**AWS NOTES - SHREYAS**

<https://aws.amazon.com/iam/faqs/?nc=sn&loc=5>

<https://aws.amazon.com/s3/faqs/?nc=sn&loc=7>

<https://aws.amazon.com/vpc/faqs/>

<https://aws.amazon.com/ec2/faqs/>

<https://aws.amazon.com/ec2/autoscaling/faqs/>

<https://aws.amazon.com/autoscaling/faqs/>

<https://aws.amazon.com/elasticloadbalancing/faqs/?nc=sn&loc=6>

**VPC**

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.

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.

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. 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. 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. 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.

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. 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.

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.

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).

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. 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.

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.

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. 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. 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 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. 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.

With EC2-Classic, your instances run in a single, flat network that you share with other customers. With Amazon VPC, your instances run in a virtual private cloud (VPC) that's logically isolated to your AWS account.

The EC2-Classic platform was introduced in the original release of Amazon EC2. If you created your AWS account after 2013-12-04, it does not support EC2-Classic, so you must launch your Amazon EC2 instances in a VPC.

If your account does not support EC2-Classic, we create a default VPC for you. By default, when you launch an instance, we launch it into your default VPC. Alternatively, you can create a nondefault VPC and specify it when you launch an instance.

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. 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 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 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 does not restore the previous subnet that was deleted.

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

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

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.

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

Yes.

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. How much do VPC peering connections cost?

There is no charge for creating VPC peering connections, however, data transfer across peering connections is charged.

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.

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

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

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. Does Inter-Region VPC Peering support with IPv6?

No.

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.

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

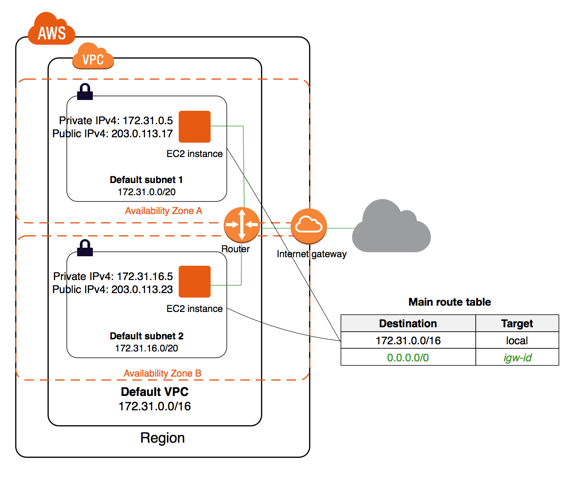
You can have:

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

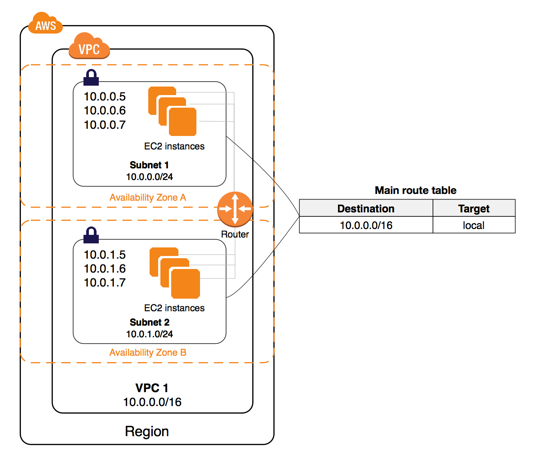
One internet gateway per Amazon VPC



By default, each instance that you launch into a nondefault subnet has a private IPv4 address, but no

public IPv4 address, unless you specifically assign one at launch, or you modify the subnet's public IP

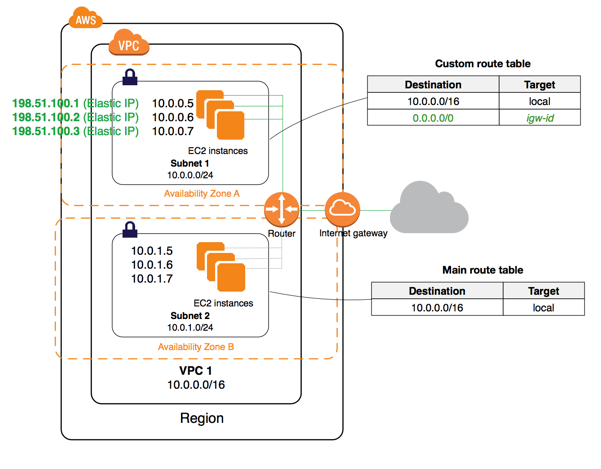
address attribute. These instances can communicate with each other, but can't access the internet.



You can enable internet access for an instance launched into a nondefault subnet by attaching an

internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the

instance.



Alternatively, to allow an instance in your VPC to initiate outbound connections to the internet but

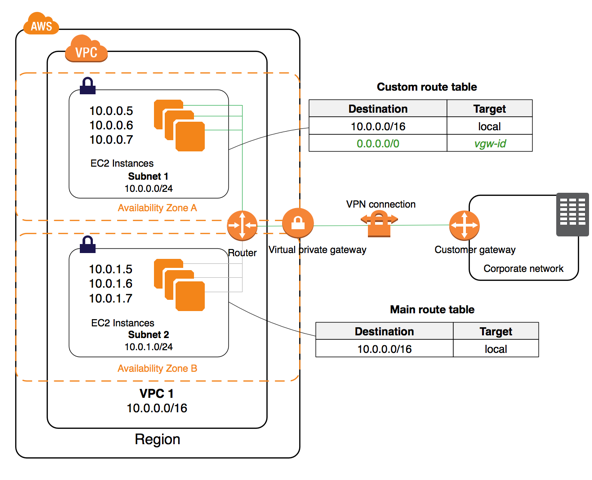
prevent unsolicited inbound connections from the internet, you can use a network address translation

(NAT) device for IPv4 traffic. NAT maps multiple private IPv4 addresses to a single public IPv4 address. A

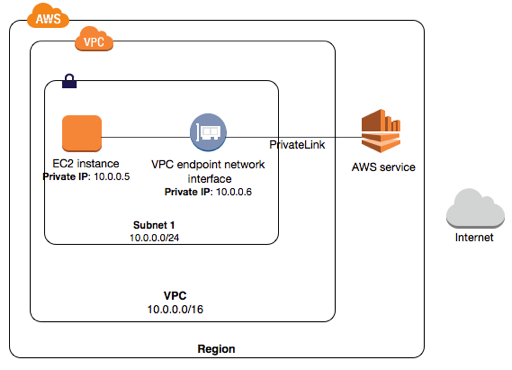
NAT device has an Elastic IP address and is connected to the internet through an internet gateway. You

can connect an instance in a private subnet to the internet through the NAT device, which routes traffic

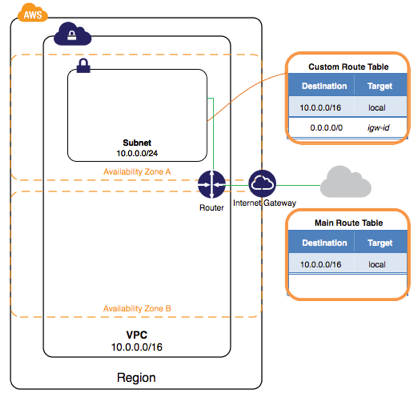
from the instance to the internet gateway, and routes any responses to the instance.



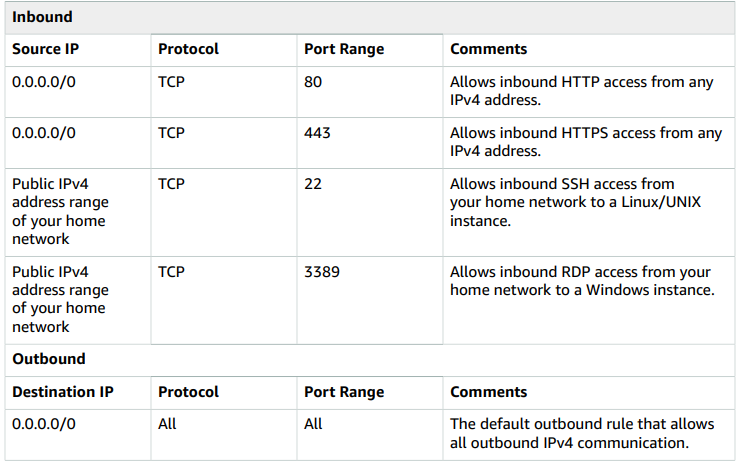
Accessing a Corporate or Home Network



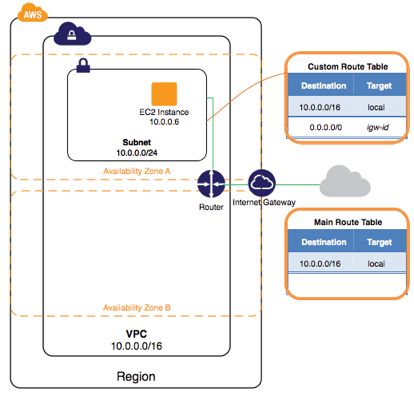
You can create your own AWS PrivateLink-powered service (endpoint service) and enable other AWS customers to access your service.



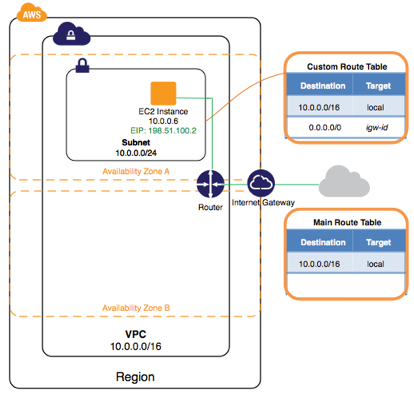
Create the VPC



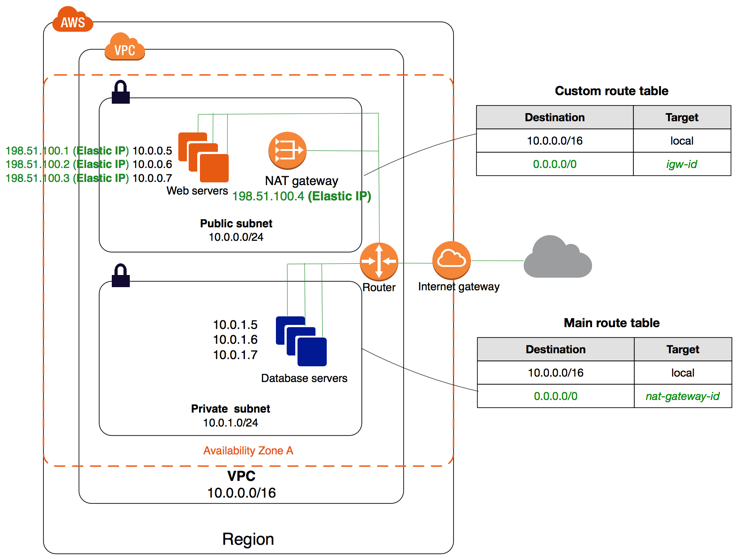
Security Group Rules



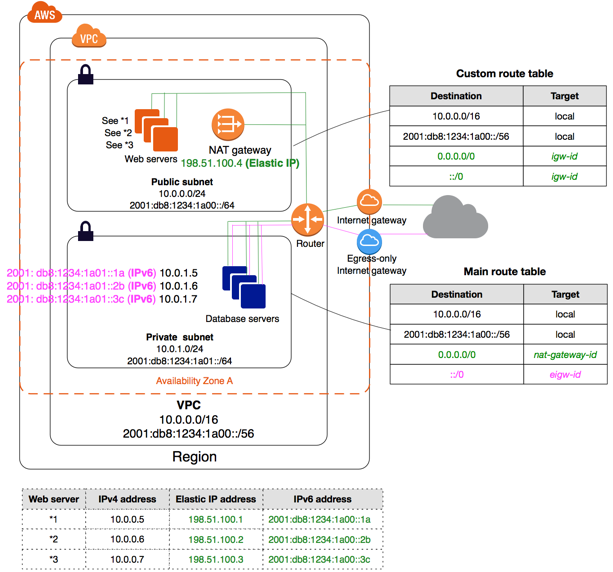
Launch an Instance into Your VPC



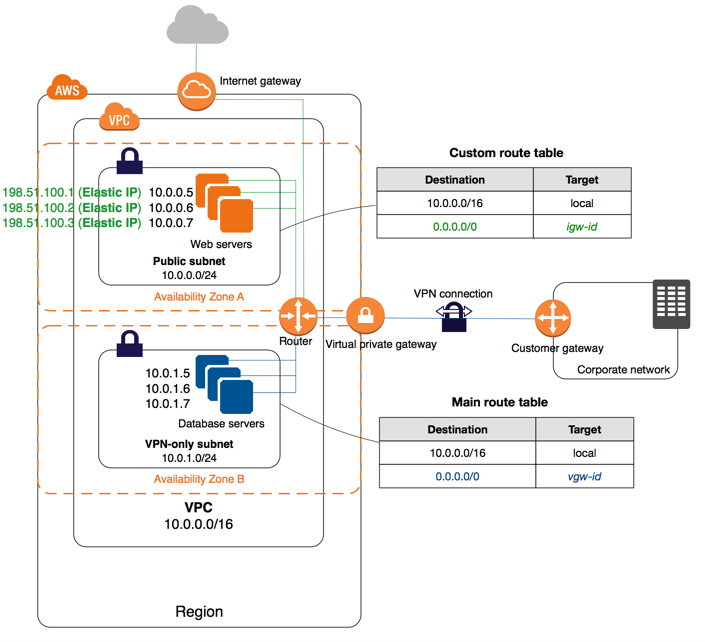
Assign an Elastic IP Address to Your Instance



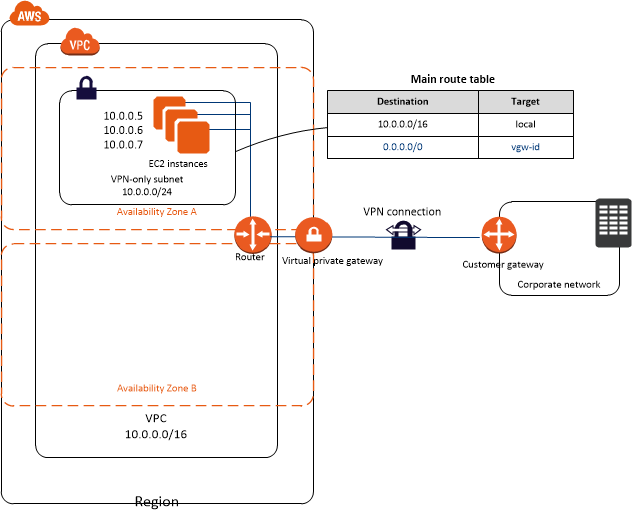
VPC with Public and Private Subnets (NAT) – IPv4



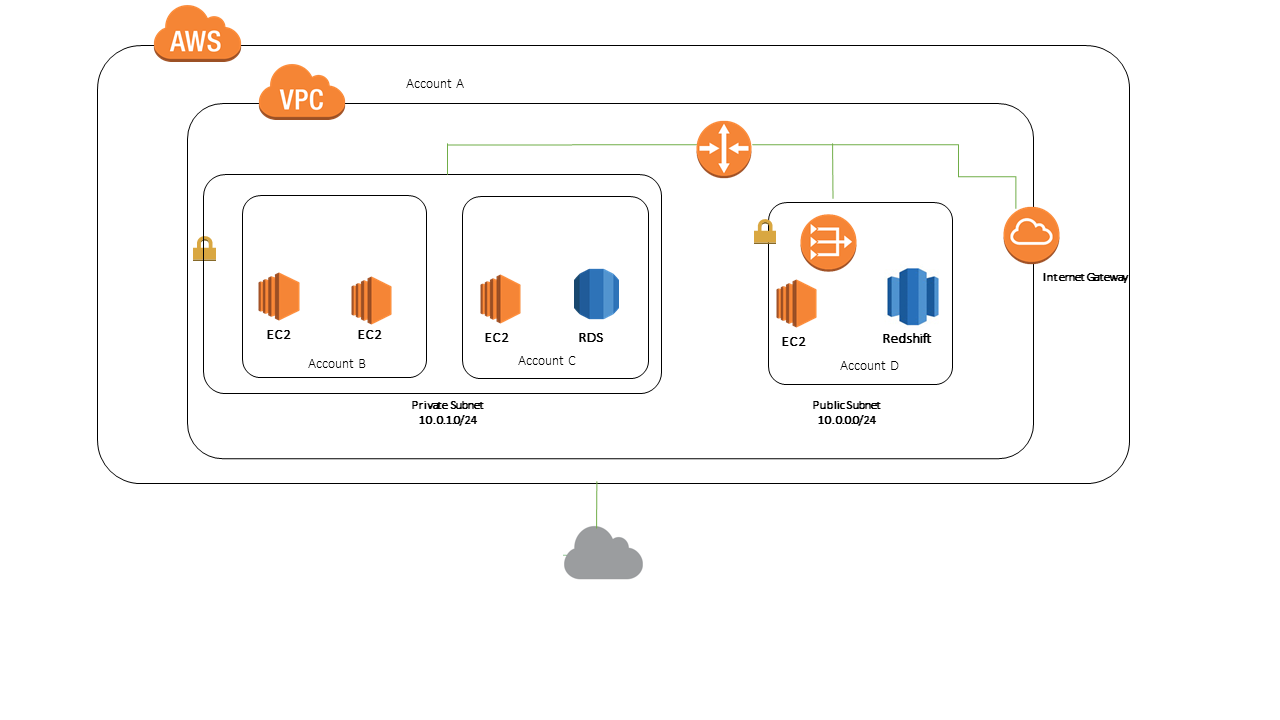
VPC with Public and Private Subnets (NAT) – IPv6



VPC with Public and Private Subnets and AWS Site-to-Site VPN Access

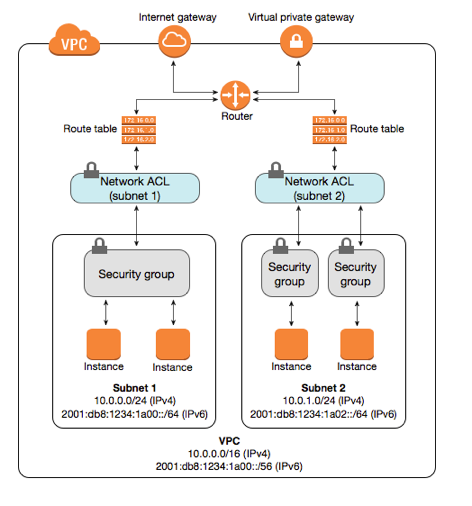


VPC with a Private Subnet Only and AWS Site-to-Site VPN Access



Example: Sharing Public Subnets and Private

Subnets



Security Groups and Network ACLs

**VPC DEMO**

1) create VPC

- name

- ip4 cidr block 10.0.0.0/16

- tenancy default

If you delete default VPC. You have to contact amazon.

**Security Groups -** at instance level

**NACL**

- between route table and subnet

- at subnet level

- rule 100 - allow/deny

**create vpc**

= it will create default route table, security group, NACL

= it will not create subnet, IGW, NAT

2) create 2 public and private subnets

VPC address range 10.0.0.0/16

Public subnets address range 10.0.1.0/24, 10.0.2.0/24

Private subnets address range 10.0.3.0/24, 10.0.4.0/24

3) create internet gateway and attach it to the VPC.

4) create a public and private route table

add routes in the route tables

0.0.0.0/0 target-igw

click public route table - add public subnets

click private route table - add private subnets

5) create NAT gateway

add routes to private route table (NOT PUBLIC, though NAT instance and NAT gateway needs to be put in public subnet)

6) create NACL

default rule 100 allow

create rule 200 allow/deny

create public NACL - add public subnets

create private NACL - add private subnets

in private NACL - database exists -

add rule 100 - RDP - 3389

add rule 200 - MY SQL - 1433

7) create private security group

inbound rules:

MS SQL

RDP

create public security group

inbound rules:

SSH

HTTP

HTTPS

8) Launch 2 EC2 instances.

Create web server in public subnet and database server in private subnet.

a. WEB SERVER

select default VPC

select public subnet

auto-assign ip = enable

b. DATABASE SERVER

select default VPC

select private subnet

auto-assign ip = disable

To delete VPC,

Delete/terminate EC2 instances

Delete/terminate NAT gateways

Delete/release elastic IPs

When you delete a VPC, below components will be deleted

subnets

security groups

NACLs

IGW

egress only IGW

route tables

network interfaces

peering connections

endpoints

To connect AWS to on-premise, use hardware VPN or AWS Direct Connect

AWS Snowmobile

<https://www.youtube.com/watch?v=8vQmTZTq7nw>

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-instance-metadata.html

**IAM**

IAM login

using console, cli, sdk

programmatic access - cli, sdk

management console - browser

AWS CLI Commands

aws --version

aws configure = options: table, json, text

aws iam list-users

iam > policies >

add users > rajesh, suresh

delete default AdministratorAccess policy.

groups > dev

**AMI**

AMI 2 types

Instance Store = template stored in s3 = ephemeral storage

EBS Store = root volumes

linux AMIs 2 types of virtualization

PV

HVM

**EC2**

Q: How many instances can I run in Amazon EC2?

You are limited to running up to a total of 20 On-Demand instances across the instance family, purchasing 20 Reserved Instances, and requesting Spot Instances per your dynamic Spot limit per region.

Q: What are Accelerated Computing instances?

Accelerated Computing instance family is a family of instances which use hardware accelerators, or co-processors, to perform some functions, such as floating-point number calculation and graphics processing, more efficiently than is possible in software running on CPUs. Amazon EC2 provides three types of Accelerated Computing instances – GPU compute instances for general-purpose computing, GPU graphics instances for graphics intensive applications, and FPGA programmable hardware compute instances for advanced scientific workloads.

Q. When should I use Compute Optimized instances?

Compute Optimized instances are designed for applications that benefit from high compute power. These applications include compute-intensive applications like high-performance web servers, high-performance computing (HPC), scientific modelling, distributed analytics and machine learning inference.

Q: What are Amazon EC2 A1 instances?

Amazon EC2 A1 instances are new general purpose instances powered by the AWS Graviton Processors that are custom designed by AWS.

Q: How are Burstable Performance Instances different?

Amazon EC2 allows you to choose between Fixed Performance Instances (e.g. C, M and R instance families) and Burstable Performance Instances (e.g. T2). Burstable Performance Instances provide a baseline level of CPU performance with the ability to burst above the baseline.

Q: Which instance types offer NVMe instance storage?

Today, I3en, I3, C5d, M5d, M5ad, R5d, R5ad, z1d, and F1 instances offer NVMe instance storage.

Q: How does Elastic Fabric Adapter (EFA) communication work?

EFA devices provide all ENA devices functionalities plus a new OS bypass hardware interface that allows user-space applications to communicate directly with the hardware-provided reliable transport functionality. Most applications will use existing middleware, such as the Message Passing Interface (MPI), to interface with EFA.

Q: Why am I charged when my Elastic IP address is not associated with a running instance?

In order to help ensure our customers are efficiently using the Elastic IP addresses, we impose a small hourly charge for each address when it is not associated to a running instance.

Q: Do I need one Elastic IP address for every instance that I have running?

No. You do not need an Elastic IP address for all your instances. By default, every instance comes with a private IP address and an internet routable public IP address. The private IP address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated. The public address is associated exclusively with the instance until it is stopped, terminated or replaced with an Elastic IP address.

Q: Why should I hibernate an instance?

You can hibernate an instance to get your instance and applications up and running quickly, if they take long time to bootstrap (e.g. load memory caches). You can start instances, bring them to a desired state and hibernate them. These “pre-warmed” instances can then be resumed to reduce the time it takes for an instance to return to service. Hibernation retains memory state across Stop/Start cycles.

Q: What is the difference between hibernate and stop?

In the case of hibernate, your instance gets hibernated and the RAM data persisted. In the case of Stop, your instance gets shutdown and RAM is cleared.

In both the cases, data from your EBS root volume and any attached EBS data volumes is persisted. Your private IP address remains the same, as does your elastic IP address (if applicable). The network layer behavior will be similar to that of EC2 Stop-Start workflow. Stop and hibernate are available for Amazon EBS backed instances only. Local instance storage is not persisted.

Q: How can I hibernate an instance?

Hibernation needs to be enabled when you launch the instance. Once enabled, you can use the StopInstances API with an additional ‘Hibernate’ parameter to trigger hibernation. You can also do this through the console by selecting your instance, then clicking Actions> Instance State > Stop - Hibernate.

Q. What is VM Import/Export?

VM Import/Export enables customers to import Virtual Machine (VM) images in order to create Amazon EC2 instances. Customers can also export previously imported EC2 instances to create VMs.

Q. What virtual machine file formats are supported?

You can import VMware ESX VMDK images, Citrix Xen VHD images, Microsoft Hyper-V VHD images and RAW images as Amazon EC2 instances.

You can export EC2 instances to VMware ESX VMDK, VMware ESX OVA, Microsoft Hyper-V VHD or Citrix Xen VHD images.

Q. What is VMDK?

VMDK is a file format that specifies a virtual machine hard disk encapsulated within a single file. It is typically used by virtual IT infrastructures such as those sold by VMware, Inc.

Q. What is VHD?

VHD (Virtual Hard Disk) is a file format that that specifies a virtual machine hard disk encapsulated within a single file. The VHD image format is used by virtualization platforms such as Microsoft Hyper-V and Citrix Xen.

Q. How do I import a virtual machine to an Amazon EC2 instance?

You can import your VM images using the Amazon EC2 API tools:

Import the VMDK, VHD or RAW file via the ec2-import-instance API. The import instance task captures the parameters necessary to properly configure the Amazon EC2 instance properties (instance size, Availability Zone, and security groups) and uploads the disk image into Amazon S3.

If ec2-import-instance is interrupted or terminates without completing the upload, use ec2-resume-import to resume the upload. The import task will resume where it left off.

Use the ec2-describe-conversion-tasks command to monitor the import progress and obtain the resulting Amazon EC2 instance ID.

Once your import task is completed, you can boot the Amazon EC2 instance by specifying its instance ID to the ec2-run-instances API.

Finally, use the ec2-delete-disk-image command line tool to delete your disk image from Amazon S3 as it is no longer needed.

Alternatively, if you use the VMware vSphere virtualization platform, you can import your virtual machine to Amazon EC2 using a graphical user interface provided through AWS Management Portal for vCenter.

Q: What is a Convertible RI?

A Convertible RI is a type of Reserved Instance with attributes that can be changed during the term.

Like Standard RIs, Convertible RIs are available for purchase for a one-year or three-year term.

Q. What is Amazon EC2 Fleet?

With a single API call, EC2 Fleet lets you provision compute capacity across different instance types, Availability Zones and across On-Demand, Reserved Instances (RI) and Spot Instances purchase models to help optimize scale, performance and cost.

Q. What is the Reserved Instance Marketplace?

The Reserved Instance Marketplace is an online marketplace that provides AWS customers the flexibility to sell their Amazon Elastic Compute Cloud (Amazon EC2) Reserved Instances to other businesses and organizations. Customers can also browse the Reserved Instance Marketplace to find an even wider selection of Reserved Instance term lengths and pricing options sold by other AWS customers.

Q. What is a Spot Instance?

Spot Instances are spare EC2 capacity that can save you up 90% off of On-Demand prices that AWS can interrupt with a 2-minute notification. Spot uses the same underlying EC2 instances as On-Demand and Reserved Instances, and is best suited for fault-tolerant, flexible workloads. Spot Instances provides an additional option for obtaining compute capacity and can be used along with On-Demand and Reserved Instances.

Q. How is a Spot Instance different than an On-Demand instance or Reserved Instance?

While running, Spot Instances are exactly the same as On-Demand or Reserved instances. The main differences are that Spot Instances typically offer a significant discount off the On-Demand prices, your instances can be interrupted by Amazon EC2 for capacity requirements with a 2-minute notification, and Spot prices adjust gradually based on long term supply and demand for spare EC2 capacity.

Q: How do I select the right instance type?

Amazon EC2 instances are grouped into 5 families: General Purpose, Compute Optimized, Memory Optimized, Storage Optimized and Accelerated Computing instances.

General Purpose Instances have memory to CPU ratios suitable for most general purpose applications and come with fixed performance (M5, M4) or burstable performance (T2);

Compute Optimized instances (C5, C4) have proportionally more CPU resources than memory (RAM) and are well suited for scale out compute-intensive applications and High Performance Computing (HPC) workloads;

Memory Optimized Instances (X1e, X1, R4) offer larger memory sizes for memory-intensive applications, including database and memory caching applications;

Accelerating Computing instances (P3, P2, G3, F1) take advantage of the parallel processing capabilities of NVIDIA Tesla GPUs for high performance computing and machine/deep learning;

GPU Graphics instances (G3) offer high-performance 3D graphics capabilities for applications using OpenGL and DirectX;

F1 instances deliver Xilinx FPGA-based reconfigurable computing;

Storage Optimized Instances (H1, I3, I3en, D2) that provide very high, low latency, I/O capacity using SSD-based local instance storage for I/O-intensive applications, with D2 or H1, the dense-storage and HDD-storage instances, provide local high storage density and sequential I/O performance for data warehousing, Hadoop and other data-intensive applications.

When choosing instance types, you should consider the characteristics of your application with regards to resource utilization (i.e. CPU, Memory, Storage) and select the optimal instance family and instance size.

Q. What is the Nitro Hypervisor?

The launch of C5 instances introduced a new hypervisor for Amazon EC2, the Nitro Hypervisor. As a component of the Nitro system, the Nitro Hypervisor primarily provides CPU and memory isolation for EC2 instances. VPC networking and EBS storage resources are implemented by dedicated hardware components, Nitro Cards that are part of all current generation EC2 instance families. The Nitro Hypervisor is built on core Linux Kernel-based Virtual Machine (KVM) technology, but does not include general-purpose operating system components.

**Elastic Block Store (EBS)**

Q: What happens to my data when a system terminates?

The data stored on a local instance store will persist only as long as that instance is alive. However, data that is stored on an Amazon EBS volume will persist independently of the life of the instance.

Therefore, we recommend that you use the local instance store for temporary data and, for data requiring a higher level of durability, we recommend using Amazon EBS volumes or backing up the data to Amazon S3.

If you are using an Amazon EBS volume as a root partition, you will need to set the Delete On Terminate flag to "N" if you want your Amazon EBS volume to persist outside the life of the instance.

Q: What are Throughput Optimized HDD (st1) and Cold HDD (sc1) volume types?

ST1 volumes are backed by hard disk drives (HDDs) and are ideal for frequently accessed, throughput intensive workloads with large datasets and large I/O sizes, such as MapReduce, Kafka, log processing, data warehouse, and ETL workloads. These volumes deliver performance in terms of throughput, measured in MB/s, and include the ability to burst up to 250 MB/s per TB, with a baseline throughput of 40 MB/s per TB and a maximum throughput of 500 MB/s per volume. ST1 is designed to deliver the expected throughput performance 99% of the time and has enough I/O credits to support a full-volume scan at the burst rate.

SC1 volumes are backed by hard disk drives (HDDs) and provides the lowest cost per GB of all EBS volume types. It is ideal for less frequently accessed workloads with large, cold datasets. Similar to st1, sc1 provides a burst model: these volumes can burst up to 80 MB/s per TB, with a baseline throughput of 12 MB/s per TB and a maximum throughput of 250 MB/s per volume. For infrequently accessed data, sc1 provides extremely inexpensive storage. SC1 is designed to deliver the expected throughput performance 99% of the time and has enough I/O credits to support a full-volume scan at the burst rate.

Q: Do you support multiple instances accessing a single volume?

While you are able to attach multiple volumes to a single instance, attaching multiple instances to one volume is not supported at this time.

Q: Do volumes need to be un-mounted in order to take a snapshot? Does the snapshot need to complete before the volume can be used again?

No, snapshots can be done in real time while the volume is attached and in use. However, snapshots only capture data that has been written to your Amazon EBS volume, which might exclude any data that has been locally cached by your application or OS.

In order to ensure consistent snapshots on volumes attached to an instance, we recommend cleanly detaching the volume, issuing the snapshot command, and then reattaching the volume.

For Amazon EBS volumes that serve as root devices, we recommend shutting down the machine to take a clean snapshot.

Q: Are snapshots versioned? Can I read an older snapshot to do a point-in-time recovery?

Each snapshot is given a unique identifier, and customers can create volumes based on any of their existing snapshots.

Q: What charges apply when using Amazon EBS shared snapshots?

If you share a snapshot, you won’t be charged when other users make a copy of your snapshot. If you make a copy of another user’s shared volume, you will be charged normal EBS rates.

Q: Can users of my Amazon EBS shared snapshots change any of my data?

Users who have permission to create volumes based on your shared snapshots will first make a copy of the snapshot into their account. Users can modify their own copies of the data, but the data on your original snapshot and any other volumes created by other users from your original snapshot will remain unmodified.

Q: How can I discover Amazon EBS snapshots that have been shared with me?

You can find snapshots that have been shared with you by selecting “Private Snapshots” from the viewing dropdown in the Snapshots section of the AWS Management Console. This section will list both snapshots you own and snapshots that have been shared with you.

Q: How can I find what Amazon EBS snapshots are shared globally?

You can find snapshots that have been shared globally by selecting “Public Snapshots” from the viewing dropdown in the Snapshots section of the AWS Management Console.

Q: Do you offer encryption on Amazon EBS volumes and snapshots?

Yes.

**Elastic File System (EFS)**

Q. How do I access a file system from an Amazon EC2 instance?

To access your file system, you mount the file system on an Amazon EC2 Linux-based instance using the standard Linux mount command and the file system’s DNS name. Once you’ve mounted, you can work with the files and directories in your file system just like you would with a local file system.

Amazon EFS uses the NFSv4.1 protocol.

Q. How do I access my file system from outside my VPC?

Amazon EC2 instances within your VPC can access your file system directly, and Amazon EC2 Classic instances outside your VPC can mount a file system via ClassicLink. On-premises servers can mount your file systems via an AWS Direct Connect connection to your VPC.

**Elastic Load Balancing**

Q: How do I decide which load balancer to select for my application?

A: Elastic Load Balancing supports three types of load balancers. You can select the appropriate load balancer based on your application needs. If you need to load balance HTTP requests, we recommend you to use Application Load Balancer. For network/transport protocols (layer4 – TCP, UDP) load balancing, and for extreme performance/low latency applications we recommend using Network Load Balancer. If your application is built within the EC2 Classic network then you should use Classic Load Balancer.

Q: How do I manage both Application and Classic Load Balancers simultaneously?

In the CLI you will describe your Classic Load Balancers using `aws elb describe-load-balancers` and your Application Load Balancers using `aws elbv2 describe-load-balancers`

Q: Can I convert my Classic Load Balancer to an Application Load Balancer (and vice versa)?

A: No

Q: Can I migrate to Application Load Balancer from Classic Load Balancer?

A: Yes.

**Autoscaling**

1. launch configuration

select AMI

2. Create autoscaling group

#!/bin/bash

yum update -y

yum install httpd -y

service httpd start

chkconfig httpd on

cd /var/www/html

echo "<html><h1>This is Web Server 01</h1></html>" > index.html

ssh ec2-user@52.23.243.201 -i EC2Key.pem

BeanStalk - deploying applications

CloudFormation - infrastructure as code

ECS - Containders remove OS requirements.

S3 Versioning

Versioning enabled : id=11111

Versioning disabled : null

cloudfront - service

physical location - edge location

host static website

go to s3 bucket > properties > static website hosting

upload files on bucket

LOAD BALANCERS

Application Load Balancer

Network Load Balancer

Classic Load Balancer

Autoscaling

1. Launch Configuration

2. select AMI

3. create autoscaling group

group size - 2

select VPC

select sbunets

health check grace period

basic monitoring enabled

2 instances will be launched

4. create load balancer

select all 3 AZs

select security group

5. configure routing

a. create target group

target type = instance

protocol = HTTP

port = 80

health checks = protocol HTTP

b. go to autoscaling group > edit

Select Target Group

Scaling Policies

create alarm

select step policy

create launch template

advanced options:

sport instance

t2/t3 option

termination protection

create template from instance

Health Checks

by default, ASG uses EC2 status checks

enable ELB health checks

go to autoscaling > edit > health check type

EC2 or ELB

Autoscaling Termination Policies:

1. which AZ has most instances

2. instances having oldest lauch template

3. instances having oldest launch configuration

4. unprotected instances closest to the next billing hour

go to autoscaling > edit > termination policies > default

Enable cross zone load balancing on

Step 5: add EC2 instance

**S3**

Q: How much data can I store in Amazon S3?

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from a minimum of 0 bytes to a maximum of 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

Q: What options do I have for encrypting data stored on Amazon S3?

SSE-S3 provides an integrated solution where Amazon handles key management and key protection using multiple layers of security. You should choose SSE-S3 if you prefer to have Amazon manage your keys.

SSE-C enables you to leverage Amazon S3 to perform the encryption and decryption of your objects while retaining control of the keys used to encrypt objects. With SSE-C, you don’t need to implement or use a client-side library to perform the encryption and decryption of objects you store in Amazon S3, but you do need to manage the keys that you send to Amazon S3 to encrypt and decrypt objects. Use SSE-C if you want to maintain your own encryption keys, but don’t want to implement or leverage a client-side encryption library.

SSE-KMS enables you to use AWS Key Management Service (AWS KMS) to manage your encryption keys. AWS KMS provides additional security controls to support customer efforts to comply with PCI-DSS, HIPAA/HITECH, and FedRAMP industry requirements.

Q: What is an Amazon VPC Endpoint for Amazon S3?

An Amazon VPC Endpoint for Amazon S3 is a logical entity within a VPC that allows connectivity only to S3. The VPC Endpoint routes requests to S3 and routes responses back to the VPC.

Q: What is Amazon Macie?

Amazon Macie is an AI-powered security service that helps you prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in Amazon S3. Amazon Macie uses machine learning to recognize sensitive data such as personally identifiable information (PII) or intellectual property, assigns a business value, and provides visibility into where this data is stored and how it is being used in your organization. Amazon Macie continuously monitors data access activity for anomalies, and delivers alerts when it detects risk of unauthorized access or inadvertent data leaks.

Q: How durable is Amazon S3?

Amazon S3 Standard, S3 Standard–IA, S3 One Zone-IA, and S3 Glacier are all designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects.

Q: How are Amazon S3 and Amazon S3 Glacier designed to achieve 99.999999999% durability?

Amazon S3 Standard, S3 Standard-IA, and S3 Glacier storage classes redundantly store your objects on multiple devices across a minimum of three Availability Zones (AZs) in an Amazon S3 Region before returning SUCCESS. The S3 One Zone-IA storage class stores data redundantly across multiple devices within a single AZ.

Q: What checksums does Amazon S3 employ to detect data corruption?

Amazon S3 uses a combination of Content-MD5 checksums and cyclic redundancy checks (CRCs) to detect data corruption. Amazon S3 performs these checksums on data at rest and repairs any corruption using redundant data. In addition, the service calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

: What is Versioning?

Versioning allows you to preserve, retrieve, and restore every version of every object stored in an Amazon S3 bucket. Once you enable Versioning for a bucket, Amazon S3 preserves existing objects anytime you perform a PUT, POST, COPY, or DELETE operation on them. By default, GET requests will retrieve the most recently written version. Older versions of an overwritten or deleted object can be retrieved by specifying a version in the request.

Q: Can I setup a trash, recycle bin, or rollback window on my Amazon S3 objects to recover from deletes and overwrites?

You can use Lifecycle rules along with Versioning to implement a rollback window for your Amazon S3 objects. For example, with your versioning-enabled bucket, you can set up a rule that archives all of your previous versions to the lower-cost Glacier storage class and deletes them after 100 days, giving you a 100-day window to roll back any changes on your data while lowering your storage costs.

Q: What is S3 Intelligent-Tiering?

Amazon S3 Intelligent-Tiering (S3 Intelligent-Tiering) is an S3 storage class for data with unknown access patterns or changing access patterns that are difficult to learn. It is the first cloud storage class that delivers automatic cost savings by moving objects between two access tiers when access patterns change. One tier is optimized for frequent access and the other lower-cost tier is designed for infrequent access.

Q: How do I get my data into S3 Intelligent-Tiering?

There are two ways to get data into S3 Intelligent-Tiering. You can directly PUT into S3 Intelligent-Tiering by specifying INTELLIGENT\_TIERING in the x-amz-storage-class header or set lifecycle policies to transition objects from S3 Standard or S3 Standard-IA to S3 INTELLIGENT\_TIERING.

Q: Is there a minimum duration for S3 Intelligent-Tiering?

S3 Intelligent-Tiering has a minimum storage duration of 30 days, which means that data that is deleted, overwritten, or transitioned to a different S3 Storage Class before 30 days will incur the normal usage charge plus a pro-rated charge for the remainder of the 30-day minimum.

Q: Is there a minimum object size for S3 Intelligent-Tiering?

S3 Intelligent-Tiering has no minimum billable object size, but objects smaller than 128KB are not eligible for auto-tiering and will always be stored at the frequent access tier rate.

Q: What is S3 Standard-Infrequent Access?

Amazon S3 Standard-Infrequent Access (S3 Standard-IA) is an Amazon S3 storage class for data that is accessed less frequently but requires rapid access when needed. S3 Standard-IA offers the high durability, throughput, and low latency of the Amazon S3 Standard storage class, with a low per-GB storage price and per-GB retrieval fee. This combination of low cost and high performance make S3 Standard-IA ideal for long-term storage, backups, and as a data store for disaster recovery. The S3 Standard-IA storage class is set at the object level and can exist in the same bucket as the S3 Standard or S3 One Zone-IA storage classes, allowing you to use S3 Lifecycle policies to automatically transition objects between storage classes without any application changes.

Q: Why would I choose to use S3 Standard-IA?

S3 Standard-IA is ideal for data that is accessed less frequently, but requires rapid access when needed. S3 Standard-IA is ideally suited for long-term file storage, older sync and share storage, and other aging data.

Q: Is there a minimum storage duration charge for S3 Standard-IA?

S3 Standard-IA is designed for long-lived but infrequently accessed data that is retained for months or years. Data that is deleted from S3 Standard-IA within 30 days will be charged for a full 30 days.

Q: Is there a minimum object storage charge for S3 Standard-IA?

S3 Standard-IA is designed for larger objects and has a minimum object storage charge of 128KB. Objects smaller than 128KB in size will incur storage charges as if the object were 128KB.

Q: What is S3 One Zone-IA storage class?

S3 One Zone-IA storage class is an Amazon S3 storage class that customers can choose to store objects in a single availability zone. S3 One Zone-IA storage redundantly stores data within that single Availability Zone to deliver storage at 20% less cost than geographically redundant S3 Standard-IA storage, which stores data redundantly across multiple geographically separate Availability Zones.

Q: What use cases are best suited for S3 One Zone-IA storage class?

Customers can use S3 One Zone-IA for infrequently-accessed storage, like backup copies, disaster recovery copies, or other easily re-creatable data.

Q: How much data can I retrieve from Amazon S3 Glacier for free?

You can retrieve 10GB of your Amazon S3 Glacier data per month for free with the AWS free tier.

Q: What is S3 Glacier Deep Archive?

S3 Glacier Deep Archive is a new Amazon S3 storage class that provides secure and durable object storage for long-term retention of data that is accessed once or twice in a year. From just $0.00099 per GB-month (less than one-tenth of one cent, or about $1 per TB-month), S3 Glacier Deep Archive offers the lowest cost storage in the cloud, at prices significantly lower than storing and maintaining data in on-premises magnetic tape libraries or archiving data off-site.

Q: How does S3 Glacier Deep Archive differ from S3 Glacier?

S3 Glacier Deep Archive expands our data archiving offerings, enabling you to select the optimal storage class based on storage and retrieval costs, and retrieval times. Choose S3 Glacier when some of your archived data is needed in as little as 1-5 minutes using Expedited retrievals. S3 Glacier Deep Archive, in contrast, is designed for colder data that is very unlikely to be accessed, but still requires long-term, durable storage. S3 Glacier Deep Archive is up to 75% less expensive than S3 Glacier and provides retrieval within 12 hours using the Standard retrieval speed. You may also reduce retrieval costs by selecting Bulk retrieval, which will return data within 48 hours.

Q: How durable and available is S3 Glacier Deep Archive?

S3 Glacier Deep Archive is designed for the same 99.999999999% durability as the S3 Standard and S3 Glacier storage classes. S3 Glacier Deep Archive is designed for 99.9% availability.

Q: How do you recommend migrating data from my existing tape archives to S3 Glacier Deep Archive?

There are multiple ways to migrate data from existing tape archives to S3 Glacier Deep Archive. You can use the AWS Tape Gateway to integrate with existing backup applications using a virtual tape library (VTL) interface. This interface presents virtual tapes to the backup application. These can be immediately used to store data in Amazon S3, S3 Glacier, and S3 Glacier Deep Archive.

You can also use AWS Snowball or Snowmobile to migrate data. Snowball and Snowmobile accelerate moving terabytes to petabytes of data into and out of AWS using physical storage devices designed to be secure for transport. Using Snowball and Snowmobile helps to eliminate challenges that can be encountered with large-scale data transfers including high network costs, long transfer times, and security concerns.

Finally, you can use AWS Direct Connect to establish dedicated network connections from your premises to AWS. In many cases, Direct Connect can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Q: What is "Query in Place" functionality?

Amazon S3 allows customers to run sophisticated queries against data stored without the need to move data into a separate analytics platform.

Q: What is S3 Select?

S3 Select is an Amazon S3 feature that makes it easy to retrieve specific data from the contents of an object using simple SQL expressions without having to retrieve the entire object. You can use S3 Select to retrieve a subset of data using SQL clauses, like SELECT and WHERE, from objects stored in CSV, JSON, or Apache Parquet format. It also works with objects that are compressed with GZIP or BZIP2 (for CSV and JSON objects only), and server-side encrypted objects.

Q: What can I do with S3 Select?

You can use S3 Select to retrieve a smaller, targeted data set from an object using simple SQL statements. You can use S3 Select with AWS Lambda to build serverless applications that use S3 Select to efficiently and easily retrieve data from Amazon S3 instead of retrieving and processing entire object. You can also use S3 Select with Big Data frameworks, such as Presto, Apache Hive, and Apache Spark to scan and filter the data in Amazon S3.

Q: Why should I use S3 Select?

S3 Select provides a new way to retrieve specific data using SQL statements from the contents of an object stored in Amazon S3 without having to retrieve the entire object. S3 Select simplifies and improves the performance of scanning and filtering the contents of objects into a smaller, targeted dataset by up to 400%. With S3 Select, you can also perform operational investigations on log files in Amazon S3 without the need to operate or manage a compute cluster.

Q: What is Amazon Athena?

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL queries. Athena is serverless, so there is no infrastructure to setup or manage, and you can start analyzing data immediately.

Q: What is Amazon Redshift Spectrum?

Amazon Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of unstructured data in Amazon S3 with no loading or ETL required. When you issue a query, it goes to the Amazon Redshift SQL endpoint, which generates and optimizes a query plan. Amazon Redshift determines what data is local and what is in Amazon S3, generates a plan to minimize the amount of Amazon S3 data that needs to be read, requests Redshift Spectrum workers out of a shared resource pool to read and process data from Amazon S3.

Q: What are Amazon S3 Event Notifications?

Amazon S3 event notifications can be sent in response to actions in Amazon S3 like PUTs, POSTs, COPYs, or DELETEs. Notification messages can be sent through either Amazon SNS, Amazon SQS, or directly to AWS Lambda.

Q: What is S3 Transfer Acceleration?

Amazon S3 Transfer Acceleration enables fast, easy, and secure transfers of files over long distances between your client and your Amazon S3 bucket. S3 Transfer Acceleration leverages Amazon CloudFront’s globally distributed AWS Edge Locations. As data arrives at an AWS Edge Location, data is routed to your Amazon S3 bucket over an optimized network path.

Q: How fast is S3 Transfer Acceleration?

One customer measured a 50% reduction in their average time to ingest 300 MB files from a global user base spread across the US, Europe, and parts of Asia to a bucket in the Asia Pacific (Sydney) region. Another customer observed cases where performance improved in excess of 500% for users in South East Asia and Australia uploading 250 MB files (in parts of 50MB) to an S3 bucket in the US East (N. Virginia) region.

Q: Who should use S3 Transfer Acceleration?

If you are uploading to a centralized bucket from geographically dispersed locations, or if you regularly transfer GBs or TBs of data across continents, you may save hours or days of data transfer time with S3 Transfer Acceleration.

Q: How should I choose between S3 Transfer Acceleration and Amazon CloudFront’s PUT/POST?

S3 Transfer Acceleration optimizes the TCP protocol and adds additional intelligence between the client and the S3 bucket, making S3 Transfer Acceleration a better choice if a higher throughput is desired. If you have objects that are smaller than 1GB or if the data set is less than 1GB in size, you should consider using Amazon CloudFront's PUT/POST commands for optimal performance.

Q: How should I choose between S3 Transfer Acceleration and AWS Snow Family (Snowball, Snowball Edge, and Snowmobile)?

The AWS Snow Family is ideal for customers moving large batches of data at once. The AWS Snowball has a typical 5-7 days turnaround time. As a rule of thumb, S3 Transfer Acceleration over a fully-utilized 1 Gbps line can transfer up to 75 TBs in the same time period. In general, if it will take more than a week to transfer over the Internet, or there are recurring transfer jobs and there is more than 25Mbps of available bandwidth, S3 Transfer Acceleration is a good option. Another option is to use both: perform initial heavy lift moves with an AWS Snowball (or series of AWS Snowballs) and then transfer incremental ongoing changes with S3 Transfer Acceleration.

Q: What are S3 object tags?

S3 object tags are key-value pairs applied to S3 objects which can be created, updated or deleted at any time during the lifetime of the object.

Q: How much do object tags cost?

Object tags are priced based on the quantity of tags and a request cost for adding tags. The requests associated with adding and updating Object Tags are priced the same as existing request prices.

Q: What is Amazon S3 Object Lock?

Amazon S3 Object Lock is a new Amazon S3 feature that blocks object version deletion during a customer-defined retention period so that you can enforce retention policies as an added layer of data protection or for regulatory compliance. You can migrate workloads from existing write-once-read-many (WORM) systems into Amazon S3, and configure S3 Object Lock at the object- and bucket-levels to prevent object version deletions prior to pre-defined Retain Until Dates or Legal Hold Dates. S3 Object Lock protection is maintained regardless of which storage class the object resides in and throughout S3 Lifecycle transitions between storage classes.

: What is S3 Lifecycle management?

S3 Lifecycle management provides the ability to define the lifecycle of your object with a predefined policy and reduce your cost of storage. You can set a lifecycle transition policy to automatically migrate objects stored in the S3 Standard storage class to the S3 Standard-IA, S3 One Zone-IA, and/or S3 Glacier storage classes based on the age of the data. You can also set lifecycle expiration policies to automatically remove objects based on the age of the object. You can set a policy for multipart upload expiration, which expires incomplete multipart uploads based on the age of the upload.

Q: How do I set up an S3 Lifecycle management policy?

You can set up and manage Lifecycle policies in the AWS Management Console, S3 REST API, AWS SDKs, or AWS Command Line Interface (CLI). You can specify the policy at the prefix or at the bucket level.

Q: How much does it cost to use S3 Lifecycle management?

There is no additional cost to set up and apply Lifecycle policies. A transition request is charged per object when an object becomes eligible for transition according to the Lifecycle rule.

Q: How can I use Amazon S3 Lifecycle management to help lower my Amazon S3 storage costs?

With Amazon S3 Lifecycle policies, you can configure your objects to be migrated to from the S3 Standard storage class to S3 Standard-IA or S3 One Zone-IA and/or archived to S3 Glacier. You can also specify an S3 Lifecycle policy to delete objects after a specific period of time. You can use this policy-driven automation to quickly and easily reduce storage costs as well as save time. In each rule you can specify a prefix, a time period, a transition to S3 Standard-IA, S3 One Zone-IA, or S3 Glacier, and/or an expiration. For example, you could create a rule that archives into S3 Glacier all objects with the common prefix “logs/” 30 days from creation and expires these objects after 365 days from creation. You can also create a separate rule that only expires all objects with the prefix “backups/” 90 days from creation. S3 Lifecycle policies apply to both existing and new S3 objects, helping you optimize storage and maximize cost savings for all current data and any new data placed in S3 without time-consuming manual data review and migration. Within a lifecycle rule, the prefix field identifies the objects subject to the rule. To apply the rule to an individual object, specify the key name. To apply the rule to a set of objects, specify their common prefix (e.g. “logs/”). You can specify a transition action to have your objects archived and an expiration action to have your objects removed. For time period, provide the creation date (e.g. January 31, 2015) or the number of days from creation date (e.g. 30 days) after which you want your objects to be archived or removed. You may create multiple rules for different prefixes.

Q: What is Amazon S3 Cross-Region Replication (CRR)?

CRR is an Amazon S3 feature that automatically replicates data between AWS Regions. With CRR, you can set up replication at a bucket level, a shared prefix level, or an object level using S3 object tags. You can use CRR to provide lower-latency data access in different geographic regions. CRR can also help if you have a compliance requirement to store copies of data hundreds of miles apart.

Q: What is IPv6?

Every server and device connected to the Internet must have a unique address. Internet Protocol Version 4 (IPv4) was the original 32-bit addressing scheme. However, the continued growth of the Internet means that all available IPv4 addresses will be utilized over time. Internet Protocol Version 6 (IPv6) is the new addressing mechanism designed to overcome the global address limitation on IPv4.

You can get started by pointing your application to Amazon S3’s new “dual-stack” endpoint, which supports access over both IPv4 and IPv6.

**Q. Storage pricing**

S3 Standard Storage

First 50 TB / Month $0.023 per GB

Next 450 TB / Month $0.022 per GB

Over 500 TB / Month $0.021 per GB

S3 Standard-Infrequent Access (S3 Standard-IA) Storage

All storage / Month $0.0125 per GB

S3 One Zone-Infrequent Access (S3 One Zone-IA) Storage

All storage / Month $0.01 per GB

S3 Glacier Storage

All storage / Month $0.004 per GB

S3 Glacier Deep Archive Storage

All storage / Month $0.00099 per GB

S3 Intelligent-Tiering Storage, Frequent Access Tier

First 50 TB / Month $0.023 per GB

Next 450 TB / Month $0.022 per GB

Over 500 TB / Month $0.021 per GB

S3 Intelligent-Tiering Storage, Infrequent Access Tier

All storage / Month $0.0125 per GB

S3 Intelligent-Tiering Storage

Monitoring and Automation, All storage / Month $0.0025 per 1,000 objects