Session: 202130

Charles Sturt University

Cloud Computing

Assessment No.3

AWS Implementation

Case study

Submitted by:

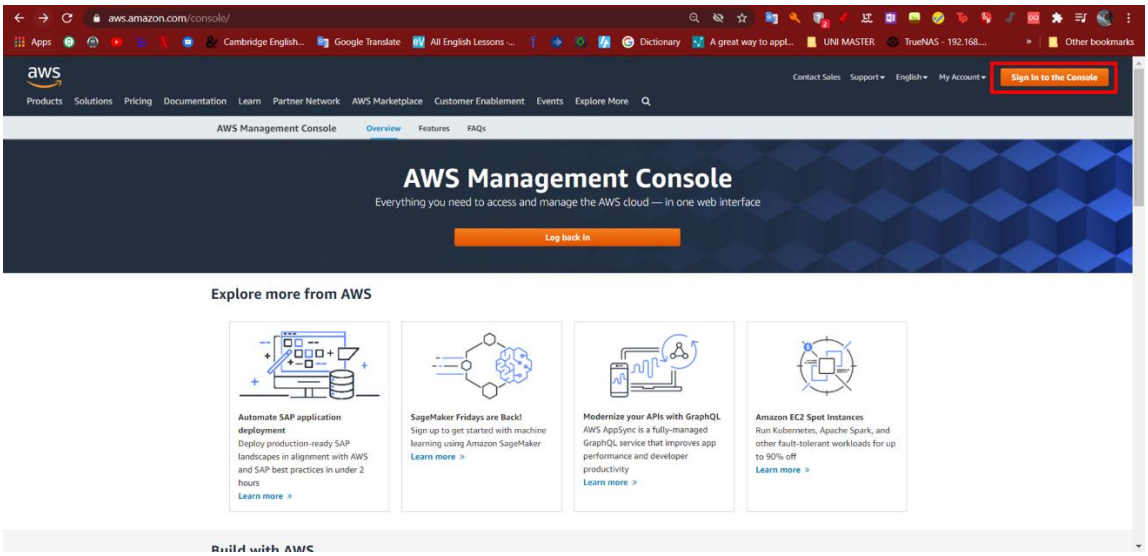
Johan Sebastian Ramirez Vallejo

Contents

1. Access DR alarms to AWS management Console

1.1. Steps AWS management Console

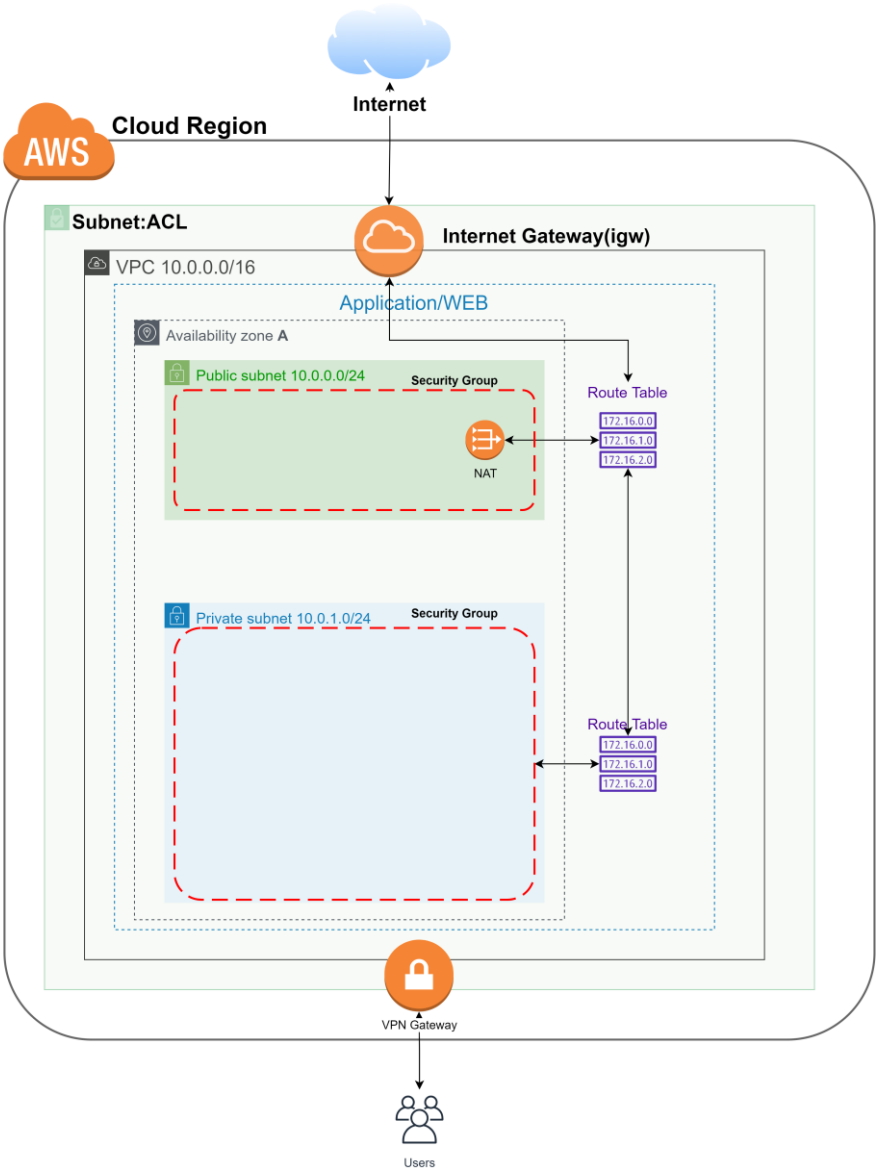
- Log in https://aws.amazon.com/console/ web site
    - The account must be setup before to access – This can be done for the consultant that allow the users in DR Alarms access to the platform with administrative access policy.



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).**

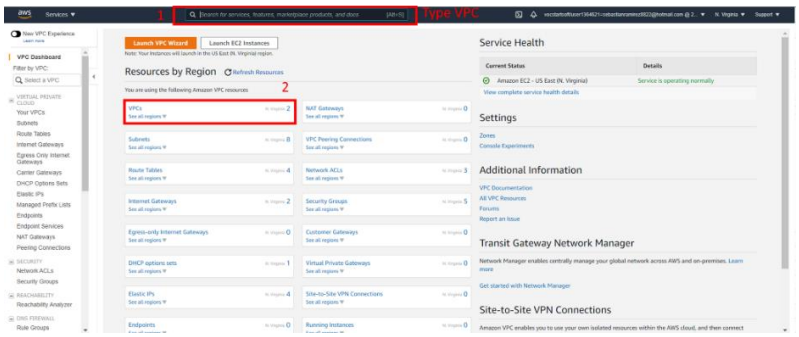
To secure the VPC are used two layers: **Network ACLs** and **Security groups** that act as Firewalls in this network. The next diagram will show the virtual public network created by DR alarms services.



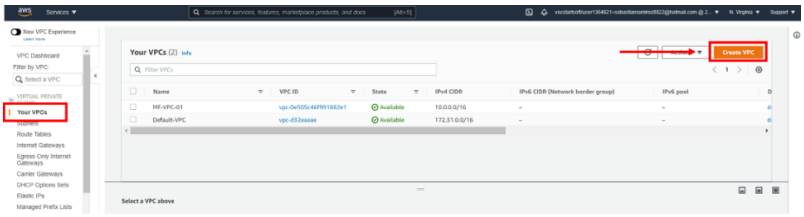
2.1. Create a VPC.

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).

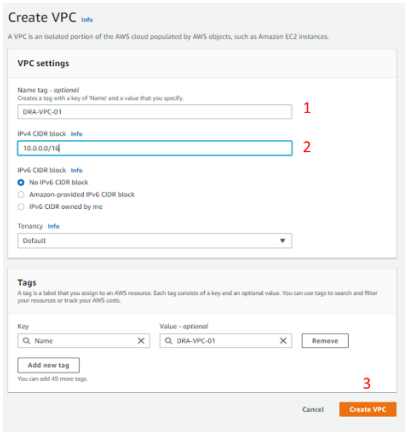
- **Open AWS VPC console**
  - Type VPC in the top search bar and select VPC.
  - On VPC dashboard click on VPC**.**



- **Create VPC**
  - Click on Create VPC



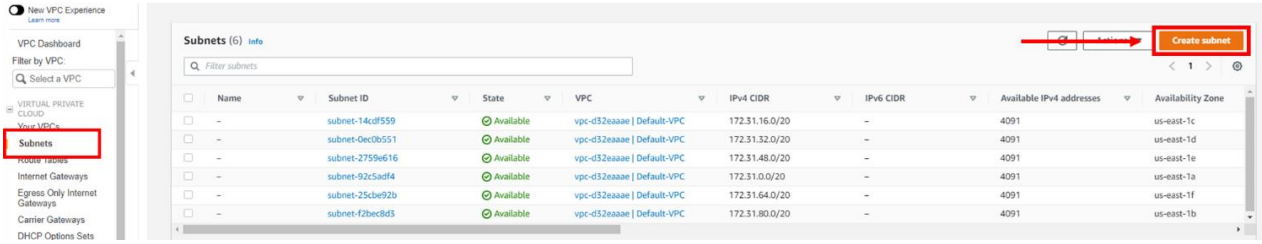
- **Settings VPC**
  - **Name tag** – represents the optional name for the VPC.
  - **IPv4 CIDR Block** – represents the IPv4 address **range** for the VPC, this means that the VPC need to be set as a higher legacy class (B) that is represented in CIDR notation 10.0.0.0/16 to see in detail follow next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



2.2. Create Private and Public Subnets

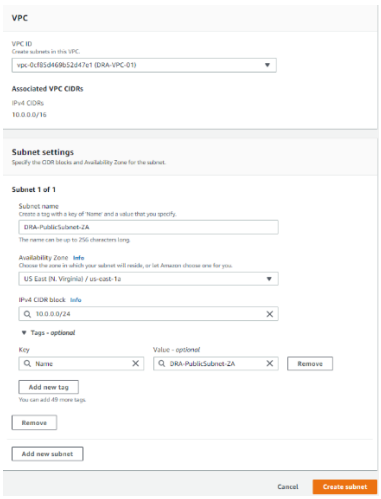
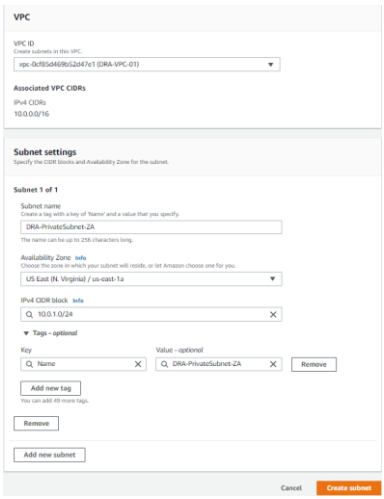
The next steps allow to create the subnets in an availability zone to provide the services (instances), they are interconnected, but logically separate to provide different type of services such us a website in a public subnet or database in a private subnet. The logically difference between them is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



- **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
	

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.

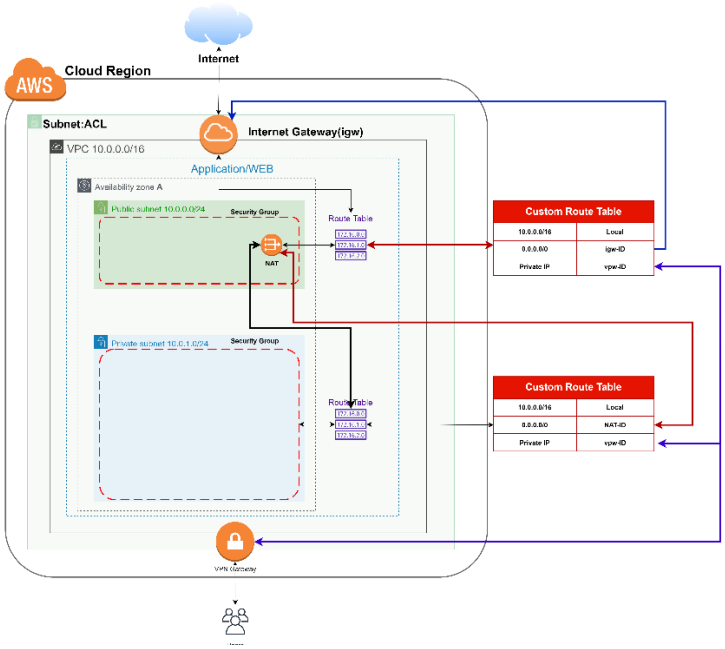
3.1. Security VPC: Route tables, Internet gateway, VPN gateway and NAT gateway

To secure DR Alarms requires route the traffic trough 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.

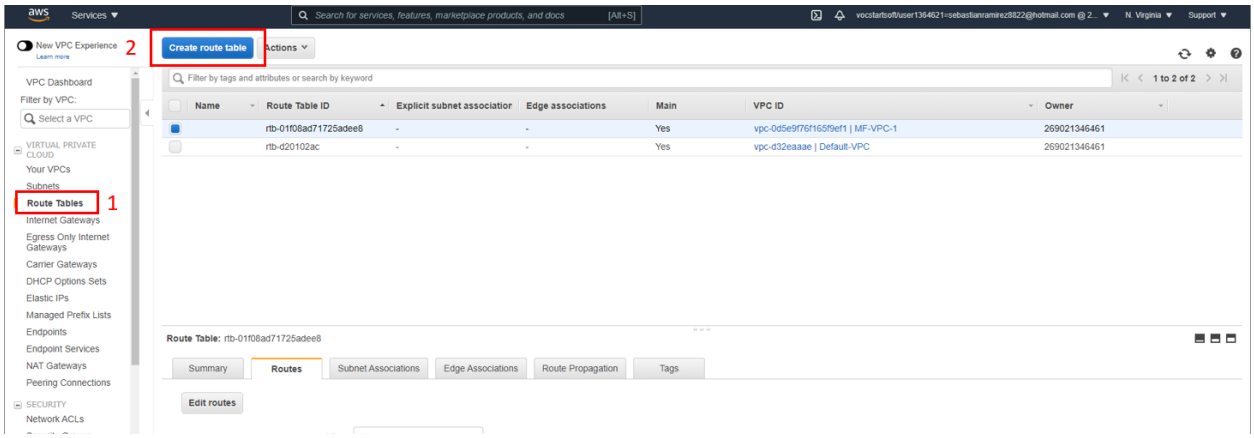
VPN gateway: it is required to a secure connection between costumer and AWS services, it was taken account in the design for DR Alarms, but AWS Educate account does not allow to create one.



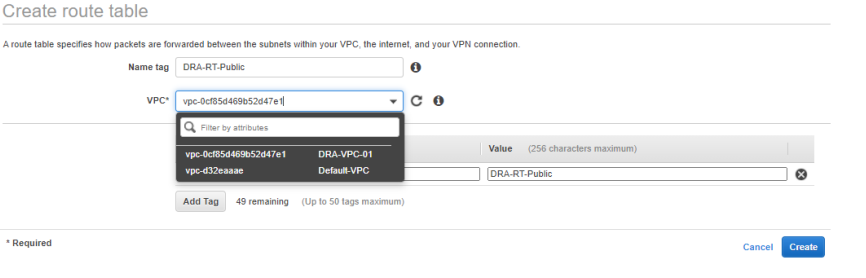
3.1.1. Route tables

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



- **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.**

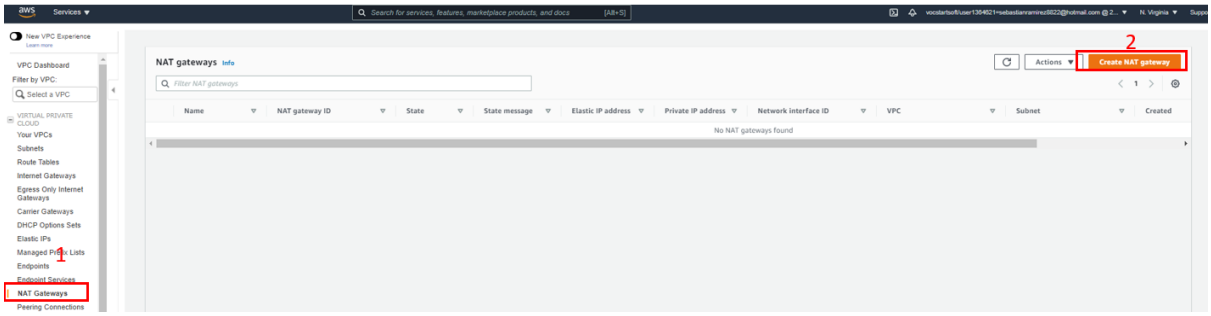
Route Table for the Private Subnet	
Route Table for the Public Subnet	

3.1.2. NAT gateway and NAT instances

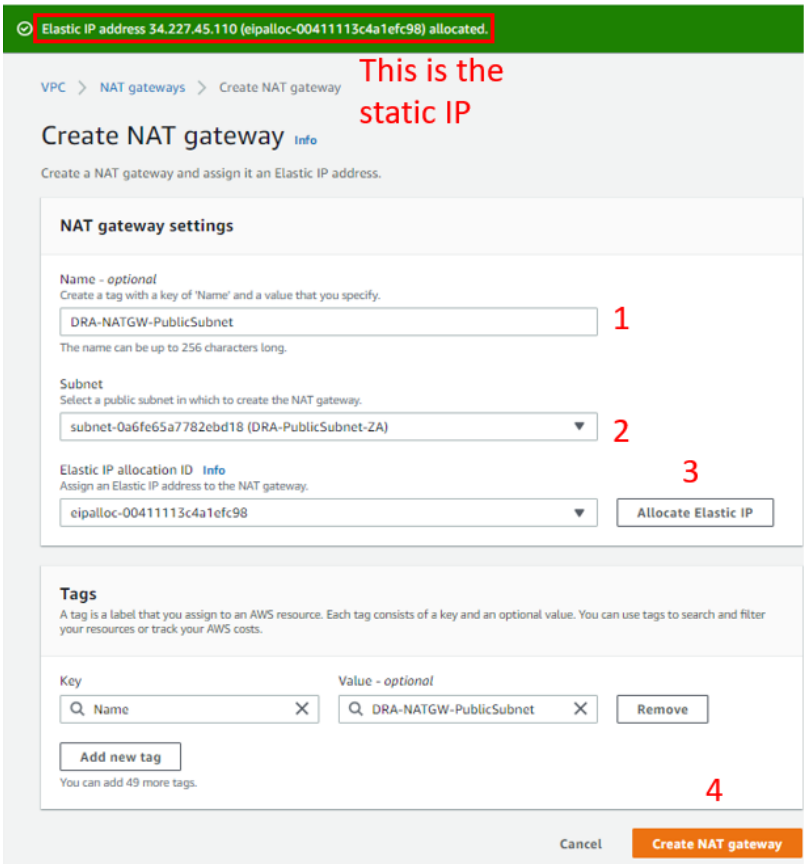
3.1.2.1. NAT gateway (it is not free)

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.**



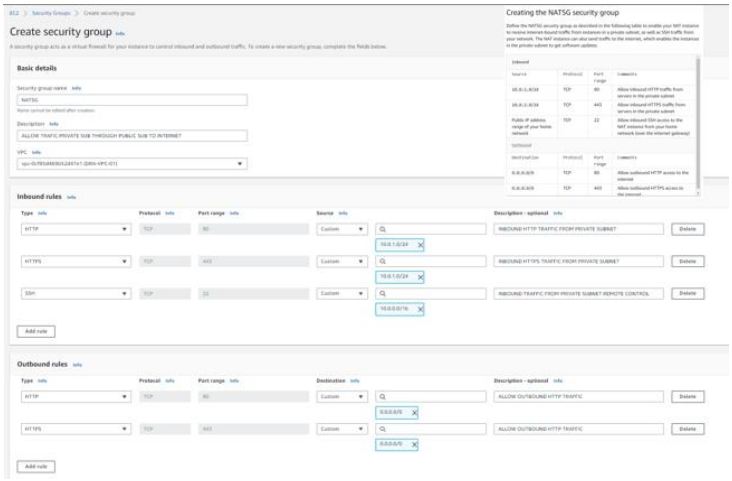
- **Create the NAT Gateway**
  - **Name –** Identification NAT gateway
  - **Subnet –** Chose the public subnet, because it is the subnet which is connected directly to the Internet.
  - **Elastic IP-** click in Allocate Elastic IP- it is necessary to stablish a static IP because a NAT works as a instance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



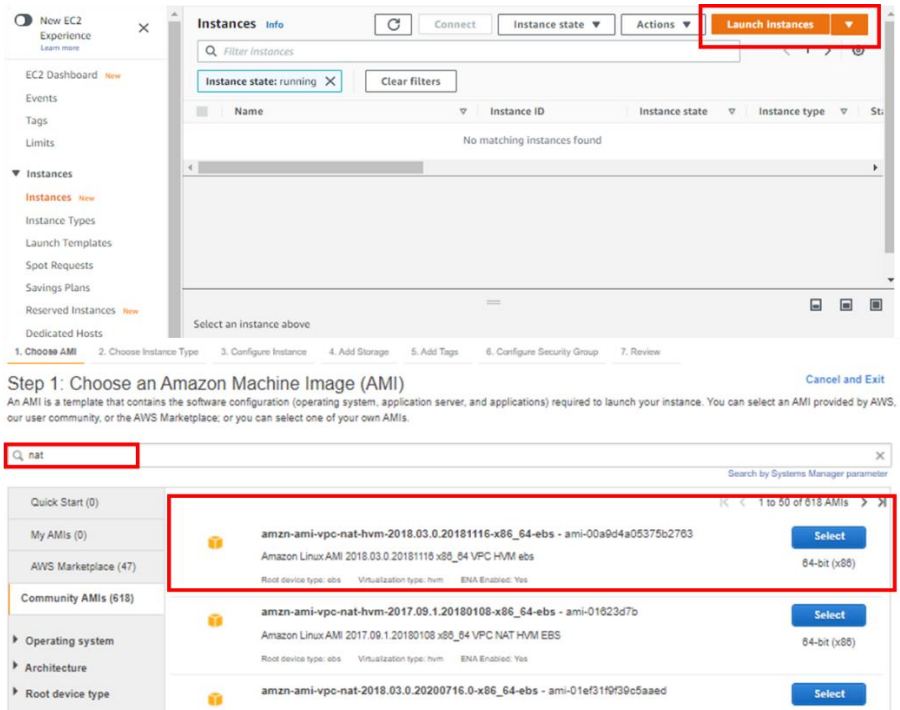
3.1.2.2. NAT Instance

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

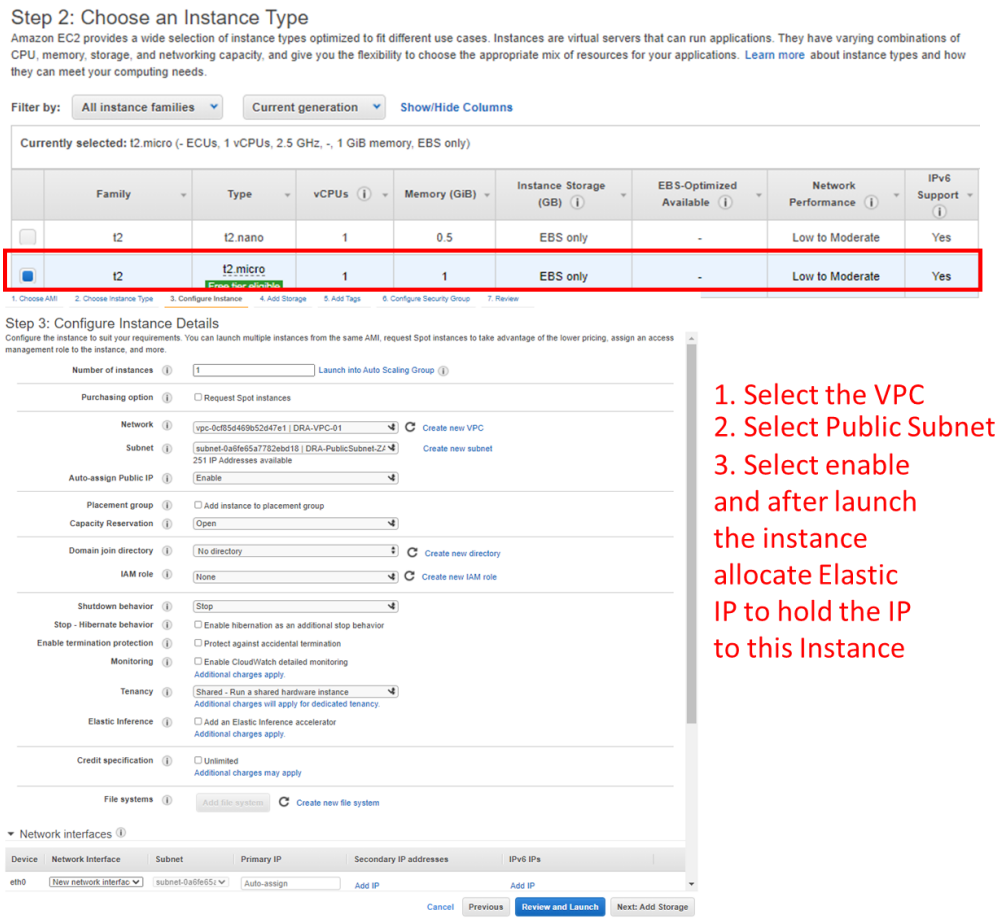
- **Create the Security group**
  - Select the ports to allow the traffic and point the inbound rules to the private subnet.
  - **Allow traffic from outbound** – notice that remote control port is not open.



- **Create the instance.**
  - Launch the instance

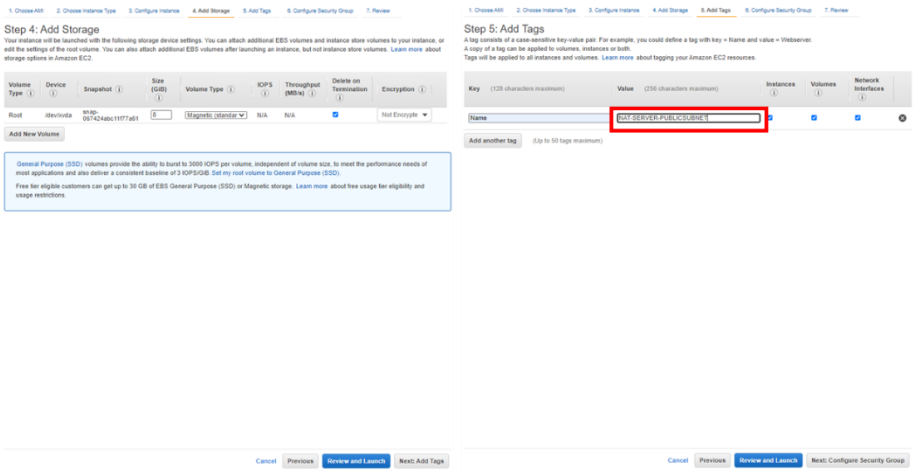


- In **community AMI** call a **NAT** and select

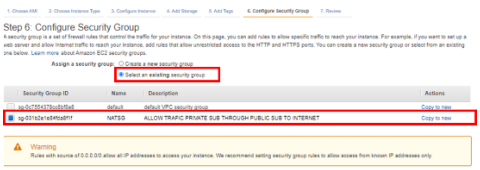


1. Select the VPC
2. Select Public Subnet
3. Select enable and after launch the instance allocate Elastic IP to hold the IP to this Instance

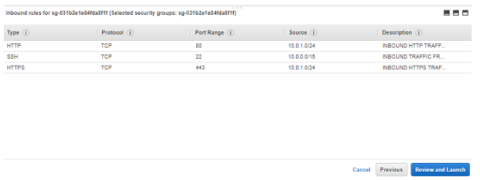
- **Next to add storage**(leave the default) and **Tag the Instance**



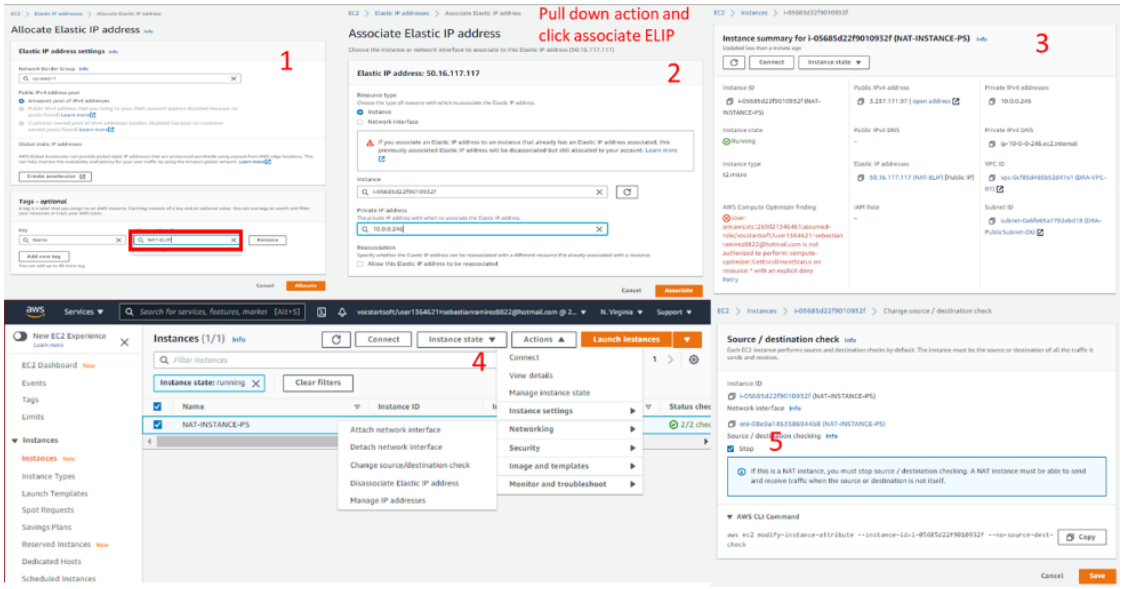
- **Select the security group that was created** – review and launch the instance.



Select the Security group that was created



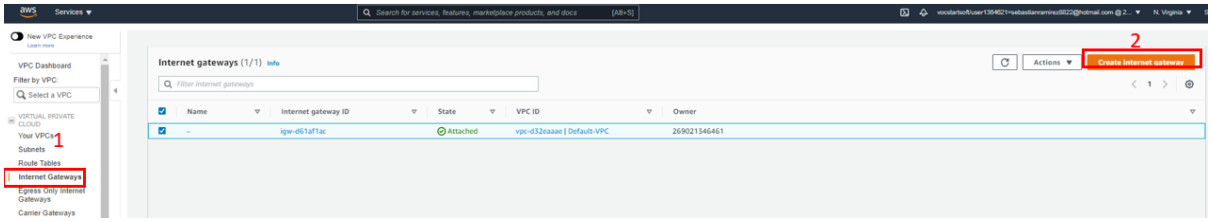
- **Setting the NAT instance in the network**
  - **Allocate Elastic IP address (Option is find in the EC2 dashboard left hand)** – it is necessary to allocate a static IP in the network to point the instance always to the same address.
  - **Associate Elastic IP address** – Assign the address to the 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.



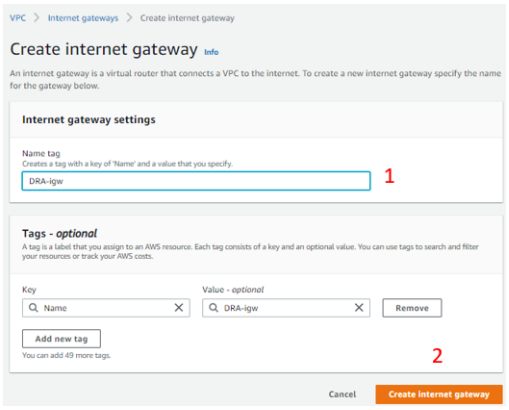
3.1.3. Internet gateway

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

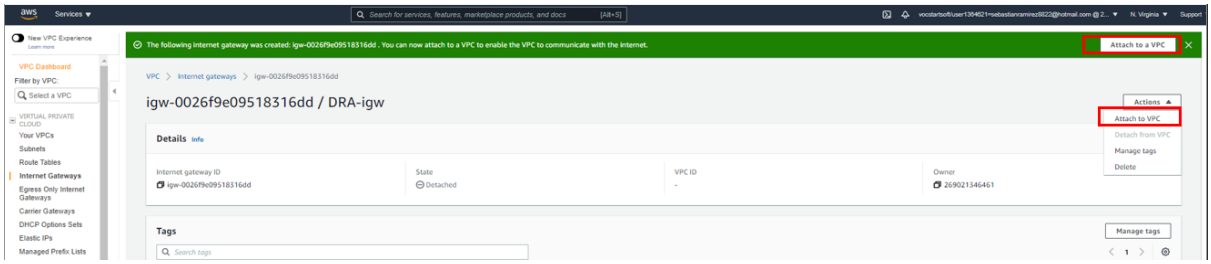
- **Click on Internet gateway in the VPC dashboard left hand.**



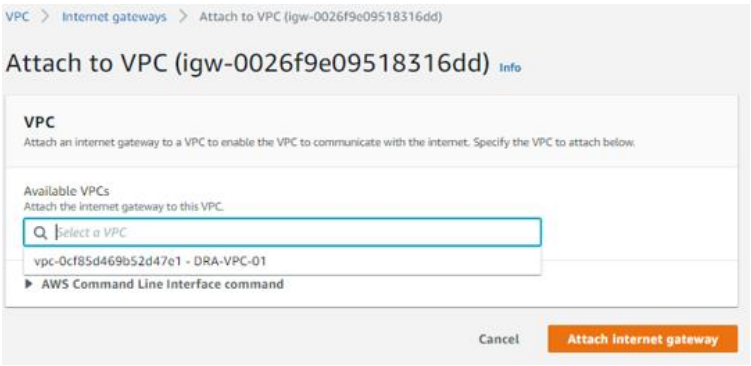
- **Create internet gateway.**
  - **Name tag** – identification for Internet Gateway



- **Attach internet gateway to VPC.**
  - Find to options after creatin an Internet gateway to attach to the VPC.

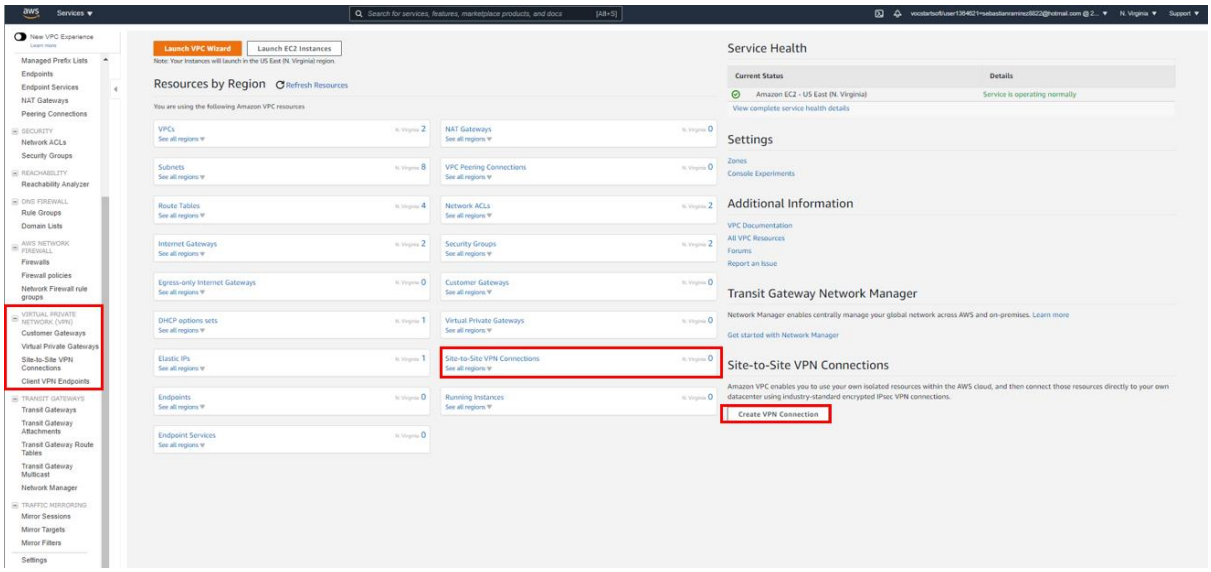


- **Select the VPC that was created.**
  - Attach internet gateway.



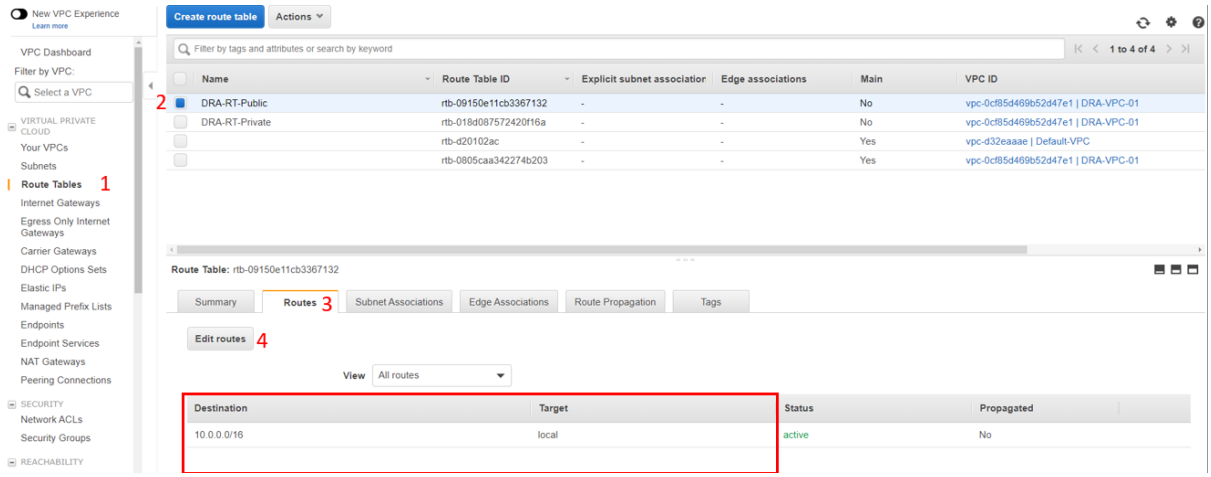
3.1.4. VPN gateway

- 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)**

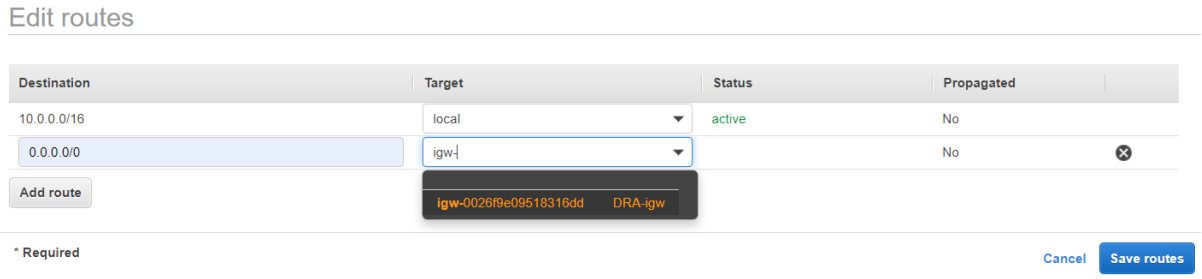


3.1.5. Association between Public and Private subnets, NAT gateway/NAT instance, and Internet gateway

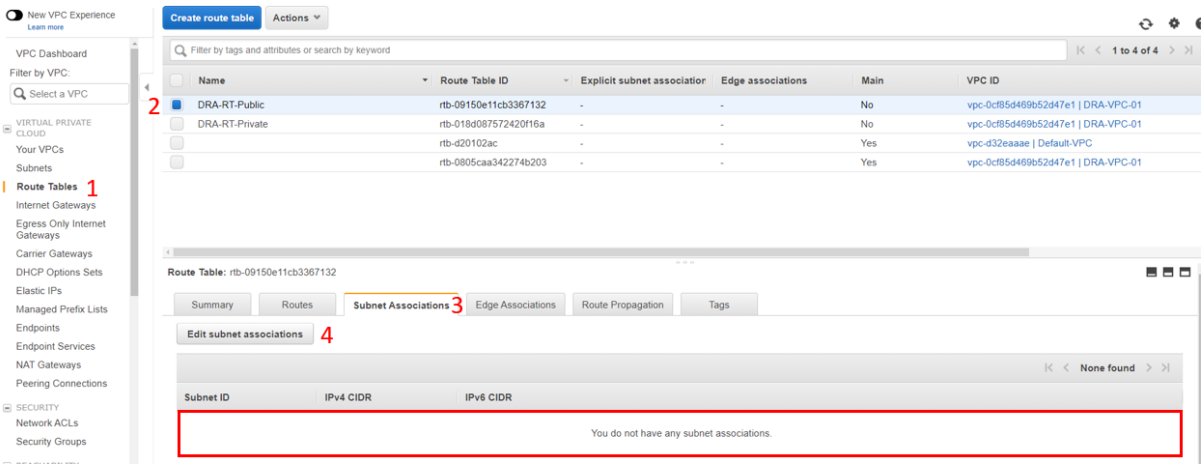
- **Public association**
  - The public association consist of to connect a route table pointed to the local network and internet network (refer to the diagram), **the VPN connection is simulated,** but it is connected through the route table.
  - **Click on Route tables in the left hand VPC dashboard.**
    - 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.



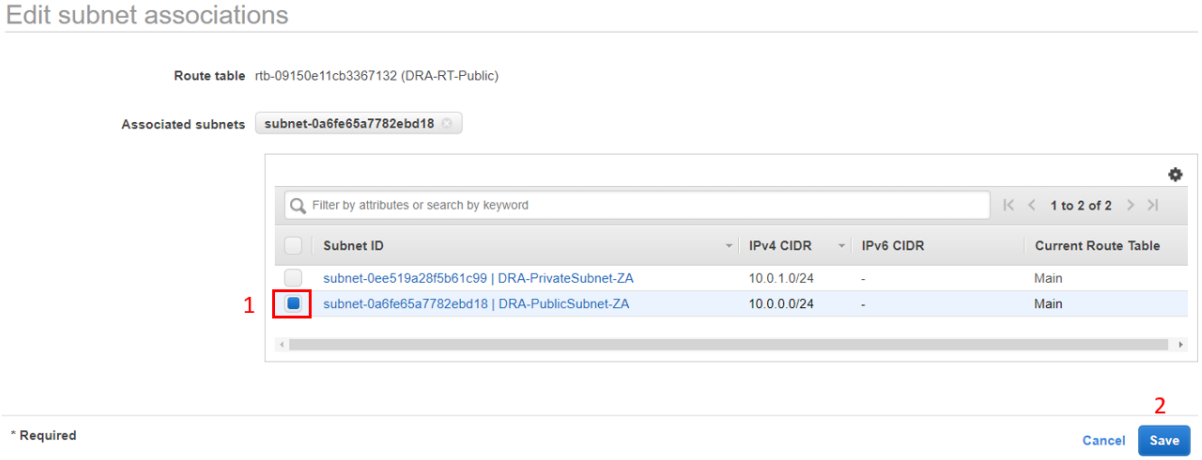
- **Click Edit routes –** create the route to traffic data through the Internet gateway that was created above – 0.0.0.0/0, which represents all IPv4 addresses. The target is the internet gateway that's attached to your VPC (Amazon Web Services, 2021i).
- **Select the igw and Save routes.**



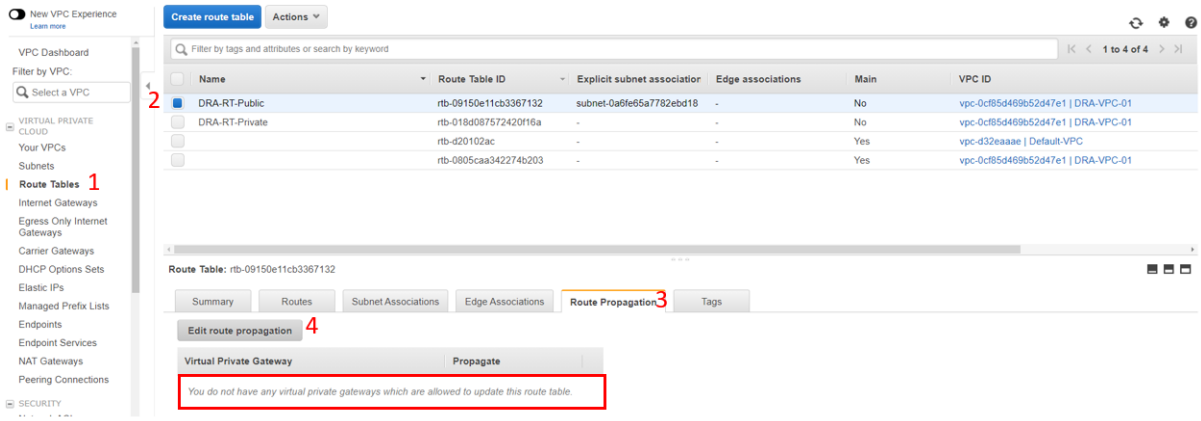
- **Subnet Associations – Edit subnet associations** which literally associate the public subnet to the public route table. Notice that the Public RT doe does not have any association. For default this is not associate



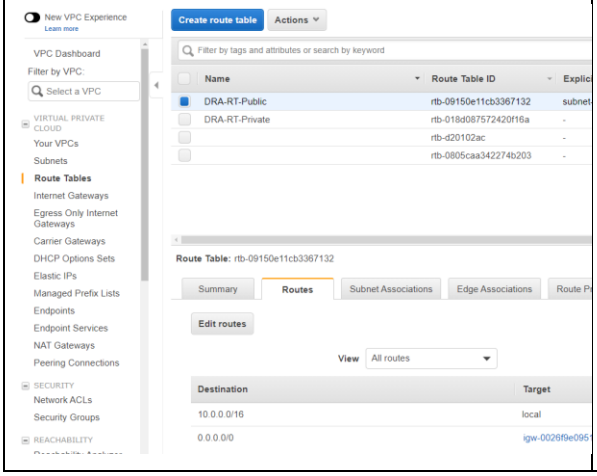
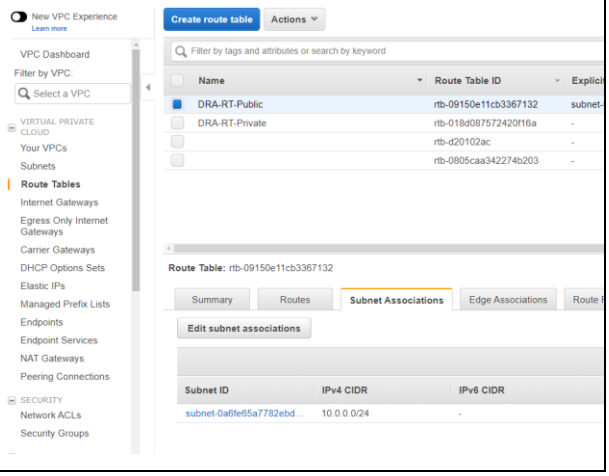
- **Select the Public subnet - Save.**



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

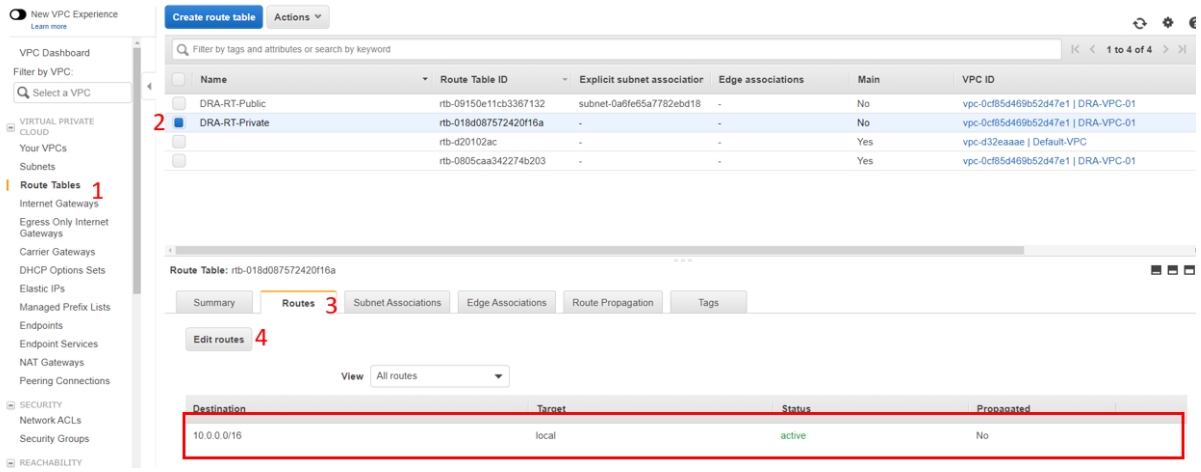


- **Results Association Public subnet**

Public Route	Public association
	

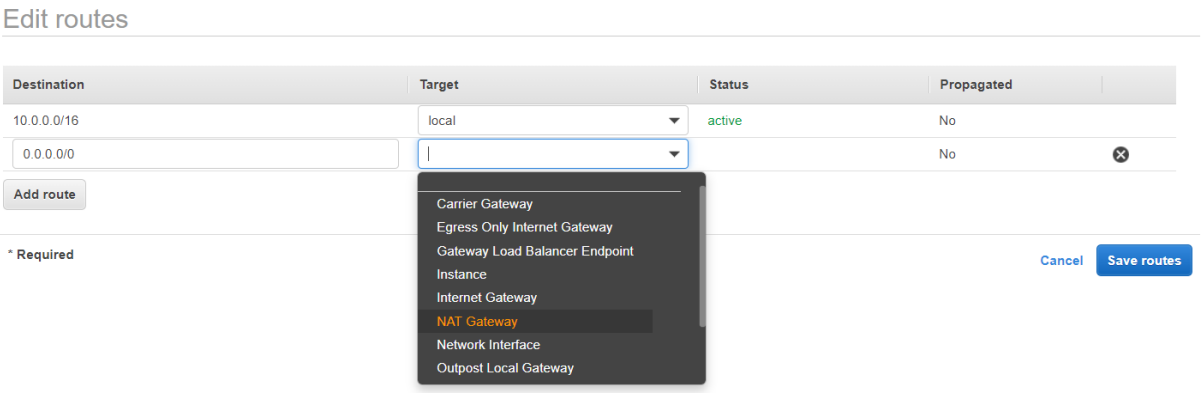
Observe that the route table is pointed to the local network and internet.

- **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.

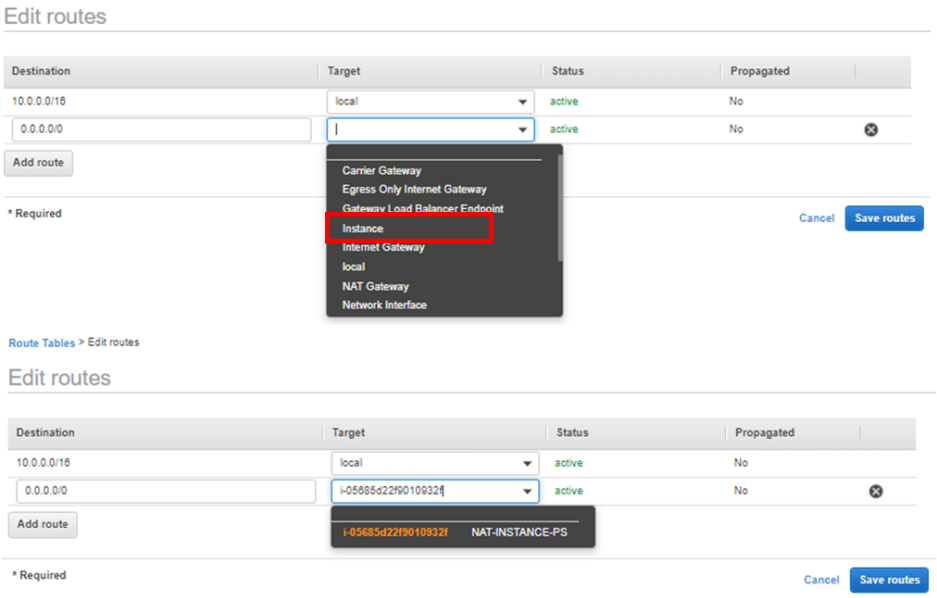


- **Click Edit routes –** create the route to traffic data through the Internet gateway that was created above – 0.0.0.0/0, which represents all IPv4 addresses. The target is the NAT gateway that was putted in the public subnet.
- **Select the NAT gateway/or NAT instance and Save routes.**

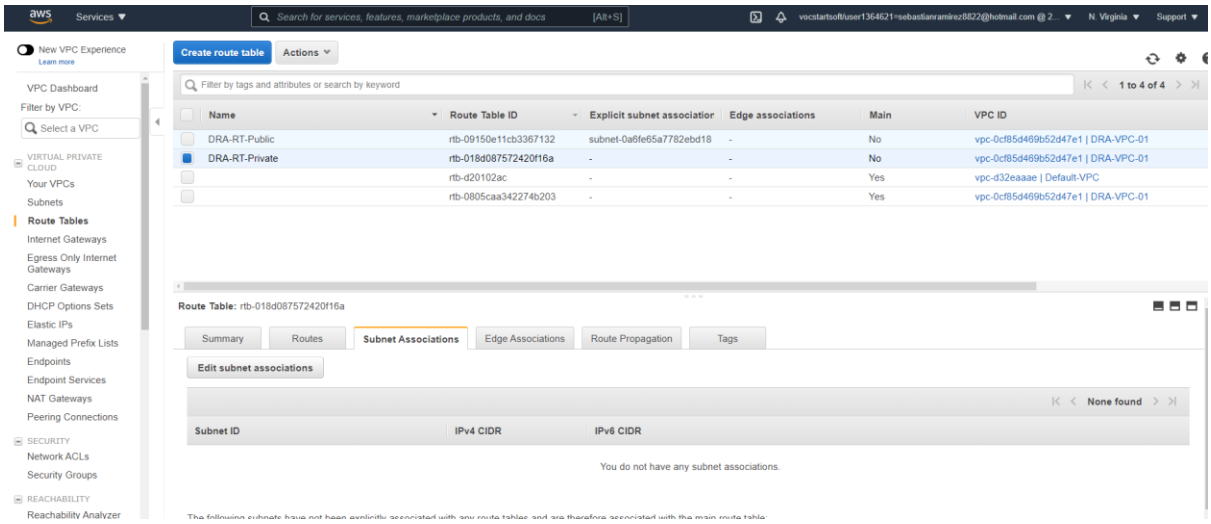
  - **NAT gateway**



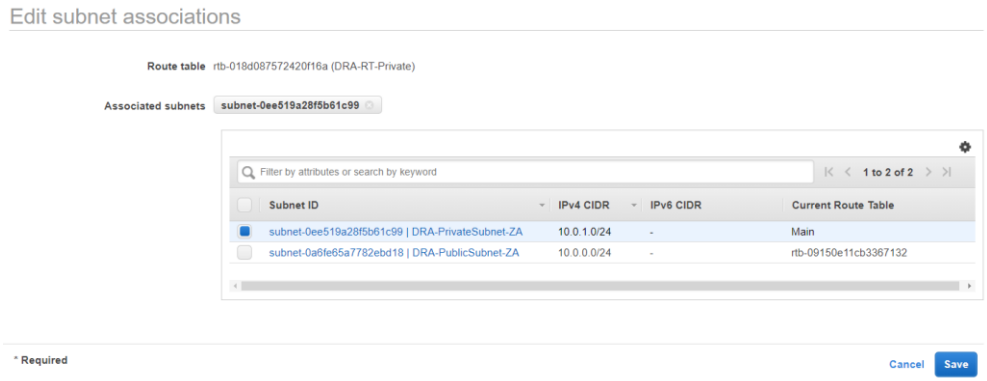
- **NAT Instance**



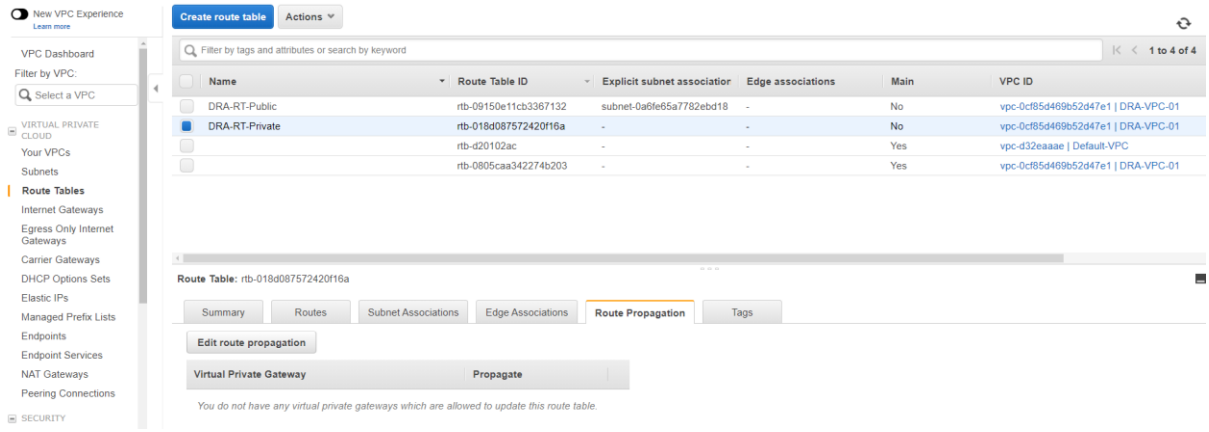
- **Subnet Associations – Edit subnet associations** which literally associate the public subnet to the public route table. Notice that the Public RT does not have any association. For default this is not associate.



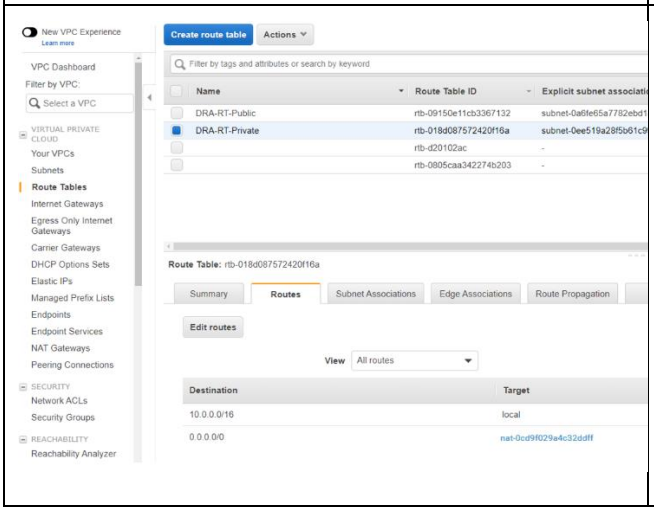
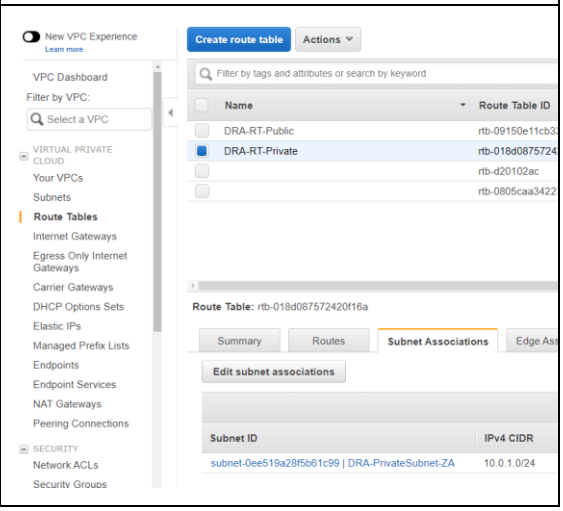
- **Select the Public subnet – Save.**



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



- **Results Association Public subnet**

Private Route	Private association
	

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 form 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.

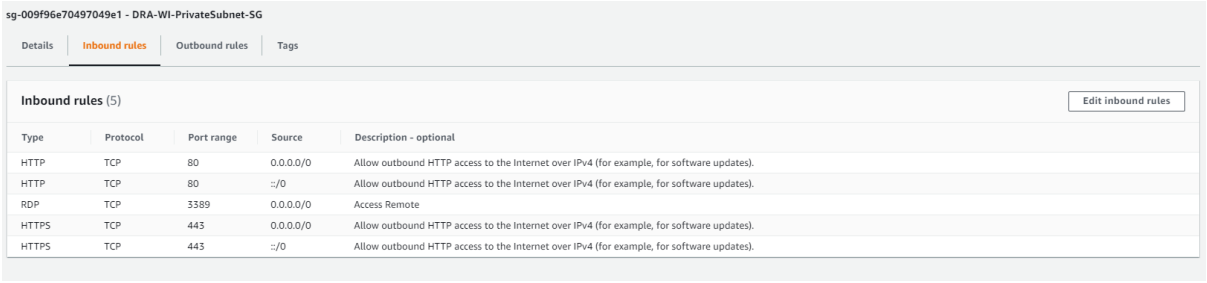
3.2.1. Security groups

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



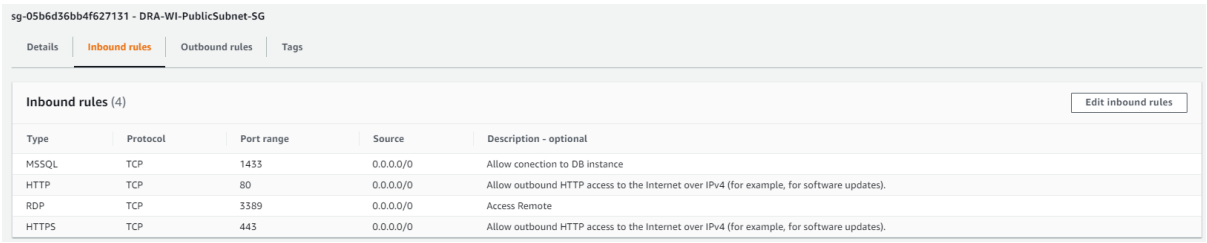
sg-009f96e70497049e1 - DRA-WI-PrivateSubnet-SG

Details | Inbound rules | Outbound rules | Tags

Inbound rules (5) — Edit inbound rules

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 HTTP access to the Internet over IPv4 (for example, for software updates).
HTTPS	TCP	443	::/0	Allow outbound HTTP access to the Internet over IPv4 (for example, for software updates).

Instances Public Group DB rules



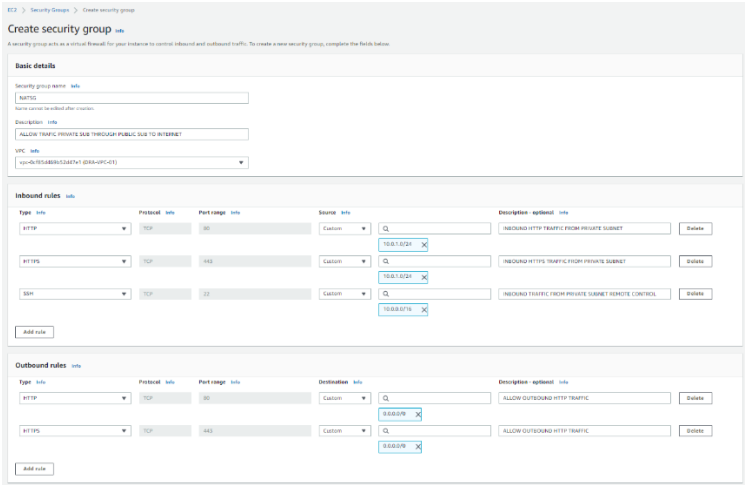
sg-05b6d36bb4f627131 - DRA-WI-PublicSubnet-SG

Details | Inbound rules | Outbound rules | Tags

Inbound rules (4) — Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
MSSQL	TCP	1433	0.0.0.0/0	Allow conection 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 HTTP access to the Internet over IPv4 (for example, for software updates).

NAT Instance rules



Create security group

Basic details

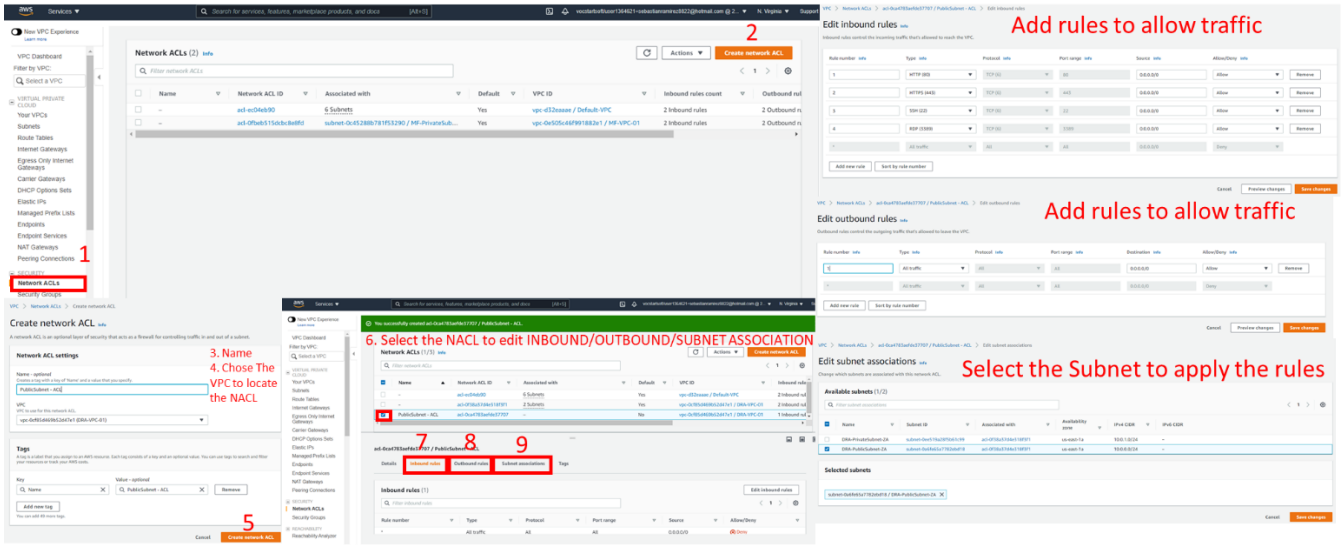
Inbound rules

Outbound rules

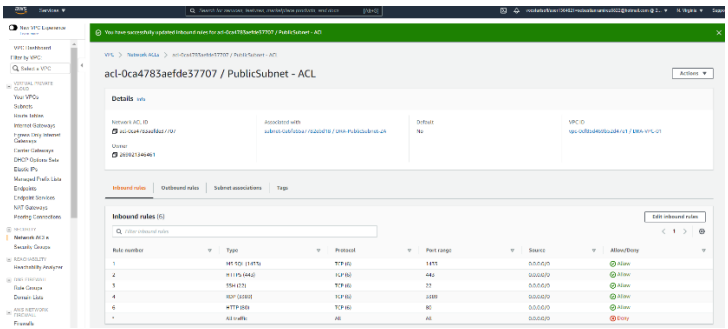
3.2.2. Network ACLs

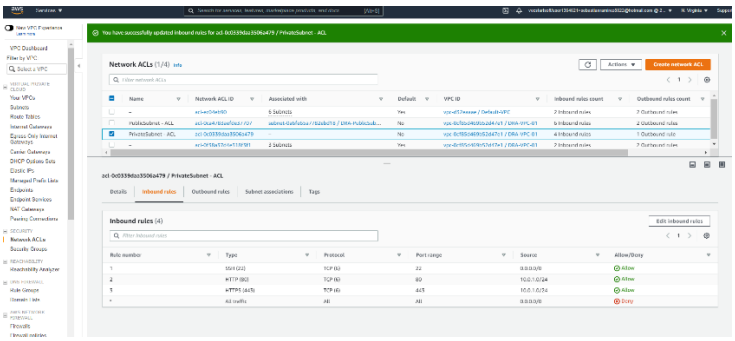
A network control list (ACL) act as a firewall controlling the traffic in a subnet layer, they must be similar to the security group rules(Amazon Web Services, 2021h).

- **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 rules created for the subnets were:





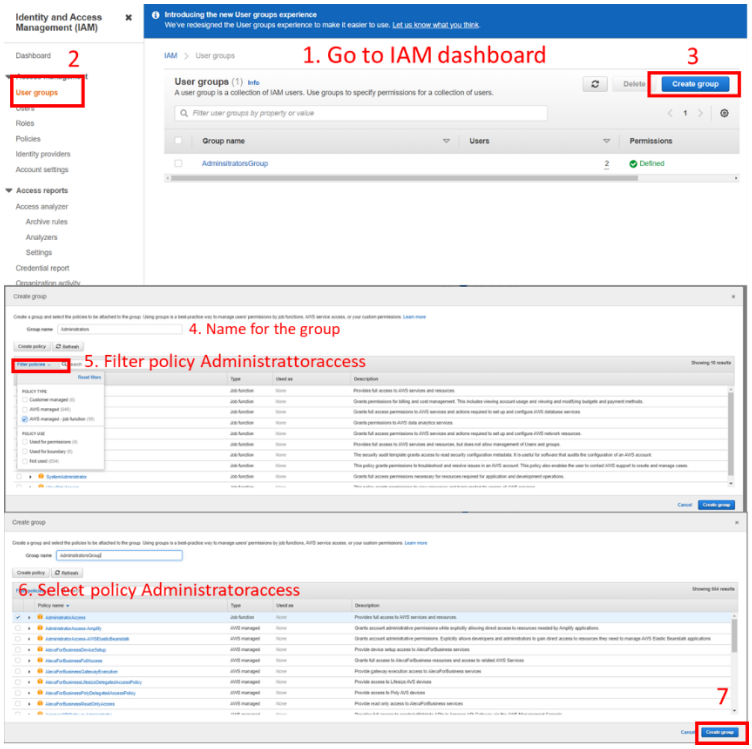
3.3. Security AWS Identity and Access Management (IAM)

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).

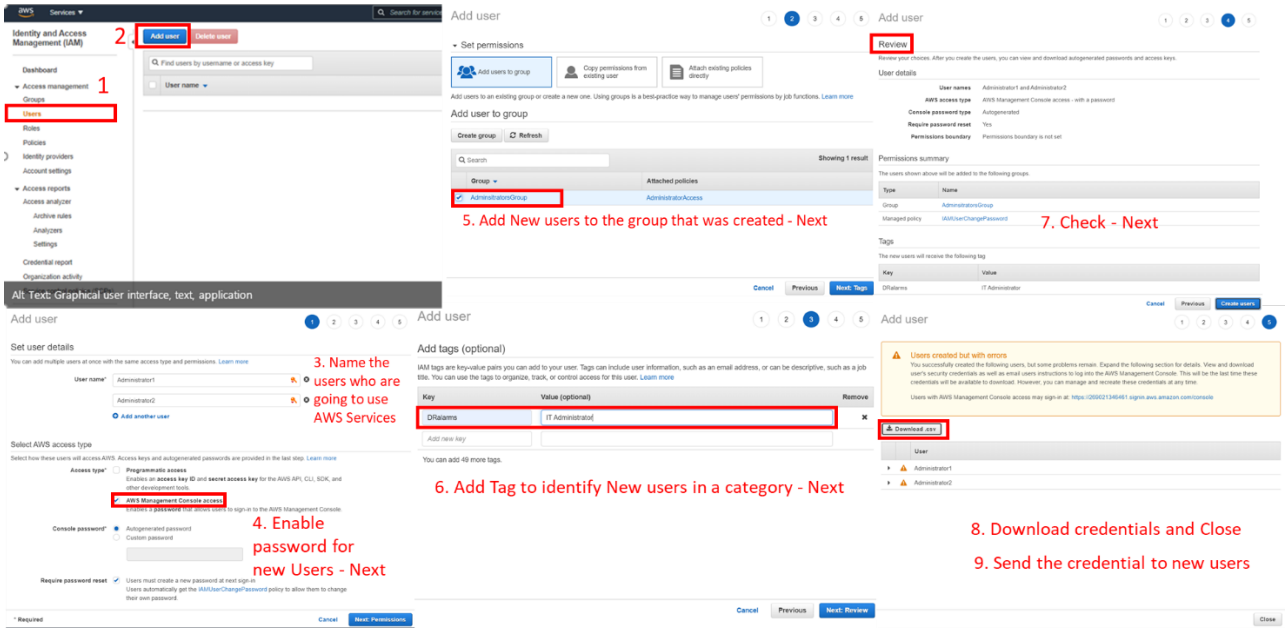
- **AWS IAM Authentication** - the users must authenticate before user AWS Management Console, AWS CLI or AWS SDKs. Users need to get credentials to use the resources.
    - **Groups** - Support manage **roles** and **polices** to different categories of groups in the organizations that need to access 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 use 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.



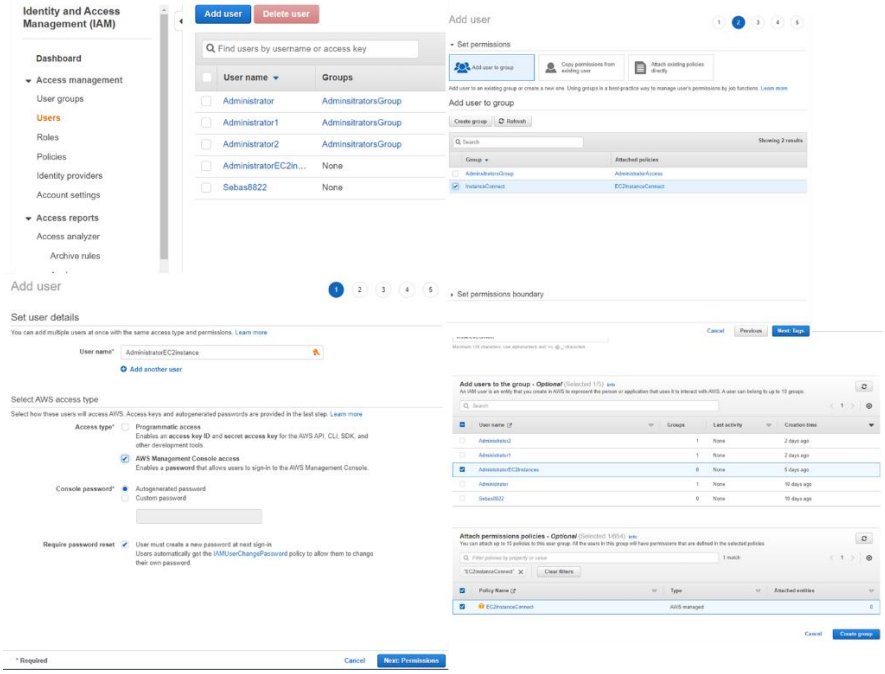
- **Add the user.**
  - **Click On user in the IAM dashboard and add user.**
  - **Name the new users** – mark AWS management console access to create a password.
  - **Add the user to the group** – next.
  - **Add tag** – next.
  - **Check** – create user.
  - **Download credentials** and send to the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



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

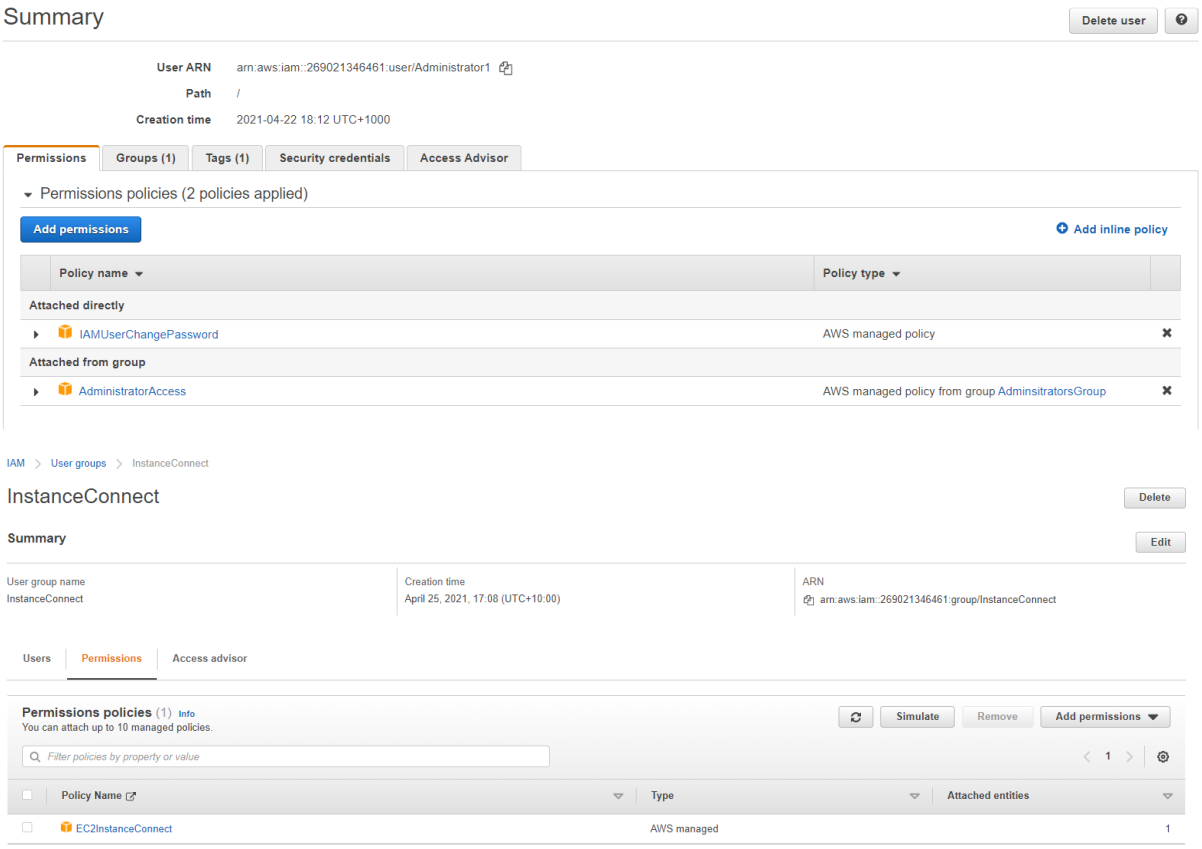
- **Create a group and policy and create a user within this group.**

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



- **Results**

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

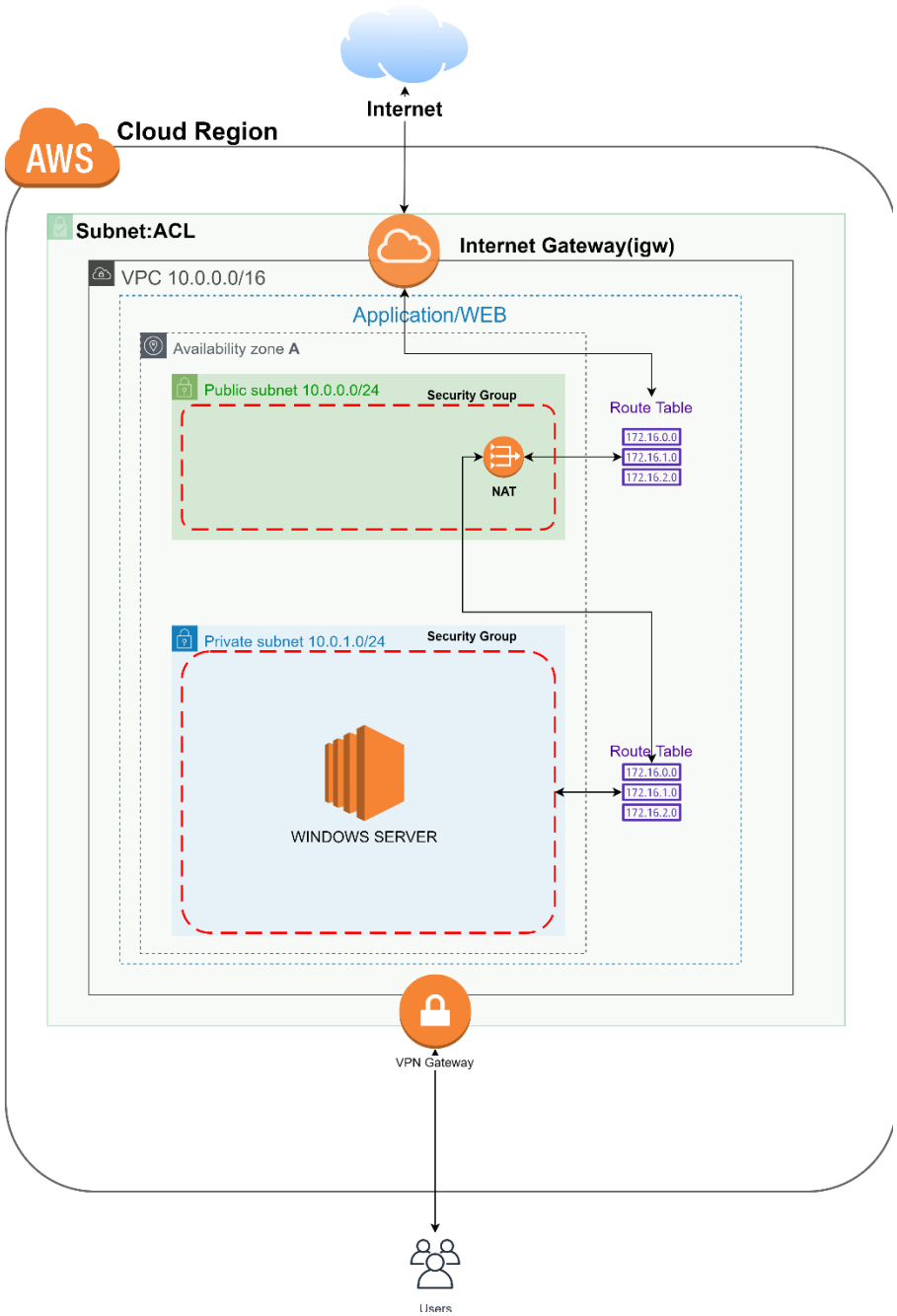


Every USER appears in the user panel where it shows every feature and user configuration. Therefore, policies and permissions can be added to individual user, control credentials, access keys and other features.

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

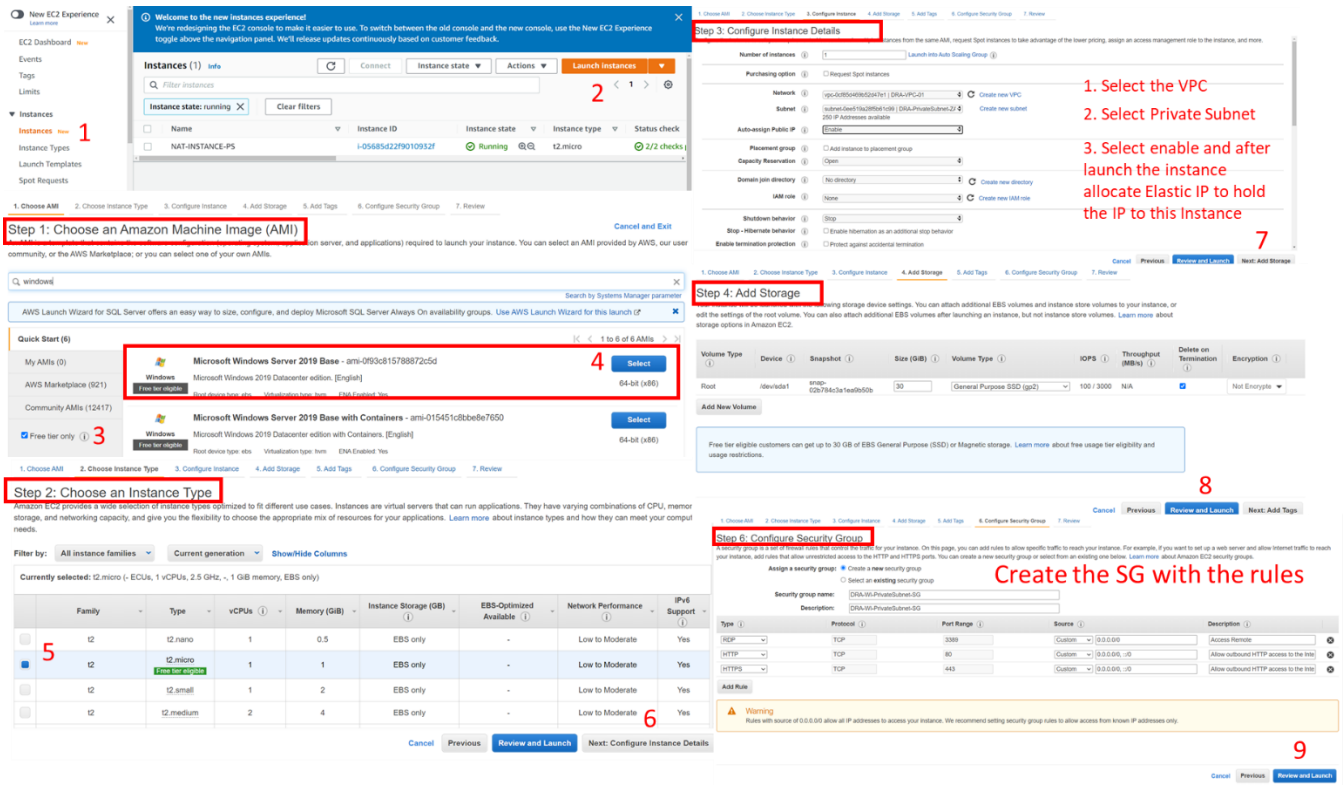
4. A Windows server in the private subnet.

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.

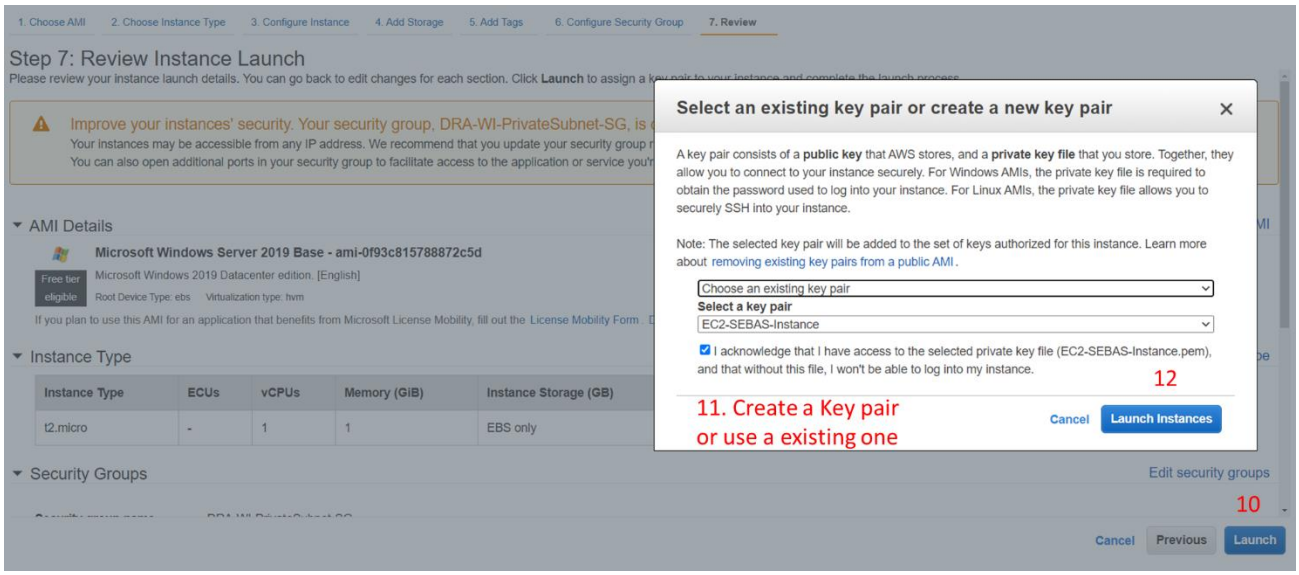


4.1. Create a EC2 instance

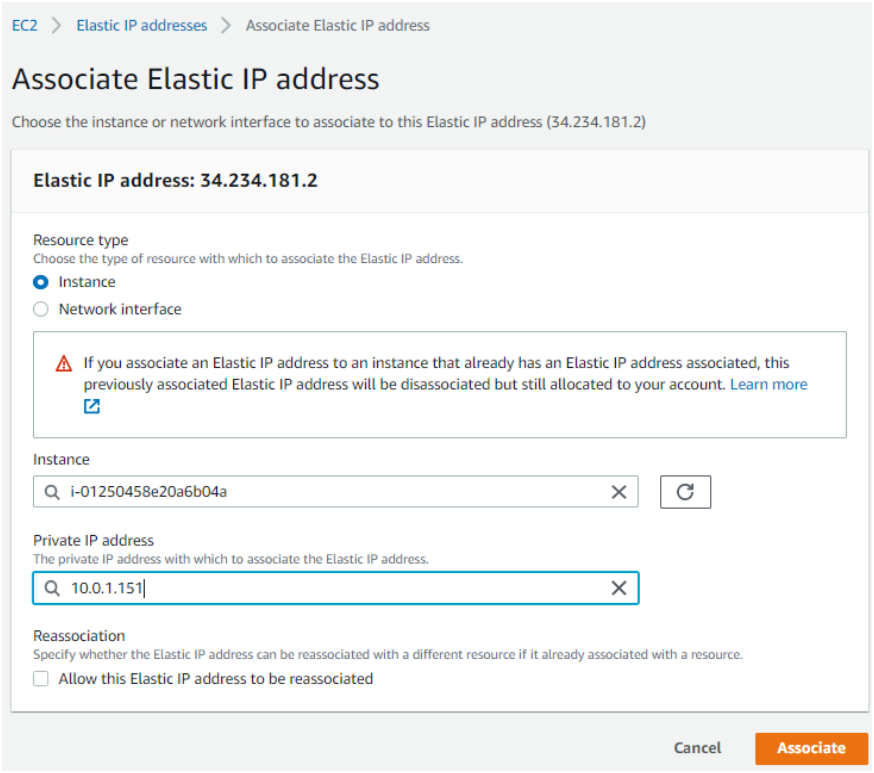
- **Launch an instance** – click on instances in the EC2 dashboard and click in launch instances.
- The launch instance – **Choose and Amazon machine** – in this case windows server and select.
- **Choose an instance Type** - Select a free tier -next configure instance details.
- **Configure instance** – 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



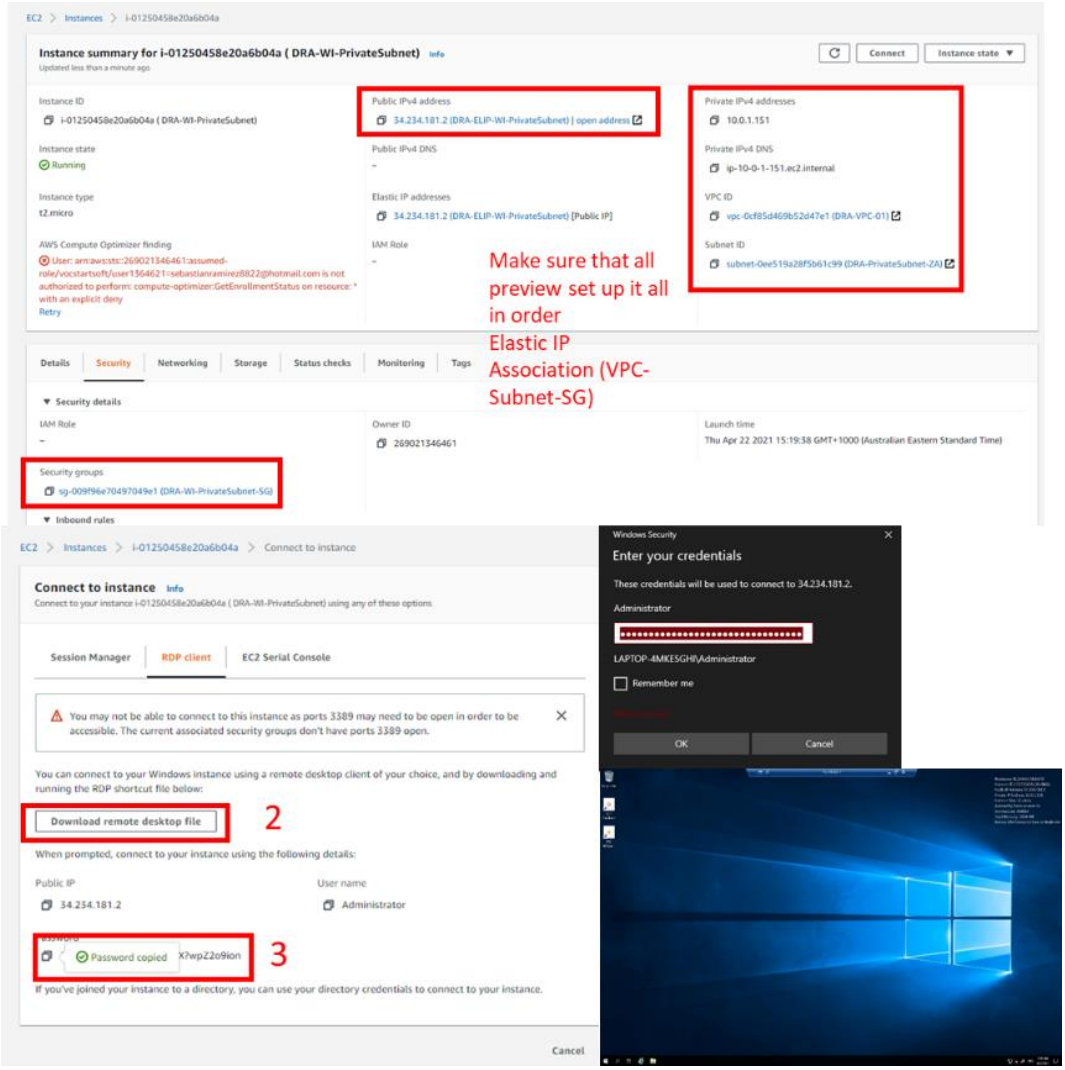
- **Create or choose a key pair –** the users allow to access to AWS have access key for the instances previously created in Identity and Access Management (IAM)



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



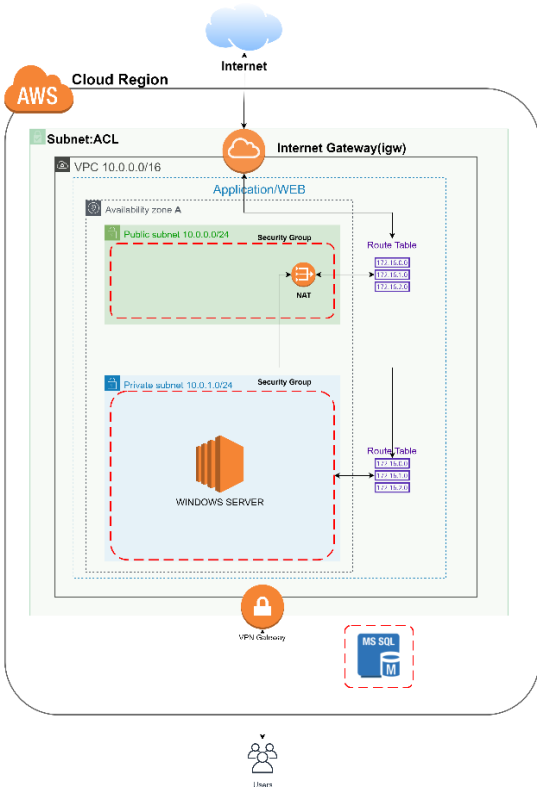
- **Check and access to the instance –** Access to the instance and start to use it.



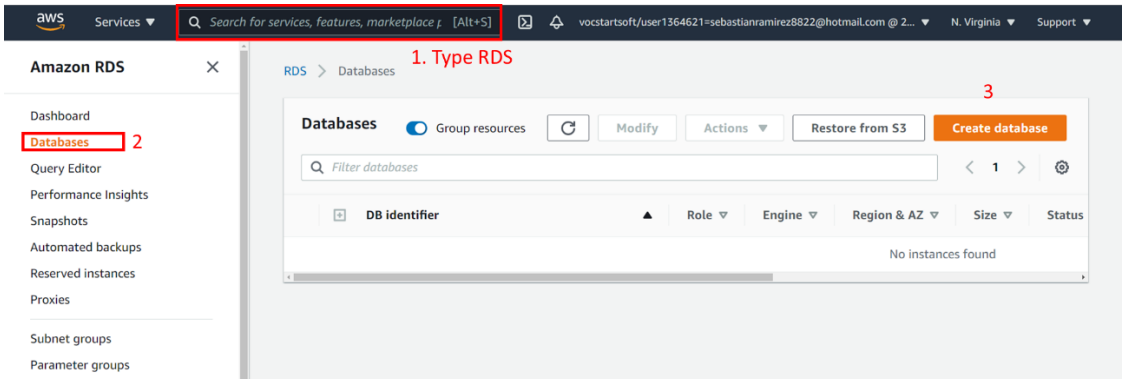
5. Database instance

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.

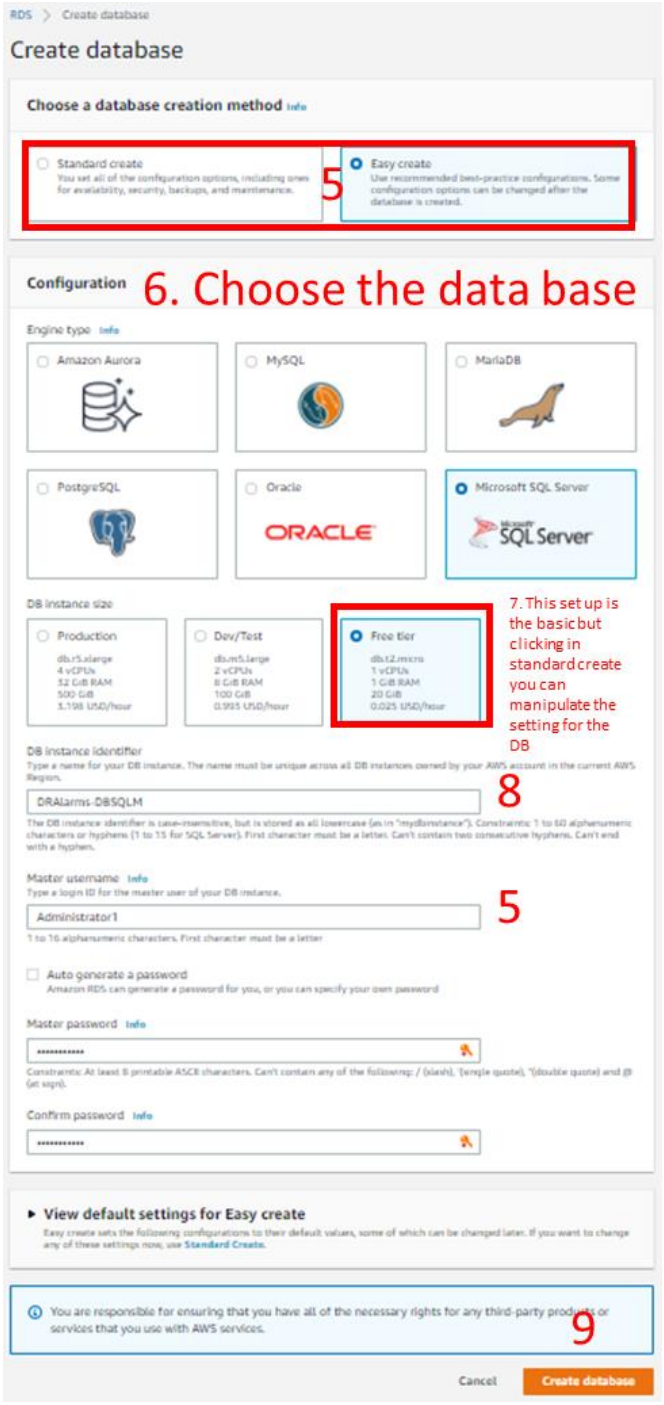
5.1. Create DB instance RDS.



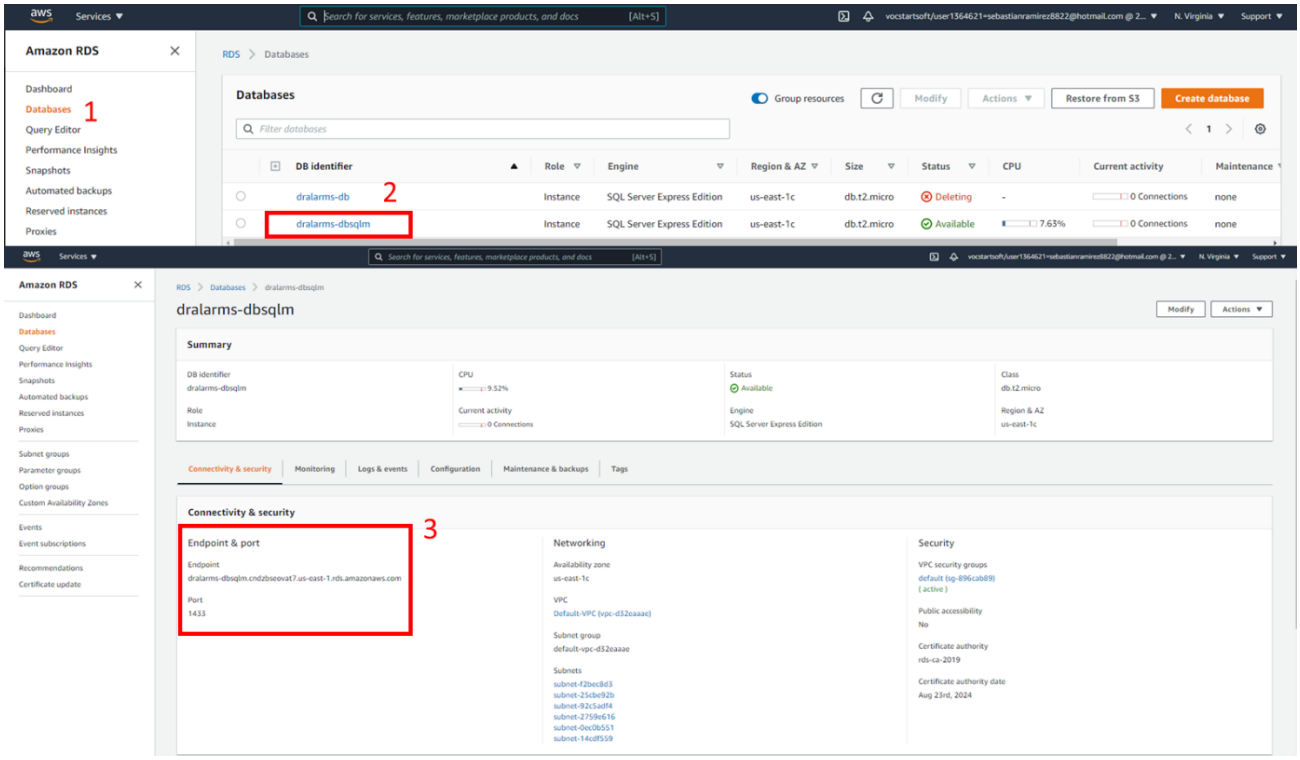
- Type RDS on top in AWS manage console.
- Go to databases - create databases.



- **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.**

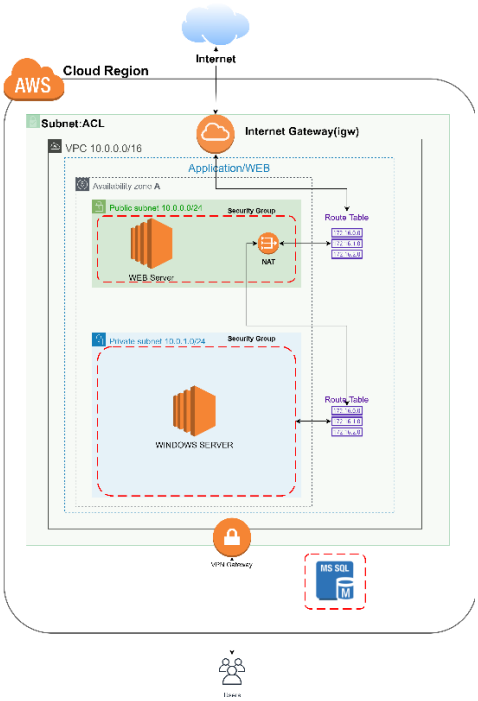


- Wait until it is created and get the Endpoint & port (this port must be open in the security group in the instance that we want to connect to the DB)

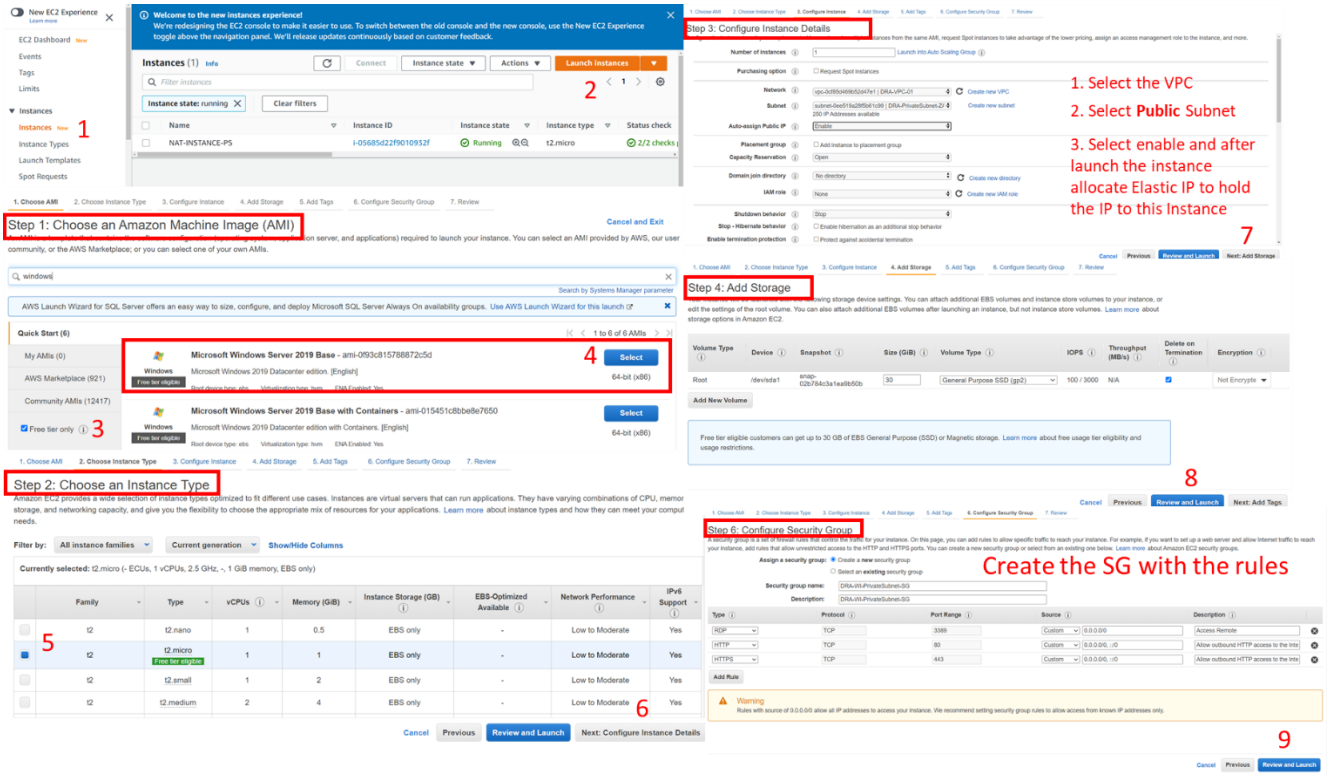


5.2. Create EC2 instance to connect DB Instance.

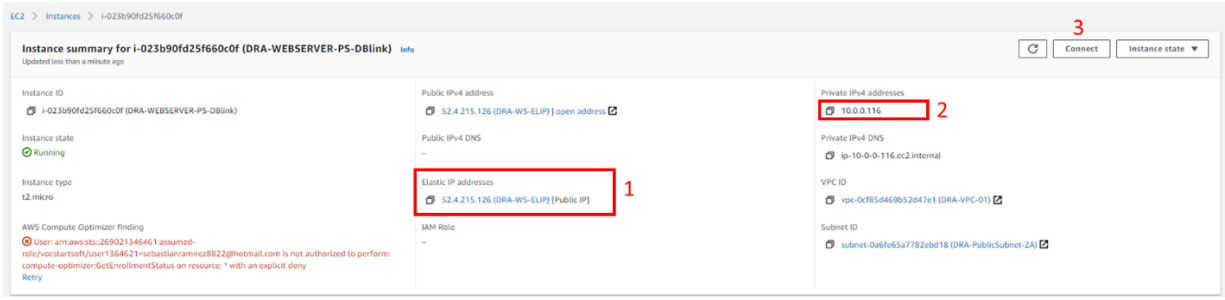
The next step is to create a EC2 instance in a public subnet to connect DR Alarm's WEB site the DB instance that was created.



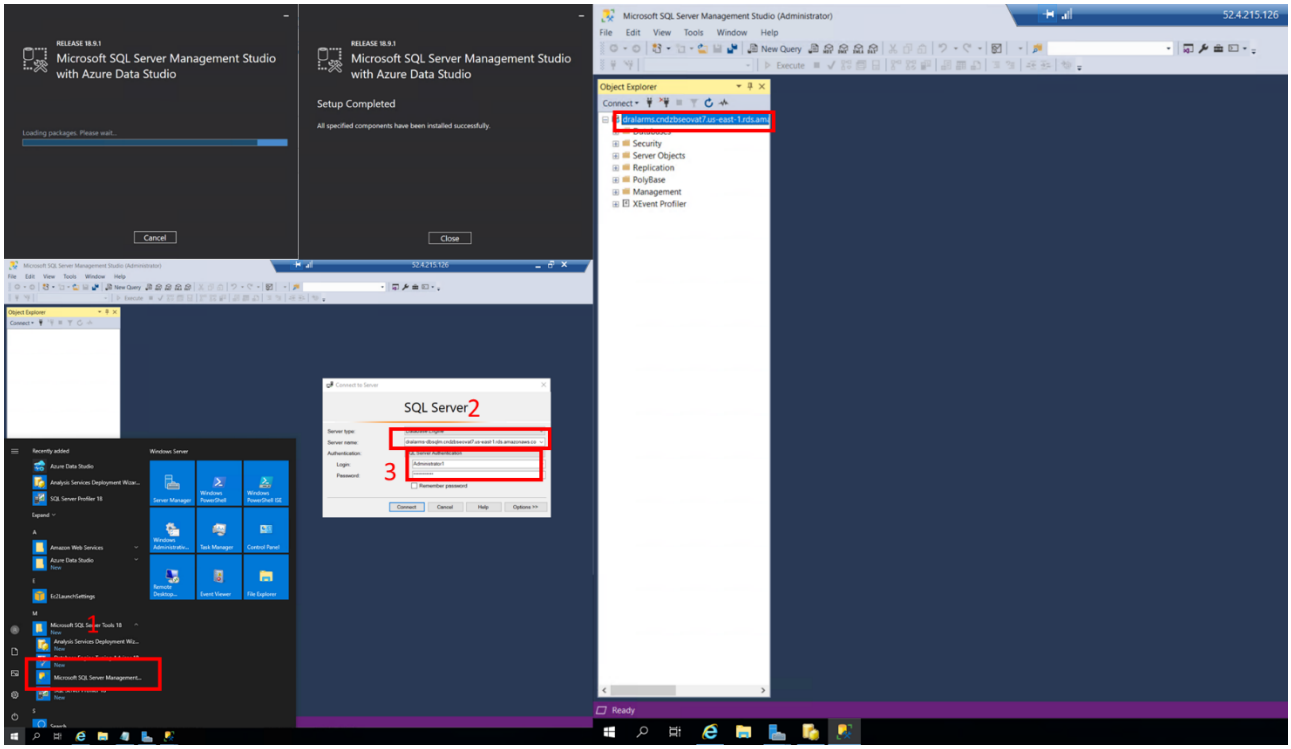
- **Create the instance such as was done in the module 4 –** chose public subnet- and allocate an elastic IP.



- **Check setup and Connect.**

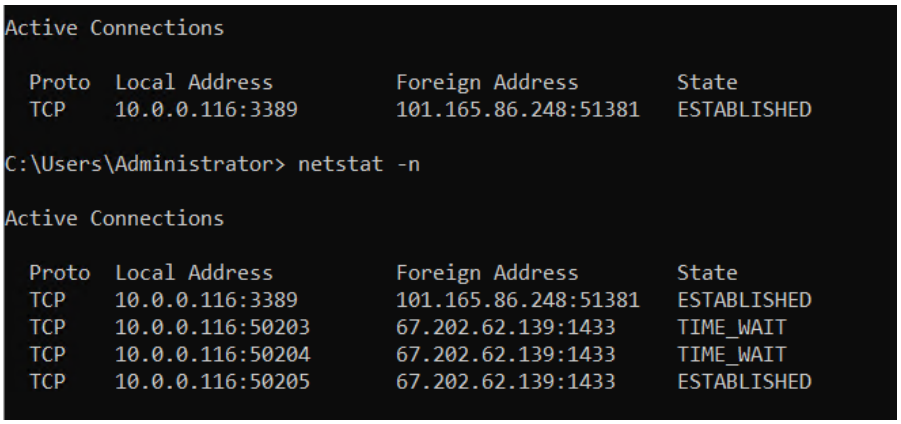
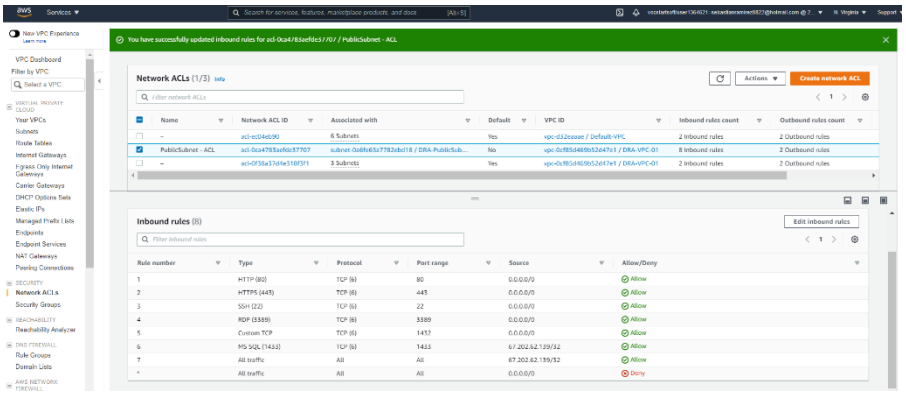
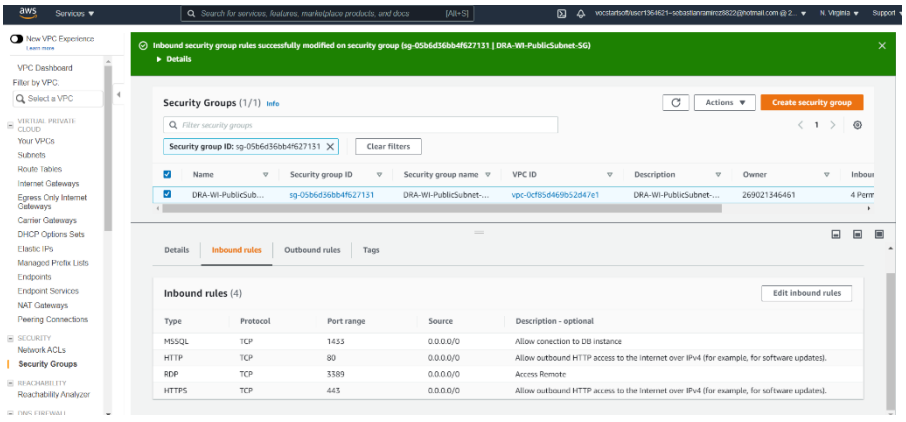


- Install from Microsoft.com – download the Microsoft server management studio- open and put the Endpoint – Master Username and password used in the step above. (**it is recommendable use a semicolon after server name example dralarms.cndzbseovat7.us-east-1.rds.amazonaws.com, 1433)**



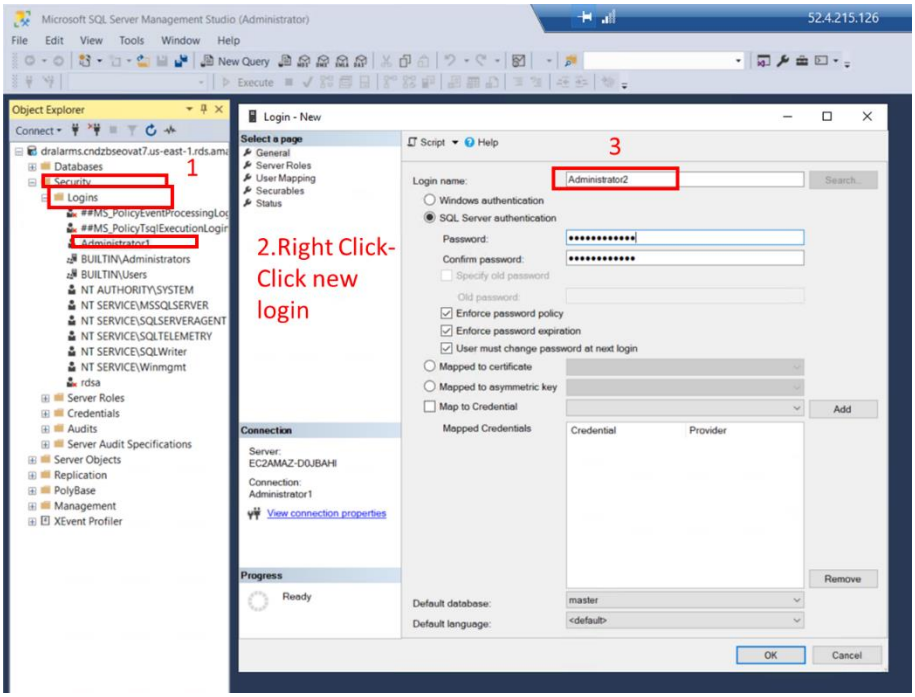
Troubleshooting

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).

Netstat -n (ao/aon) command in CMD EC2 instance to see the connections and port open	
Network ACL	
Security group Instance	

5.3. Create the second user access.

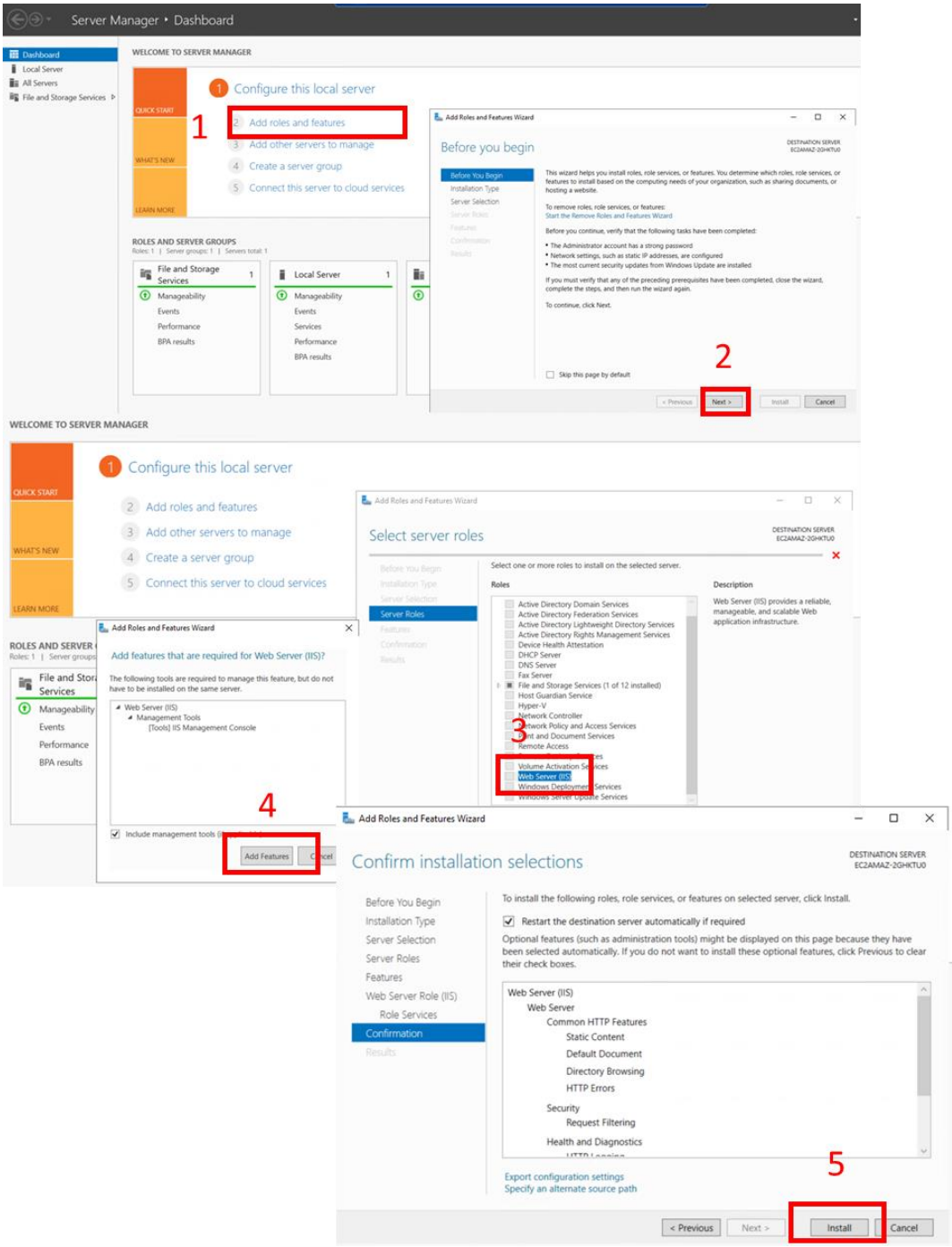
- The first user was created when the DB instance was created, now the second user will be created.
    - Inside database create the second user going **SECURITY – LOGINS – RIGHT** click and create new user.



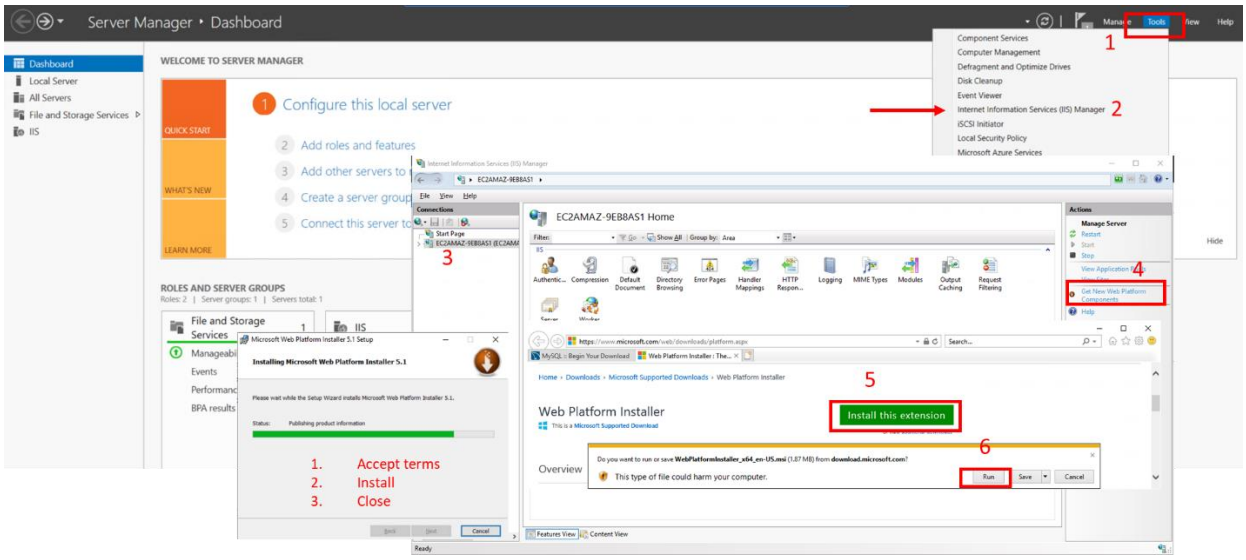
6. WordPress instance

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 443in a public subnet. To do this follow the next steps (Amazon Web Services, 2021j):

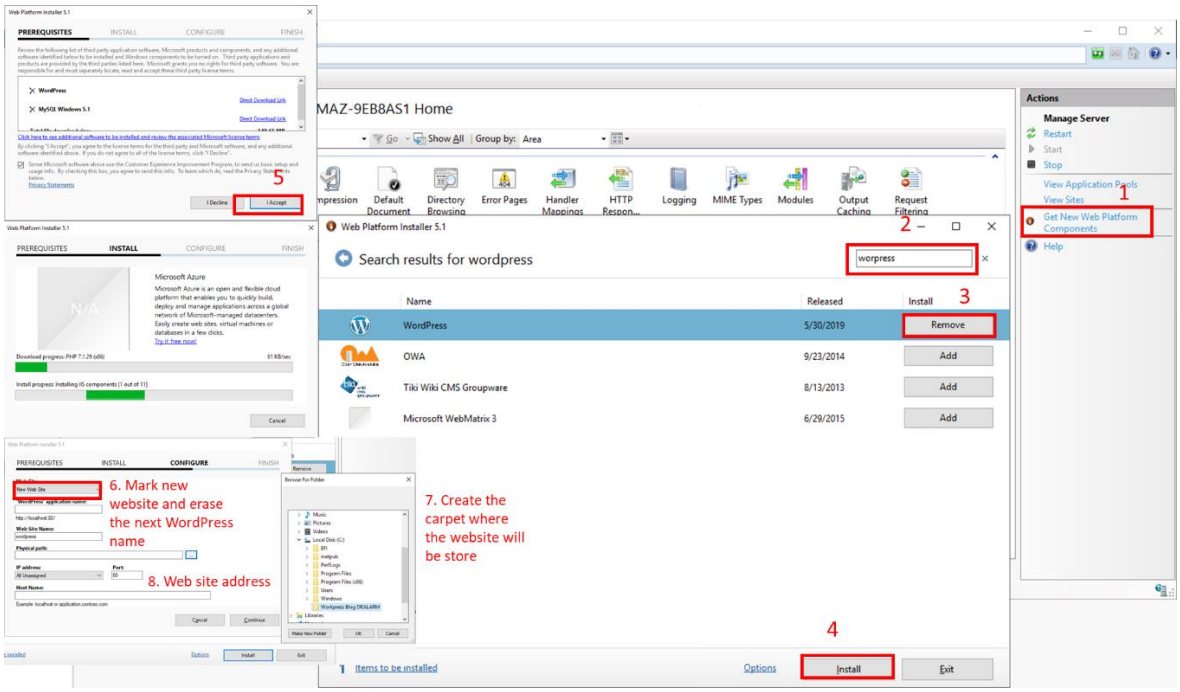
- **Install web server features.**
  - **Open server manager** in the windows server instance
  - **Click next until server selection.**
  - **Select web server (IIS)** and next until Install the features.



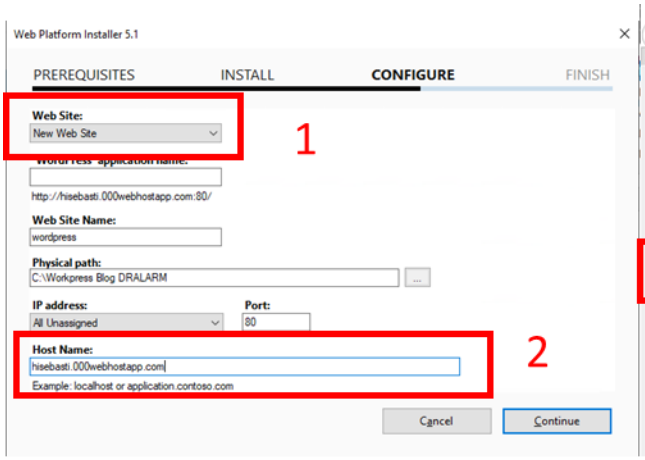
- **Download Web platform Installer.**
    - Go to tools on the top of server management – click.
    - Internet Information Services (IIS) Manager
    - Mark the connection
    - Get new web platform components.
    - Install extension from Microsoft website.

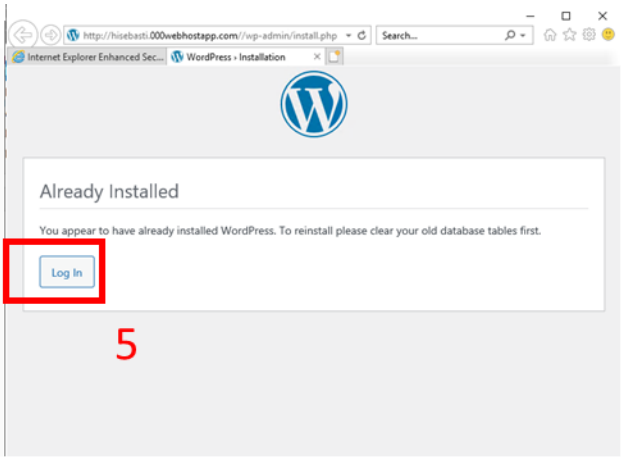


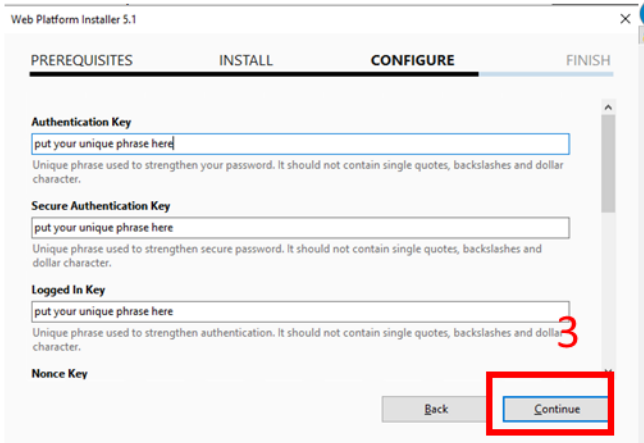
- **Install WordPress.**
    - **Open web platform Installer**
    - **Search for WordPress** – ADD – Install
    - **Install prerequisites** and accept the terms.
    - **Set up the WordPress website** – create a file where the website will be store.

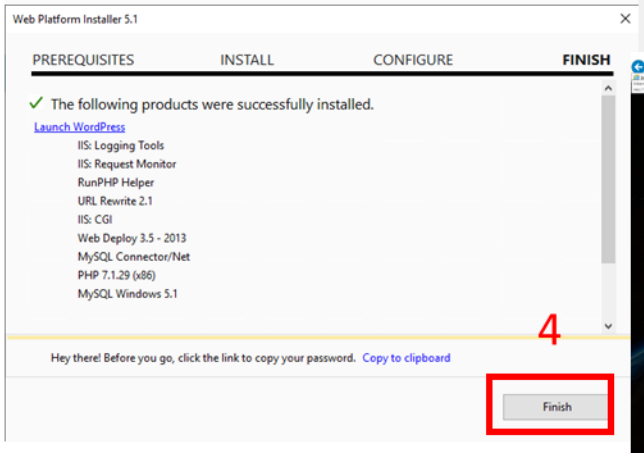


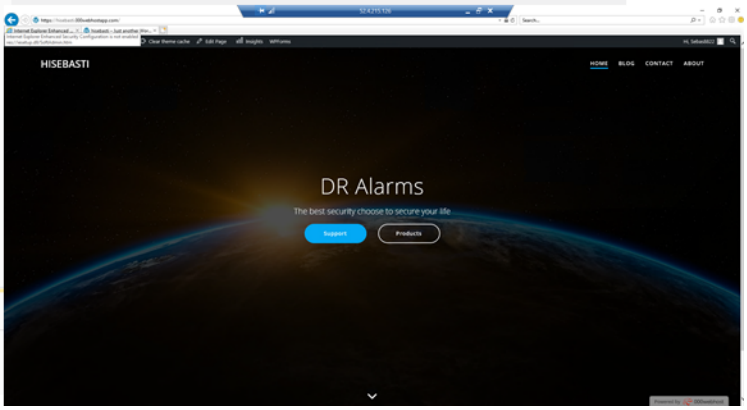
- **Configuration host name**











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

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

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

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

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

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

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