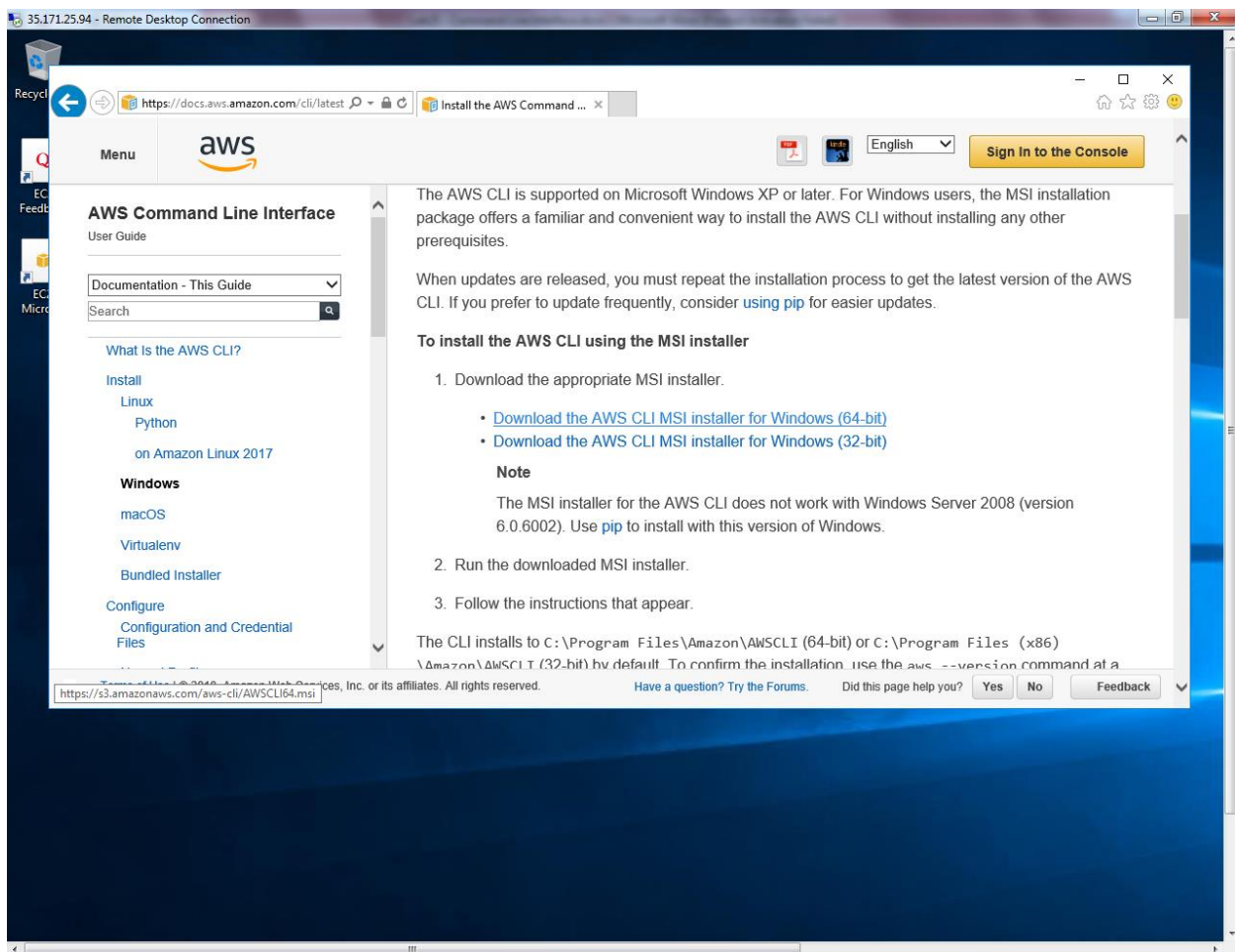


## Lab 26

### Configuring Endpoint and access the s3 bucket

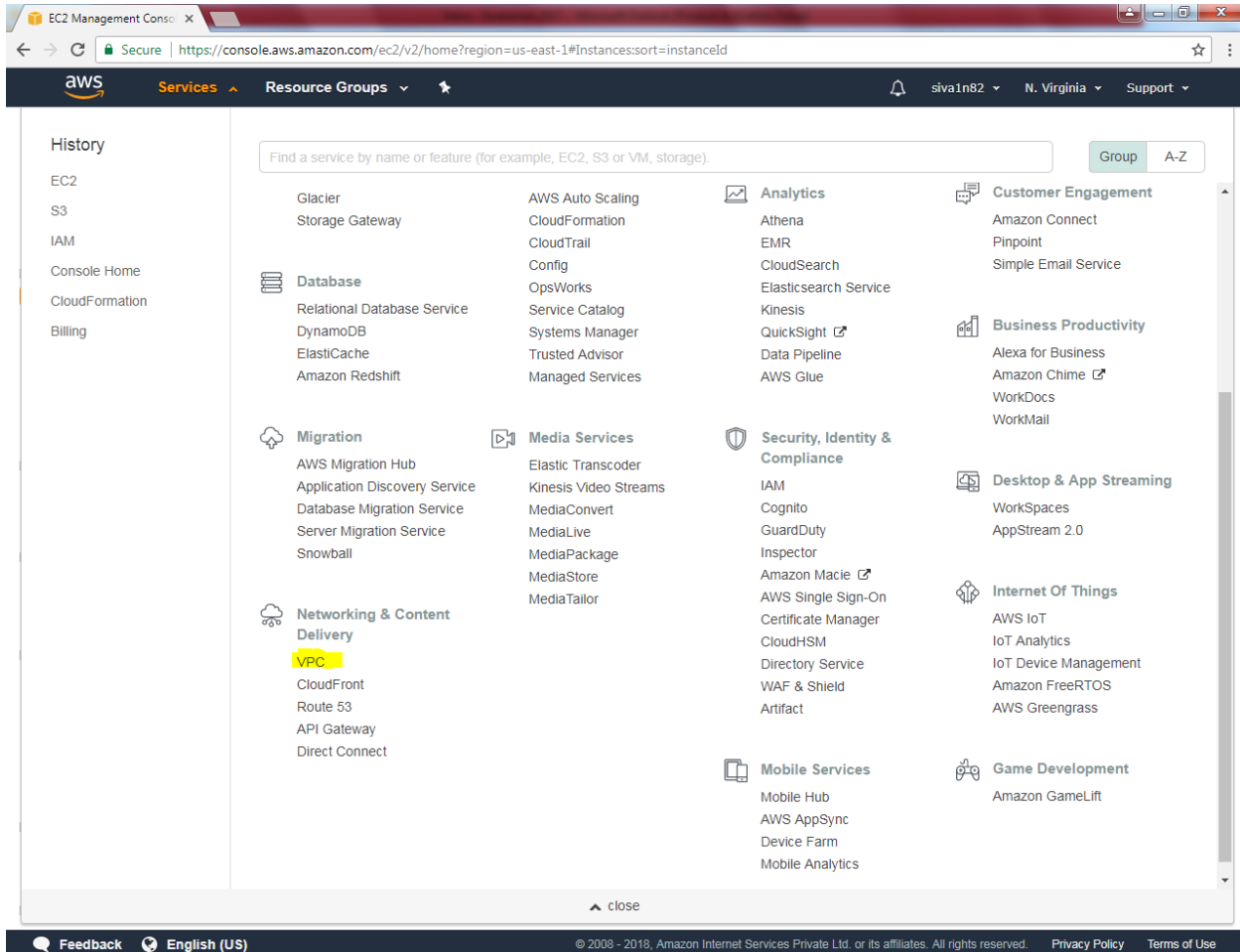
**Scenario: We have required to access s3 service without internet access from private subnet.**

Create one windows instance with Public subnet. We need to install command line interface tool in that instance.



Download the package in public instance.

Go to services and click “VPC”.



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a 'Services' dropdown menu, and a 'Resource Groups' dropdown. The main content area displays a grid of service categories and individual services. The 'Networking & Content Delivery' category is expanded, and the 'VPC' service is highlighted in yellow. Other visible categories include Database, Migration, Media Services, Analytics, Security, Identity & Compliance, Mobile Services, Customer Engagement, Business Productivity, Desktop & App Streaming, Internet Of Things, and Game Development. The left sidebar shows a 'History' list with items like EC2, S3, IAM, Console Home, CloudFormation, and Billing. The bottom of the console features a footer with 'Feedback', 'English (US)', and copyright information.

History

- EC2
- S3
- IAM
- Console Home
- CloudFormation
- Billing

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Group A-Z

**Database**

- Relational Database Service
- DynamoDB
- ElastiCache
- Amazon Redshift

**Migration**

- AWS Migration Hub
- Application Discovery Service
- Database Migration Service
- Server Migration Service
- Snowball

**Networking & Content Delivery**

- VPC**
- CloudFront
- Route 53
- API Gateway
- Direct Connect

**Media Services**

- Elastic Transcoder
- Kinesis Video Streams
- MediaConvert
- MediaLive
- MediaPackage
- MediaStore
- MediaTailor

**Analytics**

- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- QuickSight
- Data Pipeline
- AWS Glue

**Security, Identity & Compliance**

- IAM
- Cognito
- GuardDuty
- Inspector
- Amazon Macie
- AWS Single Sign-On
- Certificate Manager
- CloudHSM
- Directory Service
- WAF & Shield
- Artifact

**Mobile Services**

- Mobile Hub
- AWS AppSync
- Device Farm
- Mobile Analytics

**Customer Engagement**

- Amazon Connect
- Pinpoint
- Simple Email Service

**Business Productivity**

- Alexa for Business
- Amazon Chime
- WorkDocs
- WorkMail

**Desktop & App Streaming**

- WorkSpaces
- AppStream 2.0

**Internet Of Things**

- AWS IoT
- IoT Analytics
- IoT Device Management
- Amazon FreeRTOS
- AWS Greengrass

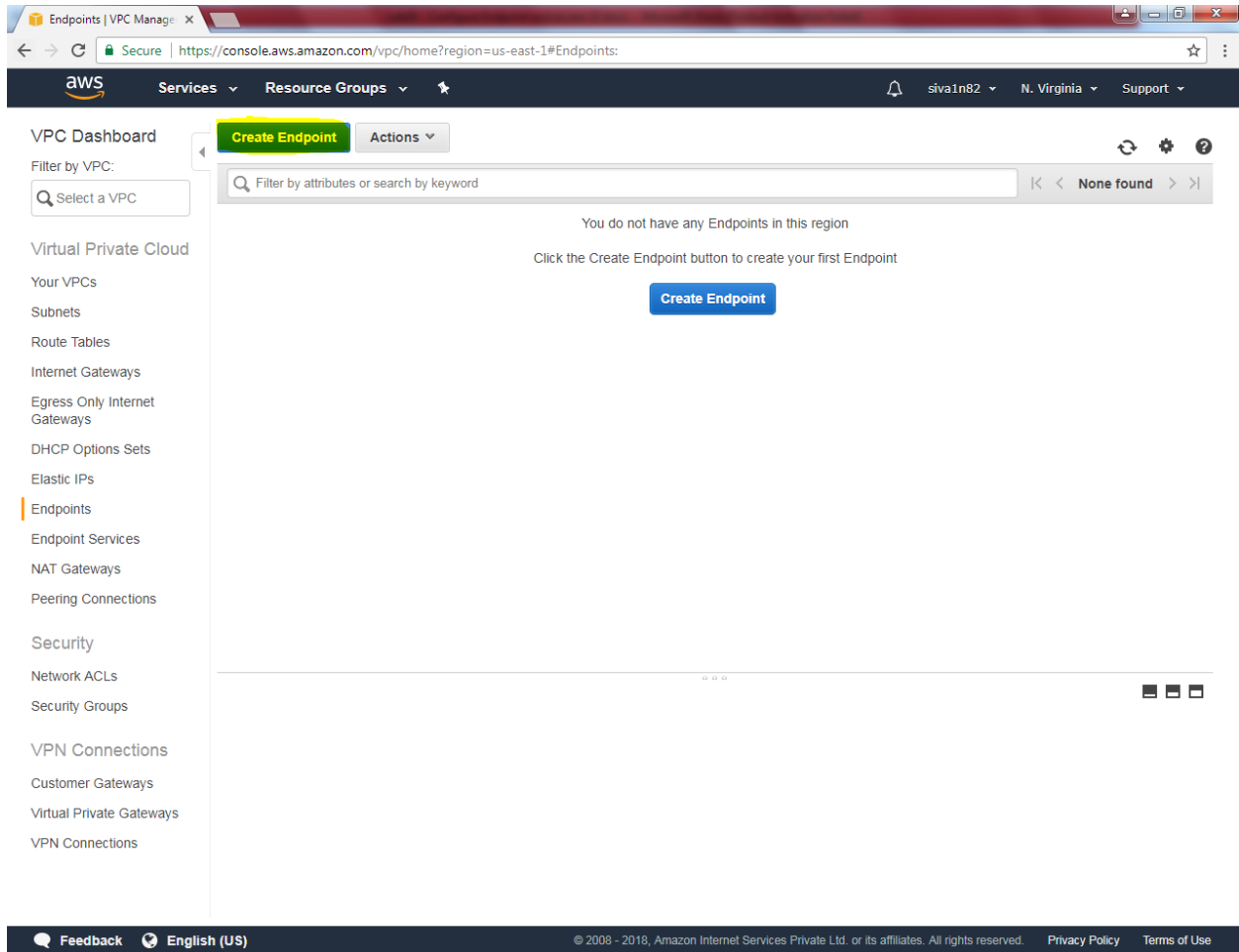
**Game Development**

- Amazon GameLift

close

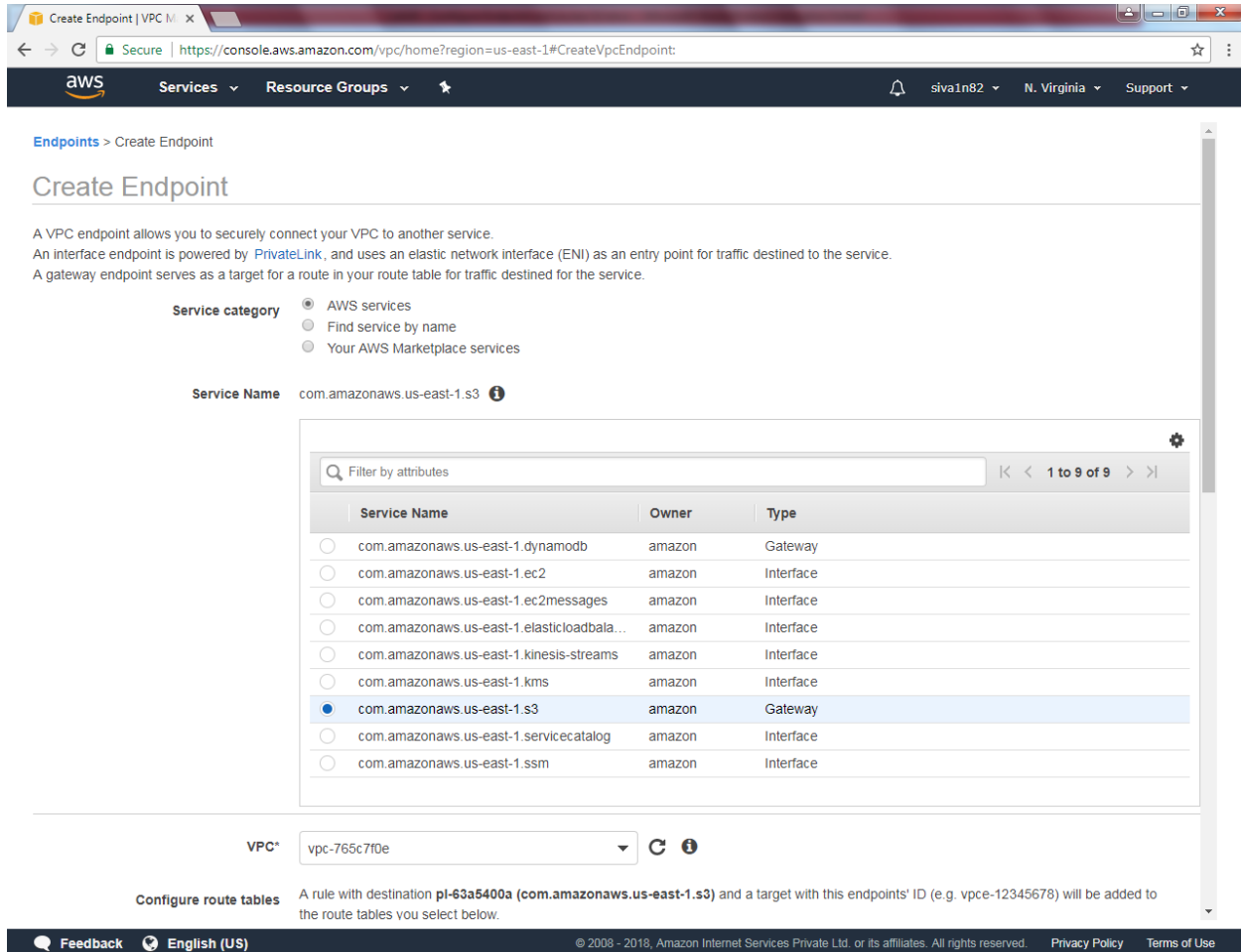
Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click Endpoints and click “Create Endpoint”.



The screenshot shows the AWS Management Console for VPC Endpoints. The left-hand navigation pane is expanded to show the 'Endpoints' section under 'Virtual Private Cloud'. The main content area displays a message: 'You do not have any Endpoints in this region. Click the Create Endpoint button to create your first Endpoint.' A prominent blue 'Create Endpoint' button is centered on the screen. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The bottom footer contains 'Feedback', 'English (US)', and copyright information.

Select S3.



**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

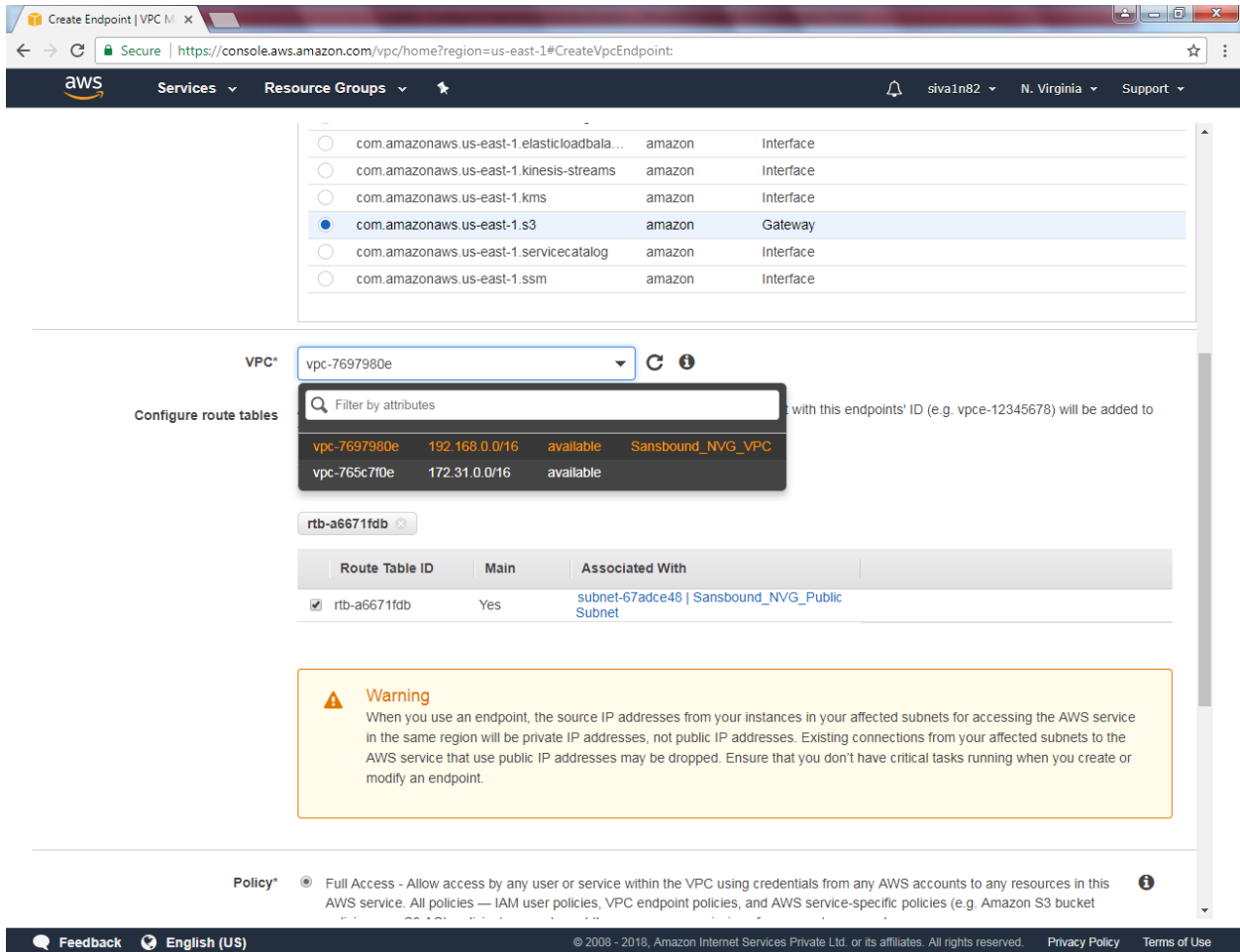
**Service Name** com.amazonaws.us-east-1.s3 ⓘ

Service Name	Owner	Type
<input type="radio"/> com.amazonaws.us-east-1.dynamodb	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-1.ec2	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.ec2messages	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.elasticloadbala...	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.kinesis-streams	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.kms	amazon	Interface
<input checked="" type="radio"/> com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.us-east-1.servicecatalog	amazon	Interface
<input type="radio"/> com.amazonaws.us-east-1.ssm	amazon	Interface

**VPC\*** vpc-765c7f0e ⓘ

**Configure route tables** A rule with destination **pl-63a5400a (com.amazonaws.us-east-1.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

Select VPC and select sanbound VPC's subnet.



Create Endpoint | VPC M x

Secure | https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint:

aws Services Resource Groups siva1n82 N. Virginia Support

<input type="radio"/>	com.amazonaws.us-east-1.elasticloadbala...	amazon	Interface
<input type="radio"/>	com.amazonaws.us-east-1.kinesis-streams	amazon	Interface
<input type="radio"/>	com.amazonaws.us-east-1.kms	amazon	Interface
<input checked="" type="radio"/>	com.amazonaws.us-east-1.s3	amazon	Gateway
<input type="radio"/>	com.amazonaws.us-east-1.servicecatalog	amazon	Interface
<input type="radio"/>	com.amazonaws.us-east-1.ssm	amazon	Interface

VPC\* vpc-7697980e

Configure route tables

Filter by attributes

vpc-7697980e	192.168.0.0/16	available	Sansbound_NVG_VPC
vpc-765c7f0e	172.31.0.0/16	available	

rtb-a6671fdb

Route Table ID	Main	Associated With
<input checked="" type="checkbox"/> rtb-a6671fdb	Yes	subnet-67adce48   Sansbound_NVG_Public Subnet

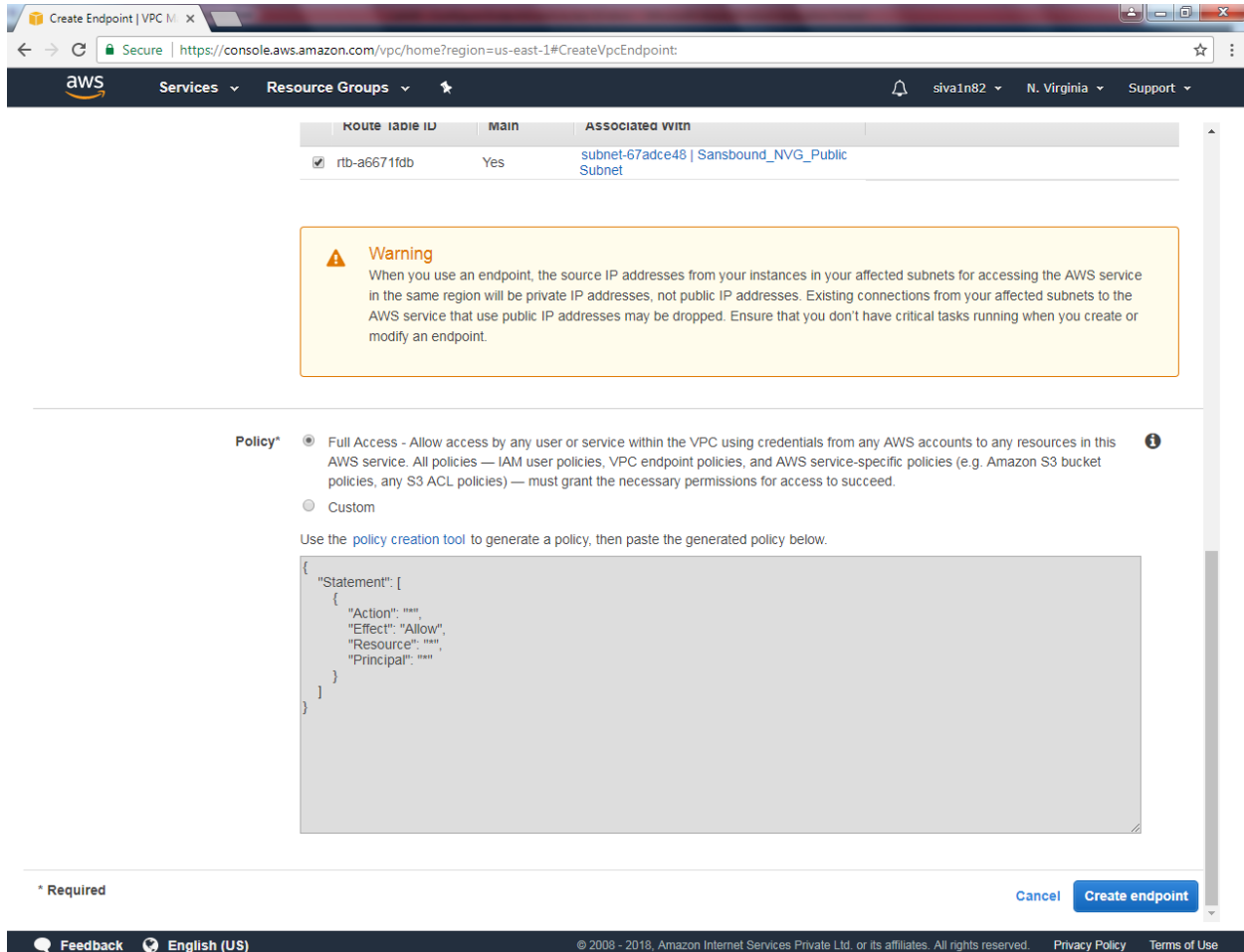
**Warning**

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

Policy\* Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

## Create “Create Endpoint”



Create Endpoint | VPC M x

Secure | <https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint>

aws Services Resource Groups siva1n82 N. Virginia Support

Route table ID	Main	Associated with
<input checked="" type="checkbox"/> rtb-a6671fdb	Yes	subnet-67adce48   Sansbound_NVG_Public Subnet

**Warning**

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

**Policy\***

☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
 ☐ Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

```

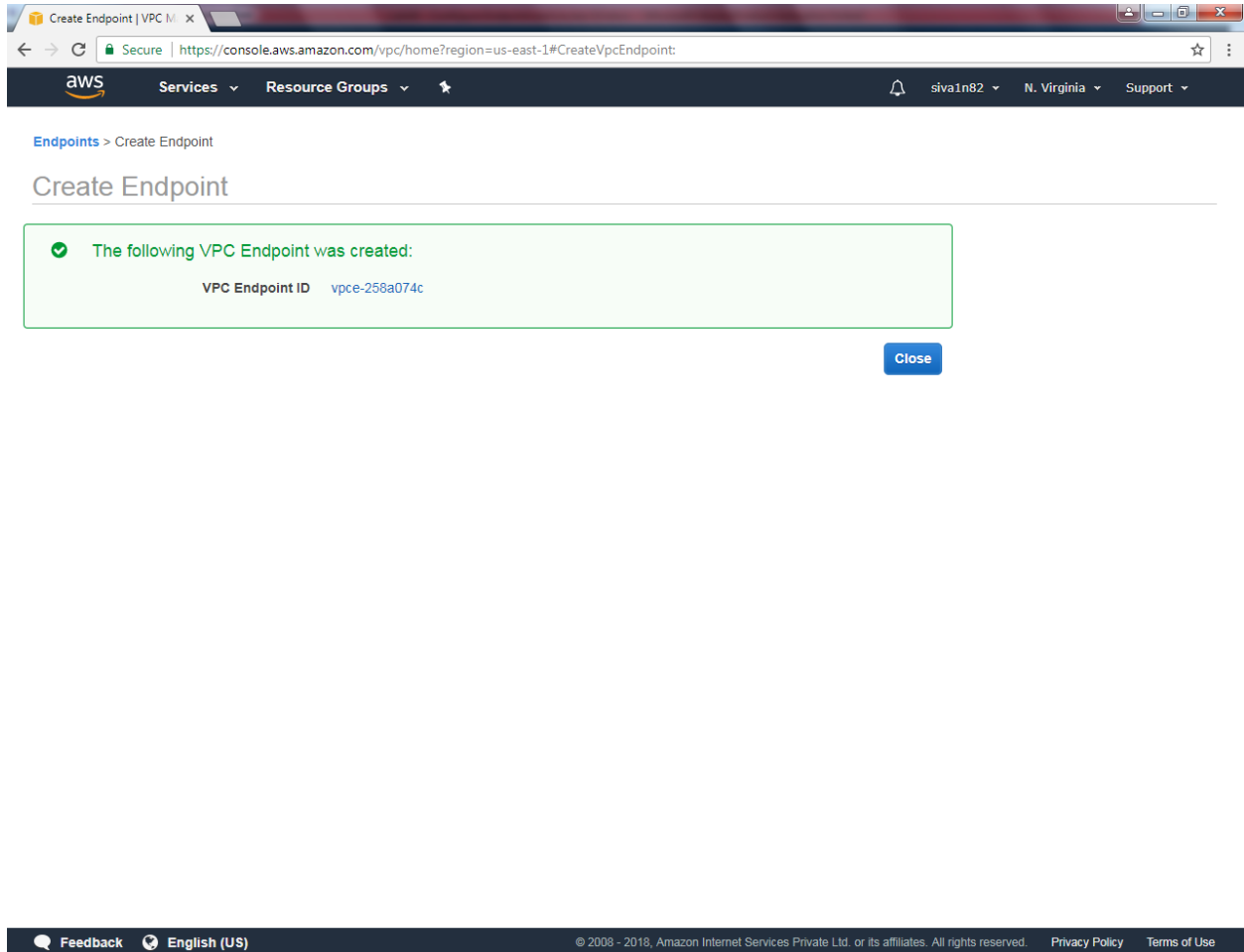
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
  
```

\* Required

Cancel **Create endpoint**

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Endpoint has been successfully created.



The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82' in 'N. Virginia'. Below this, the breadcrumb 'Endpoints > Create Endpoint' is visible. The main heading is 'Create Endpoint'. A green notification box with a checkmark icon states: 'The following VPC Endpoint was created:'. Below this, it lists 'VPC Endpoint ID' as 'vpce-258a074c'. A 'Close' button is located at the bottom right of the notification. The footer contains a 'Feedback' link, 'English (US)' language selector, and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' along with 'Privacy Policy' and 'Terms of Use' links.

Create Endpoint | VPC M x

Secure | <https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint>

aws Services Resource Groups siva1n82 N. Virginia Support

Endpoints > Create Endpoint

## Create Endpoint

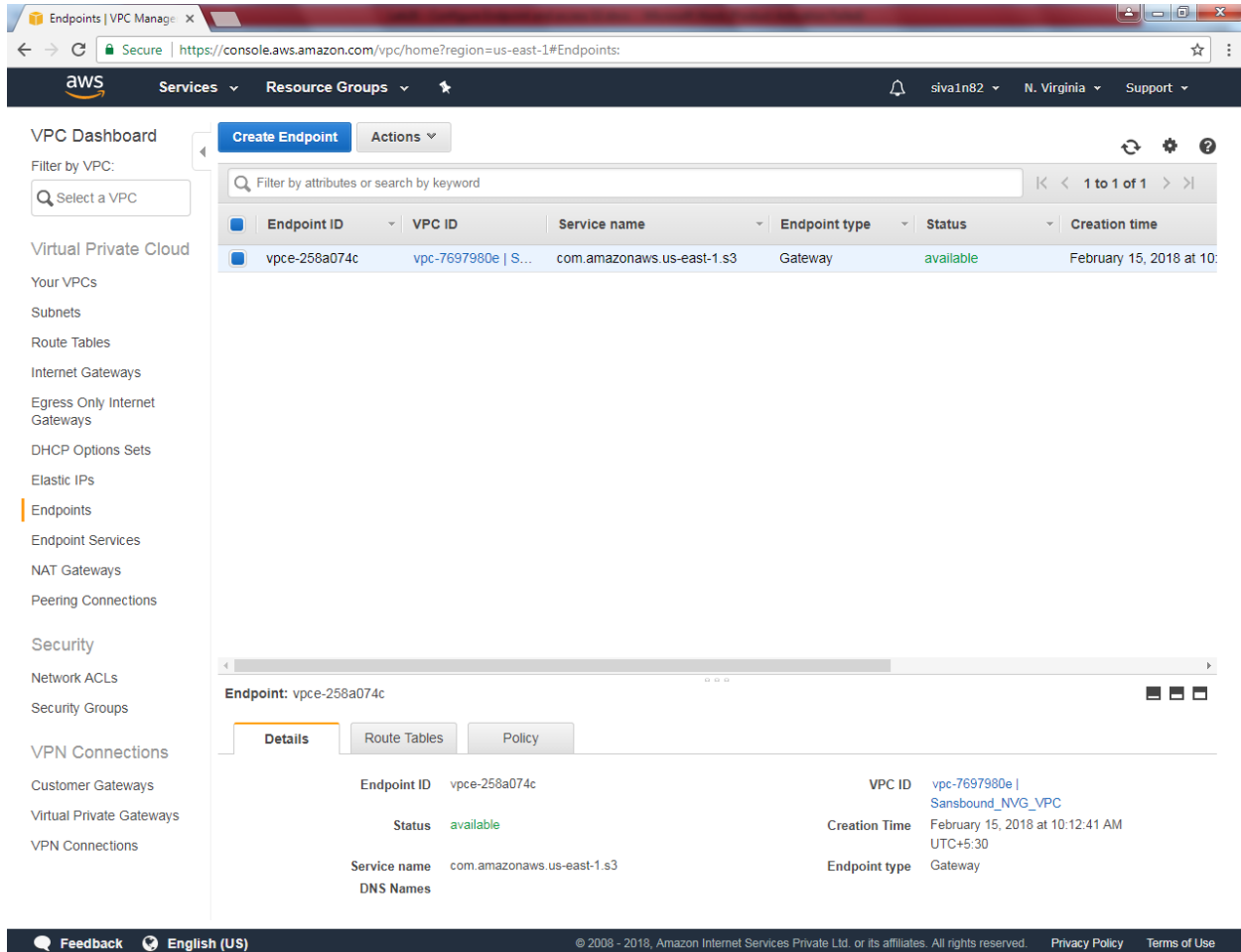
✓ The following VPC Endpoint was created:

VPC Endpoint ID `vpce-258a074c`

Close

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Endpoint is now available.



The screenshot shows the AWS VPC Dashboard in a web browser. The left sidebar contains navigation links for VPC resources. The main content area displays a table of endpoints. Below the table, the details for the selected endpoint 'vpce-258a074c' are shown, including its VPC ID, status, service name, creation time, and endpoint type.

**VPC Dashboard**

Filter by 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

VPN Connections

- Customer Gateways
- Virtual Private Gateways
- VPN Connections

**Create Endpoint** **Actions**

Filter by attributes or search by keyword

Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
vpce-258a074c	vpc-7697980e   S...	com.amazonaws.us-east-1.s3	Gateway	available	February 15, 2018 at 10:

**Endpoint: vpce-258a074c**

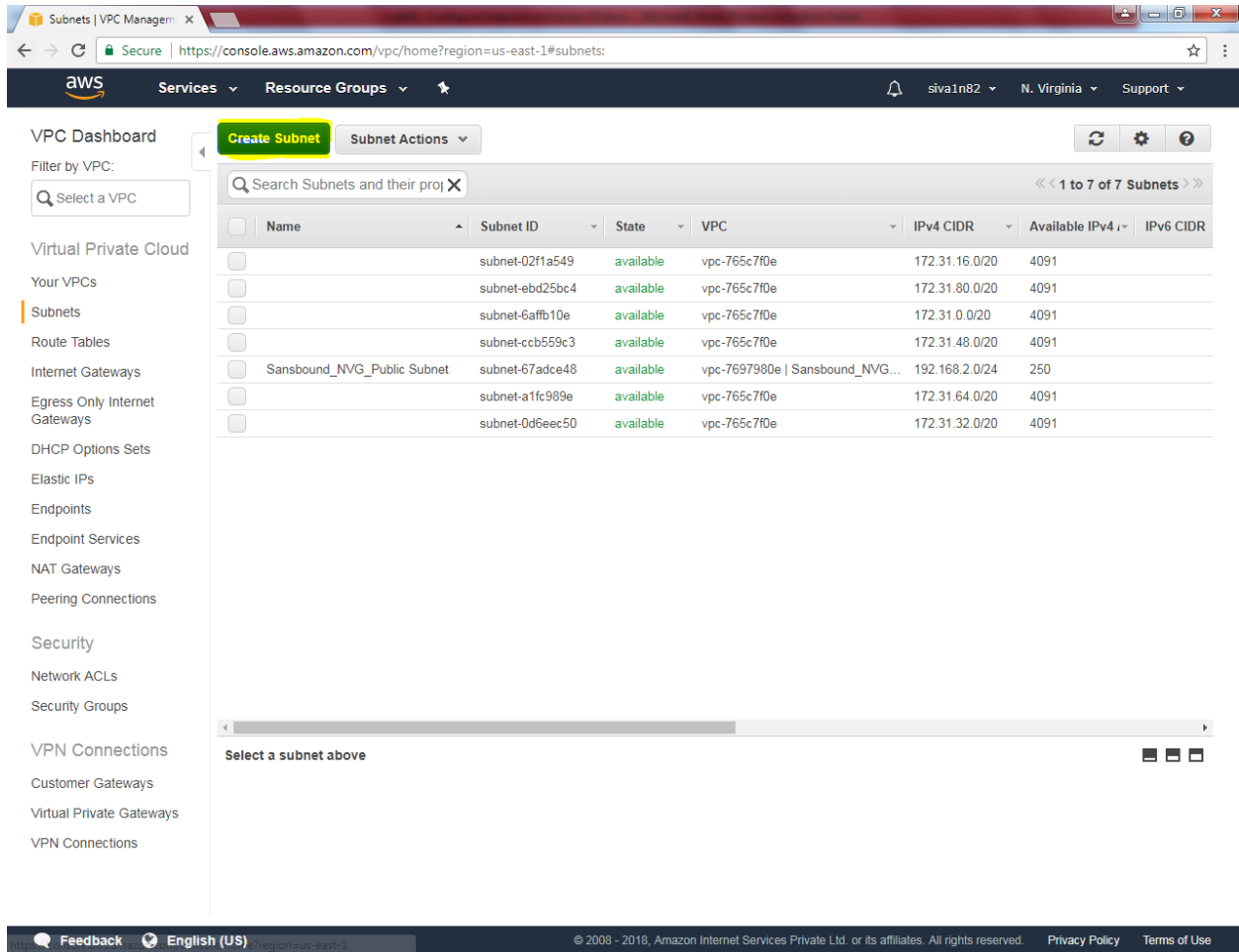
**Details** **Route Tables** **Policy**

Endpoint ID	vpce-258a074c	VPC ID	vpc-7697980e   Sansbound_NVG_VPC
Status	available	Creation Time	February 15, 2018 at 10:12:41 AM UTC+5:30
Service name	com.amazonaws.us-east-1.s3	Endpoint type	Gateway
DNS Names			

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use



Create a new subnet in North Virginia.



The screenshot shows the AWS Management Console interface for the 'Subnets' page in the 'N. Virginia' region. The 'Create Subnet' button is highlighted in green. The table below lists the existing subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
	subnet-02f1a549	available	vpc-765c7f0e	172.31.16.0/20	4091	
	subnet-ebd25bc4	available	vpc-765c7f0e	172.31.80.0/20	4091	
	subnet-6affb10e	available	vpc-765c7f0e	172.31.0.0/20	4091	
	subnet-ccb559c3	available	vpc-765c7f0e	172.31.48.0/20	4091	
Sansbound_NVG_Public Subnet	subnet-67adce48	available	vpc-7697980e   Sansbound_NVG...	192.168.2.0/24	250	
	subnet-a1fc989e	available	vpc-765c7f0e	172.31.64.0/20	4091	
	subnet-0d6eec50	available	vpc-765c7f0e	172.31.32.0/20	4091	

While creating subnet,

Name tag as “Sansbound\_Private\_Subnet\_NVG”

VPC as “Sansbound\_NVG\_VPC”.

IPv4 CIDR Block: 192.168.1.0/24

**Create Subnet** ✕

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

**Name tag**  i

**VPC**  i

**VPC CIDRs**

CIDR	Status	Status Reason
192.168.0.0/16	associated	

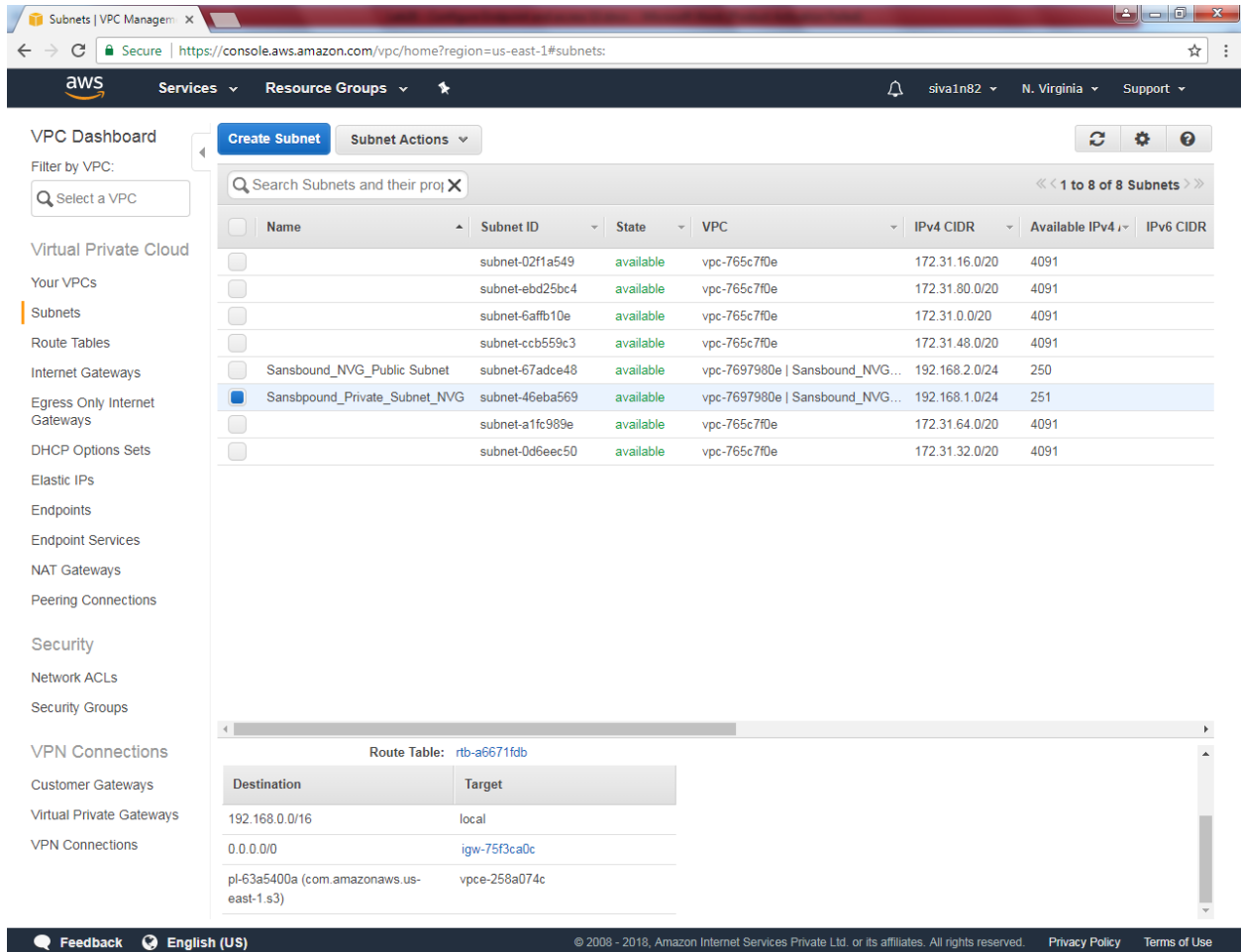
**Availability Zone**  i

**IPv4 CIDR block**  i

Cancel Yes, Create

Click “Yes create”.

We can able to see s3 routing information in private routing table.



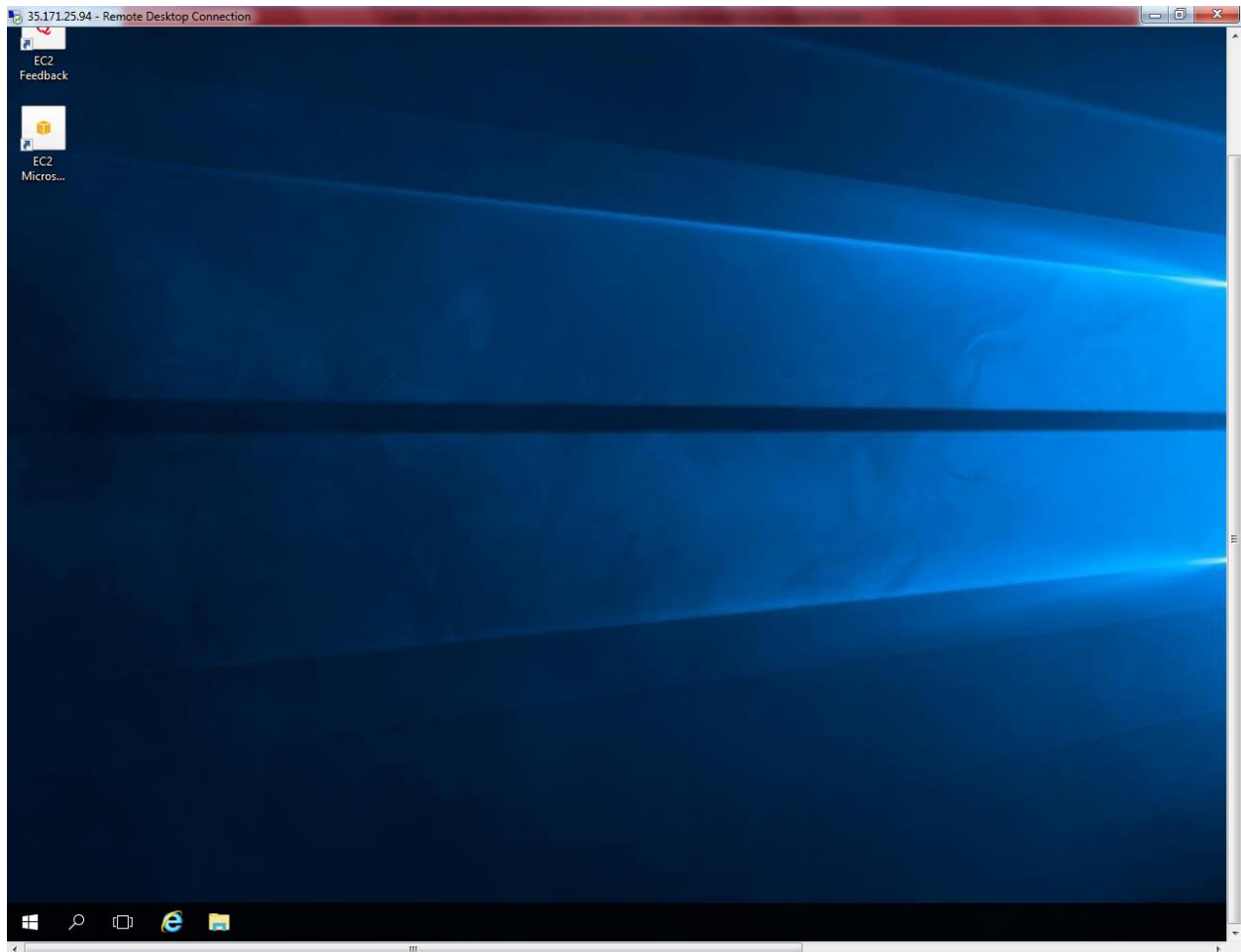
The screenshot displays the AWS Management Console interface for the 'Subnets' page. The left-hand navigation pane shows various VPC-related services, with 'Subnets' currently selected. The main content area shows a list of subnets. The subnet 'Sansbound\_Private\_Subnet\_NVG' (ID: subnet-46eba569) is highlighted. Below the subnet list, the 'Route Table: rtb-a6671fdb' is expanded, showing a table of routes. The table has two columns: 'Destination' and 'Target'. The routes listed are:

Destination	Target
192.168.0.0/16	local
0.0.0.0/0	igw-75f3ca0c
pl-63a5400a (com.amazonaws.us-east-1.s3)	vpce-258a074c

The bottom of the console shows a footer with 'Feedback', 'English (US)', and copyright information for Amazon Internet Services Private Ltd.

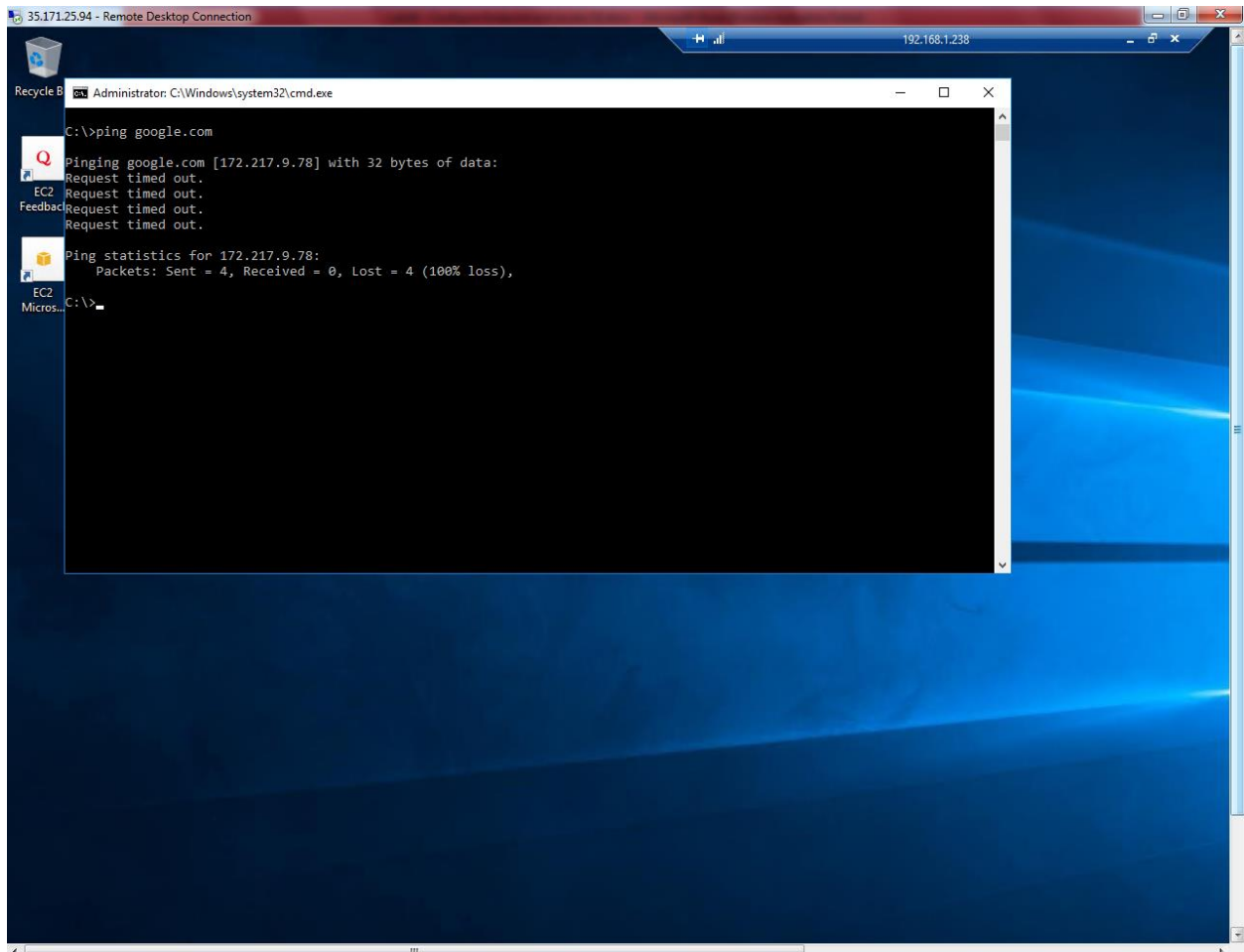
Create an windows 2016 instance by using regular steps.

Login to private instance.

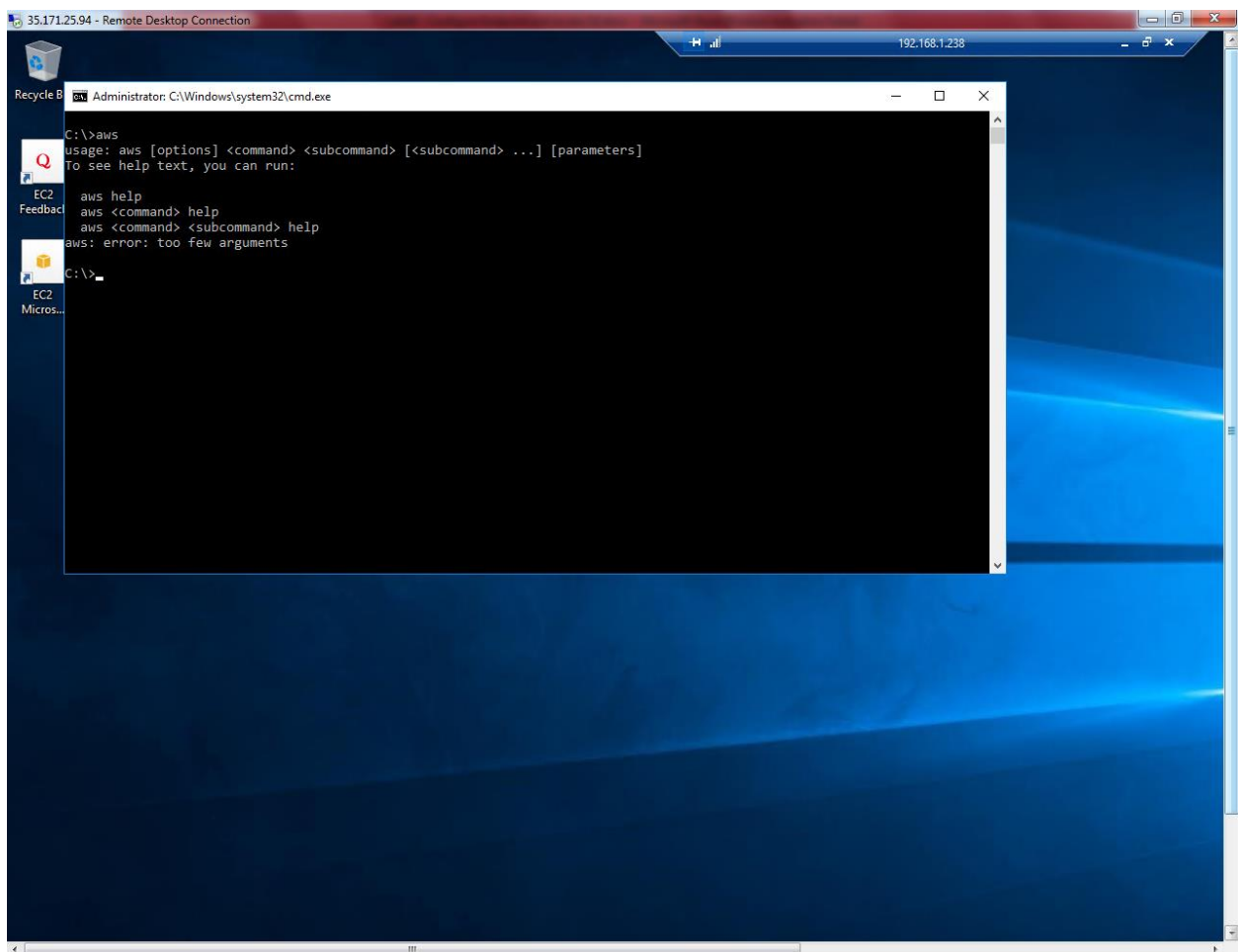


Copy and paste the command line interface setup in private server. Then run the setup in private subnet server.

Try to ping google.com from private subnet, you would not able to connect.



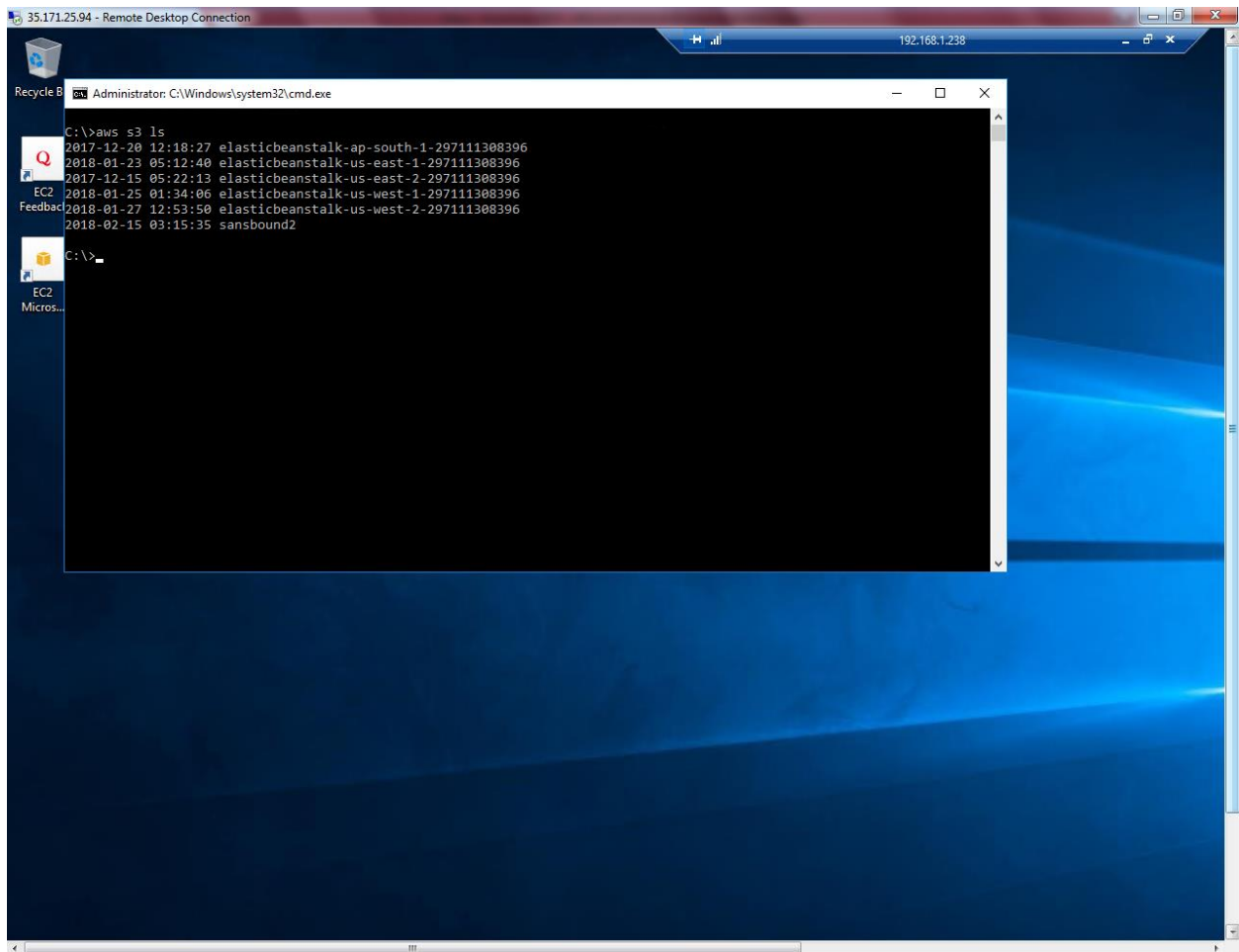
Type aws



The screenshot shows a Windows Remote Desktop connection window titled "35.171.25.94 - Remote Desktop Connection". The desktop background is the standard Windows 7 blue wallpaper. On the left taskbar, there are icons for Recycle Bin, a folder named "EC2", a folder named "Feedback", and a folder named "Micros...". An "Administrator: C:\Windows\system32\cmd.exe" command prompt window is open in the center. The command prompt shows the following text:

```
C:\>aws
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: too few arguments
C:\>
```

Type `aws s3 ls` in command prompt.

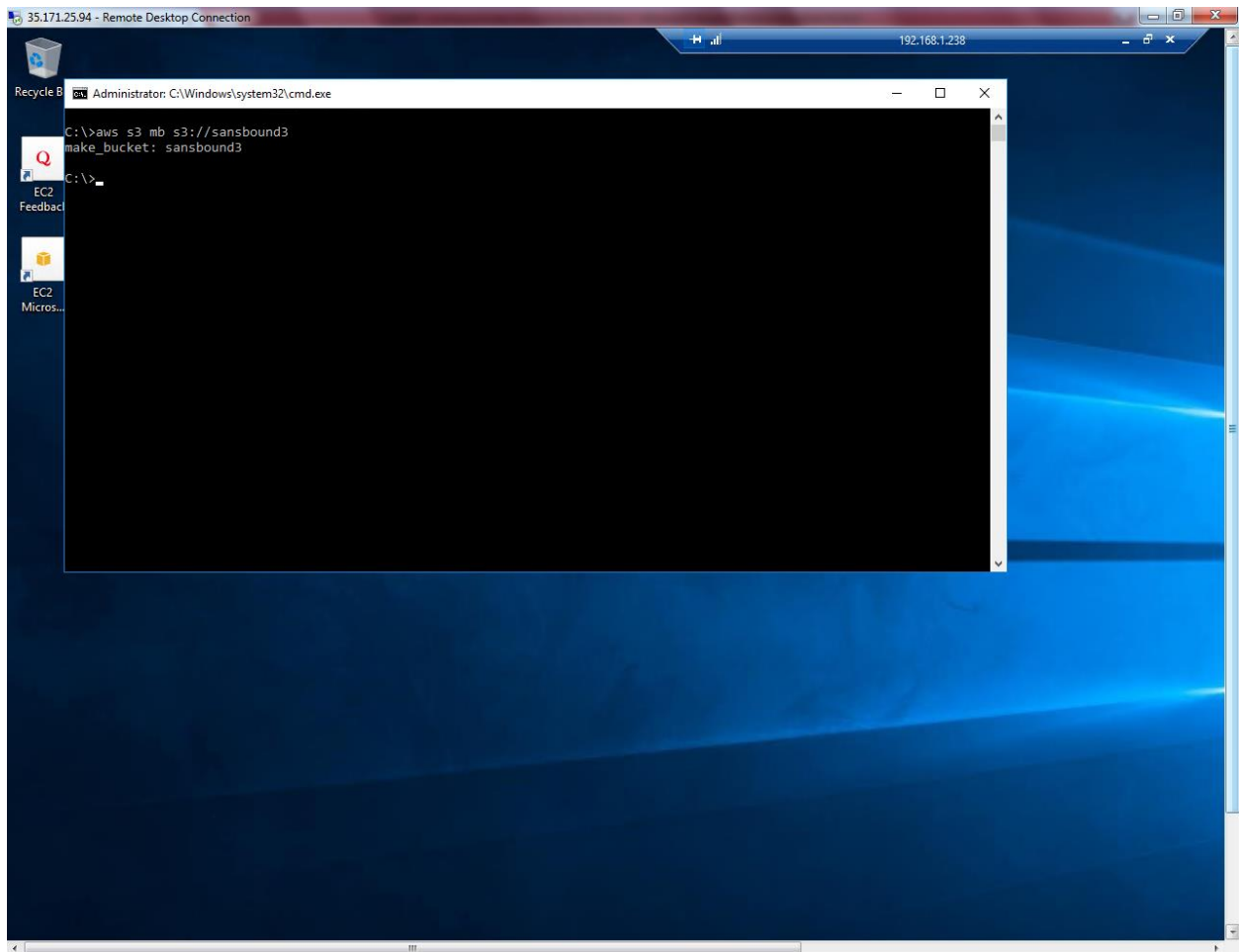


The screenshot shows a Windows Remote Desktop connection to an EC2 instance. The title bar indicates the connection is to 35.171.25.94. The desktop background is the standard Windows 7 blue logo wallpaper. A command prompt window is open, displaying the output of the `aws s3 ls` command. The output lists several S3 buckets, including `elasticbeanstalk-ap-south-1-297111308396`, `elasticbeanstalk-us-east-1-297111308396`, `elasticbeanstalk-us-east-2-297111308396`, `elasticbeanstalk-us-west-1-297111308396`, `elasticbeanstalk-us-west-2-297111308396`, and `sansbound2`. The command prompt window title is "Administrator: C:\Windows\system32\cmd.exe".

```
C:\>aws s3 ls
2017-12-20 12:18:27 elasticbeanstalk-ap-south-1-297111308396
2018-01-23 05:12:40 elasticbeanstalk-us-east-1-297111308396
2017-12-15 05:22:13 elasticbeanstalk-us-east-2-297111308396
2018-01-25 01:34:06 elasticbeanstalk-us-west-1-297111308396
2018-01-27 12:53:50 elasticbeanstalk-us-west-2-297111308396
2018-02-15 03:15:35 sansbound2
C:\>
```

S3 can be able to access without internet.

Type `aws s3 mb s3://sansbound3`

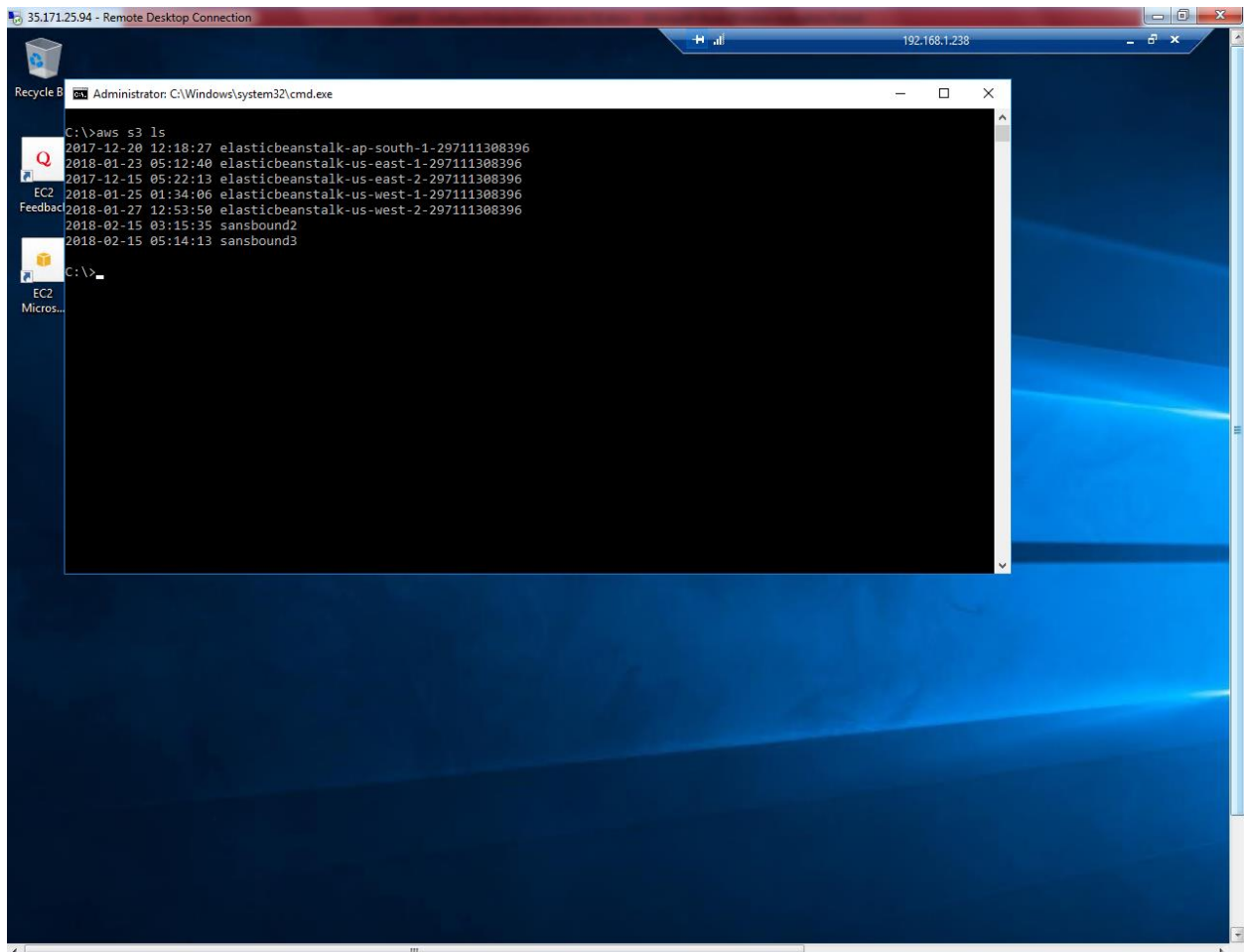


Sansbound3 bucket has been created.



Type

Aws s3 ls

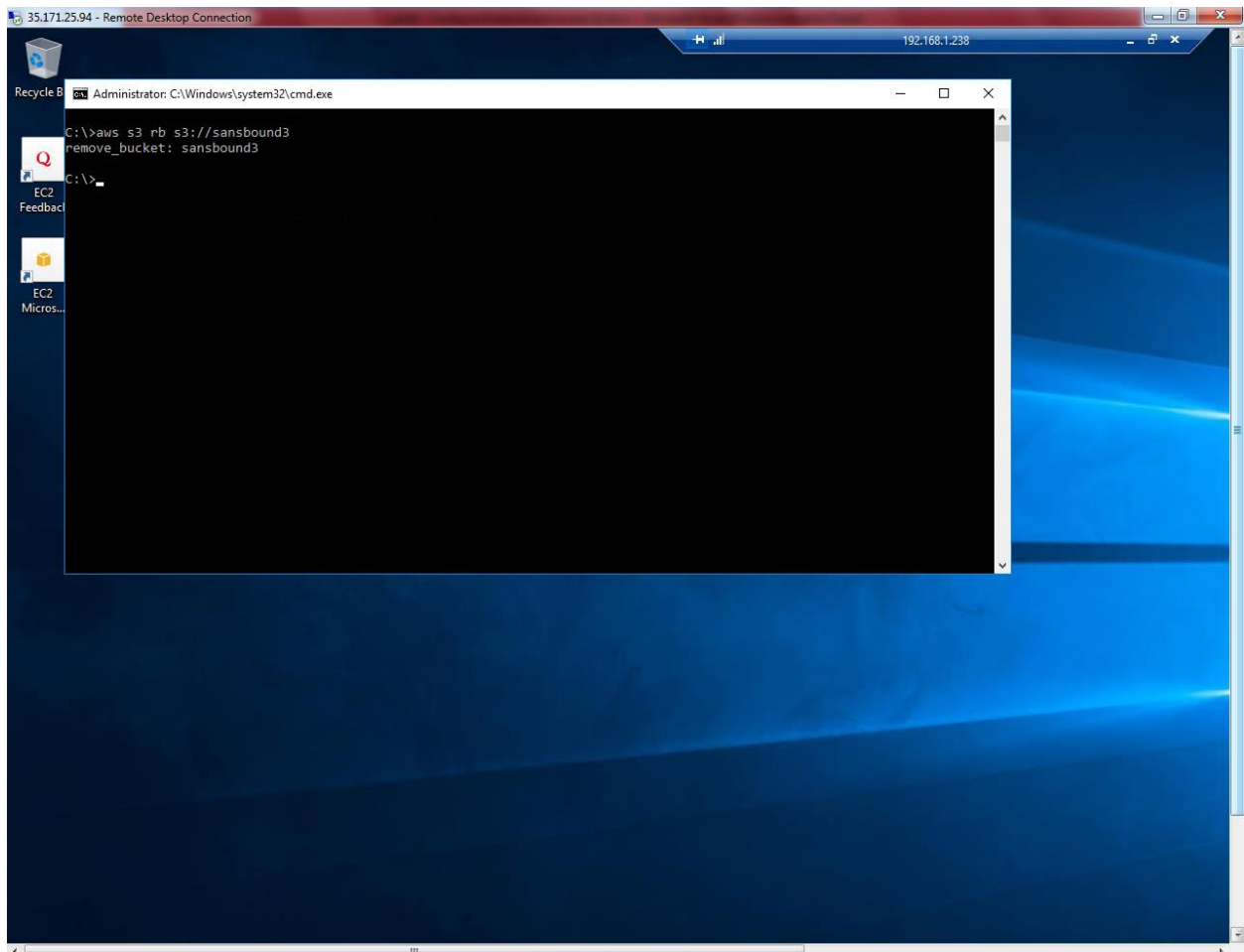


The screenshot shows a Windows Remote Desktop connection window titled "35.171.25.94 - Remote Desktop Connection". The remote desktop shows a Windows 7 desktop with a blue background. A command prompt window is open, displaying the output of the command `aws s3 ls`. The output lists several S3 buckets with their creation dates, times, and names.

```
C:\>aws s3 ls
2017-12-20 12:18:27 elasticbeanstalk-ap-south-1-297111308396
2018-01-23 05:12:40 elasticbeanstalk-us-east-1-297111308396
2017-12-15 05:22:13 elasticbeanstalk-us-east-2-297111308396
2018-01-25 01:34:06 elasticbeanstalk-us-west-1-297111308396
2018-01-27 12:53:50 elasticbeanstalk-us-west-2-297111308396
2018-02-15 03:15:35 sansbound2
2018-02-15 05:14:13 sansbound3
```

Type

Aws s3 rb s3://sansbound3



Sanbound3 bucket has been removed successfully.