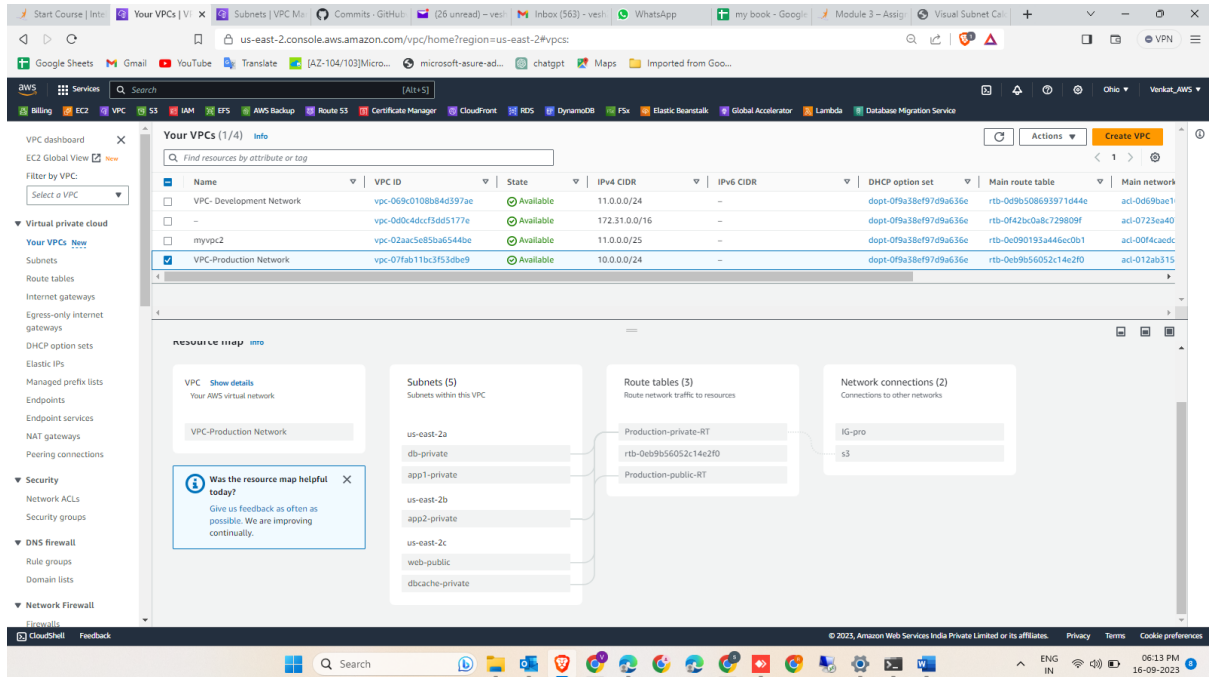


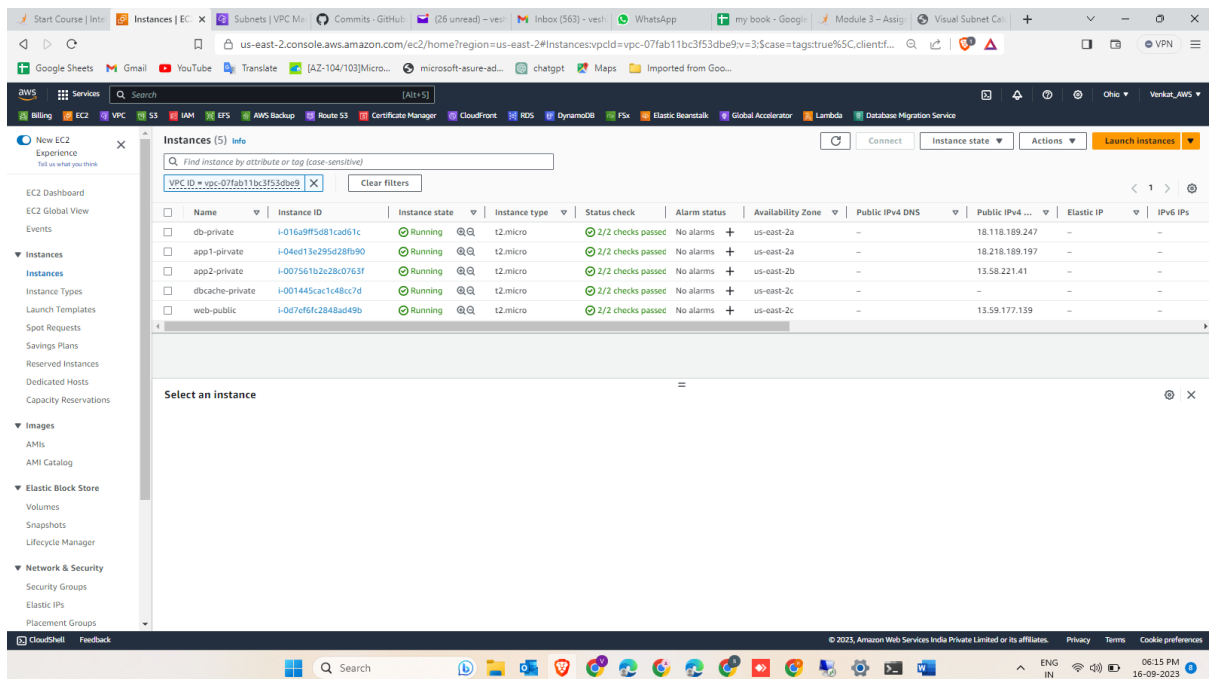
Case Study – VPC And Peering

Production Network

1. Created five subnets. Among them, four privates with names app1, app2, dbcache, and db, and the fifth one public with the name web.



2. Launched instances in all subnets, and name them as per the subnet as they are launched in.



Case Study – VPC And Peering

3. The dbcache instance can send Internet requests to app1 subnet.

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for various AWS services. The main content area displays the 'Security Groups (1/16) info' page. The 'app1-private-sg' security group is selected, and its 'Outbound rules' are shown. The rule allows traffic to the 'sg-03ba33e4947ed2049' security group on port 3306.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
sg-041e9e113d0c8c0c	sg-041e9e113d0c8c0c	launch-wizard-1	vpc-0d0c40cf3d05177e	launch-wizard-1 create...	556609594559	3 Permission entries	1 Permission entry
sg-00e4137ba66963faa	sg-00e4137ba66963faa	launch-wizard-3	vpc-02aac5e85ba6544be	launch-wizard-3 create...	556609594559	1 Permission entry	1 Permission entry
sg-03ba33e4947ed2049	sg-03ba33e4947ed2049	app1-private-sg	vpc-07fab11bc3f53dbe9	app1-private-sg	556609594559	3 Permission entries	1 Permission entry
sg-00f8dc7473dace05	sg-00f8dc7473dace05	web-public-security gr...	vpc-07fab11bc3f53dbe9	web-public-security gr...	556609594559	3 Permission entries	1 Permission entry
sg-00cfe86ed0154aa1	sg-00cfe86ed0154aa1	dbcache-private-sg	vpc-07fab11bc3f53dbe9	dbcache-private-sg	556609594559	2 Permission entries	1 Permission entry
sg-0035787df24602311	sg-0035787df24602311	default	vpc-02aac5e85ba6544be	default VPC security gr...	556609594559	1 Permission entry	1 Permission entry
sg-083d56fd96945cf3	sg-083d56fd96945cf3	fix	vpc-0d0c40cf3d05177e	launch-wizard-5 create...	556609594559	3 Permission entries	2 Permission entries

sg-03ba33e4947ed2049 - app1-private-sg

Outbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
sg-04c775278b3dc27f1	sg-04c775278b3dc27f1	--	MySQL/Aurora	TCP	3306	sg-03ba33e4947ed20...	--

4. Created a VPC Endpoint for the S3 service, and we can access the objects in any bucket from within the VPC.

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for various AWS services. The main content area displays the 'VPC Endpoint' page. The 'vpce-04e7581079a47e3c6' VPC Endpoint is selected, and its details are shown. The endpoint is for the S3 service and is in the 'Available' state.

Successfully added route tables
rtb-053bd94487e68bd63

VPC > Endpoints > vpce-04e7581079a47e3c6

vpce-04e7581079a47e3c6 / s3

Details

Endpoint ID	Status	Creation time	Endpoint type
vpce-04e7581079a47e3c6	Available	Saturday, September 16, 2023 at 17:31:55 GMT+5:30	Gateway

VPC ID
vpc-07fab11bc3f53dbe9 (VPC-Production Network)

Status message
-

Service name
com.amazonaws.us-east-2.s3

Private DNS names enabled
No

Route tables (2)

Name	Route Table ID	Main	Associated ID
Production-private-RT	rtb-0216a167c91109a2e (Production-p...	No	4 subnets
Production-public-RT	rtb-053bd94487e68bd63 (Production-...	No	subnet-07fbc3faea0aba9a8 (web-public)

Case Study – VPC And Peering

Development Network

1. Created two subnets named web and db, and launch instances in both subnets, naming them as per the subnet names.

The screenshot displays the AWS Management Console for the 'Your VPCs' section. The 'VPC-Development Network' is selected, showing its details and a resource map. The resource map illustrates the VPC connected to two subnets: 'us-east-2a' and 'us-east-2b'. The 'us-east-2a' subnet is connected to a route table 'development-RT', which is associated with a main route table 'rtb-0d9b508693971044e'. The 'us-east-2b' subnet is connected to a main route table 'rtb-0c990193a446c0b1'. The 'Network connections' section shows a connection to 'IG-dev'.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network
VPC-Development Network	vpc-069c0108b84d397ae	Available	11.0.0.0/24	-	dopt-0f9a38ef97d9a636e	rtb-0d9b508693971044e	acl-0d09bae1
-	vpc-0d0c4dcf3dd5177e	Available	172.31.0.0/16	-	dopt-0f9a38ef97d9a636e	rtb-0f42bc0a8c729809f	acl-0723ea40
myvpc2	vpc-02aac5e85ba6544be	Available	11.0.0.0/25	-	dopt-0f9a38ef97d9a636e	rtb-0c990193a446c0b1	acl-00f4ca0c
VPC-Production Network	vpc-07fab11bc3f53b0e9	Available	10.0.0.0/24	-	dopt-0f9a38ef97d9a636e	rtb-0eb9b56052c14e2f0	acl-012ab315

The screenshot displays the AWS Management Console for the 'Instances' section. The 'Instances' page shows a list of instances, including 'dev-web-1a-tier' and 'dev-db-tier', both in a 'Running' state. The 'dev-web-1a-tier' instance is associated with the 'us-east-2a' availability zone, and the 'dev-db-tier' instance is associated with the 'us-east-2b' availability zone. The 'Instances' page also shows a 'Select an instance' dialog box.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
dev-web-1a-tier	i-09cc3a6b21c61c06	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	-	-	-	-
dev-db-tier	i-08c32391aba1610ed	Running	t2.micro	2/2 checks passed	No alarms	us-east-2b	-	3.138.153.246	-	-

Case Study – VPC And Peering

- Only web subnet can send Internet requests. Db subnet cannot sent the internet requests, because I removed outbound rule.

The screenshot shows the AWS Management Console interface for a VPC. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC resources. The main content area displays the 'Security Groups (1/16)' page. A table lists several security groups, with 'sg-01dbb6f4d35eabd45 - dev-web-1a-sg' selected. Below the table, the 'Outbound rules' section for this group is shown, containing a single rule 'sg-057e519c023ae059' that allows all traffic to 0.0.0.0/0.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
-	sg-028b7977f1219a88	default	vpc-069c0108b84d397ae	default VPC security gr...	556609594559	1 Permission entry	1 Permission entry
-	sg-06912b74421eb61ca	app2-private-sg	vpc-07fab11bc3f53dbe9	app2-private-sg	556609594559	3 Permission entries	1 Permission entry
✓	sg-01dbb6f4d35eabd45	dev-web-1a-sg	vpc-069c0108b84d397ae	dev-web-1a-sg	556609594559	3 Permission entries	1 Permission entry
-	sg-0901b5744a617acb	default	vpc-07fab11bc3f53dbe9	default VPC security gr...	556609594559	1 Permission entry	1 Permission entry
-	sg-041e9ef13daceacd	launch-wizard-1	vpc-0d0c4dcf3dd5177e	launch-wizard-1 create...	556609594559	3 Permission entries	1 Permission entry
-	sg-00e4137ba66963faa	launch-wizard-3	vpc-02aac5e8bba6544be	launch-wizard-3 create...	556609594559	1 Permission entry	1 Permission entry

sg-01dbb6f4d35eabd45 - dev-web-1a-sg

Outbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
✓	sg-057e519c023ae059	IPv4	All traffic	All	All	0.0.0.0/0	-

The screenshot shows the AWS Management Console interface for a VPC. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC resources. The main content area displays the 'Security Groups (1/16)' page. A table lists several security groups, with 'sg-004c3c1a5d5ad6165 - dev-db-tier-1b-sg' selected. Below the table, the 'Outbound rules' section for this group is shown, containing a single rule 'sg-0b0c2e14f286feb1e' that allows all traffic to 0.0.0.0/0.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
-	sg-0035787df24602311	default	vpc-02aac5e8bba6544be	default VPC security gr...	556609594559	1 Permission entry	1 Permission entry
-	sg-083d56f0c96945cf3	Fix	vpc-0d0c4dcf3dd5177e	launch-wizard-5 create...	556609594559	3 Permission entries	2 Permission entries
✓	sg-004c3c1a5d5ad6165	dev-db-tier-1b-sg	vpc-069c0108b84d397ae	dev-db-tier-1b-sg	556609594559	2 Permission entries	0 Permission entries
-	sg-0b0c2e14f286feb1e	default	vpc-0d0c4dcf3dd5177e	default VPC security gr...	556609594559	2 Permission entries	1 Permission entry
-	sg-0eabfc3006303d7d4	launch-wizard-2	vpc-02aac5e8bba6544be	launch-wizard-2 create...	556609594559	2 Permission entries	1 Permission entry
-	sg-03236a0df6750c4fd	launch-wizard-4	vpc-0d0c4dcf3dd5177e	launch-wizard-4 create...	556609594559	1 Permission entry	1 Permission entry

sg-004c3c1a5d5ad6165 - dev-db-tier-1b-sg

Outbound rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
-	sg-0b0c2e14f286feb1e	IPv4	All traffic	All	All	0.0.0.0/0	-

Case Study – VPC And Peering

3. Created a peering connection between the production network and the development network.

The screenshot shows the AWS VPC console interface. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC resources. The main content area displays the 'Peering connections (1/2)' page. A table lists the peering connections, with one connection highlighted. Below the table, the 'Route tables' section for the selected peering connection is shown, listing route tables associated with the VPCs.

Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDR	Accepter CIDRs	Requester owner ID	Accepter owner ID
DEV-PRo	pcx-09b095808514dc947	Active	vpc-07fab11bc3f53dbe9 / VPC-Production Network	vpc-069c0108b84c397ae / VPC-Development Network	10.0.0.0/24	11.0.0.0/24	556609594559	556609594559

Route table ID	VPC ID	Main	Associated with
rtb-0216a167c91109a2e / Production-private-RT	vpc-07fab11bc3f53dbe9 / VPC-Production Network	No	4 subnets
rtb-0a055818653634958 / development-RT	vpc-069c0108b84c397ae / VPC-Development Network	No	2 subnets

4. Created a connection between the db subnets of both the production network and the development network.

The screenshot shows the AWS VPC console interface, specifically the 'Route tables (1/7)' page. A table lists the route tables for the VPCs. Below the table, the 'Routes (3)' section is shown, displaying the routes configured for the peering connection.

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
Production-private-RT	rtb-0216a167c91109a2e	4 subnets	-	No	vpc-07fab11bc3f53dbe9 / VPC-Production Network	556609594559
development-RT	rtb-0a055818653634958	2 subnets	-	No	vpc-069c0108b84c397ae / VPC-Development Network	556609594559
-	rtb-0d9b0508693971644e	-	-	Yes	vpc-069c0108b84c397ae / VPC-Development Network	556609594559
-	rtb-0f42bcb08c729809f	-	-	Yes	vpc-0d0c4dcd3d5177e / VPC-Development Network	556609594559
MYRT	rtb-0e090193446ec0b1	-	-	Yes	vpc-02aac5e85ba6544be / myv...	556609594559
-	rtb-0eb9656052c14e2f0	-	-	Yes	vpc-07fab11bc3f53dbe9 / VPC-Production Network	556609594559
Production-public-RT	rtb-053bd94487e68bd63	subnet-07b3fae0aba9...	-	No	vpc-07fab11bc3f53dbe9 / VPC-Production Network	556609594559

Destination	Target	Status	Propagated
pl-7ba54012	vpce-04c7581079a47e3c6	Active	No
0.0.0.0/0	pcx-09b095808514dc947	Active	No
10.0.0.0/24	local	Active	No

Case Study – VPC And Peering

The screenshot displays the AWS Management Console interface for the 'Route tables' section. The left sidebar shows the navigation menu with categories like Virtual private cloud, Security, DNS firewall, and Network Firewall. The main content area shows a list of route tables, with 'development-RT' selected. Below the list, the 'Routes' tab is active, showing two routes: '0.0.0.0/0' pointing to 'pcx-09b095808514dc947' and '11.0.0.0/24' pointing to 'local'. The bottom of the screen shows the Windows taskbar with various application icons and the system clock.

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
Production-private-RT	rtb-0216a167c91109a2e	4 subnets	-	No	vpc-07fab11bc3f53dbe9 VPC...	556609594559
development-RT	rtb-0a055818653634958	2 subnets	-	No	vpc-069c0108b84c397ae VPC...	556609594559
-	rtb-0d9b508693971d44e	-	-	Yes	vpc-069c0108b84c397ae VPC...	556609594559
-	rtb-0f42bc0a8c729809f	-	-	Yes	vpc-0d0c4dcf3d5177e	556609594559
MYRT	rtb-0e0901933446ec0b1	-	-	Yes	vpc-02aac5e85ba6544de myv...	556609594559
-	rtb-0eb9b56052c14e2f0	-	-	Yes	vpc-07fab11bc3f53dbe9 VPC...	556609594559
Production-public-RT	rtb-053bd94487e68bd63	subnet-07fbc3faa0aba9...	-	No	vpc-07fab11bc3f53dbe9 VPC...	556609594559

Destination	Target	Status	Propagated
0.0.0.0/0	pcx-09b095808514dc947	Active	No
11.0.0.0/24	local	Active	No