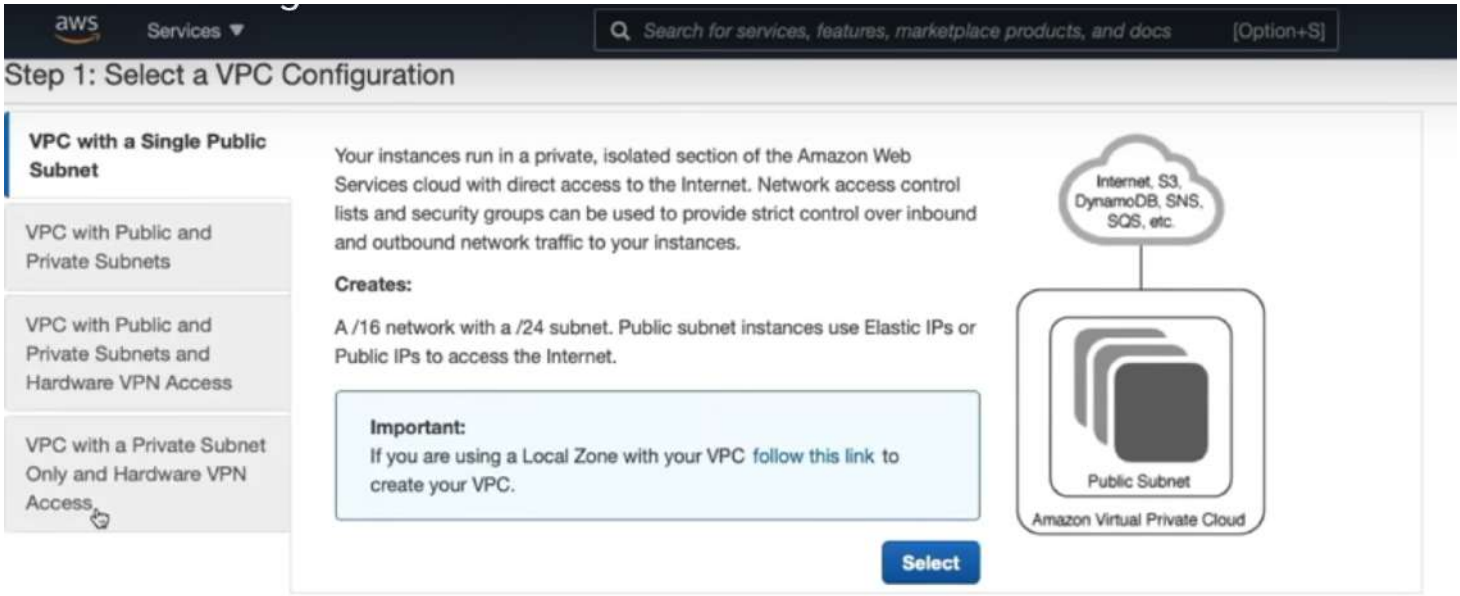
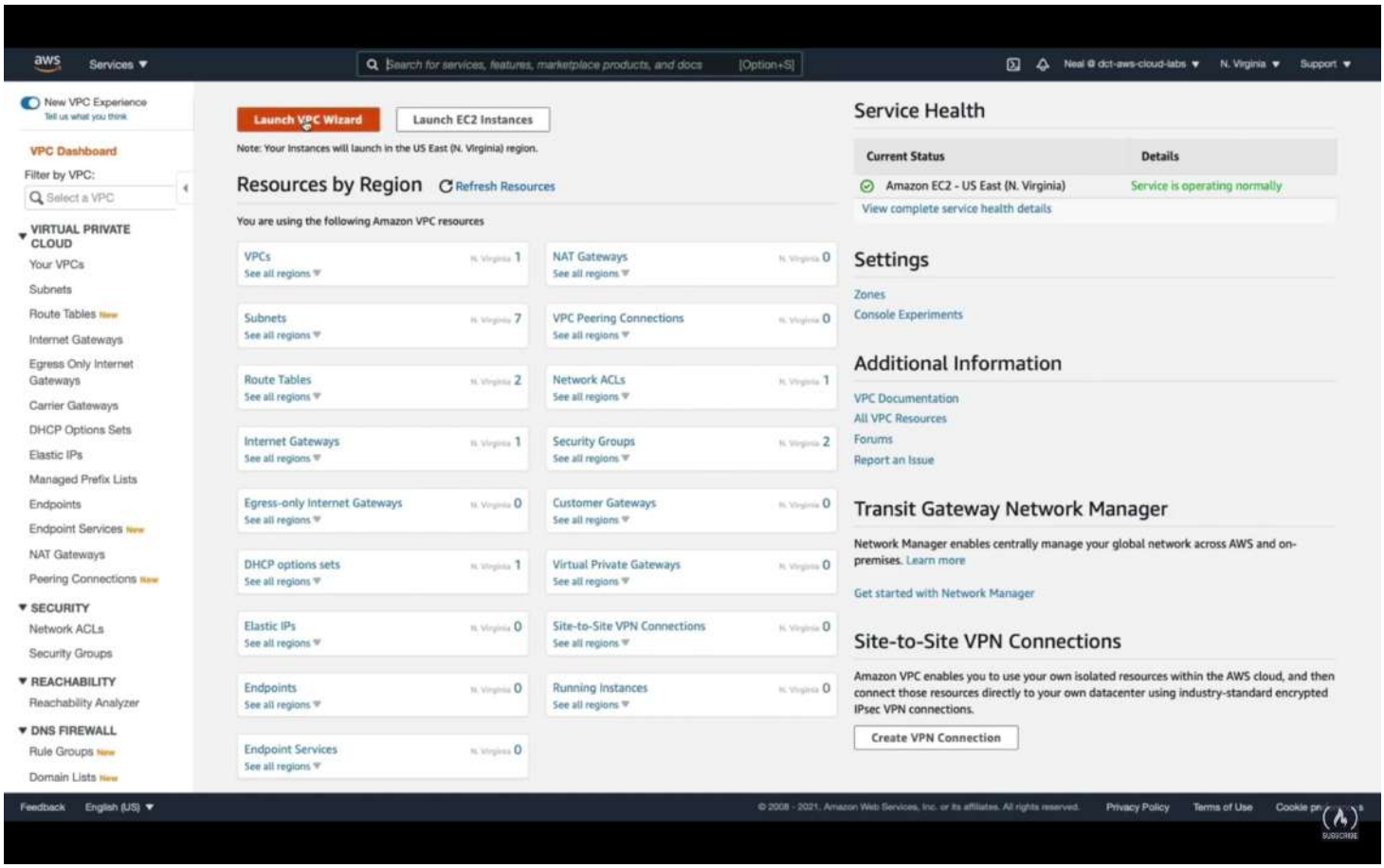
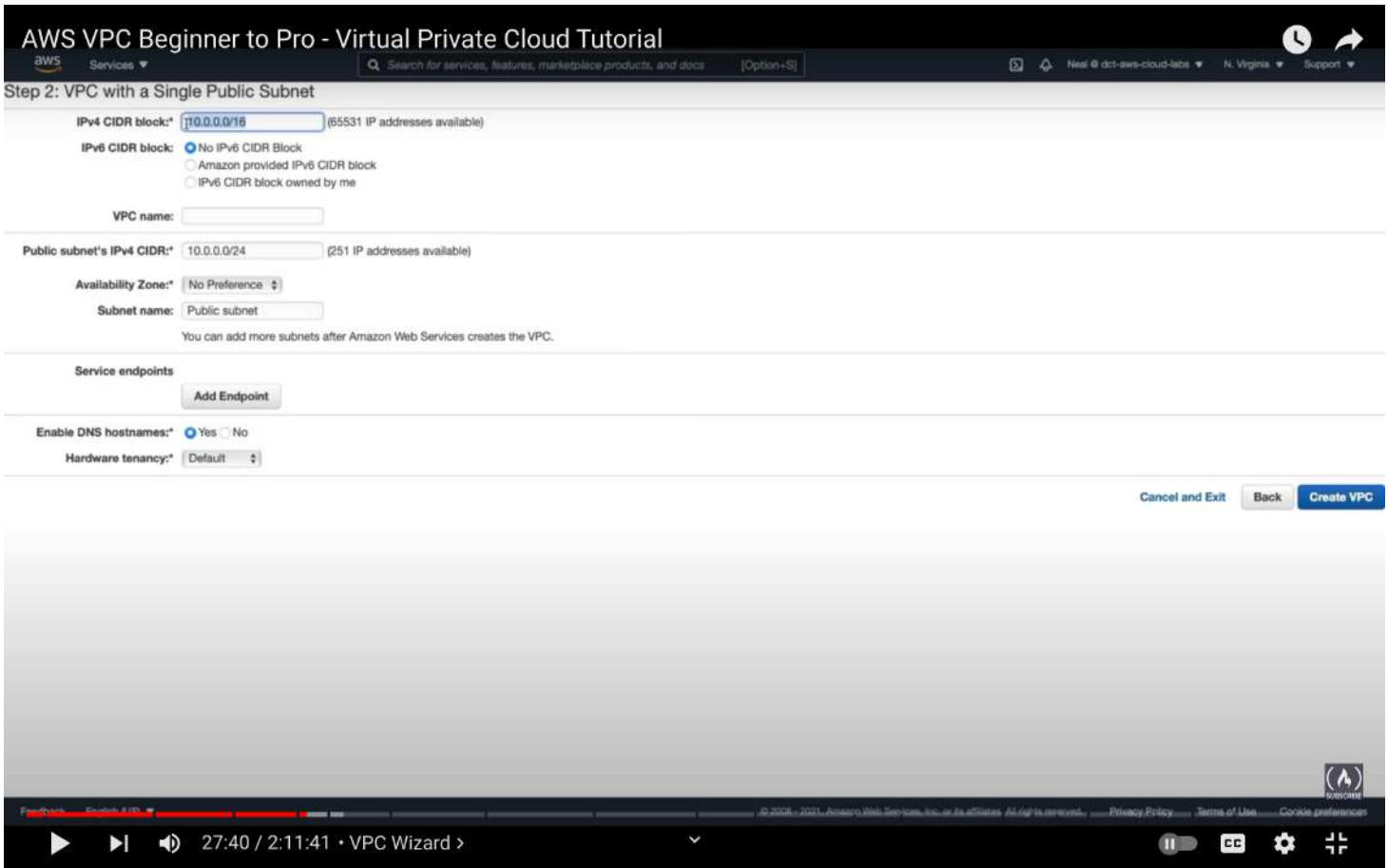
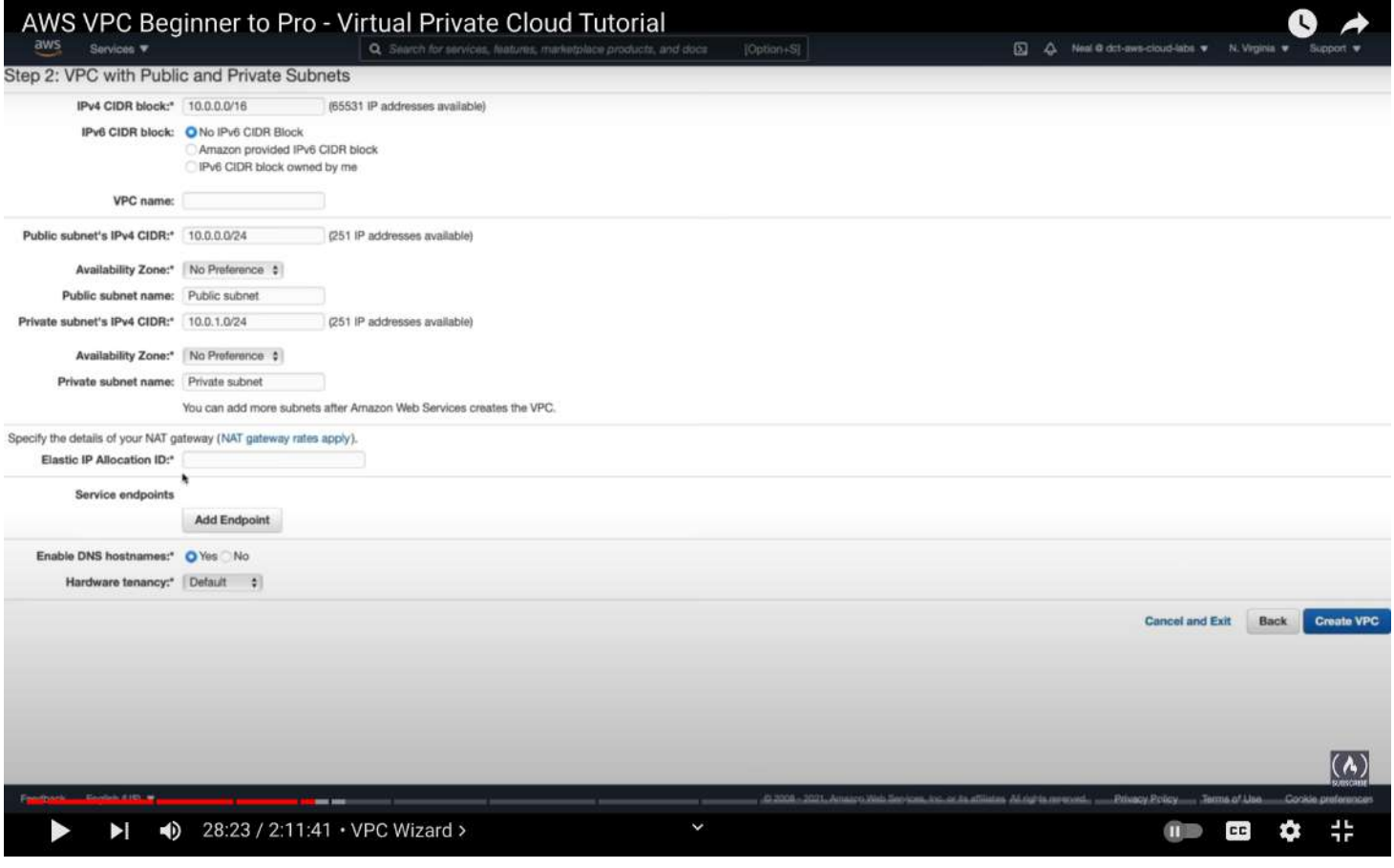

aws
Services
Search for services, features, marketplace products, and docs [Option+S]
Step 1: Select a VPC Configuration
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Your instances run in a private, isolated section of the Amazon Web Services cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.
Creates:
A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.
Important:
If you are using a Local Zone with your VPC follow this link to create your VPC.
Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Public Subnet
Amazon Virtual Private Cloud


aws
Services
Search for services, features, marketplace products, and docs [Option+S]
Neal @ dct-aws-cloud-labs
N. Virginia
Support
New VPC Experience
Tell us what you think
VPC Dashboard
Filter by VPC:
Select a VPC
VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables New
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Endpoint Services New
NAT Gateways
Peering Connections New
SECURITY
Network ACLs
Security Groups
REACHABILITY
Reachability Analyzer
DNS FIREWALL
Rule Groups New
Domain Lists New
Launch VPC Wizard
Launch EC2 Instances
Note: Your instances will launch in the US East (N. Virginia) region.
Resources by Region
Refresh Resources
You are using the following Amazon VPC resources
VPCs 1
NAT Gateways 0
Subnets 7
VPC Peering Connections 0
Route Tables 2
Network ACLs 1
Internet Gateways 1
Security Groups 2
Egress-only Internet Gateways 0
Customer Gateways 0
DHCP options sets 1
Virtual Private Gateways 0
Elastic IPs 0
Site-to-Site VPN Connections 0
Endpoints 0
Running Instances 0
Endpoint Services 0
Service Health
Current Status
Details
Amazon EC2 - US East (N. Virginia)
Service is operating normally
View complete service health details
Settings
Zones
Console Experiments
Additional Information
VPC Documentation
All VPC Resources
Forums
Report an Issue
Transit Gateway Network Manager
Network Manager enables centrally manage your global network across AWS and on-premises. Learn more
Get started with Network Manager
Site-to-Site VPN Connections
Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.
Create VPN Connection
Feedback
English (US)
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


AWS VPC Beginner to Pro - Virtual Private Cloud Tutorial
Step 2: VPC with a Single Public Subnet
IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
IPv6 CIDR block owned by me
VPC name:
Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)
Availability Zone:* No Preference
Subnet name: Public subnet
You can add more subnets after Amazon Web Services creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames:* Yes No
Hardware tenancy:* Default
Cancel and Exit
Back
Create VPC
27:40 / 2:11:41 • VPC Wizard ›


AWS VPC Beginner to Pro - Virtual Private Cloud Tutorial
Step 2: VPC with Public and Private Subnets
IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
IPv6 CIDR block owned by me
VPC name:
Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)
Availability Zone:* No Preference
Public subnet name: Public subnet
Private subnet's IPv4 CIDR:* 10.0.1.0/24 (251 IP addresses available)
Availability Zone:* No Preference
Private subnet name: Private subnet
You can add more subnets after Amazon Web Services creates the VPC.
Specify the details of your NAT gateway (NAT gateway rates apply).
Elastic IP Allocation ID:*
Service endpoints
Add Endpoint
Enable DNS hostnames:* Yes No
Hardware tenancy:* Default
Cancel and Exit
Back
Create VPC
28:23 / 2:11:41 • VPC Wizard ›

AWS VPC Beginner to Pro - Virtual Private Cloud Tutorial

Step 2: VPC with Public and Private Subnets and Hardware VPN Access

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: No IPv6 CIDR Block / Amazon provided IPv6 CIDR block / IPv6 CIDR block owned by me

VPC name:

Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Public subnet name: Public subnet

Private subnet's IPv4 CIDR:* 10.0.1.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Private subnet name: Private subnet

You can add more subnets after Amazon Web Services creates the VPC.

Enable DNS hostnames:* Yes No

Hardware tenancy:* Default

Cancel and Exit Back Next

28:55 / 2:11:41 • VPC Wizard ›

Create a Custom VPC with Subnets

DigitalCloud TRAINING

VPC CIDR Block and Subnets

VPC CIDR Block	10	0	0	0
/16 Subnet Mask	255	255	0	0

Subnet Name	IPv4 CIDR block	Availability Zone	Route Table	Auto-assign Public IPv4
private-1a	10.0.3.0/24	us-east-1a	Private-RT	No
private-1b	10.0.4.0/24	us-east-1b	Private-RT	No
public-1a	10.0.1.0/24	us-east-1a	MAIN	Yes
public-1b	10.0.2.0/24	us-east-1b	MAIN	Yes

Has a route to an **Internet Gateway**

Automatically assign **IPv4 Public addresses**

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.
MyVPC

IPv4 CIDR block Info
10.0.0.0/16

IPv6 CIDR block Info
- (•) No IPv6 CIDR block
- ( ) Amazon-provided IPv6 CIDR block
- ( ) IPv6 CIDR owned by me

Tenancy Info
Default

Tags

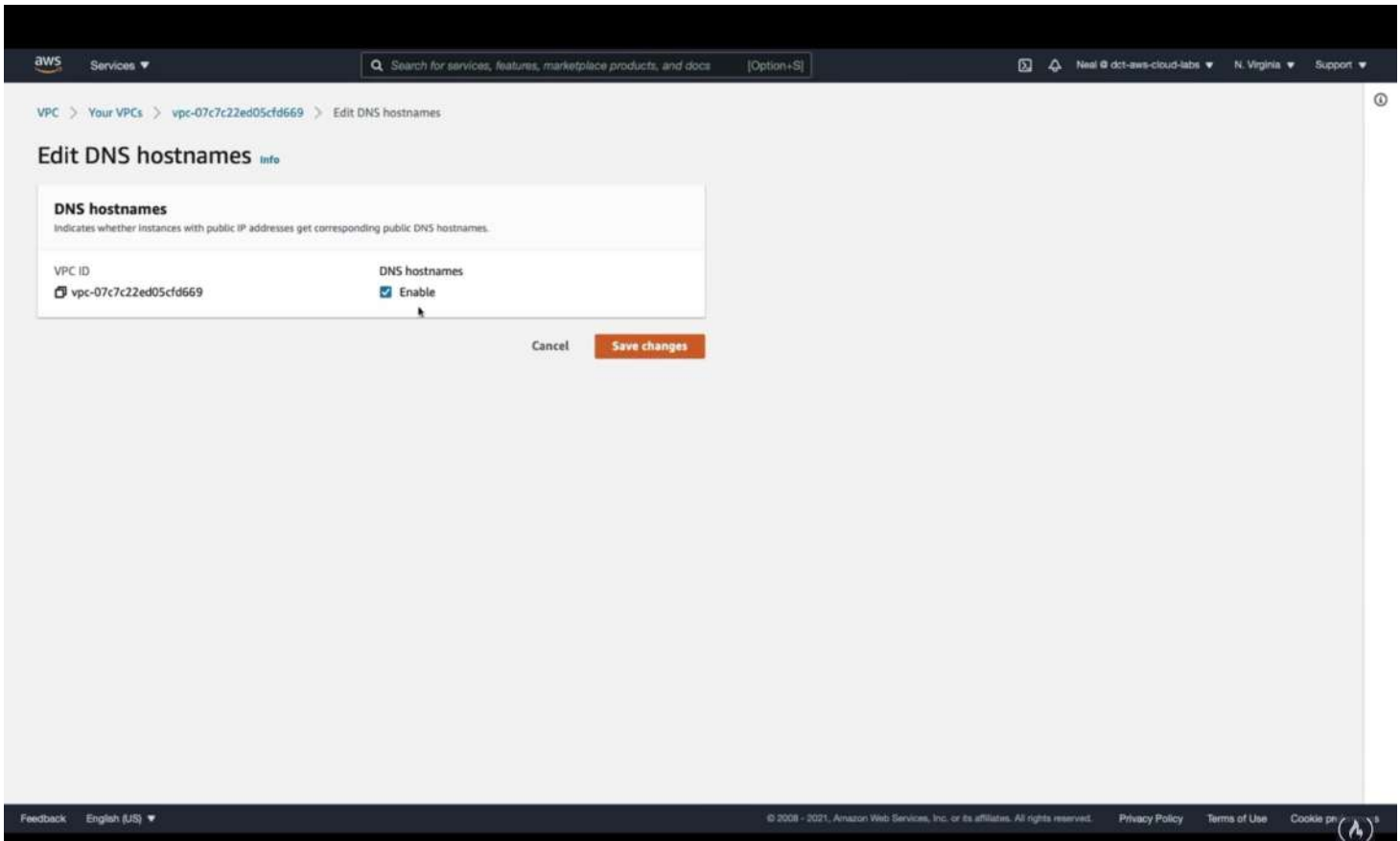
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

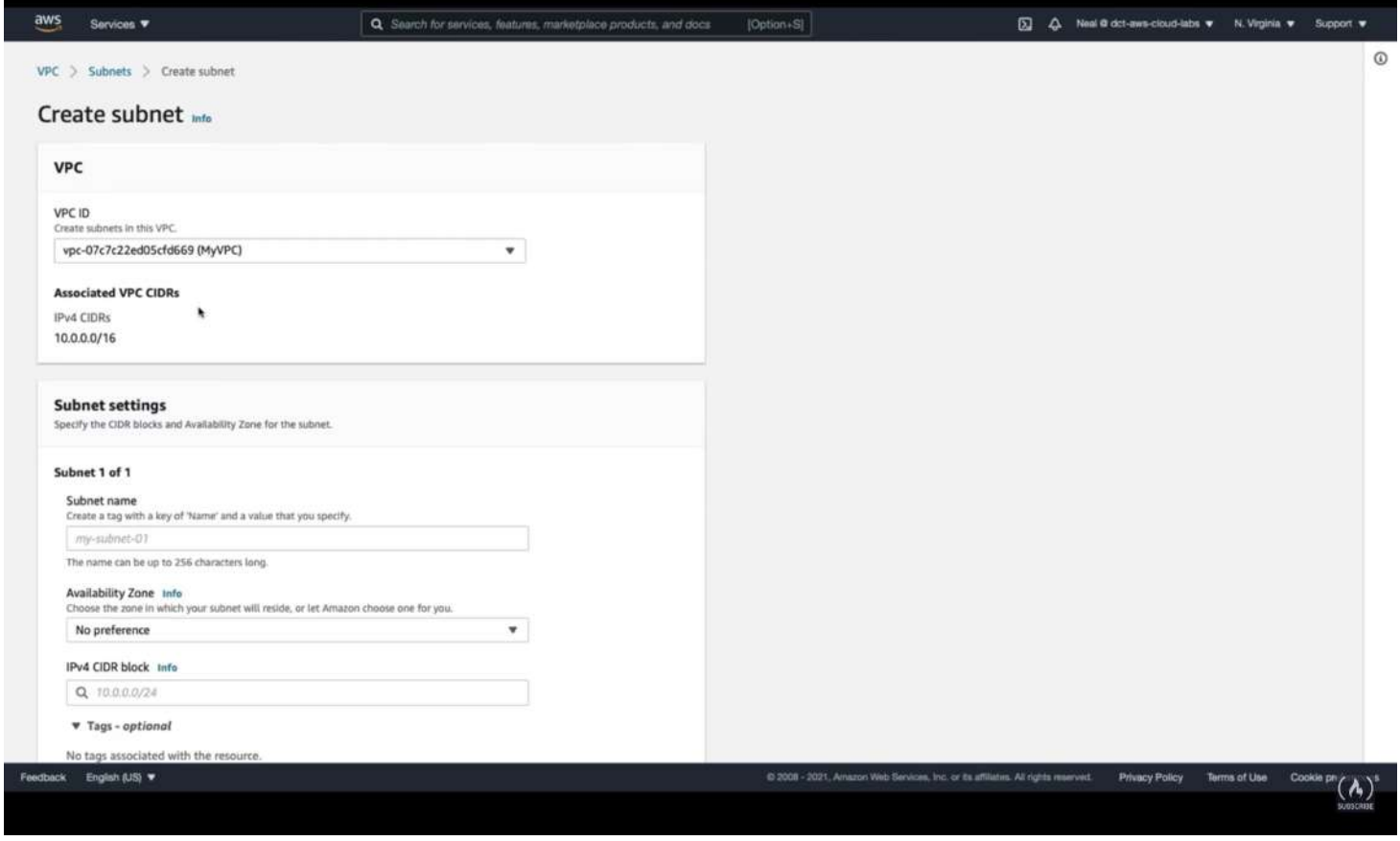
Key	Value - *optional*	
Name	MyVPC	Remove

Add new tag

You can add 49 more tags.

Cancel Create VPC


aws
Services
Search for services, features, marketplace products, and docs [Option+S]
Neal @ dct-aws-cloud-labs
N. Virginia
Support
VPC > Your VPCs > vpc-07c7c22ed05cfd669 > Edit DNS hostnames
Edit DNS hostnames Info
DNS hostnames
Indicates whether instances with public IP addresses get corresponding public DNS hostnames.
VPC ID
vpc-07c7c22ed05cfd669
DNS hostnames
Enable
Cancel
Save changes
Feedback
English (US)
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
SUBSCRIBE


aws
Services
Search for services, features, marketplace products, and docs [Option+S]
Neal @ dct-aws-cloud-labs
N. Virginia
Support
VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-07c7c22ed05cfd669 (MyVPC)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
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
Tags - optional
No tags associated with the resource.
Feedback
English (US)
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
SUBSCRIBE

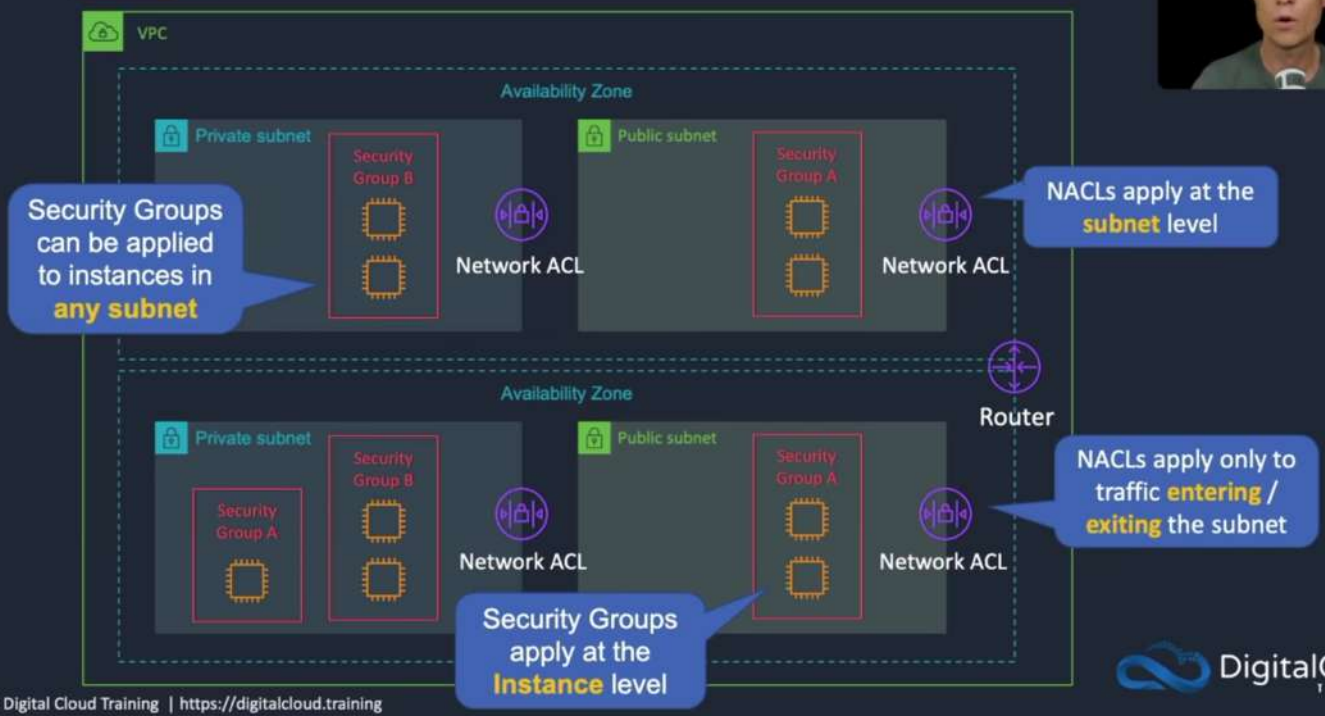
Launch Instances and Test VPC

DigitalCloud TRAINING

Security Groups and Network ACLs

DigitalCloud TRAINING

Security Groups and Network ACLs



Stateful vs Stateless Firewalls

PROTOCOL	SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT
HTTP	10.1.1.1	10.2.1.10	65188	80
HTTP	10.2.1.10	10.1.1.1	80	65188

A stateful firewall allows the return traffic automatically

A stateless firewall checks for an allow rule for both connections

Security Group Rules

Security groups support **allow** rules only

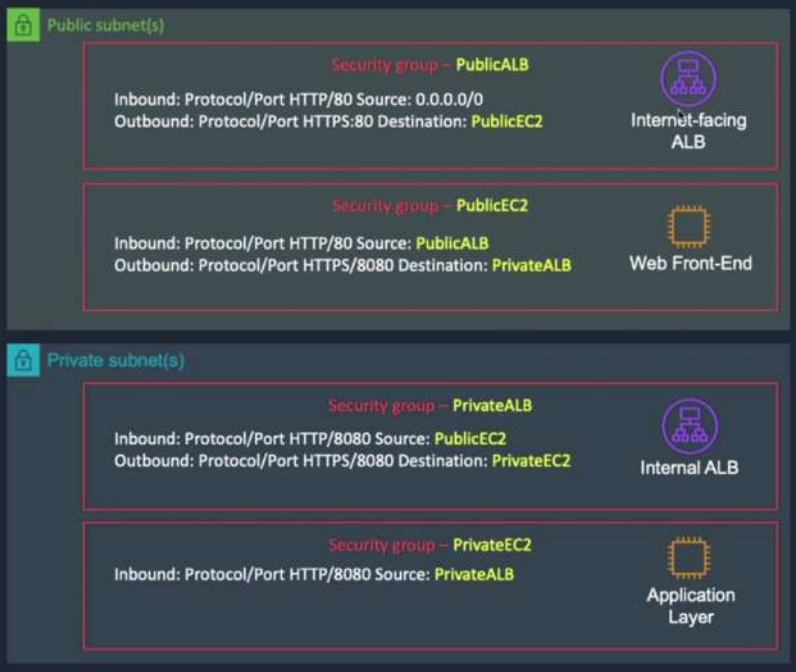
Inbound rules

Type	Protocol	Port range	Source
SSH	TCP	22	0.0.0.0/0
RDP	TCP	3389	0.0.0.0/0
RDP	TCP	3389	::/0
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0
All ICMP - IPv4	ICMP	All	0.0.0.0/0

Separate rules are defined for outbound traffic

A source can be an **IP address** or **security group ID**

Security Groups Best Practice



Network ACLs

Inbound Rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Outbound Rules

Rule #	Type	Protocol	Port Range	Destination	
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

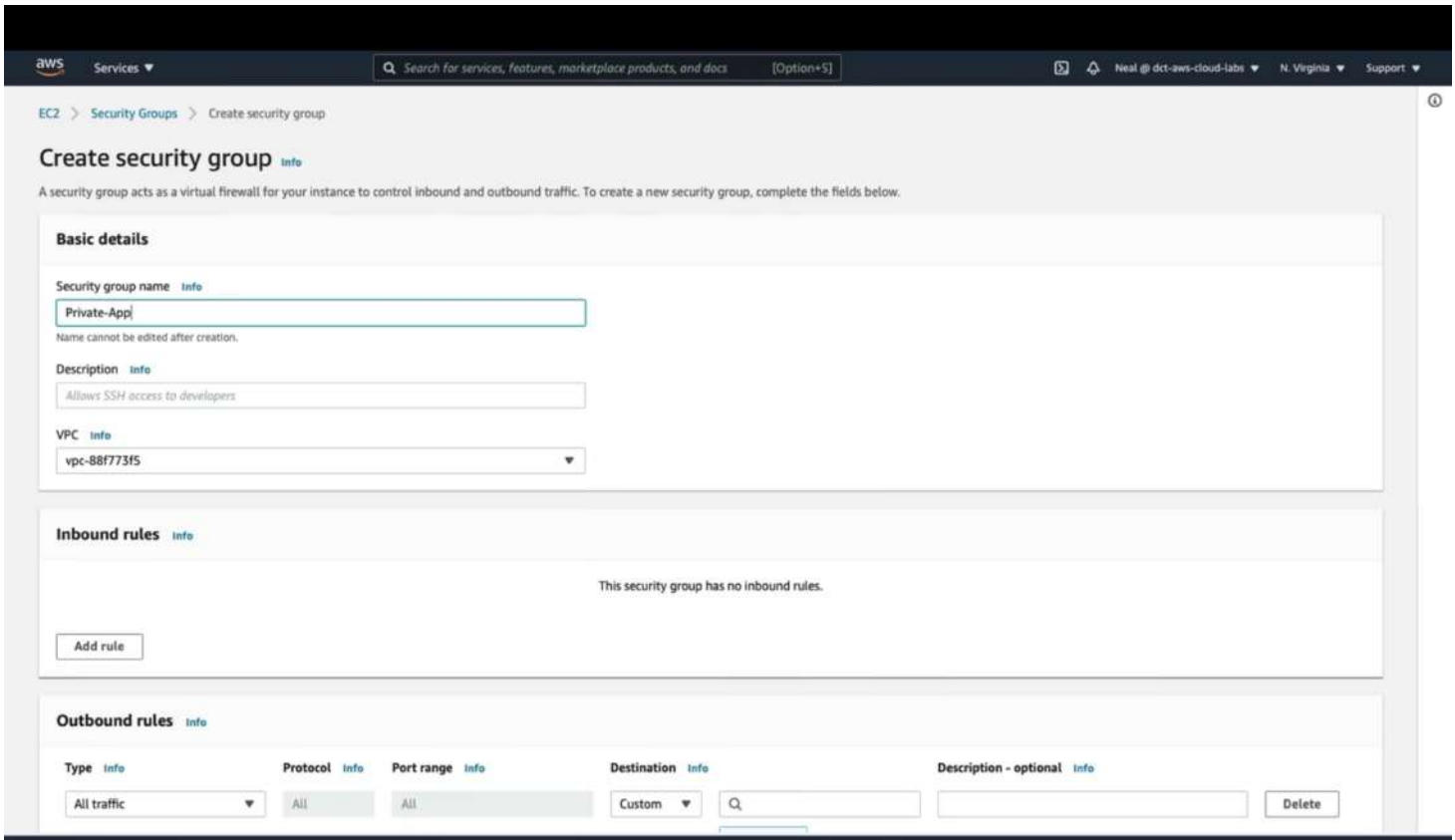
NACLs have an explicit deny

Rules are processed in order

DigitalCloud TRAINING

Configure Security Groups and NACLs

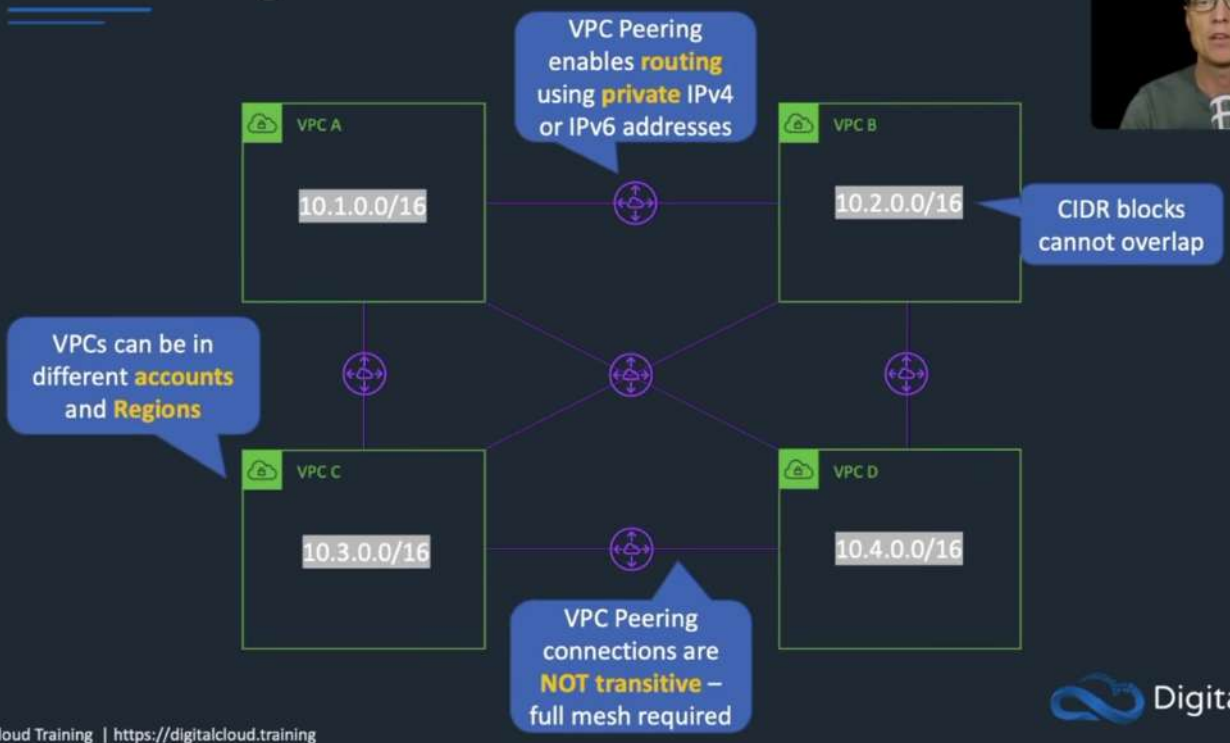
DigitalCloud TRAINING



VPC Peering

DigitalCloud TRAINING

VPC Peering



DigitalCloud TRAINING

SUBSCRIBE

VPC Peering

Security group (Region1-SG)

Protocol	Port	Source
ICMP	All	10.1.0.0/16
TCP	22	0.0.0.0/0

Security group (Region2-SG)

Protocol	Port	Source
ICMP	All	10.0.0.0/16
TCP	22	0.0.0.0/0

Route Table

Destination	Target
10.1.0.0/16	peering-id

Route Table

Destination	Target
10.0.0.0/16	peering-id

DigitalCloud TRAINING

SUBSCRIBE

Configure VPC Peering

If you only have one account, use a different Region

VPC Peering

Security group (VPCPEER-MGMT)

Protocol	Port	Source
ICMP	All	10.1.0.0/16
TCP	22	0.0.0.0/0

Security group (VPCPEER-PROD)

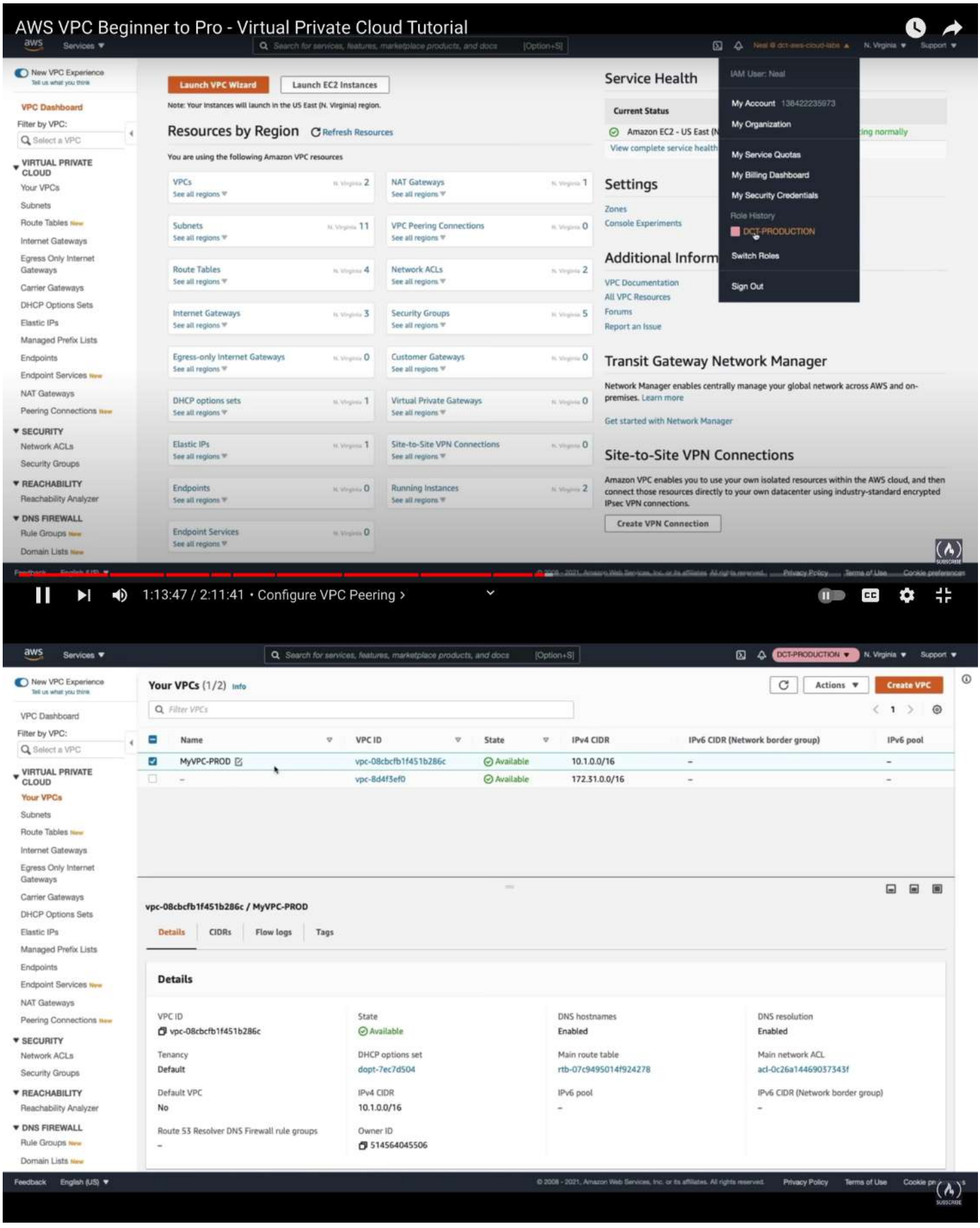
Protocol	Port	Source
ICMP	All	10.0.0.0/16
TCP	22	0.0.0.0/0

Route Table

Destination	Target
10.1.0.0/16	peering-id

Route Table

Destination	Target
10.0.0.0/16	peering-id


AWS VPC Beginner to Pro - Virtual Private Cloud Tutorial
Launch VPC Wizard
Launch EC2 Instances
Note: Your instances will launch in the US East (N. Virginia) region.
Resources by Region
Refresh Resources
You are using the following Amazon VPC resources
Service Health
Settings
Additional Inform
Transit Gateway Network Manager
Network Manager enables centrally manage your global network across AWS and on-premises. Learn more
Get started with Network Manager
Site-to-Site VPN Connections
Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.
Create VPN Connection
1:13:47 / 2:11:41 • Configure VPC Peering ›
Your VPCs (1/2) Info
MyVPC-PROD
vpc-08cbcfb1f451b286c / MyVPC-PROD
Details
CIDRs
Flow logs
Tags

custom-vpc-prod.md

Users > Neal > Documents > Code > Amazon VPC > custom-vpc-prod.md > # Create VPC

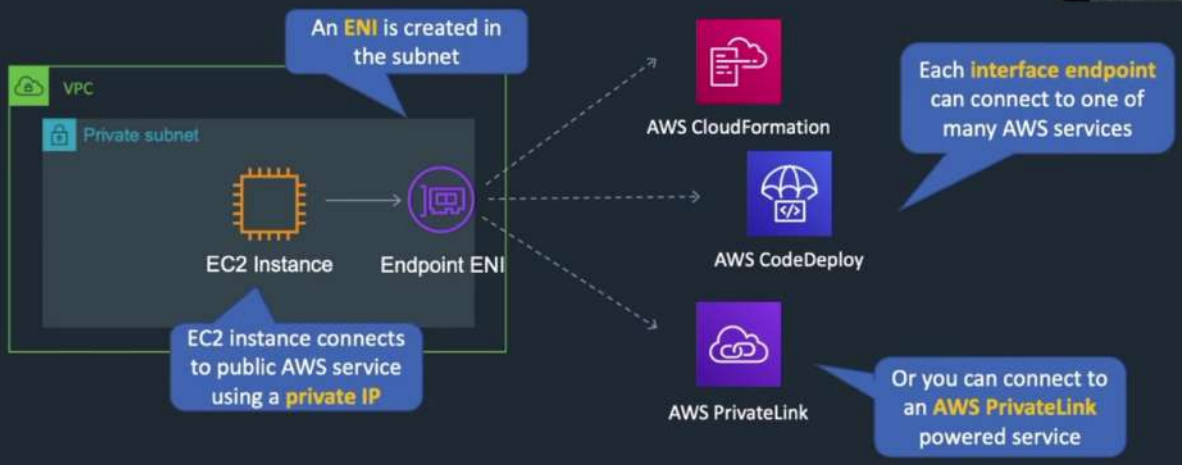
```
# Create VPC
Name: MyVPC-PROD
IPv4 CIDR Block: 10.1.0.0/16

# Create Subnets

Name: Public-1A
Availability Zone: us-east-1a
IPv4 CIDR Block: 10.1.1.0/24

Name: Public-1B
Availability Zone: us-east-1b
IPv4 CIDR Block: 10.1.2.0/24

Name: Private-1A
Availability Zone: us-east-1a
IPv4 CIDR Block: 10.1.3.0/24

Name: Private-1B
Availability Zone: us-east-1b
IPv4 CIDR Block: 10.1.4.0/24

# Create private route table

Name: Private-RT
VPC: MyVPC-PROD
Subnet associations: Private-1A, Private-1B

# Create Internet Gateway

Name: MyIGW-PROD
VPC: MyVPC-PROD
```

Restricted Mode ⊗ 0 ⚠ 0 Ln 1, Col 13 Spaces: 4 UTF-8 LF Markdown

VPC Endpoints

DigitalCloud TRAINING

VPC Interface Endpoints



VPC Gateway Endpoints

Route Table

Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	*vpce-ID*

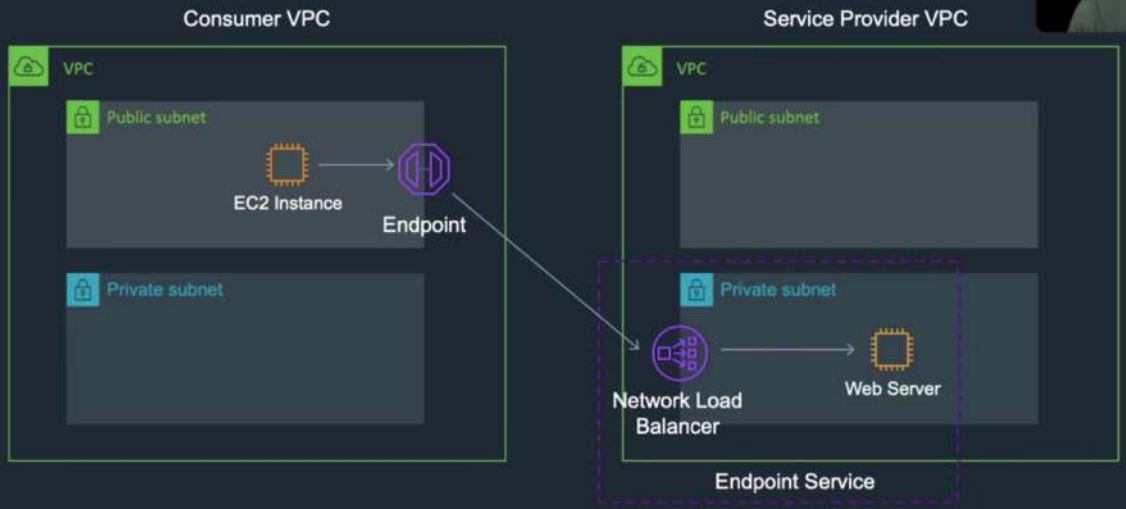
A route table entry is required with the prefix list for S3 and the gateway ID

VPC Endpoints

	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

DigitalCloud TRAINING

Service Provider Model



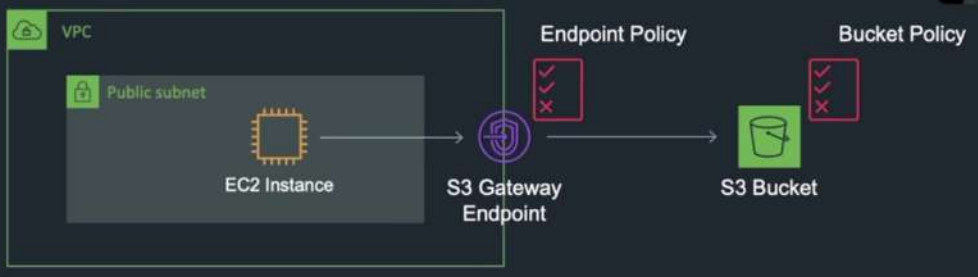
DigitalCloud TRAINING

Create VPC Endpoint

DigitalCloud TRAINING

SUBSCRIBE

VPC Gateway Endpoints

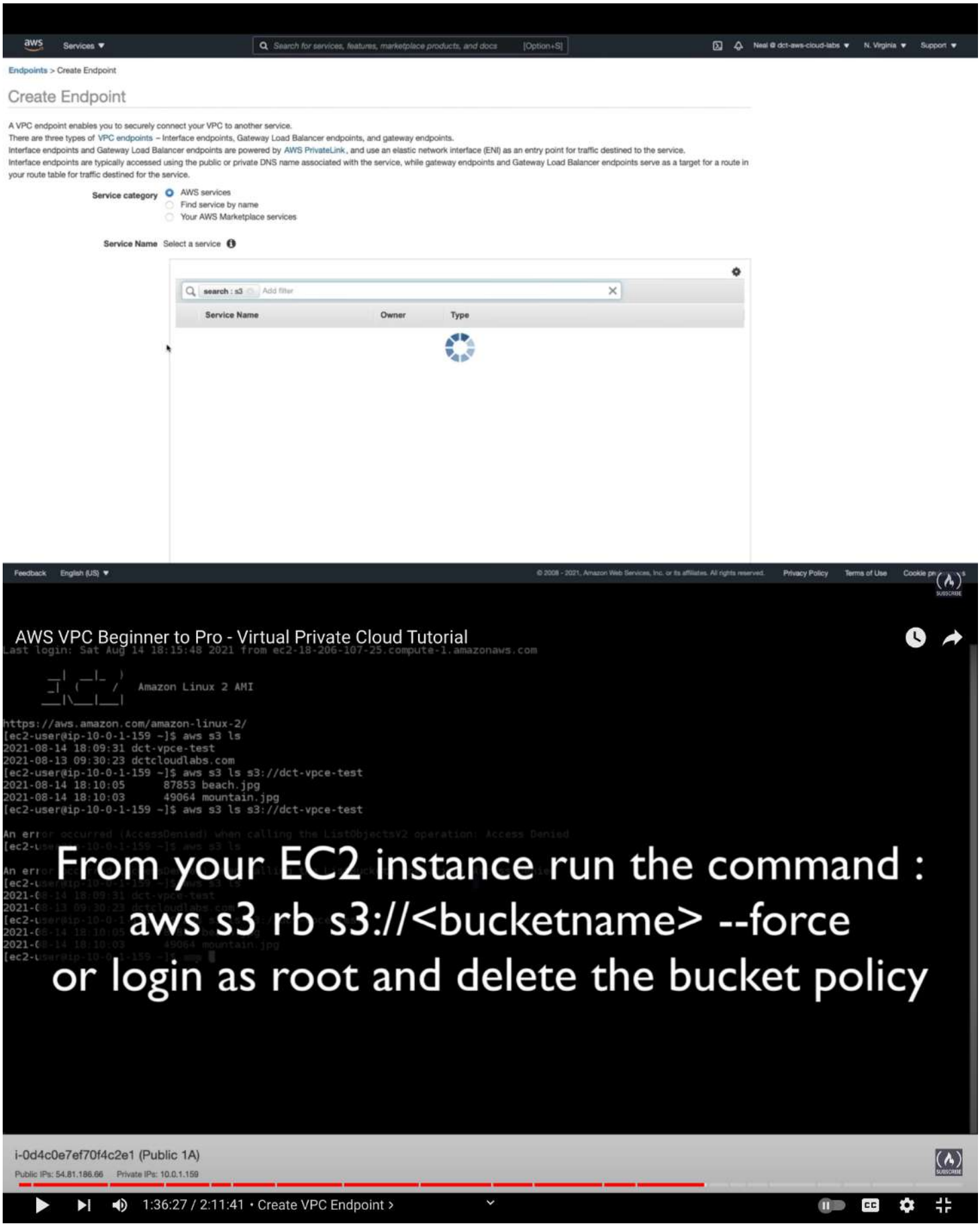


Route Table

Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	*vpce-ID*

DigitalCloud TRAINING

SUBSCRIBE


Endpoints > Create Endpoint
Create Endpoint
A VPC endpoint enables you to securely connect your VPC to another service.
There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints.
Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an elastic network interface (ENI) as an entry point for traffic destined to the service.
Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.
Service category
AWS services
Find service by name
Your AWS Marketplace services
Service Name
Select a service
search : s3
Add filter
Service Name
Owner
Type
AWS VPC Beginner to Pro - Virtual Private Cloud Tutorial
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls
2021-08-14 18:09:31 dct-vpce-test
2021-08-13 09:30:23 dctcloudlabs.com
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls s3://dct-vpce-test
2021-08-14 18:10:05 87853 beach.jpg
2021-08-14 18:10:03 49064 mountain.jpg
[ec2-user@ip-10-0-1-159 ~]$ aws s3 ls s3://dct-vpce-test
From your EC2 instance run the command :
aws s3 rb s3://<bucketname> --force
or login as root and delete the bucket policy
i-0d4c0e7ef70f4c2e1 (Public 1A)
Public IPs: 54.81.186.66 Private IPs: 10.0.1.159
1:36:27 / 2:11:41 • Create VPC Endpoint >