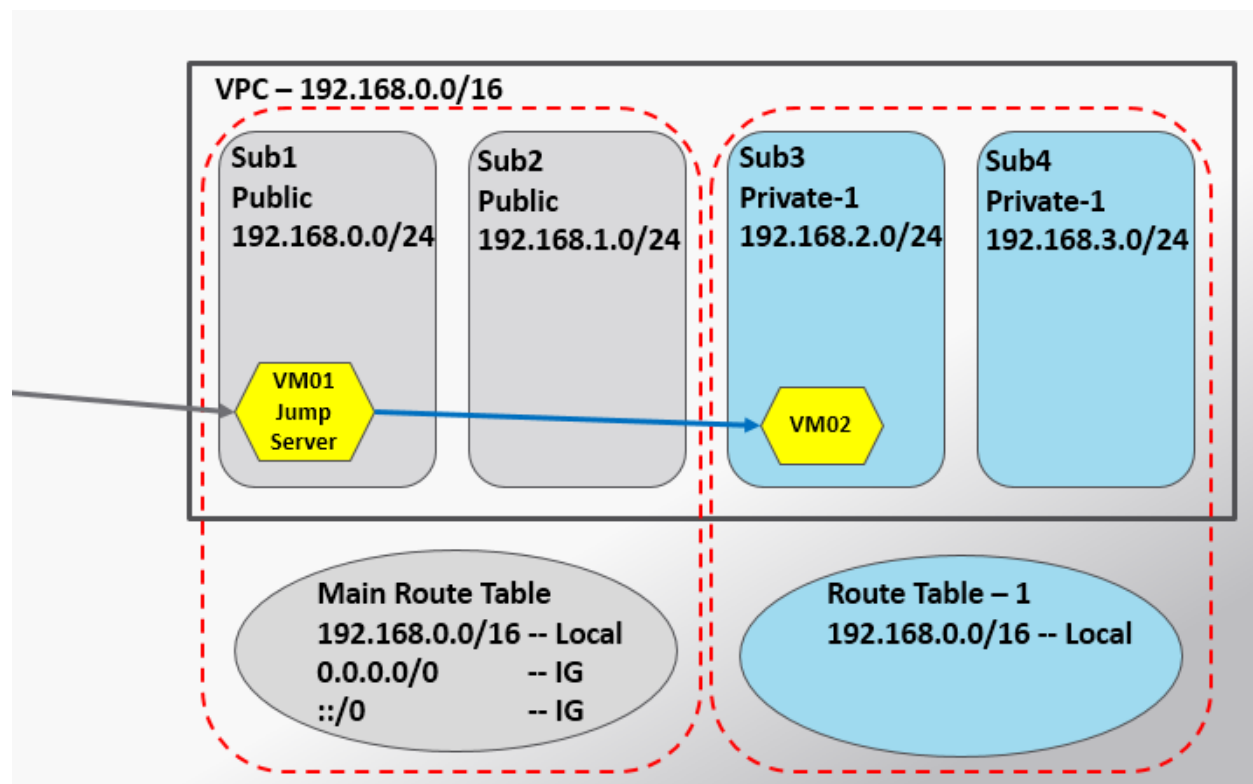


Route Table Scenario

Objective:

Login to EC2 VM02 in the Private Subnet from the VM01 that is in the public Subnet.

Diagram:



Steps:

1. Create a VPC and 4 Subnets with Default Gateway on the MAIN Route Table.

| | | | | | | |
|-------------------------------------|------------|--------------------------|-----------|-------------------------------|----------------|-----|
| <input type="checkbox"/> | Sub1-VPC-1 | subnet-0d947f797b23007db | available | vpc-08449eee4519750b1 VPC-1 | 192.168.1.0/24 | 251 |
| <input checked="" type="checkbox"/> | Sub2-VPC-1 | subnet-04d509f0eb4eda1ab | available | vpc-08449eee4519750b1 VPC-1 | 192.168.2.0/24 | 250 |
| <input type="checkbox"/> | Sub3-VPC-1 | subnet-00bd78c2b31b04589 | available | vpc-08449eee4519750b1 VPC-1 | 192.168.3.0/24 | 251 |
| <input type="checkbox"/> | Sub4-VPC-1 | subnet-0d3bcb4311578ce2e | available | vpc-08449eee4519750b1 VPC-1 | 192.168.4.0/24 | 251 |

Output of Route Table

Filter by tags and attributes or search by keyword

| Name | Route Table ID | Explicitly Associated with | Main | VPC ID | Owner |
|------|-----------------------|----------------------------|------|--------------------------------|-------------|
| RT01 | rtb-01a08dbe480393af1 | - | Yes | vpc-08ed4f70 | 55845764464 |
| | rtb-0c13432e2d4a0a3eb | - | Yes | vpc-08449eee4519750b1 VPC-1 | 55845764464 |
| | rtb-0efd434257370b1e7 | - | Yes | vpc-00ded5fec721b7fb5 vpc-01 | 55845764464 |

Summary Routes Subnet Associations Route Propagation Tags

Edit subnet associations

None found

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--|-----------|-----------|
| You do not have any subnet associations. | | |

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table.

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---------------------------|----------------|-------------------------|
| subnet-0d3bcb4311578ce... | 192.168.4.0/24 | 2600:1f14:b5a:7e05::/64 |

2. Assign Sub3 and Sub4 to the new Route Table for the same VPC

The screenshot shows the AWS Management Console interface for a Route Table. The top section displays a list of Route Tables. The second row, **RT-01-VPC-1**, is selected and highlighted with a black oval. Below this, the **Route Table: rtb-03794fcd6360615c3** details are shown. The **Subnet Associations** tab is active, displaying a table of associated subnets, which is also circled with a black oval.

| Name | Route Table ID | Explicitly Associated with | Main | VPC ID | Owner |
|--------------------|------------------------------|----------------------------|------|--------------------------------|--------------|
| RT01 | rtb-01a08dbe480393af1 | - | Yes | vpc-08ed4f70 | 558457644648 |
| RT-01-VPC-1 | rtb-03794fcd6360615c3 | 2 subnets | No | vpc-08449eee4519750b1 VPC-1 | 558457644648 |
| | rtb-0c13432e2d4a0a3eb | - | Yes | vpc-08449eee4519750b1 VPC-1 | 558457644648 |
| | rtb-0efd434257370b1e7 | - | Yes | vpc-00ded5fec721b7fb5 vpc-01 | 558457644648 |

Route Table: rtb-03794fcd6360615c3

Summary Routes **Subnet Associations** Route Propagation Tags

Edit subnet associations

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---------------------------------------|----------------|-------------------------|
| subnet-0d3bcb4311578ce2e Sub4-VPC-1 | 192.168.4.0/24 | 2600:1f14:b5a:7e05::/64 |
| subnet-00bd78c2b31b04589 Sub3-VPC-1 | 192.168.3.0/24 | 2600:1f14:b5a:7e03::/64 |

Also there is no Route to the Internet in the new Route Table.

The screenshot shows the AWS Management Console interface for the same Route Table, **RT-01-VPC-1**. The **Routes** tab is active, displaying a table of routes. The table shows two local routes for the subnets 192.168.0.0/16 and 2600:1f14:b5a:7e00::/56, both with a status of 'active' and 'No' propagation.

| Destination | Target | Status | Propagated |
|-------------------------|--------|--------|------------|
| 192.168.0.0/16 | local | active | No |
| 2600:1f14:b5a:7e00::/56 | local | active | No |

3. Create 2 instances

Both the instance needs to be Linux.

First Instance in Subnet1 and **Second Instance in Subnet3.**

Make sure Public IPv4 and public IPv6 is “ENABLED” on First Instance.

The screenshot shows the AWS Management Console for instance VM01. The instance is in the 'us-west-2a' availability zone, running on a 't2.micro' instance type. The status is 'running'. The public IP address is 34.216.129.76. The instance is associated with the 'us-west-2a' availability zone, the 'SSH-' security group, and the 'amzn2-ami-hvm-2.0.20190508-x86_64-gp2' AMI. The VPC ID is 'vpc-08449eee4519750b1 (VPC-1)' and the Subnet ID is 'subnet-0d947f79b23007db (Sub1-VPC-1)'. The instance has a public IPv4 address of 34.216.129.76 and a private IPv4 address of 192.168.1.242.

| Instance ID | Instance state | Instance type | Elastic IPs | Availability zone | Security groups | Scheduled events | AMI ID | Public DNS (IPv4) | IPv4 Public IP | IPv6 IPs | Private DNS | Private IPs | Secondary private IPs | VPC ID | Subnet ID |
|---------------------|----------------|---------------|-------------|-------------------|---|---------------------|---|-------------------|----------------|--|---|---------------|-----------------------|-------------------------------|--------------------------------------|
| i-0279ba7f51e93fc7a | running | t2.micro | | us-west-2a | SSH- view inbound rules view outbound rules | No scheduled events | amzn2-ami-hvm-2.0.20190508-x86_64-gp2 (ami-0cb72367e98845d43) | - | 34.216.129.76 | 2600:1f14:b5a:7e00:1d8d:7598:53f7:c5bf | ip-192-168-1-242.us-west-2.compute.internal | 192.168.1.242 | | vpc-08449eee4519750b1 (VPC-1) | subnet-0d947f79b23007db (Sub1-VPC-1) |

And on the Second Instance it should “DISABLED”.

The screenshot shows the AWS Management Console for instance i-048ca60c9031f2dea. The instance is in the 'us-west-2a' availability zone, pending on a 't2.micro' instance type. The status is 'pending'. The private IP address is 192.168.3.71. The instance is associated with the 'us-west-2a' availability zone, the 'SSH-' security group, and the 'amzn2-ami-hvm-2.0.20190508-x86_64-gp2' AMI. The VPC ID is 'vpc-08449eee4519750b1 (VPC-1)' and the Subnet ID is 'subnet-00bd78c2b31b04589 (Sub3-VPC-1)'. The instance has a private IPv4 address of 192.168.3.71 and a network interface of 'eth0'.

| Instance ID | Instance state | Instance type | Elastic IPs | Availability zone | Security groups | Scheduled events | AMI ID | Platform | IAM role | Public DNS (IPv4) | IPv4 Public IP | IPv6 IPs | Private DNS | Private IPs | Secondary private IPs | VPC ID | Subnet ID | Network interfaces | SourceDest check |
|---------------------|----------------|---------------|-------------|-------------------|---|------------------|---|----------|----------|-------------------|----------------|----------|--|--------------|-----------------------|-------------------------------|---------------------------------------|--------------------|------------------|
| i-048ca60c9031f2dea | pending | t2.micro | | us-west-2a | SSH- view inbound rules view outbound rules | - | amzn2-ami-hvm-2.0.20190508-x86_64-gp2 (ami-0cb72367e98845d43) | - | - | - | - | - | ip-192-168-3-71.us-west-2.compute.internal | 192.168.3.71 | | vpc-08449eee4519750b1 (VPC-1) | subnet-00bd78c2b31b04589 (Sub3-VPC-1) | eth0 | True |

4. To login to both the Machines.

Note:-- We cannot login to VM02 from the internet, as it has only private IP and also the Route Table does not have the internet route.

So , first we would login to the VM01.

```
type help to learn how to use Ashell prompt.  
[C:\~]$ ssh 34.216.129.76  
  
Connecting to 34.216.129.76:22...  
Connection established.  
To escape to local shell, press 'Ctrl+Alt+J'.  
  
WARNING! The remote SSH server rejected X11 forwarding request.  
  
  _ | _ | _ )  
  _ | ( _ | /  Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-192-168-1-242 ~]$ ping 192.168.3.71
```

Then, Ping the VM02 (if the ICMP is allow in the SG on both the VM's).

Command to be executed “Ping <VM02 private ip> -c 4”

```
[ec2-user@ip-192-168-1-242 ~]$ ping 192.168.3.71  
PING 192.168.3.71 (192.168.3.71) 56(84) bytes of data:  
64 bytes from 192.168.3.71: icmp_seq=1 ttl=255 time=0.423 ms  
^C  
--- 192.168.3.71 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.423/0.423/0.423/0.000 ms
```

5. Login to VM02 from VM01.

We need the private key of the VM02 on the VM01 to login successfully.

I. \$ sudo su

```
[ec2-user@ip-192-168-1-242 ~]$ sudo su  
[root@ip-192-168-1-242 ec2-user]#
```

II. Create the key1.pem file

\$ vi key1.pem

In the blank window , press “I” to go into insert mode in editing the file in linux.

**Copy the content of the .pem file from the desktop
And “right clic” and “paste” it here on the blank screen.**

Note: -- Make sure the pem file starts with “----” and ends with “-----”.

Then press “esc”

Then “:wq”

This would save the file and quit the editing window.

Run the command \$ cat key1.pem

To see the output as below screen.

```
[root@ip-192-168-1-242 ec2-user]# vi key1.pem

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAzKZ9UECwB3yfgZxL48KBG7IztnLDxh6dddtbj8PbTpFTMMbPuUC3prxGKnJ
P9+DgKRhTdaBJh/TxsSyQRvhyLf21ZLRaoxWCARTF8n8rp3T03FZudDmFXjFYfJn0xHYRiKYGOJp
IzzaXtr3gdH0JGwHJF4yY3Clm3QK+Cl093vZoTyyTHandmyM8TAIsW3AwSLqUhr3dLroZsFm020/
YhyddeJ0SV9sEMK9QjAG3ZIVGeYnTRfnJj9Ik8MJPM7DLzuXAip1bJjsQQtqTLCxkbRloTrmrkng
PLj5oN33L2zz8nC6HADg7LM7fBqfIStVH+8/tXNpL3gJgcRGXNXiQwIDAQABAoIBAA3q8LDJhW8s
6YgeA8vmiXNBvkSVL31Ezb6a5QVPYpQyGRMWXb78QikZdNwRh+9BGydfhoKNqQDXv0ZQUdMfW06U
PEQwF0/jFWLY7Dw872NMtoA1wD1j2JHzQbE0LB0FpKi4Z5GhrDbKR6uVxqlchGFzu1Sc115t5cVZ
sflIKHzYH0TpqS2fxSLtN82BFhTvtSYNh021GYz+G8MYj5rMzTYT5bILMw0qIyow8AkEqtah0a
+WGwUwQNHfvc0TjEFUJDrc5aPqs9i3vFNCQ1R6Wmh5qGfS17bTbSATgHK0qcCMp2g1QpWEi9tpmD
CVUY8HBjiXsWh1nHKTHfnyDPL1ECgYEA6GbXsevBn60gts45PXFLiULdBL6mXeA5scyI5Vh4SFdA
/igbQy6Ymxxx4tuAsna1NgmS94aQKMcIiZ9McdKAUPIFn+VRS+DKYtmH6jgP02LY2YEKtEedwNyB
Zxkj5z0Cw9SNCHRE7YV7ocrJQLiGEz9pIaVdPc3NL0dTtIi++0kCgYEA4W5DzBfSPnvlqorgL/oS
N7gZmkc8ZyFEuu+vCrBwj6eJp5cL9yfI9GaP2PjqtT+LJqEaVptJReXRJ0LXqx5VEtJYAy0kr6D
FFQAUds1GQkLPByfLw00u1zQ0G0EzJ90c4ULIKTKo4f08/jKkkRxtHJNYF4WJ05Nr507kePPRSsC
gYEA5nrP4UjhHp2R0xqsU84fToJ8NS9qS0GN9LHVvJZ2G7BE6YoW93qnpya3L3fnW5Yk5MF7+nV+
VjiKUHAmXR+ZWC2d/GRtSqYlsQDxNQziTRVGI3dBiWcZAWLuBrQ9EhbY0aPjNoYwsarW4K7/Bmu5
tC8H8XFRVnDa0XSdZAbV+NkCgYAKNrJtduYvY3fhja22B1Yl3U0/m3H4nz+LSDW2YeGzMhbK9VjW
u21s1Y0GLOVUTCMix0m+Iu1lRMSAIT5/lvVmtTF0XJYlFLVR7qyu69Fp1CoZ3f80bj3fm2lwEIyk
0nKn3Bu6wr5Kxuxyx0TF2njpo/MKKBmMm6GfNl9TLtfQ0KBgC7cCwDXQ08nyRbDRfA2Nv+GfyH
oay6w7W69YuGZ//d/hIk5S0YDPVjvgouTVz1+c+V+TL0LIPyLWfAdkdZafYQBjCZtXg29IUb+VDC
72GYNfIc1F0Czz2Wc3NLBrQBWT5qJGAYnN5MgeorWltUKHcIMEhhMvkuLDva0Hb+uEsD
-----END RSA PRIVATE KEY-----
```

The key should be copied from the VM02 Private Key .pem.

III. We need to change the permission of the key file (that's the requirement of Linux Machines).

\$ chmod 600 key1.pem

```
[root@ip-192-168-1-242 ec2-user]# ls -l
total 4
-rw-r--r-- 1 root root 1671 May 20 13:31 key1.pem
[root@ip-192-168-1-242 ec2-user]# chmod 600 key1.pem
[root@ip-192-168-1-242 ec2-user]# ls -l
total 4
-rw----- 1 root root 1671 May 20 13:31 key1.pem
[root@ip-192-168-1-242 ec2-user]#
```

Now login to the VM01 with SSH command

```
[root@ip-192-168-1-242 ~]# ssh -i key1.pem ec2-user@192.168.3.71
The authenticity of host '192.168.3.71 (192.168.3.71)' can't be established.
ECDSA key fingerprint is SHA256:vnXHzGxdG9hnXKPt81TG7PFi3oGidCmI5yaGeoErRUU.
ECDSA key fingerprint is MD5:87:b4:f7:34:91:c3:d2:3d:8a:ef:b0:0e:dd:71:14:58.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.71' (ECDSA) to the list of known hosts.

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-192-168-3-71 ~]$
```

VM01 - Private IP

VM02 - Private IP

\$ ssh -i key1.pem ec2-user@<private ip of the vm02>

Now we have logged in to the VM02 from VM01.