VPC - A virtual network dedicated to your AWS account.

## Service Overview

*Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways*

*Concepts for VPCs:*

* [***Subnet***](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html)*— A range of IP addresses in your VPC. Each subnet in your VPC must be associated with a network ACL. If you don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL*
* [***Route table***](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html)*— A set of rules, called routes, that are used to determine where network traffic is directed. The following are the key concepts for route tables.*
  + *Main route table—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.*
  + *Custom route table—A route table that you create for your VPC.*
  + *Edge association—A route table that you use to route inbound VPC traffic to an appliance. You associate a route table with the internet gateway or virtual private gateway, and specify the network interface of your appliance as the target for VPC traffic.*
  + *Route table association—The association between a route table and a subnet, internet gateway, or virtual private gateway.*
  + *Subnet route table—A route table that's associated with a subnet.*
  + *Gateway route table—A route table that's associated with an internet gateway or virtual private gateway.*
* [***CIDR block***](http://en.wikipedia.org/wiki/CIDR_notation)*—Classless Inter-Domain Routing. An internet protocol address allocation and route aggregation methodology. For more information, see*[*Classless Inter-Domain Routing*](http://en.wikipedia.org/wiki/CIDR_notation)*in Wikipedia.*
* *Your VPC can operate in dual-stack mode: your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 addresses are independent of each other; you must configure routing and security in your VPC separately for IPv4 and IPv6. IPv6 characteristics and restrictions:*
  + *The format is 128-bit, 8 groups of 4 hexadecimal digits.*
  + *The VPC CIDR block size is fixed at /56.*
  + *The subnet CIDR block size is fixed at /64.*
  + *We choose the IPv6 CIDR block for your VPC from Amazon's pool of IPv6 addresses. You cannot select your own range.*
  + *No distinction between public and private IP addresses. IPv6 addresses are public.*
  + *Amazon-provided DNS hostnames are not supported.*
  + *Elastic IPv6 addresses are not supported.*
  + *Not supported for customer gateways, virtual private gateways, NAT devices, and VPC endpoints.*

*The following best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.*

*The following are general best practices:*

* *Use multiple Availability Zone deployments so you have high availability.*
* *Use security groups and network ACLs. For more information, see*[*Security groups for your VPC*](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)*and*[*Network ACLs*](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html)*.*
* *Use IAM policies to control access.*
* *Use Amazon CloudWatch to monitor your VPC components and VPN connections.*
* *Use flow logs to capture information about IP traffic going to and from network interfaces in your VPC. For more information*

## Use cases / Considerations

*What can we do with a VPC?*

* *Host a simple, public-facing website*
* *Host multi-tier web applications*
* *Back up and recover your data after a disaster*
* *Extend your corporate network into the cloud*
* *Securely connect cloud applications to your datacenter*
* *Launch instances into a subnet of your choosing*
* *Assign custom IP address ranges in each subnet*
* *Configure route tables between subnets*
* *Create internet gateway and attach it to our VPC*
* *Much better security control over your AWS resources*
* *Instance security groups*
* *Subnet network access control lists (ACLS*

## Governance

*Monitoring tools:*

* *VPC Flow logs*
* *CloudWatch*

## Cautions

* *You can create 5 VPCs per Region. The quota for internet gateways per Region is directly correlated to this one. Increasing this quota increases the quota on internet gateways per Region by the same amount. You can have 100s of VPCs per Region for your needs even though the default quota is 5 VPCs per Region.*
* *Subnets per VPC – 200*
* *IPv4 CIDR blocks per VPC - 5*
* *IPv6 CIDR blocks per VPC -1*
* 1 Subnet = 1 Availability Zone
* *Route tables per VPC – 200. The main route table counts toward this quota.*
* *Routes per route table (non-propagated routes) – 50.You can increase this quota up to a maximum of 1,000; however, network performance might be impacted. This quota is enforced separately for IPv4 routes and IPv6 routes.If you have more than 125 routes, we recommend that you paginate calls to describe your route tables for better performance. If you reference a customer-managed prefix list in a route, the maximum number of entries for the prefix lists equals the same number of routes.*
* *BGP advertised routes per route table (propagated routes) – 100. This quota cannot be increased. If you require more than 100 prefixes, advertise a default route.*
* *The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses).*
* *After you've created your VPC, you can associate secondary CIDR blocks with the VPC.*
* *The CIDR block of a subnet can be the same as the CIDR block for the VPC*
* *Five IP addresses from CIDR are reserved (Routing, DNS,broadcasting)*

## Pricing considerations

*There's no additional charge for using a VPC. There are charges for the following VPC components: Site-to-Site VPN connection, PrivateLink, Traffic Mirroring, and a NAT gateway. For more information, see* [Amazon VPC Pricing](https://aws.amazon.com/vpc/pricing/)*.*

## More details

[VPCs and subnets - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html)

[Working with VPCs and subnets - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html)

[Examples for VPC - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenarios.html)

[Route tables for your VPC - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html)

https://www.youtube.com/watch?v=fpxDGU2KdkA