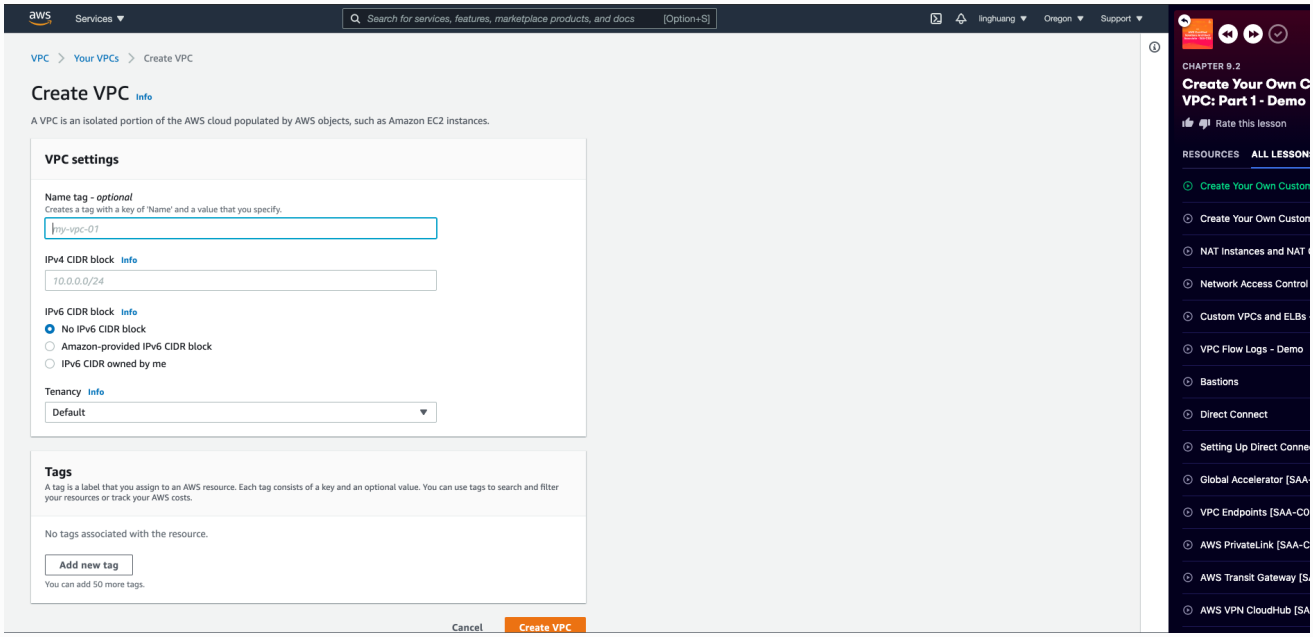
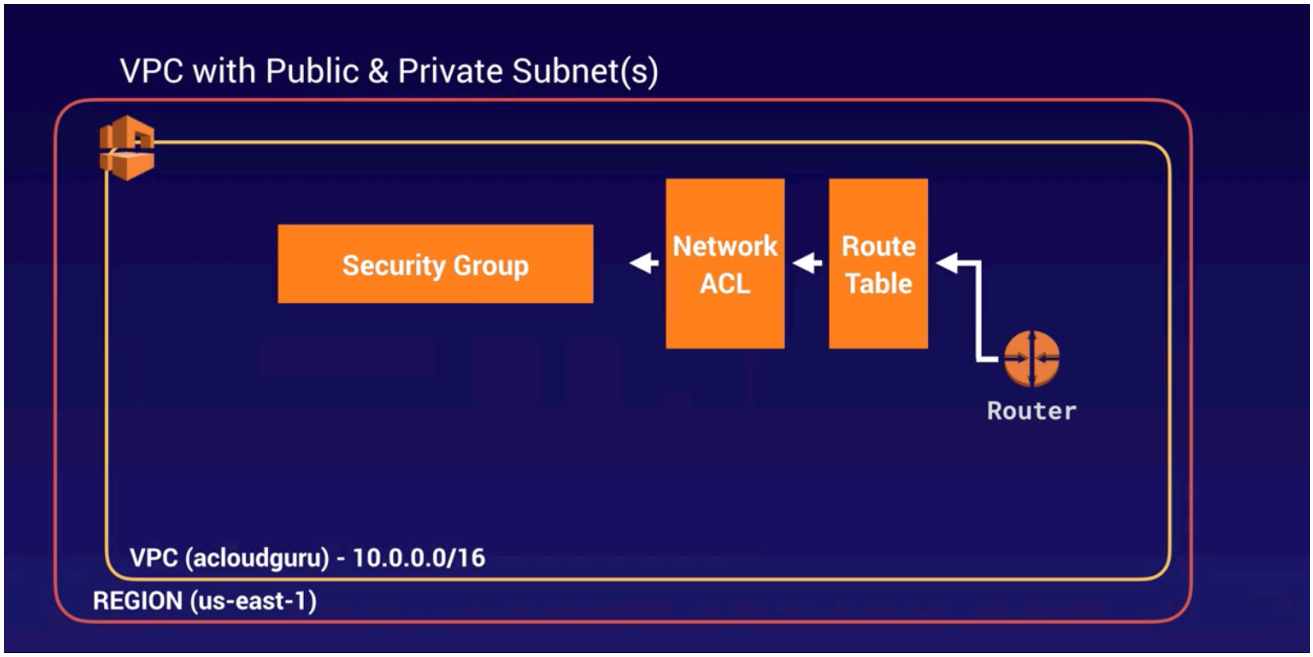
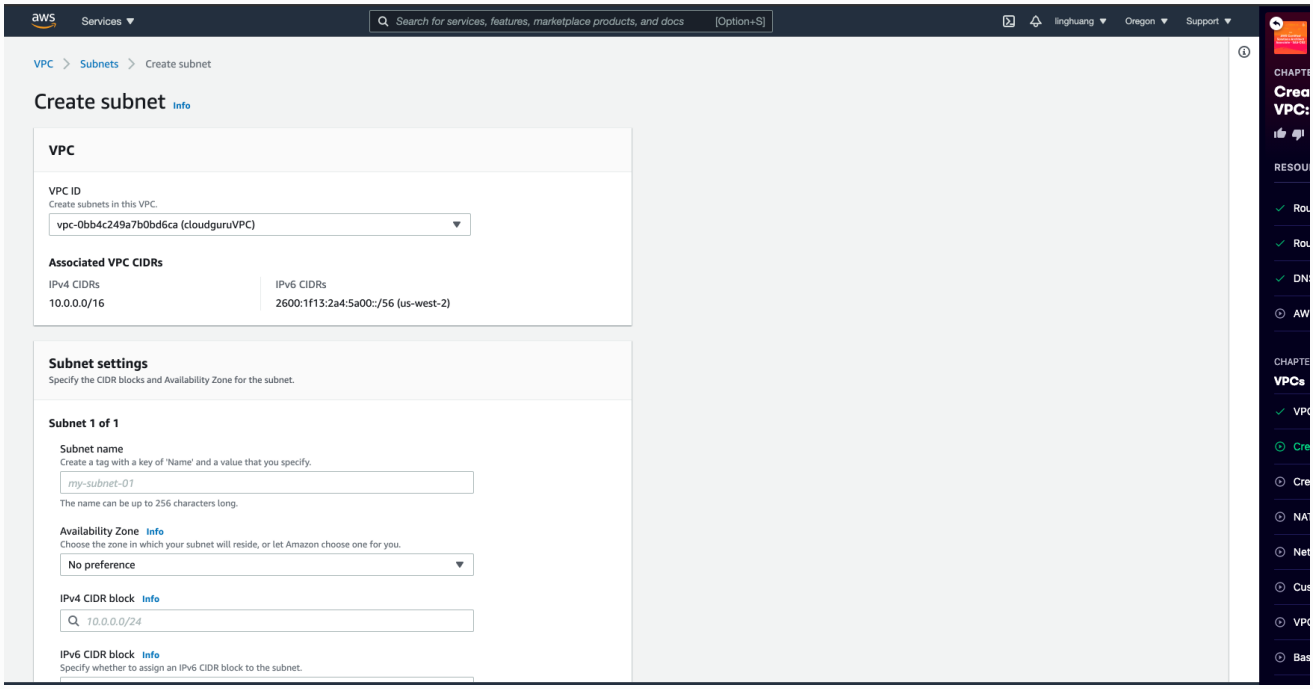
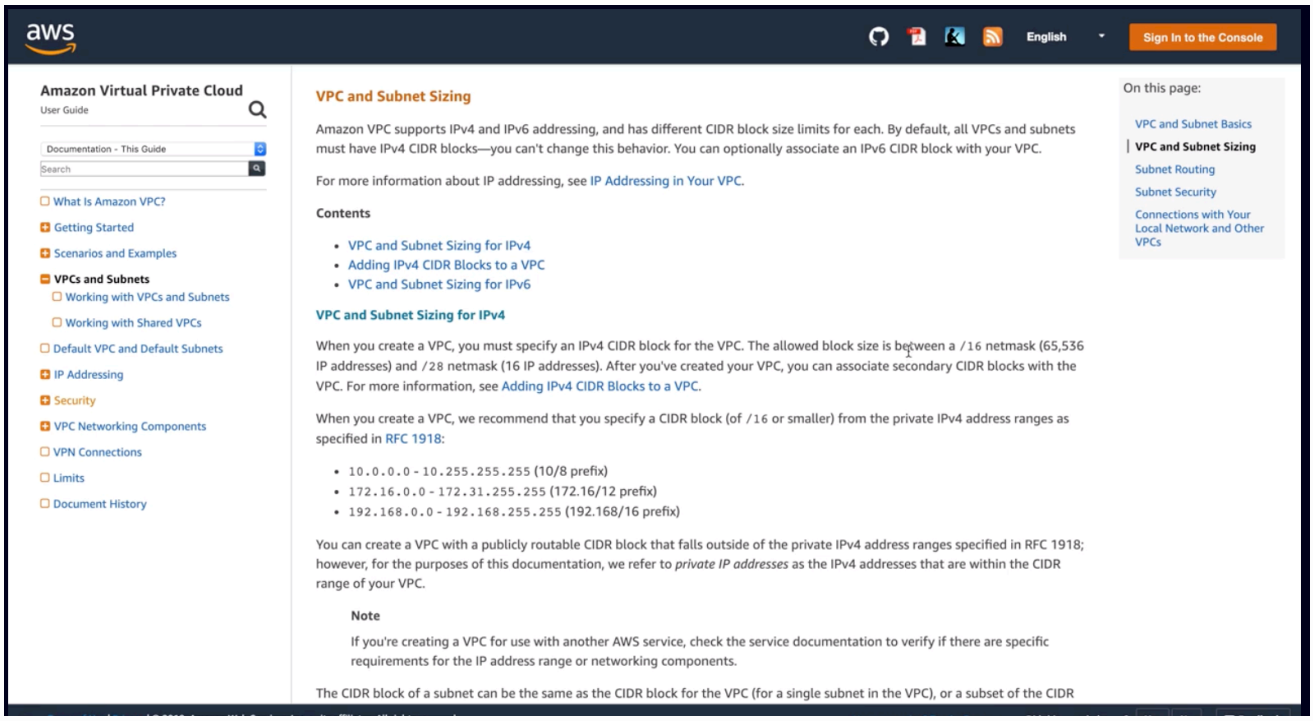

Services
Search for services, features, marketplace products, and docs [Option+S]
linghuang
Oregon
Support
VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.
VPC settings
Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
my-vpc-01
IPv4 CIDR block Info
10.0.0.0/24
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default
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.
No tags associated with the resource.
Add new tag
You can add 50 more tags.
Cancel
Create VPC
CHAPTER 9.2
Create Your Own C
VPC: Part 1 - Demo
Rate this lesson
RESOURCES
ALL LESSON
Create Your Own Custom
Create Your Own Custom
NAT Instances and NAT
Network Access Control
Custom VPCs and ELBs
VPC Flow Logs - Demo
Bastions
Direct Connect
Setting Up Direct Conne
Global Accelerator [SAA
VPC Endpoints [SAA-CO
AWS PrivateLink [SAA-C
AWS Transit Gateway [S
AWS VPN CloudHub [SA


VPC with Public & Private Subnet(s)
Security Group
Network ACL
Route Table
Router
VPC (acloudguru) - 10.0.0.0/16
REGION (us-east-1)


Services
Search for services, features, marketplace products, and docs [Option+S]
linghuang
Oregon
Support
VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-0bb4c249a7b0bd6ca (cloudguruVPC)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
IPv6 CIDRs
2600:1f13:2a4:5a00::/56 (us-west-2)
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-01
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference
IPv4 CIDR block Info
10.0.0.0/24
IPv6 CIDR block Info
Specify whether to assign an IPv6 CIDR block to the subnet.


aws
English
Sign In to the Console
Amazon Virtual Private Cloud
User Guide
Documentation - This Guide
Search
What Is Amazon VPC?
Getting Started
Scenarios and Examples
VPCs and Subnets
Working with VPCs and Subnets
Working with Shared VPCs
Default VPC and Default Subnets
IP Addressing
Security
VPC Networking Components
VPN Connections
Limits
Document History
VPC and Subnet Sizing
Amazon VPC supports IPv4 and IPv6 addressing, and has different CIDR block size limits for each. By default, all VPCs and subnets must have IPv4 CIDR blocks—you can't change this behavior. You can optionally associate an IPv6 CIDR block with your VPC.
For more information about IP addressing, see IP Addressing in Your VPC.
Contents
VPC and Subnet Sizing for IPv4
Adding IPv4 CIDR Blocks to a VPC
VPC and Subnet Sizing for IPv6
VPC and Subnet Sizing for IPv4
When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses). After you've created your VPC, you can associate secondary CIDR blocks with the VPC. For more information, see Adding IPv4 CIDR Blocks to a VPC.
When you create a VPC, we recommend that you specify a CIDR block (of /16 or smaller) from the private IPv4 address ranges as specified in RFC 1918:
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
You can create a VPC with a publicly routable CIDR block that falls outside of the private IPv4 address ranges specified in RFC 1918; however, for the purposes of this documentation, we refer to private IP addresses as the IPv4 addresses that are within the CIDR range of your VPC.
Note
If you're creating a VPC for use with another AWS service, check the service documentation to verify if there are specific requirements for the IP address range or networking components.
The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR
On this page:
VPC and Subnet Basics
VPC and Subnet Sizing
Subnet Routing
Subnet Security
Connections with Your Local Network and Other VPCs

If you're creating a VPC for use with another AWS service, check the service documentation to verify if there are specific requirements for the IP address range or networking components.

The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR block for the VPC (for multiple subnets). The allowed block size is between a `/28` netmask and `/16` netmask. If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

For example, if you create a VPC with CIDR block `10.0.0.0/24`, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block `10.0.0.0/25` (for addresses `10.0.0.0` - `10.0.0.127`) and the other uses CIDR block `10.0.0.128/25` (for addresses `10.0.0.128` - `10.0.0.255`).

There are many tools available to help you calculate subnet CIDR blocks; for example, see http://www.subnet-calculator.com/cidr.php. Also, your network engineering group can help you determine the CIDR blocks to specify for your subnets.

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use, and cannot be assigned to an instance. For example, in a subnet with CIDR block `10.0.0.0/24`, the following five IP addresses are reserved:

- `10.0.0.0`: Network address.
- `10.0.0.1`: Reserved by AWS for the VPC router.
- `10.0.0.2`: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information, see Amazon DNS Server.
- `10.0.0.3`: Reserved by AWS for future use.
- `10.0.0.255`: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

Adding IPv4 CIDR Blocks to a VPC

You can associate secondary IPv4 CIDR blocks with your VPC. When you associate a CIDR block with your VPC, a route is automatically added to your VPC route tables to enable routing within the VPC (the destination is the CIDR block and the target is `local`).

In the following example, the VPC on the left has a single CIDR block (`10.0.0.0/16`) and two subnets. The VPC on the right represents the architecture of the same VPC after you've added a second CIDR block (`10.2.0.0/16`) and created a new subnet from the range of the second CIDR.

Modify auto-assign IP settings Info

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

Settings

Subnet ID

subnet-0df99803db0a88aef

Auto-assign IPv4 Info

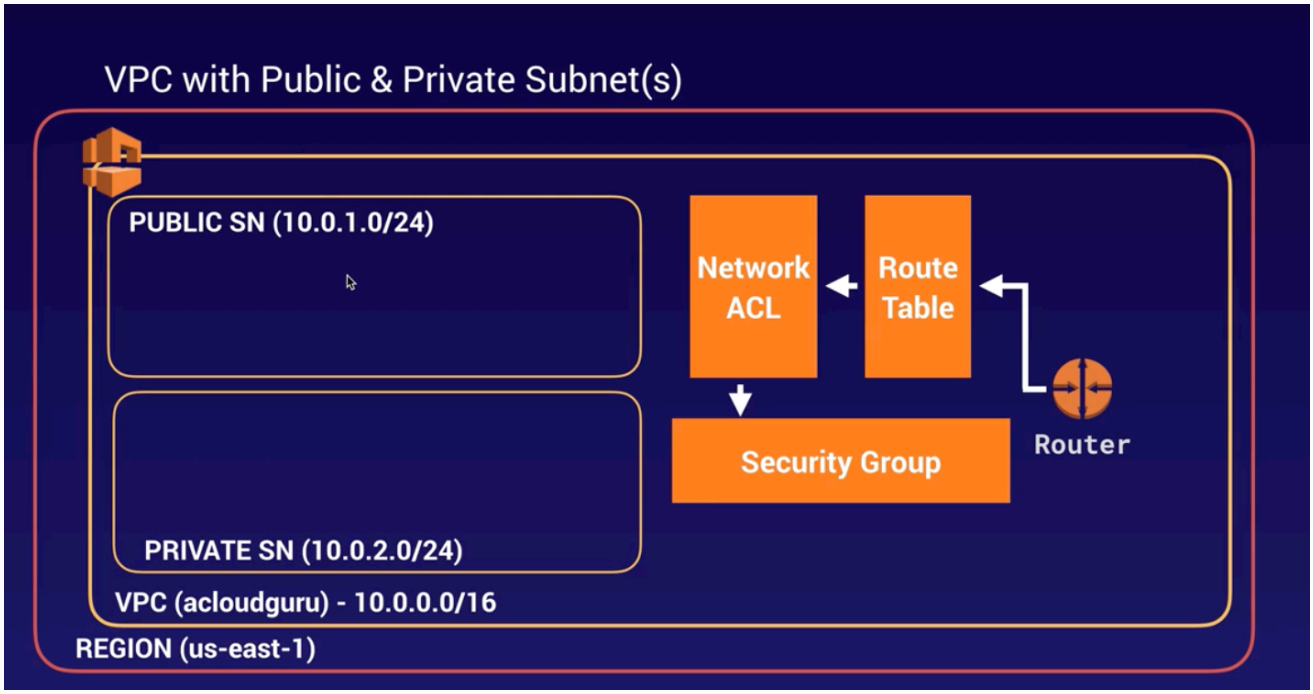
☑ Enable auto-assign public IPv4 address

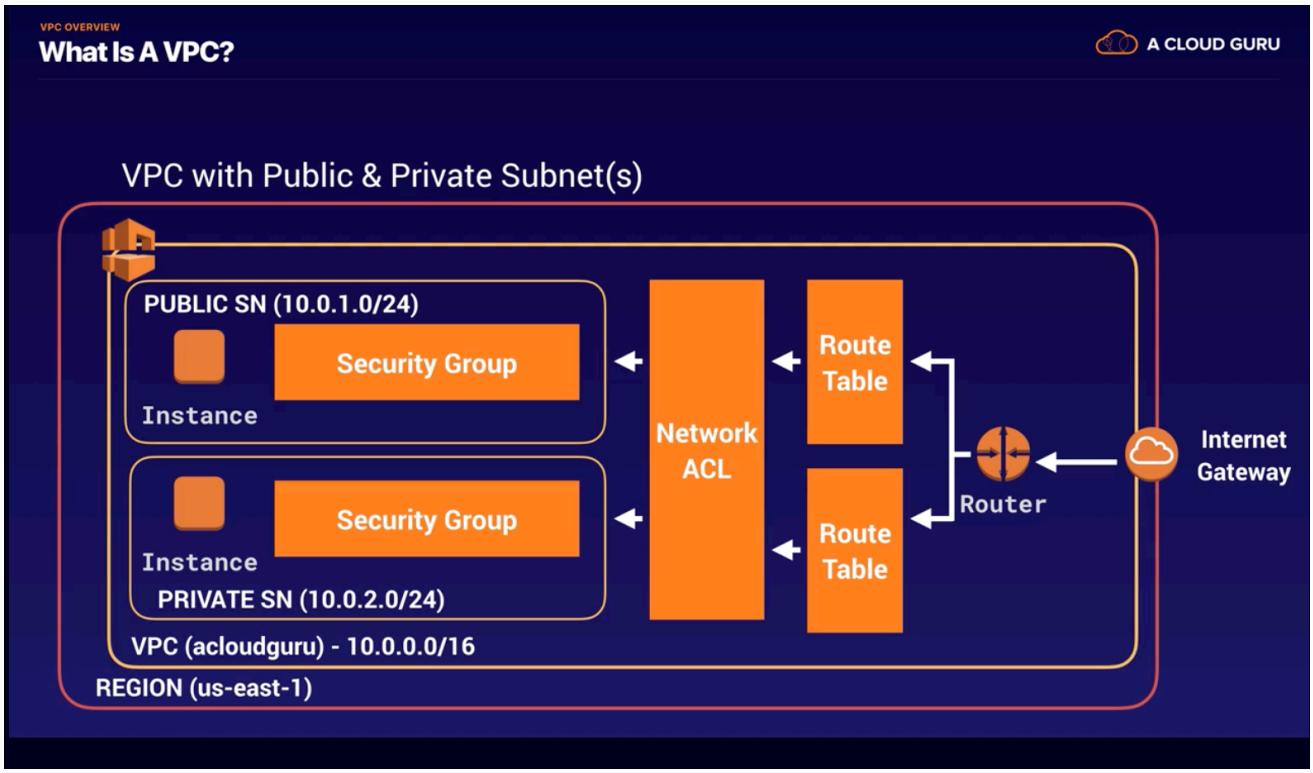
Auto-assign customer-owned IPv4 address Info

☐ Enable auto-assign customer-owned IPv4 address

Option disabled because no customer owned pools found.

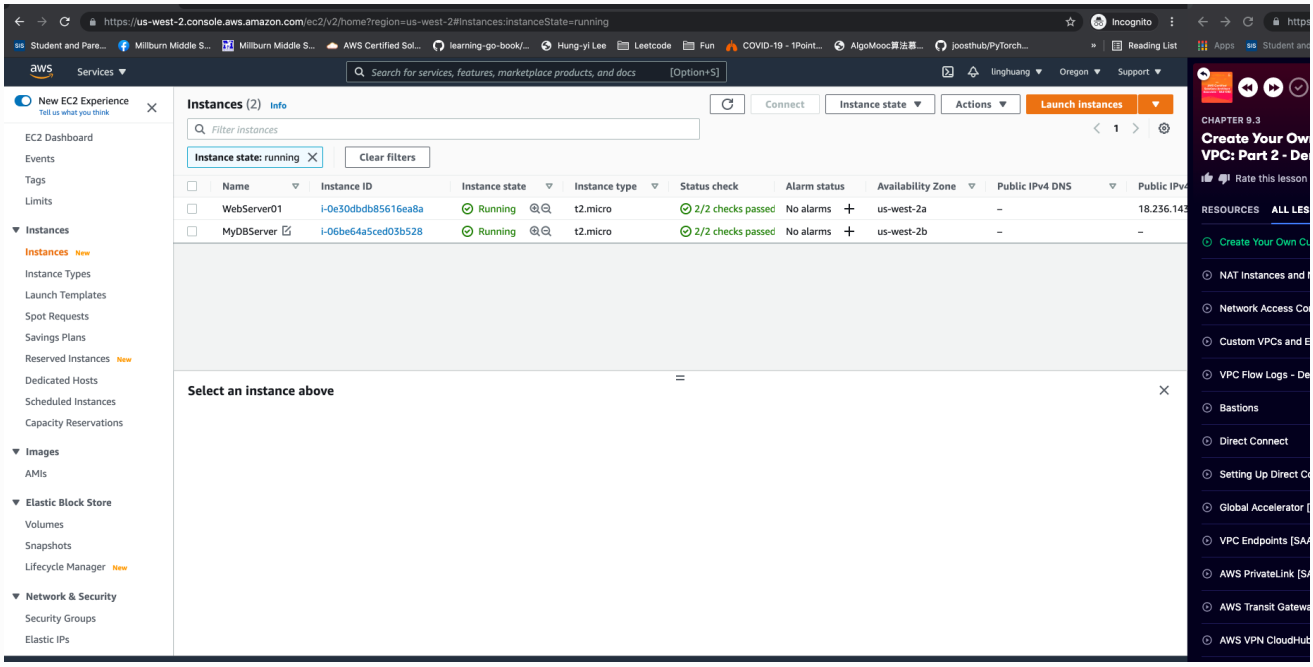
Cancel Save


VPC with Public & Private Subnet(s)
PUBLIC SN (10.0.1.0/24)
Network ACL
Route Table
Router
Security Group
PRIVATE SN (10.0.2.0/24)
VPC (acloudguru) - 10.0.0.0/16
REGION (us-east-1)


VPC OVERVIEW
What Is A VPC?
A CLOUD GURU
VPC with Public & Private Subnet(s)
PUBLIC SN (10.0.1.0/24)
Instance
Security Group
Network ACL
Route Table
Router
Internet Gateway
Instance
Security Group
Route Table
PRIVATE SN (10.0.2.0/24)
VPC (acloudguru) - 10.0.0.0/16
REGION (us-east-1)

Remember the following;

- When you create a VPC a default Route Table, Network Access Control List (NACL) and a default Security Group.
- It won't create any subnets, nor will it create a default internet gateway.
- US-East-1A in your AWS account can be a completely different availability zone to US-East-1A in another AWS account. The AZ's are randomized.
- Amazon always reserve 5 IP addresses within your subnets.
- You can only have 1 Internet Gateway per VPC.
- Security Groups can't span VPCs.



```
➜  ssh git:(master) ✗ ssh ec2-user@18.236.143.199 -i NewKP.pem
Last login: Mon Jul 26 01:27:18 2021 from pool-72-79-56-92.nwrknj.east.verizon.net

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
16 package(s) needed for security, out of 18 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-55 ~]$ sudo so
sudo: so: command not found
[ec2-user@ip-10-0-1-55 ~]$ sudo su
[root@ip-10-0-1-55 ec2-user]# ping 10.0.2.34
PING 10.0.2.34 (10.0.2.34) 56(84) bytes of data.
64 bytes from 10.0.2.34: icmp_seq=1 ttl=255 time=0.840 ms
64 bytes from 10.0.2.34: icmp_seq=2 ttl=255 time=0.860 ms
64 bytes from 10.0.2.34: icmp_seq=3 ttl=255 time=0.899 ms
64 bytes from 10.0.2.34: icmp_seq=4 ttl=255 time=0.815 ms
64 bytes from 10.0.2.34: icmp_seq=5 ttl=255 time=0.908 ms
64 bytes from 10.0.2.34: icmp_seq=6 ttl=255 time=0.842 ms
64 bytes from 10.0.2.34: icmp_seq=7 ttl=255 time=0.864 ms
64 bytes from 10.0.2.34: icmp_seq=8 ttl=255 time=0.816 ms
^C
--- 10.0.2.34 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7084ms
rtt min/avg/max/mdev = 0.815/0.855/0.908/0.043 ms
```

```
D3WM+PGt9BSH/URsHtJS2M4HRtV8sD8EZVoARQt6ARtVFb1G+IY=
-----END RSA PRIVATE KEY-----
[root@ip-10-0-1-55 ec2-user]# nano NewKP.pem
[root@ip-10-0-1-55 ec2-user]# cat NewKP.pem
cat: NewKP.pem: No such file or directory
[root@ip-10-0-1-55 ec2-user]# ls
NewKP.pemes
[root@ip-10-0-1-55 ec2-user]# chmod NewKP.pem
chmod: missing operand after ‘NewKP.pem’
Try 'chmod --help' for more information.
[root@ip-10-0-1-55 ec2-user]# chmod 400 NewKP.pem
chmod: cannot access ‘NewKP.pem’: No such file or directory
[root@ip-10-0-1-55 ec2-user]# nano NewKP.pem
[root@ip-10-0-1-55 ec2-user]# nano NewKP.pem
[root@ip-10-0-1-55 ec2-user]# chmod 400 NewKP.pem
[root@ip-10-0-1-55 ec2-user]# ls
NewKP.pem  NewKP.pemes
[root@ip-10-0-1-55 ec2-user]# ssh 10.0.2.34
The authenticity of host '10.0.2.34 (10.0.2.34)' can't be established.
ECDSA key fingerprint is SHA256:FDHNp3hGOdZyv2etQB6nvHoPJ8DhbatLTcCgXq5AwsY.
ECDSA key fingerprint is MD5:28:eb:62:c2:45:9d:58:58:51:a3:c5:4c:6b:cd:08:a7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.34' (ECDSA) to the list of known hosts.
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[root@ip-10-0-1-55 ec2-user]# ssh ec2-user@10.0.2.34 -i NewKP.pem

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-34 ~]$
```