Can I run more than one DB instance for Amazon RDS for free?  
Can S3 be used with EC2 instances, if yes, how?  
Define auto-scaling.  
Distinguish between scalability and flexibility  
Explain can you vertically scale an Amazon instance? How?  
Explain what is T2 instances?  
How can you send request to Amazon S3?  
How can you speed up data transfer in Snowball?  
How do you choose an Availability Zone?  
How is a Spot instance different from an On-Demand instance or Reserved Instance?  
How is Amazon RDS, DynamoDB and Redshift different?  
How is stopping and terminating an instance different from each other?  
How many buckets can you create in AWS by default?  
how is the buffer used in Amazon web services?

How the processes start, stop and terminate works? How?  
If my AWS Direct Connect fails, will I lose my connectivity?  
In CloudFront what happens when content is NOT present at an Edge location and a request is made to it?  
Is it possible to scale an Amazon instance vertically? How?  
Name the several layers of Cloud Computing.  
Name the various layers of the cloud architecture  
What are the best practices for Security in Amazon EC2?  
What are the components involved in Amazon Web Services?  
what are the key components of AWS?  
What does an AMI include?  
What does the following command do with respect to the Amazon EC2 security groups? ec2-create-group CreateSecurityGroup  
what is AMI?  
What is AWS?  
What is Cloud Computing  
what is S3?

what is the difference between Amazon S3 and EC2?  
What is the importance of buffer in Amazon Web Services?  
What is the relation between an instance and AMI?  
what is the relation between an instance and AMI?  
What is the way to secure data for carrying in the cloud?  
Which automation gears can help with spinup services?  
While connecting to your instance what are the possible connection issues one might face?  
Why do you make subnets?

**What Is Amazon Ec2 Service ?**

**Answer :**

Amazon Elastic Compute Cloud (Amazon EC2) is a Amazon web service that provides resizable (scalable) computing capacity in the cloud. You can use Amazon EC2 to launch as many virtual servers you need. In Amazon EC2 you can configure security and networking as well as manage storage.Amazon EC2 service also helps in obtaining and configuring capacity using minimal friction.

**What Are The Features Of The Amazon Ec2 Service ?**

**Answer :**

As the Amazon EC2 service is a cloud service so it has all the cloud features.

**Amazon EC2 provides the following features:**

* Virtual computing environment (known as instances)
* Pre-configured templates for your instances (known as Amazon Machine Images – AMIs)
* Amazon Machine Images (AMIs) is a complete package that you need for your server (including the operating system and additional software)
* Amazon EC2 provides various configurations of CPU, memory, storage and networking capacity for your instances (known as instance type)
* Secure login information for your instances using key pairs (AWS stores the public key and you can store the private key in a secure place)
* Storage volumes of temporary data is deleted when you stop or terminate your instance (known as instance store volumes)
* Amazon EC2 provides persistent storage volumes (using Amazon Elastic Block Store – EBS)
* A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using security groups
* Static IP addresses for dynamic cloud computing (known as Elastic IP address)
* Amazon EC2 provides metadata (known as tags)
* Amazon EC2 provides virtual networks that are logically isolated from the rest of the AWS cloud, and that you can optionally (Salesforce Certification Training) connect to your own network (known as virtual private clouds – VPCs)

**What Are The Security Best Practices For Amazon Ec2 ?**

**Answer :**

**For secure Amazon EC2 best practices, follow the following steps:**

* Use AWS identity and access management to control access to your AWS resources
* Restrict access by allowing only trusted hosts or networks to access ports on your instance
* Review the rules in your security groups regularly
* Only open up permissions that your require
* Disable password-based login, for instance, launched from your AMI Complete Amazon Web Services Tutorials

**Explain Storage For Amazon Ec2 Instance ?**

**Answer :**

Amazon EC2 provides many data storage options for your instances. Each option has a unique combination of performance and durability. These storages can be used independently or in combination to suit your requirements.

**There are mainly four types of storages provided by AWS:**

* **Amazon EBS:** Its durable, block-level storage volumes can attached in running Amazon EC2 instance. The Amazon EBS volume persists independently from the running life of an Amazon EC2 instance. After an EBS volume is attached to an instance, you can use it like any other physical hard drive. Amazon EBS encryption feature supports encryption feature.
* **Amazon EC2 Instance Store:** Storage disk that is attached to the host computer is referred to as instance store. The instance storage provides temporary block-level storage for Amazon EC2 instances. The data on an instance store volume persists only (sap training) during the life of the associated Amazon EC2 instance; if you stop or terminate an instance, any data on instance store volumes is lost.
* **Amazon S3:** Amazon S3 provides access to reliable and inexpensive data storage infrastructure. It is designed to make web-scale computing easier by enabling you to store and retrieve any amount of data, at any time, from within Amazon EC2 or anywhere on the web.
* **Adding Storage:** Every time you launch an instance from an AMI, a root storage device is created for that instance. The root storage device contains all the information necessary to boot the instance. You can specify storage volumes in addition to the root device volume when you create an AMI or launch an instance using block device mapping.

**Explain Stopping, Starting, And Terminating An Amazon Ec2 Instance ?**

**Answer :**

Stopping and Starting an instance: When an instance is stopped, the instance performs a normal shutdown and then transitions to a stopped state. All of its Amazon EBS volumes remain attached, and you can start the instance again at a later time. You are not charged for additional instance hours while the instance is in a stopped state.

Terminating an instance: When an instance is terminated, the instance performs a normal shutdown, then the attached Amazon EBS volumes are deleted unless the volume’s deleteOnTermination attribute is set to false. The instance itself is also deleted, and you can’t start the instance again at a later time.

**What Are Regions And Availability Zones In Amazon Ec2 ? Explain In Brief ?**

**Answer :**

Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of regions and Availability Zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as Availability Zones.

Each region is completely independent. Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links. The following diagram illustrates the relationship between regions and Availability Zones.

**What Is Amazon Ec2 Root Device Volume ?**

**Answer :**

When you launch an instance, the Root Device Volume contains the image used to boot the instance.

**You can launch an instance from one of two types of AMIs:**

1. Instance store-backed AMI
2. EBS based storage

**What Is Security Group In Amazon Ec2 ?**

**Answer :**

Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level.

**What Are The Features Of Security Group In Amazon Ec2 ?**

**Answer :**

**Following are the features of the Security Group in Amazon EC2:**

* We can add rules to a security group that enable us to connect to our instance from our IP address using SSH.
* We can also add rules that allow inbound and outbound HTTP and HTTPS access from anywhere

**How To Create Security Group In Amazon Ec2 ?**

**Answer :**

We can create Security Group in Amazon EC2 using the Amazon EC2 console. To launch instances in multiple regions, we’ll need to create a Security Group in each region.

**Following are the steps to create Security Group in Amazon EC2:**

* Open the Amazon EC2 console.
* From the left navigation bar, select a region for the security group.
* Click Security Groups in the navigation pane.
* Click Create Security Group.
* Enter a name for the new security group and a description.
* In the VPC list, select your VPC.
* On the Inbound tab, click Add Rule for each new rule, and then click Create.

**How To Launch An Amazon Ec2 Instance ?**

**Answer :**

We can launch Linux/Windows Amazon EC2 instance using AWS Management Console.

**Following are the steps to create Amazon EC2 instance:**

* Open the Amazon EC2 console.
* From the console dashboard, choose Launch Instance.
* Choose an Amazon Machine Image (AMI).
* Choose an Instance Type.
* Click on Review and Launch to let the wizard complete the other configuration setting.
* On the Review Instance Launch page, under Security Groups select a Security Group.
* Click on Launch on the Review Instance Launch.
* Select an Existing ket pair when it prompte for key pair.
* Click on View Instance to return on the console to see instance is launching.

**How To Connect To Your Amazon Ec2 Instance ?**

**Answer :**

There are several ways to connect to a Linux instance. One of the commonly used method is to connect Linux instance from Windows local machine using PuTTY.

**Following are the steps to connect to a Linux instance:**

* Install PuTTY on your local machine.
* Get your instance ID.
* Get the public DNS name of the instance.
* Locate the private key.
* Enable inbound SSH traffic from your IP address to your instance.
* Converting Your Private Key Using PuTTYgen.
* Starting a PuTTY Session.
* Now you are connected to your EC2 instance.

**How To Add A Ebs Volume To Your Amazon Ec2 Instance ?**

**Answer :**

We can attach an EBS volume to one of our instances that is in the same Availability Zone as the Volume.

**Following are the steps to attache an EBS volumn to an instance using console:**

* Open the Amazon EC2 console.
* In the left navigation pane, choose Volumes.
* Select a volume and choose Attach Volume.
* Select the instance to which you want to attach the volume.
* Click on Attach.
* Now connect to your instance and make the volume available.

**What Are The Best Practices For Amazon Ec2 ?**

**Answer :**

To get the maximum benefit from and satisfaction with Amazon EC2.

**There are mainly four best practices:**

* Security and Network Best Practices
* Storage
* Resource Management
* Backup and Recovery

**What Is Amazon Machine Image (ami) ?**

**Answer :**

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, we launch an instance, which is a copy of the AMI running as a virtual server in the cloud. We can even launch multiple instances of an AMI.

**What Is The Relation Between Instance And Ami ?**

**Answer :**

We can launch different types of instances from a single AMI. An instance type essentially determines the hardware of the (pivotal training) host computer used for your instance. Each instance type offers different compute and memory capabilities.

After we launch an instance, it looks like a traditional host, and we can interact with it as we would do with any computer. We have complete control of our instances; we can use sudo to run commands that require root privileges.

**How To Migrate An Instance To Another Availability Zone ?**

**Answer :**

You can migrate your EC2 instance from one Availability Zone to another.

**Following are the steps to migrate an Instance to another Availability Zone:**

* Create an AMI from the running instance
* Launch an instance from the AMI that you just created, specify the new Availability Zone
* You can use the same instance type as the original instance, or select a new instance type
* If the original instance has an associated Elastic IP address, then associate it with the new instance
* If the original instance is a Reserved Instance, change the Availability Zone for your reservation

**What Is Key Pair ?**

**Answer :**

AWS uses public-key cryptography to secure the login information for your instance. A Linux instance has no password; you use a key pair to log in to your instance securely.

You specify the name of the key pair when you launch your instance, then provide the private key when you log in using SSH.

**How To Create Key Pair ?**

**Answer :**

We can create one using the Amazon EC2 console. To launch instances in multiple regions, we’ll need to create a key pair in each region.

**Following are the steps to create Key Pair:**

* Sign in to Amaon Web Service.
* From the AWS dashboard, choose EC2 to open the Amazon EC2 console.
* From the navigation bar, select a region for the key pair.
* In the left navigation pane, under NETWORK & SECURITY, click Key Pairs.
* Click Create Key Pair.
* Enter a name for the new key pair in the Key pair name field of the Create Key Pair dialog box, and then click Create.
* The private key file is automatically downloaded by your browser. The base file name is the name you specified as the name of your key pair, and the file name extension is .pem.

**What Is The Use Of Key Pair ?**

**Answer :**

Key pair is used to log in to your instance securely. This is public-key cryptography to secure the login information for your instance.

**How To Create Your Own Amazon Machine Image (ami) ?**

**Answer :**

You can customize a instance that is launched from a public AMI and then save that configuration as a custom AMI for your own use.

Instances that you launch from your AMI use all the customizations that you’ve made.

**How To Determine The Root Device Type Of Your Ami ?**

**Answer :**

We can determine the Root Device type of AMI using following 2 methods.

**Method 1:** Following are the steps to determine the Root Device type of an AMI using the console

1. Open the Amazon EC2 console
2. In the navigation pane, click AMIs, and select the AMI
3. Check the value of Root Device Type in the Details tab as follows

* If the value is ebs, this is an Amazon EBS-backed AMI
* If the value is instance store, this is an instance store-backed AMI

**Method 2:** Following are the steps to determine the root device type of an AMI using the command line

We can use one of the following commands.

1. describe-images (AWS CLI)
2. Get-EC2Image (AWS Tools for Windows PowerShell)

**What Is The Size Limit For Amazon Ec2 Instance Store-backed Amis And Amazon Ebs-backed Amis ?**

**Answer :**

All AMIs are categorized as either backed by Amazon EBS or backed by instance store.

**Backed by Amazon EBS** – means that the root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot.

**Backed by instance store** – means that the root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.

**Root device size limit for** –

Amazon EBS – Backed is 16 TiB

Amazon Instance Store-Backed is 10 GiB

**How You’re Charged In Amazon Ec2? Explain In Detail ?**

**Answer :**

* Charges varies upon AMIs backed and storage volums.
* AMIs backed by instance storage charged for: AMI storage + Instance usage
* AMIs backed by Amazon EBS storage charged for: Volume storage + Usage in addition to the AMI + instance usage
* When an Amazon EBS-backed instance is stopped, you are not charged for instance usage, but you are still charged for volume storage.
* AWS charges a full instance hour for every transition from a stopped state to a running state, even if we transition the instance multiple times within a single hour.

**For example:** if hourly instance charge for your instance is $0.10 and if you were to run that instance for one hour without stopping it, you would be charged $0.10. If you stopped and restarted that instance twice during that hour, then you would be charged $0.30 for that hour of usage (the initial $0.10, plus 2 x $0.10 for each restart).

**What Is Shared Ami ?**

**Answer :**

A shared AMI is an AMI that a developer created and made available for other developers to use.

One of the easiest ways to get started with Amazon EC2 is to use a shared AMI that has the components you need and then add custom content. You can also create your own AMIs and share them with others.

* Use a shared AMI at your own risk. Amazon can’t vouch for the integrity or security of AMIs shared by other Amazon EC2 users. AWS recommends that you get an AMI from a trusted source.

**How To Update Ami Tools At Boot Time ?**

**Answer :**

AWS recommends that your AMIs download and upgrade the Amazon

EC2 AMI creation tools during startup. This ensures that new AMIs based on your shared AMIs have the latest AMI tools.

**For Amazon Linux, add the following to /etc/rc.local:**

# Update the Amazon EC2 AMI tools

echo ” + Updating EC2 AMI tools”

yum update -y aws-amitools-ec2

echo ” + Updated EC2 AMI tools”

**How To Disable Password-based Logins For Root In Amazon Ec2 Instance ?**

**Answer :**

Using a fixed root password for a public AMI is a security risk that can quickly become known. Even relying on users to change the password after the first login opens a small window of opportunity for potential abuse.

**Following are the steps to disable password-based remote logins for the root user:**

**Open the /etc/ssh/sshd\_config file with a text editor and locate the following line:**  
#PermitRootLogin yes  
**Change the line to:**  
PermitRootLogin without-password  
The location of this configuration file might differ for your distribution.

**What Is Public Key Credentials And How To Install It ?**

**Answer :**

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair.

After configuring the AMI to prevent logging in using a password, you must make sure users can log in using another mechanism.

**How Is A Spot Instance Different From An On-demand Instance Or Reserved Instance ?**

**Answer :**

First of all, let’s understand that Spot Instance, On-Demand instance and Reserved Instances are all models for pricing. Moving along, spot instances provide the ability for customers to purchase compute capacity with no upfront commitment, at hourly rates usually lower than the On-Demand rate in each region. Spot instances are just like bidding, the bidding price is called Spot Price.

The Spot Price fluctuates based on supply and demand for instances, but customers will never pay more than the maximum price they have specified. If the Spot Price moves higher than a customer’s maximum price, the customer’s EC2 instance will be shut down automatically.

But the reverse is not true, if the Spot prices come down again, your EC2 instance will not be launched automatically, one has to do that manually. In Spot and On demand instance, there is no commitment for the duration from the user side, however in reserved instances one has to stick to the time period that he has chosen.

**Is It Possible To Change The Private Ip Addresses Of An Ec2 While It Is Running/stopped In A Vpc ?**

**Answer :**

The primary private IP address cannot be changed. Secondary private addresses can be unassigned, assigned or moved between interfaces or instances at any point.

**Can S3 Be Used With Ec2 Instances, If Yes, How ?**

**Answer :**

Yes, it can be used for instances with root devices backed by local instance storage. By using Amazon S3, developers have access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites. In order to execute systems in the Amazon EC2 environment, developers use the tools provided to load their Amazon Machine Images (AMIs) into Amazon S3 and to move them between Amazon S3 and Amazon EC2.

Another use case could be for websites hosted on EC2 to load their static content from S3.

**If You Want To Launch Amazon Elastic Compute Cloud (ec2) Instances And Assign Each Instance A Predetermined Private Ip Address You Should ?**

**Answer :**

The best way of connecting to your cloud resources (for ex- ec2 instances) from your own data center (for eg- private cloud) is a VPC. Once you connect your datacenter to the VPC in which your instances are present, each instance is assigned a private IP address which can be accessed from your datacenter. Hence, you can access your public cloud resources, as if they were on your own network.

**Explain What Happens When I Reboot An Ec2 Instance ?**

**Answer :**

Rebooting an instance is like rebooting a PC. The hard disk isn’t affected. You don’t return to the image’s original state, but the contents of the hard disks are those before the reboot.

Rebooting isn’t associated with billing. Billing starts when you instantiate an image and stops when you terminate it. Rebooting in between hasn’t any effect.

**How You Will Change The Root Ebs Device Of My Amazon Ec2 Instance ?**

**Answer :**

* Stop the instance.
* Detach the root EBS volume.
* Attach the alternate EBS volume (as the root e.g. /dev/sda1)
* Start the instance.
* This presupposes that your alternate EBS volume is bootable, of course – it has to contain the bootable OS image.

**What Is The Underlying Hypervisor For Ec2 ?**

**Answer :**

Xen

**What Are Spot Instances In Amazon Ec2 ?**

**Answer :**

In Amazon EC2, we can even bid for getting a computing instance. Any instance procured by bidding is a Spot Instance. Multiple users bid for an EC2 Instance. Once the bid price exceeds the Spot price, the user with the highest bid gets it. As long as their bid price remains higher than the Spot price, they can keep using it.

Spot price varies with the supply and demand. Once Spot price exceeds Bid price, the instance will be taken back from the user

**What Is The Difference Between A Spot Instance And A Demand Instance On Ec2 ?**

**Answer :**

“On-Demand” instances allow the user to use the compute by hour without requiring long term commitment. There are no guarantees that the user will always be able to launch specific instance types in an availability zone, though AWS tries it’s best to meet the needs. This service is preferable for POCs and they do not suffer an interruption of the service(by AWS) like Spot instances.

“Spot” instances are a bid\_for\_low\_price version of On-Demand instances, but could be shut down by AWS anytime the Spot instance price goes higher than bid price. Spot price fluctuates based on the supply and demand of the capacity. It’s essentially the leftover capacity of AWS to be used. There is no difference in the performance compared to On-Demand instances and is usually cheaper than On-demand instances as there is no guarantee provided over the availability. The user can choose a start time and end time for the instances or can make a persistent request(no end time specified) for this service. This service is preferable for computing needs which are not tied to any deadlines, computing needs are large and the interruption of service is acceptable.

**What Are The Main Features Of Classic Load Balancer In Ec2 ?**

**Answer :**

**Some of the main features of Classic Load Balancer (CLB) in Amazon EC2 are as follows:**

**Health Check:** Based on the result of Health Check, Classic Load Balancer can decide to route the traffic. If any instance has unhealthy results, CLB will not route the traffic to that instance.

**Security:** We can create security groups for CLB in Virtual Private Cloud (VPC). With these features, it is easy to implement secure load balancing within a network.

**High Availability:** With CLB, we can distribute traffic among EC2 instances in single or multiple Availability Zones. This helps in providing very high scale of availability for the incoming traffic.

**Sticky Sessions:** CLB also supports sticky session by using cookies. The sticky sessions make sure that the traffic from a user is always routed to the same instance so that user gets seamless experience.

**IPv6:** CLB also support Internet Protocol version 6.

**Operational Monitoring:** We can also perform operational monitoring CLB and collect statistics on request count, latency etc. These metrics can be monitored in CloudWatch.

**What Are The Main Features Of Application Load Balancer (alb) In Amazon Ec2 ?**

**Answer :**

**Main features of Application Load Balancer (ALB) are as follows:**

* **Content-Based Routing:** In ALB, we can make use of content in the request to decide the routing of a request to a specific service.
* **HTTP/2:** ALB supports the new version of HTTP protocol. In this protocol, we can send multiple requests on same connection. It also supports TLS and header compression.
* **WebSockets:** ALB supports WebSockets in EC2. With WebSockets, a server can exchange real-time messages with the end-users.
* **Layer-7 Load Balancing:** ALB can also load balance HTTP/HTTPS application with layer-7 specific features.
* **Delete Protection:** ALB also provides Delete Protection option by which we can prevent it from getting deleted by mistake.
* **Containerized Application Support:** We can use ALB to load balance multiple containers across multiple ports on same EC2 instance.

**What Is A Placement Group In Ec2 ?**

**Answer :**

AWS provides an option of creating a Placement Group in EC2 to logically group the instances within as single Availability Zone.

We get the benefits of low network latency and high network throughput by using a Placement Group.

Placement Group is a free option as of now. When we stop an instance, it will run in same Placement Group in restart at a later point of time.

The biggest limitation of Placement Group is that we cannot add Instances from multiple availability zones to one Placement Group.

**What Types Of Issues Do You Face While Connecting To An Ec2 Instance ?**

**Answer :**

**Some of the possible connection issues with EC2 instance are:**

* Connection time out
* Permission denied due to host key not found
* Unprotected private key file
* Permission denied due to user key not recognized by server
* No supported authentication method available
* Server refused the key AWS Video Training

**What Is Aws?**

**Answer :**

AWS (Amazon Web Services) is a platform to provide secure cloud services, database storage, offerings to compute power, content delivery, and other services to help business level and develop.

**What Are The Key Components Of Aws?**

**Answer :**

**The fundamental elements of AWS are:**

**Route 53:** A DNS web service

**Easy E-mail Service:** It permits addressing e-mail utilizing RESTFUL API request or through normal SMTP

**Identity and Access Management:** It gives heightened protection and identity control for your AWS account

**Simple Storage Device or (S3):** It is warehouse equipment and the well-known widely utilized AWS service

**Elastic Compute Cloud (EC2):** It affords on-demand computing sources for hosting purposes. It is extremely valuable in trouble of variable workloads

**Elastic Block Store (EBS):** It presents persistent storage masses that connect to EC2 to enable you to endure data beyond the lifespan of a particular EC2

**Cloud Watch:** To observe AWS sources, It permits managers to inspect and obtain key Additionally, one can produce a notification alert in the state of crisis.

**What Is The Way To Secure Data For Carrying In The Cloud?**

**Answer :**

One thing must be ensured that no one should seize the information in the cloud while data is moving from point one to another and also there should not be any leakage with the security key from several storerooms in the cloud. Segregation of information from additional companies’ information and then encrypting it by means of approved methods is one of the options.

**Name The Several Layers Of Cloud Computing?**

**Answer :**

Here is the list of layers of the cloud computing

* **PaaS** – Platform as a Service
* **IaaS** – Infrastructure as a Service
* **SaaS** – Software as a Service

**What Are The Different Types Of Events Triggered By Amazon Cloud Front?**

**Answer :**

**Different types of events triggered by Amazon CloudFront are as follows:**

**Viewer Request:** When an end user or a client program makes an HTTP/HTTPS request to CloudFront, this event is triggered at the Edge Location closer to the end user.

**Viewer Response:** When a CloudFront server is ready to respond to a request, this event is triggered.

**Origin Request:** When CloudFront server does not have the requested object in its cache, the request is forwarded to Origin server. At this time this event is triggered.

**Origin Response:** When CloudFront server at an Edge location receives the response from Origin server, this event is triggered.

**What Is Amazon Ec2 Service?**

**Answer :**

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable (scalable) computing capacity in the cloud. You can use Amazon EC2 to launch as many virtual servers you need. In Amazon EC2 you can configure security and networking as well as manage storage.Amazon EC2 service also helps in obtaining and configuring capacity using minimal friction.

**What Is Amazon Cloudwatch?**

**Answer :**

CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. CloudWatch can monitor resources such as EC2 instances, DynamoDB tables, and RDS DB instances.

**Which Operating Systems Does Cloudwatch Support?**

**Answer :**

CloudWatch receives and provides metrics for all EC2 instances and should work with any operating system currently supported by the EC2 service.

**What Is Amazon Cloudwatch Logs?**

**Answer :**

Amazon CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files. With CloudWatch Logs, you can monitor your logs, in near real time, for specific phrases, values or patterns. For example, you could set an alarm on the number of errors that occur in your system logs or view graphs of latency of web requests from your application logs. You can then view the original log data to see the source of the problem. Log data can be stored and accessed indefinitely in highly durable, low-cost storage so you don't have to worry about filling up hard drives.

**What Kinds Of Things Can I Do With Cloudwatch Logs?**

**Answer :**

CloudWatch Logs is capable of monitoring and storing your logs to help you better understand and operate your systems and applications.

**You can use CloudWatch logs in a number of ways:**

1. Real Time application and system monitoring,
2. Long term log retention.

**Does The Cloudwatch Logs Agent Support Iam Roles?**

**Answer :**

Yes. The CloudWatch Logs Agent is integrated with IAM and includes support for both access keys and IAM roles

**Does The Amazon Cloudwatch Monitoring Charge Change Depending On Which Ec2 Instance I Monitor?**

**Answer :**

No, CloudWatch monitoring charge does not vary by EC2 instance type.

**What Can I Measure With Amazon Cloudwatch Metrics?**

**Answer :**

CloudWatch allows you to monitor AWS cloud resources and the applications you run on AWS. Metrics are provided automatically for a number of AWS products and services, including EC2 instances, EBS volumes, ELBs, Autoscaling groups, EMR job flows, RDS DB instances, DynamoDB tables, ElastiCache clusters, RedShift clusters, OpsWorks stacks, Route 53 health checks, SNS topics, SQS queues, SWF workflows, and Storage Gateways. You can also monitor custom metrics generated by your own applications and services.

**What Is The Retention Period Of All Metrics?**

**Answer :**

**CloudWatch retains metric data as follows:**

1. Data points with a period of less than 60 seconds are available for 3 hours. These data points are high-resolution custom metrics,
2. Data points with a period of 60 seconds (1 minute) are available for 15 days,
3. Data points with a period of 300 seconds (5 minute) are available for 63 days,
4. Data points with a metric of 3600 seconds (1 hr) are available for 455 days (15 months). Data points that are initially published with a shorter period are aggregated together for long-term storage.

**Will I Lose The Metrics Data If I Disable Monitoring For An Ec2 Instance?**

**Answer :**

No. You can always retrieve metrics data for any EC2 instance based on the retention schedules. However, the CloudWatch console limits the search of metrics to 2 weeks after a metric is last ingested to ensure that the most up to date instances are shown in your namespace.

**Can I Access The Metrics Data For A Terminated Ec2 Instance Or A Deleted Elb?**

**Answer :**

Yes, CloudWatch stores metrics for terminated EC2 instances or deleted ELBs for 15 months.

**What Metrics Are Available At High Resolution?**

**Answer :**

Currently, only customer metrics that you publish to CloudWatch are available at high resolution.

**Are High-resolution Custom Metrics Priced Differently Than Regular Custom Metrics?**

**Answer :**

No, high-resolution custom metrics are priced in the same manner as standard 1-min custom metrics.

**What Statistics Can I View And Graph In Cloudwatch?**

**Answer :**

You can retrieve, graph, and set alarms on the following statistical metrics: average, sum, min, max, and sample count.

**What Log Monitoring Does Cloudwatch Provide?**

**Answer :**

CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files. With CloudWatch Logs, you can monitor your logs, in near real time, for specific phrases, values or patterns.

**What Kinds Of Things Can I Do With My Logs In Cloudwatch?**

**Answer :**

CloudWatch Logs is capable of monitoring and storing your logs to help you better understand and operate your systems and applications. When you use CloudWatch Logs with your logs, your existing log data is used for monitoring, so no code changes are required.

**How Frequently Does The Cloudwatch Logs Agent Send Data?**

**Answer :**

The CloudWatch Logs Agent will send log data files every five seconds by default and is configurable by the user.

**What If I Configure The Cloudwatch Logs Agent To Send Non-text Log Data?**

**Answer :**

The CloudWatch Logs Agent will record an error in the event it has been configured to report non-text log data.

**What Is The Syntax Of Metric Filter Patterns?**

**Answer :**

A Metric Filter pattern can contain search terms or a specification of your common log or JSON event format. CloudWatch Logs can also be used to extract values from a log even in common log or JSON format.

**How Do I Retrieve My Log Data?**

**Answer :**

You can retrieve any of your log data using the CloudWatch Logs console or through the CloudWatch Logs CLI. Log events are retrieved based on the Log Group, Log Stream and time with which they are associated.

**How Long Does Cloudwatch Logs Store My Data?**

**Answer :**

You can store your log data for as long as you want. By default, CloudWatch Logs will store your log data indefinitely. You can change the retention for each LogGroup at any time.

**What Types Of Cloudwatch Alarms Can Be Created?**

**Answer :**

You can create an alarm to monitor any CloudWatch metric in your account. You can also create an alarm on custom metrics that are specific to your custom application or infrastructure.

**What Actions Can I Take From A Cloudwatch Alarm?**

**Answer :**

When you create an alarm, you can configure it to perform one or more automated actions when the metric you chose to monitor exceeds a threshold you define.

**Ex:** send an email, publish to SQS, stop/terminate an EC2 instance, or execute an auto-scaling policy.

**What Thresholds Can I Set To Trigger A Cloudwatch Alarm?**

**Answer :**

When you create an alarm, you first choose the CloudWatch metric you want it to monitor. Next, you choose the evaluation period and a statistical value to measure. To set a threshold, set a target value and choose whether the alarm will trigger when the value is greater, equal, or less than that value.

**What Is Standard Instances?**

**Answer :**

It provides small instances, large instances, extra large instances that give various configuration options from low range to very high range like Computing power unit, memory, processor, etc.

**Can You Please Explain The Difference Between Demand And Reserved Instances?**

**Answer :**

* On demand instance allow user to pay for the computing capacity according to their use every hour, whereas reserved instances provide user to pay for every instance which they use and they want to reserve.
* On demand instance provide user a free working environment in which there is no need for too much of planning related to complexities, whereas reserved instances provide user with discounts on the hourly charge of an instance and provide a easy way to manage the instances as well.
* On demand instance provide maintenance of hardware and transforms fixed cost into much smaller variable costs, whereas reserved instance provide easy way to balance the pay package.

**How To Upload Files In Amazon S3 In Cloud Computing?**

**Answer :**

Amazon S3 provides uploading of large files and retrieve small offsets for end-to-end transfer data rates. The large file gets stored into small files that are smaller in size. Amazon S3 stores multiple of files together in a bundle or in a compressed form for example in .gzip or .gz format and then convert them into Amazon S3 objects. The files get uploaded on the Amazon server by the use of FTP or another protocol and then retrieved through the HTTP GET request. The request includes the defined parameters like URL, offset (byte-range) and size (length).

**Tell Me How Buffer Is Used In Amazon Web Services?**

**Answer :**

Buffer is used to make the system more resilient to burst of traffic or load by synchronizing different component. The components always receive and process the requests in unbalanced way. Buffer keeps the balance between different components and makes them work at the same speed to provide faster services.

**What Is High Memory Instances?**

**Answer :**

It provides large memory sizes for high end application and it includes memory caching applications as well.

**What Is Micro Instances?**

**Answer :**

It provides small consistent resources like CPU, memory and computing unit. It provides the resources to the applications that consume less amount of computing unit.

**What Is The Function Of A Amazon Controller?**

**Answer :**

The functions that are involved with an Amazon controller are:

* Controllers are used to control the flow in which the messages between the other system components has to be passed.
* It controls the overall structure of the Amazon and all to retrieve the message, process the message, execute a function and store the message in other queue that are completely isolated from other controllers.
* It manages and monitors the messages passed between the systems.

**Explain What Are The Different Types Of Instances Used In Amazon Ec2?**

**Answer :**

The instances that can be used in Amazon EC2 are:

1. Standard instances: it provides small instances, large instances, extra large instances that give various configuration options from low range to very high range like Computing power unit, memory, processor, etc.
2. Micro Instances: It provides small consistent resources like CPU, memory and computing unit. It provides the resources to the applications that consume less amount of computing unit.
3. High memory instances: It provides large memory sizes for high end application and it includes memory caching applications as well.

**What Is An Aws Availability Zone?**

**Answer :**

Availability zones (within a region) work together to make up a collection of your AWS resources. Properly designed applications will utilize multiple availability zones for high availability and fault tolerance. AZ’s have direct low latency connections between each other, and each AZ is isolated from the others to ensure fault tolerance.

**What Is The (generic) Definition Of Scalable?**

**Answer :**

The ability to easily grow in size, capacity, and/or scope when required (usually based on demand).

**What Are The Main Problem(s) With Only Using An Ip Address To Access A Website?**

**Answer :**

**It assumes that:**

* You already know (or can obtain) the IP Address of the web server.
* Can easily remember the IP Address for future use.

**When A User Inputs A Domain Name Into A Web Browser – What Occurs To Bring The Website Content Back To The User?**

**Answer :**

1. The web browser contacts a DNS server and asks for the IP address associated with the domain name.
2. The DNS server sends the IP address back to the Browser.
3. The Browser sends a request (for content) to the IP address associated with the domain name.
4. The web server hosting web content receives the request and sends the web content back to the user.

**What Is A Primary Consumer Use Of Cloud Services?**

**Answer :**

Storage. Many consumers use cloud services to store their data (videos, music, movies, pictures, files, etc).

**What If The (generic) Definition Of High Availability?**

**Answer :**

Refers to the concept of something being accessible when you attempt to access it (and/or the ability to access something via multiple platforms).

**Why Are Common Language Domain Names Used Instead Of Ip Addresses For Accessing Websites?**

**Answer :**

Domain names are much easier to communicate and remember.

**What Is The (generic) Definition Of Elastic?**

**Answer :**

The ability to not only grow (scale) when required, but also reduce in size when required.

**What Two Items Are Required For A Website To Work?**

**Answer :**

1. properly configured web server with a public IP address and web formatted content.
2. A user (you) with a web browser and the IP address of the web server.

**What Is An Ip Address?**

**Answer :**

An IP address is the location/address of a computer on a network (internet). Think of it as the computers phone number or mailing address. It is how the computer can be located.

**What Is The (generic) Definition Of Fault Tolerant?**

**Answer :**

The ability to withstand a certain amount of failure and still remain functional (and/or be self-healing and return to full capacity).

**What Are Some Common Consumer Cloud-based Services?**

**Answer :**

1. ICloud
2. Dropbox

**What Are Some Common Uses Of Aws?**

**Answer :**

* Storage
* Compute Power
* Databases
* Networking
* Security
* Monitoring and Analytics

**When You Use A “cloud” Service – What Are You Utilizing?**

**Answer :**

When you use a cloud service (such as iCloud or Dropbox) – you are utilizing server computers owned, operated, and managed by those companies.

**How Does The Concept Of Fault Tolerance Apply To Consumers/enterprise Users Of Aws?**

**Answer :**

If you cannot access your files from one device/location, but can access from another device/location – then you have sustained a fault in your system but where still able to access your file.

**What Is An Aws Data Center?**

**Answer :**

Located in each Availability Zone is one or more AWS Data Centers. These data centers contain the physical servers that run AWS resources.

**What Must A User/web Browser Have In Order To Initiate A Request To A Web Server?**

**Answer :**

The IP address of the web server.

**What Type Of Service Aws Can Provide?**

**Answer :**

AWS is a cloud services provider. Also known as Infrastructure as a Service (Iaas).

**What Is An Aws Region?**

**Answer :**

At the highest level, AWS’ physical infrastructure is made up of numerous regions that are located all around the world.

Each region is comprised of multiple Availability Zones, which are where specific AWS data centers are located.

**What Is The Purpose Of Dns Servers?**

**Answer :**

To act as a “look up” service for converting domain names into IP addresses.

**What Are Two Of The Main Reasons Consumers Use Cloud-based Services For Storage?**

**Answer :**

1. Redundant backups of stored files.
2. Ability to share/access files from multiple devices.

**How Does The Concept Of High Availability Apply To Consumers/enterprise Users Of Aws?**

**Answer :**

Redundant backups and the ability to share/access files across multiple devices make files stored in the cloud “highly available”

**How Does The Concept Of Elasticity Apply To Consumers/enterprise Users Of Aws?**

**Answer :**

As demand (user base) on a web application increases and decreases – Elastic systems allow for the quick addition and subtraction of servers. The removal of unused servers can drastically reduce cost.

**Why Do We Use Aws For Devops?**

**Answer :**

**There are many benefits of using AWS for DevOps, thery are:**

* **Get Started Fast** – Each AWS service is ready to use if you have an AWS account. There is no setup required or software to install.
* **Fully Managed Services** – These services can help you take advantage of AWS resources quicker. You can worry less about setting up, installing, and operating infrastructure on your own. This lets you focus on your core product.
* **Built for Scale** – You can manage a single instance or scale to thousands using AWS services. These services help you make the most of flexible compute resources by simplifying provisioning, configuration, and scaling.
* **Programmable** – You have the option to use each service via the AWS Command Line Interface or through APIs and SDKs. You can also model and provision AWS resources and your entire AWS infrastructure using declarative AWS Cloud Formation templates.
* **Automation** – AWS helps you use automation so you can build faster and more efficiently. Using AWS services, you can automate manual tasks or processes such as deployments, development & test workflows, container management, and configuration management.
* **Secure** – Use AWS Identity and Access Management (IAM) to set user permissions and policies. This gives you granular control over who can access your resources and how they access those resources.
* **Large Partner Ecosystem** – AWS supports a large ecosystem of partners which integrate with and extend AWS services. Use your preferred third-party and open source tools with AWS to build an end-to-end solution.
* **Pay-As-You-Go** – With AWS purchase services as you need them and only for the period when you plan to use them. AWS pricing has no upfront fees, termination penalties, or long term contracts. The AWS Free Tier helps you get started with AWS.

**What Is Amazon Ec2 In Aws Devops?**

**Answer :**

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.

**What Is Amazon S3 In Aws Devops?**

**Answer :**

Amazon Simple Storage Service (Amazon S3) is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web.

**What Is Amazon Rds In Aws Devops?**

**Answer :**

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud.

**What Is Vpc?**

**Answer :**

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. You can configure or create your VPC as per requirement like select region, create subnets (IP- CIDR), configure route tables, security groups, Internet gateway etc to your AWS account By which you can launch your AWS resources, such as Amazon EC2, RDS instances etc, into your VPC.

So basically you can say that Amazon VPC is the networking layer for AWS Infrastructure.

**What Is Ebs (elastic Block Storage)?**

**Answer :**

EBS is a virtualized SAN or storage area network. Elastic Block Store (Amazon EBS) provides persistence block level storage volumes for use with EC2 instances. EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone.

**What Is The Difference Between Scalability And Elasticity?**

**Answer :**

Scalability is the ability of a system to increase the workload on its current hardware resources to handle variability in demand.

Elasticity is the ability of a system to increase the workload on its current and additional hardware resources, thereby enabling businesses to meet demand without investing in infrastructure up-front.

**What Is Amazon Virtual Private Cloud (amazon Vpc)?**

**Answer :**

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

**What Are The Connectivity Options For My Vpc?**

**Answer :**

**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)

**How Do You Connect My Vpc To The Internet?**

**Answer :**

Amazon VPC supports the creation of an Internet gateway. This gateway enables Amazon EC2 instances in the VPC to directly access the Internet.

**What Are The Components Of Amazon Vpc?**

**Answer :**

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

* **A Virtual Private Cloud (VPC):** A logically isolated virtual network in the AWS cloud. You define a VPC’s IP address space from a range you select.
* **Subnet:** A segment of a VPC’s IP address range where you can place groups of isolated resources.
* **Internet Gateway:** The Amazon VPC side of a connection to the public Internet.
* **NAT Gateway:** A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.
* **Hardware VPN Connection:** A hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.
* **Virtual Private Gateway:** The Amazon VPC side of a VPN connection.
* **Customer Gateway:** Your side of a VPN connection.
* **Router:** Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets.
* **•Peering Connection:** A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
* **VPC Endpoint for S3:** Enables Amazon S3 access from within your VPC without using an Internet gateway or NAT, and allows you to control the access using VPC endpoint p
* **LI>Egress-only Internet Gateway:** A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet

**What Are The Steps To Build A Custom Vpc?**

**Answer :**

**Below are the steps of build a custome VPC:**

1. Create a VPC
2. Create subnets
3. Create an internet gateway (IGW)
4. Attach the new IGW to your VPC
5. Create a new route table (RT)
6. Add the IGW as a route to the new RT
7. Add a subnet to the RTs subnet associations (this will be the public facing subnet)
8. Create web server (public subnet) and database server (private subnet) instances
9. Create a new security group for the NAT instance
10. Add HTTP and HTTPS inbound rules that allow traffic from the private subnets IP
11. Create a NAT instance (public subnet).
    * 1. Community AMIs.
      2. Search for amzn-ami-vpc-natChoose the first image.
      3. Diable Auto-assign Public IP.
      4. Add it to the NAT security group

* Create an Elastic IP
* Associate the Elastic IP to the NAT
* Disable Source/Destination Checks for the NAT
* Add the NAT instance as a route to the initial VPC RT

**Why Should You Use Amazon Vpc, Advantage Of Using Aws Vpc?**

**Answer :**

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, is exposed to the Internet. You can also leverage the greatly enhanced security options in Amazon VPC to provide more granular access both to and from the Amazon EC2 instances in your virtual network

**Can Amazon Ec2 Instances Within A Vpc Communicate With Amazon Ec2 Instances Not Within A Vpc?**

**Answer :**

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.

**Why Can’t You Ping The Router, Or My Default Gateway, That Connects My Subnets?**

**Answer :**

Ping (ICMP Echo Request and Echo Reply) requests to the router in your VPC is not supported. Ping between Amazon EC2 instances within VPC is supported as long as your operating system's firewalls, VPC security groups, and network ACLs permit such traffic.

**Can You Monitor The Network Traffic In Your Vpc?**

**Answer :**

Yes. You can use the Amazon VPC Flow Logs feature to monitor the network traffic in your VPC.

**Can A Vpc Span Multiple Availability Zones?**

**Answer :**

Yes.

**Can You Use Your Existing Amis In Amazon Vpc?**

**Answer :**

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.

**How Do You Specify Which Availability Zone My Amazon Ec2 Instances Are Launched In?**

**Answer :**

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.

**Are There Any Bandwidth Limitations For Internet Gateways? Do You Need To Be Concerned About Its Availability? Can It Be A Single Point Of Failure?**

**Answer :**

No. An Internet gateway is horizontally-scaled, redundant, and highly available. It imposes no bandwidth constraints

**How Do You Secure Amazon Ec2 Instances Running Within My Vpc?**

**Answer :**

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).

**What Are The Differences Between Security Groups In A Vpc And Network Acls In A Vpc?**

**Answer :**

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.

**What Is The Difference Between Stateful And Stateless Filtering?**

**Answer :**

Stateful filtering tracks the origin of a request and can automatically allow the reply to the request to be returned to the originating computer. For example, a stateful filter that allows inbound traffic to TCP port 80 on a webserver will allow the return traffic, usually on a high numbered port (e.g., destination TCP port 63, 912) to pass through the stateful filter between the client and the webserver. The filtering device maintains a state table that tracks the origin and destination port numbers and IP addresses. Only one rule is required on the filtering device: Allow traffic inbound to the web server on TCP port 80.

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

**How Do You Determine Which Availability Zone My Subnets Are Located In?**

**Answer :**

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.

**When You Call Describeinstances(), Do You See All Of My Amazon Ec2 Instances, Including Those In Ec2-classic And Ec2-vpc?**

**Answer :**

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.

**When You Call Describevolumes(), Do You See All Of My Amazon Ebs Volumes, Including Those In Ec2-classic And Ec2-vpc?**

**Answer :**

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

**Can You Employ Auto Scaling Within Amazon Vpc?**

**Answer :**

Yes

**What Is The Ip Range Of A Default Vpc?**

**Answer :**

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

**How Many Default Vpcs Can You Have?**

**Answer :**

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

**How Many Default Subnets Are In A Default Vpc?**

**Answer :**

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

**Can You Launch Amazon Ec2 Cluster Instances In A Vpc?**

**Answer :**

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

**What Is A Default Vpc?**

**Answer :**

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.

**Can You Create Other Vpcs And Use Them In Addition To My Default Vpc?**

**Answer :**

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

**Can You Create Additional Subnets In My Default Vpc, Such As Private Subnets?**

**Answer :**

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

**Can You Use My Existing Amazon Ebs Snapshots?**

**Answer :**

Yes, you may use Amazon EBS snapshots if they are located in the same region as your VPC.

**Can You Boot An Amazon Ec2 Instance From An Amazon Ebs Volume Within Amazon Vpc?**

**Answer :**

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.

**Can You Use Amazon Ec2 Reserved Instances With Amazon Vpc?**

**Answer :**

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.

**Do You Need To Have A Vpn Connection To Use A Default Vpc?**

**Answer :**

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.

**Can You Delete A Default Vpc?**

**Answer :**

Yes. Contact AWS Support if you've deleted your default VPC and want to have it reset

**Can You Delete A Default Subnet?**

**Answer :**

Yes, but once deleted, it’s gone. Your future instance launches will be placed in your remaining default subnet(s).

**If You Delete My Side Of A Peering Connection, Will The Other Side Still Have Access To My Vpc?**

**Answer :**

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

**How Are Iam Accounts Impacted By Default Vpc?**

**Answer :**

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

**Can You Create A Peering Connection To A Vpc In A Different Region?**

**Answer :**

No. Peering connections are only available between VPCs in the same region.

**Can You Peer My Vpc With A Vpc Belonging To Another Aws Account?**

**Answer :**

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

**Can You Have More Than Two Network Interfaces Attached To My Ec2 Instance?**

**Answer :**

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.

**Can You Attach A Network Interface In One Availability Zone To An Instance In Another Availability Zone?**

**Answer :**

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

**Can You Attach A Network Interface In One Vpc To An Instance In Another Vpc?**

**Answer :**

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

**Can You Detach The Primary Interface (eth0) On My Ec2 Instance?**

**Answer :**

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

**Can You Use Aws Direct Connect Or Hardware Vpn Connections To Access Vpcs I’m Peered With?**

**Answer :**

No. “Edge to Edge routing” isn’t supported in Amazon VPC. Refer to the VPC Peering Guide for additional information.

**Can You Peer Two Vpcs With Matching Ip Address Ranges?**

**Answer :**

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

**What Is Classiclink?**

**Answer :**

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.

**How Do You Use Classiclink?**

**Answer :**

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.

**Does The Ec2-classic Instance Become A Member Of The Vpc?**

**Answer :**

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.

**Can You Modify The Vpc Route Tables? How?**

**Answer :**

Yes. You can create route rules to specify which subnets are routed to the Internet gateway, the virtual private gateway, or other instances.

**Can You Use The Aws Management Console To Control And Manage Amazon Vpc?**

**Answer :**

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

**How Many Vpcs, Subnets, Elastic Ip Addresses, Internet Gateways, Customer Gateways, Virtual Private Gateways, And Vpn Connections Can You Create?**

**Answer :**

**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 VPC
* Five virtual private gateways per AWS account per region
* Fifty customer gateways per AWS account per region
* Ten IPsec VPN Connections per virtual private gateway

**How Do Instances In A Vpc Access The Internet?**

**Answer :**

You can use public IP addresses, including Elastic IP addresses (EIPs), to give instances in the VPC the ability to both directly communicate outbound to the Internet and to receive unsolicited inbound traffic from the Internet (e.g., web servers)

**How Do Instances Without Public Ip Addresses Access The Internet?**

**Answer :**

**Instances without public IP addresses can access the Internet in one of two ways:**

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.

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.

**What Is Ipsec?**

**Answer :**

IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

**How Does A Hardware Vpn Connection Work With Amazon Vpc?**

**Answer :**

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.

**Name Any Vpcs For Which You Cannot Enable Classiclink?**

**Answer :**

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

**What Tools Are Available To Me To Help Troubleshoot My Hardware Vpn Configuration?**

**Answer :**

The DescribeVPNConnection API displays the status of the VPN connection, including the state ("up"/"down") of each VPN tunnel and corresponding error messages if either tunnel is "down". This information is also displayed in the AWS Management Console.

**How Do I Connect A Vpc To My Corporate Datacenter?**

**Answer :**

Establishing a hardware VPN connection between your existing network and Amazon VPC allows you to interact with Amazon EC2 instances within a VPC as if they were within your existing network. AWS does not perform network address translation (NAT) on Amazon EC2 instances within a VPC accessed via a hardware VPN connection.

**How Do You Assign Ip Address Ranges To Vpcs?**

**Answer :**

You assign a single Classless Internet Domain Routing (CIDR) IP address block when you create a VPC. Subnets within a VPC are addressed from this range by you. A VPC can be assigned at most one (1) IP address range at any given time; addressing a VPC from multiple IP address ranges is currently not supported. 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.

**What Ip Address Ranges Are Assigned To A Default Vpc?**

**Answer :**

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.

**Can You Assign Any Ip Address To An Instance?**

**Answer :**

**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

**Can You Change A Vpc's Size?**

**Answer :**

No. To change the size of a VPC you must terminate your existing VPC and create a new one.

**How Many Subnets Can I Create Per Vpc?**

**Answer :**

Currently you can create 200 subnets per VPC. If you would like to create more, please submit a case at the support center.

**Is There A Limit On How Large Or Small A Subnet Can Be?**

**Answer :**

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.

**How Do You Assign Private Ip Addresses To Amazon Ec2 Instances Within A Vpc?**

**Answer :**

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.

**How Do You Disable Nat-t On My Connection?**

**Answer :**

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.