

Objective:- NACL and Security Groups

S1) Create VPC and Subnet

The screenshot shows the 'Create VPC' page in the AWS Management Console. The breadcrumb navigation at the top reads 'VPC > Your VPCs > Create VPC'. The main heading is 'Create VPC' with an 'Info' link. Below this is a descriptive sentence: 'A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.'

The page is divided into two main sections: 'VPC settings' and 'Preview'.

VPC settings:

- Resources to create:** Two radio buttons are present: 'VPC only' (unselected) and 'VPC and more' (selected).
- Name tag auto-generation:** A section with an 'Info' link. It contains a checkbox labeled 'Auto-generate' which is checked. Below it is a text input field containing 'MyVPC'.
- IPv4 CIDR block:** A section with an 'Info' link. It contains a text input field with '172.21.0.0/18' and a label '16,384 IPs'. Below the input is a note: 'CIDR block size must be between /16 and /28.'

Preview:

The preview section shows a diagram of the VPC setup. It includes a box labeled 'VPC Show details' with the text 'Your AWS virtual network' and 'MyVPC-vpc'. To its right is a box labeled 'Subnets (2)' with the text 'Subnets within this VPC'. Under 'Subnets (2)', there is a sub-section 'us-east-1a' containing two subnets: 'MyVPC-subnet-public1-us-east-1a' and 'MyVPC-subnet-private1-us-east-1a'. Lines connect the VPC box to the subnet box.

The screenshot shows the 'Customize subnets' page in the AWS Management Console. The breadcrumb navigation at the top reads 'aws > Services > Search > [Alt+S]'. The main heading is 'Customize subnets' with an 'Info' link. Below this is a descriptive sentence: 'Choose the number of Availability Zones (AZs) in which to provision subnets. We recommend at least two AZs for high availability.'

The page is divided into several sections:

- Number of Availability Zones (AZs):** A section with an 'Info' link. It contains three buttons: '1', '2' (selected), and '3'. Below it is a link 'Customize AZs'.
- Number of public subnets:** A section with an 'Info' link. It contains two buttons: '0' and '2' (selected). Below it is a link 'Customize subnets CIDR blocks'.
- Number of private subnets:** A section with an 'Info' link. It contains three buttons: '0', '2' (selected), and '4'. Below it is a link 'Customize subnets CIDR blocks'.
- NAT gateways (\$):** A section with an 'Info' link. It contains a descriptive sentence: 'Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.' Below this are three buttons: 'None' (selected), 'In 1 AZ', and '1 per AZ'.

The screenshot shows the bottom section of the 'Create VPC' page in the AWS Management Console. The breadcrumb navigation at the top reads 'aws > Services > Search > [Alt+S]'. The main heading is 'Create VPC' with an 'Info' link. Below this is a descriptive sentence: 'Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.'

The page is divided into several sections:

- NAT gateways (\$):** A section with an 'Info' link. It contains a descriptive sentence: 'Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.' Below this are three buttons: 'None' (selected), 'In 1 AZ', and '1 per AZ'.
- VPC endpoints:** A section with an 'Info' link. It contains a descriptive sentence: 'Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.' Below this are two buttons: 'None' (selected) and 'S3 Gateway'.
- DNS options:** A section with an 'Info' link. It contains two checkboxes: 'Enable DNS hostnames' (checked) and 'Enable DNS resolution' (checked).
- Additional tags:** A section with a link 'Additional tags'.

At the bottom of the page are two buttons: 'Cancel' and 'Create VPC'.

aws

Services

Search

[Alt+S]

N. Virginia

Sarvesh Chaudhari

EC2 > Instances > Launch an instance

Launch an instance

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

Name

Webserver-1

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0440d3b780d96b29d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Review commands

aws

Services

Search

[Alt+S]

N. Virginia

Sarvesh Chaudhari

Network settings

VPC - required

vpc-0b0760faaf92e2297 (MyVPC-vpc)

172.21.0.0/18

Subnet

subnet-0e4896b35f2f8d81b

MyVPC-subnet-public1-us-east-1a

VPC: vpc-0b0760faaf92e2297 Owner: 992382819518

Availability Zone: us-east-1a IP addresses available: 1019 CIDR: 172.21.0.0/22

Create new subnet

Auto-assign public IP

Enable

Firewall (security groups)

Create security group

Select existing security group

Security group name - required

Feb23

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0440d3b780d96b29d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Review commands

Add security group inbound rules as ssh, http, https

aws

Services

Search

[Alt+S]

N. Virginia

Sarvesh Chaudhari

Launch an instance

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

Name

Webserver2-ssh allowed

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0440d3b780d96b29d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Review commands

SSH, HTTP, HTTPS allowed

Network settings

VPC - required [Info](#)

vpc-0b0760faaf92e2297 (MyVPC-vpc)
172.21.0.0/18

Subnet [Info](#)

subnet-09c5af1446cb3be56 MyVPC-subnet-public2-us-east-1b
VPC: vpc-0b0760faaf92e2297 Owner: 992382819518
Availability Zone: us-east-1b IP addresses available: 1019 CIDR: 172.21.4.0/22

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

Feb23-1

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, spaces, and _-./!@#.%&*~[]\$*

Description - required [Info](#)

Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...[read more](#)
ami-0440d3b780d96b29d

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel **Launch instance** [Review commands](#)

Give Security groups name

Security Groups (17) [Info](#)

[Find resources by attribute or tag](#)

	Name	Security group ID	Security group name	VPC ID
<input type="checkbox"/>	-	sg-0b6bb1ab/3c20z6z4	default	vpc-0bu7buraat9zezz
<input type="checkbox"/>	Demoserver-2	sg-0579e261cf58f5c0	Feb23-1	vpc-0b0760faaf92e22
<input type="checkbox"/>	Demoserver-1	sg-09354499bcbfeda423	Feb23	vpc-0b0760faaf92e22
<input type="checkbox"/>	-	sg-03cd7395acef78fc5	default	vpc-075f37c839f9253

Create security group

Give NACL names

Network interfaces (1/2) [Info](#)

[Search](#)

	Name	Network interface ID	Subnet ID	VPC ID	Availability Zone
<input checked="" type="checkbox"/>	DS-2	eni-06509e94ccb49ef2d	subnet-09c5af1446cb3be56	vpc-0b0760faaf92e2297	us-east-1b
<input type="checkbox"/>	DS-1	eni-015174192253e9510	subnet-0e4896b35f2f8d81b	vpc-0b0760faaf92e2297	us-east-1a

Create network interface

Now create NACL for VPC

aws Services Search [Alt+S] N. Virginia Sarvesh Chaudhari

Create network ACL Info

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

Name - optional
Creates a tag with a key of 'Name' and a value that you specify.

VPC
VPC to use for this network ACL.

vpc-0b0760faf92e2297 (MyVPC-vpc)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key **Value - optional**

You can add 49 more tags

Now associate the Subnets to the new VPC

aws Services Search [Alt+S] N. Virginia Sarvesh Chaudhari

VPC > Network ACLs > acl-0e73f96a23936cc18 / MyNACL > Edit subnet associations

Edit subnet associations Info

Change which subnets are associated with this network ACL.

Available subnets (2/2)

Filter subnet associations

<input checked="" type="checkbox"/>	Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	MyVPC-subnet-public1-...	subnet-0e4896b35f2f8...	acl-0e73f96a23936cc18 / MyN...	us-east-1a	172.21.0.0/22	-
<input checked="" type="checkbox"/>	MyVPC-subnet-public2-...	subnet-09c5af1446cb3...	acl-0e73f96a23936cc18 / MyN...	us-east-1b	172.21.4.0/22	-

Selected subnets

subnet-0e4896b35f2f8d81b / MyVPC-subnet-public1-us-east-1a subnet-09c5af1446cb3be56 / MyVPC-subnet-public2-us-east-1b

aws Services Search [Alt+S] N. Virginia Sarvesh Chaudhari

VPC dashboard EC2 Global View Filter by VPC: Select a VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways

You have successfully updated inbound rules for acl-0e73f96a23936cc18 / MyNACL

Network ACLs (1/3) Info

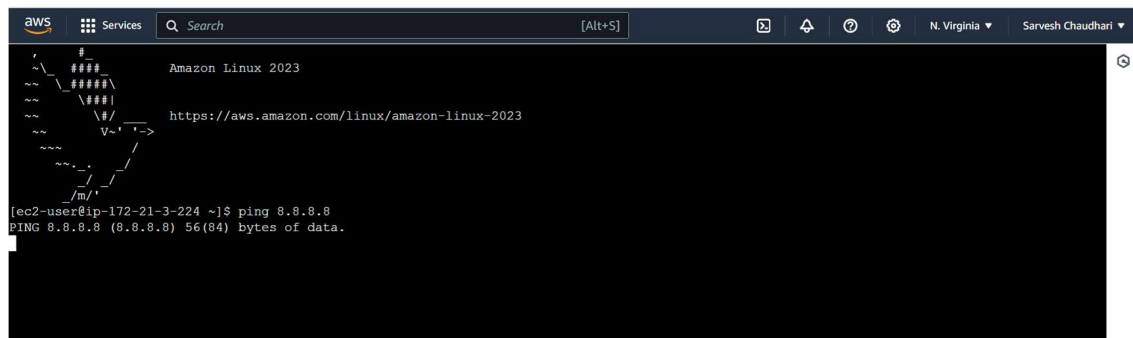
Find resources by attribute or tag

<input checked="" type="checkbox"/>	Name	Network ACL ID	Associated with	Default	VPC ID
<input type="checkbox"/>	VPC-bydefault	acl-04f0800d09407856a	-	Yes	vpc-0b0760faf92e2297
<input type="checkbox"/>	-	acl-0804aaef30d3cab2	6 Subnets	Yes	vpc-075f37d3
<input checked="" type="checkbox"/>	MyNACL	acl-0e73f96a23936cc18	2 Subnets	No	vpc-0b0760faf92e2297

Inbound rules

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
125	HTTP (80)	TCP (6)	80	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
150	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny



```
aws Services Search [Alt+S] N. Virginia Sarvesh Chaudhari
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-21-3-224 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Now trying to allow and deny some permissions in Sg and NACL to check the access to the instances.