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.

- **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:

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 of the Amazon VPC product page.

Q. What defines billable VPN connection-hours?

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.

Connectivity

Q. What are the connectivity options for my VPC?

You may connect your VPC to:

- The Internet (via an Internet gateway)
- Your corporate data center using a Hardware 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 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. 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. How does a hardware VPN connection work with Amazon VPC?

A hardware 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 a hardware VPN connection.

Q. What is IPsec?

- Utilize the SHA-1 or SHA-2 (256) hashing function
- Utilize Diffie-Hellman (DH) Perfect Forward Secrecy in "Group 2" mode, or one of the additional DH groups we support
- Perform packet fragmentation prior to encryption

In addition to the above capabilities, devices supporting dynamically-routed VPN connections must be able to:

- Establish Border Gateway Protocol (BGP) peerings
- Bind tunnels to logical interfaces (route-based VPN)
- Utilize IPsec Dead Peer Detection

Q. Which Diffie-Hellman groups do you support?

We support the following Diffie-Hellman (DH) groups in Phase1 and Phase2.

- Phase1 DH groups 2, 14-18, 22, 23, 24
- Phase2 DH groups 2, 5, 14-18, 22, 23, 24

Q. What customer gateway devices are known to work with Amazon VPC?

The following devices meeting the aforementioned requirements are known to work with hardware VPN connections, and have support in the command line tools for automatic generation of configuration files appropriate for your device:

- Statically-routed VPN connections:
  - Cisco ASA 5500 Series version 8.2 (or later) software

- Juniper J-Series Service Router running JunOS 9.5 (or later) software
- Juniper SRX-Series Services Gateway running JunOS 9.5 (or later) software
- Juniper SSG running ScreenOS 6.1, or 6.2 (or later) software
- Juniper ISG running ScreenOS 6.1, or 6.2 (or later) software
- Microsoft Windows Server 2008 R2 or 2012 R2 software
- Netgate pfSense running OS 2.2.5 (or later) software
- Palo Alto Networks PANOS running 4.1.2 (or later), or 7.0 (or later) software
- WatchGuard XTM, Firebox Fireware OS 11.11.4 software
- Yamaha RTX Routers Rev.10.01.16 (or later) software
- Zyxel Zywall Series running 4.20 (or later) software

- Dynamically-routed VPN connections (requires BGP)
  - Barracuda NextGen Firewall F-Series running 6.2 (or later) software
  - Check Point Security Gateway running R77.10 (or later) software
  - Cisco ISR running Cisco IOS 12.4 (or later) software
  - Dell SonicWALL Next Generation Firewalls (TZ, NSA, SuperMassive Series) running SonicOS5.9 (or later)
  - F5 Big-IP v12.0.0 (or later) software
  - Fortinet Fortigate 40+ Series running FortiOS 4.0 (or later), or 5.0 (or later) software

- Vyatta Network OS 6.5 (or later) software
- Yamaha RTX Routers Rev.10.01.16 (or later) software
- Zyxel Zywall Series running 4.30 (or later) software

Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2. You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups.

Q. If my device is not listed, where can I go for more information about using it with Amazon VPC?

We recommend checking the Amazon VPC forum as other customers may be already using your device.

Q. What is the approximate maximum throughput of a VPN connection?

VGW supports IPSEC VPN throughput upto 1.25 Gbps. Multiple VPN connections to the same VPC are cumulatively bound by the VGW throughput of 1.25 Gbps.

Q. What factors affect the throughput of my VPN connection?

VPN connection throughput can depend on multiple factors, such as the capability of your Customer Gateway (CGW), the capacity of your connection, average packet size, the protocol being used (TCP vs. UDP), and the network latency between your CGW and the Virtual Private Gateway (VGW).

Q. What tools are available to me to help troubleshoot my Hardware VPN configuration?

Yes, you will need to enable NAT-T and open UDP port 4500 on your NAT device.

Q. What IP address do I use for my CGW address?

You will use the public IP address of your NAT device.

Q. How do I disable NAT-T on my connection?

You will need to disable NAT-T on your device. If you don't plan on using NAT-T and it is not disabled on your device, we will attempt to establish a tunnel over UDP port 4500. If that port is not open the tunnel will not establish.

Q: I would like to have multiple CGWs behind a NAT, what do I need to do to configure that?

You will use the public IP address of your NAT device for the CGW for each of your connections. You will also need to make sure UDP port 4500 is open.

Q: How many IPsec security associations can be established concurrently per tunnel?

The AWS VPN service is a route-based solution, so when using a route-based configuration you will not run into SA limitations. If, however, you are using a policy-based solution you will need to limit to a single SA, as the service is a route-based solution.

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 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 hardware VPN, and to my VPC?

Yes, you can route traffic via the hardware 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 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.

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.

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 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.

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

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 the Amazon VPC Flow Logs feature to monitor the network traffic in your VPC.

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.

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.

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.

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 page for further details.

Q. Can I employ Amazon CloudWatch within Amazon VPC?

Yes.

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 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

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

See Differences between EC2-Classic and EC2-VPC 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.

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. 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?

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 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 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?

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.

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?

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.

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.

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?

There is no additional charge for this feature.

Q. How can I configure/assign my ASN to be advertised as Amazon side ASN?

You can configure/assign an ASN to be advertised as the Amazon side ASN during creation of the new Virtual Private Gateway (VGW). You can create a VGW using the VPC console or a EC2/CreateVpnGateway API call.

Q. What ASN did Amazon assign prior to this feature?

Amazon assigned the following ASNs: EU West (Dublin) 9059; Asia Pacific (Singapore) 17493 and Asia Pacific (Tokyo) 10124. All other regions were assigned an ASN of 7224; these ASNs are referred as “legacy public ASN” of the region.

Q. Can I use any ASN – public and private?

You can assign any private ASN to the Amazon side. You can assign the "legacy public ASN" of the region until June 30th 2018, you cannot assign any other public ASN. After June 30th 2018, Amazon will provide an ASN of 64512.

Q. Why can’t I assign a public ASN for the Amazon half of the BGP session?

Amazon is not validating ownership of the ASNs, therefore, we’re limiting the Amazon-side ASN to private ASNs. We want to protect customers from BGP spoofing.

Q. What ASN can I choose?

Amazon will provide an ASN for the VGW if you don't choose one. Until June 30th 2018, Amazon will continue to provide the "legacy public ASN" of the region. After June 30th 2018, Amazon will provide an ASN of 64512.

Q. Where can I view the Amazon side ASN?

You can view the Amazon side ASN in the VGW page of VPC console and in the response of EC2/DescribeVpnGateways API.

Q. If I have a public ASN, will it work with a private ASN on the AWS side?

Yes, you can configure the Amazon side of the BGP session with a private ASN and your side with a public ASN.

Q. I have private VIFs already configured and want to set a different Amazon side ASN for the BGP session on an existing VIF. How can I make this change?

You will need to create a new VGW with desired ASN, and create a new VIF with the newly created VGW. Your device configuration also needs to change appropriately.

Q. I have VPN connections already configured and want to modify the Amazon side ASN for the BGP session of these VPNs. How can I make this change?

You will need to create a new VGW with the desired ASN, and recreate your VPN connections between your Customer Gateways and the newly created VGW.

region. After June 30th 2018, Amazon will provide an ASN of 64512.

Q. I have a VGW and a private VIF/VPN connection configured using an Amazon assigned public ASN of 7224. If Amazon auto generates the ASN for the new private VIF/VPN connection using the same VGW, what Amazon side ASN will I be assigned?

Amazon will assign 7224 to the Amazon side ASN for the new VIF/VPN connection. The Amazon side ASN for your new private VIF/VPN connection is inherited from your existing VGW and defaults to that ASN.

Q. I'm attaching multiple private VIFs to a single VGW. Can each VIF have a separate Amazon side ASN?

No, you can assign/configure separate Amazon side ASN for each VGW, not each VIF. Amazon side ASN for VIF is inherited from the Amazon side ASN of the attached VGW.

Q. I'm creating multiple VPN connections to a single VGW. Can each VPN connection have a separate Amazon side ASN?

No, you can assign/configure separate Amazon side ASN for each VGW, not each VPN connection. Amazon side ASN for VPN connection is inherited from the Amazon side ASN of the VGW.

Q. Where can I select my own ASN?

When creating a VGW in the VPC console, uncheck the box asking if you want an auto-generated Amazon BGP ASN and provide your own private ASN for the Amazon half of the BGP session. Once VGW is configured with Amazon side ASN, the private VIFs or VPN connections created using the VGW will use your Amazon side ASN.

No. You can do this with the same API as before (EC2/CreateVpnGateway). We just added a new parameter (amazonSideAsn) to this API.

Q. Is there a new API to view the Amazon side ASN?

No. You can view the Amazon side ASN with the same EC2/DescribeVpnGateways API. We just added a new parameter (amazonSideAsn) to this API.

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

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?

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), and US-West (Oregon) AWS Regions.

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

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, Internet gateways, customer gateways, virtual private gateways, and VPN connections can I create?

You can have:

- Five Amazon VPCs per AWS account per region
- Two hundred subnets per Amazon VPC

Yes. Click here for more information on AWS Support.

Q. Can I use 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

Ready to get started?

Sign up

Have more questions?

Contact us

Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services

.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Quick Starts

Manage Your Account

Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon VPC

Overview

Features

Pricing

Getting Started

Resources

FAQs