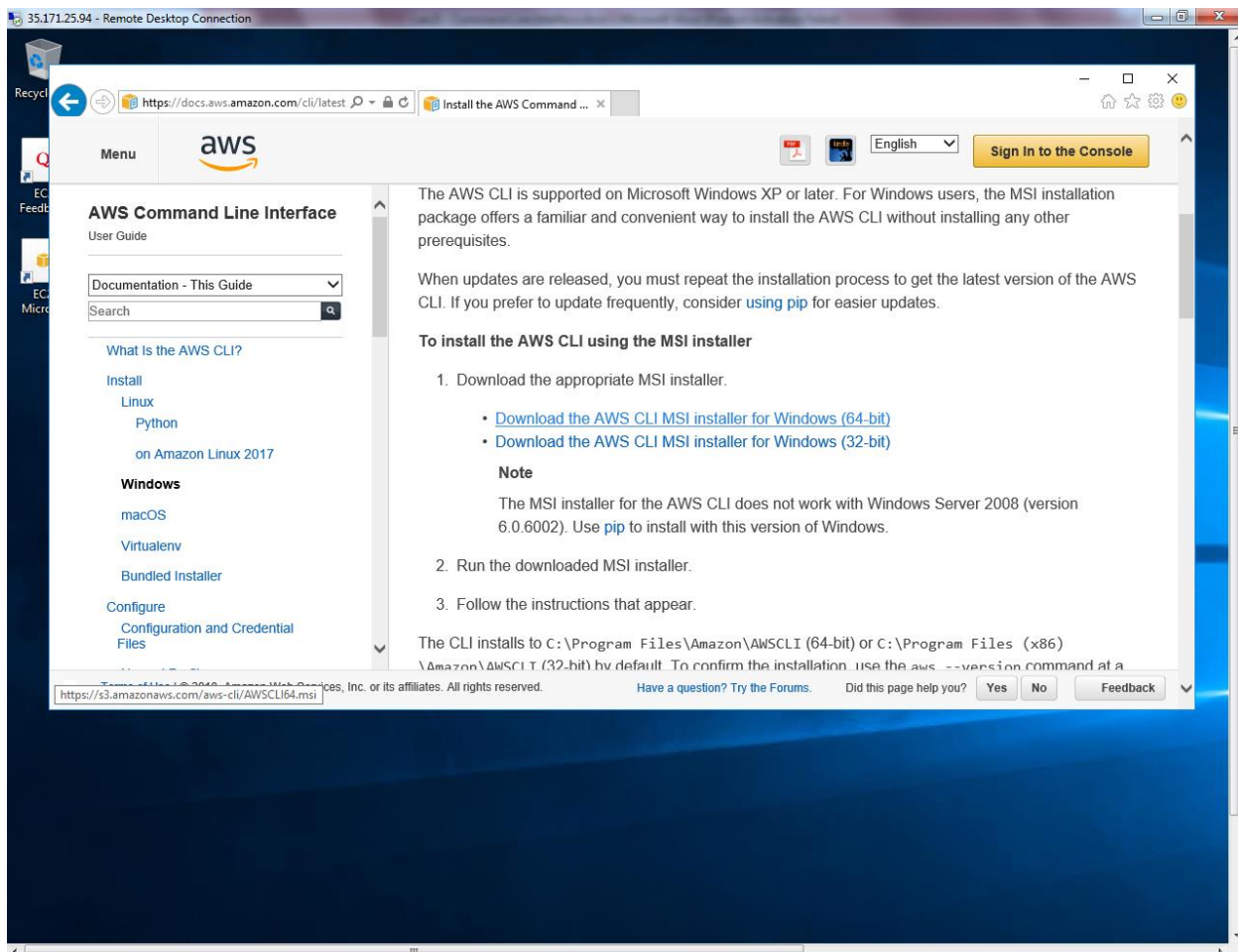


## Lab 26

### Configuring Endpoint and access the s3 bucket

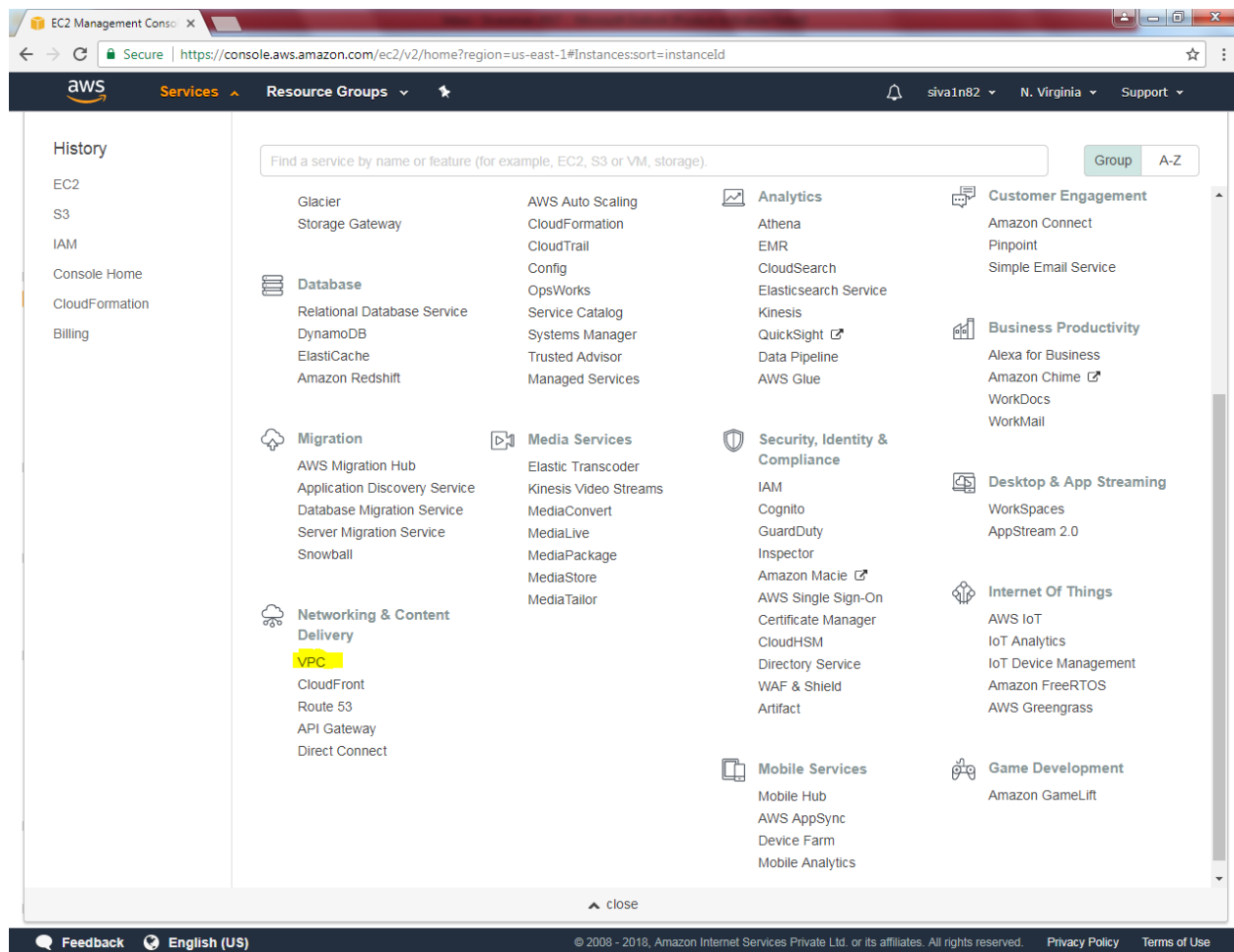
**Scenario: We have required to access s3 service without internet access from private subnet.**

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

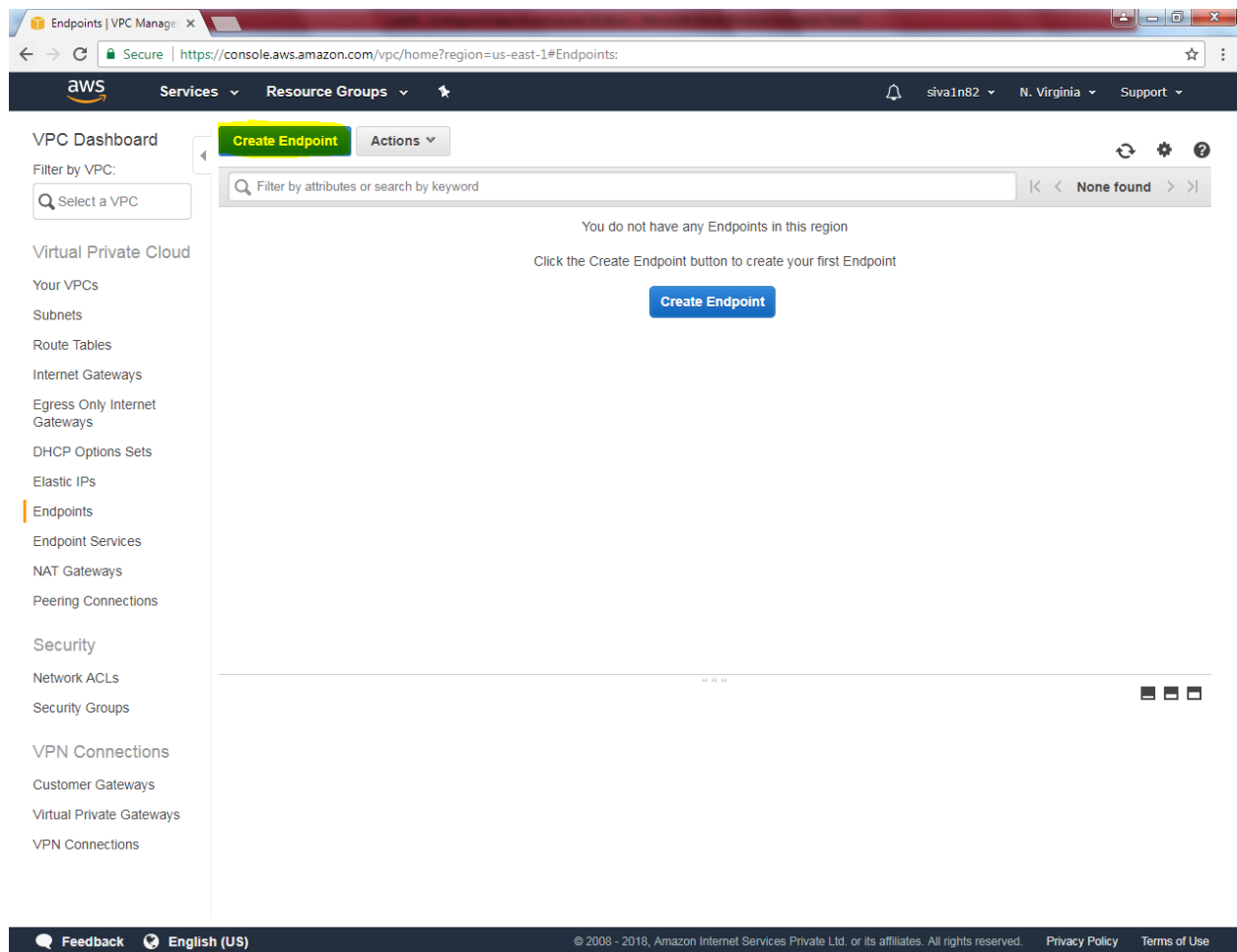


Download the package in public instance.

Go to services and click "VPC".



Click Endpoints and click “Crete Endpoint”.



Select S3.

Create Endpoint | VPC M x

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

Services Resource Groups

Endpoints > Create 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** com.amazonaws.us-east-1.s3 ⓘ

Filter by attributes

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.

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

Select VPC and select sanbound VPC's subnet.

The screenshot shows the AWS Management Console 'Create Endpoint' page for a VPC. The browser address bar shows the URL: <https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateVpcEndpoint>.

**Services List:**

Service	Provider	Interface
com.amazonaws.us-east-1.elasticloadbalancing	amazon	Interface
com.amazonaws.us-east-1.kinesis-streams	amazon	Interface
com.amazonaws.us-east-1.kms	amazon	Interface
com.amazonaws.us-east-1.s3	amazon	Gateway
com.amazonaws.us-east-1.servicecatalog	amazon	Interface
com.amazonaws.us-east-1.ssm	amazon	Interface

**VPC:** vpc-7697980e

**Configure route tables:**

Filter by attributes: [Search bar] with this endpoints' ID (e.g. vpce-12345678) will be added to

VPC ID	IP Address	Availability	Subnet
vpc-7697980e	192.168.0.0/16	available	Sansbound_NVG_VPC
vpc-765c7f0e	172.31.0.0/16	available	

**Route Table ID:** rtb-a6671fdb

Route Table ID	Main	Associated With
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.

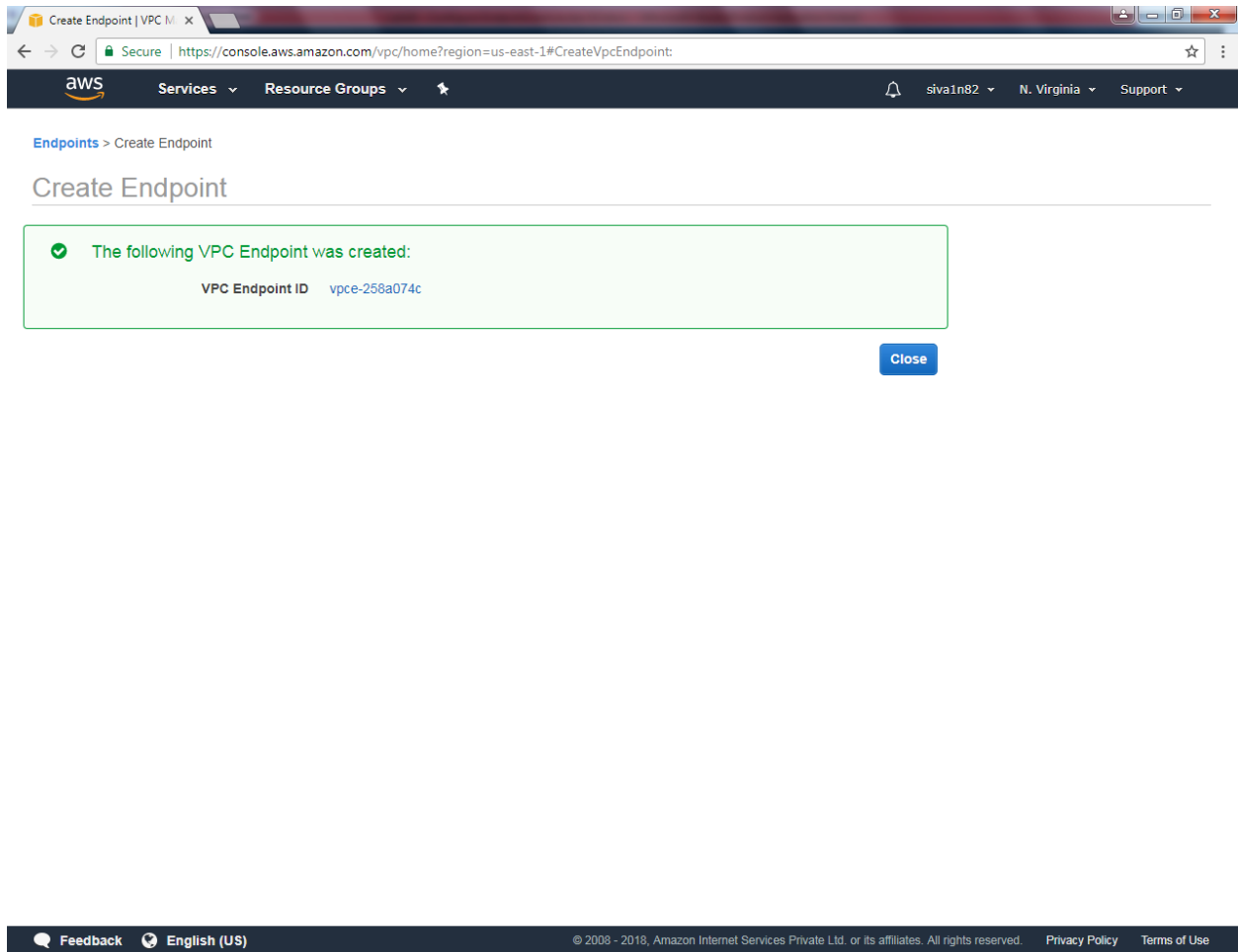
```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

\* 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.



Endpoint is now available.

The screenshot shows the AWS VPC Dashboard in the console. The left sidebar contains navigation links for VPC resources. The main area displays a table of endpoints. Below the table, the details for the selected endpoint 'vpce-258a074c' are shown, including its ID, VPC ID, service name, status, 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 VPC Dashboard in the us-east-1 region. The 'Create Subnet' button is highlighted in yellow. The dashboard displays a list of existing subnets with the following details:

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	

Below the table, there is a section titled 'Select a subnet above' with three small icons.

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

Sansbound\_Private\_Subnet\_NVG

VPC

vpc-7697980e | Sansbound\_NVG\_VPC

VPC CIDRs

CIDR	Status	Status Reason
192.168.0.0/16	associated	

Availability Zone

No Preference

IPv4 CIDR block

192.168.1.0/24

Cancel

Yes, Create

Click “Yes create”.

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

The screenshot displays the AWS VPC console interface. On the left, the 'VPC Dashboard' sidebar lists various network services. The main content area shows a list of subnets under the 'Subnets' section. The subnet 'Sansbound\_Private\_Subnet\_NVG' is selected. Below the subnet list, the 'Route Table: rtb-a6671fdb' is expanded, showing a routing table with three entries. The first entry routes traffic from 192.168.0.0/16 to the 'local' target. The second entry routes traffic from 0.0.0.0/0 to the 'igw-75f3ca0c' target. The third entry routes traffic from 'pl-63a5400a (com.amazonaws.us-east-1.s3)' to the 'vpce-258a074c' target.

**Subnets List:**

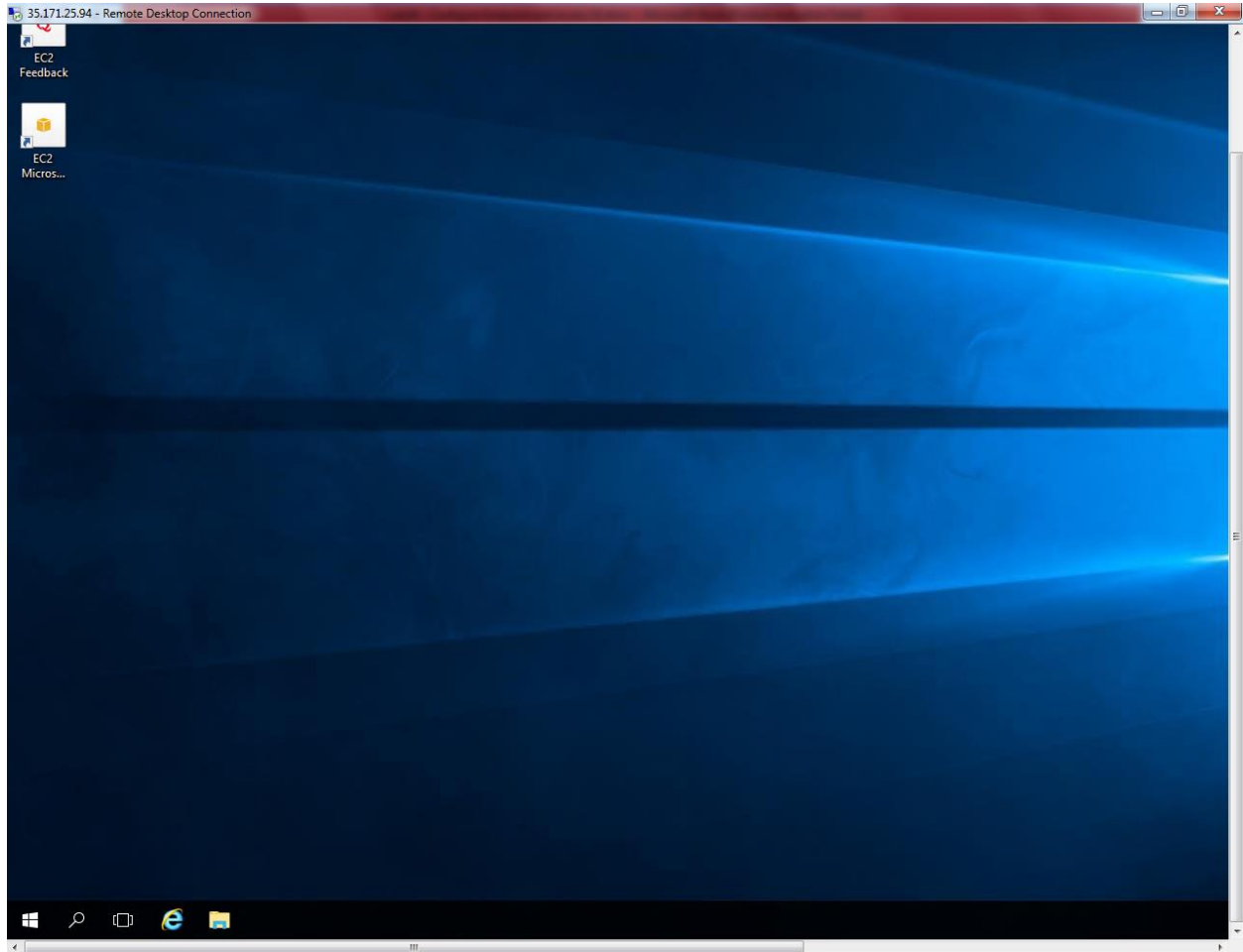
Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
	subnet-02f1a549	available	vpc-765c7f0e	172.31.16.0/20	4091	
	subnet-ebd25bc4	available	vpc-765c7f0e	172.31.80.0/20	4091	
	subnet-6affb10e	available	vpc-765c7f0e	172.31.0.0/20	4091	
	subnet-ccb559c3	available	vpc-765c7f0e	172.31.48.0/20	4091	
Sansbound_NVG_Public Subnet	subnet-67adce48	available	vpc-7697980e   Sansbound_NVG...	192.168.2.0/24	250	
<b>Sansbound_Private_Subnet_NVG</b>	<b>subnet-46eba569</b>	<b>available</b>	<b>vpc-7697980e   Sansbound_NVG...</b>	<b>192.168.1.0/24</b>	<b>251</b>	
	subnet-a1fc989e	available	vpc-765c7f0e	172.31.64.0/20	4091	
	subnet-0d6ec50	available	vpc-765c7f0e	172.31.32.0/20	4091	

**Route Table: rtb-a6671fdb**

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

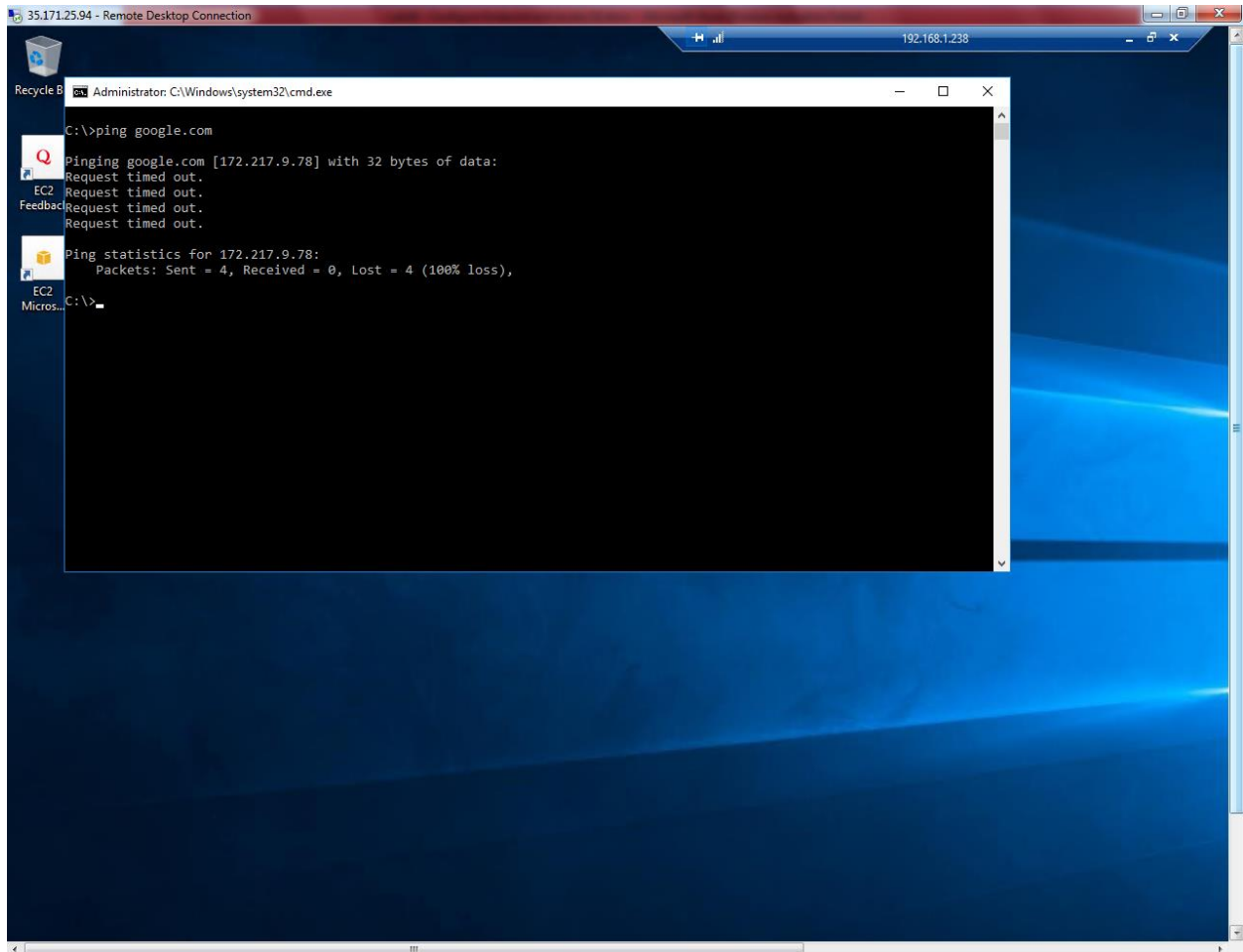
Create an windows 2016 instance by using regular steps.

Login to private instance.

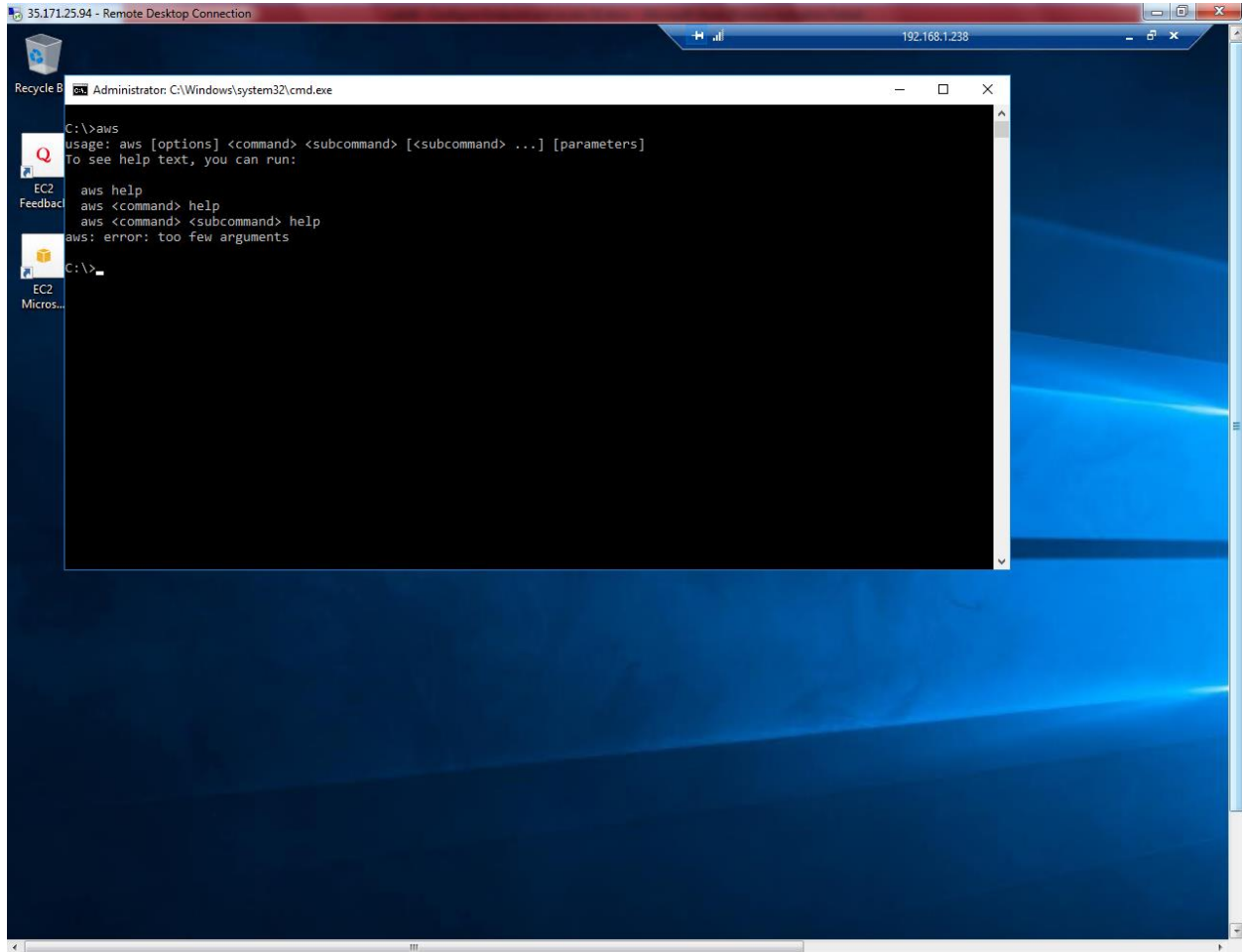


Copy and paste the command line interface setup in private server. Then run the setup in private subnet server.

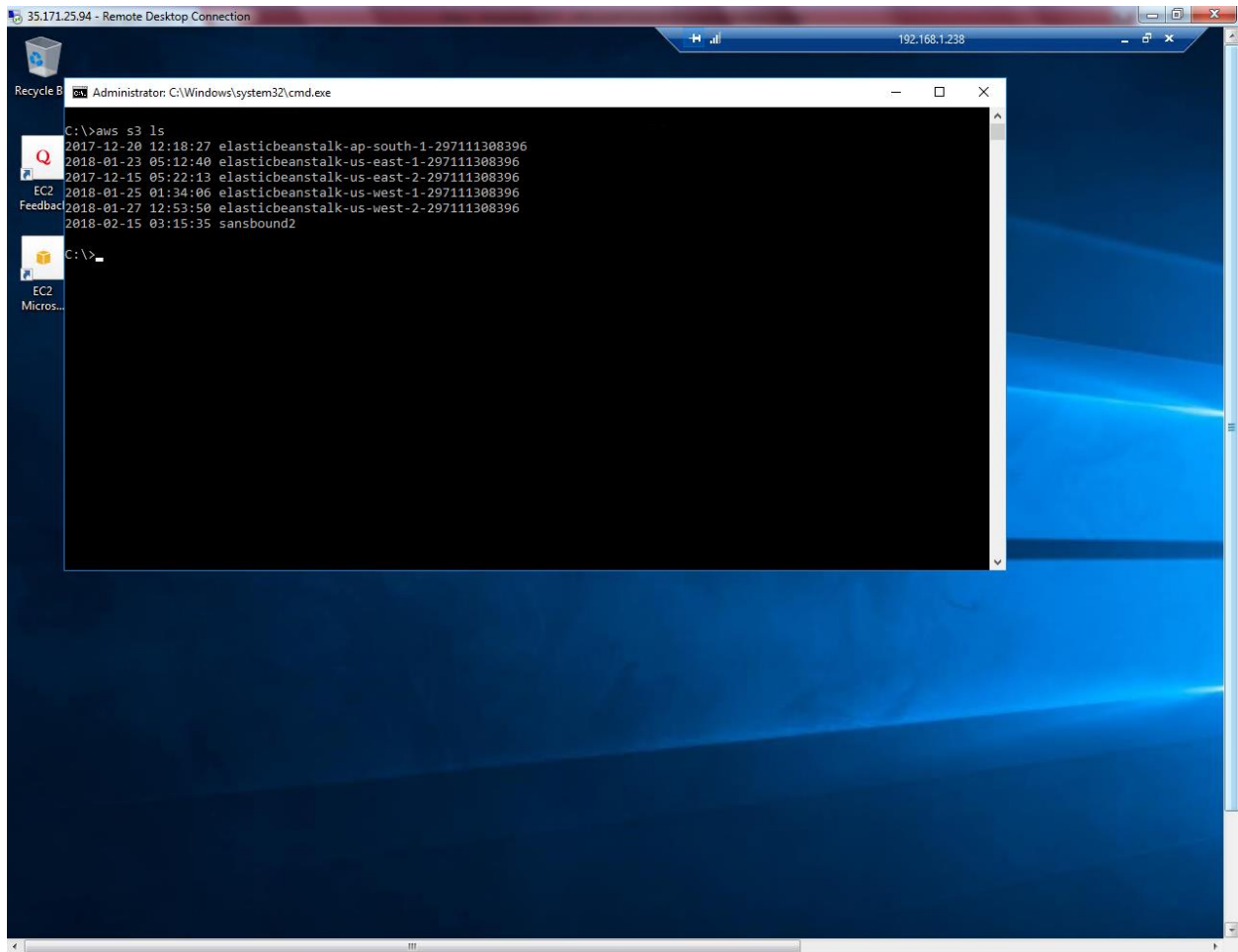
Try to ping google.com from private subnet, you would not able to connect.



Type aws

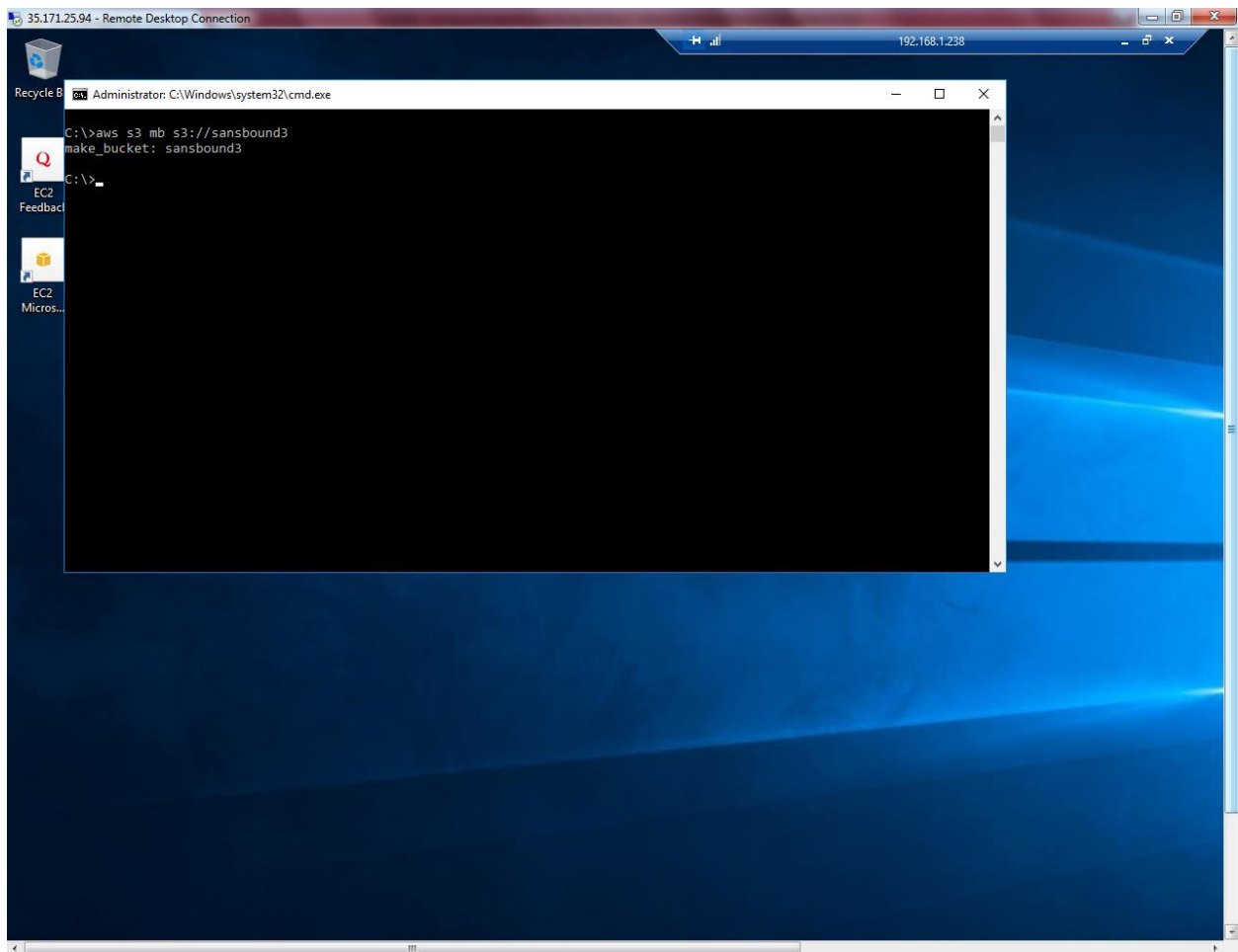


Type aws s3 ls in command prompt.



S3 can be able to access without internet.

Type `aws s3 mb s3://sansbound3`

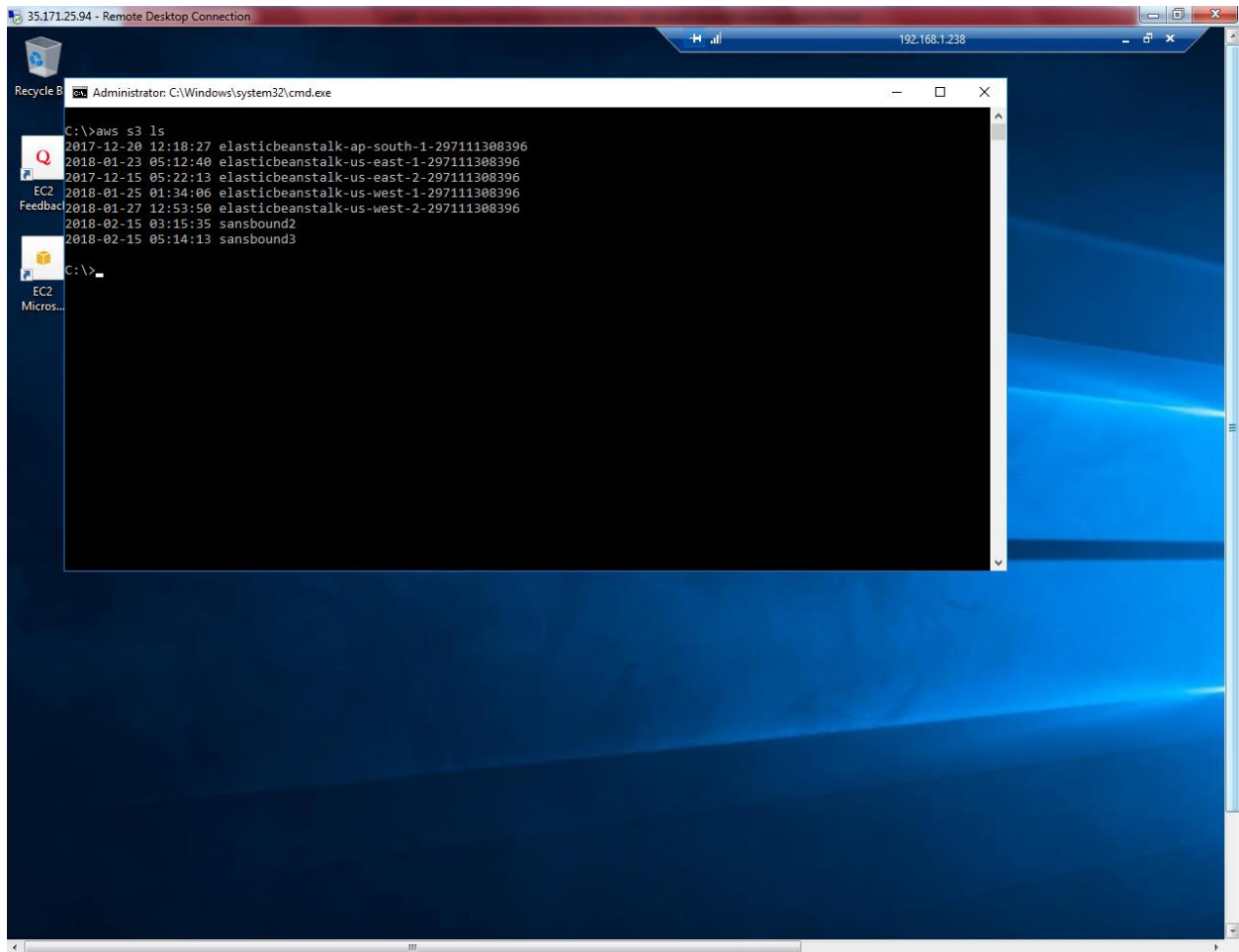


Sansbound3 bucket has been created.

Type

Aws s3 ls

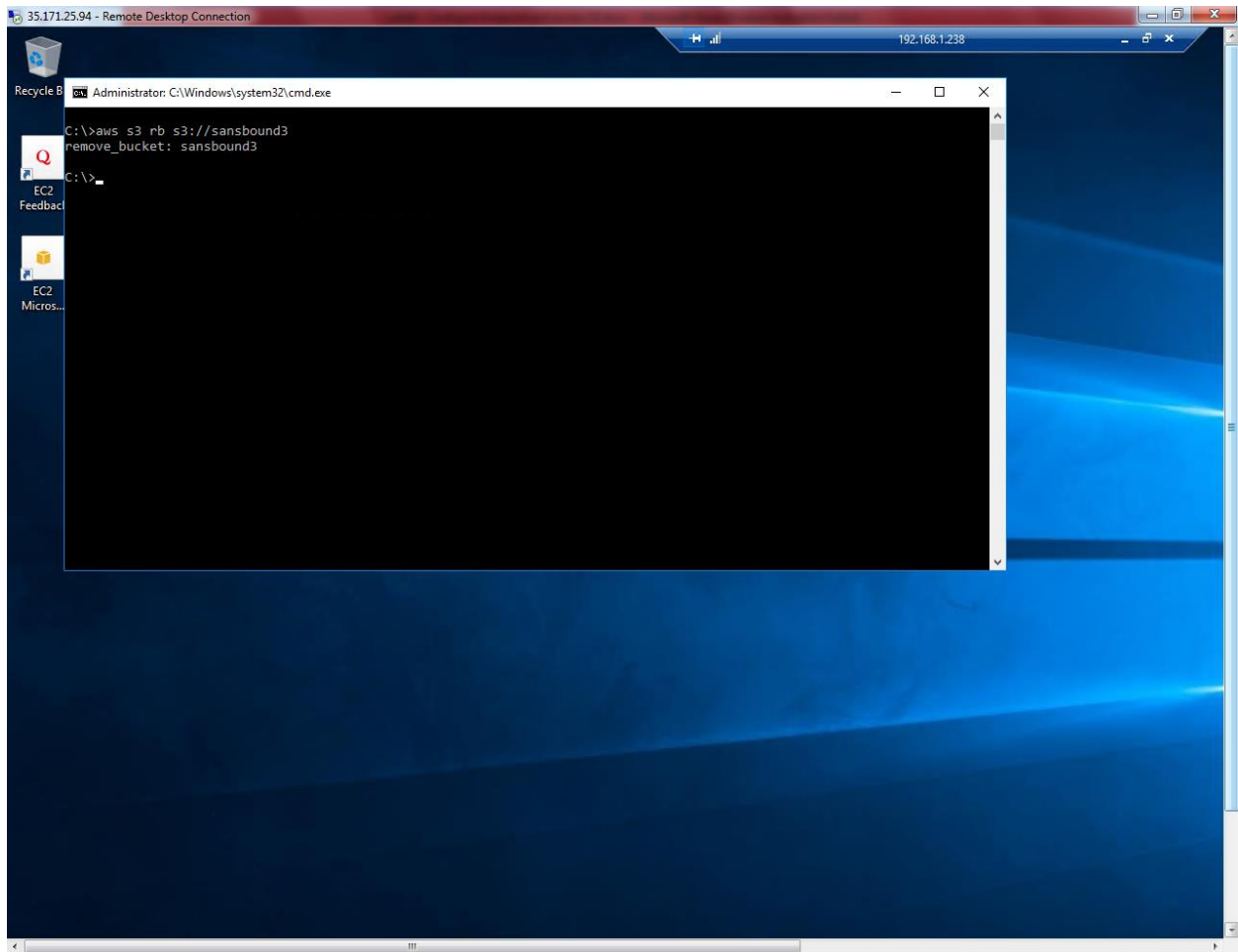




```
C:\>aws s3 ls
2017-12-20 12:18:27 elasticbeanstalk-ap-south-1-297111308396
2018-01-23 05:12:40 elasticbeanstalk-us-east-1-297111308396
2017-12-15 05:22:13 elasticbeanstalk-us-east-2-297111308396
2018-01-25 01:34:06 elasticbeanstalk-us-west-1-297111308396
2018-01-27 12:53:50 elasticbeanstalk-us-west-2-297111308396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

Type

Aws s3 rb s3://sansbound3



Sanbound3 bucket has been removed successfully.