

Designing and Configuring a Virtual LAN with Public and Private Subnets using AWS

Objective

The objective of this project is to design and configure a Virtual Private Cloud (VPC) in AWS with both public and private subnets. This setup ensures secure communication between instances and demonstrates subnet connectivity, isolation, and internet accessibility for the public subnet.

VPC Dashboard (Start)

The screenshot shows the AWS VPC Dashboard. At the top, there are buttons for 'Create VPC' and 'Launch EC2 Instances'. Below this, a note says 'Note: Your instances will launch in the Europe region.' A 'Refresh Resources' button is also present. On the left, a sidebar lists 'Virtual private cloud' and 'Security' sections. The main area displays 'Resources by Region' for the Stockholm region, showing counts for VPCs, Subnets, Route Tables, Internet Gateways, NAT Gateways, VPC Peering Connections, Network ACLs, and Security Groups. Each resource type has a 'See all regions' link. A vertical sidebar on the right contains service links like 'View current details', 'Block IP', 'Zones', 'Console', and 'Additions'.

Open the VPC Dashboard to begin creating the VPC.

Create VPC (VPC and more)

The screenshot shows the 'Create VPC' wizard. On the left, under 'VPC settings', the 'Resources to create' section has 'VPC and more' selected. The 'Name tag auto-generation' section has 'Auto-generate' checked and 'my' entered. The 'IPv4 CIDR block' section shows '10.0.0.0/16' with 65,536 IPs available. The 'IPv6 CIDR block' section has 'No IPv6 CIDR block' selected. The 'Tenancy' section has 'Default' selected. On the right, the 'Preview' panel shows a VPC named 'my-vpc' with four subnets: 'eu-north-1a' containing 'my-subnet-public1-eu-north-1a' and 'my-subnet-private1-eu-north-1a'; and 'eu-north-1b' containing 'my-subnet-public2-eu-north-1b' and 'my-subnet-private2-eu-north-1b'.

Choose 'VPC and more' to let AWS create subnets and routing automatically.

VPC CIDR and Name Tag

This screenshot shows the 'VPC CIDR and Name Tag' configuration screen. It includes sections for 'Tenancy' (Default), 'Number of Availability Zones (AZs)' (1 selected), 'Number of public subnets' (1 selected), 'Number of private subnets' (1 selected), 'Customize subnets CIDR blocks' (not shown in detail), and 'NAT gateways (\$)' (None selected). The 'Preview' panel on the right shows a VPC named 'my-vpc'.

Set the VPC name and IPv4 CIDR block (e.g., 10.0.0.0/16).

Choose AZs and Subnet Counts

Select number of availability zones and number of public/private subnets.

The screenshot shows the 'Create VPC workflow' success page. At the top, there's a navigation bar with 'aws' logo, search bar, and various icons. Below it, the breadcrumb trail reads: 'VPC > Your VPCs > Create VPC > Create VPC resources'. The main content area has a 'Success' message with a checkmark icon. A 'Details' section is expanded, listing 21 successful steps in a bulleted list, each with a link icon:

- Create VPC: vpc-0097f7790d04b6897
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-0097f7790d04b6897
- Create S3 endpoint: vpce-0af1cbe298b6f1b1
- Create subnet: subnet-09999dc5c7b9287f
- Create subnet: subnet-05a80efda36573745
- Create internet gateway: igw-0b52a7faf441ef351
- Attach internet gateway to the VPC
- Create route table: rtb-05dcc654961a4ed2
- Create route
- Associate route table
- Create route table: rtb-056afc2ee782a2db3
- Associate route table
- Verifying route table creation
- Associate S3 endpoint with private subnet route tables: vpce-0af1cbe298b6f1b1

VPC Creation Workflow (Success)

The screenshot shows the 'VPC dashboard' for the newly created VPC. The left sidebar includes 'AWS Global View' and sections for 'Virtual private cloud' (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways), 'CIDR', 'Flow logs', 'Tags', and 'Integrations'. The main panel displays the 'Details' tab for 'vpc-0097f7790d04b6897 / my-vpc'. The details are organized into four columns:

Details	Info	Actions
VPC ID	vpc-0097f7790d04b6897	Actions
DNS resolution	Enabled	Actions
Main network ACL	acl-0564ab9bbbaef4063	Actions
IPv6 CIDR (Network border group)	-	Actions
State	Available	Actions
Tenancy	default	Actions
Default VPC	No	Actions
Network Address Usage metrics	Disabled	Actions
Block Public Access	Off	Actions
DHCP option set	dopt-09e9ca9be0b35c4aa	Actions
IPv4 CIDR	10.0.0.0/16	Actions
Route 53 Resolver DNS Firewall rule groups	-	Actions
DNS hostnames	Enabled	Actions
Main route table	rtb-00f4fd6aa7a791425	Actions
IPv6 pool	-	Actions
Owner ID	072087969837	Actions

Below the details, there are tabs for 'Resource map', 'CIDRs', 'Flow logs', 'Tags', and 'Integrations'. A 'Show all details' button is located at the bottom right.

VPC Details (my-vpc)

Verify VPC details: VPC ID, DNS, CIDR and route table references.

Subnets List

The screenshot shows the AWS VPC Subnets List page. The left sidebar shows the VPC dashboard with sections for Virtual private cloud, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, and Security. The main area displays a table titled "Subnets (5) Info" with columns for Name, Subnet ID, State, VPC, Block Public..., and IP. The subnets listed are:

Name	Subnet ID	State	VPC	Block Public...	IP
-	subnet-00f59e1219002f218	Available	vpc-04c424b1e61df21cc	Off	172.31.1.0/24
my-subnet-public1-eu-north-1a	subnet-09999dc5c7b9287f	Available	vpc-0097f7790d04b6897 my-vpc	Off	172.31.2.0/24
-	subnet-06746047d13fef1be	Available	vpc-04c424b1e61df21cc	Off	172.31.3.0/24
my-subnet-private1-eu-north-1a	subnet-05a80efda36573745	Available	vpc-0097f7790d04b6897 my-vpc	Off	172.31.4.0/24
-	subnet-024ccccca5cb89134a	Available	vpc-04c424b1e61df21cc	Off	172.31.5.0/24

A message at the bottom says "Select a subnet".

View the created subnets: public and private subnets listed under the VPC.

Internet Gateways (Attached)

The screenshot shows the AWS VPC Internet Gateways List page. The left sidebar shows the VPC dashboard with sections for Virtual private cloud, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, and Security. The main area displays a table titled "Internet gateways (2) Info" with columns for Name, Internet gateway ID, State, VPC ID, and Owner. The internet gateway listed is:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-005386f7b42c8bba1	Attached	vpc-04c424b1e61df21cc	0720879
my-igw	igw-0b52a7faf441ef551	Attached	vpc-0097f7790d04b6897 my-vpc	0720879

A message at the bottom says "Select an internet gateway above".

Confirm the Internet Gateway is created and attached to the VPC.

Route Tables

The screenshot shows the AWS VPC Route Tables page. On the left, there's a sidebar for 'Virtual private cloud' with options like 'Your VPCs', 'Subnets', 'Route tables', and 'Internet gateways'. The main area displays a table titled 'Route tables (4) Info' with columns for Name, Route table ID, Explicit subnet assoc..., and Edge association. The table lists four entries:

Name	Route table ID	Explicit subnet assoc...	Edge association
my-rtb-private1-eu-north-1a	rtb-056afc2ee782a2db3	subnet-05a80efda36573...	-
-	rtb-0e2bce5cf8638bfc1	-	-
-	rtb-00f4fd6aa7a791425	-	-
my-rtb-public	rtb-05dccc654961a4ed2	subnet-09999dcd5c7b92...	-

A search bar at the top says 'Find route tables by attribute or tag'. A note at the top right says 'Last updated less than a minute ago'.

Check public and private route tables and their subnet associations.

Launch EC2

The screenshot shows the AWS EC2 'Launch an instance' page. The top navigation bar includes 'Search' and 'EC2 > Instances > Launch an instance'. The main form has a 'Name and tags' section where 'VPC-Ec2' is entered. To the right, a 'Summary' panel shows 'Number of instances: 1'. Below this are sections for 'Software Image (Amazon Linux 2023 kernel-6.1 AMI)', 'Virtual server type (t3.micro)', 'Firewall (security group New security group)', 'Storage (volumes 1 volume(s) - 8 GiB)', and a 'Cancel' button. The central area features a grid of recent and quick start AMIs, with 'macOS' currently selected. At the bottom, a detailed view of the 'Amazon Linux 2023 kernel-6.1 AMI' is shown, including its AMI ID, virtualization type (hvm), ENA enabled status, and root device type (ebs). A 'Free tier eligible' badge is also present.

▼ Network settings [Info](#)

VPC - required | [Info](#)

vpc-0097f7790d04b6897 (my-vpc)
10.0.0.0/16

Subnet | [Info](#)

subnet-09999dc5c7b9287f my-subnet-public1-eu-north-1a
VPC: vpc-0097f7790d04b6897 Owner: 072087969837
Availability Zone: eu-north-1a (eun1-az1) Zone type: Availability Zone
IP addresses available: 4091 CIDR: 10.0.0.0/20

[Create new subnet](#)

EC2 > Instances > Launch an instance

ⓘ It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices
[Take a walkthrough](#) [Do not show me this message again.](#)

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name Add additional tags

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Recents | [Quick Start](#)

▼ Summary

Number of instances: 1

Software Image: Amazon Linux : ami-0c7d68785e1

Virtual server type: t3.micro

Firewall (security groups): New security group

Storage (volumes): 1 volume(s) - 8

[Cancel](#)

EC2 > Instances > Launch an instance

VPC - required | [Info](#)

vpc-0097f7790d04b6897 (my-vpc)
10.0.0.0/16

Subnet | [Info](#)

subnet-05a80efda36573745 my-subnet-private1-eu-north-1a
VPC: vpc-0097f7790d04b6897 Owner: 072087969837
Availability Zone: eu-north-1a (eun1-az1) Zone type: Availability Zone
IP addresses available: 4091 CIDR: 10.0.128.0/20

[Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable

Firewall (security groups) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required

launch-wizard-4

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, -, _, and .

Instances Running (overview)

Instances (4) Info		Last updated less than a minute ago	Connect	Instance state	Actions	Launch instances	
		<input type="text"/> Find Instance by attribute or tag (case-sensitive)		All states			
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>		i-074b10c0c4dc5046f	Running View details Logs	t3.micro	3/3 checks passed View alarms +	View alarms	eu-north-1a
<input type="checkbox"/>	nida-ec2-lab	i-04daca2c062b9c1aa	Running View details Logs	t3.micro	3/3 checks passed View alarms +	View alarms +	eu-north-1a
<input type="checkbox"/>	VPC-Ec2	i-0482c7bb9975d956f	Running View details Logs	t3.micro	Initializing	View alarms +	eu-north-1a
<input type="checkbox"/>	VPC-EC2Pvt	i-0e62b4ba1823beadc	Running View details Logs	t3.micro	-	View alarms +	eu-north-1a

Instances launched: public and private instances should appear here.

Select Public Instance & Connect

Instances (1/4) Info		Last updated less than a minute ago	Connect	Instance state	Actions	Launch instances	
		<input type="text"/> Find Instance by attribute or tag (case-sensitive)		All states			
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>		i-074b10c0c4dc5046f	Running View details Logs	t3.micro	3/3 checks passed View alarms +	View alarms	eu-north-1a
<input type="checkbox"/>	nida-ec2-lab	i-04daca2c062b9c1aa	Running View details Logs	t3.micro	3/3 checks passed View alarms +	View alarms +	eu-north-1a
<input checked="" type="checkbox"/>	VPC-Ec2	i-0482c7bb9975d956f	Running View details Logs	t3.micro	3/3 checks passed View alarms +	View alarms +	eu-north-1a
<input type="checkbox"/>	VPC-EC2Pvt	i-0e62b4ba1823beadc	Running View details Logs	t3.micro	3/3 checks passed View alarms +	View alarms +	eu-north-1a

i-0482c7bb9975d956f (VPC-Ec2)

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | [Storage](#) | [Tags](#)

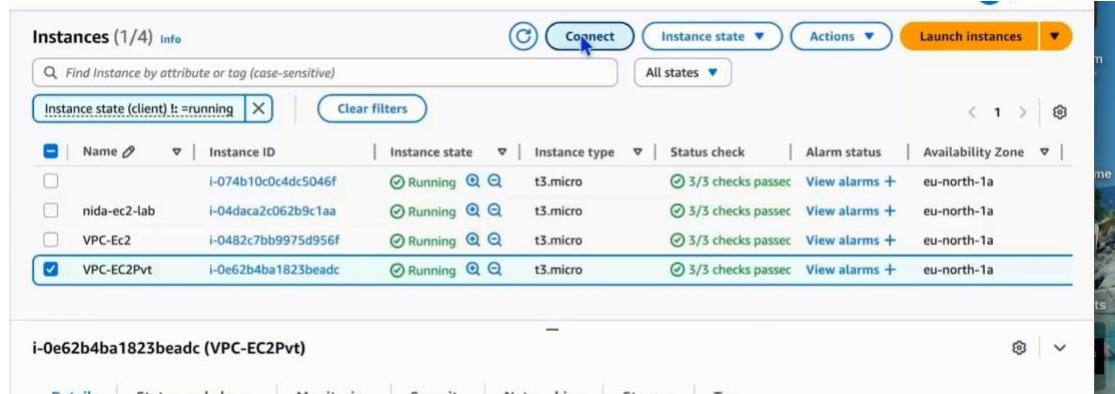
Select the public instance (VPC-Ec2) to connect using Instance Connect.

Ping Test from Public Instance

```
'`#`          Amazon Linux 2023
--`##`-
--`##`|
--`##`| https://aws.amazon.com/linux/amazon-linux-2023
--`##`| V-`-'>
---`-`/
--`-.`-`/
`-`m`-`/
Last login: Wed Nov 12 13:28:37 2025 from 13.48.4.202
[ec2-user@ip-10-0-9-30 ~]$ ping google.com
PING google.com (142.251.38.110) 56(84) bytes of data.
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=1 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=2 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=3 ttl=119 time=3.28 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=4 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=5 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=6 ttl=119 time=3.26 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=7 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=8 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=9 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=10 ttl=119 time=3.27 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=11 ttl=119 time=3.28 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=12 ttl=119 time=3.26 ms
64 bytes from lcarna-ac-in-f14.le100.net (142.251.38.110): icmp_seq=13 ttl=119 time=3.27 ms
```

Ping google.com from the public instance to verify internet access.

Select Private Instance & Connect Attempt



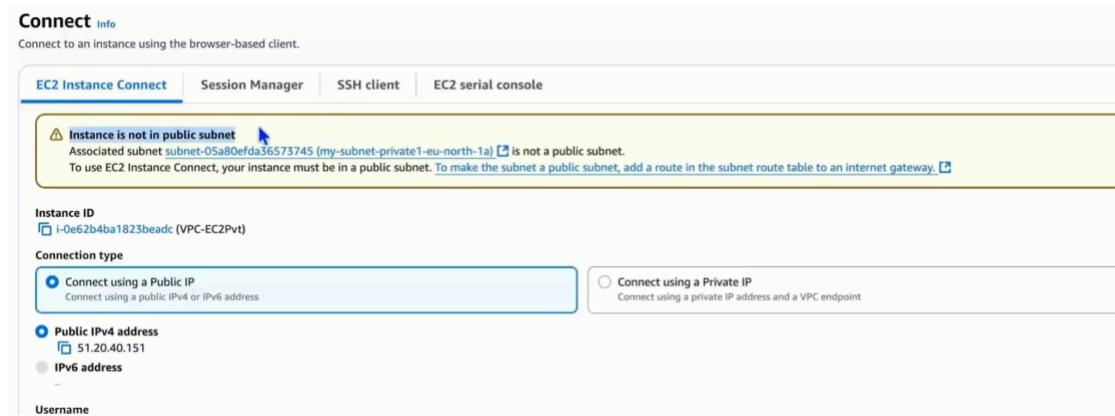
The screenshot shows the AWS EC2 Instances page. At the top, there are buttons for 'Instances (1/4) Info', 'Connect' (which is highlighted with a blue arrow), 'Instance state', 'Actions', and 'Launch instances'. Below this is a search bar and a 'Clear filters' button. A table lists four instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
i-074b10c0c4dc5046f	i-074b10c0c4dc5046f	Running	t3.micro	3/3 checks passed	View alarms +	eu-north-1a
nida-ec2-lab	i-04daca2c062b9c1aa	Running	t3.micro	3/3 checks passed	View alarms +	eu-north-1a
VPC-Ec2	i-0482c7bb9975d956f	Running	t3.micro	3/3 checks passed	View alarms +	eu-north-1a
VPC-EC2Pvt	i-0e62b4ba1823beadc	Running	t3.micro	3/3 checks passed	View alarms +	eu-north-1a

Below the table, the selected instance is shown in a details panel: **i-0e62b4ba1823beadc (VPC-EC2Pvt)**.

Attempt to connect to the private instance — shows instance is not in public subnet.

Network Settings while launching EC2 (subnet selection)



The screenshot shows the 'EC2 Instance Connect' page. At the top, there are tabs for 'EC2 Instance Connect', 'Session Manager', 'SSH client', and 'EC2 serial console'. A warning message is displayed: **Instance is not in public subnet**. It states that the associated subnet [subnet-05a80efda36573745 \(my-subnet-private1-eu-north-1a\)](#) is not a public subnet. To use EC2 Instance Connect, the instance must be in a public subnet. [To make the subnet a public subnet, add a route in the subnet route table to an internet gateway.](#)

Below the warning, the 'Instance ID' is listed as **i-0e62b4ba1823beadc (VPC-EC2Pvt)**. The 'Connection type' section shows two options: 'Connect using a Public IP' (selected) and 'Connect using a Private IP'. Under 'Public IPv4 address', the IP **51.20.40.151** is listed. There is also an option for 'IPv6 address' which is currently disabled. A 'Username' field is present at the bottom.

This instance is in a private subnet — hence, it cannot be accessed directly from the internet

Conclusion

A Virtual LAN (VPC) with public and private subnets is now created and validated. The public subnet provides internet access via the Internet Gateway (verified by the ping test), while the private subnet remains isolated (connect attempts show it is not public). This setup demonstrates secure separation of internet-facing and internal resources in AWS.