Q: What factors should be considered when selecting a CIDR block for a VPC and its subnets?

Choosing the right CIDR (Classless Inter-Domain Routing) blocks for your Virtual Private Cloud (VPC) and its subnets is a foundational decision in cloud architecture. It impacts scalability, connectivity, and future flexibility.

VPC CIDR Block Selection

The VPC CIDR block defines the entire private IP address space available for your network within the cloud.

- **Size Considerations:**
  - **Plan for Future Growth and Scaling Needs:** This is paramount. It's much easier to start with a larger CIDR block than to try and expand it later. Anticipate future applications, services, and instance counts.
  - **/16 provides 65,536 IP addresses (Recommended for Most Cases):** This is a widely adopted and highly flexible choice. It offers ample IP addresses for the vast majority of enterprise and growing deployments, allowing for numerous subnets and resources without quickly running out of space.
  - **/20 provides 4,096 IP addresses (Smaller Deployments):** Suitable for smaller, more contained projects or specific use cases where the total number of resources is well-defined and not expected to grow significantly.
  - **/24 provides 256 IP addresses (Very Small Environments):** While technically possible, a /24 for an entire VPC is generally too restrictive. It only allows for a single subnet (as a VPC must contain at least one subnet), severely limiting any future expansion or the ability to segment your network into different Availability Zones (AZs).
  - **Cannot Expand VPC CIDR After Creation (Plan Generously):** This is a critical limitation in cloud environments (like AWS). Once a VPC is created with a specific CIDR block, it cannot be expanded or changed. If you run out of IP addresses, your options are limited, often requiring a complex migration to a new VPC, which is a significant undertaking.
- **IP Range Selection:**

- **Use RFC 1918 Private IP Ranges Only:** Always select IP address ranges from the private IP address blocks defined by RFC 1918. These ranges are not routable on the public internet, ensuring your internal network remains private.
    - 10.0.0.0/8 (ranging from 10.0.0.0 to 10.255.255.255)
    - 172.16.0.0/12 (ranging from 172.16.0.0 to 172.31.255.255)
    - 192.168.0.0/16 (ranging from 192.168.0.0 to 192.168.255.255)
- **Avoid Conflicts with On-Premises Networks:** If you plan to establish VPN connections or Direct Connect links to your on-premises data centers, ensure your VPC CIDR does not overlap with any of your existing internal network ranges. Overlapping CIDRs will cause routing conflicts and prevent successful communication.
- **Avoid Conflicts with Other VPCs for Peering:** If you intend to use VPC peering to connect this VPC with other VPCs (within the same or different accounts/regions), ensure their CIDR blocks do not overlap. VPC peering cannot be established between VPCs with overlapping IP spaces.

Subnet CIDR Planning

Subnets are logical subdivisions of your VPC's IP address range. They are tied to specific Availability Zones (AZs) for high availability.

- **Distribution Strategy:**
    - **Divide VPC CIDR into Smaller Subnet Blocks:** Break down your large VPC CIDR block into smaller, contiguous blocks for individual subnets. For example, a /16 VPC can contain many /24 or /20 subnets.
    - **Plan for Multiple AZs (Minimum 2 for High Availability):** To ensure your application remains available even if an entire Availability Zone experiences an outage, deploy your resources across at least two (and ideally more) AZs. This means creating separate subnets in each AZ for different tiers of your application.
    - **Reserve Space for Future Subnets:** Don't allocate every possible subnet immediately. Leave gaps in your IP addressing scheme to accommodate new application tiers, services, or environments that you might add later.
    - **Consider Public vs. Private Subnet Requirements:**
        - **Public Subnets:** Contain resources that need direct internet access (e.g., web servers, load balancers, NAT gateways). They are associated with a route table that has a route to an Internet Gateway.
        - **Private Subnets:** Contain resources that should not be directly accessible from the internet (e.g., database instances, application servers). Their route tables typically route outbound internet traffic through a NAT Gateway in a public subnet or a corporate VPN/Direct Connect connection.
- **Common Patterns (Example using 10.0.0.0/16 VPC):**
    - **VPC CIDR:** 10.0.0.0/16 (65,536 IPs)
    - **Public Subnet AZ-1a:** 10.0.1.0/24 (256 IPs) - For public-facing resources in AZ-1a.
    - **Private Subnet AZ-1a:** 10.0.2.0/24 (256 IPs) - For private resources (application servers) in AZ-1a.

- **Public Subnet AZ-1b:** 10.0.3.0/24 (256 IPs) - For public-facing resources in AZ-1b.
- **Private Subnet AZ-1b:** 10.0.4.0/24 (256 IPs) - For private resources (application servers) in AZ-1b.
- **Database Subnet AZ-1a:** 10.0.5.0/24 (256 IPs) - Dedicated subnet for databases in AZ-1a (often isolated for security).
- **Database Subnet AZ-1b:** 10.0.6.0/24 (256 IPs) - Dedicated subnet for databases in AZ-1b.
- *Note:* You could also have /20 subnets if you need more IPs per subnet, as long as they fit within the /16 VPC.

Best Practices

Adhering to these practices will make your network easier to manage, more scalable, and more robust.

- **Leave Gaps Between Subnets for Future Expansion:** Instead of sequentially allocating 10.0.1.0/24, 10.0.2.0/24, consider leaving gaps, e.g., 10.0.1.0/24 then 10.0.3.0/24. This allows you to insert new subnets (like 10.0.2.0/24 for a new service) without having to re-IP existing ones.
- **Use a Consistent Numbering Scheme:** Establish a clear pattern for your subnet CIDRs. For instance, dedicate ranges for public, private, and database subnets, or specific applications. This greatly improves readability and simplifies network troubleshooting.
- **Document IP Allocation Strategy:** Maintain clear documentation of your VPC CIDR, all subnet CIDRs, their purpose, and the AZs they belong to. This is invaluable for new team members, auditing, and troubleshooting.
- **Consider Reserved IPs (e.g., AWS Reserves First 4 and Last 1):** In cloud providers like AWS, each subnet has a few IP addresses reserved for internal use (e.g., network address, VPC router, DNS, future use, broadcast address). Factor these into your calculations, especially for smaller subnets. For a /24, this means 5 IPs are unusable, leaving 251 for your instances.
- **Plan for Different Tiers (Web, App, Database, Management):** Segmenting your network into logical tiers enhances security and simplifies network access control (e.g., using Security Groups and Network ACLs).
- **Account for Auto-Scaling Requirements:** Ensure your subnets have sufficient available IP addresses to accommodate the maximum number of instances that your auto-scaling groups might launch during peak load or scaling events. Running out of IPs can prevent new instances from launching.

Q1: Which of the following CIDR blocks is most commonly recommended for a new VPC in AWS for future scalability?

A. 10.0.0.0/24
B. 10.0.0.0/20
C. 10.0.0.0/16
D. 10.0.0.0/30

✅ **Answer: C. 10.0.0.0/16**

Q2: Why should you avoid using overlapping CIDR blocks in different VPCs?
A. It slows down the VPC
B. It increases cost
C. It causes conflicts during VPC peering
D. It makes subnet routing faster

✅ **Answer: C. It causes conflicts during VPC peering**

Q3: Which of the following are valid private IP address ranges as per RFC 1918? (Choose all that apply)
A. 10.0.0.0/8
B. 172.16.0.0/12
C. 192.168.0.0/16
D. 8.8.8.0/24

✅ **Answer: A, B, C**

Q4: What is the major limitation of a VPC CIDR block once created?
A. It can't be used for subnets
B. It cannot be resized later
C. It is always public
D. It only supports IPv6

✅ **Answer: B. It cannot be resized later**