
	rtb-d20102ac	-	-	Yes	vpc-d32eaae   Default-VPC
	rtb-0805caa342274b203	-	-	Yes	vpc-0cf85d469b52d47e1   DRA-VPC-01

Route Table: rtb-018d087572420f16a

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit route propagation

Virtual Private Gateway Propagate

You do not have any virtual private gateways which are allowed to update this route table.

### • Results Association Public subnet

Private Route	Private association																																			
<p>New VPC Experience</p> <p>VPC Dashboard Filter by VPC: Select a VPC</p> <p>VIRTUAL PRIVATE CLOUD Your VPCs Subnets</p> <p><b>Route Tables</b></p> <ul style="list-style-type: none"> <li>Internet Gateways</li> <li>Egress Only Internet Gateways</li> <li>Carrier Gateways</li> <li>DHCP Options Sets</li> <li>Elastic IPs</li> <li>Managed Prefix Lists</li> <li>Endpoints</li> <li>Endpoint Services</li> <li>NAT Gateways</li> <li>Peering Connections</li> </ul> <p>SECURITY</p> <p>REACHABILITY</p> <p>Reachability Analyzer</p> <p>Create route table Actions</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Route Table ID</th> <th>Explicit subnet association</th> </tr> </thead> <tbody> <tr> <td>DRA-RT-Public</td> <td>rtb-09150e11cb3367132</td> <td>subnet-0a6fe65a7782ebd18</td> </tr> <tr> <td><b>DRA-RT-Private</b></td> <td><b>rtb-018d087572420f16a</b></td> <td><b>subnet-0ee519a28f5b61c99</b></td> </tr> <tr> <td></td> <td>rtb-d20102ac</td> <td>-</td> </tr> <tr> <td></td> <td>rtb-0805caa342274b203</td> <td>-</td> </tr> </tbody> </table> <p>Route Table: rtb-018d087572420f16a</p> <p>Summary Routes Subnet Associations Edge Associations Route Propagation Tags</p> <p>Edit routes</p> <p>View All routes</p> <table border="1"> <thead> <tr> <th>Destination</th> <th>Target</th> </tr> </thead> <tbody> <tr> <td>10.0.0.0/16</td> <td>local</td> </tr> <tr> <td>0.0.0.0/0</td> <td>nat-0cf9f029a4c32ddf</td> </tr> </tbody> </table>	Name	Route Table ID	Explicit subnet association	DRA-RT-Public	rtb-09150e11cb3367132	subnet-0a6fe65a7782ebd18	<b>DRA-RT-Private</b>	<b>rtb-018d087572420f16a</b>	<b>subnet-0ee519a28f5b61c99</b>		rtb-d20102ac	-		rtb-0805caa342274b203	-	Destination	Target	10.0.0.0/16	local	0.0.0.0/0	nat-0cf9f029a4c32ddf	<p>New VPC Experience</p> <p>VPC Dashboard Filter by VPC: Select a VPC</p> <p>VIRTUAL PRIVATE CLOUD Your VPCs Subnets</p> <p><b>Route Tables</b></p> <ul style="list-style-type: none"> <li>Internet Gateways</li> <li>Egress Only Internet Gateways</li> <li>Carrier Gateways</li> <li>DHCP Options Sets</li> <li>Elastic IPs</li> <li>Managed Prefix Lists</li> <li>Endpoints</li> <li>Endpoint Services</li> <li>NAT Gateways</li> <li>Peering Connections</li> </ul> <p>SECURITY</p> <p>REACHABILITY</p> <p>Reachability Analyzer</p> <p>Create route table Actions</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Route Table ID</th> </tr> </thead> <tbody> <tr> <td>DRA-RT-Public</td> <td>rtb-09150e11cb3367132</td> </tr> <tr> <td><b>DRA-RT-Private</b></td> <td><b>rtb-018d087572420f16a</b></td> </tr> <tr> <td></td> <td>rtb-d20102ac</td> </tr> <tr> <td></td> <td>rtb-0805caa342274b203</td> </tr> </tbody> </table> <p>Route Table: rtb-018d087572420f16a</p> <p>Summary Routes Subnet Associations Edge Associations</p> <p>Edit subnet associations</p> <table border="1"> <thead> <tr> <th>Subnet ID</th> <th>IPv4 CIDR</th> </tr> </thead> <tbody> <tr> <td>subnet-0ee519a28f5b61c99   DRA-PrivateSubnet-ZA</td> <td>10.0.1.0/24</td> </tr> </tbody> </table>	Name	Route Table ID	DRA-RT-Public	rtb-09150e11cb3367132	<b>DRA-RT-Private</b>	<b>rtb-018d087572420f16a</b>		rtb-d20102ac		rtb-0805caa342274b203	Subnet ID	IPv4 CIDR	subnet-0ee519a28f5b61c99   DRA-PrivateSubnet-ZA	10.0.1.0/24
Name	Route Table ID	Explicit subnet association																																		
DRA-RT-Public	rtb-09150e11cb3367132	subnet-0a6fe65a7782ebd18																																		
<b>DRA-RT-Private</b>	<b>rtb-018d087572420f16a</b>	<b>subnet-0ee519a28f5b61c99</b>																																		
	rtb-d20102ac	-																																		
	rtb-0805caa342274b203	-																																		
Destination	Target																																			
10.0.0.0/16	local																																			
0.0.0.0/0	nat-0cf9f029a4c32ddf																																			
Name	Route Table ID																																			
DRA-RT-Public	rtb-09150e11cb3367132																																			
<b>DRA-RT-Private</b>	<b>rtb-018d087572420f16a</b>																																			
	rtb-d20102ac																																			
	rtb-0805caa342274b203																																			
Subnet ID	IPv4 CIDR																																			
subnet-0ee519a28f5b61c99   DRA-PrivateSubnet-ZA	10.0.1.0/24																																			

## 3.2. Security groups and Network ACLs

These 2 layers of security act as a firewall in different layers within VPC, Security groups for Instance level and Network ACLs subnet level. They contain the rules to which allow certain traffic into the VPC network from Internet. They must be synchronized with the same rules to avoid problems. The next table will provide the ports that are required to allow traffic inbound and outbound.

### 3.2.1. Security groups

The security group acts a firewall for each instance that it has in the network, each instance can be act different to each other and can be assigned different set of security groups.

When an instance is created a security group is needed. Establish the rules before create instance is a good practice. But they also can be created with the instance process.

To create the security group, I listed the rules that are required.

#### Instances Private group rules

Inbound rules (5)					<a href="#">Edit inbound rules</a>
Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	0.0.0.0/0	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).	
HTTP	TCP	80	::/0	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).	
RDP	TCP	3389	0.0.0.0/0	Access Remote	
HTTPS	TCP	443	0.0.0.0/0	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).	
HTTPS	TCP	443	::/0	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).	

#### Instances Public Group DB rules

Inbound rules (4)					<a href="#">Edit inbound rules</a>
Type	Protocol	Port range	Source	Description - optional	
MSSQL	TCP	1433	0.0.0.0/0	Allow connection to DB instance	
HTTP	TCP	80	0.0.0.0/0	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).	
RDP	TCP	3389	0.0.0.0/0	Access Remote	
HTTPS	TCP	443	0.0.0.0/0	Allow outbound HTTPS access to the Internet over IPv4 (for example, for software updates).	

#### NAT Instance rules

[Create security group](#)

A security group acts as a critical firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name:  Name cannot be edited after creation.

Description:

VPC:

**Inbound rules**

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom <input type="text" value="10.0.1.0/24"/>	INBOUND HTTP TRAFFIC FROM PRIVATE SUBNET
HTTPS	TCP	443	Custom <input type="text" value="10.0.1.0/24"/>	INBOUND HTTPS TRAFFIC FROM PRIVATE SUBNET
SSH	TCP	22	Custom <input type="text" value="10.0.0.0/16"/>	INBOUND TRAFFIC FROM PRIVATE SUBNET REMOTE CONTROL

[Add rule](#)

**Outbound rules**

Type	Protocol	Port range	Destination	Description - optional
HTTP	TCP	80	Custom <input type="text" value="0.0.0.0/0"/>	ALLOW OUTBOUND HTTP TRAFFIC
HTTPS	TCP	443	Custom <input type="text" value="0.0.0.0/0"/>	ALLOW OUTBOUND HTTPS TRAFFIC

[Add rule](#)

### 3.2.2. Network ACLs

A network control list (ACL) act as a firewall controlling the traffic in a subnet layer, they must be similar to the security group rules(Amazon Web Services, 2021h).

- **Create Network ACLs**

- **Click on Network ACLs in VPC dashboard – create network.**
- **Name – ID name for the Network ACLs**
- **VPC – Chose the VPC where it is going to apply - Create.**
- **On Network ACLs - select the network that was created and edit inbound, outbound and subnet association.**

The screenshot shows the AWS VPC Network ACL creation and configuration process across three main windows:

- Top Window:** Shows the "Edit inbound rules" configuration. It lists four rules:
 

Rule number	Type	Protocol	Port range	Source	Action
1	HTTP	TCP/80	All	0.0.0.0/0	Allow
2	HTTP (443)	TCP/443	All	0.0.0.0/0	Allow
3	SMB (22)	TCP/22	All	0.0.0.0/0	Allow
4	HTTP (5000)	TCP/5000	All	0.0.0.0/0	Allow

 A red box highlights the "Add new rule" button at the bottom left, with the text "Add rules to allow traffic".
- Middle Window:** Shows the "Edit outbound rules" configuration. It lists one rule:
 

Rule number	Type	Protocol	Port range	Destination	Action
1	All traffic	All	All	0.0.0.0/0	Allow

 A red box highlights the "Add new rule" button at the bottom left, with the text "Add rules to allow traffic".
- Bottom Window:** Shows the "Select the Subnet to apply the rules" configuration. It lists two subnets:
 

Name	Subnet ID	Associated with	Availability zone	IPv4 CIDR	IPv6 CIDR
PublicSubnet-2A	subnet-0f288b78f1f53290	vpc-05123eae / subnets-0f288b78f1f53290	us-east-1a	100.1.0.0/24	-
PublicSubnet-2B	subnet-0f288b78f1f53291	vpc-05123eae / subnets-0f288b78f1f53291	us-east-1a	100.1.1.0/24	-

 A red box highlights the "Select" button at the bottom right, with the text "Select the Subnet to apply the rules".

The rules created for the subnets were:

The screenshot shows the successful creation of Network ACL rules for two subnets:

- Top Window:** Shows the "acl-0ca4783aefde37707 / PublicSubnet - ACL" details. It lists an associated subnet: "subnet-0f288b78f1f53290 / subnets-0f288b78f1f53290".
- Middle Window:** Shows the "Inbound rules (6)" configuration for the "PublicSubnet - ACL". It lists six rules:
 

Rule number	Type	Protocol	Port range	Source	Action
1	Set to (443)	TCP/443	443	0.0.0.0/0	Allow
2	HTTP (443)	TCP/443	All	0.0.0.0/0	Allow
3	HTTP (80)	TCP/80	80	0.0.0.0/0	Allow
4	HTTP (5000)	TCP/5000	All	0.0.0.0/0	Allow
5	All traffic	All	All	0.0.0.0/0	Deny

 A red box highlights the "Edit inbound rules" button at the bottom right, with the text "Edit inbound rules".
- Bottom Window:** Shows the "Network ACLs (1/4) info" configuration for the "PrivateSubnet - ACL". It lists an associated subnet: "subnet-0f288b78f1f53291 / subnets-0f288b78f1f53291".
- Bottom Middle Window:** Shows the "Inbound rules (4)" configuration for the "PrivateSubnet - ACL". It lists four rules:
 

Rule number	Type	Protocol	Port range	Source	Action
1	HTTP (80)	TCP/80	80	10.0.1.0/24	Allow
2	HTTP (443)	TCP/443	All	10.0.1.0/24	Allow
3	All traffic	All	All	0.0.0.0/0	Deny

 A red box highlights the "Edit inbound rules" button at the bottom right, with the text "Edit inbound rules".

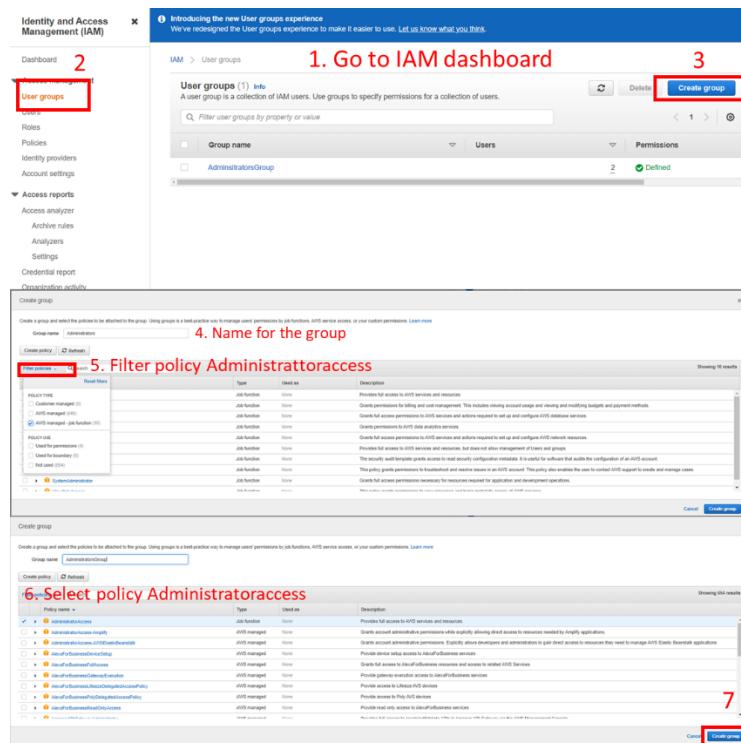
### 3.3. Security AWS Identity and Access Management (IAM)

The AWS identity and access Management enable securely Control to individual and group access to AWS resources. For example. Compute, storage, networking demand, databases, VPC etc. (Amazon Web Services, 2021b).

- **AWS IAM Authentication** - the users must authenticate before user AWS Management Console, AWS CLI or AWS SDKs. Users need to get credentials to use the resources.
  - **Groups** - Support manage **roles** and **policies** to different categories of groups in the organizations that need to access to AWS Resources. For Example, IT administrators, Billing etc. Groups are collections of IAM Users.
  - **IAM User** – attach policies with permissions that determined what identity can and cannot do in AWS. The security credentials are controlled under a single AWS account.
  - **Policy** – it is an explicitly list permissions defines the effect, actions, resources, and optional conditions.
  - **Roles** – they are attaching to the policy and the same that Users, applications, and services may assume Roles. The roles can be used temporally for different reasons.

Considering DR Alarms users, it is necessary set up in this case **2 IT administrator Users** and place them in an **Administrator group** to allow to use the services and resources of AWS. This group will carry the policy that granted permission to the users contain in the Group. The next steps will show how to create the group attach the policy and add the users to that group.

- **Go to the IAM dashboard** - User groups -Create the group – attach policy.



- **Add the user.**
  - **Click On user in the IAM dashboard and add user.**
  - **Name the new users – mark AWS management console access to create a password.**
  - **Add the user to the group – next.**
  - **Add tag – next.**
  - **Check – create user.**
  - **Download credentials and send to the new users.**

The screenshot shows the AWS IAM 'Add user' wizard. Step 1: 'Add user' button highlighted. Step 2: 'User' selected in the left sidebar. Step 3: 'Administrator1' selected in 'User name'. Step 4: 'Programmatic access' checked. Step 5: 'AWS Management Console access' checked. Step 6: 'AdministratorAccess' policy attached. Step 7: 'AdministratorGroup' selected. Step 8: 'DfAlams' tag added. Step 9: 'Download key' button highlighted.

**5. Add New users to the group that was created - Next**

**7. Check - Next**

**6. Add Tag to identify New users in a category - Next**

**8. Download credentials and Close**

**9. Send the credential to new users**

To create a user with non-administrative access but allow to connect the instance.

- **Create a group and policy and create a user within this group.**

The policy I create was EC2instanceconnect which just allow to connect the user to the instance.

The screenshot shows the AWS IAM 'Add user' wizard for a non-administrative user. Step 1: 'Add user' button. Step 2: 'User' selected in the left sidebar. Step 3: 'Administrator1C2Instance' selected in 'User name'. Step 4: 'Programmatic access' checked. Step 5: 'AWS Management Console access' checked. Step 6: 'None' selected in 'Groups'. Step 7: 'EC2instanceConnect' policy attached. Step 8: 'AdministratorEC2Instances' group selected. Step 9: 'AdministratorEC2Instances' user listed in the group.

- **Results**

Every group with its policy and the Administrators can access to the resources.

Summary

[Delete user](#) [?](#)

User ARN: arn:aws:iam::269021346461:user/Administrator1  
Path: /  
Creation time: 2021-04-22 18:12 UTC+1000

Permissions | Groups (1) | Tags (1) | Security credentials | Access Advisor

▼ Permissions policies (2 policies applied)

Add permissions [Add inline policy](#)

Policy name	Policy type
IAMUserChangePassword	AWS managed policy
AdministratorAccess	AWS managed policy from group AdministratorsGroup

IAM > User groups > InstanceConnect

InstanceConnect

[Delete](#)

Summary [Edit](#)

User group name: InstanceConnect  
Creation time: April 25, 2021, 17:08 (UTC+10:00)  
ARN: arn:aws:iam::269021346461:group/InstanceConnect

Users | **Permissions** | Access advisor

Permissions policies (1) [Info](#)  
You can attach up to 10 managed policies.  
[Filter policies by property or value](#)

Add permissions [Simulate](#) [Remove](#) [Add permissions](#)

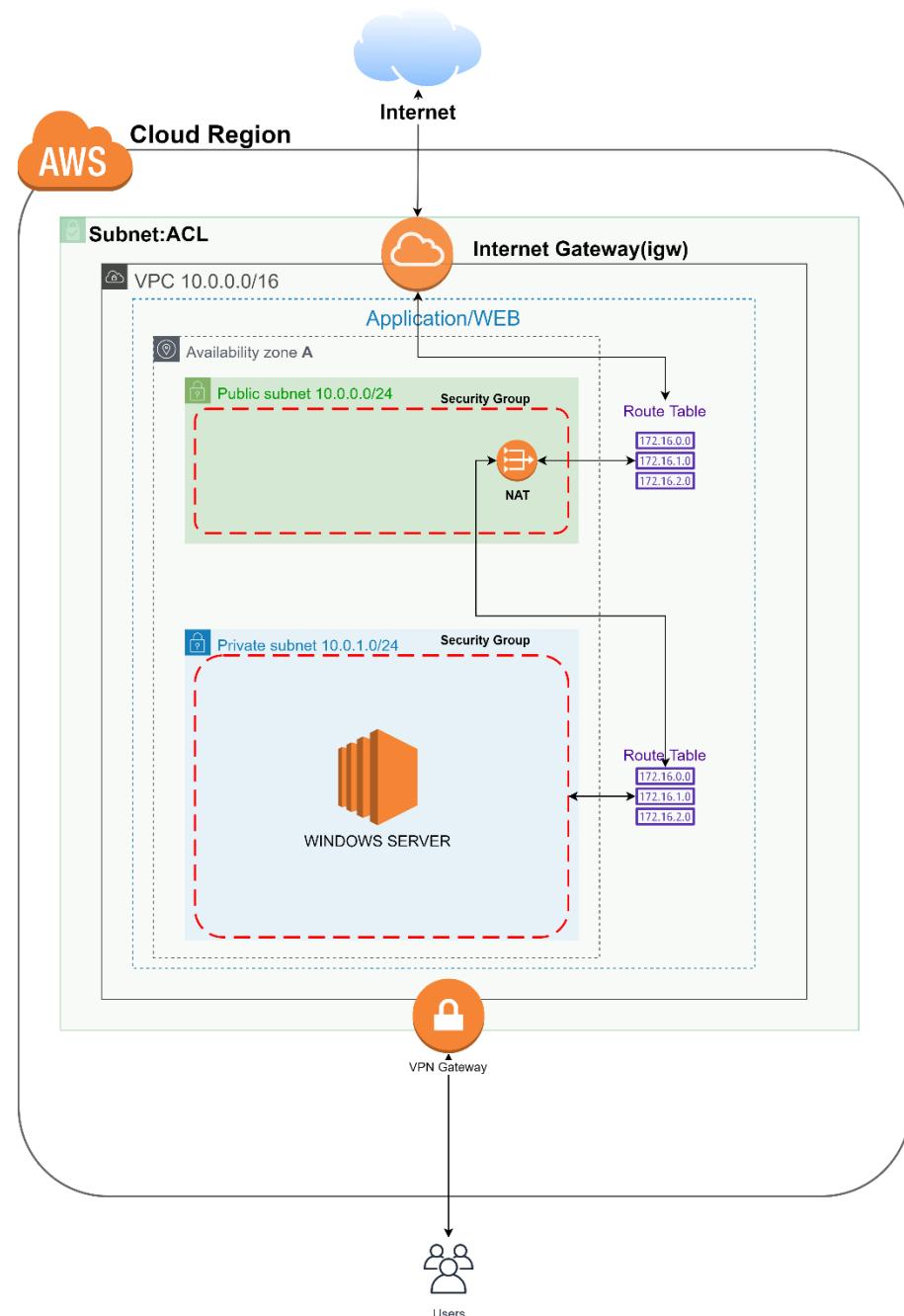
Policy Name	Type	Attached entities
EC2InstanceConnect	AWS managed	1

Every USER appears in the user panel where it shows every feature and user configuration. Therefore, policies and permissions can be added to individual user, control credentials, access keys and other features.

To create a user with non-administrative access just add the policy to user who will not have the permission.

## 4. A Windows server in the private subnet.

After creating a secure environment to use launch the instance now it is possible to create instances in Public and Private subnets. Now a windows server will be created in a private subnet allow access to DR alarms IT admin, the next diagram and steps will show how to create a EC2 instance in a private subnet.



## 4.1. Create a EC2 instance

- **Launch an instance** – click on instances in the EC2 dashboard and click in launch instances.
- The launch instance – **Choose and Amazon machine** – in this case windows server and select.
- **Choose an instance Type** - Select a free tier -next configure instance details.
- **Configure instance** – Locate the instance in the VPC created – locate the instance in a private subnet – and enable (allocate Elastic IP at the end of the process)
- **Add storage** – choose storage for your Instance.
- **Add Tag** – Name the Instance
- **Configure Security Group** – Rules Inbound and Outbound traffic

The screenshot shows the AWS EC2 instance creation process across several tabs:

- Step 1: Choose an Amazon Machine Image (AMI)** (highlighted in red box 1): Shows the AMI selection screen where "Microsoft Windows Server 2019 Base - ami-093c81578872c5d" is selected. A note indicates it's a "Free tier eligible" AMI.
- Step 2: Choose an Instance Type** (highlighted in red box 2): Shows the instance type selection screen where "t2.micro" is selected. A note indicates it's a "Free tier eligible" instance type.
- Step 3: Configure Instance Details** (highlighted in red box 3): Shows the instance configuration screen. A note says "Select the VPC" (highlighted in red box 4). Other fields include Network (subnet-0ef19a29bfb109), Auto-assign Public IP (selected), and IAM role (None).
- Step 4: Add Storage** (highlighted in red box 5): Shows the storage configuration screen where "Root" volume is set to "General Purpose SSD (gp2)" with 30 GiB.
- Step 5: Configure Security Group** (highlighted in red box 6): Shows the security group configuration screen. A note says "Create the SG with the rules" (highlighted in red box 7). The security group is named "DRA-JP-PrivateSubnet-5G" and contains three rules for HTTP, TCP port 80, and TCP port 443.
- Step 6: Configure Security Group** (highlighted in red box 8): Shows the security group configuration screen with a warning about allowing all IP addresses.
- Step 7: Review and Launch** (highlighted in red box 9): Shows the final review screen before launching the instance.

- **Create or choose a key pair** – the users allow to access to AWS have access key for the instances previously created in Identity and Access Management (IAM)

**Step 7: Review Instance Launch**

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete this launch process.

**AMI Details**

Microsoft Windows Server 2019 Base - ami-0f93c815788872c5d  
Free tier eligible Microsoft Windows 2019 Datacenter edition. [English]  
Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#).

**Instance Type**

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)
t2.micro	-	1	1	EBS only

**Security Groups**

**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**  
EC2-SEBAS-Instance

I acknowledge that I have access to the selected private key file (EC2-SEBAS-Instance.pem), and that without this file, I won't be able to log into my instance.

**11. Create a Key pair or use a existing one**

**Launch Instances**

- **Create and associate an Elastic IP address** – IP address is keeping attach to the instance.

**Associate Elastic IP address**

Choose the instance or network interface to associate to this Elastic IP address (34.234.181.2)

**Elastic IP address: 34.234.181.2**

**Resource type**  
Choose the type of resource with which to associate the Elastic IP address.  
 Instance  
 Network interface

**Instance**  
i-01250458e20a6b04a

**Private IP address**  
The private IP address with which to associate the Elastic IP address.  
10.0.1.151

**Reassociation**  
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.  
 Allow this Elastic IP address to be reassigned

**Associate**

- Check and access to the instance – Access to the instance and start to use it.

**Make sure that all preview set up it all in order**

**Elastic IP Association (VPC-Subnet-SG)**

Public IPv4 address: 34.234.181.2 [DRA-ELIP-WI-PrivateSubnet] [open address]

Private IP addresses: 10.0.1.151

Public IPv4 DNS: ip-10-0-1-151.ec2.internal

VPC ID: vpc-0cf85d469b52d47e1 (DRA-VPC-01)

Subnet ID: subnet-0ee519a28fsb61c99 (DRA-PrivateSubnet-ZA)

**Security details**

IAM Role: -

Owner ID: 269021346461

Launch time: Thu Apr 22 2021 15:19:38 GMT+1000 (Australian Eastern Standard Time)

Security groups: sg-009f9ee70497049e1 (DRA-WI-PrivateSubnet-SG)

Inbound rules:

**Connect to instance**

Session Manager | RDP client | EC2 Serial Console

**2**

You may not be able to connect to this instance as ports 3389 may need to be open in order to be accessible. The current associated security groups don't have ports 3389 open.

Download remote desktop file

**3**

When prompted, connect to your instance using the following details:

Public IP: 34.234.181.2 User name: Administrator

Administrator Password copied: XwpZze9ion

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

**Windows Security**

Enter your credentials

These credentials will be used to connect to 34.234.181.2.

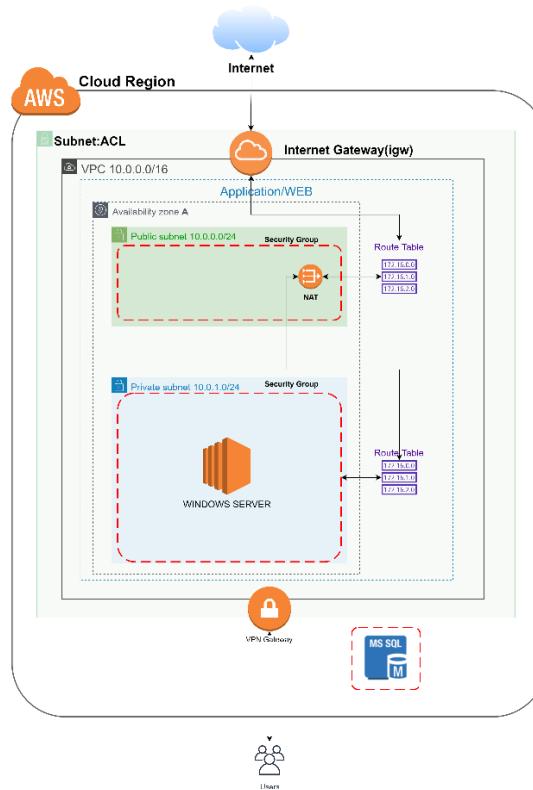
Administrator

OK Cancel

## 5. Database instance

To set up a RDS instance const of two big steps, Create a DB instance and Create a EC2 Instance to connect the instance with the application such a web site (Amazon Web Services, 2021a). The next diagram and steps will show how to create a DB instance and connection.

### 5.1. Create DB instance RDS.



- Type RDS on top in AWS manage console.
- Go to databases - create databases.

A screenshot of the AWS RDS management console. The left sidebar shows 'Databases' selected. The main area is titled '1. Type RDS'. It features a search bar, a 'Create database' button, and a table for managing databases. The table has columns for 'DB identifier', 'Role', 'Engine', 'Region & AZ', 'Size', and 'Status'. A red box highlights the 'Create database' button, and a red number '3' is placed above the table.

- **Chose the database that you want to create.**
  - The settings can be varied between, versions, license, storage capacity, autoscaling control, and connectivity that allow to locate the DB within our VPC or in AWS region. this important to know where the database is (Chef, 2020).
- **Name the database.**
- **Create a master user and its password.**
- **Create data base.**

**5**

**6. Choose the data base**

**Configuration**

Engine type: Microsoft SQL Server

DB instance size: Free tier

DB instance identifier: DRALarms-DBSQLM

Master username: Administrator1

Master password: \*\*\*\*\*

Confirm password: \*\*\*\*\*

**7. This set up is the basic but clicking in standard create you can manipulate the setting for the DB**

**8**

**9**

**Create database**

- Wait until it is created and get the Endpoint & port (this port must be open in the security group in the instance that we want to connect to the DB)

The screenshot shows two main views of the AWS RDS console.

**Left View (Dashboard):**

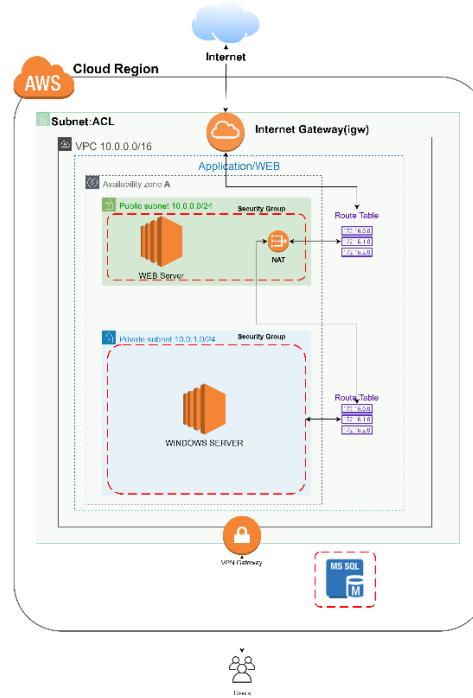
- Amazon RDS Services menu.
- Databases section (highlighted with a red box labeled 1).
- DB identifier: dalarms-db (highlighted with a red box labeled 2).
- DB identifier: dalarms-dbsqlm (highlighted with a red box labeled 3).

**Right View (Database Configuration):**

- RDS > Databases > dalarms-dbsqlm.
- Summary:**
  - DB identifier: dalarms-dbsqlm
  - CPU: 9.52%
  - Status: Available
  - Engine: SQL Server Express Edition
  - Region & AZ: us-east-1c
  - Class: db.t2.micro
- Connectivity & security:**
  - Endpoint & port:
    - Endpoint: dalarms-dbsqlm.cnzbseovat7.us-east-1.rds.amazonaws.com
    - Port: 1433
  - Networking:
    - Availability zone: us-east-1c
    - VPC: Default-VPC (vpc-d32eaaae)
    - Subnet group: default-vpc-d32eaaae
    - Subnets:
      - subnet-2f2dec8d3
      - subnet-25cbe92b
      - subnet-92c5ad74
      - subnet-14c0f1f6
      - subnet-0cc0b551
      - subnet-14cdff59
  - Security:
    - VRIC security groups: default (sg-096cab89) (active)
    - Public accessibility: No
    - Certificate authority: rds-ca-2019
    - Certificate authority date: Aug 23rd, 2024

## 5.2. Create EC2 instance to connect DB Instance.

The next step is to create a EC2 instance in a public subnet to connect DR Alarm's WEB site the DB instance that was created.



- Create the instance such as was done in the module 4 – chose public subnet- and allocate an elastic IP.

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

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**

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**

1. Select the VPC

2. Select Public Subnet

3. Select enable and after launch the instance allocate Elastic IP to hold the IP to this Instance

**Step 4: Add Storage**

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**

Create the SG with the rules

1. Choose AMI

2. Choose Instance Type

3. Configure Instance

4. Add Storage

5. Add Tags

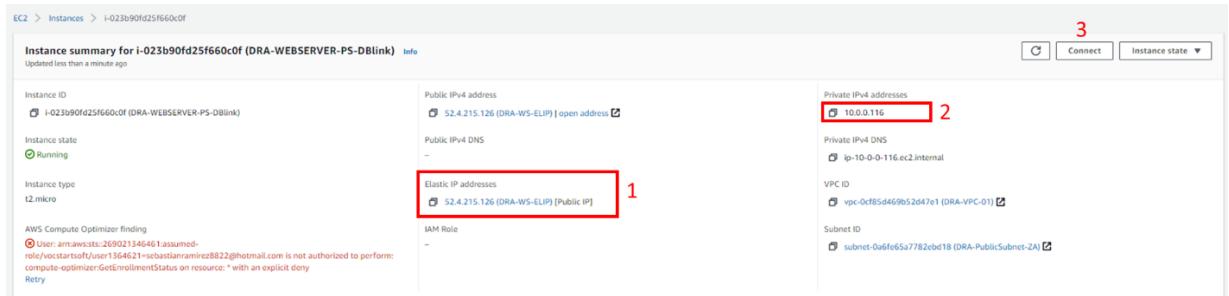
6. Configure Security Group

7. Review

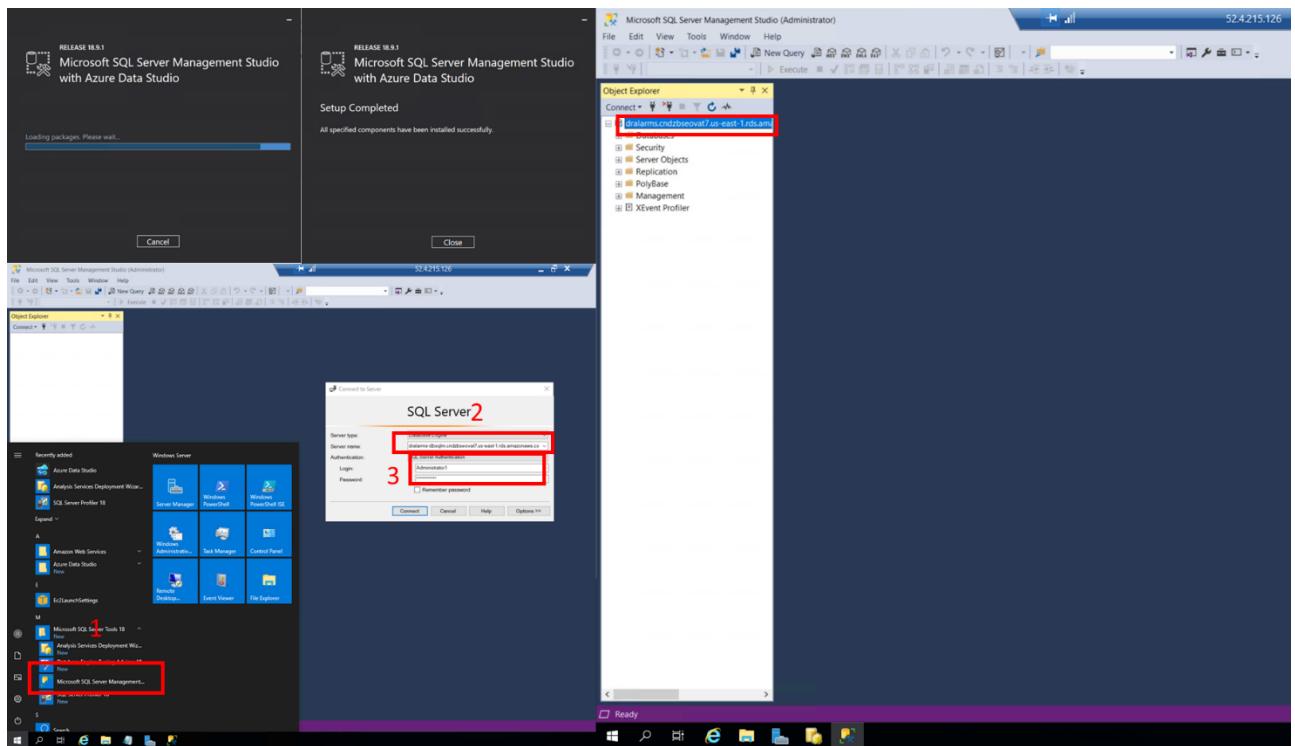
8. Review and Launch

9. Next: Add Storage

- Check setup and Connect.

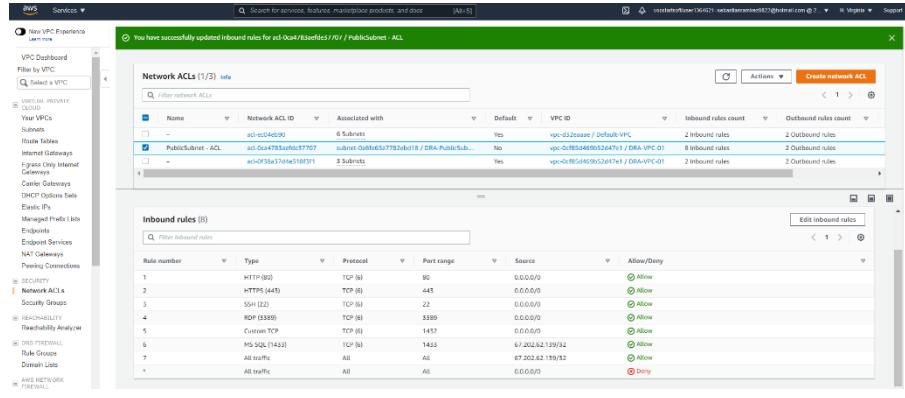
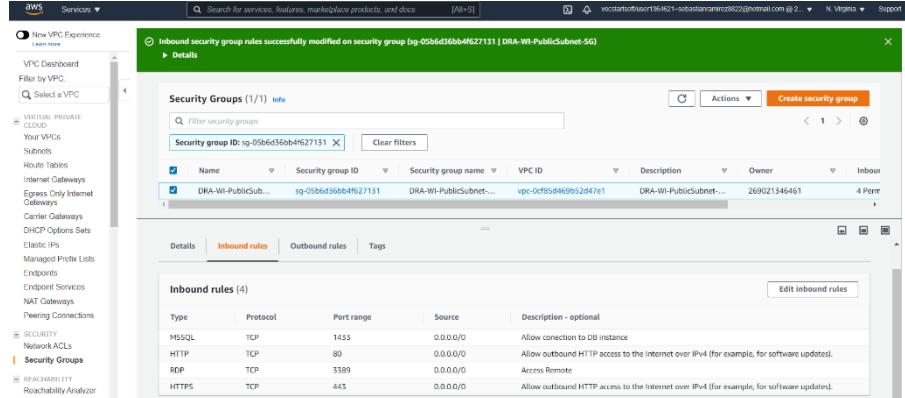


- Install from Microsoft.com – download the Microsoft server management studio– open and put the Endpoint – Master Username and password used in the step above. (it is recommendable use a semicolon after server name example dralarms.cndzbseovat7.us-east-1.rds.amazonaws.com, 1433)



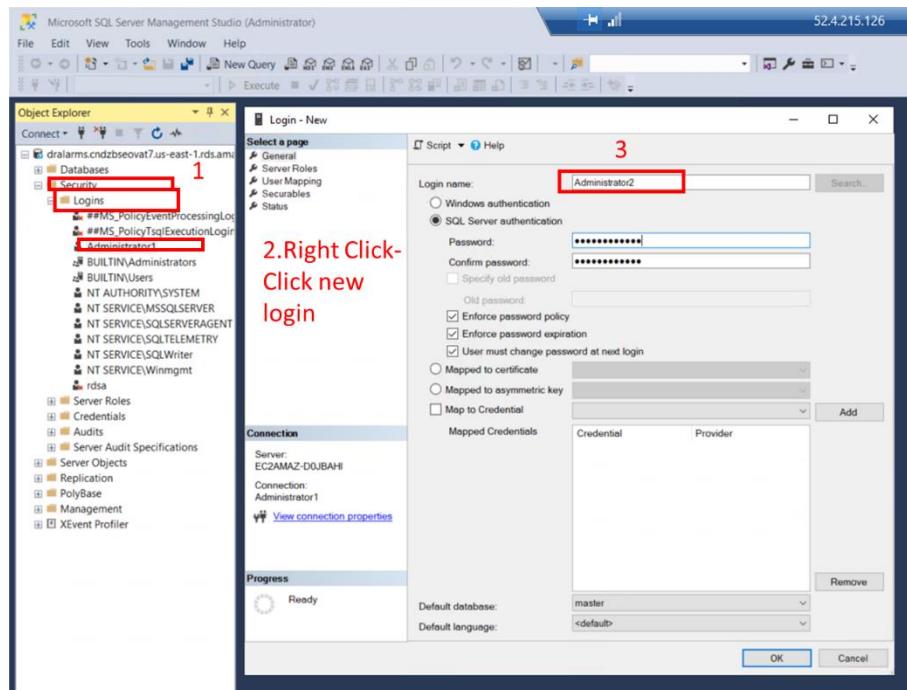
## Troubleshooting

At the first time when I try to connect the RDS MS SQL to the Instance in my public subnet, I could not to connect it. So, the troubleshooting that I did was check if I was correctly configuring the connection. I found I was not placing a comma "," and the port after the Endpoint, after that it still cannot connect, so I allow all traffic From SG and ACL and finally could connect it, but I thought it is not secure. Now, I decided to see which ports are open and see what it is the difference allowing all traffic and just allowing the 1433 port to connect the RDS instance. I found that the IP, I decide to allow all traffic coming from the RDS instance to that specific IP(amazon Web Services, 2021d).

<p>Netstat -n (ao/aon) command in CMD EC2 instance to see the connections and port open</p>	<p><b>Active Connections</b></p> <table border="1"> <thead> <tr> <th>Proto</th> <th>Local Address</th> <th>Foreign Address</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>TCP</td> <td>10.0.0.116:3389</td> <td>101.165.86.248:51381</td> <td>ESTABLISHED</td> </tr> </tbody> </table> <p>C:\Users\Administrator&gt; netstat -n</p> <p><b>Active Connections</b></p> <table border="1"> <thead> <tr> <th>Proto</th> <th>Local Address</th> <th>Foreign Address</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>TCP</td> <td>10.0.0.116:3389</td> <td>101.165.86.248:51381</td> <td>ESTABLISHED</td> </tr> <tr> <td>TCP</td> <td>10.0.0.116:50203</td> <td>67.202.62.139:1433</td> <td>TIME_WAIT</td> </tr> <tr> <td>TCP</td> <td>10.0.0.116:50204</td> <td>67.202.62.139:1433</td> <td>TIME_WAIT</td> </tr> <tr> <td>TCP</td> <td>10.0.0.116:50205</td> <td>67.202.62.139:1433</td> <td>ESTABLISHED</td> </tr> </tbody> </table>	Proto	Local Address	Foreign Address	State	TCP	10.0.0.116:3389	101.165.86.248:51381	ESTABLISHED	Proto	Local Address	Foreign Address	State	TCP	10.0.0.116:3389	101.165.86.248:51381	ESTABLISHED	TCP	10.0.0.116:50203	67.202.62.139:1433	TIME_WAIT	TCP	10.0.0.116:50204	67.202.62.139:1433	TIME_WAIT	TCP	10.0.0.116:50205	67.202.62.139:1433	ESTABLISHED																																													
Proto	Local Address	Foreign Address	State																																																																							
TCP	10.0.0.116:3389	101.165.86.248:51381	ESTABLISHED																																																																							
Proto	Local Address	Foreign Address	State																																																																							
TCP	10.0.0.116:3389	101.165.86.248:51381	ESTABLISHED																																																																							
TCP	10.0.0.116:50203	67.202.62.139:1433	TIME_WAIT																																																																							
TCP	10.0.0.116:50204	67.202.62.139:1433	TIME_WAIT																																																																							
TCP	10.0.0.116:50205	67.202.62.139:1433	ESTABLISHED																																																																							
<p><b>Network ACL</b></p>  <p>The screenshot shows the AWS VPC Network ACL configuration for a subnet. It displays two inbound rules:</p> <table border="1"> <thead> <tr> <th>Rule number</th> <th>Type</th> <th>Protocol</th> <th>Port range</th> <th>Source</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>HTTP (80)</td> <td>TCP (In)</td> <td>80</td> <td>0.0.0.0/0</td> <td>Allow</td> </tr> <tr> <td>2</td> <td>HTTPS (443)</td> <td>TCP (In)</td> <td>443</td> <td>0.0.0.0/0</td> <td>Allow</td> </tr> <tr> <td>3</td> <td>SSH (22)</td> <td>TCP (In)</td> <td>22</td> <td>0.0.0.0/0</td> <td>Allow</td> </tr> <tr> <td>4</td> <td>RDP (3389)</td> <td>TCP (In)</td> <td>3389</td> <td>0.0.0.0/0</td> <td>Allow</td> </tr> <tr> <td>5</td> <td>Custom TCP</td> <td>TCP (In)</td> <td>1433</td> <td>0.0.0.0/0</td> <td>Allow</td> </tr> <tr> <td>6</td> <td>MS SQL (1433)</td> <td>TCP (In)</td> <td>1433</td> <td>U-20.2.2.139/32</td> <td>Allow</td> </tr> <tr> <td>7</td> <td>All traffic</td> <td>All</td> <td>All</td> <td>0.0.0.0/0</td> <td>Deny</td> </tr> </tbody> </table>	Rule number	Type	Protocol	Port range	Source	Action	1	HTTP (80)	TCP (In)	80	0.0.0.0/0	Allow	2	HTTPS (443)	TCP (In)	443	0.0.0.0/0	Allow	3	SSH (22)	TCP (In)	22	0.0.0.0/0	Allow	4	RDP (3389)	TCP (In)	3389	0.0.0.0/0	Allow	5	Custom TCP	TCP (In)	1433	0.0.0.0/0	Allow	6	MS SQL (1433)	TCP (In)	1433	U-20.2.2.139/32	Allow	7	All traffic	All	All	0.0.0.0/0	Deny	<p><b>Security group Instance</b></p>  <p>The screenshot shows the AWS Security Group configuration for a security group. It displays four inbound rules:</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Protocol</th> <th>Port range</th> <th>Source</th> <th>Description - optional</th> </tr> </thead> <tbody> <tr> <td>MySQL</td> <td>TCP</td> <td>1433</td> <td>0.0.0.0/0</td> <td>Allow connection to DB instance</td> </tr> <tr> <td>HTTP</td> <td>TCP</td> <td>80</td> <td>0.0.0.0/0</td> <td>Allow outbound HTTP access to the internet over IPv4 (for example, for software updates).</td> </tr> <tr> <td>RDP</td> <td>TCP</td> <td>3389</td> <td>0.0.0.0/0</td> <td>Access Remote</td> </tr> <tr> <td>HTTPS</td> <td>TCP</td> <td>443</td> <td>0.0.0.0/0</td> <td>Allow outbound HTTPS access to the internet over IPv4 (for example, for software updates).</td> </tr> </tbody> </table>	Type	Protocol	Port range	Source	Description - optional	MySQL	TCP	1433	0.0.0.0/0	Allow connection to DB instance	HTTP	TCP	80	0.0.0.0/0	Allow outbound HTTP access to the internet over IPv4 (for example, for software updates).	RDP	TCP	3389	0.0.0.0/0	Access Remote	HTTPS	TCP	443	0.0.0.0/0	Allow outbound HTTPS access to the internet over IPv4 (for example, for software updates).
Rule number	Type	Protocol	Port range	Source	Action																																																																					
1	HTTP (80)	TCP (In)	80	0.0.0.0/0	Allow																																																																					
2	HTTPS (443)	TCP (In)	443	0.0.0.0/0	Allow																																																																					
3	SSH (22)	TCP (In)	22	0.0.0.0/0	Allow																																																																					
4	RDP (3389)	TCP (In)	3389	0.0.0.0/0	Allow																																																																					
5	Custom TCP	TCP (In)	1433	0.0.0.0/0	Allow																																																																					
6	MS SQL (1433)	TCP (In)	1433	U-20.2.2.139/32	Allow																																																																					
7	All traffic	All	All	0.0.0.0/0	Deny																																																																					
Type	Protocol	Port range	Source	Description - optional																																																																						
MySQL	TCP	1433	0.0.0.0/0	Allow connection to DB instance																																																																						
HTTP	TCP	80	0.0.0.0/0	Allow outbound HTTP access to the internet over IPv4 (for example, for software updates).																																																																						
RDP	TCP	3389	0.0.0.0/0	Access Remote																																																																						
HTTPS	TCP	443	0.0.0.0/0	Allow outbound HTTPS access to the internet over IPv4 (for example, for software updates).																																																																						

### 5.3. Create the second user access.

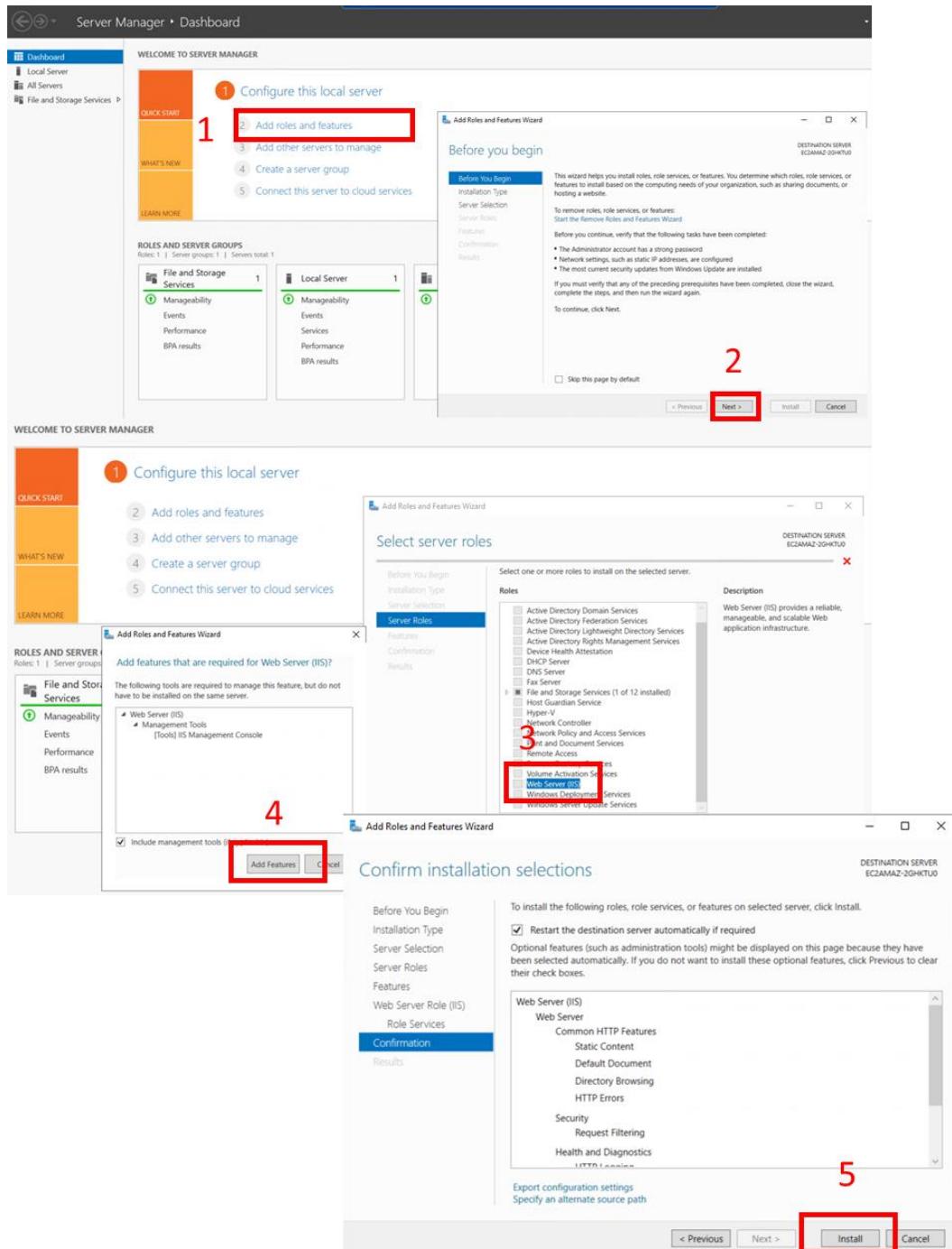
- The first user was created when the DB instance was created, now the second user will be created.
  - Inside database create the second user going **SECURITY – LOGINS – RIGHT** click and create new user.



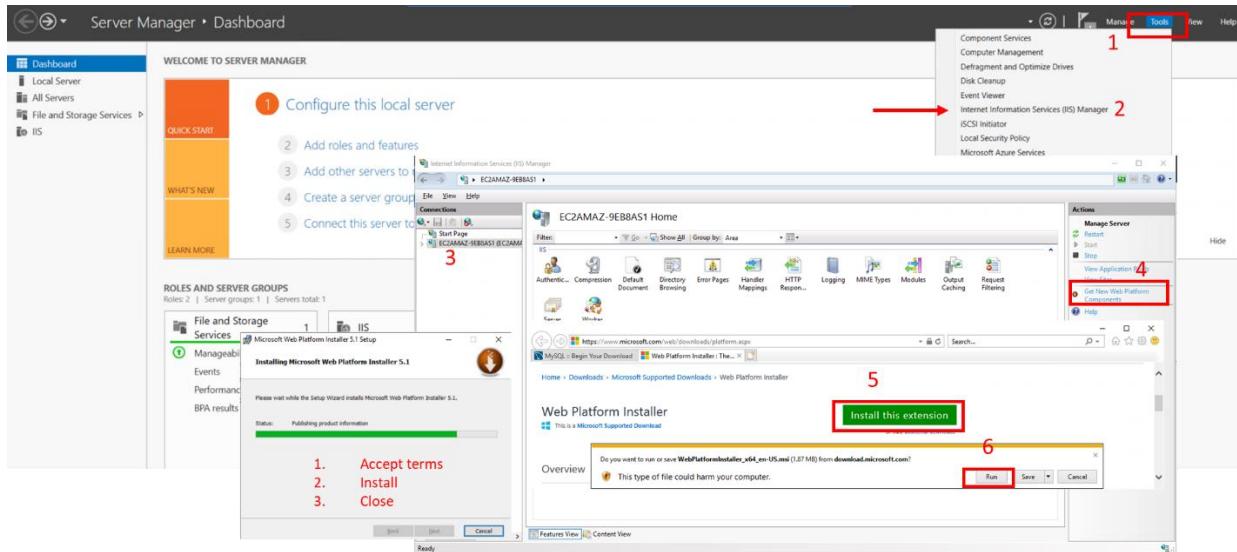
## 6. WordPress instance

To create a WordPress instance requires install the web server tools in a EC2 instance which it was created in the last module this instance has a SG with the ports 80 and 443 in a public subnet. To do this follow the next steps (Amazon Web Services, 2021j):

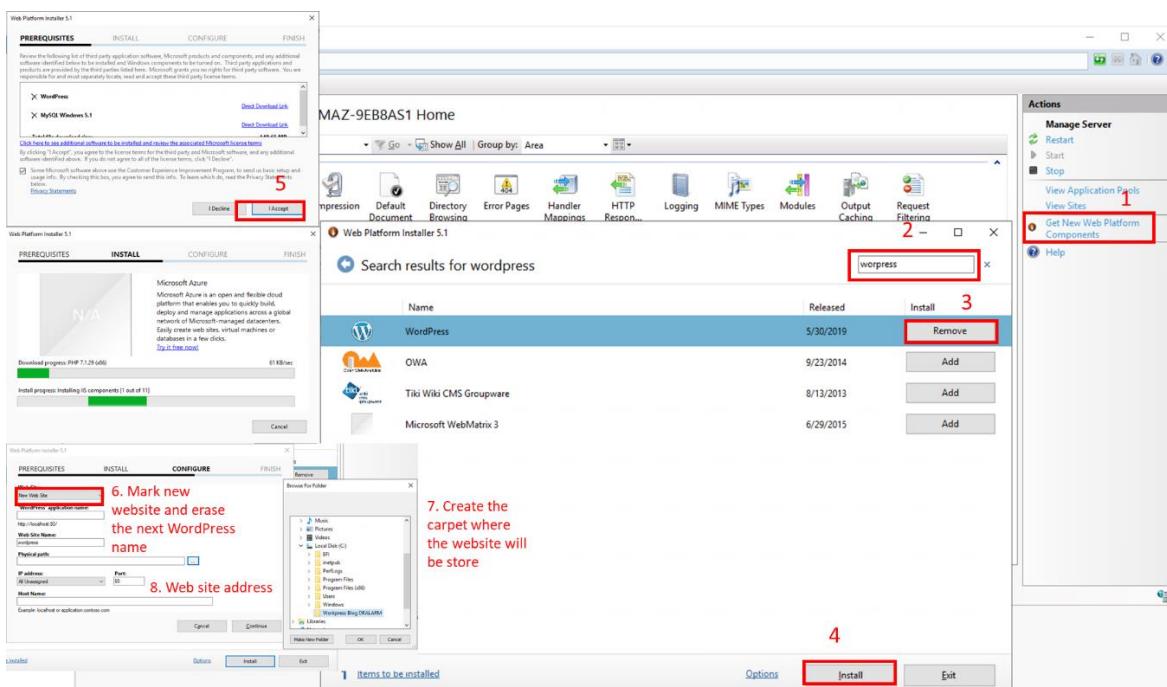
- **Install web server features.**
  - **Open server manager in the windows server instance**
  - **Click next until server selection.**
  - **Select web server (IIS) and next until Install the features.**



- **Download Web platform Installer.**
  - Go to tools on the top of server management – click.
  - Internet Information Services (IIS) Manager
  - Mark the connection
  - Get new web platform components.
  - Install extension from Microsoft website.



- **Install WordPress.**
  - Open web platform Installer
  - Search for WordPress – ADD – Install
  - Install prerequisites and accept the terms.
  - Set up the WordPress website – create a file where the website will be store.



## ○ Configuration host name

The image consists of six screenshots illustrating the configuration of a WordPress site:

- Screenshot 1:** Web Platform Installer 5.1 - **CONFIGURE** tab. The "Web Site" dropdown is set to "New Web Site". A red box highlights the "Host Name:" field, which contains "hisebasti.000webhostapp.com".
- Screenshot 2:** Web Platform Installer 5.1 - **CONFIGURE** tab. The "Host Name:" field is highlighted with a red box. The "Continue" button is visible.
- Screenshot 3:** Web Platform Installer 5.1 - **CONFIGURE** tab. The "Nonce Key" section is shown. A red box highlights the "Continue" button.
- Screenshot 4:** Web Platform Installer 5.1 - **FINISH** tab. It shows a success message: "The following products were successfully installed." A red box highlights the "Finish" button.
- Screenshot 5:** Browser screenshot showing the WordPress login page. The URL is "http://hisebasti.000webhostapp.com/wp-admin/install.php". The "Log In" button is highlighted with a red box.
- Screenshot 6:** Browser screenshot showing the WordPress login page. The URL is "https://hisebasti.000webhostapp.com/wp-login.php". The "Log In" button is highlighted with a red box.

## 7. Resources

Amazon Web Services, I. o. i. a. (2021a). *Amazon Relational Database Service*.

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide>Welcome.html>

Amazon Web Services, I. o. i. a. (2021b). *AWS Identity and Access Management*.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

Amazon Web Services, I. o. i. a. (2021c). *AWS Site-to-Site VPN*

[https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC\\_VPN.html](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html)

amazon Web Services, I. o. i. a. (2021d). Connecting to a DB instance running the Microsoft SQL Server database engine.

Amazon Web Services, I. o. i. a. (2021e). *Internet gateways*.

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html)

Amazon Web Services, I. o. i. a. (2021f). *NAT gateways*.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>

Amazon Web Services, I. o. i. a. (2021g). *NAT Instances*.

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_NAT\\_Instance.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html)

Amazon Web Services, I. o. i. a. (2021h). *Network ACLs*.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html>

Amazon Web Services, I. o. i. a. (2021i). *Route tables for your VPC*.

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Route\\_Tables.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html)

Amazon Web Services, I. o. i. a. (2021j). Tutorial: Deploy a WordPress blog on your Amazon EC2 instance running Windows Serve.

Amazon Web Services, I. o. i. a. (2021k). *VPCs and subnets*.

[https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Subnets.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html)

Center, A. T. (2020). *AWS Site To Site VPN - New video with improved steps*

<https://www.youtube.com/watch?v=5YvcyBecQts>

Chef, A. c. (2020). *HOW TO CREATE AND CONNECT TO MICROSOFT SQL SERVER DATABASE IN AWS*. [https://www.youtube.com/watch?v=hdWoQVgK\\_2Q](https://www.youtube.com/watch?v=hdWoQVgK_2Q)

Society, T. I. (2006). *Classless Inter-domain Routing (CIDR)*.  
<https://tools.ietf.org/html/rfc4632>