IPv6 support in a single-tenant setup within AWS provides enhanced capabilities for addressing and network management. Here's how it works:

Distinct IPv6 Subnets:

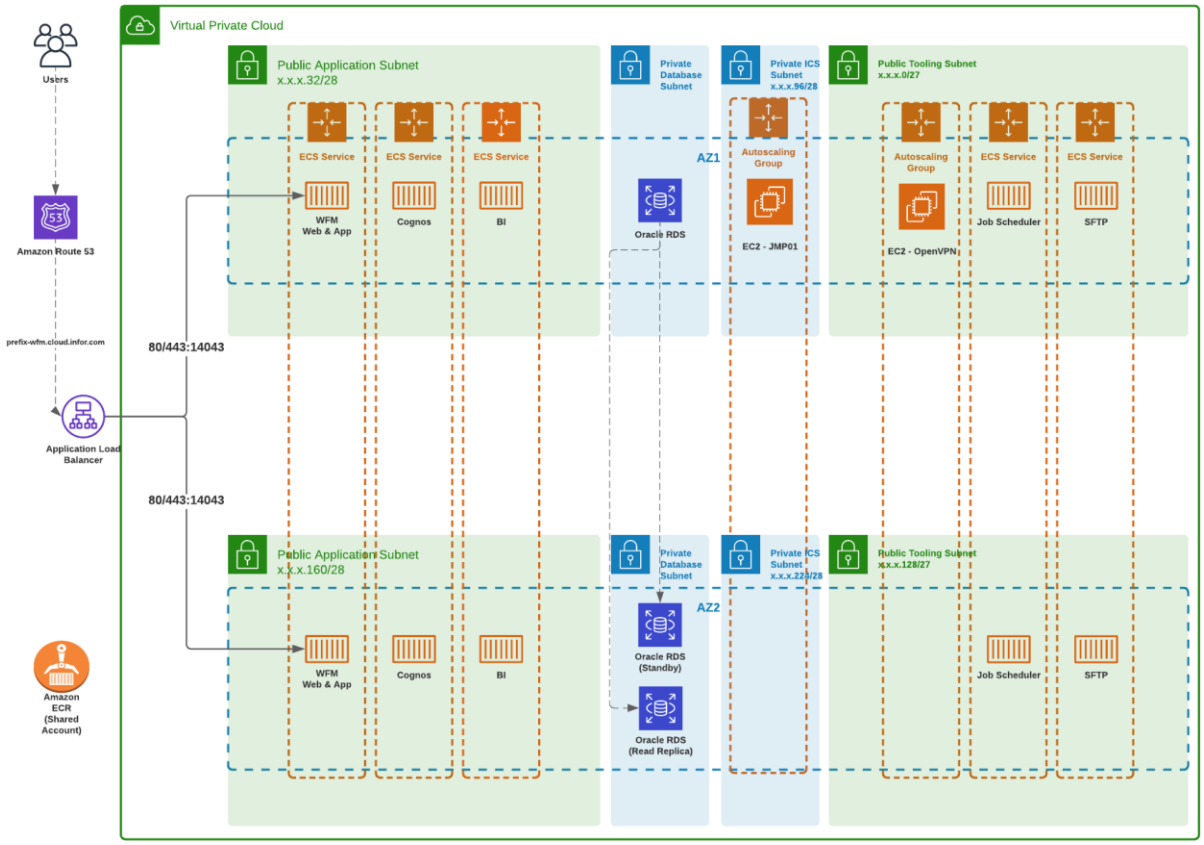
In a single-tenant setup, you can assign distinct IPv6 subnets to each component, whether it's a tenant or a Virtual Private Cloud (VPC). This ensures that each entity has its own separate IPv6 address space, promoting isolation and preventing interference between tenants. This is crucial for security and network segmentation.

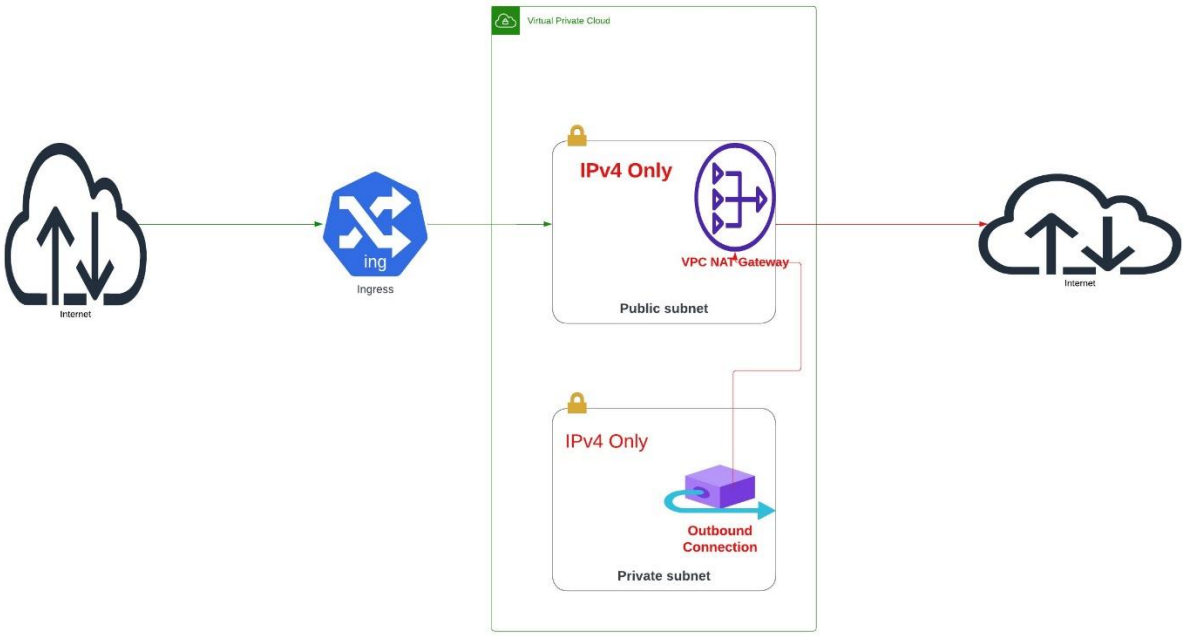
Native IPv6 Support in AWS Services:

AWS offers native support for IPv6 in various services, including Amazon VPC, EC2 instances, and Elastic Load Balancing. This means that in a single-tenant environment, tenants can utilize IPv6 for their resources seamlessly, without the need for complex workarounds or translations.

Regardless of the need for dual-stack configurations mentioned in the previous conversation:

"At the moment, we cannot solely rely on the IPv6-only option within our Infor environment as we must accommodate our customers' network topology. Since we cannot determine whether our requester network is using IPv4 or IPv6, we need to initially enable the Dual Stack feature at the VPC/Subnet level, depending on whether it's a public or private subnet."





Question and answer:

1) Our customers are using the IPv4 and they are trying to come to Infor (If in case Infor is IPv6) we cannot be IPv6 only at initial phase – we should be in Dual stack (IPv4, IPv6))

- Answer: "Yes, we do. Regardless of the customer's network/traffic (IPv4 / IPv6), the Dual stack mode enabled on the VPC will handle the incoming traffic and fulfill the requirements according to the network specifications.". Incase if we are fully IPv6 then we expect our customer network to be IPv6

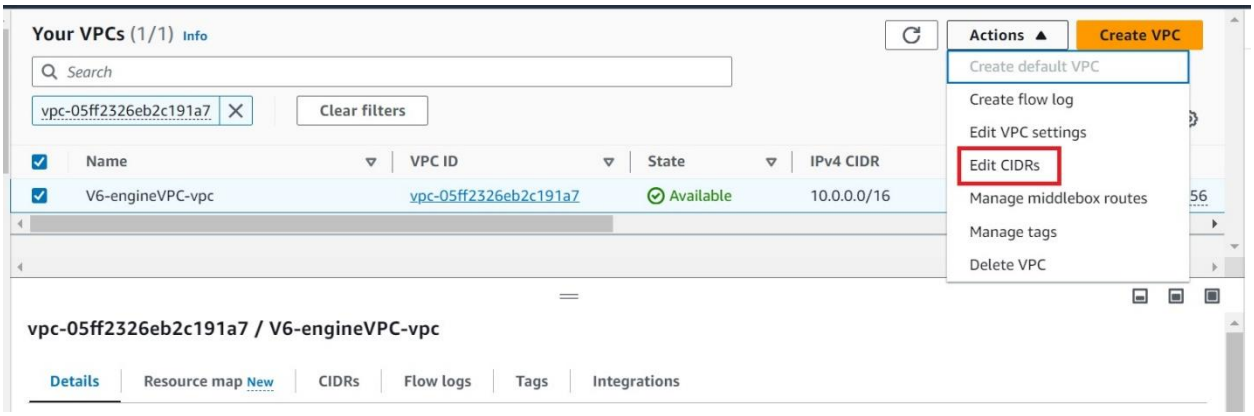
2) We have certain products like LM, Mingle/ADFS, LSF. For the prod - customer expect this should be available over the internet

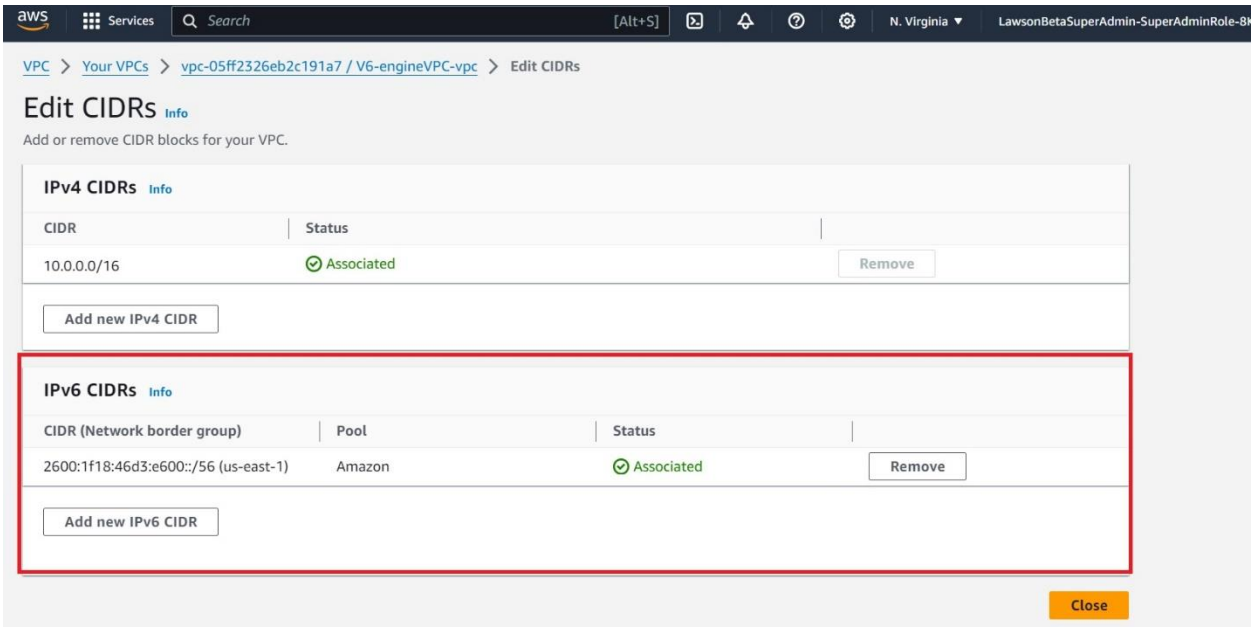
"Case 1: At Infor, irrespective of the application/product intended to be accessible over the internet, the application-hosted instance will remain the same, with no EIP assigned to it. This is because at Infor, we utilize an Application Load Balancer to access this product. At this point, we are unawareof whether our customer is using IPv4 exclusively. One key point to understand here is that when a customer or end user attempts to access an application over the internet, the Internet Service Provider(ISP) will assign both IPv6 and IPv4 to that end user. In the scenario where we enable the VPC in Dual Stack mode and the subnet within that VPC has opted for IPv6, the ALB sitting in that VPC'sIPv6 subnet will become associated with an IPv6 range. Consequently, regardless of the incoming traffic type, we can fulfill the requests.

Case 2: In contrast to the afore mentioned use case, we have certain applications intended to be accessible via an internal Load Balancer, meaning they won't be facing the internet directly. You might be wondering how customers can access these applications in such a setup. In this scenario, our end users connect through a VPN. For instance, if a customer is using IPv4 exclusively and we only support IPv6 (Note: AWS does not facilitate address translation for inbound traffic between IPv4 and IPv6), we employ a Bastion Host. This setup ensures that all IPv4-only traffic is directed to a Dual Stack EC2 instance (using both ENI v4 and ENI v6). this solution is an alternative to AWS-provided options and involves NATing." – not recommended.

Note: By default the V6 CIDR on VPC is /56 and subnet is /64 and it is in Hexadecimal format

How to enable IPv6 on preexisting VPC:



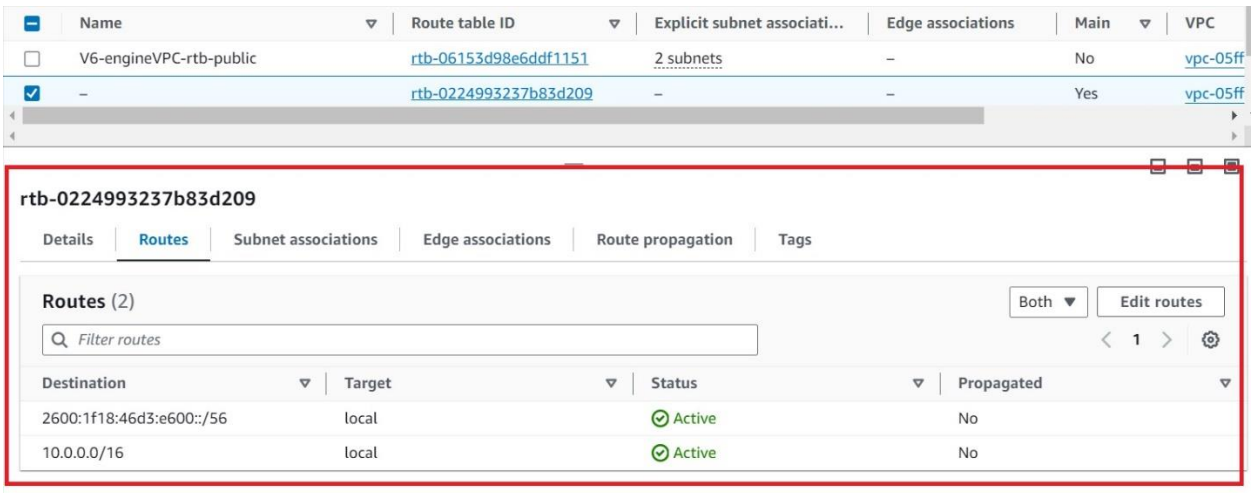


<u>The above two steps are required to enable IPv6 on VPC level.</u>

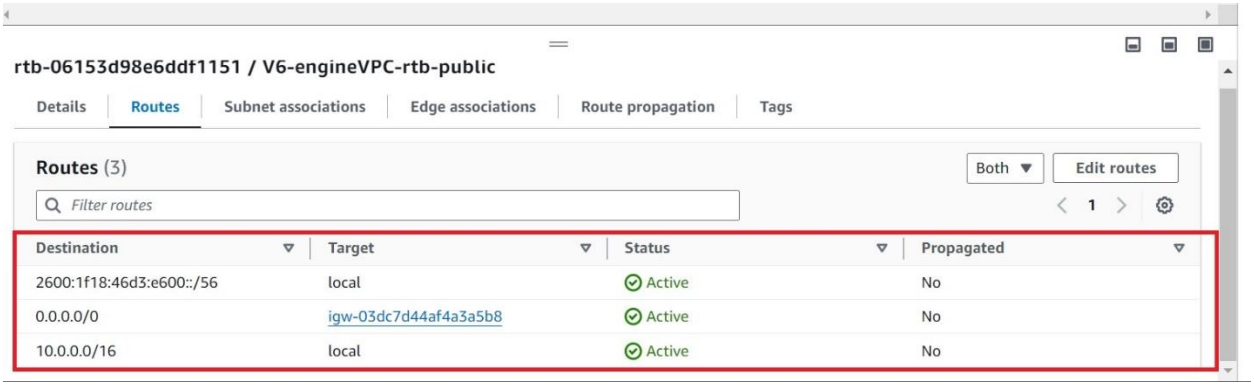
How does the Route Tables, Security Group and NACL will affect after enabling IPv6 on VPC level.

<u>Route Table:</u>

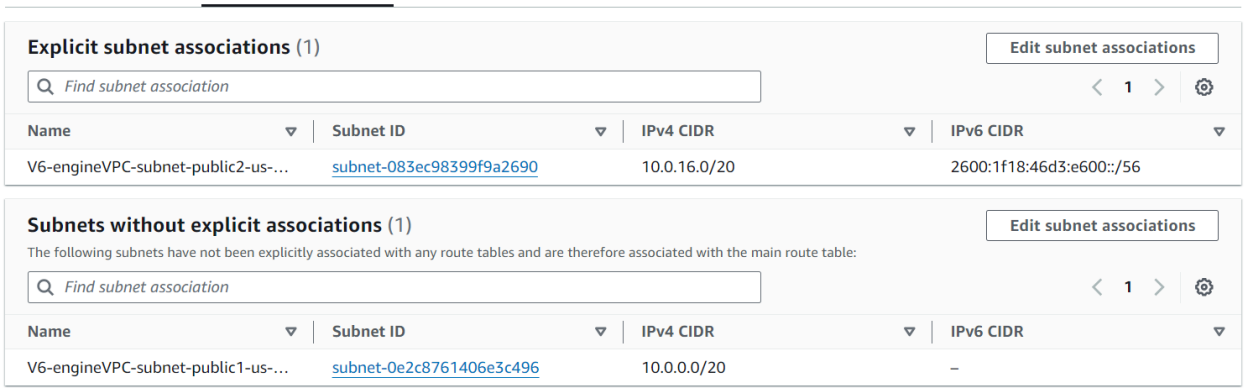
<u>Default Route Table:</u>



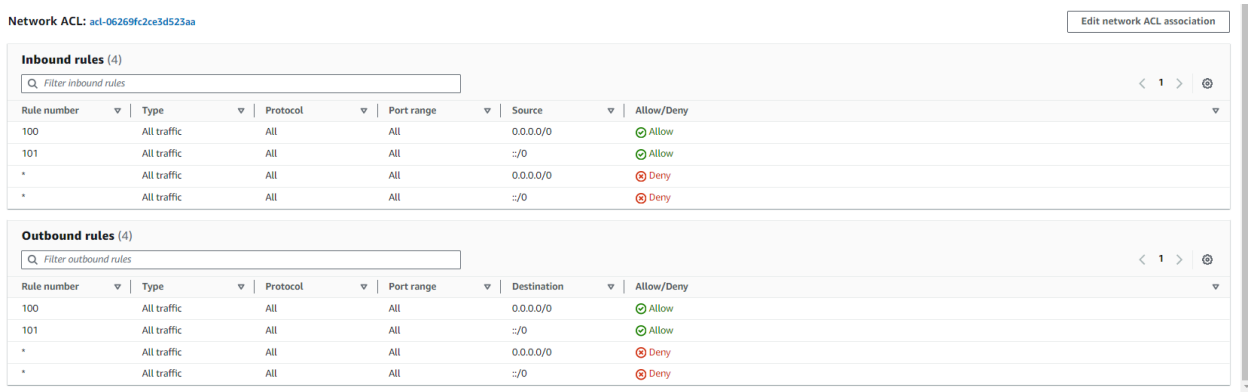
Custom Route Table:



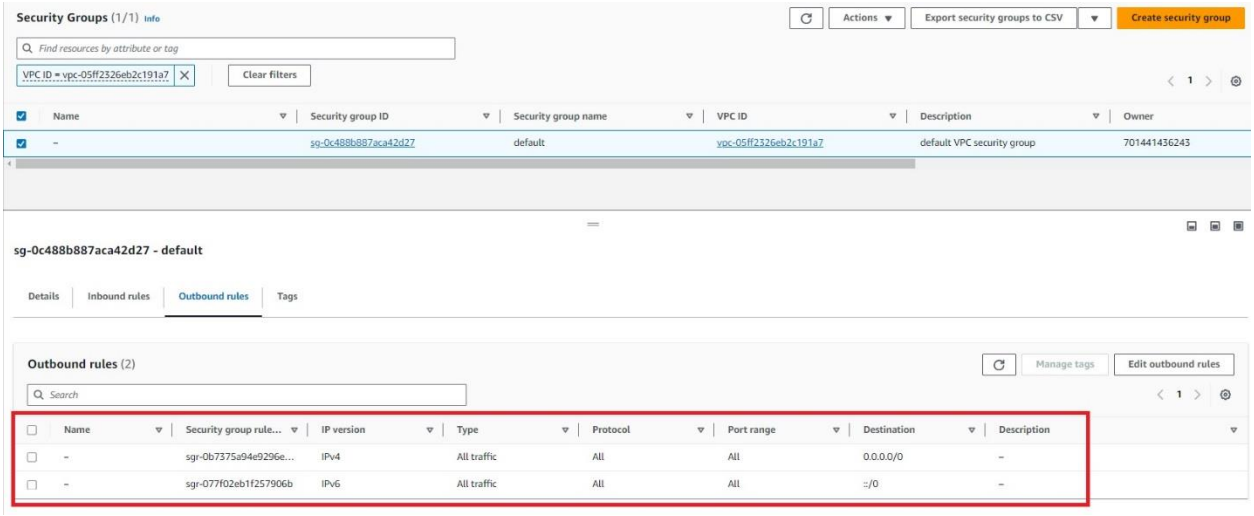
Subnet Association on Route Table:



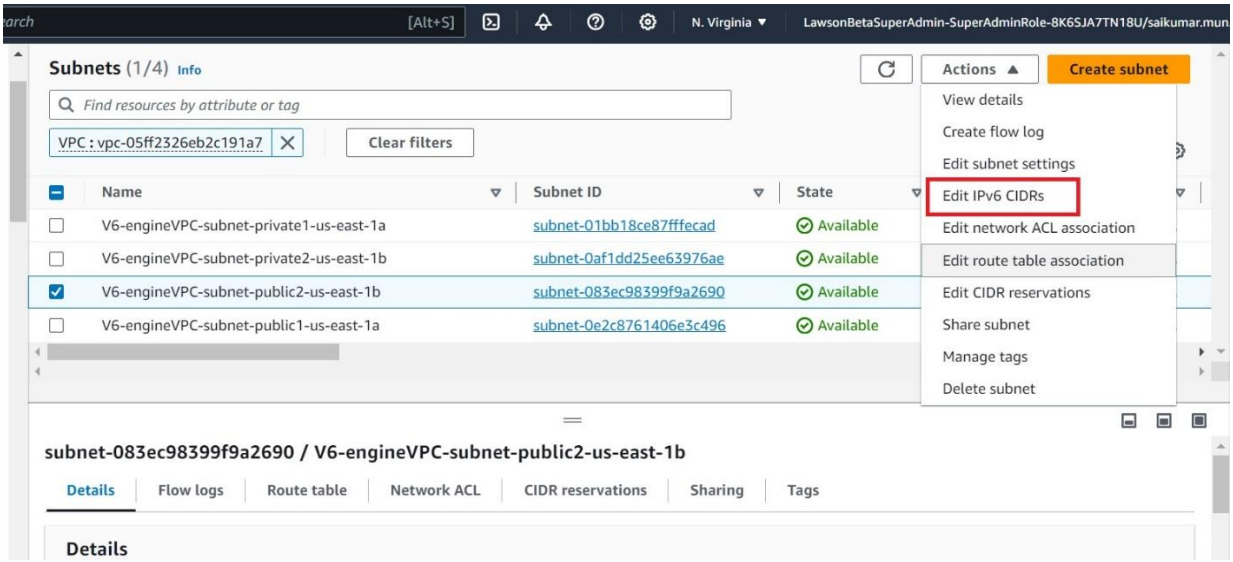
NACL:

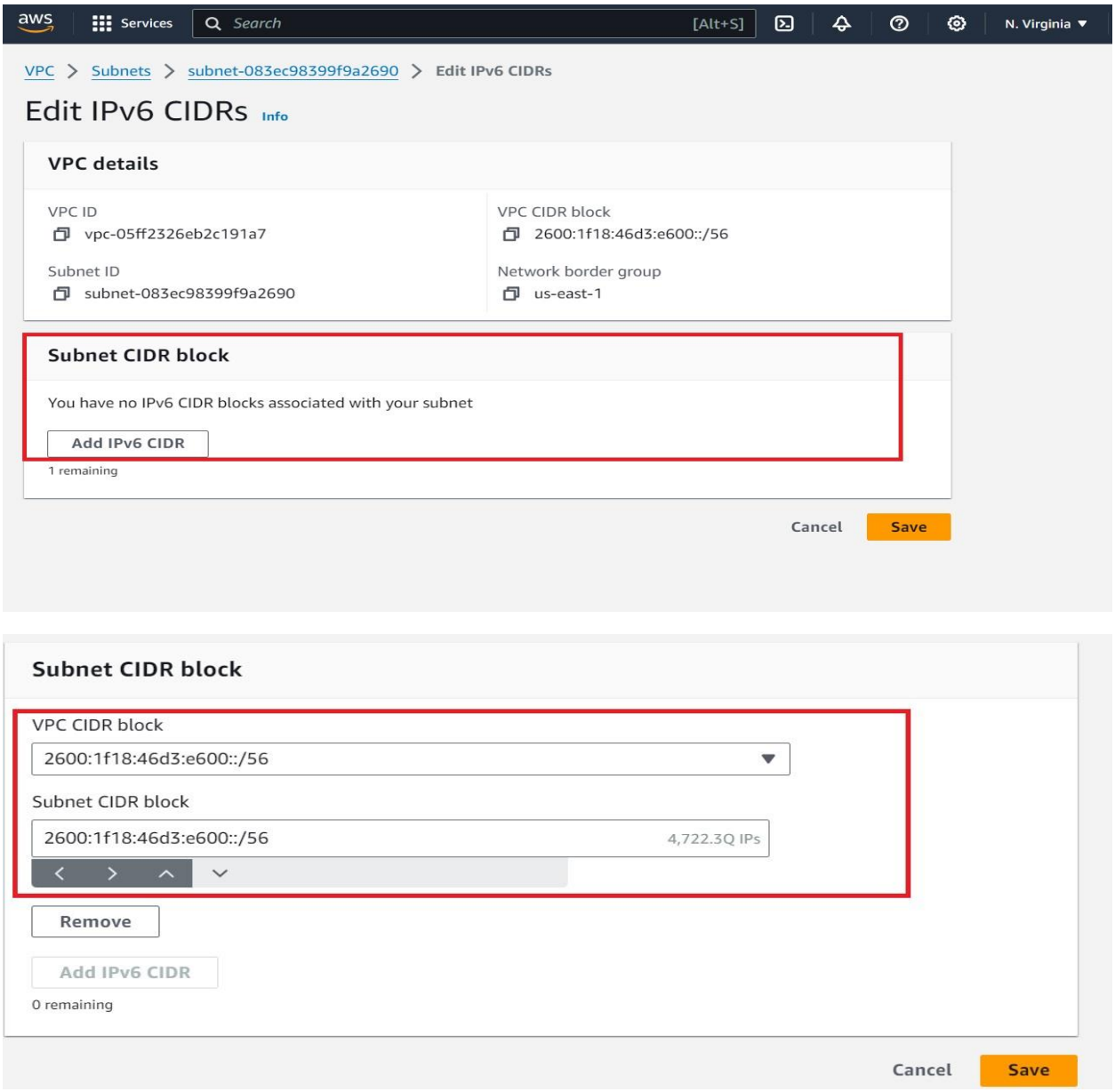


Security Group:



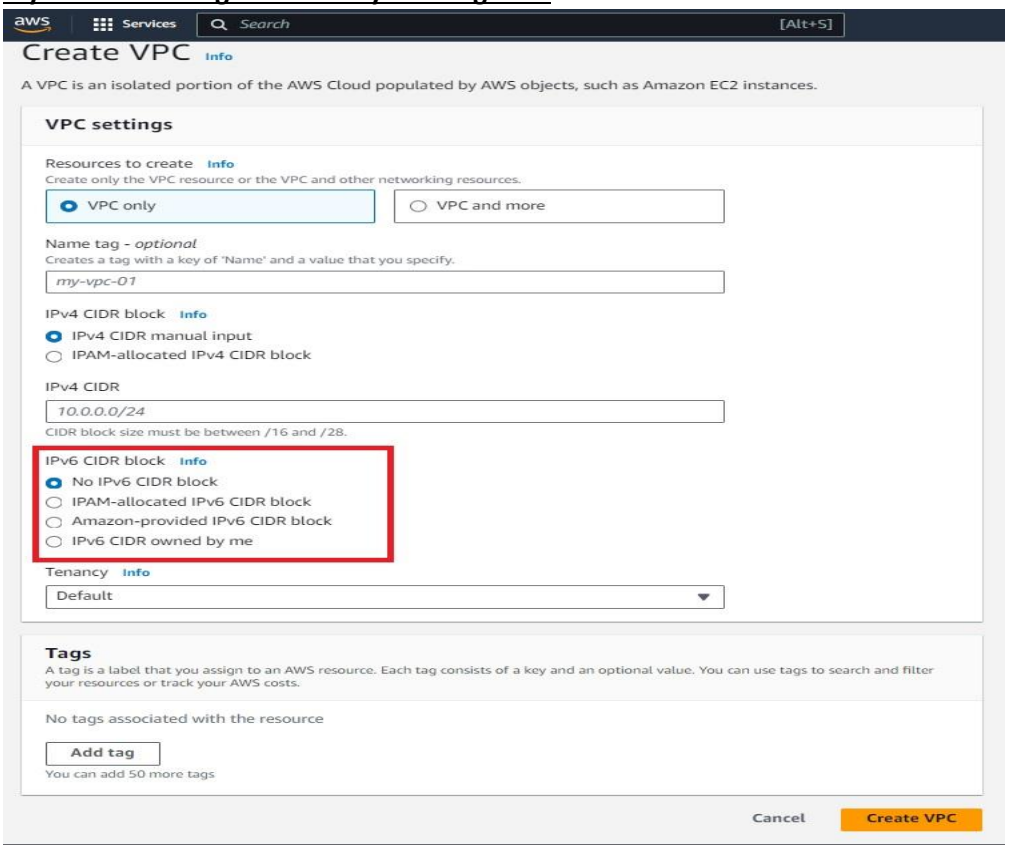
Enabling v6 at Subnet Level:




aws
Services
Search
[Alt+S]
N. Virginia
VPC > Subnets > subnet-083ec98399f9a2690 > Edit IPv6 CIDRs
Edit IPv6 CIDRs Info
VPC details
VPC ID
vpc-05ff2326eb2c191a7
VPC CIDR block
2600:1f18:46d3:e600::/56
Subnet ID
subnet-083ec98399f9a2690
Network border group
us-east-1
Subnet CIDR block
You have no IPv6 CIDR blocks associated with your subnet
Add IPv6 CIDR
1 remaining
Cancel
Save

Subnet CIDR block
VPC CIDR block
2600:1f18:46d3:e600::/56
Subnet CIDR block
2600:1f18:46d3:e600::/56
4,722.3Q IPs
Remove
Add IPv6 CIDR
0 remaining
Cancel
Save

If you are enabling v6 on newly creating VPC.



In the process of enabling IPv6 for existing infrastructure/VPC, this can be accomplished through both automation and manual processes from the AWS console. When IPv6 is enabled on the VPC, the default Security Group and NACL will automatically receive v6 rules. However, it's important to note that the Subnet will not inherit the v6 address automatically.

Enabling IPv6 on the subnet or VPC will not directly impact the application. However, if outbound traffic from the subnet to the internet is required, the use of the Egress-only Internet Gateway service on top of the VPC becomes necessary.

Point to be considered: After manual deletion/disablement of IPv6 on VPC will only remove v6 route from default and custom Route Tables but still the rules will exist on Security group and NACL.

Implementing IPv6 in an existing network can pose some challenges and potential impacts on applications and services. Here are some key considerations:

Compatibility Issues:

Some older applications and devices may not fully support IPv6. Ensuring compatibility and testing applications for IPv6 readiness is crucial.

Dual-Stack Complexity:

Running both IPv4 and IPv6 concurrently (dual-stack) can introduce complexity. Systems need to be capable of handling both address formats, and administrators must manage both IPv4 and IPv6 configurations.

Firewall and Security Configuration:

Firewalls and security policies may need adjustments to accommodate IPv6 traffic. Existing firewall rules designed for IPv4 may not be directly applicable, and security policies must be adapted to cover IPv6.

DNS Considerations:

DNS infrastructure needs to support IPv6 addresses. DNS servers, records, and configurations must be updated to handle IPv6 queries. This is essential for proper name resolution.

Application-Level Support:

Applications should be tested to ensure they can work seamlessly with IPv6. This includes validating that the application logic and communication protocols can handle IPv6 addresses.

Network Address Translation (NAT) Issues:

NAT is less common in IPv6 due to the availability of a larger address space. Applications relying on IPv4 NAT may require modification to work in an IPv6 environment.

Routing Challenges:

IPv6 introduces new routing protocols and considerations. Network administrators need to ensure that routers and routing tables are configured to handle IPv6 routes effectively.

Monitoring and Management Tools:

Existing network management and monitoring tools may not fully support IPv6. Upgrading or replacing these tools may be necessary to effectively monitor and manage IPv6-enabled networks.

Third-Party Services and APIs:

Applications relying on third-party services or APIs may face challenges if those services are not IPv6-compatible. Ensuring compatibility with external services is essential for end-to-end communication.

Quality of Service (QoS):

IPv6 introduces changes in header structures that may impact Quality of Service (QoS) policies. Network administrators should reassess and adjust QoS configurations accordingly.

Documentation and Communication:

Proper documentation is crucial during the transition to IPv6. Clear communication with stakeholders, including end-users and support teams, helps manage expectations and address concerns.

By addressing these challenges proactively and conducting thorough testing before implementation, organizations can minimize the potential impacts on existing applications and services during the transition to IPv6.

Note:

we added a IPv6 CIDR block for already created VPC. Upon added the IPv6 CIDR we saw 3 main changes:

1. Default IPv6 traffic was allowed at the Outbound of already created Security Groups under that VPC sgr-0f3f8e697baef4ad5 IPv6 All traffic All All ::/0

2. Below rule was automatically added the Network ACLs under that VPC for both Inbound and Outbound rules: * All traffic All All 0.0.0.0/0 Deny

3. Local route was added to the RTs for IPv6 traffic: 2600:1f11:bb4:8d00::/56 local Active == Routing: IPv6 addresses are globally unique, and are therefore public by default. However, they can be configured to remain private or reachable over the Internet. If you want your instance to be able to access the internet, but you want to prevent resources on the internet from initiating communication with your instance, you can use an egress-only internet gateway. To do this, create an egress-only internet gateway in your VPC, and then add a route to your route table that points all IPv6 traffic (::/0)

or a specific range of IPv6 address to the egress-only internet gateway. IPv6 traffic in the subnet that's associated with the route table is routed to the egress-only internet gateway. == Subnetting:

Later, I recreated a VPC with Ipv6 CIDR say: 2600:1f11:bb4:8d00::/56. I created 3 Subnets using this 3rd party Subnet Calculator: https://www.site24x7.com/tools/ipv6-subnetcalculator.html

Accordingly, you can create 256 Subnets with /64. For testing, I created below 3 subnets 2600:1f11:bb4:8d01::/64 2600:1f11:bb4:8d02::/64 2600:1f11:bb4:8d03::/64 Similarly you can use above tool to calculate Subnets and configure IPv6 CIDRs using Network address. == Impact of adding IPv6 CIDR on EC2 Instances and Load Balancer: Once you update the VPC with IPv6 CIDRs, this will not change the EC2 instances IP unless you create a new resource using IPv6 addresses. == Dynamic nature of Load Balancers IP address: Upon recreating your use-case of ALB/NLB getting IPv6 address, please note you will need edit the ALB/NLB and enable dualstack support. [1] After adding the dualstack support, you will get dynamic IPv6 address on your ALB/NLB.