



*This is a practical assignment. (submission is mandatory)*

## AGENDA: Enabling communication between overlapping networks which will solve Private IP exhaustion with Private

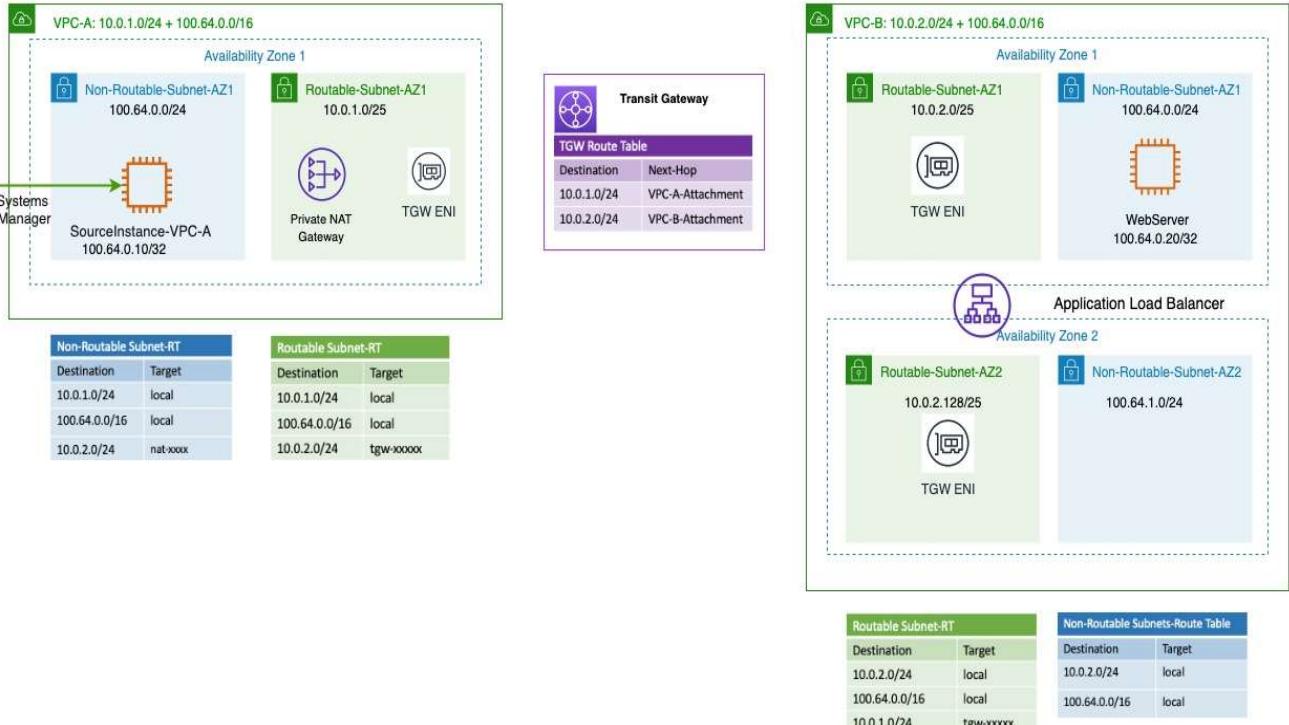
### NAT Solution.

#### Solution Overview:

This solution illustrates a mechanism to conserve and manage the RFC1918 IP address space allocation using the concept of routable & non-routable IP ranges. Furthermore, the solution describes how to connect overlapping CIDR ranges using a Private NAT Gateway that is located in the non-overlapping (or routable) IP space.

If a business unit in an organization wishes to deploy a workload that demands the use of thousands of IP addresses, the workload will be deployed on the non-routable IP address range. The non-routable IP space is used by many other business units and the overlapping nature of this space makes it non-routable. The workload will be assigned a small routable IP address range by the centralized IP Address Management (IPAM) team. The assigned routable IP range can be used by the individual business units to connect to the consolidated network. When identifying routable and non-routable IP spaces, use compatible CIDR ranges, as the CIDR blocks that can be attached as the secondary CIDR to a VPC are restricted based on the VPC's primary CIDR block.

The following diagram (Figure 1) shows how to use AWS Transit Gateway and Private NAT to solve IP exhaustion problem and enable communication between two Amazon Virtual Private Clouds (VPCs) with overlapping CIDR ranges.



## Scenario Walkthrough:

In this section, we will use routable and non-routable IP address ranges to establish connectivity from VPC-A to VPC-B with overlapping CIDRs using Private NAT Gateway. This walkthrough is divided into three sections as follows:

1. Identify the routable IP address space
2. Assign the IP address space
3. Configure the routing to enable connectivity

### 1. Identify the routable IP address space:

For non-routable address ranges, any IPv4 address range, including RFC 1918 or publicly routable IP ranges can be used as the secondary CIDR block of the VPC. Multiple teams can use the same secondary address range and thus, it should be treated as non-routable. Please keep in mind that there are some constraints when it comes to allocating IP addresses in a VPC.

The routable space is carefully allocated by the IP management team from the central routable IP pool. Only the routable IP space is unique and advertised to the organization's consolidated network through Transit Gateway or Virtual Private Gateway.



## 2. Assign the IP address space:

In this blog post, the project team provisions the VPCs with primary CIDR from the routable range and uses the non-routable CIDR range as the secondary CIDR. In this walk through, non-routable and routable IP addresses are allocated as follows:

For non-routable address range we have assigned 100.64.0.0/16 IP range from the Shared Address Space(RFC 6598: i.e., 100.64.0.0/10) as the secondary CIDR to both VPC-A and VPC-B. For routable address range, we have assigned 10.0.1.0/24 to VPC-A and 10.0.2.0/24 to VPC-B as primary address ranges from RFC1918. These CIDR ranges were selected after ensuring that they are compatible with the limitations for adding a secondary CIDR block to VPC, as described in the “Solution Overview” section.

The IP address allocation for both VPC-A and VPC-B is depicted in the following diagram (Figure 2).



## 3. Configure the routing to enable connectivity:

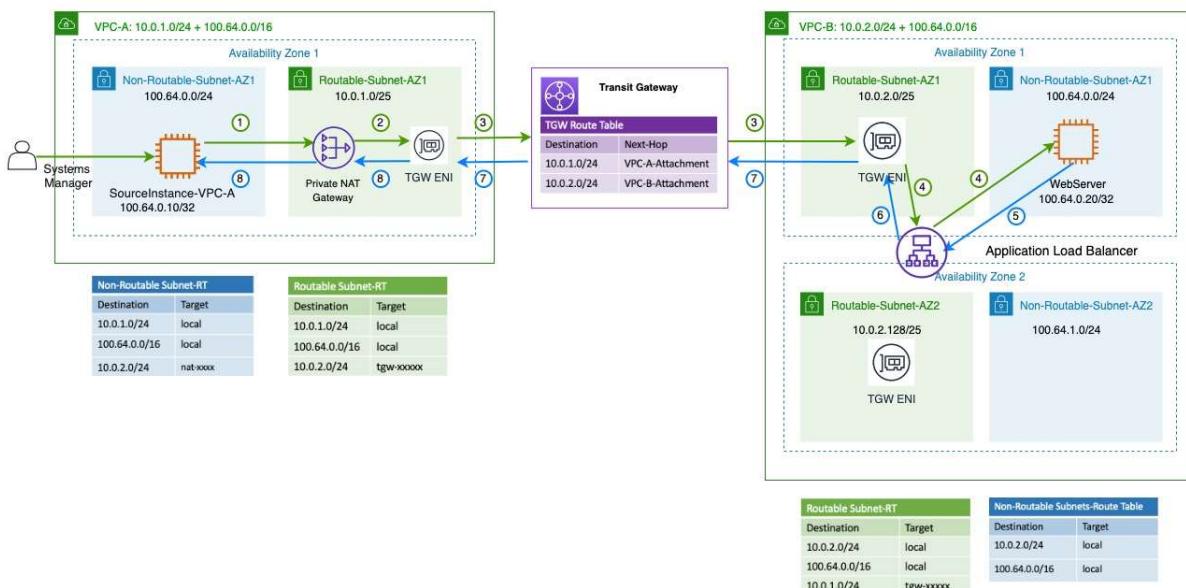
Now that we have assigned the primary and secondary IP ranges for both VPC-A and VPC-B, let's configure the routing to enable the connectivity between VPC-A and VPC-B. We are using an internal Application Load Balancer (ALB) to expose the resources in the non-routable subnet inside VPC-B. A Private NAT Gateway is deployed in VPC-A to Source NAT the non-routable IP to a routable IP in VPC-A.

To achieve this desired state of connectivity:



1. ALB is placed in the routable subnets in VPC-B and the back-end instances in the non-routable subnets in VPC-B.
2. Private NAT Gateway is created in the routable subnets in VPC-A and the “SourceInstance-VPC-A” is created in the non-routable subnets in VPC-A to test the connectivity.
3. A Transit Gateway is created with two attachments, in routable subnets of both VPC-A and VPC-B.

Now that we understand the architecture, let's walk through a life of a packet when “SourceInstance-VPC-A” in VPC-A communicates with the ALB in VPC-B.



### Packet flow from SourceInstance-VPC-A to the WebServer:

**Step 1:** “SourceInstance-VPC-A” in VPC-A wishes to communicate with the WebServer in VPC-B, which is located behind the ALB in VPC-B. As a result, the packet originates from “SourceInstance-VPC-A” (Source IP: 100.64.0.10/32) and is headed to the ALB. The “SourceInstance-VPC-A” will do a DNS lookup on the ALB DNS name to get the destination IP (Destination IP: 10.0.2.x/32). The “Non-Routable Subnet-RT” in VPC-A is configured to route the traffic destined for 10.0.2.0/24 to the Private NAT Gateway.

**Step 2:** The Private NAT Gateway translates Source IP from non-routable IP address to a routable IP address and then sends the traffic to the Transit Gateway Attachment in VPC-A as it is associated with the “Routable Subnet-RT” route table in VPC-A.

**Step 3:** Transit Gateway uses the 10.0.2.0/24 route and sends the traffic to VPC-B Transit Gateway Attachment.

**Step 4:** TGW ENI in VPC-B uses the VPC-B local route to forward the traffic to the ALB which then forwards the traffic to the WebServer behind the ALB.



## Steps to return traffic from WebServer to the SourceInstance-VPC-A:

**Step 5:** WebServer behind the ALB receives the request sent by the “SourceInstance-VPC-A” instance and returns a response to the ALB using the VPC-B local route.

**Step 6:** The ALB forwards the response traffic to the Transit Gateway Attachment in VPC-B as it is associated with the “Routable Subnet-RT” route table in VPC-B. This response traffic from the ALB has source IP address of the ALB and destination IP address of the Private NAT Gateway.

**Step 7:** Transit Gateway uses the 10.0.1.0/24 route and sends the traffic to VPC-A Transit Gateway Attachment.

**Step 8:** The TGW ENI in VPC-A uses the local route to forward the traffic to the Private NAT Gateway, which then translates the destination IP to that of the “SourceInstance-VPC-A” instance. This packet is routed to “SourceInstance-VPC-A” using the local route

## Prerequisites:

To complete this walk-through, you need:

1. An [AWS account](#)
2. An IAM user with access to AWS resources, including Systems Manager, AWS Transit Gateway, VPC and [Amazon EC2](#).

## Deployment Instructions:

In this section, we demonstrate how to deploy the architecture from figure 1, including Transit Gateway, VPCs, Subnets, Private NAT Gateway, Transit Gateway Route Tables, VPC Route Tables, Application Load Balancer, EC2 instances, etc., using the provided CloudFormation template.

**Launch Stack**

1. Click on **Launch Stack** to deploy the CloudFormation template.
2. By default, the link takes you to the Create stack page within the CloudFormation console in the N. Virginia Region (us-east-1) and the solution’s CloudFormation template is automatically populated. You can change the region at the top right corner of the console if needed.
3. If needed to deploy with the help of direct upload of code, below is the Cloud formation code which will deploy the setup.



tgw\_natgw\_overlappi  
ng\_cidrs.yaml

CloudFormation > Stacks > Create stack

Step 1 Specify template

Step 2 Specify stack details

Step 3 Configure stack options

Step 4 Review

## Create stack

### Prerequisite - Prepare template

Prepare template  
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Template is ready  Use a sample template  Create template in Designer

### Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source  
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL  Upload a template file

Upload a template file

Choose file  cron.yaml  
JSON or YAML formatted file

S3 URL: <https://s3-external-1.amazonaws.com/cf-templates-qdipjfmmpng27-us-east-1/2022157UqR-cron.yaml> [View in Designer](#)

[Cancel](#) [Next](#)

4.



Step 1  
Specify template

Step 2  
**Specify stack details**

Step 3  
Configure stack options

Step 4  
Review

### Specify stack details

**Stack name**

Stack name  
  
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**VPC A info**

pVPCACidr  
VPC A Routable CIDR:

pVPCAAAdditionalCidr  
VPC A non-routable CIDR:

**VPC B info**

pVPCBCidr  
VPC B Routable CIDR:

pVPCBAdditionalCidr  
VPC B non-routable CIDR:

**VPC A Source Instance Info**

pVPCASourceInstanceIP  
VPC A Source Instance IP:

**VPC B Web Server Info**

pVPCBWebServerIP  
VPC B Web Server IP:

**Other parameters**

LatestAmiId

Cancel

5.



CloudFormation > Stacks > Create stack

## Quick create stack

### Template

#### Template URL

[https://awsiammedia.s3.amazonaws.com/public/sample/Solve-Private-IP-exhaustion-Private-NAT/tgw\\_natgw\\_overlapping\\_cidrs.yaml](https://awsiammedia.s3.amazonaws.com/public/sample/Solve-Private-IP-exhaustion-Private-NAT/tgw_natgw_overlapping_cidrs.yaml)

#### Stack description

=

### Stack name

#### Stack name

PrivateNATGatewayDemo

Stack name can include letters {A-Z and a-z}, numbers {0-9}, and dashes {-}.

### Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

#### VPC A info

##### pVPCACidr

##### VPC A Routable CIDR

10.0.1.0/24

##### pVPCAAAdditionalCidr

##### VPC A non-routable CIDR

100.64.0.0/16

#### VPC B info

##### pVPCBCidr

##### VPC B Routable CIDR

10.0.2.0/24

##### pVPCBAAAdditionalCidr

##### VPC B non-routable CIDR

100.64.0.0/16

#### VPC A Source Instance Info

##### pVPCASourceInstanceIP

##### VPC A Source Instance IP

100.64.0.10

#### VPC B Web Server Info

##### pVPCBWebServerIP

##### VPC B Web Server IP

100.64.0.20

#### Other parameters

##### LatestAmiId

/aws/service/amazon-linux-latest/amzn2-ami-hvm-x86\_64-gp2

### Capabilities

#### The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources.

Cancel

Create change set

Create stack



1. Enter a name for the stack in the Stack name and all the required parameters are populated with default values. In our demo environment, we have chosen to name our stack "PrivateNATGatewayDemo". Click "Create Stack" to continue.

**Below are the modules created by default with EC2server,VPC setup, Elastic Load Balancer created with the help of cloud formation template as per below snippets:**

CloudFormation > Stacks > PrivateNATGatewayDemo

**PrivateNATGatewayDemo**

Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Stacks (1)	Events (1)	Resources	Outputs	Parameters	Template	Create stack
PrivateNATGatewayDemo 2022-06-06 15:09:26 UTC+0530 <span style="color: green;">CREATE_IN_PROGRESS</span>	Events (1) Search events	Logical ID	Status	Status reason		
	Timestamp					
	2022-06-06 15:09:26 UTC+0530	PrivateNATGatewayDemo	<span style="color: green;">CREATE_IN_PROGRESS</span>	User Initiated		

2.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

**Instances (2) Info**

Name	Instance ID	Instance state	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv6 DNS
WebServer-VPC-B	i-04e24d08d7428a677	Running @ Q	2/2 checks passed	No alarms	+ us-east-1a	-	-
SourceInstance-VPC-A	i-0eb9ea0f199ad54	Running @ Q	2/2 checks passed	No alarms	+ us-east-1a	-	-

3.

VPC-A	vpc-08298112666ecfc87	Available	2 CIDRs
VPC-B	vpc-0ae71c57ec4761ad1	Available	2 CIDRs

4.

**Transit gateways (1/1) Info**

Name	Transit gateway ID	Owner ID	State
TGW-OverlappingC...	tgw-04f490cfbda7aac63	171624961120	Available

5.

**NAT gateways (1/1) Info**

Name	NAT gateway ID	Connectivity	State	State message	Elastic IP address	Private IP address
-	nat-06a972a5c9b32a1a6	Private	Available	-	-	10.0.1.20

6.



	Name	Route table ID	Explicit subnet associat...	Edge associations
<input type="checkbox"/>	VPC1-Private-RT	rtb-0cf41db5ffa23b1cb	subnet-0338f1a5ca976...	-
<input type="checkbox"/>	VPC1-Public-RT	rtb-09b78f6edbd9ba2b1	subnet-0cb064d577453...	-
<input type="checkbox"/>	VPCB-Non-Routable-RouteTable	rtb-0c60cc20faa53f70f	2 subnets	-
<input type="checkbox"/>	VPC2-Private-RT	rtb-000da883f6e4d8997	subnet-0ce3b53bc7326...	-
<input type="checkbox"/>	-	rtb-0c3bbfef1566fe30d	-	-
<input type="checkbox"/>	VPC2-Public-RT	rtb-0dc852aeef43d2a65	subnet-0061e4ee90ca6f...	-
<input type="checkbox"/>	VPCA-Non-Routable-RouteTable	rtb-0e6e5355b8b57b96d	subnet-021c0d24132fc...	-
<input type="checkbox"/>	-	rtb-0771b957352806ce6	-	-
<input type="checkbox"/>	-	rtb-01454d2209fe1cb4c	subnet-0d411d274581b...	-
<input type="checkbox"/>	VPCB-Routable-RouteTable	rtb-0d86ea7c613c68671	2 subnets	-
<input type="checkbox"/>	VPCA-Routable-RouteTable	rtb-0f8ce38da5f403f6a	subnet-03fb536c11768...	-

7.

Create Load Balancer		Actions ▾					
<input type="text"/> Filter by tags and attributes or search by keyword							
	Name	DNS name	State	VPC ID			
<input checked="" type="checkbox"/>	OverlappingCIDR-ALB	internal-OverlappingCIDR-A...	Active	vpc-0ae71c57ec4761ad1			

8.

## Validation:

1. To connect to the SourceInstance-VPC-A instance securely using Session Manager, select the instance ID in the EC2 console and click on the Connect button.
2. There are four different ways to connect to the EC2 instance. Select the Session Manager tab and Click on Connect which opens a new browser-based shell session of your instance. Please keep in mind that it may take few minutes to be able to connect to the SourceInstance-VPC-A instance via the Session Manager.



aws Services ▾

EC2 > Instances > Connect to instance

**Connect to instance** [Info](#)

Connect to your instance i ,SourceInstance-VPC-A) using any of these options

EC2 Instance Connect [Session Manager](#) [SSH client](#) [EC2 Serial Console](#)

**Session Manager usage:**

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

[Cancel](#) [Connect](#)

1. To verify that the “SourceInstance-VPC-A” can reach the web service which is running in VPC-B (100.64.0.0/24 non-routable subnet), use curl to connect the ALB DNS name(Refer ALB Hostname value in the outputs section of the CloudFormation stack).

Verification:

2. Need to grab LB URL from Load Balancing Dashboard

**curl <ALB DNS>** (Here the ALB URL will be the DNS name from Load balancer Dashboard)



Screenshot of the AWS CloudFront console showing the creation of a new distribution. The 'Create Distribution' button is highlighted in blue. The distribution configuration includes a custom domain name 'internal-OverlappingCIDR-ALB-2052382187.us-east-1.elb.amazonaws.com' and a target origin 'OverlappingCIDR-ALB'. The 'SSL Certificate' dropdown shows 'AWS-managed SSL certificate' selected. The 'TLS Policy' dropdown shows 'TLS 1.3 (recommended)' selected. The 'Default Cache Behavior' section shows 'Cache based on query string' selected. The 'Custom Headers' section is empty. The 'Advanced Settings' section is collapsed.

## Cleanup:

After testing the connectivity, please go ahead and [delete](#) the CloudFormation stack to avoid any costs associated with the resources launched by the CloudFormation template.

## Conclusion:

In this post, you learned how to use routable and non-routable IP CIDR ranges along with AWS Transit Gateway and Private NAT Gateway to tackle Private IP exhaustion issue and enable communication between two Amazon VPCs with overlapping CIDR ranges. Please note that this illustration shows how to establish connectivity between two VPCs with over-lapping CIDR's. The same can be extended to a VPC and on-premises network or two on-premises networks with overlapping CIDRs.



Here are the snapshots of the activity being carried out.

The screenshot shows the AWS CloudFormation 'Quick create stack' interface. On the left, a sidebar lists 'CloudFormation' under 'Services', along with 'Stacks', 'StackSets', 'Exports', 'Designer', 'Registry' (with 'Public extensions', 'Activated extensions', and 'Publisher' listed), 'Spotlight New', and 'Feedback'. The main area is titled 'Quick create stack' and contains a 'Template' section with a 'Template URL' field set to [https://awsiammedia.s3.amazonaws.com/public/sample/Solve-Private-IP-exhaustion-Private-NAT/tgw\\_natgw\\_overlapping\\_cidrs.yaml](https://awsiammedia.s3.amazonaws.com/public/sample/Solve-Private-IP-exhaustion-Private-NAT/tgw_natgw_overlapping_cidrs.yaml) and a 'Stack description' field containing a dash. Below this is a 'Stack name' section with a 'Stack name' field containing 'PrivateNATGatewayDemo' and a note that stack names can include letters (A-Z and a-z), numbers (0-9), and dashes (-). The bottom section is titled 'Parameters' with a note that parameters are defined in the template and allow custom values. A 'VPC A info' section shows 'pVPCACidr' set to '10.0.1.0/24'. A 'VPC B info' section shows 'pVPCBCidr' set to '10.0.2.0/24'. A 'VPC A Source Instance Info' section shows 'pVPCASourceInstanceIp' set to '100.64.0.10'. The browser status bar at the bottom indicates it's from 'aws' and 'CloudFormation' services, with a timestamp of '17-02-2023'.

This screenshot shows the 'Parameters' configuration interface for the CloudFormation stack. It lists several parameters: 'pVPCACidr' (set to '10.0.1.0/24'), 'pVPCAdditionalCidr' (set to '100.64.0.0/16'), 'pVPCBCidr' (set to '10.0.2.0/24'), and 'pVPCBAdditionalCidr' (set to '100.64.0.0/16'). Below these are sections for 'VPC A Source Instance Info' with 'pVPCASourceInstanceIp' set to '100.64.0.10'. The browser status bar at the bottom indicates it's from 'aws' and 'CloudFormation' services, with a timestamp of '17-02-2023'.



Screenshot of the AWS CloudFormation console showing the creation of a new stack. The left sidebar shows navigation options like Stacks, Designer, Registry, and Spotlight. The main area displays two sections: "VPC A Source Instance Info" and "VPC B Web Server Info". Under "VPC A Source Instance Info", the "pVPCASourceInstanceIP" field is set to "100.64.0.10". Under "VPC B Web Server Info", the "pVPCBWebServerIP" field is set to "100.64.0.20" and the "LatestAmiId" field contains "/ami/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86\_64-gp2". A "Capabilities" section contains a note about IAM requirements and an acknowledgement checkbox. At the bottom right are "Create change set" and "Create stack" buttons.

Screenshot of the AWS CloudFormation console showing the status of a stack named "PrivateNATGatewayDemo". The left sidebar shows the "Stack details" section selected. The main area displays the "Events (11)" table, which lists the following events:

Timestamp	Logical ID	Status	Status reason
2023-02-17 09:25:19 UTC+0530	rVPCA	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:19 UTC+0530	rVPCB	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:17 UTC+0530	rEC2InstanceRole	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:17 UTC+0530	rVPCA	CREATE_IN_PROGRESS	-
2023-02-17 09:25:17 UTC+0530	rTGW	CREATE_IN_PROGRESS	-
2023-02-17 09:25:17 UTC+0530	rEC2InstanceRole	CREATE_IN_PROGRESS	-
2023-02-17 09:25:17 UTC+0530	rVPCB	CREATE_IN_PROGRESS	-
2023-02-17 09:25:11 UTC+0530	PrivateNATGatewayDemo	CREATE_IN_PROGRESS	User Initiated



Screenshot of the AWS CloudFormation console showing the "PrivateNATGatewayDemo" stack. The "Events" tab is selected, displaying 11 events related to the creation of resources like rVPCB, rVPCA, and rTGW.

Timestamp	Logical ID	Status	Status reason
2023-02-17 09:25:30 UTC+0530	rVPCB	CREATE_COMPLETE	-
2023-02-17 09:25:30 UTC+0530	rVPCA	CREATE_COMPLETE	-
2023-02-17 09:25:19 UTC+0530	rTGW	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:19 UTC+0530	rVPCA	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:19 UTC+0530	rVPCB	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:17			Resource creation

Screenshot of the AWS CloudFormation console showing the "PrivateNATGatewayDemo" stack. The "Events" tab is selected, displaying over 100 events related to the creation of resources like rVPCASubnet1RouteTableAssociation and rSessionManagerVPCEndp.

Timestamp	Logical ID	Status	Status reason
2023-02-17 09:25:59 UTC+0530	rVPCASubnet1RouteTableAssociation	CREATE_COMPLETE	-
2023-02-17 09:25:59 UTC+0530	rVPCBNonRoutableSubnetA22Association	CREATE_COMPLETE	-
2023-02-17 09:25:59 UTC+0530	rVPCASubnet1RouteTableAssociation	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:58 UTC+0530	rSessionManagerVPCEndp0intEC2Messages	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:58 UTC+0530	rSessionManagerVPCEndp0intSSMMessages	CREATE_IN_PROGRESS	Resource creation Initiated
2023-02-17 09:25:58	rSessionManagerVPCEndp0intVPCFnIn		Resource creation



Screenshot of the AWS CloudFormation console showing the 'PrivateNATGatewayDemo' stack. The left sidebar shows 'CloudFormation > Stacks > PrivateNATGatewayDemo'. The main area displays the stack details, including a table of events:

Timestamp	Logical ID	Status	Status reason
2023-02-17 09:28:49 UTC+0530	PrivateNATGatewayDemo	CREATE_COMPLETE	-
2023-02-17 09:28:47 UTC+0530	rALBListener	CREATE_COMPLETE	-
2023-02-17 09:28:47 UTC+0530	rALBListener	CREATE_IN_PROGRESS	Resource creation initiated
2023-02-17 09:28:45 UTC+0530	rALBListener	CREATE_IN_PROGRESS	-
2023-02-17 09:28:43 UTC+0530	rApplicationLoadBalancer	CREATE_COMPLETE	-
2023-02-17 09:28:25 UTC+0530	rAmazonLinuxInstance	CREATE_COMPLETE	-
2023-02-17 09:27:54 UTC+0530	rAmazonLinuxInstance	CREATE_IN_PROGRESS	Resource creation initiated
2023-02-17 09:27:52 UTC+0530	rAmazonLinuxInstance	CREATE_IN_PROGRESS	-
2023-02-17 09:27:50 UTC+0530	rEC2InstanceProfile	CREATE_COMPLETE	-

Screenshot of the AWS VPC dashboard. The left sidebar includes sections for Virtual private cloud, Security, Network Analysis, and DNS firewall. The main area shows 'Resources by Region' with a table:

Category	Region	Count
VPCs	US East (N. Virginia)	3
Subnets	US East (N. Virginia)	12
Route Tables	US East (N. Virginia)	7
Internet Gateways	US East (N. Virginia)	1
Egress-only Internet Gateways	US East (N. Virginia)	0
DHCP Option Sets	US East (N. Virginia)	1
Elastic IPs	US East (N. Virginia)	0
Managed Prefix Lists	US East (N. Virginia)	0
Endpoints	US East (N. Virginia)	4
Endpoint Services	US East (N. Virginia)	0
NAT Gateways	US East (N. Virginia)	1
Peering Connections	US East (N. Virginia)	0
Customer Gateways	US East (N. Virginia)	0
Virtual Private Gateways	US East (N. Virginia)	0
Site-to-Site VPN Connections	US East (N. Virginia)	2
Running Instances	US East (N. Virginia)	2



Screenshot of the AWS VPC dashboard showing three VPCs (VPC-A, VPC-B, and a new one) and their subnets.

**Your VPCs (3) Info**

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
VPC-A	vpc-0d60cd95f0de8df1	Available	2.0.0.0/16	-	dopt-052734ba635d3...	rtb-0a4cd1d554c497c7f
VPC-B	vpc-0358fe71efe90a3f3	Available	2.0.0.0/16	-	dopt-052734ba635d3...	rtb-0fb4d0176db731949
-	vpc-0c983b88ad6fa5f30	Available	172.31.0.0/16	-	dopt-052734ba635d3...	rtb-0479c965e59ec6c7a

**Subnets (12) Info**

Subnet	VPC	State	IPv4 Range	IPv6 Range	Network ACLs	Route Tables
subnet-0bd011a25fb0889d	vpc-0358fe71efe90a3f3   VPC-B	Available	100.64.0.0/24	-	-	us-east-1
subnet-0a7184283c90c7894	vpc-0c983b88ad6fa5f30	Available	172.51.32.0/20	-	-	us-east-1
subnet-091c21006405864d	vpc-0c983b88ad6fa5f30	Available	172.51.16.0/20	-	-	us-east-1
subnet-086645dd95fc6f143	vpc-0c983b88ad6fa5f30	Available	172.31.0.0/20	-	-	us-east-1
subnet-03240a17cb0210cd7	vpc-0c983b88ad6fa5f30	Available	172.31.48.0/20	-	-	us-east-1
subnet-0cc01e7294d0399db	vpc-0358fe71efe90a3f3   VPC-B	Available	10.0.2.128/25	-	-	us-east-1
subnet-0ac80cc4e33c93e7	vpc-0d60cd95f0de8df1   VP...	Available	100.64.0.0/24	-	-	us-east-1
subnet-01760a260c47ab53	vpc-0c983b88ad6fa5f30	Available	172.31.64.0/20	-	-	us-east-1
subnet-01b59279be9a8589e	vpc-0d60cd95f0de8df1   VP...	Available	10.0.1.0/25	-	-	us-east-1
subnet-03029924d745e0bf4	vpc-0358fe71efe90a3f3   VPC-B	Available	10.0.2.0/25	-	-	us-east-1
subnet-08405bd70f38c436	vpc-0c983b88ad6fa5f30	Available	172.31.80.0/20	-	-	us-east-1
subnet-07b582773bb266d4	vpc-0358fe71efe90a3f3   VPC-B	Available	100.64.1.0/24	-	-	us-east-1



Screenshot of the AWS VPC dashboard showing Route tables (7). The table lists route tables with their IDs, names, subnets, and associated VPCs.

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
VPCB-Non-Routabl...	rtb-09fb86428c26d2ea1	2 subnets	-	No	vpc-0358fe71efe90a3f5   VPC-B	846780726677
-	rtb-0479e965a59ec6c7a	-	-	Yes	vpc-0c983b88ad6fa5f30	846780726677
VPCA-Non-Routabl...	rtb-04ac0df875fce8c3	subnet-0ac80bcd4e33c...	-	No	vpc-0d60cd95f0fe8dd1   V...	846780726677
VPCB-Routable-Ro...	rtb-024d661b01900ff0	2 subnets	-	No	vpc-0358fe71efe90a3f5   VPC-B	846780726677
VPCA-Routable-Ro...	rtb-0358a45343b7036c2	subnet-01b59279be9a8...	-	No	vpc-0d60cd95f0fe8dd1   V...	846780726677
-	rtb-0a4cd1d554c497cf	-	-	Yes	vpc-0d60cd95f0fe8dd1   V...	846780726677
-	rtb-0fb4d40176db731949	-	-	Yes	vpc-0358fe71efe90a3f5   VPC-B	846780726677

Screenshot of the AWS VPC dashboard showing NAT gateways (1/1). The table lists the single NAT gateway.

Name	NAT gateway ID	Connectivit...	State	State message	Primary public I...	Primary private ...	Primary networ...	VPC
-	nat-01c6d4e9c618a8cf3	Private	Available	-	-	10.0.1.110	eni-02132259208e...	vpc-0d60cd95f0de

Details for nat-01c6d4e9c618a8cf3:

Details	Secondary IPv4 addresses	Monitoring	Tags
<b>Details</b>			
NAT gateway ID nat-01c6d4e9c618a8cf3	Connectivity type Private	State Available	State message -
NAT gateway ARN arn:aws:ec2:us-east-1:846780726677:natgateway/nat-01c6d4e9c618a8cf3	Primary public IPv4 address -	Primary private IPv4 address 10.0.1.110	Primary network interface ID eni-02132259208e0e9f
VPC vpc-0d60cd95f0fe8dd1 / VPC-A	Subnet subnet-01b59279be9a8389e / VPCA-routable-Subnet-672	Created Friday, February 17, 2023 at 09:25:41 GMT+5:30	Deleted -



NAT gateways (1/1) Info

Name	NAT gateway ID	Connectivity type	State	State message	Primary public IP address	Primary private IP address	Primary network interface ID	VPC
nat-01c6d4e9c618a8cf3	nat-01c6d4e9c618a8cf3	Private	Available	-	10.0.1.110	eni-02132259208ec09f	vpc-0d60dc95f0de	

nat-01c6d4e9c618a8cf3

Details Secondary IPv4 addresses Monitoring Tags

**Details**

NAT gateway ID nat-01c6d4e9c618a8cf3	Connectivity type Private	State Available	State message -
NAT gateway ARN arn:aws:ec2:us-east-1:846780726677:natgateway/nat-01c6d4e9c618a8cf3	Primary public IPv4 address -	Primary private IPv4 address 10.0.1.110	Primary network interface ID eni-02132259208ec09f
VPC vpc-0d60dc95f0de8fd1 / VPC-A	Subnet subnet-01b59279be9a8389e / VPCA-routable-Subnet-A71	Created Friday, February 17, 2023 at 09:25:41 GMT+5:30	Deleted -

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Feedback Language 24°C Sunny 09:30 AM 17-02-2023

Transit gateways (1) Info

Name	Transit gateway ID	Owner ID	State
TGW-OverlappingC...	tgw-05f39082d56ec0a70	846780726677	Available

Select a transit gateway

Feedback Language 24°C Sunny 09:30 AM 17-02-2023



Screenshot of the AWS EC2 Dashboard in the US East (N. Virginia) Region:

**Resources**

Instances (running)	2	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	2	Key pairs	0
Load balancers	1	Placement groups	0	Security groups	7
Snapshots	0	Volumes	2		

**Launch instance**  
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Service health**  
Region: US East (N. Virginia) Status: This service is operating normally

**Zones**

Zone name	Zone ID
us-east-1a	use1-az1
us-east-1b	use1-az2
us-east-1c	use1-az4
us-east-1d	use1-az6
us-east-1e	use1-az3

**Account attributes**

- Supported platforms: VPC
- Default VPC: vpc-0c983b88bad6fa5f30

**Explore AWS**

**10 Things You Can Do Today to Reduce AWS Costs**  
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

**Save up to 90% on EC2 with Spot Instances**  
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

**Enable Best Price-Performance with AWS Graviton2**  
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

**Additional information**

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 09:30 AM 17-02-2023

Screenshot of the AWS EC2 Instances page in the US East (N. Virginia) Region:

**Instances (2) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
SourceInstanc...	i-015b035a2c4d0627b	Running	t2.nano	2/2 checks passed	No alarms	us-east-1a	-	-	-
WebServer-VP...	i-04e4c27fda5627079	Running	t2.nano	2/2 checks passed	No alarms	us-east-1a	-	-	-

**Select an instance**

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 09:31 AM 17-02-2023



Screenshot of the AWS CloudWatch Metrics console showing the Metrics Insights page. The search bar at the top contains the query: "CloudWatch Metrics Metrics Insights". The results table shows two metrics:

Name	Description	Unit	Last Value	Period
CloudWatch Metrics Metrics Insights	CloudWatch Metrics Metrics Insights	Count	1	1 minute

Screenshot of the AWS CloudWatch Metrics console showing the Metrics Insights page. The search bar at the top contains the query: "CloudWatch Metrics Metrics Insights". The results table shows two metrics:

Name	Description	Unit	Last Value	Period
CloudWatch Metrics Metrics Insights	CloudWatch Metrics Metrics Insights	Count	1	1 minute

Screenshot of the AWS CloudWatch Metrics console showing the Metrics Insights page. The search bar at the top contains the query: "CloudWatch Metrics Metrics Insights". The results table shows two metrics:

Name	Description	Unit	Last Value	Period
CloudWatch Metrics Metrics Insights	CloudWatch Metrics Metrics Insights	Count	1	1 minute



Screenshot of the AWS CloudFormation console showing the 'Stacks' section. The page displays a list of stacks, each with a status indicator (e.g., CREATE\_IN\_PROGRESS, CREATE\_FAILED, UPDATE\_IN\_PROGRESS), stack name, ARN, creation time, and last update time. The 'Actions' column provides options like 'Edit', 'Delete', and 'View details'.

Stack ID	Name	Status	Creation Time	Last Update Time
arn:aws:cloudformation:us-east-1:123456789012:stack/MyFirstStack/12345678901234567890	MyFirstStack	CREATE_IN_PROGRESS	2023-02-17T09:25:00+00:00	2023-02-17T09:25:00+00:00
arn:aws:cloudformation:us-east-1:123456789012:stack/MySecondStack/12345678901234567890	MySecondStack	CREATE_FAILED	2023-02-17T09:25:00+00:00	2023-02-17T09:25:00+00:00

Screenshot of the AWS CloudFormation console showing the 'Stacks' section. The page displays a list of stacks, each with a status indicator (e.g., CREATE\_IN\_PROGRESS, CREATE\_FAILED, UPDATE\_IN\_PROGRESS), stack name, ARN, creation time, and last update time. The 'Actions' column provides options like 'Edit', 'Delete', and 'View details'.

Stack ID	Name	Status	Creation Time	Last Update Time
arn:aws:cloudformation:us-east-1:123456789012:stack/MyFirstStack/12345678901234567890	MyFirstStack	CREATE_IN_PROGRESS	2023-02-17T09:25:00+00:00	2023-02-17T09:25:00+00:00
arn:aws:cloudformation:us-east-1:123456789012:stack/MySecondStack/12345678901234567890	MySecondStack	CREATE_FAILED	2023-02-17T09:25:00+00:00	2023-02-17T09:25:00+00:00



A screenshot of a web browser window showing the AWS EC2 Connect interface. The URL is https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ConnectToInstance?instanceId=i-015b035a2c4d0627b. The page title is "EC2 &gt; Instances &gt; i-015b035a2c4d0627b &gt; Connect to instance". A modal dialog box is open titled "Connect to instance" with the "Info" tab selected. It contains instructions: "Connect to your instance i-015b035a2c4d0627b (SourceInstance-VPC-A) using any of these options". Below are four tabs: "EC2 Instance Connect" (selected), "Session Manager" (highlighted in blue), "SSH client", and "EC2 serial console". Under "Session Manager usage", there is a bulleted list: "Connect to your instance without SSH keys or a bastion host.", "Sessions are secured using an AWS Key Management Service key.", "You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.", and "Configure sessions on the Session Manager Preferences page." At the bottom of the modal are "Cancel" and "Connect" buttons, with "Connect" being orange.

A screenshot of a Windows desktop environment showing a terminal window. The taskbar at the top includes icons for Billing, CloudFront, EC2, VPC, Connect, AWS, Inbox, Free, Intel, AWS Inv, FutureSI, NumPy, Home, Raghur, Bengaluru, and Step by Step. The system tray shows the date and time as 09:38 AM 17-02-2023. The desktop background is dark. In the center, a terminal window is open with the following command and output:

```
Session ID: mnr-0baed5e8b7a86b2d Instance ID: i-015b035a2c4d0627b
sh-4.2$ curl -v internal-OverlappingCIDR-ALB-1253278795.us-east-1.elb.amazonaws.com
sh: syntax error near unexpected token `newline'
sh-4.2$ curl internal-OverlappingCIDR-ALB-1253278795.us-east-1.elb.amazonaws.com
Great! If you are seeing this message, you were able to reach the destination website with overlapping IP address from the SourceInstance-VPC-A
sh-4.2$
```

The terminal window has a "Terminate" button at the top right.



Screenshot of the AWS CloudFormation console showing the 'PrivateNATGatewayDemo' stack. The stack status is 'DELETE\_IN\_PROGRESS'. The Events tab shows a list of 100+ events, mostly related to the deletion of EC2 resources.

Timestamp	Logical ID	Status	Status reason
2023-02-17 09:39:38 UTC+0530	rEC2InstanceRole	DELETE_COMPLETE	-
2023-02-17 09:39:37 UTC+0530	rEC2InstanceRole	DELETE_IN_PROGRESS	-
2023-02-17 09:39:37 UTC+0530	rEC2InstanceProfile	DELETE_COMPLETE	-
2023-02-17 09:39:36 UTC+0530	rVPCBNonRoutableSubnet	DELETE_COMPLETE	-
2023-02-17 09:39:36 UTC+0530	t2z2	DELETE_COMPLETE	-
2023-02-17 09:39:36 UTC+0530	rVPCBNonRoutableRouteTable	DELETE_COMPLETE	-
2023-02-17 09:39:35 UTC+0530	rEC2InstanceProfile	DELETE_IN_PROGRESS	-
2023-02-17 09:39:34 UTC+0530	rVPCBNonRoutableRouteTable	DELETE_IN_PROGRESS	-
2023-02-17 09:39:34 UTC+0530	t2e2	DELETE_IN_PROGRESS	-
2023-02-17 09:39:34 UTC+0530	rAmazonLinuxInstance	DELETE_COMPLETE	-

Screenshot of the AWS CloudFormation console showing the 'PrivateNATGatewayDemo' stack. The stack status is 'DELETE\_IN\_PROGRESS'. The Events tab shows a list of 100+ events, mostly related to the deletion of VPC resources.

Timestamp	Logical ID	Status	Status reason
2023-02-17 09:42:30 UTC+0530	PrivateNATGatewayDemo	DELETE_COMPLETE	-
2023-02-17 09:42:29 UTC+0530	rVPC	DELETE_COMPLETE	-
2023-02-17 09:42:27 UTC+0530	rVPC	DELETE_IN_PROGRESS	-
2023-02-17 09:42:26 UTC+0530	rVPCAdditionalCidr	DELETE_COMPLETE	-
2023-02-17 09:42:11 UTC+0530	rEC2SecurityGroup	DELETE_COMPLETE	-
2023-02-17 09:42:10 UTC+0530	rVPCAdditionalCidr	DELETE_IN_PROGRESS	-
2023-02-17 09:42:09 UTC+0530	rEC2SecurityGroup	DELETE_IN_PROGRESS	-
2023-02-17 09:42:09 UTC+0530	rVPCNonRoutableSubnet	DELETE_COMPLETE	-
2023-02-17 09:42:08 UTC+0530	rSessionManagerVPCEndpointSG	DELETE_COMPLETE	-