Amazon VPC infrastructure

Creating an Amazon VPC

Amazon Virtual Private Cloud (VPC) is a logically isolated section of the AWS Cloud where you can create and manage a virtual network for your resources. To create a VPC, navigate to the **VPC Dashboard** in the AWS Management Console and click **Create VPC**. Specify a **CIDR block** (such as 10.0.0.0/16) to define the range of IP addresses for your VPC. A CIDR block represents a network range that will be used to allocate subnets and other resources within the VPC. Next, assign a descriptive name to your VPC for easier identification and enable optional features such as **DNS hostnames**, which allow instances within the VPC to resolve domain names.

Creating Public and Private Subnets

Subnets are smaller subdivisions of the VPC's CIDR block. They segregate resources to enhance security and control. Start by going to the **Subnets** section in the VPC Dashboard and clicking **Create Subnet**. For each subnet, choose the **VPC ID** that you just created and specify a smaller **CIDR block**. For example, you can use 10.0.1.0/24 for a public subnet and 10.0.2.0/24 for a private subnet. This segmentation separates resources exposed to the internet (e.g., web servers) from those requiring restricted access (e.g., databases). Ensure subnets are distributed across multiple **Availability Zones** to increase fault tolerance and high availability.

Creating an Internet Gateway

An **Internet Gateway (IGW)** is a horizontally scaled and redundant gateway that enables your VPC to connect to the internet. To create an Internet Gateway, navigate to the **Internet Gateways** section in the VPC Dashboard and click **Create Internet Gateway**. Once created, attach it to your VPC. The Internet Gateway facilitates bi-directional communication between public-facing resources in your VPC and the internet.

Configuring a Routing Table and Associating It with a Subnet

A **Route Table** defines the rules for directing traffic within a VPC. To configure a route table, go to the **Route Tables** section and click **Create Route Table**. Add a route that directs all internet-bound traffic (0.0.0.0/0) to the Internet Gateway as the target. This route ensures resources in the public subnet can communicate with external networks. Finally, associate the route table with the public subnet to apply these routing rules.

Creating an Amazon EC2 Instance and Making It Publicly Accessible

Launch an **Amazon EC2 instance** in the public subnet by selecting the appropriate VPC and subnet during the instance creation process. Assign a **public IP address** to the instance to

enable internet access. Attach a **security group** with rules that permit inbound traffic, such as **SSH (port 22)** for remote access and **HTTP/HTTPS (ports 80/443)** for web traffic. After launching the instance, verify its accessibility using the public IP or DNS name.

Isolating an Amazon EC2 Instance in a Private Subnet

Launch another EC2 instance, but this time place it in the **private subnet** of your VPC. Ensure the instance is not assigned a public IP address to keep it isolated from direct internet access. If the instance needs internet connectivity (e.g., for software updates), use a **NAT Gateway** or **NAT Instance** located in the public subnet. Configure the instance's **security group** to restrict access, permitting only essential traffic, such as database connections from other resources within the VPC.

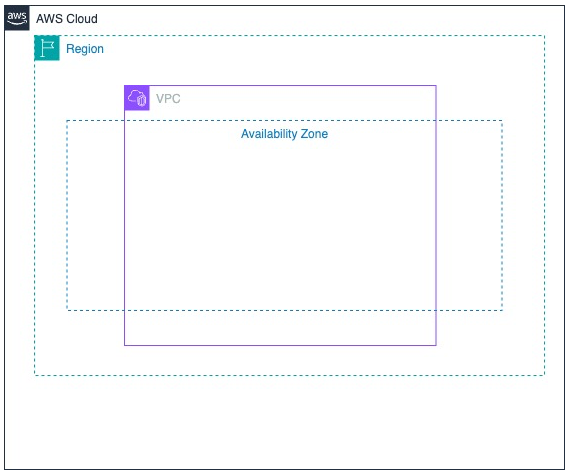
Creating and Assigning Security Groups

Security Groups act as virtual firewalls to control traffic at the instance level. Create a security group with specific rules to allow or deny traffic based on your requirements. For example, allow **SSH traffic (port 22)** only from trusted IP addresses or enable **HTTP/HTTPS (ports 80/443)** for web servers. Assign the appropriate security group to each EC2 instance during creation or afterward. Security groups can be modified at any time to adapt to changing requirements.

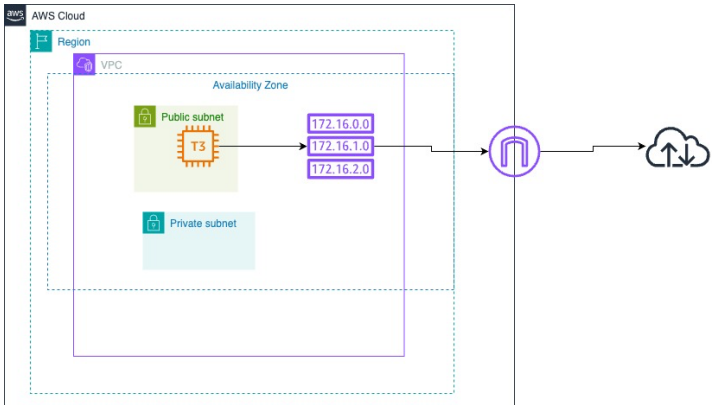
Connecting to Amazon EC2 Instances Using Session Manager

Session Manager, a feature of AWS Systems Manager, provides secure and auditable access to EC2 instances without the need for SSH keys or public IPs. First, assign an **IAM role** to your EC2 instance with permissions for Systems Manager. Enable Session Manager by configuring it in the Systems Manager console. To connect, use the **AWS Management Console**, **CLI**, or **SDK** to initiate a session. This eliminates the need to expose your instance to the internet while maintaining secure access.

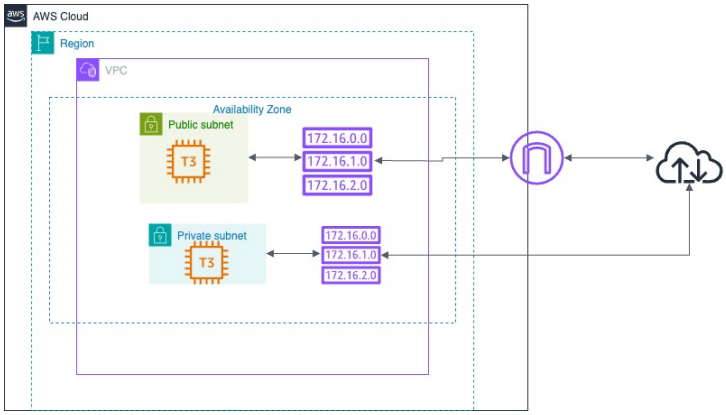
a.



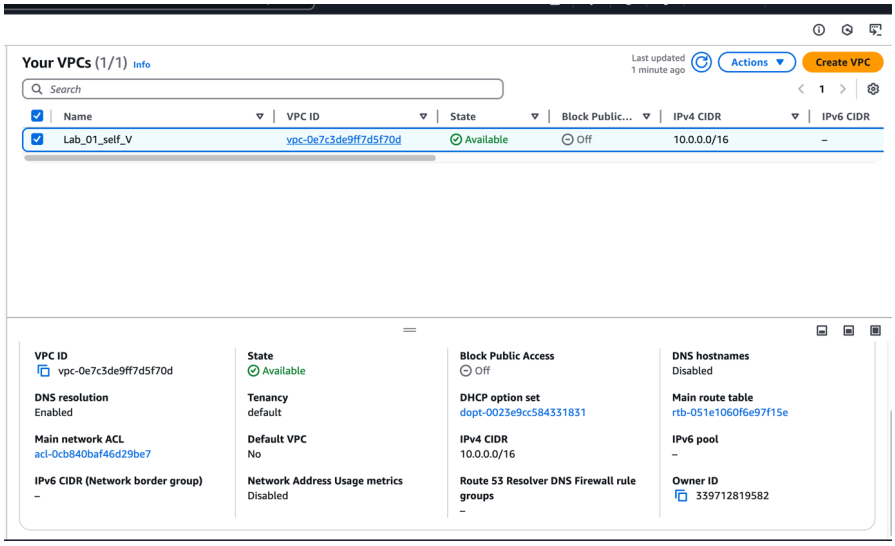
b.


AWS Cloud
Region
VPC
Availability Zone
Public subnet
T3
172.16.0.0
172.16.1.0
172.16.2.0
Private subnet

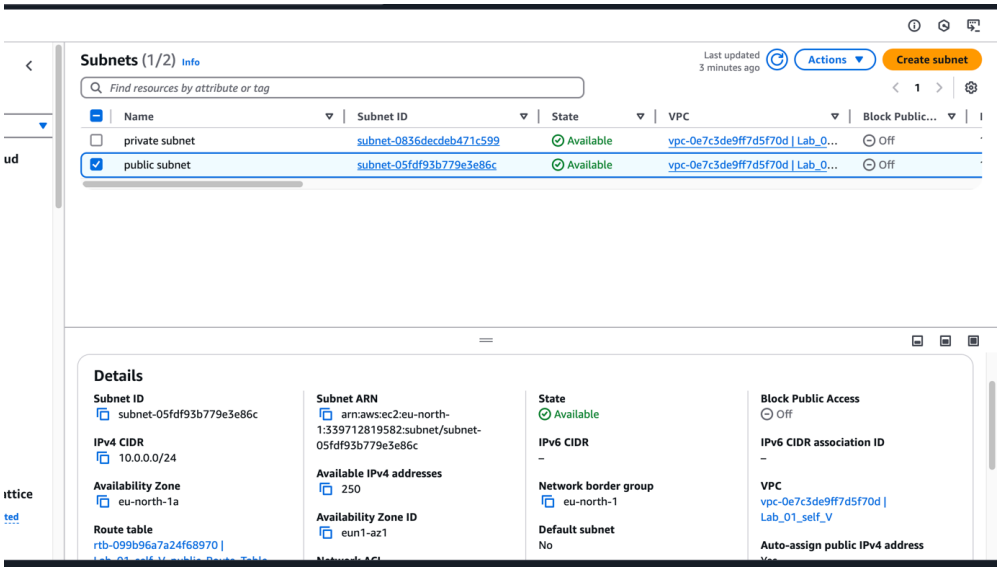
c.


AWS Cloud
Region
VPC
Availability Zone
Public subnet
T3
172.16.0.0
172.16.1.0
172.16.2.0
Private subnet
T3
172.16.0.0
172.16.1.0
172.16.2.0

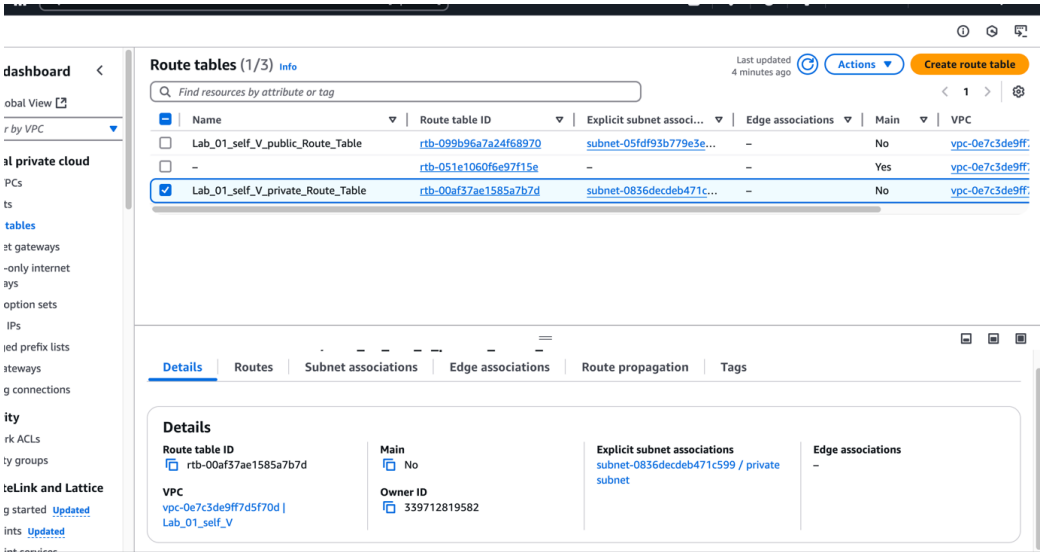
1.


Your VPCs (1/1) Info
Last updated 1 minute ago
Actions
Create VPC
Search
1
Name
VPC ID
State
Block Public...
IPv4 CIDR
IPv6 CIDR
Lab_01_self_V
vpc-0e7c3de9ff7d5f70d
Available
Off
10.0.0.0/16
–
VPC ID
vpc-0e7c3de9ff7d5f70d
State
Available
Block Public Access
Off
DNS hostnames
Disabled
DNS resolution
Enabled
Tenancy
default
DHCP option set
dopt-0023e9cc584331831
Main route table
rtb-051e1060f6e97f15e
Main network ACL
acl-0cb840baf46d29be7
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
339712819582

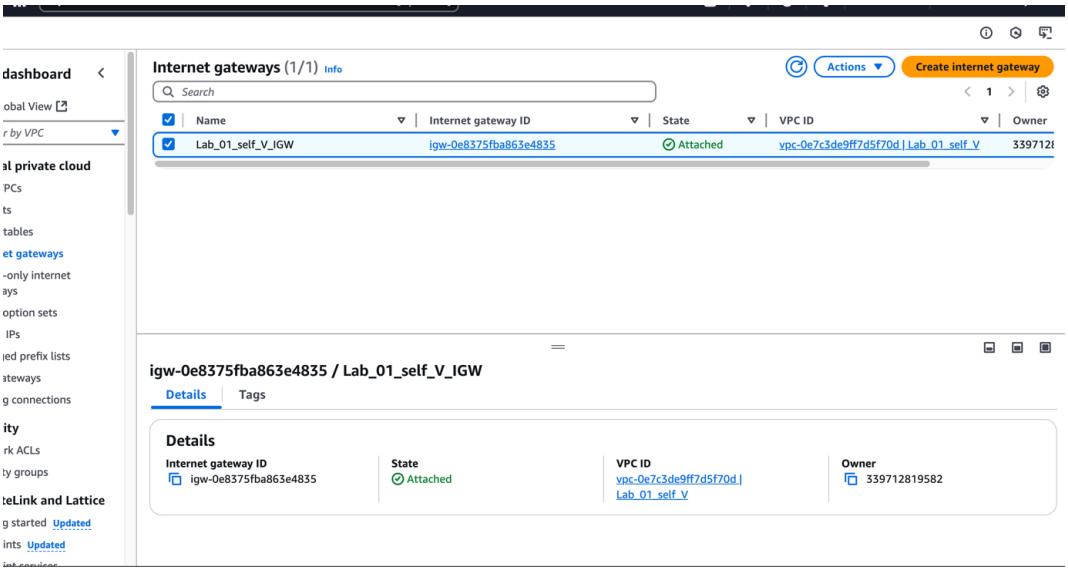
2.


Subnets (1/2) Info
Last updated 3 minutes ago
Actions
Create subnet
Find resources by attribute or tag
Name
Subnet ID
State
VPC
Block Public...
private subnet
subnet-0836decdeb471c599
Available
vpc-0e7c3de9ff7d5f70d | Lab_0...
Off
public subnet
subnet-05fdf93b779e3e86c
Available
vpc-0e7c3de9ff7d5f70d | Lab_0...
Off
Details
Subnet ID
subnet-05fdf93b779e3e86c
Subnet ARN
arn:aws:ec2:eu-north-1:339712819582:subnet/subnet-05fdf93b779e3e86c
State
Available
Block Public Access
Off
IPv4 CIDR
10.0.0.0/24
IPv6 CIDR
–
IPv6 CIDR association ID
–
Availability Zone
eu-north-1a
Available IPv4 addresses
250
Network border group
eu-north-1
VPC
vpc-0e7c3de9ff7d5f70d | Lab_01_self_V
Route table
rtb-099b96a7a24f68970 |
Availability Zone ID
eun1-az1
Default subnet
No
Auto-assign public IPv4 address

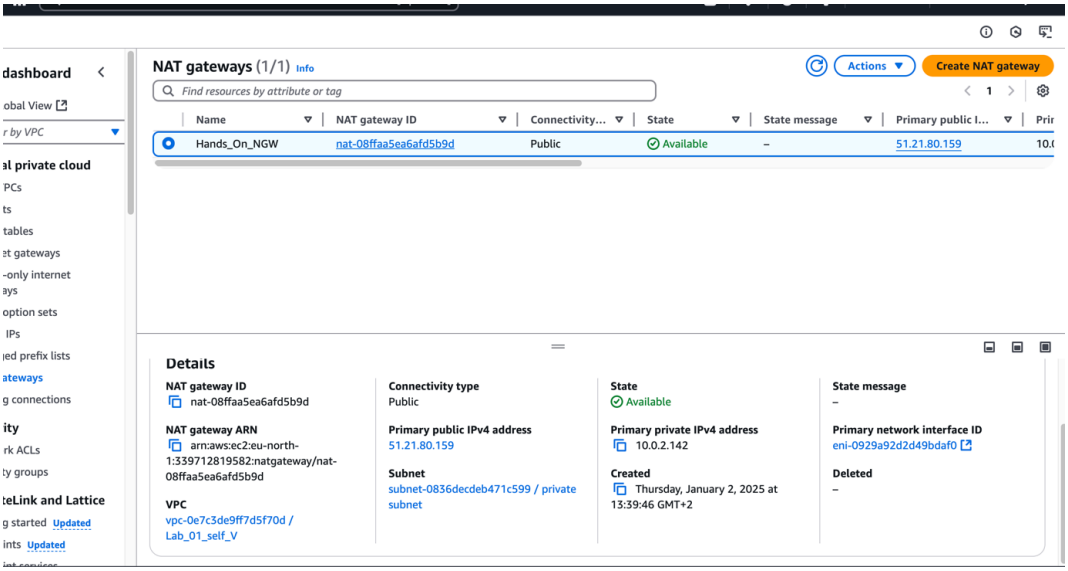
3.


Route tables (1/3) Info
Last updated 4 minutes ago
Actions
Create route table
Find resources by attribute or tag
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
Lab_01_self_V_public_Route_Table
rtb-099b96a7a24f68970
subnet-05fdf93b779e3e...
–
No
–
rtb-051e1060f6e97f15e
–
–
Yes
Lab_01_self_V_private_Route_Table
rtb-00af37ae1585a7b7d
subnet-0836decdeb471c...
–
No
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Details
Route table ID
rtb-00af37ae1585a7b7d
Main
No
Explicit subnet associations
subnet-0836decdeb471c599 / private subnet
Edge associations
–
VPC
vpc-0e7c3de9ff7d5f70d | Lab_01_self_V
Owner ID
339712819582

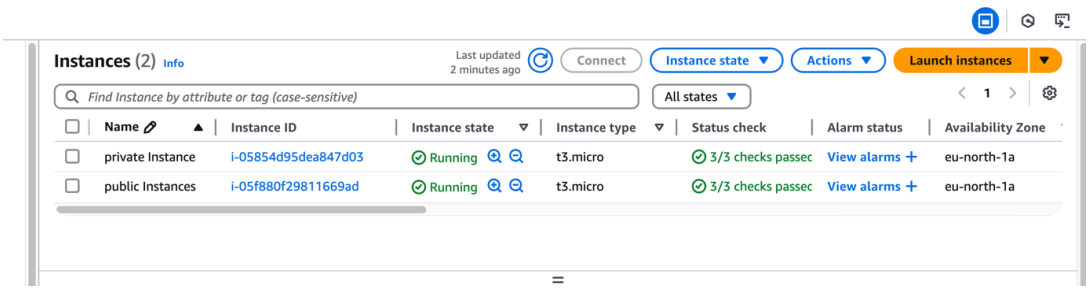
4.


dashboard
Internet gateways (1/1) Info
Search
Actions
Create internet gateway
Name
Internet gateway ID
State
VPC ID
Owner
Lab_01_self_V_IGW
igw-0e8375fba863e4835
Attached
vpc-0e7c3de9ff7d5f70d | Lab_01_self_V
igw-0e8375fba863e4835 / Lab_01_self_V_IGW
Details
Tags
Details
Internet gateway ID
igw-0e8375fba863e4835
State
Attached
VPC ID
vpc-0e7c3de9ff7d5f70d | Lab_01_self_V
Owner
339712819582

5.


dashboard
NAT gateways (1/1) Info
Find resources by attribute or tag
Actions
Create NAT gateway
Name
NAT gateway ID
Connectivity...
State
State message
Primary public I...
Hands_On_NGW
nat-08ffaa5ea6afd5b9d
Public
Available
51.21.80.159
Details
NAT gateway ID
nat-08ffaa5ea6afd5b9d
NAT gateway ARN
arn:aws:ec2:eu-north-1:339712819582:natgateway/nat-08ffaa5ea6afd5b9d
VPC
vpc-0e7c3de9ff7d5f70d / Lab_01_self_V
Connectivity type
Public
Primary public IPv4 address
51.21.80.159
Subnet
subnet-0836decdeb471c599 / private subnet
State
Available
Primary private IPv4 address
10.0.2.142
Created
Thursday, January 2, 2025 at 13:39:46 GMT+2
State message
–
Primary network interface ID
eni-0929a92d2d49bdaf0
Deleted
–

6.


Instances (2) Info
Last updated 2 minutes ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
private Instance
i-05854d95dea847d03
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1a
public Instances
i-05f880f29811669ad
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1a