A CLOUD GURU

VPC Endpoints

Ryan Kroonenburg
AWS COMMUNITY HERO & ALEXA CHAMPION
FOUNDER OF A CLOUD GURU

A VPC Endpoint:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

There are two types of VPC endpoints:

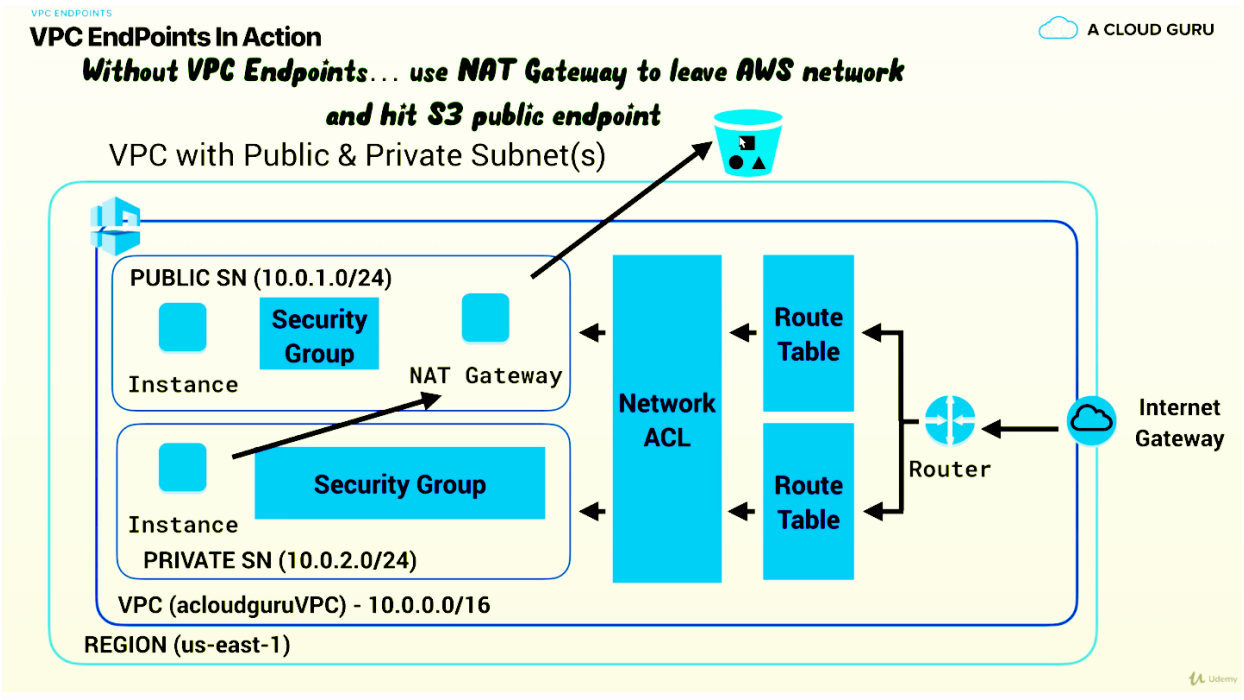
- Interface Endpoints
- Gateway Endpoints

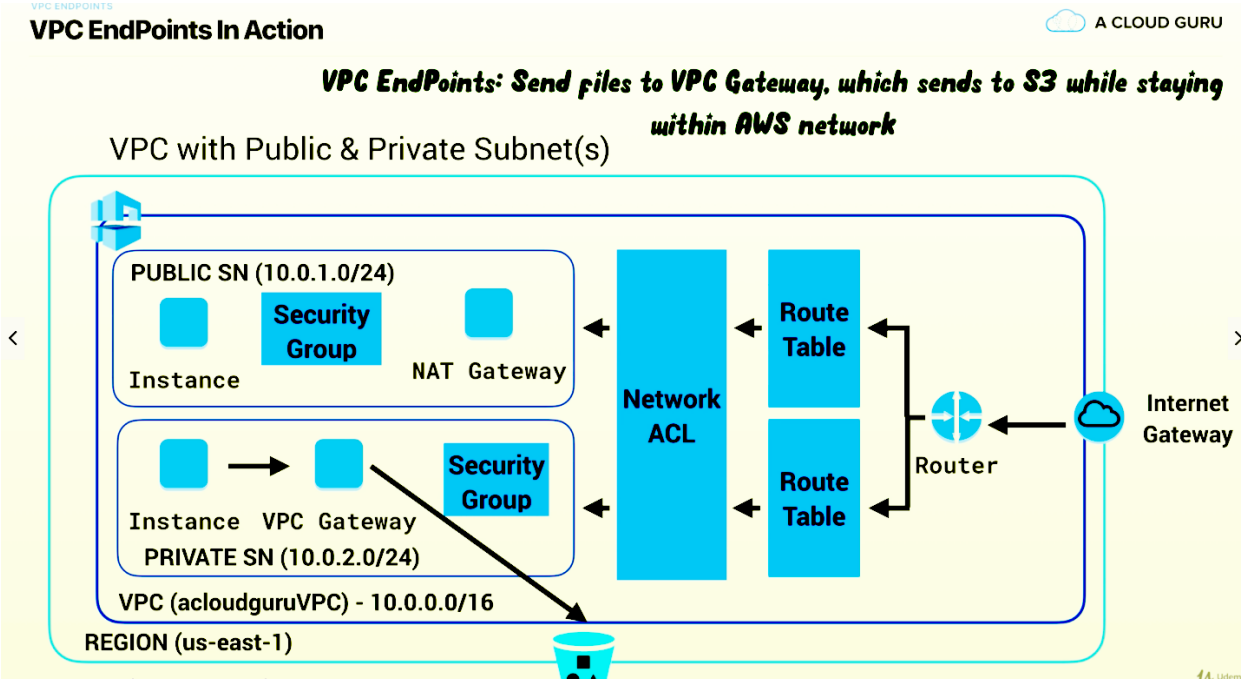
An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service. The following services are supported:

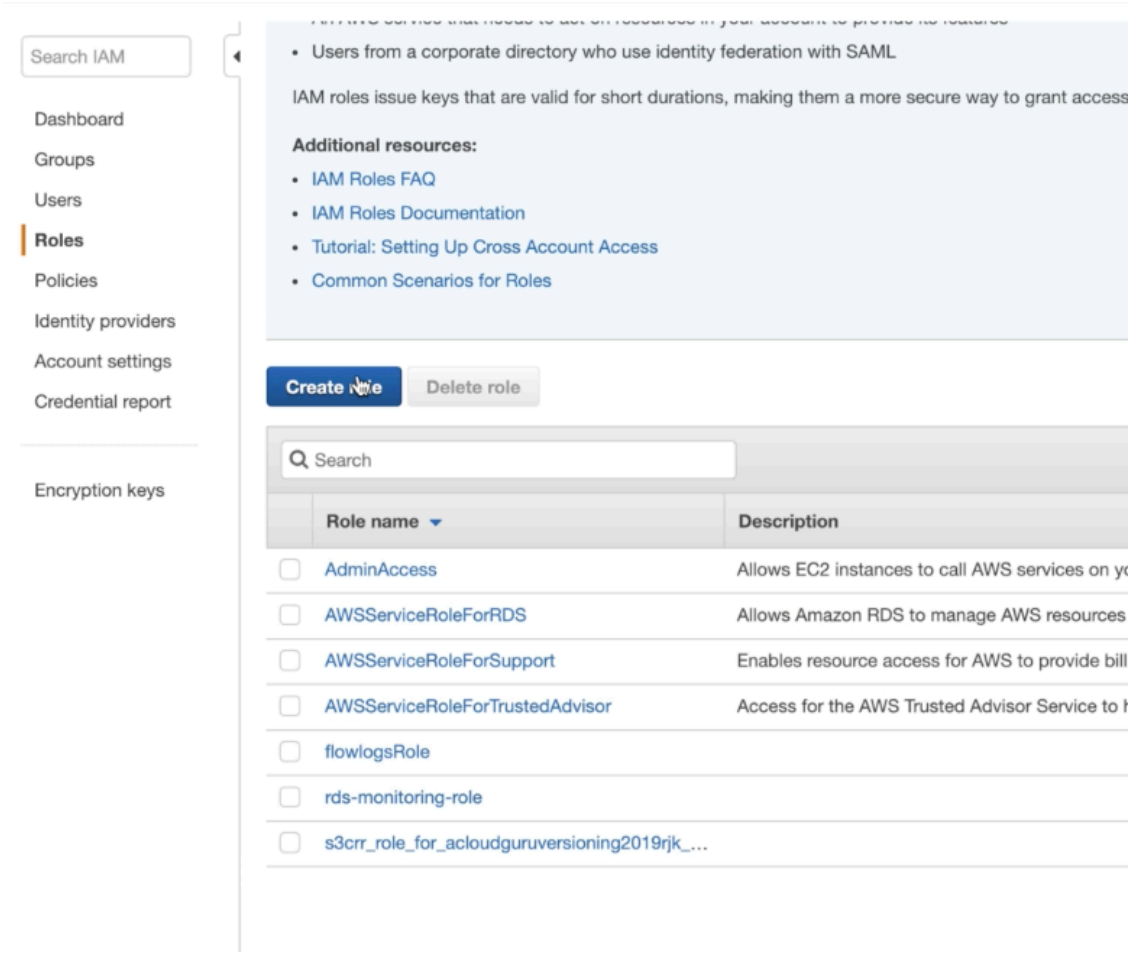
- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS CodeBuild
- AWS Config
- Amazon EC2 API
- Elastic Load Balancing API
- AWS Key Management Service
- Amazon Kinesis Data Streams
- Amazon SageMaker and Amazon SageMaker Runtime
- Amazon SageMaker Notebook Instance
- AWS Secrets Manager
- AWS Security Token Service
- AWS Service Catalog
- Amazon SNS
- Amazon SQS
- AWS Systems Manager
- Endpoint services hosted by other AWS accounts
- Supported AWS Marketplace partner services

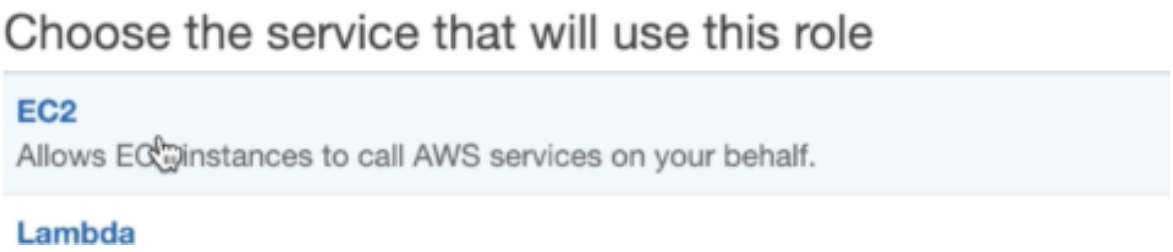
Currently Gateway Endpoints Support

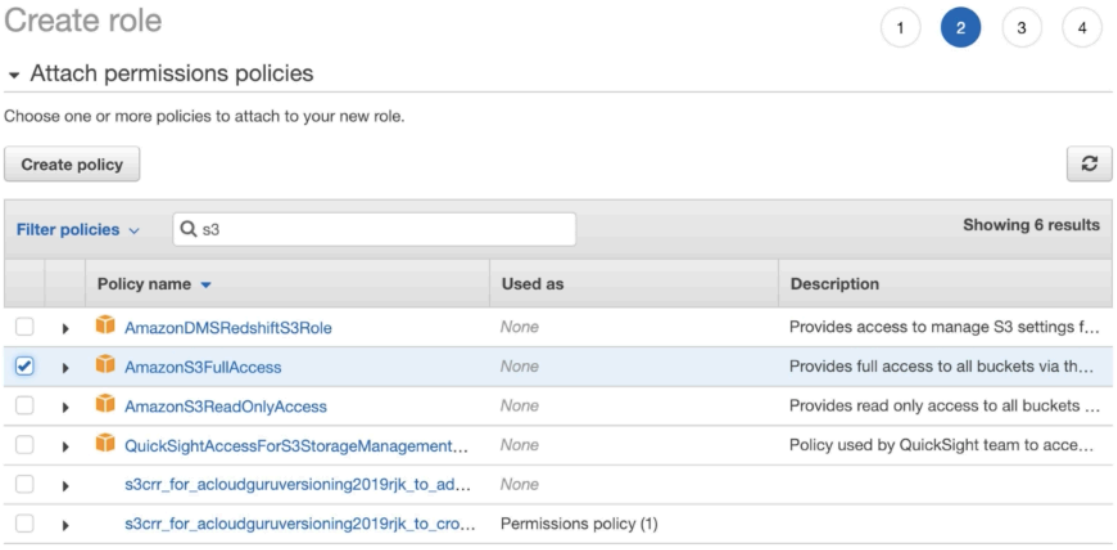
- Amazon S3
- DynamoDB




VPC ENDPOINTS
VPC EndPoints In Action
A CLOUD GURU
VPC EndPoints: Send files to VPC Gateway, which sends to S3 while staying within AWS network
VPC with Public & Private Subnet(s)
PUBLIC SN (10.0.1.0/24)
Security Group
Instance
NAT Gateway
Network ACL
Route Table
Route Table
Router
Internet Gateway
Security Group
Instance
VPC Gateway
PRIVATE SN (10.0.2.0/24)
VPC (acloudguruVPC) - 10.0.0.0/16
REGION (us-east-1)


Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Users from a corporate directory who use identity federation with SAML
IAM roles issue keys that are valid for short durations, making them a more secure way to grant access
Additional resources:
IAM Roles FAQ
IAM Roles Documentation
Tutorial: Setting Up Cross Account Access
Common Scenarios for Roles
Create role
Delete role
Search
Role name
Description
AdminAccess
AWSServiceRoleForRDS
Allows Amazon RDS to manage AWS resources
AWSServiceRoleForSupport
Enables resource access for AWS to provide bill
AWSServiceRoleForTrustedAdvisor
Access for the AWS Trusted Advisor Service to
flowlogsRole
rds-monitoring-role
s3crr_role_for_acloudguruversioning2019rjk_...


Choose the service that will use this role
EC2
Allows EC2 instances to call AWS services on your behalf.
Lambda


Create role
1
2
3
4
Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
Filter policies
s3
Showing 6 results
Policy name
Used as
Description
AmazonDMSRedshiftS3Role
None
Provides access to manage S3 settings f...
AmazonS3FullAccess
None
Provides full access to all buckets via th...
AmazonS3ReadOnlyAccess
None
Provides read only access to all buckets ...
QuickSightAccessForS3StorageManagement...
None
Policy used by QuickSight team to acce...
s3crr_for_acloudguruversioning2019rjk_to_ad...
None
s3crr_for_acloudguruversioning2019rjk_to_cro...
Permissions policy (1)

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* S3AdminAccess

Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.

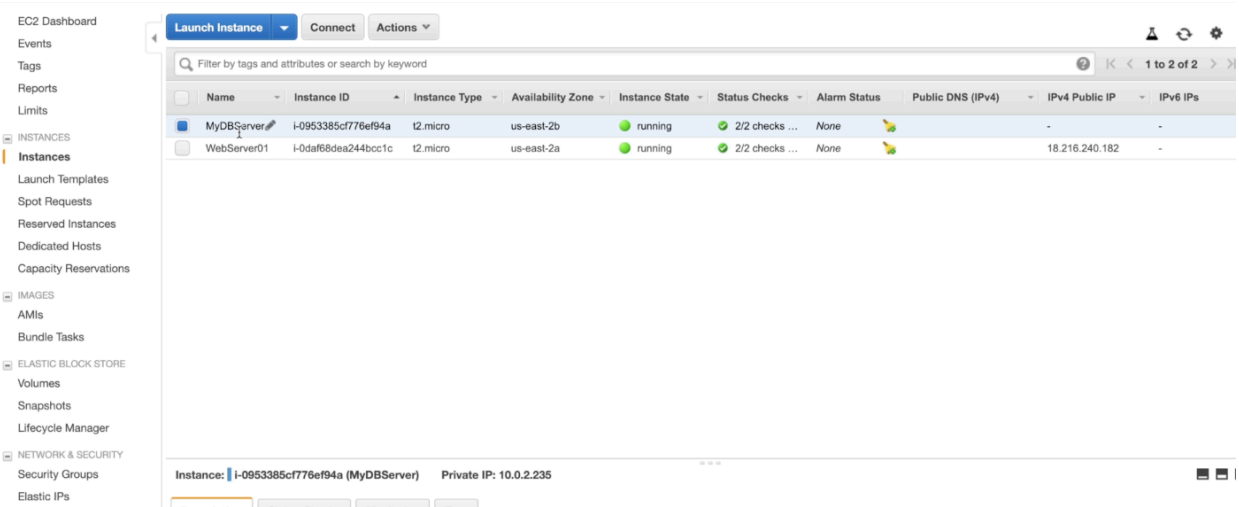
Role description Allows EC2 instances to call AWS services on your behalf.

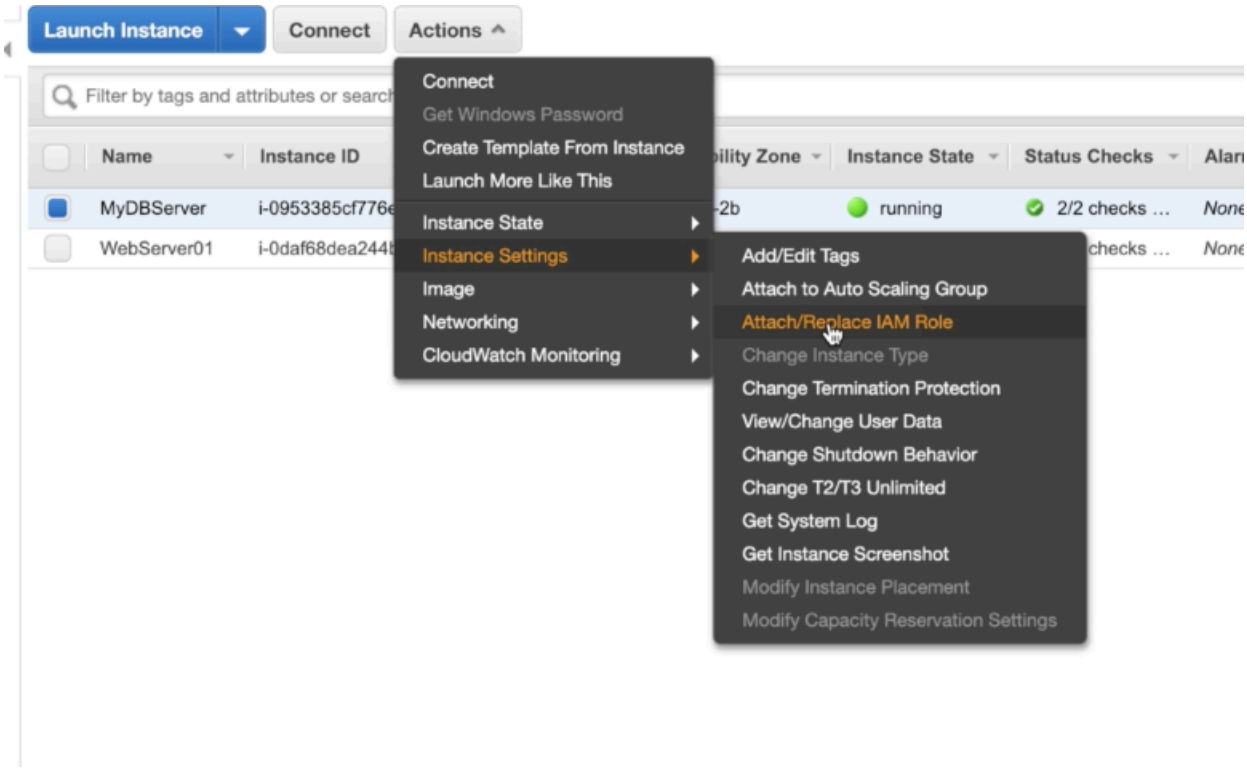
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonS3FullAccess

Permissions boundary Permissions boundary is not set





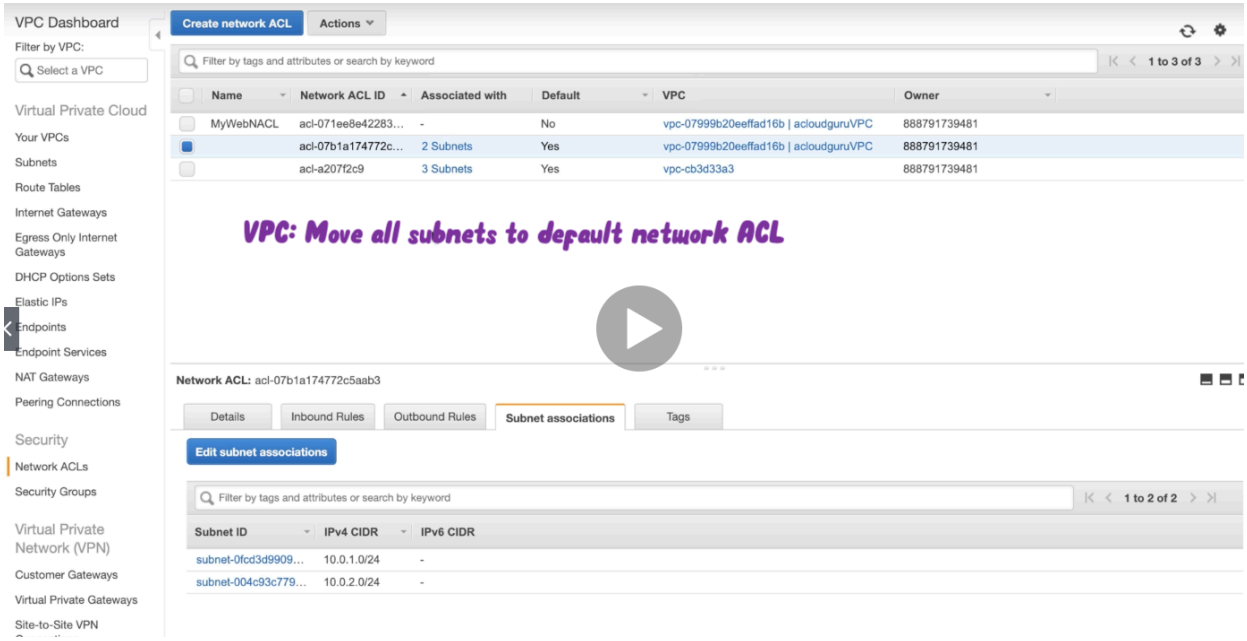
Attach/Replace IAM Role

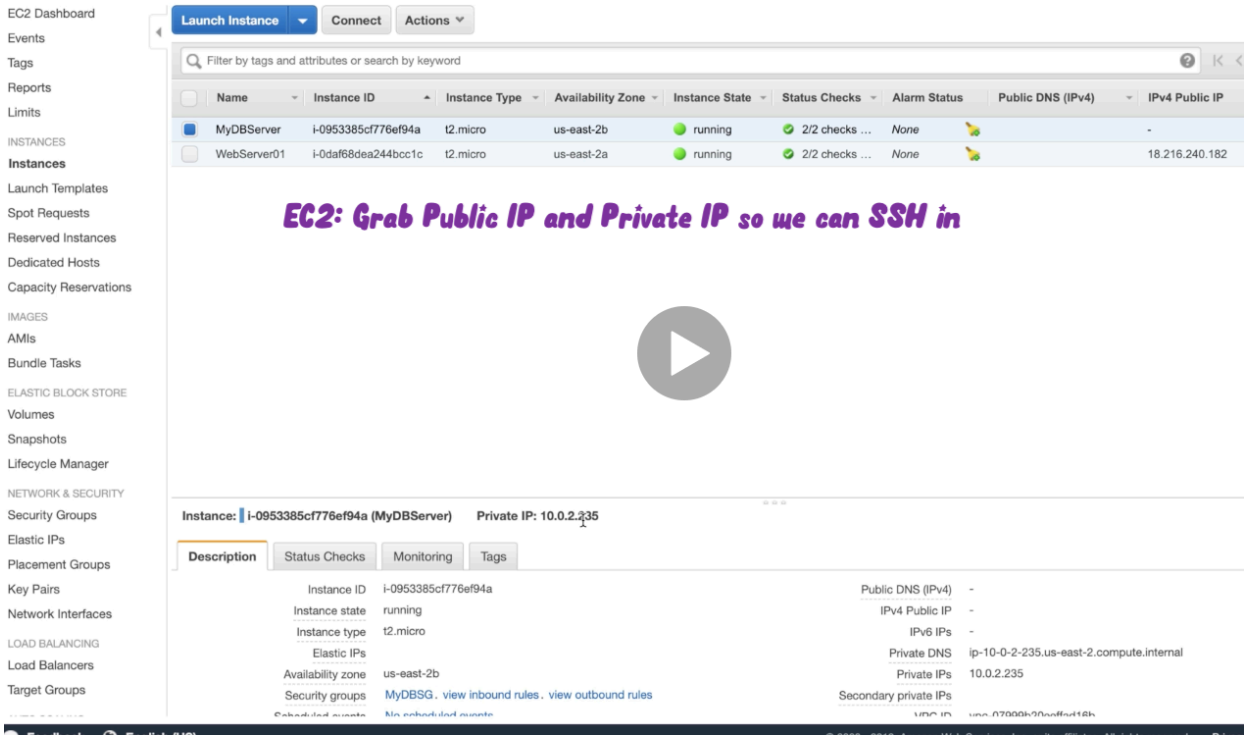
Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console.
If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-0953385cf776ef94a (MyDBServer)

IAM role* S3AdminAccess Create new IAM role

* Required


VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Virtual Private Network (VPN)
Customer Gateways
Virtual Private Gateways
Site-to-Site VPN
Create network ACL
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Network ACL ID
Associated with
Default
VPC
Owner
MyWebNACL
acl-071ee8e42283...
-
No
vpc-07999b20eeffad16b | acloudguruVPC
888791739481
acl-07b1a174772c...
2 Subnets
Yes
vpc-07999b20eeffad16b | acloudguruVPC
888791739481
acl-a207f2c9
3 Subnets
Yes
vpc-cb3d33a3
888791739481
VPC: Move all subnets to default network ACL
Network ACL: acl-07b1a174772c5aab3
Details
Inbound Rules
Outbound Rules
Subnet associations
Tags
Edit subnet associations
Filter by tags and attributes or search by keyword
1 to 2 of 2
Subnet ID
IPv4 CIDR
IPv6 CIDR
subnet-0fcd3d9909...
10.0.1.0/24
-
subnet-004c93c779...
10.0.2.0/24
-


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
MyDBServer
i-0953385cf776ef94a
t2.micro
us-east-2b
running
2/2 checks ...
None
-
WebServer01
i-0daf68dea244bcc1c
t2.micro
us-east-2a
running
2/2 checks ...
None
18.216.240.182
EC2: Grab Public IP and Private IP so we can SSH in
Instance: i-0953385cf776ef94a (MyDBServer)
Private IP: 10.0.2.235
Description
Status Checks
Monitoring
Tags
Instance ID
i-0953385cf776ef94a
Instance state
running
Instance type
t2.micro
Elastic IPs
Availability zone
us-east-2b
Security groups
MyDBSG. view inbound rules. view outbound rules
Public DNS (IPv4)
-
IPv4 Public IP
-
IPv6 IPs
-
Private DNS
ip-10-0-2-235.us-east-2.compute.internal
Private IPs
10.0.2.235
Secondary private IPs

```
Ryans-iMac:Downloads ryankroonenburg$ ssh ec2-user@18.216.240.182 -i MyN
ewKP.pem
Last login: Tue Jan 29 23:32:36 2019 from 107.16.110.187

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

https://aws.amazon.com/amazon-linux-2/
3 package(s) needed for security, out of 3 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-89 ~]$ sudo su
```

ssh into Public IP

upgrade privileges to root

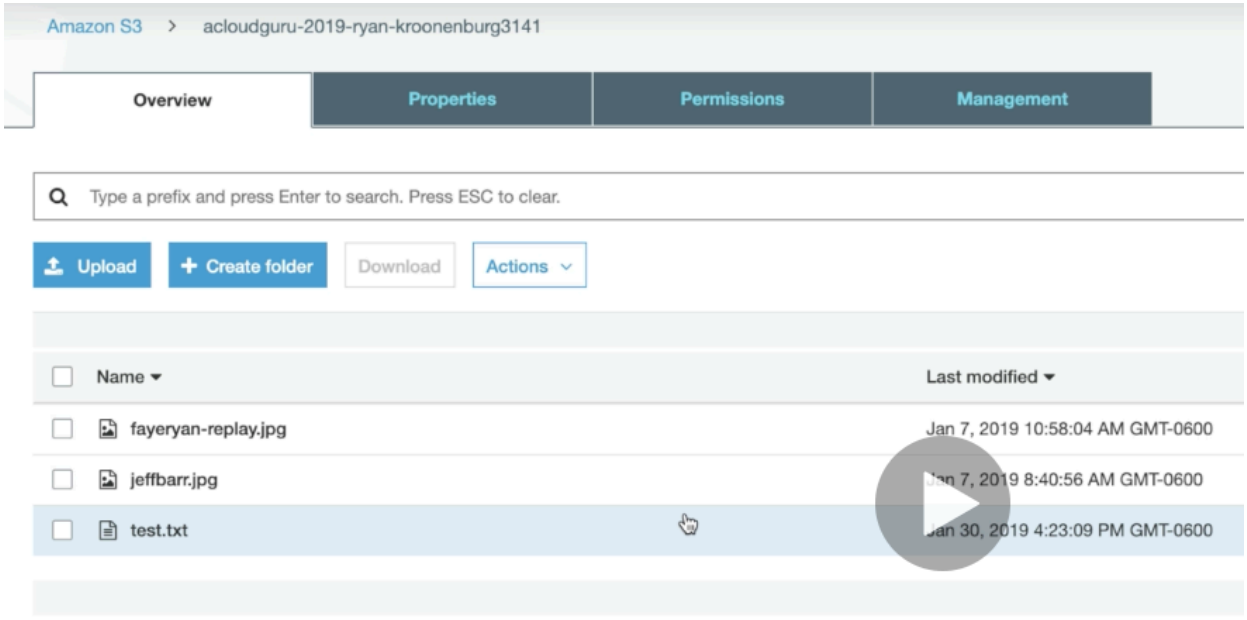
```
[root@ip-10-0-1-89 ec2-user]# ls
MyPvKey.pem
[root@ip-10-0-1-89 ec2-user]# ssh ec2-user@10.0.2.235 -i MyPvKey.pem
Last login: Tue Jan 29 23:33:07 2019 from 10.0.1.89

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-2-235 ~]$ sud
```

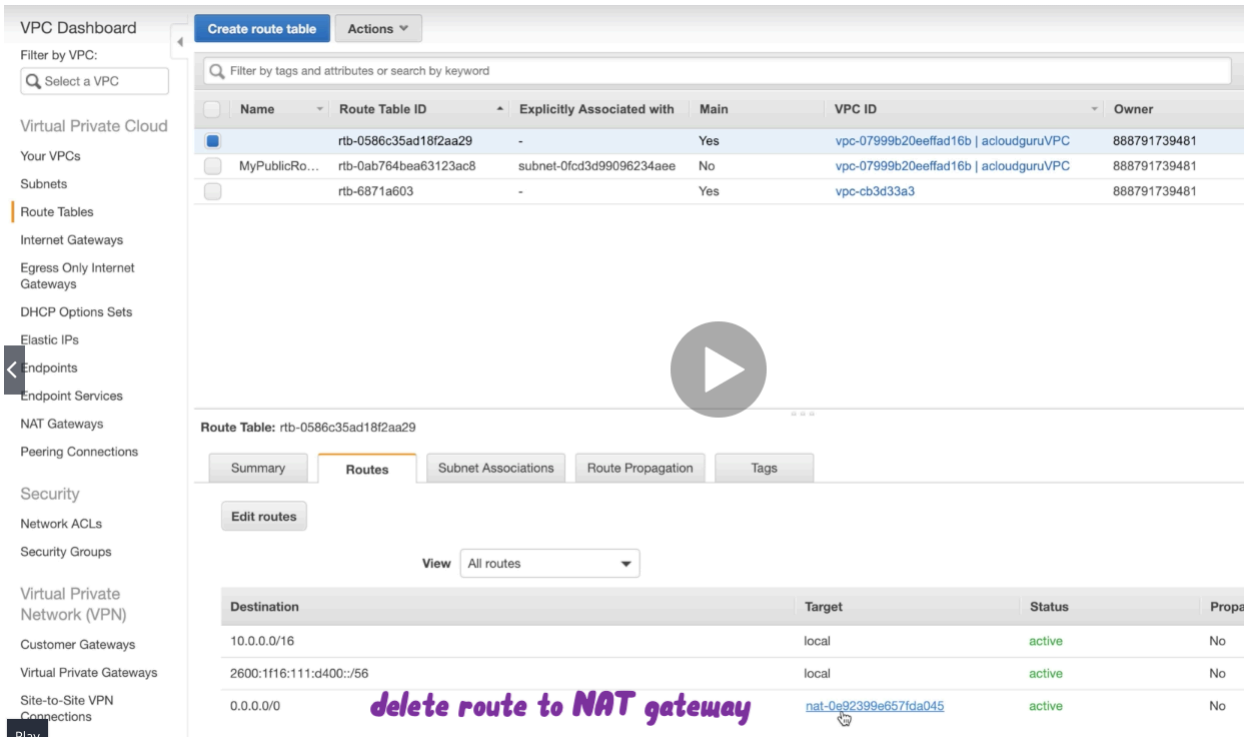
still have private key saved

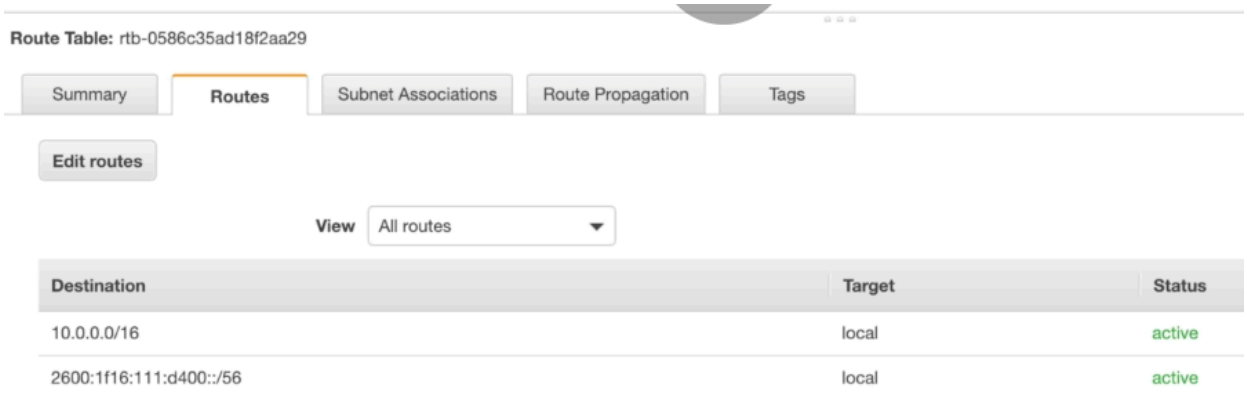
ssh into Private IP (from Public)

```
[root@ip-10-0-2-235 ec2-user]# aws s3 ls
2019-01-07 14:40:13 acloudguru-2019-ryan-kroonenburg3141
2019-01-08 10:11:21 acloudguruversioning2019rjk
2019-01-08 12:05:29 crossregionreplication542322423
2019-01-15 11:11:20 skaldjflkadsj382748237
[root@ip-10-0-2-235 ec2-user]# echo "test" > test.txt
[root@ip-10-0-2-235 ec2-user]# ls
test.txt
[root@ip-10-0-2-235 ec2-user]# aws s3 cp test.txt s3://acloudguru-2019-r
yan-kroonenburg3141
upload: ./test.txt to s3://acloudguru-2019-ryan-kroonenburg3141/test.txt
[root@ip-10-0-2-235 ec2-user]#
```

create test file and upload to s3 bucket

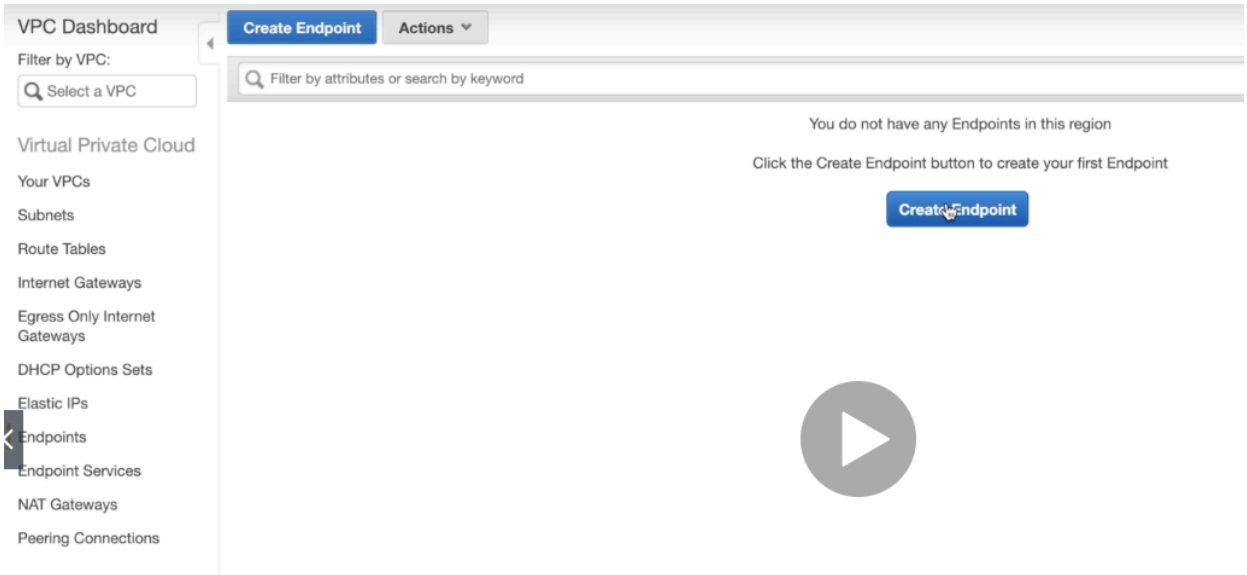



VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Virtual Private Network (VPN)
Customer Gateways
Virtual Private Gateways
Site-to-Site VPN Connections
Create route table
Actions
Filter by tags and attributes or search by keyword
Name
Route Table ID
Explicitly Associated with
Main
VPC ID
Owner
rtb-0586c35ad18f2aa29 - Yes vpc-07999b20eeffad16b | acloudguruVPC 888791739481
MyPublicRo... rtb-0ab764bea63123ac8 subnet-0fcd3d99096234aee No vpc-07999b20eeffad16b | acloudguruVPC 888791739481
rtb-6871a603 - Yes vpc-cb3d33a3 888791739481
Route Table: rtb-0586c35ad18f2aa29
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit routes
View All routes
Destination
Target
Status
Propa
10.0.0.0/16 local active No
2600:1f16:111:d400::/56 local active No
0.0.0.0/0 nat-0e92399e657fda045 active No
delete route to NAT gateway


Route Table: rtb-0586c35ad18f2aa29
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit routes
View All routes
Destination
Target
Status
10.0.0.0/16 local active
2600:1f16:111:d400::/56 local active

```
[root@ip-10-0-2-235 ec2-user]# aws s3 ls
```

will not work because no route to internet... let's add a VPC endpoint



Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.
An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
A gateway endpoint serves 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

Filter by attributes

	Service Name	Owner	Type
( )	com.amazonaws.us-east-2.execute-api	amazon	Interface
( )	com.amazonaws.us-east-2.kinesis-streams	amazon	Interface
( )	com.amazonaws.us-east-2.kms	amazon	Interface
( )	com.amazonaws.us-east-2.logs	amazon	Interface
( )	com.amazonaws.us-east-2.monitoring	amazon	Interface
( )	com.amazonaws.us-east-2.s3	amazon	Gateway
( )	com.amazonaws.us-east-2.sagemaker.api	amazon	Interface

VPC* vpc-07999b20eeffad16b

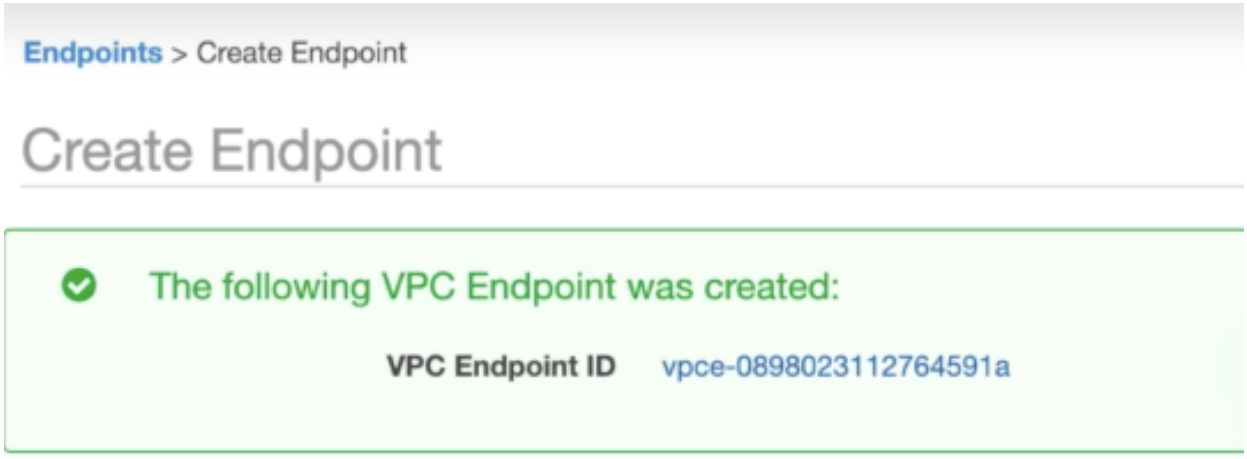
Configure route tables A rule with destination **pl-7ba54012 (com.amazonaws.us-east-2.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will
tables you select below.

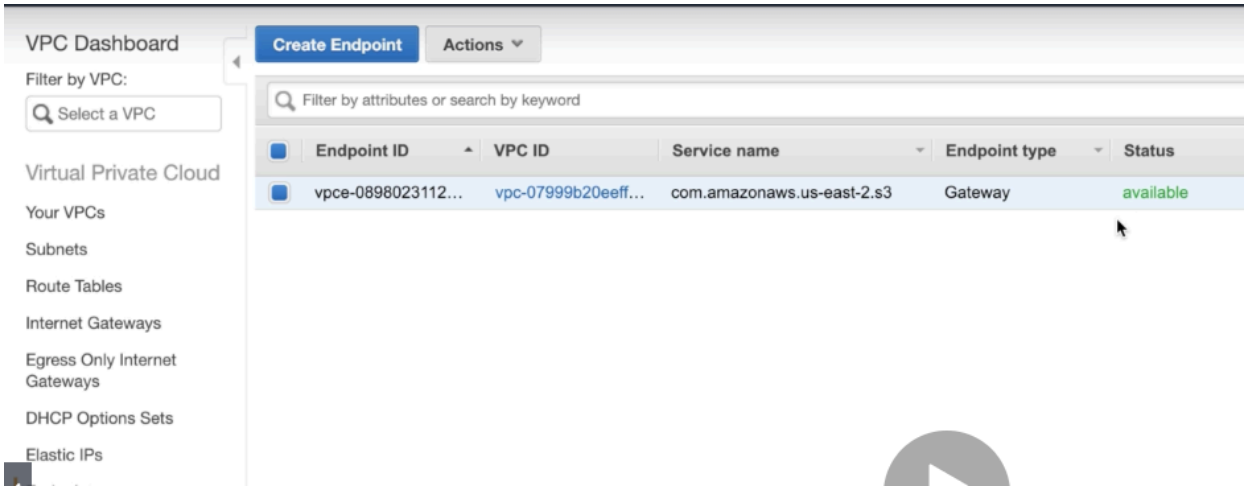
Subnets associated with selected route tables will be able to access this endpoint.

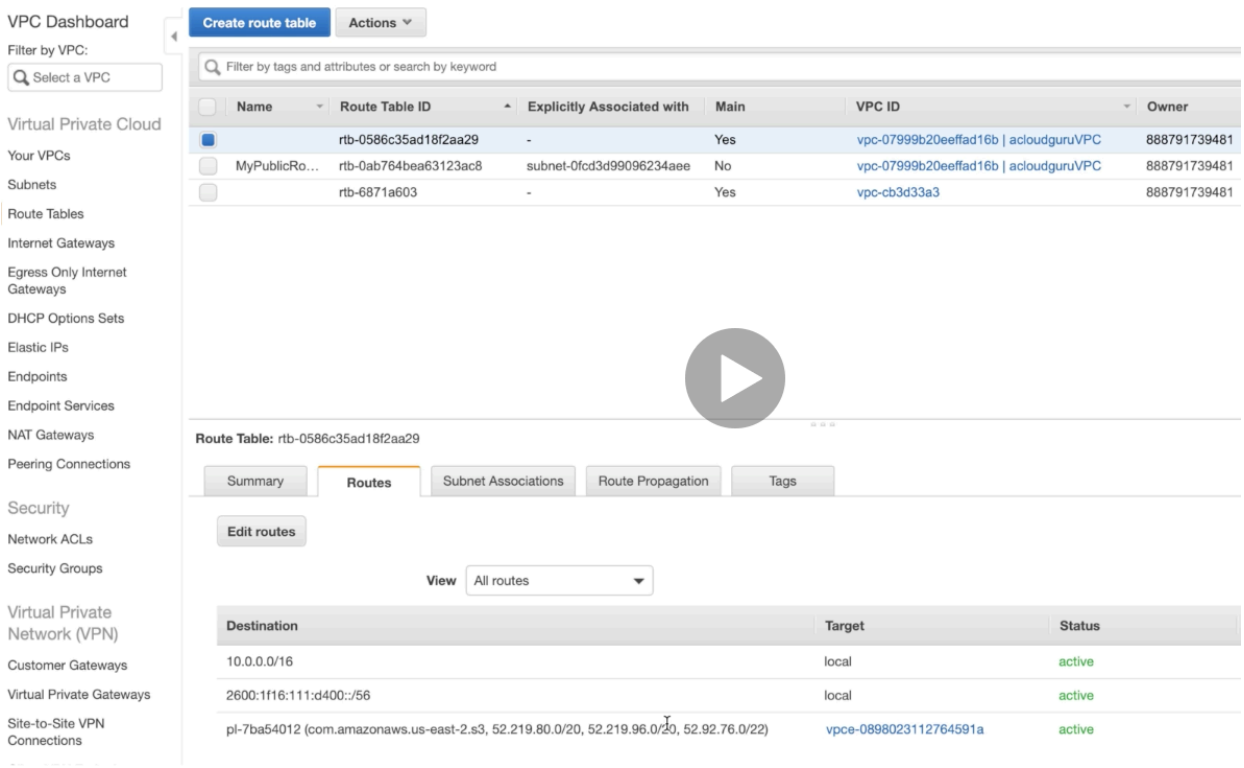
rtb-0586c35ad18f2aa29

	Route Table ID	Main	Associated With
[ ]	rtb-0ab764bea63123ac8	No	subnet-0fcd3d99096234aee | 10.0.1.0 - us-east-2a
[x]	rtb-0586c35ad18f2aa29	Yes	subnet-094c93c7790c162a4 | 10.0.2.0 - us-east-2b

Warning
When you use an endpoint, the source IP addresses from your instances in your affected subnets for accessing the AWS
region will be private IP addresses, not public IP addresses. Existing connections from your affected subnets to the AWS
public IP addresses may be dropped. Ensure that you don't have critical tasks running when you create or modify an enc


Endpoints > Create Endpoint
Create Endpoint
The following VPC Endpoint was created:
VPC Endpoint ID
vpce-0898023112764591a


VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Create Endpoint
Actions
Filter by attributes or search by keyword
Endpoint ID
VPC ID
Service name
Endpoint type
Status
vpce-0898023112...
vpc-07999b20eeff...
com.amazonaws.us-east-2.s3
Gateway
available




```
[root@ip-10-0-2-235 ec2-user]# aws s3 ls
^C
[root@ip-10-0-2-235 ec2-user]# aws s3 ls --region us-east-2
2019-01-07 14:43:28 acloudguru-2019-ryan-kroonenburg3141
2019-01-08 12:05:31 acloudguruversioning2019rjk
2019-01-08 12:05:30 crossregionreplication542322423
2019-01-15 11:11:20 skaldjflkadsj382748237
```

pass in region to get it to work

A VPC Endpoint:

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

There are two types of VPC endpoints:

- Interface Endpoints
- Gateway Endpoints

Currently Gateway Endpoints Support:

- Amazon S3
- DynamoDB