

AWS Multi-Region VPC Peering Setup with Private and Public Subnet Instances

Project Overview

The objective of this documentation is to guide through the process of setting up a multi-region AWS Virtual Private Cloud (VPC) architecture with peering connections between two regions. This includes creating and configuring VPCs, subnets, internet gateways, NAT gateways, security groups, and EC2 instances in both Ohio (Zone A) and Mumbai (Zone B) regions. The configuration ensures that instances in the private subnets across regions can securely communicate with each other, simulating a private, interconnected network between geographically separated VPCs.

Prerequisites

AWS Account:

- You must have an active AWS account with permissions to create and manage VPCs, subnets, route tables, internet gateways, NAT gateways, security groups, and EC2 instances.

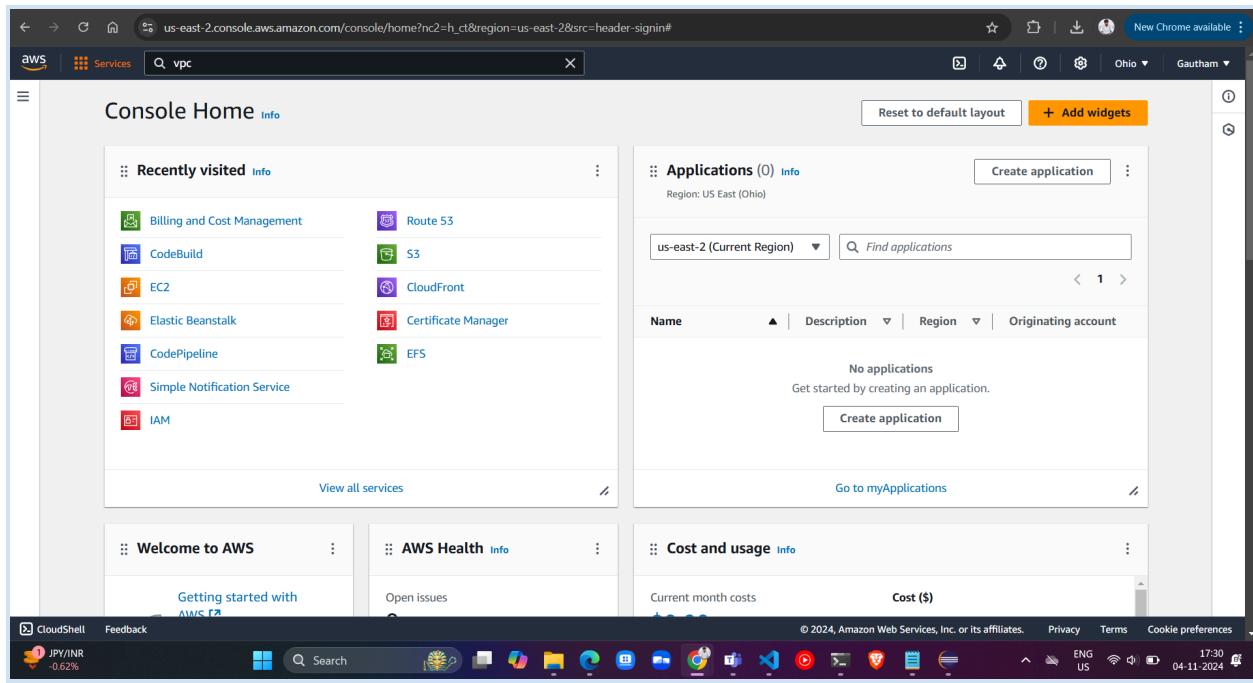
IAM User Permissions:

- The user performing this setup should have permissions for the following AWS services:
 - VPC, Subnet, Route Table, Internet Gateway, NAT Gateway, Peering Connections, Security Group, and EC2.

Procedures

Step 1: Login to AWS Account

- Log in to your AWS Management Console.



Step 2: Create a VPC in Zone A (Ohio)

- **Navigate to VPC Service:**
 - Go to VPC service dashboard and click **Create VPC**.
- **VPC Settings:**
 - Select **VPC Only**.
 - **Name Tag:** Enter **vpc-a**.
 - **IPv4 CIDR Manual Input:** Enter **118.0.0.0/16**.
 - Click **Create VPC**.

The screenshot shows two consecutive pages from the AWS VPC console.

Create VPC (Step 1: **VPC settings**)

- Resources to create:** VPC only
- Name tag - optional:** vpc-a
- IPv4 CIDR block:** IPAM-allocated IPv4 CIDR block
- IPv4 IPAM pool:** Choose an IPAM pool
- Netmask:** Choose a netmask
- IPv6 CIDR block:** No IPv6 CIDR block

VPC dashboard (Step 2: **Details**)

vpc-0ef3c374ecf1661df / vpc-a

VPC ID	State	DNS hostnames	DNS resolution
vpc-0ef3c374ecf1661df	Available	Disabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-073e0a5ef331acc33	rtb-059af50c256a27d1e	acl-0a51e349f118c6fde
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR
No	118.0.0.0/16	-	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	
Disabled	-	116981766729	

Resource map

- VPC: Show details
- Subnets (0)
- Route tables (1)

Step 3: Create Subnets in VPC-A

Public Subnet:

- Go to **Subnets** and click **Create subnet**.
- VPC ID:** Choose **vpc-a**.
- Subnet Name:** Enter **pubsub-a**.
- Availability Zone:** Select **us-east-2a**.
- IPv4 CIDR Block:** Enter **118.0.10.0/24**.

Private Subnet:

- Add another subnet.
- **Subnet Name:** Enter **pvtsub-a**.
- **Availability Zone:** Select **us-east-2b**.
- **IPv4 CIDR Block:** Enter **118.0.20.0/24**.
- Click **Create subnet**.

The screenshot shows the AWS VPC dashboard with a success message: "You have successfully created 2 subnets: subnet-08511ac4c3f6bc808, subnet-0b70c1563b92a8acc". The subnets table lists:

Name	Subnet ID	State	VPC	IPv4 CIDR
pvtsub-a	subnet-0b70c1563b92a8acc	Available	vpc-0ef3c374ecf1661df vpc-a	118.0.20.0/24
pubsub-a	subnet-08511ac4c3f6bc808	Available	vpc-0ef3c374ecf1661df vpc-a	118.0.10.0/24

Step 4: Create and Attach Internet Gateway

Public Subnet:

Navigate to Internet Gateway:

- Go to **Internet Gateways** and click **Create Internet Gateway**.
- **Name Tag:** Enter **igw-a**.

The screenshot shows the AWS VPC Internet Gateways creation interface. At the top, the URL is `us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#CreateInternetGateway`. The navigation bar includes 'AWS Services' and a search bar. On the right, there are user profile and account information.

The main content area is titled 'Create internet gateway' with a 'Info' link. A descriptive text explains that an internet gateway is a virtual router that connects a VPC to the internet. It prompts the user to specify a name for the gateway below.

The 'Internet gateway settings' section contains a 'Name tag' field where the value 'igw-a' is entered. Below this is a 'Tags - optional' section where a tag 'Name: igw-a' is added. There is also a note indicating 49 more tags can be added.

At the bottom of the form are 'Cancel' and 'Create internet gateway' buttons. The status bar at the bottom of the browser window shows the date and time as '04-11-2024 14:39'.

Attach to VPC:

- Select the created internet gateway and click **Attach to VPC**.
- Choose **vpc-a** and click **Attach Internet Gateway**.

The following internet gateway was created: igw-0b8fabd236780b83a - igw-a. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to VPC (igw-0b8fabd236780b83a) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

[X](#)

[▶ AWS Command Line Interface command](#)

[Cancel](#) [Attach internet gateway](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 14:40 04-11-2024

Internet gateway igw-0b8fabd236780b83a successfully attached to vpc-0ef3c374ecf1661df

VPC dashboard [Actions](#)

Internet gateway igw-0b8fabd236780b83a / igw-a

Details [Info](#)

Internet gateway ID igw-0b8fabd236780b83a	State Attached	VPC ID vpc-0ef3c374ecf1661df vpc-a	Owner 116981766729
--	-----------------------------------	---	---------------------------------------

Tags

Search tags	Manage tags
Key	Value
Name	igw-a

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 14:40 04-11-2024

Step 5: Create and Configure Route Tables

Public Route Table:

- Go to **Route Tables** and click **Create Route Table**.
- **Name:** Enter `pubrt-a`.
- **Routes:** Edit routes and add `0.0.0.0/0` as the destination with the internet gateway (`igw-a`) as the target.

- **Subnet Associations:** Associate with `pubsub-a`.

The screenshot shows two consecutive screenshots of the AWS VPC console interface.

Screenshot 1: Create route table

This screen is titled "Create route table" and includes the following details:

- Route table settings:**
 - Name - *optional*: pubrt-a
 - VPC: vpc-0ef3c374ecf1661df (vpc-a)
- 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: Name, Value: pubrt-a
 - Add new tag

At the bottom right, there is a prominent orange "Create route table" button.

Screenshot 2: Route table details

This screen shows the details of the newly created route table, `rtb-08a6765dc7273cf1`, which is associated with the subnet `pubrt-a`.

Details:

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-08a6765dc7273cf1	No	-	-
VPC	Owner ID		
vpc-0ef3c374ecf1661df vpc-a	116981766729		

Routes:

Destination	Target	Status	Propagation
118.0.0.0/16	local	Active	No

Edit routes

Destination	Target	Status	Propagated
118.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway igw-0b8fabd236780b83a	-	No

Add route Remove Cancel Preview Save changes

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)					
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID	
pvtsub-a	subnet-0b70c1563b92a8acc	118.0.20.0/24	-	Main (rtb-059af50c256a27d1e)	
<input checked="" type="checkbox"/> pubsub-a	subnet-08511ac4c3f6bc808	118.0.10.0/24	-	Main (rtb-059af50c256a27d1e)	

Selected subnets

subnet-08511ac4c3f6bc808 / pubsub-a

Cancel Save associations

Private Route Table:

- Create another route table and name it **pvttrt-a**.
- Associate it with **pvtsub-a** under **Subnet Associations**.

The screenshot shows two pages from the AWS VPC console:

- Edit subnet associations**: This page allows you to associate subnets with a specific route table. It lists available subnets and selected subnets. In the 'Selected subnets' section, 'subnet-0b70c1563b92a8acc / pvtsub-a' is selected. The 'Save associations' button is highlighted.
- Route tables (4) Info**: This page lists existing route tables. The table includes columns for Name, Route table ID, Explicit subnet associations, Edge associations, Main status, and VPC. The route table 'rtb-07ce7b666e74ea028' is associated with the subnet 'subnet-0b70c1563b92a8acc'.

Step 6: Create a NAT Gateway

- **Navigate to NAT Gateways:**
 - Go to **NAT Gateway** and click **Create NAT Gateway**.
 - **Name:** Enter **mynat-a**.
 - **Subnet:** Choose the public subnet (**pubsub-a**).
 - **Elastic IP:** Allocate a new elastic IP.
 - Click **Create NAT Gateway**.

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
mynat-a
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-08511ac4c3f6bc808 (pubsub-a)

Connectivity type
Select a connectivity type for the NAT gateway.
 Public
 Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.
eipalloc-0cd6f791606a00e40

► Additional settings [Info](#)

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

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- **Add Route for Private Route Table:**

- Go to **pvtprt-a** and edit routes.
- **Destination:** Enter **0.0.0.0/0** and select the created NAT Gateway (**mynat-a**) as the target.

Edit routes

Destination	Target	Status	Propagated
118.0.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway		No
	nat-08d6de406cbd2acb4		

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 7: Create Security Groups

Public Security Group (pubsg-a):

- Go to **Security Groups** and click **Create Security Group**.
- **Name:** Enter **pubsg-a**.
- **VPC:** Select **vpc-a**.
- **Inbound Rule:** Allow **All TCP** with **0.0.0.0/0**.

The screenshot shows the 'Create Security Group' wizard on the AWS EC2 console. In the 'Basic details' step, the security group name is set to 'pubsg-a'. The VPC is selected as 'vpc-a'. In the 'Inbound rules' section, a rule is defined for 'All TCP' on port range '0 - 65535' from 'Anywhere' (0.0.0.0/0). A warning message at the bottom states: '⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' The 'Outbound rules' section is currently empty.

Private Security Group (pvtsg-a):

- Create another security group named **pvtsg-a** in **vpc-a**.
- **Inbound Rule:** Allow connections from the public security group (**pubsg-a**).

The screenshot shows the 'Create Security Group' wizard on the AWS EC2 console. In the 'Basic details' step, the security group name is set to 'pvtsg-a'. The VPC is selected as 'vpc-a'. In the 'Inbound rules' section, a rule is being configured for 'All TCP' on port range '0 - 65535' from a 'Custom' source. A dropdown menu is open, showing the previously created security group 'pubsg-a' under the 'Security Groups' section. The 'Source' dropdown also lists the ID 'sg-01d72b3fce2e5393'. A warning message at the bottom states: '⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

Step 8: Launch EC2 Instances in VPC-A

Public EC2 Instance:

- Go to **EC2 Instances** and click **Launch Instances**.
- **Name:** Enter **pub-ec2-a**.
- **AMI:** Choose Windows Server 2022.
- **Network Settings:** Select **vpc-a**, **pubsub-a**, and enable **Auto-assign Public IP**.
- **Security Group:** Choose **pubsg-a**.

Private EC2 Instance:

- Launch another instance with **Name pvt-ec2-a**.
- **Subnet:** Select **pvtsub-a**, disable **Auto-assign Public IP**, and choose **pvtsg-a** as the security group.

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table of instances. There are two rows in the table:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
pub-ec2-a	i-022449a4712d70ad9	Running	t2.micro	2/2 checks passed	View alarms +	us-east-2a	-
pvt-ec2-a	i-0882ca4119f3508ec	Running	t2.micro	Initializing	View alarms +	us-east-2b	-

Below the table, there is a detailed view for the instance **i-0882ca4119f3508ec (pvt-ec2-a)**. The details include:

- Details:** Shows the instance ID (i-0882ca4119f3508ec), public IPv4 address (118.0.20.254), private IPv4 addresses (118.0.20.254), and public IPv4 DNS (ip-118-0-20-254.us-east-2.compute.internal).
- Status and alarms:** Shows the instance state as Running.
- Monitoring:** Shows the instance is not currently monitoring.
- Security:** Shows the instance is not currently secured.
- Networking:** Shows the instance has no network interfaces.
- Storage:** Shows the instance has no storage devices.
- Tags:** Shows the instance has no tags.

Step 9: Test Connectivity

- **Public EC2 to Private EC2 Connection:**
 - Use **Remote Desktop Connection** to connect **pub-ec2-a** to **pvt-ec2-a** via private IP.
 - Verify network connectivity using **ping** commands.

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-022449a4712d70ad9

aws Services Search [Alt+S]

Instance ID: i-022449a4712d70ad9 (pub-ec2-a)

Connection Type:

- Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
- Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client or by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

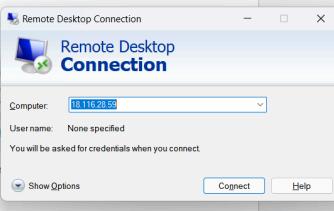
When prompted, connect to your instance using the following username and password:

Public IP: 18.116.28.59 Username Info: Administrator

Password: Get password

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel



CloudShell Feedback

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-022449a4712d70ad9

aws Services Search [Alt+S]

Instance ID: i-022449a4712d70ad9 (pub-ec2-a)

Connection Type:

- Connect using RDP client
Download a file to use with your RDP client and retrieve your password.
- Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

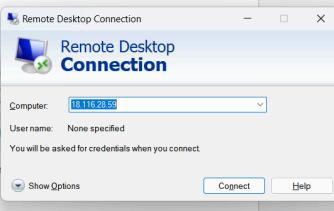
When prompted, connect to your instance using the following username and password:

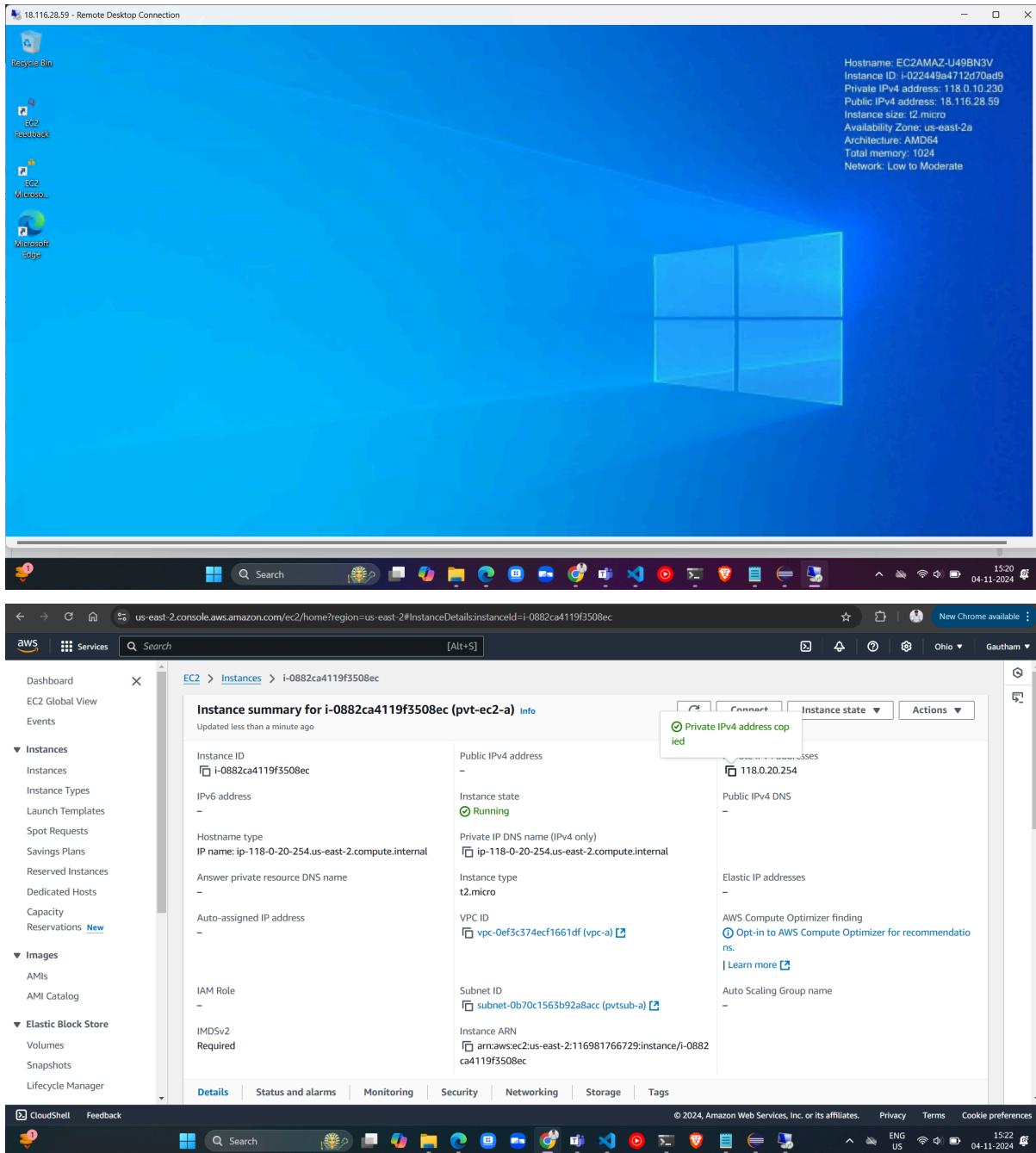
Public IP: 18.116.28.59 Username Info: Administrator

Password: vMLKHvK1dp4B0d5fk5dCWT55ljvZN.

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel





us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#ConnectToInstance:instanceId=i-0882ca4119f3508ec

Services Search [Alt+S]

I-0882ca4119f3508ec (pvt-ec2-a)

Connection Type

Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Private IP: 118.0.20.254

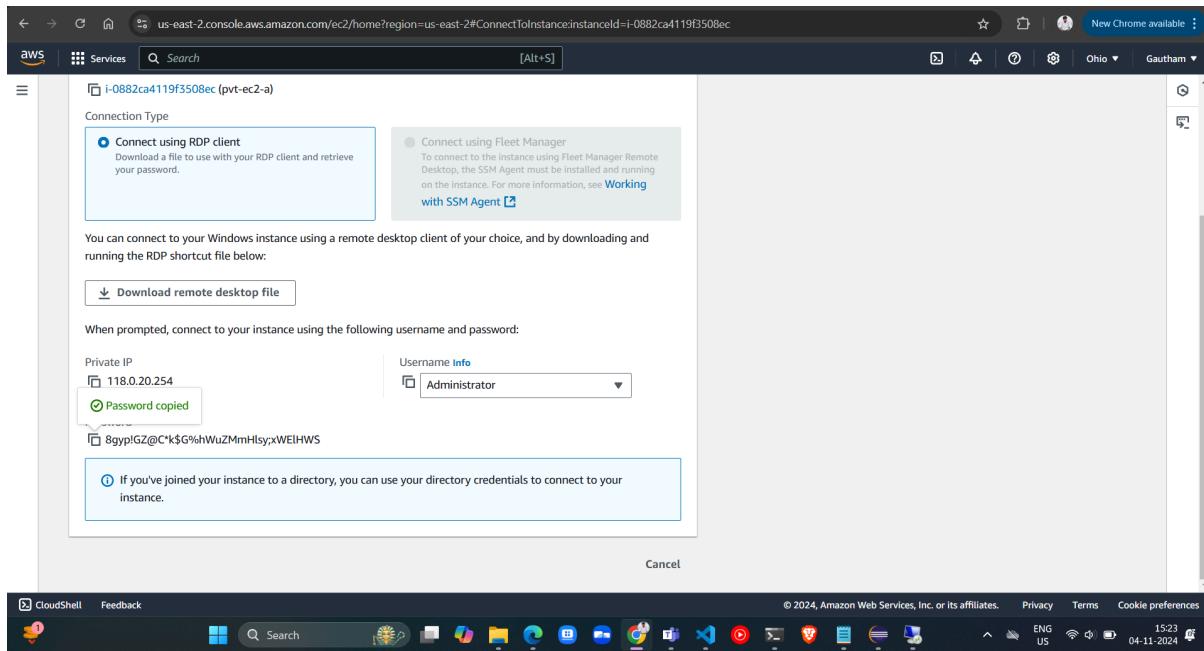
Username: Administrator

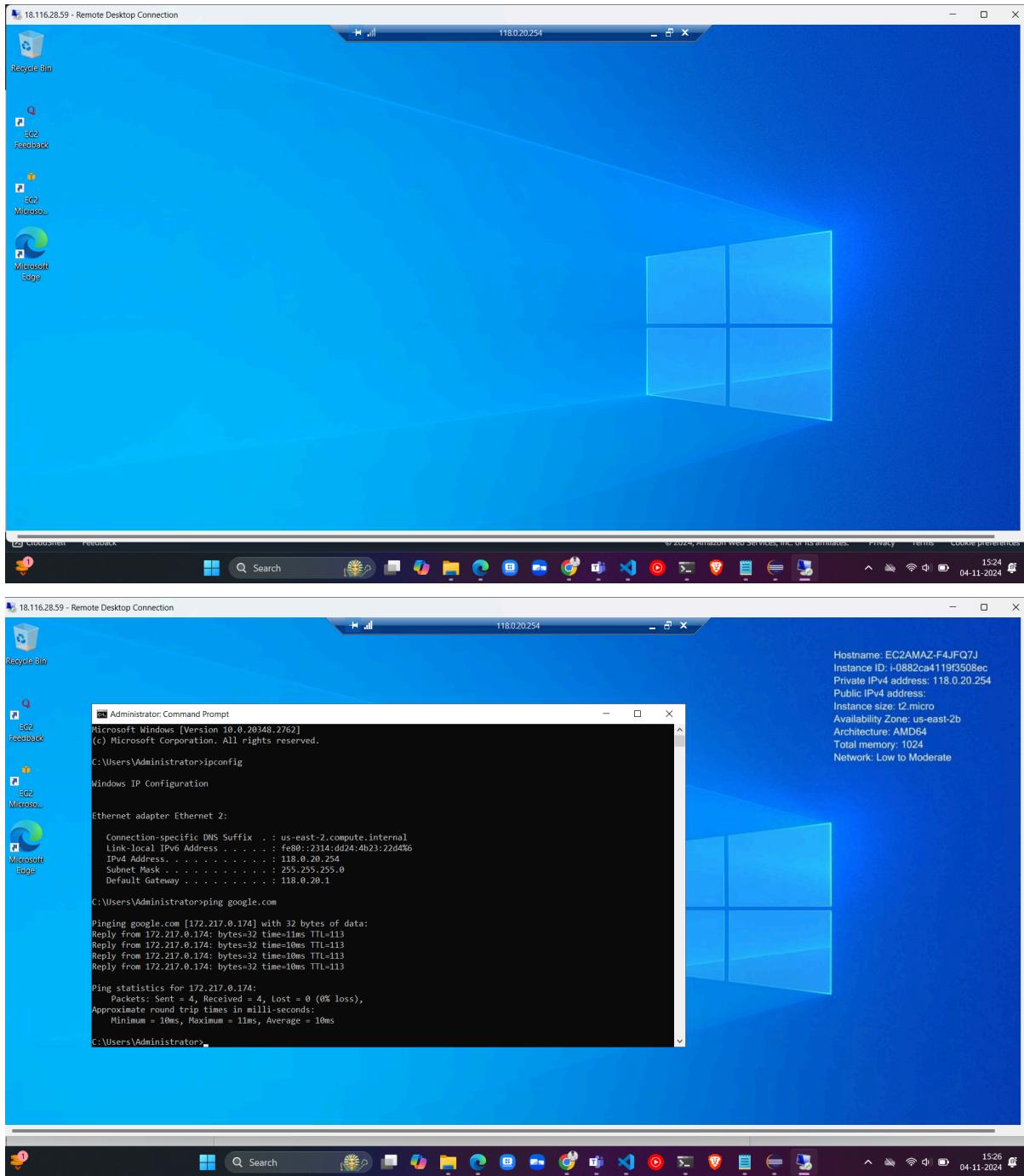
Password copied: Bgyp!GZ@C*k\$G%hWuZMmHsy;xWEIHWS

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 15:23 04-11-2024





Step 10-16: Repeat Setup in Zone B (Mumbai)

Create VPC-B and Subnets:

- VPC name: **vpc-b**, CIDR: **128.0.0.0/16**.
- Public Subnet: **pubsub-b**, CIDR: **128.0.10.0/24**.
- Private Subnet: **pvtsub-b**, CIDR: **128.0.20.0/24**.

The screenshot shows the 'Create VPC' wizard in the AWS Cloud Console. In the 'VPC settings' step, the user has selected 'VPC only'. The 'Name tag - optional' field contains 'vpc-b'. The 'IPv4 CIDR block' field is set to '128.0.0.0/16'. Below it, the 'IPv6 CIDR block' section is expanded, showing options for IPv6 CIDR block type. The 'Tenancy' section is collapsed.

Name	Subnet ID	State	VPC	IPv4 CIDR
pvtsub-b	subnet-08d21b550b47e8d1e	Available	vpc-02f5b070f4884cd74 vpc-b	128.0.20.0/24
-	subnet-04ec047a3cf31fdb3	Available	vpc-0a29d42cb53d21218	172.31.16.0/20
-	subnet-0bc26b914b61f368e	Available	vpc-0a29d42cb53d21218	172.31.0.0/20
-	subnet-064298ddd1ac93cc0	Available	vpc-0a29d42cb53d21218	172.31.32.0/20
pubsub-b	subnet-03fb41ccdf92f61613	Available	vpc-02f5b070f4884cd74 vpc-b	128.0.10.0/24

Internet Gateway and Route Tables:

- Create **igw-b**, attach to **vpc-b**.
- Public route (**pubrt-b**) routes internet traffic; **pvtprt-b** routes to NAT.

Screenshot of the AWS VPC console showing the Internet gateway configuration.

Internet gateway igw-0d1d97fc6fa06b51a / igw-b

Details

Internet gateway ID igw-0d1d97fc6fa06b51a	State Attached	VPC ID vpc-02f5b070f4884cd74 vpc-b	Owner 116981766729
--	--	---	-----------------------

Tags

Key	Value
Name	igw-b

Route tables

Updated routes for rtb-0dd81b3413f711610 / pubrt-b successfully

rtb-0dd81b3413f711610 / pubrt-b

Details

Route table ID rtb-0dd81b3413f711610	Main <input checked="" type="checkbox"/> No	Explicit subnet associations subnet-03f841cc92f61613 / pubsub-b	Edge associations -
VPC vpc-02f5b070f4884cd74 vpc-b	Owner ID 116981766729		

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0d1d97fc6fa06b51a	Active	No
128.0.0.16	local	Active	No

The screenshot shows the AWS VPC Route Tables dashboard. A success message at the top states: "You have successfully updated subnet associations for rtb-05a5da54d024822e6 / pvtsub-b." The main page displays the details of a specific route table, "rtb-05a5da54d024822e6 / pvtsub-b".

Details

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-05a5da54d024822e6	No	subnet-08d21b550b47e8d1e / pvtsub-b	-
VPC	Owner ID		
vpc-02f5b070f4884cd74	116981766729		

Routes

Destination	Target	Status	Propagated
128.0.0.0/16	local	Active	No

Below the main content, there is a navigation bar with links like CloudShell, Feedback, and a search bar. The bottom of the screen shows the Windows taskbar with various pinned icons.

NAT Gateway:

- Name: **mynat-b**, use **pubsub-b** and allocate Elastic IP.

https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateNatGateway

Elastic IP address 13.202.190.89 (eipalloc-04e4f4e5f987e794e) allocated.

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

Connectivity type
Select a connectivity type for the NAT gateway.
 Public
 Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.
 [Allocate Elastic IP](#)

[► Additional settings](#) [Info](#)

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.

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 15:39 04-11-2024

https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

NAT gateway nat-04ac84d5cd1514880 | mynat-b was created successfully.

VPC dashboard [Actions](#)

NAT gateway nat-04ac84d5cd1514880 / mynat-b

Details

NAT gateway ID	Connectivity type	State	State message
nat-04ac84d5cd1514880	Public	<input checked="" type="radio"/> Pending	Info
NAT gateway ARN	Primary public IPv4 address	Primary private IPv4 address	Primary network interface ID
arn:aws:ec2:ap-south-1:116981766729:natgateway/nat-04ac84d5cd1514880	-	-	-
VPC	Subnet	Created	Deleted
vpc-02fb070f4884cd74 / vpc-b	subnet-03f841cccd92f61613 / pubsub-b	Monday, November 4, 2024 at 15:39:59 GMT+5:30	-

[Secondary IPv4 addresses](#) [Monitoring](#) [Tags](#)

Secondary IPv4 addresses

Private IPv4 address	Network interface ID	Status	Failure message
Secondary IPv4 addresses are not available for this nat gateway.			

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 15:40 04-11-2024

The screenshot shows the 'Edit routes' page for a specific route table. A single route is defined with the following details:

Destination	Target	Status	Propagated
128.0.0.0/16	local Q local	Active	No
	NAT Gateway Q nat-04ac84d5cd1514880		No

Buttons at the bottom include 'Add route', 'Cancel', 'Preview', and 'Save changes'.

Security Group (pvtsg-b):

- Inbound rules for **RDP** (from **vpc-a** private IP) and **All ICMP - IPv4**.

The screenshot shows the 'CreateSecurityGroup' page. The security group is named 'pvtsg-b' and is associated with VPC 'vpc-02f5b070f4884cd74'. The 'Inbound rules' section is empty. The 'Outbound rules' section contains two entries:

Type	Protocol	Port range	Destination	Description - optional
RDP	TCP	3389	Custom Q 118.0.20.0/24 X 118.0.20.0/24 X	
All ICMP - IPv4	ICMP	All	Anywhere Q 0.0.0.0/0 X 0.0.0.0/0 X	

Connect the Private machine from Zone-A (Ohio) to the Private machine in Zone- B (Mumbai)

Make the following configuration changes in the zone a

In the vpc-a edit the vpc settings Enable the DNS Hostnames

VPC details

VPC ID: vpc-0ef3c374ecf1661df
Name: vpc-a

DHCP settings

DHCP option set: Info
dopt-073e0a5ef331acc33

DNS settings

Enable DNS resolution Info
 Enable DNS hostnames Info

Network Address Usage metrics settings

Enable Network Address Usage metrics Info

Cancel **Save**

Goto subnets and edit actions Enable the auto assign ip addresses

Subnet

Subnet ID: subnet-0b70c1563b92a8acc
Name: pvtsub-a

Auto-assign IP settings Info

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address Info
 Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info

Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info
 Enable resource name DNS AAAA record on launch Info

Hostname type Info
 Resource name
 IP name

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 16:03 04-11-2024

Edit subnet settings [Info](#)

Subnet

Subnet ID	Name
subnet-08511ac4c3f6bc808	pubsub-a

Auto-assign IP settings [Info](#)
Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

Enable auto-assign public IPv4 address [Info](#)

Enable auto-assign customer-owned IPv4 address [Info](#)
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings [Info](#)
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch [Info](#)

Enable resource name DNS AAAA record on launch [Info](#)

Hostname type [Info](#)
 Resource name
 IP name

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 16:04 04-11-2024

Step 17: Create VPC Peering Connection

Peering from VPC-A to VPC-B:

- Name: **peer-atob**, with **vpc-a** as requester, **vpc-b** as accepter.

A VPC peering connection ppx-0544e417e06e6cf74 / peer-atob has been requested.
Remember to change your region to ap-south-1 to accept the peering connection.

ppx-0544e417e06e6cf74 / peer-atob

Details [Info](#)

Requester owner ID 116981766729	Acceptor owner ID 116981766729	VPC Peering connection ARN arn:aws:ec2:us-east-2:116981766729:vpc-peering-connection/ppx-0544e417e06e6cf74
Peering connection ID ppx-0544e417e06e6cf74	Requester VPC vpc-0ef3c374ecf1661df / vpc-a	Acceptor VPC vpc-02f5b070f4884cd74
Status Initiating Request to 116981766729	Requester CIDRs 118.0.0.0/16	Acceptor CIDRs -
Expiration time Monday, November 11, 2024 at 16:06:09 GMT+5:30	Requester Region Ohio (us-east-2)	Acceptor Region Mumbai (ap-south-1)

DNS [Route tables](#) [Tags](#) [Edit DNS settings](#)

Requester VPC ([vpc-0ef3c374ecf1661df / vpc-a](#)) [Info](#)

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 16:06 04-11-2024

Accept Request in Zone B:

- Accept the request in Mumbai region.

The screenshot shows the AWS VPC Peering Connections page. A single peering connection is listed:

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC
-	pcx-0544e417e06e6cf74	Pending acceptance	vpc-0ef3c574ecf1661df	vpc-02f5b070f4884cd74 / vpc-1

The status is "Pending acceptance". The "Actions" menu is open, showing options: View details, Accept request (which is highlighted), Reject request, Edit DNS settings, Manage tags, and Delete peering connection.

pcx-0544e417e06e6cf74

Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Monday, November 11, 2024 at 16:06:09 GMT+5:30 to accept or reject the request, otherwise it expires.

Details | DNS | Route tables | Tags

Requester owner ID: 111001234567890 Acceptor owner ID: 111001234567890 VPC Peering connection ARN: arn:aws:vpc:ap-south-1:111001234567890:peering:pcx-0544e417e06e6cf74

The screenshot shows the AWS VPC Peering Connections console. A modal dialog titled "Accept VPC peering connection request" is open, asking if you want to accept a request from "vpc-0ef5c574ecf1661df" (Requester VPC) to "vpc-02f5b070f4884cd74 / vpc-b" (Acceptor VPC). The modal displays details such as Requester CIDR (1169.81.76.0/29), Acceptor CIDR (118.0.0.0/16), Requester Region (Ohio us-east-2), Acceptor Region (Mumbai ap-south-1), Requester owner ID (116981766729 This account), and Acceptor owner ID (116981766729 This account). At the bottom, there are "Cancel" and "Accept request" buttons, with "Accept request" highlighted in orange.

Below the modal, the main VPC Peering Connections list shows one entry:

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC
-	pcx-0544e417e06e6cf74	Pending acceptance	vpc-0ef5c574ecf1661df	vpc-02f5b070f4884cd74 / vpc-b

At the top of the page, there is a message: "Your VPC peering connection (pcx-0544e417e06e6cf74) has been established. To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables." There is also a "Modify my route tables now" button.

Route Configuration:

- Update **pvtrt-a** to route **128.0.20.0/24** through the peering connection.

Destination Target Status Propagated

118.0.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway	Active	No
128.0.20.0/24	Peering Connection ppx-0544e417e06e6cf74 Use: "ppx-0544e417e06e6cf74"	Active	No

Add route Cancel Preview Save changes

- Update **pvt**rt**-b**** to route **118.0.20.0/24** through the peering connection.**

Route table ID: rtb-05a5da54d024822e6

Main: No

Owner ID: 116981766729

Explicit subnet associations: subnet-08d21b550b47e8d1e / pvtsub-b

Edge associations: -

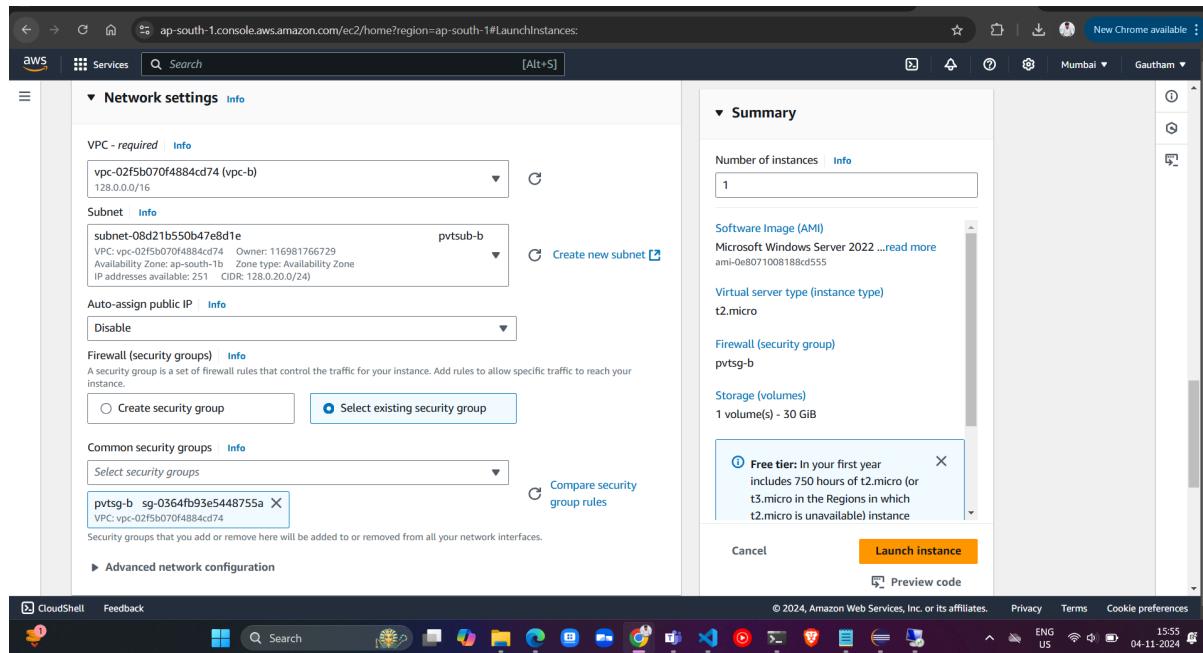
Routes (3)

Destination	Target	Status	Propagated
0.0.0.0/0	nat-04ac84d5cd1514880	Active	No
118.0.0.0/16	ppx-0544e417e06e6cf74	Active	No
128.0.0.0/16	local	Active	No

Step 18: Launch EC2 Instances in VPC-A

Private EC2 Connection:

- Connect **pvt-ec2-a** (Ohio) to **pvt-ec2-b** (Mumbai) using **Remote Desktop Connection**.
- Ensure successful connectivity by verifying the private IP address response.



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#instanceDetails:instanceId=i-0638d565a21486233

AWS Services Search [Alt+S]

EC2 Instances i-0638d565a21486233

Instance summary for i-0638d565a21486233 (pvt-ec2server-b) Info

Updated less than a minute ago

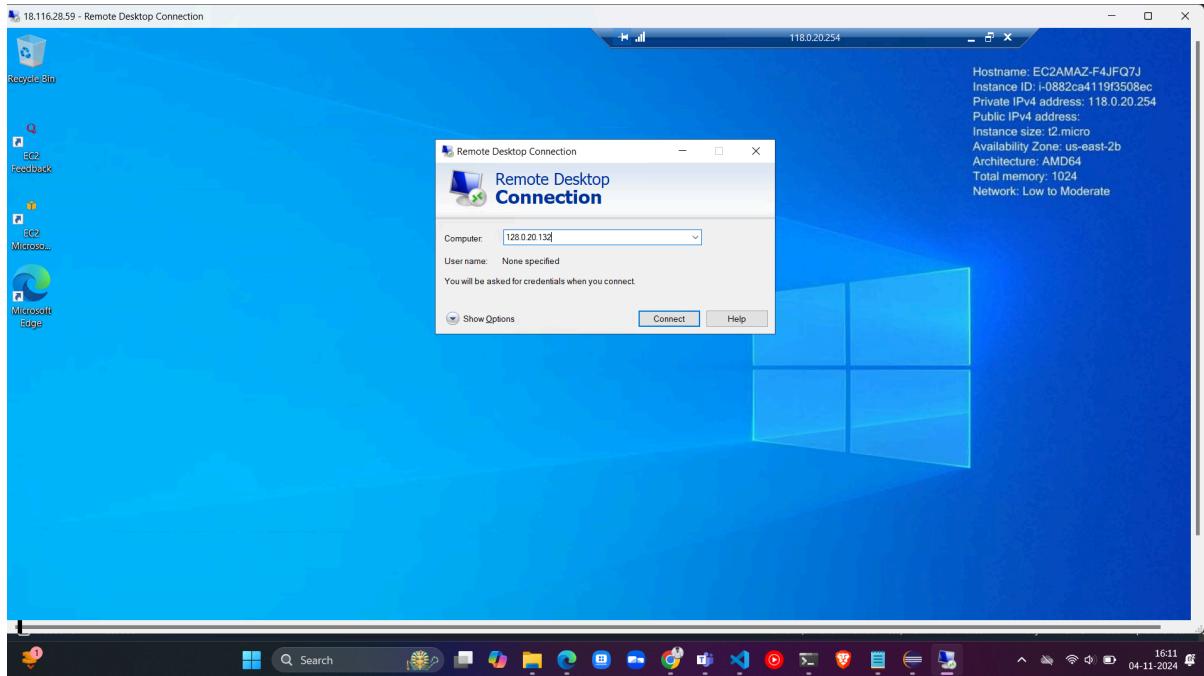
Instance ID i-0638d565a21486233	Public IPv4 address -	Private IPv4 addresses 128.0.20.9
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-128-0-20-9.ap-south-1.compute.internal	Private IP DNS name (IPv4 only) ip-128-0-20-9.ap-south-1.compute.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address -	VPC ID vpc-02f5b070f4884cd74 (vpc-b)	Learn more
IAM Role -	Subnet ID subnet-08d21b550b47e8d1e (pvtsub-b)	Auto Scaling Group name -
IMDSv2 Required	Instance ARN arn:aws:ec2:ap-south-1:116981766729:instance/i-0638d565a21486233	

Details Status and alarms Monitoring Security Networking Storage Tags

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Home

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG US 17:18 04-11-2024



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-0638d565a21486233

aws Services Search [Alt+S]

i-0638d565a21486233 (pvt-ec2server-b)

Connection Type

Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Private IP: 128.0.20.9

Username: Administrator

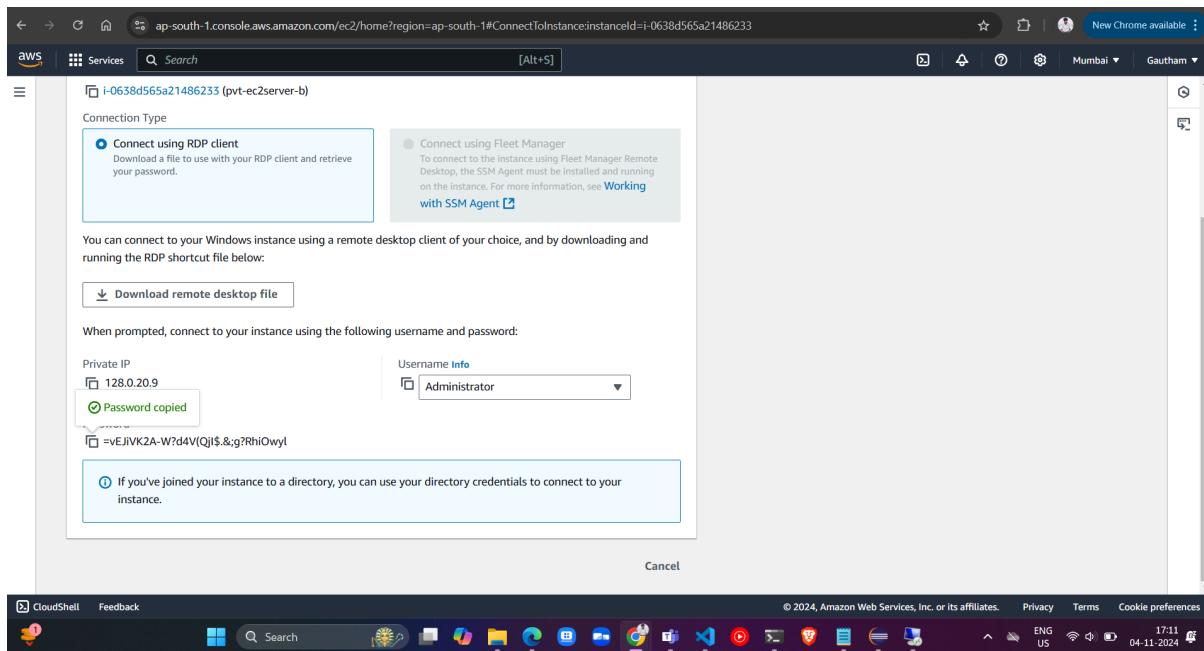
>Password copied

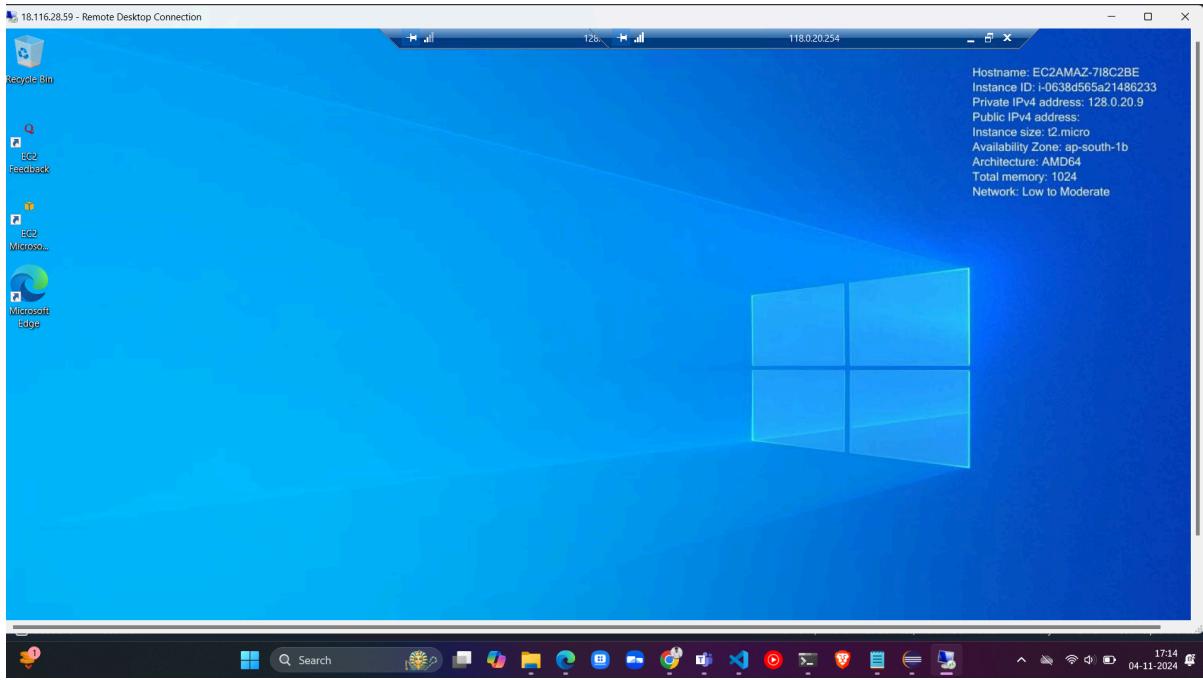
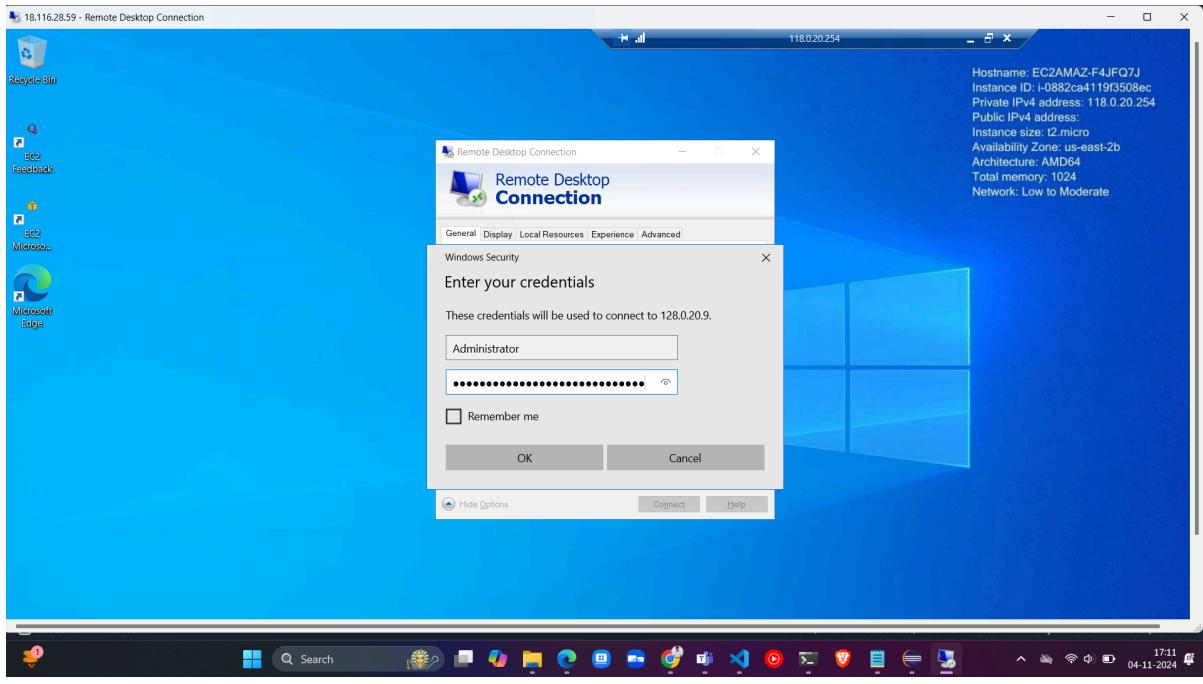
=vEJIVK2A-W?d4V(Qj\$.&g?RhiOwyl

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

Cancel

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG US 17:11 04-11-2024





Conclusion

By following this guide, users have successfully configured a secure, interconnected AWS environment with VPC peering between Ohio and Mumbai regions, enabling secure communication between private instances across regions. The multi-region setup ensures high availability and network segmentation for application workloads.