Amazon VPC FAQs

aws.amazon.com (https://aws.amazon.com/vpc/faqs/)

General Questions

Q. What is 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 ranges, creation of subnets, and configuration of route tables and network gateways. You can also create a hardware Virtual Private Network (VPN) connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Q. What are the components of Amazon VPC?

Amazon VPC comprises a variety of objects that will be familiar to customers with existing networks:

- A Virtual Private Cloud: A logically isolated virtual network in the AWS cloud. You define a VPC’s IP address space from ranges you select.
- Subnet: A segment of a VPC’s IP address range where you can place groups of isolated resources.
- Internet Gateway: The Amazon VPC side of a connection to the public Internet.
- NAT Gateway: A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.
- Virtual private gateway: The Amazon VPC side of a VPN connection.
- Peering Connection: A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
- VPC Endpoints: Enables private connectivity to services hosted in AWS, from within your VPC without using an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
- Egress-only Internet Gateway: A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

Q: Why should I use Amazon VPC?

Amazon VPC enables you to build a virtual network in the AWS cloud - no VPNs, hardware, or physical datacenters required. You can define your own network space, and control how your network and the Amazon EC2 resources inside your network are exposed to the Internet. You can also leverage the enhanced security options in Amazon VPC to provide more granular access to and from the Amazon EC2 instances in your virtual network.

Q. How do I get started with Amazon VPC?

Your AWS resources are automatically provisioned in a ready-to-use default VPC. You can choose to create additional VPCs by going to the Amazon VPC page in the AWS Management Console and selecting "Start VPC Wizard".

You'll be presented with four basic options for network architectures. After selecting an option, you can modify the size and IP address range of the VPC and its subnets. If you select an option with Hardware VPN Access, you will need to specify the IP address of the VPN hardware on your network. You can modify the VPC to add or remove secondary IP ranges and gateways, or add more subnets to IP ranges.

The four options are:

1. Amazon VPC with a single public subnet only
2. Amazon VPC with public and private subnets
3. Amazon VPC with public and private subnets and AWS Site-to-Site VPN access
4. Amazon VPC with a private subnet only and AWS Site-to-Site VPN access

Q. What are the different types of VPC endpoints available on Amazon VPC?

VPC endpoints enable you to privately connect your VPC to services hosted on AWS without requiring an Internet gateway, a NAT device, VPN, or firewall proxies. Endpoints are horizontally scalable and highly available virtual devices that allow communication between instances in your VPC and AWS services. Amazon VPC offers two different types of endpoints: gateway type endpoints and interface type endpoints.

Gateway type endpoints are available only for AWS services including S3 and DynamoDB. These endpoints will add an entry to your route table you selected and route the traffic to the supported services through Amazon's private network.

Interface type endpoints provide private connectivity to services powered by PrivateLink, being AWS services, your own services or SaaS solutions, and supports connectivity over Direct Connect. More AWS and SaaS solutions will be supported by these endpoints in the future. Please refer to VPC Pricing for the price of interface type endpoints.

Billing

Q. How will I be charged and billed for my use of Amazon VPC?

There are no additional charges for creating and using the VPC itself. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges. If you connect your VPC to your corporate datacenter using the optional hardware VPN connection, pricing is per VPN connection-hour (the amount of time you have a VPN connection in the "available" state.) Partial hours are billed as full hours. Data transferred over VPN connections will be charged at standard AWS Data Transfer rates. For VPC-VPN pricing information, please visit the pricing section (http://aws.amazon.com/vpc/pricing) of the Amazon VPC product page (http://aws.amazon.com/vpc).

Q. What usage charges will I incur if I use other AWS services, such as Amazon S3, from Amazon EC2 instances in my VPC?

Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources. Data transfer charges are not incurred when accessing Amazon Web Services, such as Amazon S3, via your VPC's Internet gateway.

If you access AWS resources via your VPN connection, you will incur Internet data transfer charges.

Q: Do your prices include taxes?

Except as otherwise noted, our prices are exclusive of applicable taxes and duties, including VAT and applicable sales tax. For customers with a Japanese billing address, use of AWS services is subject to Japanese Consumption Tax. Learn more. (https://aws.amazon.com/c-tax-faqs/)

Connectivity

Q. What are the connectivity options for my Amazon VPC?

You may connect your Amazon VPC to:

- The internet (via an internet gateway)
- Your corporate data center using an AWS Site-to-Site VPN connection (via the virtual private gateway)
- Both the internet and your corporate data center (utilizing both an internet gateway and a virtual private gateway)
- Other AWS services (via internet gateway, NAT, virtual private gateway, or VPC endpoints)
- Other Amazon VPCs (via VPC peering connections)

Q. How do I connect my VPC to the Internet?
Amazon VPC supports the creation of an Internet gateway. This gateway enables Amazon EC2 instances in the VPC to directly access the Internet.
Q. Are there any bandwidth limitations for Internet gateways? Do I need to be concerned about its availability? Can it be a single point of failure?
No. An Internet gateway is horizontally-scaled, redundant, and highly available. It imposes no bandwidth constraints.
Q. How do instances in a VPC access the Internet?
You can use public IP addresses, including Elastic IP addresses (EIPs), to give instances in the VPC the ability to both directly communicate outbound to the Internet and to receive unsolicited inbound traffic from the Internet (e.g., web servers). You can also use the solutions in the next question.
Q. How do instances without public IP addresses access the Internet
Instances without public IP addresses can access the Internet in one of two ways:

1. Instances without public IP addresses can route their traffic through a NAT gateway or a NAT instance to access the Internet. These instances use the public IP address of the NAT gateway or NAT instance to traverse the Internet. The NAT gateway or NAT instance allows outbound communication but doesn't allow

machines on the Internet to initiate a connection to the privately addressed instances.

2. For VPCs with a hardware VPN connection or Direct Connect connection, instances can route their Internet traffic down the virtual private gateway to your existing datacenter. From there, it can access the Internet via your existing egress points and network security/monitoring devices.

Q. Can I connect to my VPC using a software VPN?

Yes. You may use a third-party software VPN to create a site to site or remote access VPN connection with your VPC via the Internet gateway.

Q. Does traffic go over the internet when two instances communicate using public IP addresses?

Traffic between two EC2 instances in the same AWS Region stays within the AWS network, even when it goes over public IP addresses.

Traffic between EC2 instances in different AWS Regions stays within the AWS network, if there is an Inter-Region VPC Peering connection between the VPCs where the two instances reside.

Traffic between EC2 instances in different AWS Regions where there is no Inter-Region VPC Peering connection between the VPCs where these instances reside, is not guaranteed to stay within the AWS network.

Q. How does an AWS Site-to-Site VPN connection work with Amazon VPC?

An AWS Site-to-Site VPN connection connects your VPC to your datacenter. Amazon supports Internet Protocol Security (IPSec) VPN connections. Data transferred between your VPC and datacenter routes over an encrypted VPN connection to help maintain the confidentiality and integrity of data in transit. An internet gateway is not required to establish an AWS Site-to-Site VPN connection.

IP Addressing

Q. What IP address ranges can I use within my Amazon VPC?

You can use any IPv4 (http://en.wikipedia.org/wiki/IPv4) address range, including RFC 1918 (https://tools.ietf.org/html/rfc1918) or publicly routable IP ranges, for the primary CIDR block. For the secondary CIDR blocks, certain restrictions (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#add-cidr-block-restrictions) apply. Publicly routable IP blocks are only reachable via the Virtual Private Gateway and cannot be accessed over the Internet through the Internet gateway. AWS does not advertise customer-owned IP address blocks to the Internet. You can allocate an Amazon-provided IPv6 CIDR block to a VPC by calling the relevant API or via the AWS Management Console.

Q. How do I assign IP address ranges to Amazon VPCs?

You assign a single Classless Internet Domain Routing (CIDR) (http://en.wikipedia.org/wiki/CIDR) IP address range as the primary CIDR block when you create a VPC and can add up to four (4) secondary CIDR blocks after creation of the VPC. Subnets within a VPC are addressed from these CIDR ranges by you. Please note that while you can create multiple VPCs with overlapping IP address ranges, doing so will prohibit you from connecting these VPCs to a common home network via the hardware VPN connection. For this reason we recommend using non-overlapping IP address ranges. You can allocate an Amazon-provided IPv6 CIDR block to your VPC.

Q. What IP address ranges are assigned to a default Amazon VPC?

Default VPCs are assigned a CIDR range of 172.31.0.0/16. Default subnets within a default VPC are assigned /20 netblocks within the VPC CIDR range.

Q. Can I advertise my VPC public IP address range to the internet and route the traffic through my datacenter, via the AWS Site-to-Site VPN, and to my Amazon VPC?

Yes, you can route traffic via the AWS Site-to-Site VPN connection and advertise the address range from your home network.

Q. Can I use my public IPv4 addresses in VPC and access them over the Internet?

Yes, you can bring your public IPv4 addresses into AWS VPC and statically allocate them to subnets and EC2 instances. To access these addresses over the Internet, you will have to advertise them to the Internet from your on-premises network. You will also have to route the traffic over these addresses between your VPC and on-premises network using AWS DX or AWS VPN connection. You can route the traffic from your VPC using the Virtual Private Gateway. Similarly, you can route the traffic from your on-premises network back to your VPC using your routers.

Q. How large of a VPC can I create?

Currently, Amazon VPC supports five (5) IP address ranges, one (1) primary and four (4) secondary for IPv4. Each of these ranges can be between /28 (in CIDR notation) and /16 in size. The IP address ranges of your VPC should not overlap with the IP address ranges of your existing network.

For IPv6, the VPC is a fixed size of /56 (in CIDR notation). A VPC can have both IPv4 and IPv6 CIDR blocks associated to it.

Q. Can I change the size of a VPC?

Yes. You can expand your existing VPC by adding four (4) secondary IPv4 IP ranges (CIDRs) to your VPC. You can shrink your VPC by deleting the secondary CIDR blocks you have added to your VPC. You cannot however change the size of the IPv6 address range of your VPC.

Q. How many subnets can I create per VPC?

Currently you can create 200 subnets per VPC. If you would like to create more, please submit a case at the support center (https://aws.amazon.com/contact-us/vpc-request/).

Q. Is there a limit on how large or small a subnet can be?

The minimum size of a subnet is a /28 (or 14 IP addresses.) for IPv4. Subnets cannot be larger than the VPC in which they are created.

For IPv6, the subnet size is fixed to be a /64. Only one IPv6 CIDR block can be allocated to a subnet.

Q. Can I use all the IP addresses that I assign to a subnet?

No. Amazon reserves the first four (4) IP addresses and the last one (1) IP address of every subnet for IP networking purposes.

Q. How do I assign private IP addresses to Amazon EC2 instances within a VPC?

When you launch an Amazon EC2 instance within a VPC, you may optionally specify the primary private IP address for the instance. If you do not specify the primary private IP address, AWS automatically addresses it from the IP address range you assign to that subnet. You can assign secondary private IP addresses when you launch an instance, when you create an Elastic Network Interface, or any time after the instance has been launched or the interface has been created.

Q. Can I change the private IP addresses of an Amazon EC2 instance while it is running and/or stopped within a VPC?

Primary private IP addresses are retained for the instance's or interface's lifetime. Secondary private IP addresses can be assigned, unassigned, or moved between interfaces or instances at any time.

Q. If an Amazon EC2 instance is stopped within a VPC, can I launch another instance with the same IP address in the same VPC?

No. An IP address assigned to a running instance can only be used again by another instance once that original running instance is in a “terminated” state.

Q. Can I assign IP addresses for multiple instances simultaneously?

No. You can specify the IP address of one instance at a time when launching the instance.

Q. Can I assign any IP address to an instance?

You can assign any IP address to your instance as long as it is:

- Part of the associated subnet's IP address range
- Not reserved by Amazon for IP networking purposes
- Not currently assigned to another interface

Q. Can I assign multiple IP addresses to an instance?

Yes. You can assign one or more secondary private IP addresses to an Elastic Network Interface or an EC2 instance in Amazon VPC. The number of secondary private IP addresses you can assign depends on the instance type. See EC2 User Guide (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html) for more information on the number of secondary private IP addresses that can be assigned per instance type.

Q. Can I assign one or more Elastic IP (EIP) addresses to VPC-based Amazon EC2 instances?

Yes, however, the EIP addresses will only be reachable from the Internet (not over the VPN connection). Each EIP address must be associated with a unique private IP address on the instance. EIP addresses should only be used on instances in subnets configured to route their traffic directly to the Internet gateway. EIPs cannot be used on instances in subnets configured to use a NAT gateway or a NAT instance to access the Internet. This is applicable only for IPv4. Amazon VPCs do not support EIPs for IPv6 at this time.

Topology

Q. Can I specify which subnet will use which gateway as its default?

Yes. You may create a default route for each subnet. The default route can direct traffic to egress the VPC via the Internet gateway, the virtual private gateway, or the NAT gateway.

Q. Does Amazon VPC support multicast (http://en.wikipedia.org/wiki/IP_multicast) or broadcast (http://en.wikipedia.org/wiki/Broadcast_address#IP_network_broadcasting)?

No.

Security and Filtering

Q. How do I secure Amazon EC2 instances running within my VPC?

Amazon EC2 security groups can be used to help secure instances within an Amazon VPC. Security groups in a VPC enable you to specify both inbound and outbound network traffic that is allowed to or from each Amazon EC2 instance. Traffic which is not explicitly allowed to or from an instance is automatically denied.

In addition to security groups, network traffic entering and exiting each subnet can be allowed or denied via network Access Control Lists (ACLs).

Q. What are the differences between security groups in a VPC and network ACLs in a VPC?

Security groups in a VPC specify which traffic is allowed to or from an Amazon EC2 instance. Network ACLs operate at the subnet level and evaluate traffic entering and exiting a subnet. Network ACLs can be used to set both Allow and Deny rules. Network ACLs do not filter traffic between instances in the same subnet. In addition, network ACLs perform stateless filtering while security groups perform stateful filtering.

Q. What is the difference between stateful and stateless filtering?

Stateful filtering tracks the origin of a request and can automatically allow the reply to the request to be returned to the originating computer. For example, a stateful filter that allows inbound traffic to TCP port 80 on a webserver will allow the return traffic, usually on a high numbered port (e.g., destination TCP port 63, 912) to pass through the

stateful filter between the client and the webserver. The filtering device maintains a state table that tracks the origin and destination port numbers and IP addresses. Only one rule is required on the filtering device: Allow traffic inbound to the web server on TCP port 80.

Stateless filtering, on the other hand, only examines the source or destination IP address and the destination port, ignoring whether the traffic is a new request or a reply to a request. In the above example, two rules would need to be implemented on the filtering device: one rule to allow traffic inbound to the web server on TCP port 80, and another rule to allow outbound traffic from the webserver (TCP port range 49, 152 through 65, 535).

Q. Within Amazon VPC, can I use SSH key pairs created for instances within Amazon EC2, and vice versa?

Yes.

Q. Can Amazon EC2 instances within a VPC communicate with Amazon EC2 instances not within a VPC?

Yes. If an Internet gateway has been configured, Amazon VPC traffic bound for Amazon EC2 instances not within a VPC traverses the Internet gateway and then enters the public AWS network to reach the EC2 instance. If an Internet gateway has not been configured, or if the instance is in a subnet configured to route through the virtual private gateway, the traffic traverses the VPN connection, egresses from your datacenter, and then re-enters the public AWS network.

Q. Can Amazon EC2 instances within a VPC in one region communicate with Amazon EC2 instances within a VPC in another region?

Yes. Instances in one region can communicate with each other using Inter-Region VPC Peering, public IP addresses, NAT gateway, NAT instances, VPN Connections or Direct Connect connections.

Q. Can Amazon EC2 instances within a VPC communicate with Amazon S3?

Yes. There are multiple options for your resources within a VPC to communicate with Amazon S3. You can use VPC Endpoint for S3, which makes sure all traffic remains within Amazon's network and enables you to apply additional access policies to your Amazon S3 traffic. You can use an Internet gateway to enable Internet access from your VPC and instances in the VPC can communicate with Amazon S3. You can also make all traffic to Amazon S3 traverse the Direct Connect or VPN connection, egress from your datacenter, and then re-enter the public AWS network.

Q. Can I monitor the network traffic in my VPC?

Yes. You can use Amazon VPC traffic mirroring and Amazon VPC flow logs features to monitor the network traffic in your Amazon VPC.

VPC Traffic Mirroring

Q. What is Amazon VPC traffic mirroring?

Amazon VPC traffic mirroring makes it easy for customers to replicate network traffic to and from an Amazon EC2 instance and forward it to out-of-band security and monitoring appliances for use-cases such as content inspection, threat monitoring, and troubleshooting. These appliances can be deployed on an individual EC2 instance or a fleet of instances behind a Network Load Balancer (NLB) with User Datagram Protocol (UDP) listener.

Q. How does Amazon VPC traffic mirroring work?

The traffic mirroring feature copies network traffic from Elastic Network Interface (ENI) of EC2 instances in your Amazon VPC. The mirrored traffic can be sent to another EC2 instance or to an NLB with a UDP listener. Traffic mirroring encapsulates all copied traffic with VXLAN headers. The mirror source and destination (monitoring appliances) can be in the same VPC or in a different VPC, connected via VPC peering or AWS Transit Gateway.

Q. Which resources can be monitored with Amazon VPC traffic mirroring ?

Traffic mirroring supports network packet captures at the Elastic Network Interface (ENI) level for EC2 instances. This feature is currently supported on all virtualized Nitro based EC2 instances (https://docs.aws.amazon.com /AWSEC2/latest/UserGuide/instance-types.html#ec2-nitro-instances).

Q. What type of appliances are supported with Amazon VPC traffic mirroring?

Customers can either use open source tools or choose from a wide-range of monitoring solution available on AWS Marketplace. Traffic mirroring allows customers to stream replicated traffic to any network packet collector/broker or analytics tool, without requiring them to install vendor-specific agents.

Q. How is Amazon VPC traffic mirroring different from Amazon VPC flow logs?

Amazon VPC flow logs allow customers to collect, store, and analyze network flow logs. The information captured in flow logs includes information about allowed and denied traffic, source and destination IP addresses, ports, protocol number, packet and byte counts, and an action (accept or reject). You can use this feature to troubleshoot connectivity and security issues and to make sure that the network access rules are working as expected.

Amazon VPC traffic mirroring, provides deeper insight into network traffic by allowing you to analyze actual traffic content, including payload, and is targeted for use-cases when you need to analyze the actual packets to determine the root cause a performance issue, reverse-engineer a sophisticated network attack, or detect and stop insider abuse or compromised workloads.

Amazon VPC and EC2

Q. Within which Amazon EC2 region(s) is Amazon VPC available?

Amazon VPC is currently available in multiple Availability Zones (http://developer.amazonwebservices.com/connect

/entry.jspa?externalID=1347) in all Amazon EC2 regions.

Q. Can a VPC span multiple Availability Zones?

Yes.

Q. Can a subnet span Availability Zones?

No. A subnet must reside within a single Availability Zone.

Q. How do I specify which Availability Zone my Amazon EC2 instances are launched in?

When you launch an Amazon EC2 instance, you must specify the subnet in which to launch the instance. The instance will be launched in the Availability Zone associated with the specified subnet.

Q. How do I determine which Availability Zone my subnets are located in?

When you create a subnet you must specify the Availability Zone in which to place the subnet. When using the VPC Wizard, you can select the subnet's Availability Zone in the wizard confirmation screen. When using the API or the CLI you can specify the Availability Zone for the subnet as you create the subnet. If you don’t specify an Availability Zone, the default "No Preference" option will be selected and the subnet will be created in an available Availability Zone in the region.

Q. Am I charged for network bandwidth between instances in different subnets?

If the instances reside in subnets in different Availability Zones, you will be charged $0.01 per GB for data transfer.

Q. When I call DescribeInstances(), do I see all of my Amazon EC2 instances, including those in EC2-Classic and EC2-VPC?

Yes. DescribeInstances() will return all running Amazon EC2 instances. You can differentiate EC2-Classic instances from EC2-VPC instances by an entry in the subnet field. If there is a subnet ID listed, the instance is within a VPC.

Q. When I call DescribeVolumes(), do I see all of my Amazon EBS volumes, including those in EC2-Classic and EC2-VPC?

Yes. DescribeVolumes() will return all your EBS volumes.

Q. How many Amazon EC2 instances can I use within a VPC?

You can run any number of Amazon EC2 instances within a VPC, so long as your VPC is appropriately sized to have an IP address assigned to each instance. You are initially limited to launching 20 Amazon EC2 instances at any one time and a maximum VPC size of /16 (65,536 IPs). If you would like to increase these limits, please

complete the following form (http://aws.amazon.com/contact-us/vpc-request/).

Q. Can I use my existing AMIs in Amazon VPC?

You can use AMIs in Amazon VPC that are registered within the same region as your VPC. For example, you can use AMIs registered in us-east-1 with a VPC in us-east-1. More information is available in the Amazon EC2 Region and Availability Zone FAQ (http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/FAQ_Regions_Availability_Zones.html).

Q. Can I use my existing Amazon EBS snapshots?

Yes, you may use Amazon EBS snapshots if they are located in the same region as your VPC. More details are available in the Amazon EC2 Region and Availability Zone FAQ. (http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/FAQ_Regions_Availability_Zones.html)

Q: Can I boot an Amazon EC2 instance from an Amazon EBS volume within Amazon VPC?

Yes, however, an instance launched in a VPC using an Amazon EBS-backed AMI maintains the same IP address when stopped and restarted. This is in contrast to similar instances launched outside a VPC, which get a new IP address. The IP addresses for any stopped instances in a subnet are considered unavailable.

Q. Can I use Amazon EC2 Reserved Instances with Amazon VPC?

Yes. You can reserve an instance in Amazon VPC when you purchase Reserved Instances. When computing your bill, AWS does not distinguish whether your instance runs in Amazon VPC or standard Amazon EC2. AWS automatically optimizes which instances are charged at the lower Reserved Instance rate to ensure you always pay the lowest amount. However, your instance reservation will be specific to Amazon VPC. Please see the Reserved Instances (http://aws.amazon.com/ec2/reserved-instances) page for further details.

Q. Can I employ Amazon CloudWatch within Amazon VPC?

Yes.

Q. Can I employ Auto Scaling within Amazon VPC?

Yes.

Q. Can I launch Amazon EC2 Cluster Instances in a VPC?

Yes. Cluster instances are supported in Amazon VPC, however, not all instance types are available in all regions and Availability Zones.

Default VPCs

Q. What is a default VPC?

A default VPC is a logically isolated virtual network in the AWS cloud that is automatically created for your AWS account the first time you provision Amazon EC2 resources. When you launch an instance without specifying a subnet-ID, your instance will be launched in your default VPC.

Q. What are the benefits of a default VPC?

When you launch resources in a default VPC, you can benefit from the advanced networking functionalities of Amazon VPC (EC2-VPC) with the ease of use of Amazon EC2 (EC2-Classic). You can enjoy features such as changing security group membership on the fly, security group egress filtering, multiple IP addresses, and multiple network interfaces without having to explicitly create a VPC and launch instances in the VPC.

Q. What accounts are enabled for default VPC?

If your AWS account was created after March 18, 2013 your account may be able to launch resources in a default VPC. See this Forum Announcement (https://forums.aws.amazon.com/ann.jspa?annID=1875) to determine which regions have been enabled for the default VPC feature set. Also, accounts created prior to the listed dates may utilize default VPCs in any default VPC enabled region in which you've not previously launched EC2 instances or provisioned Amazon Elastic Load Balancing, Amazon RDS, Amazon ElastiCache, or Amazon Redshift resources.

Q. How can I tell if my account is configured to use a default VPC?

The Amazon EC2 console indicates which platforms you can launch instances in for the selected region, and whether you have a default VPC in that region. Verify that the region you'll use is selected in the navigation bar. On the Amazon EC2 console dashboard, look for "Supported Platforms" under "Account Attributes". If there are two values, EC2-Classic and EC2-VPC, you can launch instances into either platform. If there is one value, EC2-VPC, you can launch instances only into EC2-VPC. Your default VPC ID will be listed under "Account Attributes" if your account is configured to use a default VPC. You can also use the EC2 DescribeAccountAttributes API or CLI to describe your supported platforms.

Q. Will I need to know anything about Amazon VPC in order to use a default VPC?

No. You can use the AWS Management Console, AWS EC2 CLI, or the Amazon EC2 API to launch and manage EC2 instances and other AWS resources in a default VPC. AWS will automatically create a default VPC for you and will create a default subnet in each Availability Zone in the AWS region. Your default VPC will be connected to an Internet gateway and your instances will automatically receive public IP addresses, just like EC2-Classic.

Q. What are the differences between instances launched in EC2-Classic and EC2-VPC?

See Differences between EC2-Classic and EC2-VPC (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-vpc.html) in the EC2 User Guide.

Q. Do I need to have a VPN connection to use a default VPC?

No. Default VPCs are attached to the Internet and all instances launched in default subnets in the default VPC automatically receive public IP addresses. You can add a VPN connection to your default VPC if you choose.

Q. Can I create other VPCs and use them in addition to my default VPC?

Yes. To launch an instance into nondefault VPCs you must specify a subnet-ID during instance launch.

Q. Can I create additional subnets in my default VPC, such as private subnets?

Yes. To launch into nondefault subnets, you can target your launches using the console or the --subnet option from the CLI, API, or SDK.

Q. How many default VPCs can I have?

You can have one default VPC in each AWS region where your Supported Platforms attribute is set to "EC2-VPC".

Q. What is the IP range of a default VPC?

The default VPC CIDR is 172.31.0.0/16. Default subnets use /20 CIDRs within the default VPC CIDR.

Q. How many default subnets are in a default VPC?

One default subnet is created for each Availability Zone in your default VPC.

Q. Can I specify which VPC is my default VPC?

Not at this time.

Q. Can I specify which subnets are my default subnets?

Not at this time.

Q. Can I delete a default VPC?

Yes, you can delete a default VPC. Once deleted, you can create a new default VPC directly from the VPC Console or by using the CLI. This will create a new default VPC in the region. This does not restore the previous VPC that was deleted.

Q. Can I delete a default subnet?

Yes, you can delete a default subnet. Once deleted, you can create a new default subnet in the availability zone by

using the CLI or SDK. This will create a new default subnet in the availability zone specified. This does not restore the previous subnet that was deleted.

Q. I have an existing EC2-Classic account. Can I get a default VPC?

The simplest way to get a default VPC is to create a new account in a region that is enabled for default VPCs, or use an existing account in a region you've never been to before, as long as the Supported Platforms attribute for that account in that region is set to "EC2-VPC".

Q. I really want a default VPC for my existing EC2 account. Is that possible?

Yes, however, we can only enable an existing account for a default VPC if you have no EC2-Classic resources for that account in that region. Additionally, you must terminate all non-VPC provisioned Elastic Load Balancers, Amazon RDS, Amazon ElastiCache, and Amazon Redshift resources in that region. After your account has been configured for a default VPC, all future resource launches, including instances launched via Auto Scaling, will be placed in your default VPC. To request your existing account be setup with a default VPC, please go to *Account and Billing -> Service: Account -> Category: Convert EC2 Classic to VPC* and raise a request. We will review your request, your existing AWS services and EC2-Classic presence and guide you through the next steps.

Q. How are IAM accounts impacted by default VPC?

If your AWS account has a default VPC, any IAM accounts associated with your AWS account use the same default VPC as your AWS account.

Elastic Network Interfaces

Q. Can I attach or detach one or more network interfaces to an EC2 instance while it’s running?

Yes.

Q. Can I have more than two network interfaces attached to my EC2 instance?

The total number of network interfaces that can be attached to an EC2 instance depends on the instance type. See the EC2 User Guide for more information on the number of allowed network interfaces per instance type.

Q. Can I attach a network interface in one Availability Zone to an instance in another Availability Zone?

Network interfaces can only be attached to instances residing in the same Availability Zone.

Q. Can I attach a network interface in one VPC to an instance in another VPC?

Network interfaces can only be attached to instances in the same VPC as the interface.

Q. Can I use Elastic Network Interfaces as a way to host multiple websites requiring separate IP addresses on a single instance?

Yes, however, this is not a use case best suited for multiple interfaces. Instead, assign additional private IP addresses to the instance and then associate EIPs to the private IPs as needed.

Q. Will I get charged for an Elastic IP Address that is associated to a network interface but the network interface isn't attached to a running instance?

Yes.

Q. Can I detach the primary interface (eth0) on my EC2 instance?

No. You can attach and detach secondary interfaces (eth1-ethn) on an EC2 instance, but you can't detach the eth0 interface.

Peering Connections

Q. Can I create a peering connection to a VPC in a different region?

Yes. Peering connections can be created with VPCs in different regions. Inter-region VPC peering is available globally in all commercial regions (excluding China).

Q. Can I peer my VPC with a VPC belonging to another AWS account?

Yes, assuming the owner of the other VPC accepts your peering connection request.

Q. Can I peer two VPCs with matching IP address ranges?

No. Peered VPCs must have non-overlapping IP ranges.

Q. How much do VPC peering connections cost?

There is no charge for creating VPC peering connections, however, data transfer across peering connections is charged. See the Data Transfer section of the EC2 Pricing page (http://aws.amazon.com/ec2/pricing/) for data transfer rates.

Q. Can I use AWS Direct Connect or hardware VPN connections to access VPCs I'm peered with?

No. "Edge to Edge routing" isn't supported in Amazon VPC. Refer to the VPC Peering Guide (http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/) for additional information.

Q. Do I need an Internet Gateway to use peering connections?

No. VPC peering connections do not require an Internet Gateway.

Q. Is VPC peering traffic within the region encrypted?

No. Traffic between instances in peered VPCs remains private and isolated – similar to how traffic between two instances in the same VPC is private and isolated.

Q. If I delete my side of a peering connection, will the other side still have access to my VPC?

No. Either side of the peering connection can terminate the peering connection at any time. Terminating a peering connection means traffic won't flow between the two VPCs.

Q. If I peer VPC A to VPC B and I peer VPC B to VPC C, does that mean VPCs A and C are peered?

No. Transitive peering relationships are not supported.

Q. What if my peering connection goes down?

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

Inter-Region VPC Peering operates on the same horizontally scaled, redundant, and highly available technology that powers VPC today. Inter-Region VPC Peering traffic goes over the AWS backbone that has in-built redundancy and dynamic bandwidth allocation. There is no single point of failure for communication.

If an Inter-Region peering connection does go down, the traffic will not be routed over the internet.

Q. Are there any bandwidth limitations for peering connections?

Bandwidth between instances in peered VPCs is no different than bandwidth between instances in the same VPC. Note: A placement group can span peered VPCs; however, you will not get full-bisection bandwidth between instances in peered VPCs. Read more about Placement Groups (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html).

Q. Is Inter-Region VPC Peering traffic encrypted?

Traffic is encrypted using modern AEAD (Authenticated Encryption with Associated Data) algorithms. Key agreement and key management is handled by AWS.

Q. How do DNS translations work with Inter-Region VPC Peering?

By default, a query for a public hostname of an instance in a peered VPC in a different region will resolve to a public

IP address. Route 53 private DNS can be used to resolve to a private IP address with Inter-Region VPC Peering.

Q. Can I reference security groups across an Inter-Region VPC Peering connection?

No. Security groups cannot be referenced across an Inter-Region VPC Peering connection.

Q. Does Inter-Region VPC Peering support with IPv6?

No. Inter-Region VPC Peering does not support IPv6.

Q. Can Inter-Region VPC Peering be used with EC2-Classic Link?

No. Inter-Region VPC Peering cannot be used with EC2-ClassicLink.

Q. Are there AWS Services that cannot be used over Inter-Region VPC Peering?

Network Load Balancers, AWS PrivateLink and Elastic File System cannot be used over Inter-Region VPC Peering.

ClassicLink

Q. What is ClassicLink?

Amazon Virtual Private Cloud (VPC) ClassicLink allows EC2 instances in the EC2-Classic platform to communicate with instances in a VPC using private IP addresses. To use ClassicLink, enable it for a VPC in your account, and associate a Security Group from that VPC with an instance in EC2-Classic. All the rules of your VPC Security Group will apply to communications between instances in EC2-Classic and instances in the VPC.

Q. What does ClassicLink cost?

There is no additional charge for using ClassicLink; however, existing cross Availability Zone data transfer charges will apply. For more information, consult the EC2 pricing page (https://aws.amazon.com/ec2/pricing/).

Q. How do I use ClassicLink?

In order to use ClassicLink, you first need to enable at least one VPC in your account for ClassicLink. Then you associate a Security Group from the VPC with the desired EC2-Classic instance. The EC2-Classic instance is now linked to the VPC and is a member of the selected Security Group in the VPC. Your EC2-Classic instance cannot be linked to more than one VPC at the same time.

Q. Does the EC2-Classic instance become a member of the VPC?

The EC2-Classic instance does not become a member of the VPC. It becomes a member of the VPC Security Group that was associated with the instance. All the rules and references to the VPC Security Group apply to

communication between instances in EC2-Classic instance and resources within the VPC.

Q. Can I use EC2 public DNS hostnames from my EC2-Classic and EC2-VPC instances to address each other, in order to communicate using private IP?

No. The EC2 public DNS hostname will not resolve to the private IP address of the EC2-VPC instance when queried from an EC2-Classic instance, and vice-versa.

Q. Are there any VPCs for which I cannot enable ClassicLink?

Yes. ClassicLink cannot be enabled for a VPC that has a Classless Inter-Domain Routing (CIDR) that is within the 10.0.0.0/8 range, with the exception of 10.0.0.0/16 and 10.1.0.0/16. In addition, ClassicLink cannot be enabled for any VPC that has a route table entry pointing to the 10.0.0.0/8 CIDR space to a target other than "local".

Q. Can traffic from an EC2-Classic instance travel through the Amazon VPC and egress through the Internet gateway, virtual private gateway, or to peered VPCs?

Traffic from an EC2-Classic instance can only be routed to private IP addresses within the VPC. They will not be routed to any destinations outside the VPC, including Internet gateway, virtual private gateway, or peered VPC destinations.

Q. Does ClassicLink affect the access control between the EC2-Classic instance, and other instances that are in the EC2-Classic platform?

ClassicLink does not change the access control defined for an EC2-Classic instance through its existing Security Groups from the EC2-Classic platform.

Q. Will ClassicLink settings on my EC2-Classic instance persist through stop/start cycles?

The ClassicLink connection will not persist through stop/start cycles of the EC2-Classic instance. The EC2-Classic instance will need to be linked back to a VPC after it is stopped and started. However, the ClassicLink connection will persist through instance reboot cycles.

Q. Will my EC2-Classic instance be assigned a new, private IP address after I enable ClassicLink?

There is no new private IP address assigned to the EC2-Classic instance. When you enable ClassicLink on an EC2-Classic instance, the instance retains and uses its existing private IP address to communication with resources in a VPC.

Q: Does ClassicLink allow EC2-Classic Security Group rules to reference VPC Security Groups, or vice versa?

ClassicLink does not allow EC2-Classic Security Group rules to reference VPC Security Groups, or vice versa.

AWS PrivateLink

Q. What is AWS PrivateLink?

AWS PrivateLink enables customers to access services hosted on AWS in a highly available and scalable manner, while keeping all the network traffic within the AWS network. Service users can use this to privately access services powered by PrivateLink from their Amazon Virtual Private Cloud (VPC) or their on-premises, without using public IPs, and without requiring the traffic to traverse across the Internet. Service owners can register their Network Load Balancers to PrivateLink services and provide the services to other AWS customers.

Q. How can I use AWS PrivateLink?

As a service user, you will need to create interface type VPC endpoints for services that are powered by PrivateLink. These service endpoints will appear as Elastic Network Interfaces (ENIs) with private IPs in your VPCs. Once these endpoints are created, any traffic destined to these IPs will get privately routed to the corresponding AWS services.

As a service owner, you can onboard your service to AWS PrivateLink by establishing a Network Load Balancer (NLB) to front your service and create a PrivateLink service to register with the NLB. Your customers will be able to establish endpoints within their VPC to connect to your service after you whitelisted their accounts and IAM roles.

Q. Which services are currently available on AWS PrivateLink?

The following AWS services support this feature: Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Kinesis Streams, Service Catalog, EC2 Systems Manager, Amazon SNS, and AWS DataSync. Many SaaS solutions support this feature as well. Please visit AWS Marketplace (https://aws.amazon.com/marketplace) for more SaaS products powered by AWS PrivateLink.

Q. Can I privately access services powered by AWS PrivateLink over AWS Direct Connect?

Yes. The application in your on-premises can connect to the service endpoints in Amazon VPC over AWS Direct Connect. The service endpoints will automatically direct the traffic to AWS services powered by AWS PrivateLink.

Q. What CloudWatch metrics are available for the interface-based VPC endpoint?

Currently, no CloudWatch metric is available for the interface-based VPC endpoint.

Q. Who pays the data transfer costs for the traffic going via the interface-based VPC endpoint?

The concept of data transfer costs is similar to that of data transfer costs for EC2 instances. Since an interface-based VPC endpoint is an ENI in the subnet, data transfer charges depend on the source of the traffic. If the traffic to this interface is coming from a resource across AZ, EC2 cross-AZ data transfer charges apply to the consumer end. Customers in the consumer VPC can use AZ-specific DNS endpoint to make sure the traffic stays within the same AZ if they have provisioned each AZ available in their account.

Bring Your Own IP

Q. What is the Bring Your Own IP feature?

Bring Your Own IP (BYOIP) enables customers to move all or part of their existing publicly routable IPv4 address space to AWS for use with their AWS resources. Customers will continue to own the IP range, however, AWS will take over its advertisement on the internet. Customers can create Elastic IPs from the IP space they bring to AWS and use them with EC2 instances, NAT Gateways, and Network Load Balancers. Customers will continue to have access to Amazon-supplied IPs and can choose to use BYOIP Elastic IPs, Amazon-supplied IPs, or both.

Q. Why should I use BYOIP?

You may want to bring your own IP addresses to AWS for the following reasons:

IP Reputation: Many customers consider the reputation of their IP addresses to be a strategic asset and want to use those IPs on AWS with their resources. For example, customers who maintain services such as outbound e-mail MTA and have high reputation IPs, can now bring over their IP space and successfully maintain their existing sending success rate.

Customer whitelisting: BYOIP also enables customers to move workloads that rely on IP address whitelisting to AWS without the need to re-establish the whitelists with new IP addresses.

Hardcoded dependencies: Several customers have IPs hardcoded in devices or have taken architectural dependencies on their IPs. BYOIP enables such customers hassle free migration to AWS.

Regulation and compliance: Many customers are required to use certain IPs because of regulation and compliance reasons. They too are unlocked by BYOIP.

Q. How can I use IP addresses from a BYOIP prefix with AWS resources?

Your BYOIP prefix will show as an IP pool in your account. You can create Elastic IPs (EIPs) from the IP pool and use them like regular Elastic IPs (EIPs) with any AWS resource that supports EIPs. Currently, EC2 instances, NAT Gateways, and Network Load Balancers support EIPs.

Q. What happens if I release a BYOIP Elastic IP?

When you release a BYOIP Elastic IP it goes back to the BYOIP IP pool from which it was allocated.

Q. In which AWS Regions is BYOIP available?

The feature is currently available in the US-East (N.Virginia), US-East (Ohio), US-West (Oregon), EU (Dublin), EU (London), EU (Frankfurt), and Canada (Central) AWS Regions.

Q. Can a BYOIP prefix be shared with multiple VPCs in the same account?

Yes. You can use the BYOIP prefix with any number of VPCs in the same account.

Q. How many IP ranges can I bring via BYOIP?

You can bring a maximum of five IP ranges to your account.

Q. What is the most specific prefix that I can bring via BYOIP?

The most specific prefix you can bring via BYOIP is a /24 IPv4 prefix.

Q. Which RIR prefixes can I use for BYOIP?

You can use ARIN and RIPE registered prefixes.

Q. Can I bring a reassigned or reallocated prefix?

We are not accepting reassigned or reallocated prefixes at this time. IP ranges should be a net type of direct allocation or direct assignment.

Q. Can I move a BYOIP prefix from one AWS Region to another?

Yes. You can do that by de-provisioning the BYOIP prefix from the current region and then provisioning it to the new region.

Additional Questions

Q. Can I use the AWS Management Console to control and manage Amazon VPC?

Yes. You can use the AWS Management Console to manage Amazon VPC objects such as VPCs, subnets, route tables, Internet gateways, and IPSec VPN connections. Additionally, you can use a simple wizard to create a VPC.

Q. How many VPCs, subnets, Elastic IP addresses, and internet gateways can I create?

You can have:

- Five Amazon VPCs per AWS account per region
- Two hundred subnets per Amazon VPC
- Five Amazon VPC Elastic IP addresses per AWS account per region
- One internet gateway per Amazon VPC

See the Amazon VPC user guide (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html) for more information on VPC limits.

Q. Can I obtain AWS support with Amazon VPC?

Yes. Click here (http://aws.amazon.com/premiumsupport/) for more information on AWS support.

Q. Can I use ElasticFox (http://sourceforge.net/projects/elasticfox/) with Amazon VPC?

ElasticFox is no longer officially supported for managing your Amazon VPC. Amazon VPC support is available via the AWS APIs, command line tools, and the AWS Management Console, as well as a variety of third-party utilities.

Learn more about Amazon VPC

Visit the product detail page (https://aws.amazon.com/vpc/details/)
Ready to get started?
Sign up (https://portal.aws.amazon.com/gp/aws/developer/registration/index.html)
Have more questions?
Contact us (https://aws.amazon.com/contact-us/)
Page Content
General Questions Billing Connectivity IP Addressing Topology Security & Filtering VPC Traffic Mirroring Amazon VPC & EC2 Default VPCs Elastic Network Interfaces Peering Connections ClassicLink AWS PrivateLink Bring Your Own IP Additional Questions

aws.amazon.com (https://aws.amazon.com/vpc/faqs/)