============================== INTERVIEW QUESTIONS FROM UDEMY AWS COURSE ==========================================

Check out folder F:\Interview PDFs\Udemy\_Interview\AWS for Screenshots

Q1.How are different projects or client projects structured in your current environment ?

Ans : Our organisation has 2 aws accounts for two different projects and one root account which is also billing account but we dont have access to it. Only senior architect can access that root account. I was working on one of the client project, hence I have complete access to that project.Also we have two other accounts one for where we perform testing related activities & another is playground account for learning purpose.

Q2.What does AssumeRole policy do ? Do you use it any of your existing projects ?

Ans : Assume role is IAM feature that allows you to grant permission to access AWS resources to users, groups, or services within your AWS account or to trusted AWS accounts.When a user or service assumes a role, they temporarily take on the permissions defined in that role.This helps enforce the principle of least privilege and enhances security.It is mostly used for Cross-Account Access, Single Sign-On (SSO), Application-to-Application Access etc.We have used Assume role in VPC peering where we created assume role policy & attached it to the role

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::Account\_A\_ID:role/RoleInAccountA"

},

"Action": "sts:AssumeRole"

}

]

}

Q3.Consider you have a Dockerfile and the image is built using any CI/CD system.

Being a DevOps engineer.Where would you store this Docker image and why?

Ans:

In our recent project, we were using AWS ECR repository because the complete project is running on AWS environment and we don't find a need to push this image to a dockerhub. Also dockerhub is not free & we need to purchase enterprise dockerhub account to store private docker images.Also we might see some latency around this project if we use dockerhub.

Q4. Whats the role of RouteTables in AWS ?

Ans :

Route Table controls the routing of network traffic within a VPC.It determine how incoming and outgoing traffic is directed between different subnets and the internet.

As we know, the VPC by default will not have any connection to the Internet.So we attach nat gateway.But just because we have attached nat gateway to the VPC, it doesn't mean that all the Internet connection is available to the subnets inside the VPC. So to allow the subnets to access the Internet, we have to tell how to reach the nat gateway and this entry is made in the route table.

If we have not made an entry in the rount table, even though the subnet is public, it might not be able to access the internet.

Public subnet dont have direct access of internet we need internet gateway

Internet gateway allows instances within public subnets to connect to the internet and receive inbound traffic from the internet.While NAT gateway allows instances within public subnets to initiate outbound connecstions to the internet and blocks inbound traffic from reaching the instance.

Q5.What are some common AWS service you are using day to day ?

Ans :

As you are aware, my experience in AWS years is divided into two sections.

It is theoretical and real time experience also.So in theoretical there are some services that have not used yet.Example, maybe satellite app, app service , etc. Which are not related to my project.I know theoretically what they do, what is the purpose of it and basics around it.When it comes to experience with working AWS, it is related to my existing project that I am working and supporting, which will include Compute, Containerization, Network, Kubernetes and common utilities that are like EBS,S3 etc.These are some common services that I use day in and day out.If I open my this console.

Q6.What is managed node group in AWS EKS ?

In AWS EKS control plane is managed by AWS itself.

Ans : As we know AWS EKS offers a highly available control plan where we don't have to manage the control plan itself, which is a very big advantage for us.While it comes to the node groups, that is the machines itself that are reporting to the control plane.Either we can provision a bunch of EC2 instance by ourselves and add it to the control plane.This will not help us when we have a big Kubernetes cluster to manage.What will eventually happen is these EC2 instances that we have manually added to the cluster will encounter some kind of issue and Kubernetes administrator has to intervene to solve this problem.To help the engineers to resolve this kind of issues what AWS has come up with is what we call as a managed node group solution.So what is a manage an auto group solution?

It is basically a node group that is spinned by EKS itself and it has a bunch of EC2 instance. It is managed by EKS itself.So in case of any issue related to the EC2 instance or the node itself, which is under managed node group, the EKS will take care.So if we have any unhealthy EC2 instance, if you have any unhealthy node, if you have any kinds of issues with this in terms of networking, capacity or whatever then EKS itself will take care.Not just that, if you want to immediately scale the number of machines and this can also be achieved using the management node group.

if you are using manage node group, is there any disadvantages?

Generally there is no disadvantage.But if your team doesn't know how to manage the capacity planning of kubernetes, so they are expecting the pod to have 20 GB of memory example, then you will end up with having a managed node group that is scaling very heavily and you are paying a lot of cost.So ultimately there has to be a proper specification mentioned in your specs in the kubernetes that will only help you.

Q7.What is concurrancy in Lambda ?

Lambda > Create function > myfunction > Runtime : Python > Create function > paste code > Test

myfunction > Configuration > Concurrancy > Edit > 1. Use unreserved account concurrancy 2. Reserved Concurrancy

Its better to use unreserved concurrancy first & then reserved concurrancy

Ans :

Lambda basically a serverless concept, but it does have to spin up somewhere.And when it spins up in the background, we call it as cold start.Also, if we have a lot of triggers coming, then the cold start can become a problem for us.So to avoid this, we can use what is called us concurrency in lambda or this concurrency has a quota, default is 1000 and you can increase this further.We can set this up in the lambda configuration.We know all of this information.

As we know, Lambda has a serverless component in AWS and we can use it to run certain kinds of scripts.When we run certain kind of scripts, it can happen that our code start time itself can become more and we will run into issues with parallelism in lambda.To make this parallelism much better, We can use concurrency concept which is present AWS, which will help us to have lambda function much efficiently when it is invoked many times.So this many times is based on the application that we use.Lambda can be invoked ten times in a minute or it can be invoked 30 times in a minute.It depends on how the configuration of Lambda has been done, irrespective of it.If we want to have the best use of lambda when we are triggering lambda many times, then it is better to set the concurrency when we set the concurrency for the lambda.It is also good to use the unreserved concurrency first, which is present in our account and only then try to reserve more concurrency if required.

Q8.what is one way in which you can reduce the cost of DynamoDB ?

Ans : When it comes to cost saving, it depends on use case of every application.

One of the ways in which I have solved the problem doesn't mean it will solve all the problems.That being said, the way I would solve one of such problems in DynamoDB is first understand the data freshness required for my application.

If the data freshness is only for the last two days or three days, then there is no point in keeping the old data.I will immediately check with the developers team and raise this topic. And if we don't require this, I would go and set up the time to leave configuration in DynamoDB.Once I do that automatically, any data that is older than two days or 24 hours is deleted, resulting in a cost saving for us.

DynamoDB > Table name > Additional settings > Time to live (TTL) > Enable > TTL attribute name : cleanup > Simulated date & time : 60min, 24hours, 7days, Epoch time (particular time) > Enable TTL

Q9.Do you have a single sign on set up for your organisation or account ?

If you don't have this, then how are you managing this?

Ans : As of now, we have not enabled the single sign on account.The reason being we only have two accounts and our team is very small.We don't have any other team or organization that is currently using it.So as we grow, we might think about enabling the single sign on and work towards it.But currently we don't have it, and that is why we have not enabled it.

OR

Based on how the AWS accounts are set up in the organisation, we have enabled single sign on long back because we have multiple accounts like staging, production and testing.We have integrated this with the help of IT team and currently it is completely managed by the IT team.We don't really look into this at this point of time.

Q10.How is threat detection currently managed in your AWS account ? Do you have a centralised team or your team manages it ?

Ans :

devops engineer specialize on AWS.

Being the only AWS engineer and not having the security team yet taking care of the system. What I have done to my best of my knowledge is one, I have enabled Guard duty and it manages the threat detection part of it within AWS. And we also have WAF, which will help us with attacks and detection of attacks etc. So guard duty is

a must for us because one, I cannot take it off everything. So I'm using AWS default guard duty to take care of it.

And two, we also have WAF. In the future as we grow, I would definitely recommend my team to hire proper security engineers or AWS security experts who can take care of this. Or I myself, given an opportunity, will try to learn more about this and spend more time on this if required.

Q11.Can you explain the below code.

import boto3

# imports the boto3 library, which is the official AWS SDK for Python

from botocore.exceptions import ClientError

# imports the ClientError exception class from the botocore.exceptions module.

# You use this class to handle exceptions that may occur when making AWS API calls.

ec2 = boto3.client('ec2')

# initializes EC2 client using boto3, ec2 variable represents the EC2 client which # you can use to interact with EC2 instances

try:

# try-except block used to handle potential errors that may occur when rebooting an # EC2 instance

response = ec2.reboot\_instances(InstanceIds=['INSTANCE\_ID'], DryRun=False)

# reboot an EC2 instance identified by its instance ID, replace INSTANCE\_ID with

# original instance id, DryRun false means this is not a dry run, and the instance # will actually be rebooted

print('Success', response)

# If the reboot operation is successful, it will print 'Success

except ClientError as e:

print('Error', e)

# If an error occurs during the reboot operation, it will catch the ClientError

# exception and print 'Error' along with the exception details.

Ans : So let me try to explain this code first line by line, and then the whole idea about the code. They are importing the boto3 modules and we are also importing the exception which probably will be used for errors later. After this, I see that we are initializing the client for a resource ec2 and we are using a try catch block so that we are trying to do an action, if it fails, we are also able to catch the exception. After this I see that we are rebooting or trying to reboot an instance so we are passing the instance\_ID.I don't see an instance ID in this code, so I presume that here we are going to write the instance ID because this particular code snippet that you are showing me is not taking an instance\_ID.I will have to replace this instance\_ID if I have to really run this code snippet itself. Then I'm mentioning the DryRun as false because I want to really run this reboot instance. If it is successful, it is giving me a success message. If it encounters any kind of client error related to communication, permission, wrong instance, ID anything it gives me an error and the exception. This is the overall idea about this python code that I can see. So the whole gist of this code is it is time to reboot an instance.

Needless to say, which region or which IAM user it is using is not mentioned in this code. So I presume it depends on the access keys that we have downloaded. And if you ask me to improve this code, I might say that we will have to add the region, make sure we are picking the right IAM user, and also maybe we try to enrich the code with the input of the instance\_ID itself.

Q12.Are you using cloudFormation or terraform for infrastructure provisioning ?

Could you give some insight on what specific tool was chosen and why?

Ans : In our company we are currently AWS agnostic, meaning we are only using AWS cloud. But still we are using TerraForm, the reason is the resources or the people who are working with AWS or the people who are working with DevOps as of today, they are very good with TerraForm and we have an existing setup that has been built with TerraForm and we would like to continue. We are aware that cloudFormation will do the same, but why would we change an existing stack that is already built with TerraForm and managed by TerraForm. Hence We are going to continue using TerraForm Also in the future if we hire new engineers, we are confident that DevOps engineers might be aware of TerraForm and they will be able to read this code base much faster. On the contrary, if everything is built, using cloudFormation, and if we even hire the expert, they might not have come across this kind of infrastructure build using cloudFormation and we don't want to risk it. Hence we are using TerraForm. We are going with what the market is demanding.

OR

We are currently using TerraForm even though we are completely on AWS.The reason is our company has multiple projects.The project that I am currently working on is on AWS, but there are certain projects that are hosted on GCP Cloud, there are certain projects that are hosted on Microsoft Azure.So as a company, as a standard inside the company, inside their devops teams.We are using TerraForm even though we are focused on AWS.

OR

Currently I am working in a very small team and our tech stack in a is very, very small.And we are using completely serverless technology that is Lambda and API Gateway and we are building this project as of now and this project is only around 9 to 12 months old.At this point of time, We find it very easy to use clouFormation and hence we are sticking with cloudFormation.But as we go we might re-evaluate the scenario and try to move to TerraForm if required.

Q13.You have been asked with a project where the requirements are "Allow users to upload only JPG format files into an S3 bucket" How will you set up the S3 bucket to achieve the same?

Ans :

select bucket > Permissions > Bucket policy > Edit > check Q13-1.png

Based on the given information here, what I would do is try to create a S3 bucket policy focusing on the putObject action, which will check if the file uploaded is of JPEG format. If it is not the case, it will block such uploads and give an error to the user. I do not know the exact policy of course, but I will use the IAM policy generator and go through the documentation to create such a required policy. Needless to say, this particular used case is specifically suited for many of the application. I would definitely do this by using the S3 bucket policy option that we have.

Q14.Currently you have ASG means auto scaling group with minimum 15 and maximum 30.

All the EC2 instances in the ASG have been EBS attached.Do you see a way in which we can reduce the storage cost of these EC2 instance ?

Ans :

less the EBS volume the faster we can provision EC2

Based on my experience when it comes to EBS storage volumes, I understand that this is a static cost that we will have to bear as we keep on increasing the number of machines. I can also presume that if any application, we might require around 100 GB of EBS volume. This means in the given example that you asked me, we might require 1500 GB as a minimum for storage. Now, looking into the EBS volume itself, we know that all the volume have some things in common that is logs where they have to dump the logs and the application jar itself that it has to read. What we can use in this case is EFS. EFS, which stands for Elastic File System can be used and we can store the application jars and we can have a log files folder. So these two path that is required can be used in the EFS and the EBS volume can be drastically reduced to 10 GB or 20 GB. This way we can reduce the cost of this storage. Of course, we will have to do some testing because there is no one fit all solution for this. So from 100 we might not come down to 10 GB, we might come down to 15 GB, but this is what I would do to resolve this issue.

Is EFS different than EBS ? Will the applications have issues using EFS?

Ans :

EFS can support EBS definitely, but the way in which it stores the file system or the way in which it stores the data is different. Apart from this, for the EC2 itself, it will not have issues accessing folder paths or it will not have issues storing some things in the EFS. That is why EFS is compatible with EBS, but we cannot replace the EFS as a boot volume for issue instances.

how are you handling this today in your organisation right now?

Ans : Yes, we do have auto scaling groups in our organisation, but at this point of time storage is not a concern for us. We are okay with the budget of it and we have not yet received any red flags around it. And we don't want to make a change for this unless and until it is typically required. We know moving to EFS will solve the problem, but our application is not as big as we discuss as of today and storage itself is not an issue. Maybe as we grow further and as EBS volume grows and as EC2 instance minimum capacity grows, we will think about it. And possibly this is one of the solution that I would also recommend at that point of time, given it is still valid.

Q15.How to enable API authentication for your application that is using API gateway ?

Explanation : Application can be written in java, python & hosted on ASG, lambda. Application has endpoints like /books, /fashion & when somebody hits these endpoints it will do some action. To host these endpoints in secure way we use API gateways & these API gateways gets authenticated with API keys which are generated inside AWS.All these API keys can be rotated, disable.

E.g Skyscanner collects scrap data from different websites like Aii India, Emirates, Luftansa etc. It actually hits the api of these websites & access their filght information.

1.Create API keys :

API gateway > API keys > Actions > Create API key > Name: petstore > save

2.Create Usage plan :

API gateway > Usage plan > Create > Name, Rate(Request per second), Burst(requests), Quotas

3.Enable API key authentication :

API gateway > Create API gateway > petstore > click on GET request > Method request > Settings - Authentication : None, Request validator : None, API key Required : false change it to true > save (click on correct symbol)

Ans: For any application that is using API Gateway as an endpoint methodology, then it is very easy to create this API key. From what I remember last time, there should be a column called API Key required which has to be turned on. And then you can create an API key inside the AWS API Gateway service.Then you attach these keys in the usage code. That is how you can control and create the API keys. In my application currently that is something that I'm supporting, we are not using Amazon API Gateway and hence we have not yet explored this option.

Q16.how does EDGE location really helpful ? Reflect based on your experience only.

Explanation : sport streaming, netflix

Ans :

As I explained earlier, the application that I am supporting as of now We don't have anything that requires a very high latency throughput.Because it is a read only website, it does have interactions but it doesn't have anything that we have to caché or we have to serve really fast.

Most of it our documentations, most of it are something to read and some of them are just some tables that they have to view and some graphs.Because of this, we are not using the edge location at this point of time.Also because our clients are not present in a very far locations and we have not come across this latency problem yet.

But as we develop this application, if we come across this, then I think cloud front will be the way to go because indirectly edge locations are used here and that's how edge locations can help us.

OR

Based on the question, I would like to say that in our application we have a one end point where we in fact disclose some kind of videos.These videos are some training materials that has to be used by our clients and the employees of our

clients. In this case, because we are streaming some content and to give a better performance in terms of latency, we are making sure that we are using cloudFront which indirectly uses the location.

Q17.What is the "dead letter queue" concept in SQS. Have you come across it ?

Explanation : food order zomato

Ans :

Yes, I have come across this concept of dead letter que in SQS, usually the dead letter ques are used to process unacknowledged messages in SQS, that could happen for several reasons.In my project as of now we are not using the dead letter que or SQS because we don't have such a queing mechanism present.

OR

Yes, we are using SQS in our project as of now.And the reason why we are using it is because one of our application has a queuing mechanism, meaning there are certain messages that have been sent by the end user which has to be processed by the other party,meaning we have implemented as SQS.

It can happen that there are some messages in SQS that will not be consumed by this third party, and hence it could be it could be lost.So I was requested to implement this dead letter queue concept, and that is when I came across this particular terminology.All I had to do was go to AWS and enable data letter queue in the SQS configuration. And then we had a new dead letter queue and I gave this information to the software engineering team who further did some more integration on top of this dead letter queue.This is what I am aware of, the data queue and SQS.

Q18.What are the databases that you have used ? how are you handling DB upgrades in your organization?

Explanation : check mysql version, if we dont pick maintainance window AWS may pick window by themself & upgrade it.It is done usually for major upgrades only.

Ans : For first part of question :

Currently the project that I'm supporting in the AWS environment is critically an OLTP system,critically because most of the applications that are present are OLTP heavy meaning they're all transactional heavy,they require writing to as table format databases.Hence, based on the request from our software engineering team, we have set up multiple RDS, mostly it is a MySQL database and we are maintaining it as of now.

OR

Currently in the AWS project that I am working, we are using the combination of MySQL and NoSQL databases both in my current project.The reason for that is initially when we started working with this project, we only had the need of MySQL databases and we went with the standard MySQL database that comes with RDS.

But there was an extension of this project that we had to work where we had to store the NoSQL database and we had to choose DynamolDB.Hence I have experience in both of them and have tackled some issues around both of them.

For first part of question :

When it comes to maintenance or upgrades and fixes.I think the best part of all of this is using cloud.These are the reasons why we are using cloud.And in our project, what we are doing is we are using the maintenance window option provided and in the project again that we are using our maintenance window is Sunday 12 a.m. to 2 a.m midnight in US time zone Or you can say UK time zone Or you can say any time zone that is preferred. And during this window the AWS is going to apply any required changes.

This window is decided based on the application usage and it has come from the product managers and software engineers and that is the window that has been set. For any major upgrades, like if the MySQL version is changing or some critical changes are being applied. From what I remember, AWS sends notification and we take action accordingly.I have also seen that we had to reboot some databases sometime. In this case, it is a very big plan.We have to send prior notifications to all the engineers, prior notifications for downtime.Expect that there could be some issues and we go to the database console and reboot the database quickly.

There has not been a case where we have rebooted and some things have broken, but we have to follow the standard DevOps process here.Being an AWS engineer, I have to make sure all of these practices are followed.

Q19.How do you manage programmatic access to AWS in your organization ?

Ans :

Programmatic access in AWS refers to the ability to interact with AWS resources and services using APIs (Application Programming Interfaces) and automation scripts, rather than through the AWS Management Console.

When it comes to programmatic access in our project, we are currently using AWS cloudFormation.I am aware that outside this project that is in my own organization, when I speak to different other AWS engineers or cloud engineers, I am aware that they are also using TerraForm in many cases.But given our project, we are very specific with AWS.We are AWS agnostic,We only use AWS at this point of time and we have realized that because of this cloudformation works much better.Because it is a product that is given by AWS for maintaining programmatic access and infrastructure to use and it makes it easy for us to use cloud formation and it is very easy to understand when it comes to use only, and we have been trained for it.In the future, if I come across different projects where I will have to learn a tool that is other than cloudFormation, it shouldn't be difficult because all of them follow a similar format of YAML and making a declarative way of writing the systematic code that can be used to spin up resources and maintain resources.

What are some shortfalls of clouFormation ? How do you maintain the big stack of clouFormation ?

Ans : When it comes to shortfalls for cloudformation, as of now, I have not seen any, the reason is I have not also experimented with other tools like I just mentioned.When it comes to maintainability part of it.I do agree that if we end up with three or four or five different projects that it could become a bit problematic if you are using the same cloud formation script, but we don't have to.

So in our case we have two or three applications and we have different cloud formation scripts for them using which we will be able to spin up the whole tech stack and also bring down the whole tech stack.Now, this bringing up and bringing down of the stack for us is really key because of our client.So in case of disasters, we should be able to spin up the end to end application in a different region and for which the current way in which we have implemented this whole cloud formation thing is really easy.And we have also tested this.

Q20.Please explain end to end CI/CD setup adopted in your AWS environment.

Ans :

When it comes to end to end CICD processing, we currently have two structures.The first structure is related to the application code or our software code. This is currently stored in GitHub and software engineering, QA And other people contribute. Whenever there is a pull request or whenever there is a merge to the master, we have a trigger that calls code deploy and code deploy basically does the respective action. And in this case, because it is a software code, it is going to test the code or it is going to run the code, build a jar and deploy the jar if required into the infrastructure. This is one way. The other setup that we currently have is infrastructure related setup. We don't run anything locally, So all the cloudformation scripts that we have go through the CICD process. So we make some changes in the cloudformation script, We raise a pull request and when we merge it the code deploy will trigger and make the changes into our infrastructure according to the changes that have been merged to the CloudFormation script.

What is difference between codeDeploy & jenkins ?

Ans : I am aware of Jenkins fundamentally. I know what it does, but as of now, because of our project requirement, we are using core deploy and all other use cases related to our deployment of the code is satisfied by the code deploy. So if you have no reasons to alternatively think about Jenkins at this point of time. If required in the new projects, if there is a requirement of learning Jenkins I would definitely learn and it is easy to adapt after I know one kind of system CICD system.

OR

To set up Jenkins in a very big infrastructure, we might have to do a lot of things. That is, we have to set up, configure, maintain, etc.Now, because of our project, it is a very small project and we don't have that much capacity to just go and setup the whole Jenkins in the AWS we are using the code deploy. Now what are the advantages? There is no infrastructure maintenance that we have to do and all the things that Jenkins can do can be done by code deploy. You can configure alerts, We can run any kind of job,We can set up pipeline and we can do everything. Hence we are going with code deployed. Now, Jenkins, on the other hand, has some kind of advantages when it comes to plugins maybe and we can make some changes because it is open source and we can adapt it into certain requirements that is needed for us. But for this project, we don't have such requirements and codedeploy currently solving all of that for us.

Q21.How does AWS Lambda secure your code? Is it safe to run your code on Lambda?

Ans :

As we are aware, Lambda is a serverless concept, meaning we don't have any access to the infrastructure components.The first thing is whenever we upload our code to Lambda first, it is stored in an S3 bucket in the backend in an encrypted format, meaning no one can access this in the plaintext so no one has access to our code repo or code itself. The second thing is when we trigger our lambda and when our code runs, it runs on an isolated piece of environment and this is guaranteed, we don't have to worry about it. And if there is a thought about the secrets we have to make use of AWS Secrets Manager to store our secrets and retrieve it during our runtime.

========================================================================================= INTERVIEW QUESTIONS FROM UDEMY DEVOPS COURSE =================================

====================================================================================

Check F:\Interview PDFs\Udemy\_Interview for screenshots

Question 1.Your EC2 instance is running out of disk space. What actions will you take to mitigate the issue ?

Ans :

To debug the issue with the disk space,I would first understand which EBS volume is having the problem.If it is the root EBS volume, I would handle it a bit slowly because it deals with the operating system itself.And I would first like to check the logs and try to make some space for the operating system to function properly.

If it is the application volume that is having an issue, I would check something related to the application directly.What was the recent changes in the application? Are there any error logs in the applications that is causing a lot of logs to be failed? Were there any multiple deployments and jars were not clean etc.

I would also check libraries that were just hanging out there without doing anything, and I would delete something, but we can take certain actions because it is an application volume.I will use the EBS feature and I would first take a snapshot of this volume and then increase the volume capacity.

Hence, this should resolve any of the disk space related issue of EC2 instance.

Explain a different way in which Prometheus can get The Metrics?

I have not used this particular tool and have used other tools, and I might not be able to answer.

We are aware there is a lot of monitoring date and they are expecting us to see if we understand the architecture of Prometheus, if we know how Prometheus works.

Prometheus, as we know, is a monitoring tool, and it collects metrics and it stores it.Once the metrics are stored, we can do anything, we can do a dashboarding on top of it.We can also do alerting on top of ot.how does actually the metrics comfortable to use?

The first way is full based approach.

And the second way is push based approach

In the pull based approach your application, it can be a job application or it can be any application JavaScript Node.js doesn't matter.It will expose a matrix endpoint and Prometheus will scrape from the Matrix endpoint.

In a push to based approach, your application will send the matrix via a gateway node it will be stored in Prometheus.

What is the used case of Pushed based approach?

There might be some application that might not be running 24/7.They might just come up and go away.In such cases, pushed base is used

Answer :

The answer here is Prometheus collects Matrix in two ways.The first is purely based approach and second base based approach.

Both of the approaches are valid and based on the application design, we will use either pull based approach on based approach.

What is kubernetes kOps ?

KOps, basically is a way in which you can set up a kubernetes cluster instead of using kubeadmin.It is an automation tool that you can use to set up a kubernetes cluster on any cloud service.

kOps is not something that will help you to set up and managed Kubernetes cluster like EKS.

What is a managed is kubernetes cluster?It means that everything regarding a the cluster is taken care of by the cloud provider.But kops is not that

It is used to set up a cluster quickly.And one of the use cases for that is you can spin up a cluster are a small dev cluster using kops very quickly in the cloud and test your application, deploy your service or do any kind of load balancing.

Kcops will not help you to only create the cluster.It will also help you to destroy it upgraded and maintain it in production-grade if required.

But I wouldn't say this stage so unless and until you can't use any managed kubernetes service.

So what this Kops is really doing?

You might be wondering, can't I just use kubeadmin to do what it ? you can but remember when you set up a kubernetes cluster in cloud you would need integrations with EBS, right for volumes.You need integrations with EC2 for spinning up machines.ASG for spinning up the auto scaling and then, route 53.

So the issue that you will face if you just use kubeadmin is , integrating with all of these external services.And that is where our kops comes into picture.

And it will help you to make all of these integrations happen if you use Kop's to set up and cluster in AWS.As of today, supports AWS, Digital Ocean , OpenStack.

Answer :

Kops is an automation tool using which I can set up kubernetes cluster in a cloud account.

It helps me to automate the whole setup process, destroy the cluster or upgrade the cluster, maintain the cluster in production in cloud service,if I cannot use any of the managed kubernetes service for whatever reason, it is.

If I were given a chance to use kOps, then I would use this to set up a quick development or testing cluster in my company so that if we want to do certain kind of testing, load testing, application testing, we can quickly spin up a cluster tested and then destroy it using kOps.

what is instance fleet in AWS ?

Instance fleet contains configuration using which you can launch a group of EC2 instance.

But the speciality of instant fleet here is this can be a mix it set off EC2 instance.

You might have heard about auto scaling, right? And we can spin out, let's say, t2 micro

But what if I want to mix t2 micro with t3 medium or m-Series etc.That is what is instance fleet.

In AWS a fleet gives you an option to mix and match different kinds of EC2 instances.

Not only that, it also gives you options different purchasing option you can mix and match spot instances with reserved instances and On-Demand instances.

So your fleet can not just contain different kinds of machine, it can contain different pricing models.

The major use case of this instance fleet comes when you want to mix and match your EC2 instances based on the application need.

Defined separate On-Demand and spot capacity targets - You can also do that based on how you want to mix it, that's based on pricing model, and you can also specify different machine types like I mentioned.

Answer :

Instance fleet is nothing but a combination of different kinds of EC2 instances, both with respect to the capacity and pricing model.

This mix and match helps us in certain use cases of application development, wherein we can use same kind of machine types with capacity, but different family and mix of our sport instances reserved instances and on demand instances in the same group.

A typical use case of this can be in a AWS EMR, which is a big data processing tool in AWS

where you can process different data and here we can mix and match the machine types and cost in the instance fleet.

How do you pass message when you commit your code?

The answer to this question is you pass an argument, -m, then you pass and your commit command.git commit -m "commit message"

You can do a git commit without passing the message.But what will happen is on this screen you are going to see that there will be a commit done, but therewill be no message here.

It will confuse you in the future when you look into the history of commits.

You will be lost and you will be wondering what these commits were and you will have to look into the code to make a meaningful assumption of what this commit was.

Hence, it is also a very good practice.One should follow.when you are committing any of your code into the repository.

And this commit message will also appear in your pull request and it will make it simpler for the person reviewing your code.To understand what this code commit is all about.

Answer:

Git commit is a way in which we will pass a message of what this commit is all about when we are opening a pull request.This is important for me to make sure that whatever I have worked, I have summarised it as a part of this message in a few words, so that whenever the person reviews, he knows what he is looking into it for.

Needless to say, all actions on getting government will be present in the good history and indeed repository history and it will become easy for us in the future to go back into history and see what this commit messages.

Are you supporting any application? If yes, what is the application server you are using?

-

It is automation, right? What for whom are you building this automation for a developers team or an application development team

Hence, you might be closely associated with such a team, and they want to really understand if you are.

The question is about the application server, but please don't confuse the server in the sense as EC2 machine No. Application server is basically in which when you deploy a code, it helps to make sure that the functioning of the web end work properly.

what is an application service?

Java

Tomcat

JBoss

Weblogic

NodeJS

IIS

Python

Django

If you are supporting a project that is using Java, then you might be using a tomcat.

Applications server or a JBoss or WebLogic which is a license to based the application server.If you are using WebLogic, then you are paying your license.If it is nodejs , then it is IIS.If it is Python, then it is Django.

OK, now we have understood what application service is all about, and we have also understood different kinds of application services for different programming languages.

Answer :

Currently I support a team that is developing an application in Java.And they are using tomcat service for our application server deployment. Meaning it is our web end based service for all the applications related endpoints.

I am also aware that in the future if I have to support different kinds of teams that use Python,Node.js, etc there are different kinds of application services.

And as a DevOps engineer, I'm aware of what it is and I know how to debug such application if required.

How to check logs from my docker container and how to filter only the last 200 lines from the container logs ?

The command that I have used mostly to see the logs of my container is Docker container logs and container name.

If you wish to see only the last 200 lines or 300 lines or 100 lines, then you can pass an argument called -- tail 200, which will list only the last 200 lines of main container logs.

What will happen to container logs? If you restart the container, will it be lost or not?

The answer is if we start stop, restart the containers for any reason, our logs will not be deleted.But when we run, the Docker logs command, we might not see the old logs.

That depends on how our application handles log storage.

Meaning if we restart the container, if the application also restarts in this case, it might create a new file but the previous file still exists.

Also, I would like to mention that if the container itself is deleted for some reason, then the logs shall also be deleted as a part of container.

If we have a use case in which we need to persist such kind of logs, then I would strongly suggest to use an external log storage player like Splunk or any other logging capacity to so that we don't lose such logs.

what is vertical scaling and what is horizontal scaling ? Explain it the use case you have seen.

Ans.

Vertical scaling and horizontal scaling are both are important methodologies that we implement when we want to scale our application.The use case of vertical scaling will appear when we are more features to our application, and the application needs more CPU compute memory for processing our requests. Where in we need a horizontal scaling in terms of scaling our application by adding more machine types, this is mostly to handle incoming traffic, meaning we might get a sudden burst of traffic and we might want to process all of this traffic of users at the same time.We should not make our application slow, then we use horizontal scaling.

Explain replication controller in kubernetes.

We can say that Replication Controller Inc. is one of the controllers that are responsible for making sure that X number of replicas are present at any given point of time in our cluster.This X number can be three to one doesn't matter.

It is very important for us to have a replication controller if we want to have a kind of horizontal scalability present, meaning we have three and six in the future or we have to have high availability present.

Do you use helm? If yes, which version, do you use currently? And do you see benefit of using helm.

yes, we used helm and currently we are using helm 3

Helm is a way in which we are packaging all of the components is deployment related files in the format of what we call less child.This chart will help us to make the deployment easier, rollback and upgrade also very easy.Using this help chart, it also becomes a lot more easier to handle different environments like production,staging and testing.

This is by making some variations in the values file present as part of our help fight.

This is about what is help and how to answer this question if it.

Explain which python module, will you use to make a simple API testing code? The code should just check if an API endpoint is working or not.

Ans:I would use request module in Python and try to check the status code that will be returned when I try to do the get call to this API.

If this state code is 200, then everything is good.If it is not, then I would say that API is not working.I can add other functionalities to this code based on the requirement after this particular testing.

status\_code = requests.get(website).status\_code

Here we add endpoint of API endpoint in place of website

what is a remote-exec in TerraForm ? And when will we use it ?

Ans : Remote Execute is a provisioner that will execute any given script on my resource after terraform has successfully provision it.An example that I would like to give is let us say we are spinning up an EC2 instance, and after the EC2 instance spun up successfully, we might want to run certain script.In this case, I would prefer to use and remote execute so that after the resource has been successfully provisioned a by my terraform these kind of scripts can run.

SET - 8

Your development team needs your help to monitor the API endpoint, which HTTP response would you monitor and when will you trigger the alert?

Ans : To tackle this problem, I would first begin with writing a script using either Python or Linux, and I would do get call to the API endpoint and get a http response.

What I would be interested in is, what kind of response am i getting if this response is in the range of 400 or 500, then I will trigger an alert because the standard http response 400 to 500 range means we do have either client error or server error.

can we have a Jenkins agent, which is a Docker container and run our test inside this docker container ?

To use any kind of Docker containers, I would basically add it as a part of the agent and we can call any kind of images either from Dockerhub or custom images that we have build and then whatever the stages and test scripts we would mention as a part of our pipeline will run inside this docker container. If I have to suggest a best ways of implementing

this in any organization, then I will suggest this is one of the best ways to implement any test cases or have multi node Jenkins set up. Whenever we have multi node Jenkins set up, this is one of the best ways to implement complete testing and isolcation.Hence, we can scale easily our Jenkins set up also.

SET - 9

What are some ways in which you have setup alerting ?

As a part of setting, alerting and in my organization that we follow, we are currently using Prometheus and alert manager, using which if there is any issues with our systems, if we get an email notification and a phone call so that we address this issue right away.

Also, I'm aware that there are other alerting mechanisms that I can also use based on the cloud that we are using and in AWS I am aware that we have cloudWatch and SNS to the same.

And other example for open source is nagios alerting mechanism, which can also be implemented.

Which helm repository do you use today to store and access your helm charts ?

First, understand that if you are a part of a DevOps team, then try to check, which helm chart repository they are using to store it.

If you are attempting a DevOps interview by practicing DevOps and learning DevOps, and I would say you mentioned that you are storing it in S3 as a part of helm chart repository. or a JFrog repository as a part of your helm chart repository in the organization.

SET - 10

Have you used Jenkins in multi node set up? If yes, Could you explain how to add a new slave or follower to the master?

Manage nodes & clouds > We add slave nodes here

To add slave node dynamically we need ASG

Yes, I have used Jenkins multi node setup because it offers me a high availability for our production pipelines. And to add Jenkins slave machine to the master, I would log in to Jenkins, go to the settings, and I should find an option called as Manage and Nodes

and Cloud.And once they click on that option, I will be able to give the node information and the slave will be registered to the master.

If you don't know where this option is, or if you forget about this option that it exists, there is no need to panic.

You can say that, yes, I have used it.We have been using it in production.And I believe that is an option in the Jenkyns, I don't remember exactly where, but using that option, we will be able to add the slave nodes to the master and all the slave nodes will registered to the master.

Could you explain how you would block and I am user from accessing a specific S3 bucket?

It is very difficult to manage bucket level policies using IAM policy.

Go to S3 bucket > permissions > Bucket policy > Edit > Change Effect : Deny, Principal : arn of IAM user, Action : S3, Resource : S3 bucket arn

Ans: You can say that to achieve this IAM related resolution that is I have been asked to make this change.I would start by making sure that I will be able to make the changes on that bucket myself, that is, I have the permission to make those changes in the bucket policy and then I would basically apply the changes in the S3 bucket policy section.

SET - 11

You encounter a Docker image with a size 2.7GB. Would this be a cause of concern ? If yes, how would you tackle this?

Alpine images are base images with no unnecessary packages installed Lightweight images

Download particular version of package called as package locking. E.g Python request package version

Ans: To begin with, I cannot just really say how to reduce it, if the application really requires this to be 2.7GB, then it is OK. But I would say that it might result in longer build time, errors when downloading the Docker image and API rate limit with respect to our Docker hub.And at the final, when we go to scale this application, we will feel that our application is bulkier.If this is a very simple image, then I would start rebuilding this images with first alpine related images, which is base images. Using that I would start doing the multi-stage builds of this Docker image, meaning I will try to build the required image using the base image and discard all the previous images.And I remove unnecessary package binaries that are present and remove packages that are not necessary for this application.

Explain the below IAM policy.

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "AllowS3ListRead",

"Effect": "Allow",

"Action": [

"s3:GetBucketLocation",

"s3:GetAccountPublicAccessBlock",

"s3:ListAccessPoints",

"s3:ListAllMyBuckets"

],

"Resource": "arn:aws:s3:::\*"

},

{

"Sid": "AllowS3Self",

"Effect": "Allow",

"Action": "s3:\*",

"Resource": [

"arn:aws:s3:::carlossalazar/\*",

"arn:aws:s3:::carlossalazar"

]

},

{

"Sid": "DenyS3Logs",

"Effect": "Deny",

"Action": "s3:\*",

"Resource": "arn:aws:s3:::\*log\*"

}

]

}

To begin with, this is version and this is locked, this will not changed.

The next is, we have three sid policies AllowS3ListRead, AllowS3Self & DenyS3Logs

Then there is a effect, meaning what kind of action can you perform, the high level action so we have two allow actions and one deny action.

In first example And in the allow also, we are specifying specific actions that can be performed and the resource here is all resources, that is all buckets.

In second example effect is allowed, action is everything is allowed here.That means we are allowing all the actions on particular two buckets only that are in resource.

In third example all S3 actions are denied on any S3 bucket that has suffix as log

Ans : You can say that this particular policy has basically three major high level actions that is to allow and one deny.And there is one particular action that is in the first section where we are explicitly mentioning what actions are allowed and resource is all the S3 buckets.In the second one, we are allowing all kinds of actions, but we are locking it to a particular S3 bucket.And the third one, we are denying all kind of actions for any buckets with a suffix log.

SET - 12

what is PV and PVC in kubernetes ? What role do they play?

Ans: PV stands for persistent volume and PVC for persistent volume claim.To get that PV, that is to get the persistent volume, we need to use the persistent volume claim in our deployment section or in our Yaml file, and we should request the PVC to find a volume that is required for us.And the PVC will take the responsibility of finding the PV for us.And if it is provisioned then it will allot to this pod.Just having PV or just having a PVC will not help us to get the pod because that is not the way it works in kubernetes. So PV and PVC both work hand in hand if it needs to be attached to the pod.

Well, I would like to mention one point here that PV can exist independently of your pod.

If you have a PV, it doesnt mean it has to be attached to a pod.

There can be a persistent volume that is not attached to the pod and it is totally fine.It is just there on the node or attached and later the PVC will come and it will claim this particular volume and give it to the pod.

PV is a storage resource in the cluster that is independent of any individual pod.Pods can use PVCs to request storage from available Persistent Volumes, and Kubernetes takes care of binding the requested PVC to an available PV.

When using TerraForm to create a RDS, How to save the DB username and password securely ?

Ans : To make sure that we don't commit DB username and DB password into the github repository as part of our terraform code, we can integrate the terraform with hashicorp vault. We have a provider for this so we can mention vault provider in our terraform, provider section and in our main code that is terraform code we reference the key & value pairs, and we can do that by also referencing the data block.

What actually happens is when we run terraform Apply, the TerraForm Apply will try to reach out to vault address given and it is going to fetch this key value pairs from the path and then it will create the database with the DB username and password.

Needless to say, the DB username and password first has to be also registered in vault meaning you should have a key and value with a username and password so that it can be integrated during this build time.

This is how we can make sure that none of the secrets like DB username and password or for that matter, any kinds of secrets will get integrated with our GitHub repository, which is a very bad practice. If we don't want to use vault we can use other secret storage engines example in AWS we have secret manager, secret manager is also a good option if we don't have vault set up in our organization.

SET - 13

What kind of DB's have you used/supported ?

Ans : I have worked with relational databases which are running on RDS of AWS. We are using mariaDB with RDS. We have also used DynamoDB which is NOSQL database.

I have used relational databases in my company because our application requires such kind of relational databases and we are cloud users and we use AWS cloud hense in AWS we are using RDS.In the RDS we have different kinds of databases, and we prefer to use mysql or mariadb.

Your security team has insisted that certain packages (security related packages) has to be present on all the instances for a defense project.

How would you come up with a solution for such a design and ensure that these packages will be present on all the EC2 instances that you will do that you will use ?

Ans : Custom AMI & ASG with Launch template OR Hashicorp Packer

I would suggest hashicorp packer to achieve this result because it is used for creating what we call as golden images, which can be used for such a project, especially defense related projects where we want custom AMI images are operating systems.

Well, if we don't know hashicorp Packer or if we are not aware of this tool, then I would also suggest that as an alternative, we can use Amazon AMI for the same, it can also give us the result but a kind note I would like to add here is if we are using Amazon AMI, it might be restricted to the cloud, If you are using Hashicorp Packer, we can move across different multi-cloud setup or on premises also.

SET - 14

Why do we have three different kinds of IAM policy types? (Managed, Customer managed and in-line policy)

Ans :

In AWS managed policy is basically the ones that are created by AWS and are completely managed by the AWS.For e.g AdministratorAccess, PowerUserAccess, ReadOnlyAccess, AmazonEC2ReadOnlyAccess, AmazonS3ReadOnlyAccess etc

And customer managed policies are something that we create for our used cases.For e.g when we were implementing CI/CD using Jenkins, We have created a customer managed policy throgh which we allowed jenkins to access S3 with permissions like GetObject, PutObject, ListBucket also we allowed jenkins to access EC2 with permissions like DescribeInstances, DescribeInstanceStatus, RunInstances, TerminateInstances also we allowed jenkins to access cloudWatch with permissions like GetMetricStatistics, PutMetricData

In-Line policy has a very special use case,meaning it gets created as part of the IAM user group or role.And when these group,role or user is deleted, the the in-line policy also gets deleted.

Also If we create a customer managed policy, we can attach this customer managed policy to multiple different users or groups.While inline policy is restricted to this particular IAM user group or role where it got created.

IAM Role : IAM role is a secure way to grant permissions to AWS services or other AWS accounts. Roles are used when you want to give permissions to AWS services temporarily, without needing to share long-term credentials like access keys.

IAM Policy : IAM policy is a document that defines permissions and access controls. It specifies what actions are allowed or denied on AWS resources. Policies can be attached to users, groups, roles, or directly to resources.

Managed policy - For e.g if we launched lambda that wants to add data to S3, there are some default permissions required to take this action. When we create these resources it will actually ask you for creating IAM role

E.g Developers group need read-only access to Amazon S3 buckets across multiple AWS accounts.Then we add AmazonS3ReadOnlyAccess to developers group to grant read only access to S3.

Customer managed policy - Customer created

Inline policy - Created & attached directly to IAM user, group, role

IAM user need temporary permissions to start and stop specific EC2 instances.Then we create inline policy within IAM users permissions.Once the temporary access is no longer needed, you can simply remove the inline policy from the user.

Which build tool are you aware of and what are the build tools you used in your project?

Ans :

In my last project our developer team tend to use Java and they use Maven as a build tool for Java.I don't personally work on build tools, most of the times our developer team works on build tool.But I understand the importance of build tool in the software development lifecycle SDLC. Build tools are essential for automating the process of compiling source code, managing dependencies, and generating deployable artifacts. Different programming languages require different build tools based on the project requirements. In future, if I encounter any development team that uses Python or NodeJS, then I would ask them to use npm package tool for NodeJS & pip or Pybuilder build tool for python as a build tool.

We have used maven as build tool in our project with jenkins as a CI/CD tool.

SET - 15

What is ingress and egress ? Where are these terms mostly associated ?

Ans : Ingress stands for incoming traffic and Egress stands for outgoing traffic.

And these both terminologies are closely associated with security groups, and we also call them as outbound and inbound traffic.

On a side note, I would also like to add that these are also associated with our VPCs and subnets, where we control our incoming traffic from the internet and routing the traffic between our subnets.

What is difference between docker image & docker layers ?

Docker layer is basically an image itself.It gets created with every single command that we write in the Dockerfile and it is important to know that darker layers are building blocks of the whole image. We don't need to access these layers independently when we created the container, but they are important for us to understand how the Docker image gets build and is used.

SET - 16

What is bastion host or gateway server ? What role do they play ?

Ans : It is a server that is used to manage access to an internal or private network from an external network.A bastion host is also known as a gateway server, a jump box or a jump server.Bastion host is also known as Gateway Server, is basically a server that manages access to an internal network in our cloud or on premises. Certain kind of applications might require this design and bastion host will come into handy.

The critical role it plays, is to controls the flow of the external traffic into our internal system via the server, meaning if we were to block all the external access, all we have to do is shut down the bastion host server

ASG having an issue with getting/provisioning new nodes. Its using complete spot instance. What could be the issue ?

Based on the given information provided, I believe that the spot prices might have increased than our bidding value and hence the auto scaling group might be having certain issues to provision the new machines.There might also be another edge case which is EC2 quota limit, meaning every account has a particular limit, it's a soft limit and we might be hitting the soft limit.If that is the case, we would go to support and request them to increase the EC2 quota limit.

ORSDD

on-demand(per hour/per seconds), Reserved instance(1-3 years reserved), Spot(bid unused instances), Dedicated instance(specific instance is dedicated, isolation at the virtualization layer), Dedicated host(physical server is decicated, isolation at the physical server level,)

GCSGB

General purpose(M5, T3), Compute Optimized(C5), Memory Optimized(R5, X1), Storage Optimized(I3, D2), GPU Optimized/Accelerated Computing(P3, G4), Burstable Performance(T2, T3), Micro(T2.micro)

SET - 17

A pod is trying to access a volume but it gives access error.We would like this pod to have access to this volume.What can we do to achieve the same?

Ans :

The error could be appearing because we might be trying to attach a particular volume, which only allows a read write once because of this the pod is having some issues.The solution for this also is we make the changes in our pvc and pv to make sure that a separate volume is created for this or we make sure that the volume that we are trying to attach supports read, write many permission.The example of Read Write Many is NFS and an example of read write once is EBS.

How is your kubernetes setup done on AWS

Ans :

In our current setup we are using AWS managed EKS cluster as part of production setup.If there is a need to have a staging setup done, the leverage kops to do the same and using which we are setting up our staging testing setup.The reason why we are choosing managed EKS cluster is it already gives us a lot of flexibility in terms of compatibility with other AWS components and less maintainability from our end meaning we don't have to spend a lot of time maintaining this kubernetes cluster itself.

SET -18

What are the load balancers in AWS ? Briefly explain which one you have used & use cases of others.

Ans :

In my organization, we currently use application load balancer only in most cases. The reason is we support a simple website that has xyz functionalities. Hence, the suitable balancer for us is application load balancer. We are sticking with application load balancer from a very long time and it serves our purpose. With application or balancer there are the load balancer is in yes, and I can give some information about them. We have a similar Balancer network here. Balancer and get filled balancer. What I am also about is Classic Balancer is supposed to be replicated very soon. Hence, there is no point in using them. Neither would I suggest them to be used in any existing project. Next, Modular Balancer also have a very specific rule, and they use different protocols for communication. We have not come across a use case for them yet, at least in the current project, but I am working with Gateway Load Balancer, as the name suggests, is this use case for a specific purpose when it comes to balancing the gateway traffic. And we are not using this service also at this point of time.

Do you use sonatype ? If yes please share why is it important ? If no then share why it might not be required.

No, I have not used sonarqube, but I am aware of what sonarqube is because I learned it out of my own interest.

Yes, we have used Sonarqube in our recent projects. Sonarqube is a tool that is primarily used to check code quality. It has been a great help for us because it allows our peer reviews to be done much faster. When we submit a pull request for peer review, our colleagues may not have the time to review everything, such as security vulnerabilities. By implementing Sonarqube, we can automate these checks, including lint tests, code quality tests, and security vulnerability scans. This way, we can ensure that our code is thoroughly reviewed before asking for a peer review. It also ensures that they developer do not make any mistakes, such as exposing secrets in the repository or downloading packages with known security vulnerabilities.It can flag many issues that can be fixed by the developers. It is an important tool that can be implemented in all companies to improve code quality and security.

SET-19

How do you handle incidents in your team ? What devops best practices you have implemented for the same ?

In our company, we have applications that collect the metrics that are required for monitoring. These metrics are collected by our monitoring system. In our case it is promethues/cloudwacth.And after that, we have certain alert rules which will check this matrix value if there are some metrics value that are missing, if there are some metrics, value on our proper, in that case, what we do is we send out an alert notification via our alerting system and it will call or call engineer.The call engineer will come online, try to resolve it or escalate further.I would also like to add that after the incident has happened, we will do something called aftermath effect that is we look back into the incident and see what happened or we can also call it as postmortem where we sit and analyze what happened during the incident and what are some of the actions we are taking to mitigate this for future.This best practice has to be implemented in every given organization so that we have a streamlined alerting and monitoring setup.I would like to add one thing here that is we need to make sure that we have a same kind of monitoring system or alerting system as possible through the organization, which again is the best practice of DevOps.

For incident management we have used promethues & slack in our organization.Prometheus continuously monitors our applications, services, and infrastructure by scraping metrics. This allows us to effectively detect any issues or breaches in predefined thresholds.

How to validate the variable during terraform plan time ? For example you take a variable called AMI. We need to make sure its of a proper format.

SET-20

Explain CMD and ENTRYPOINT in docker. Are these 2 same or different ?

Multiple EC2 instances in auto scaling group is getting terminated and this is causing downtime on the application site.EC2 pricing quota all look good.How would you start debugging this application out of this issue?

SET-22

What does terraform state lock really mean ? Do we have a practical use of it ?

Currently we have a Jenkins job, but we don't have any kind of notifications on

job success or failure. We use slack for our internal communication.How would you enable notification service in this case?

SET-23

What do you think is a future trajectory towards your journey of being DevOps engineer ?

In Ansible playbook, we have a section which could fail on certain nodes. But we don't want the playbook to stop or exit because of this.

Is it possible to ignore this, if this part of the playbook fails ?

SET-24

If you were to make a change for a commit done 30 days ago, with respect to a machine type used. How would you go about doing this change ? Would you directly change it ?

Create a linux script that will push certain logs to S3 automatically.Explain only high level design, which is enough. Share what all steps you would do to achieve

the above script.Bonus : Also, the script should run at a particular time.

SET-25

Explain in simple terms what is a package in python ?

Tell me about yourself & what are your day to day task being a DevOps engineer ?

SET-21/26

We want to launch certain pods only on specific nodes. These nodes should explicitly

used only for these pods.Is it possible to control the deployment of pods in such a given scenario ?

Let's say you have 2 servers with different ports and different usernames.Then how can Ansible handle different machines for applying and running the same runbook?

SET-26

What is the difference between a webserver and the applications server ?

Given 2 different Dockerfile below, which one do you think will have a lesser size when built ?

SET-27

How can you handle secrets in Ansible ? Lets say we have a playbook which needs to login to on-premises server with login name & password

What is Blue-Green Deployment ?

SET-28

What is multi branch pipeline ?

What is marketplace AMI ?

SET-29

A dev team wishes to go with a NOSQL database. But what is this NOSQL database & Do we have something in AWS that can get used as a NOSQL database.

We have an on-premises Linux server, which needs some monitoring enabled. Being

a DevOps engineer, only you have access to this server.How would you setup a basic monitoring script on this on-premises server ?

SET-30

Why is logging important? What is centralized logging and what tools helps to achieve centralized logging?

What is side car in container ?

SET-31

When running terraform apply, the process gets hung.Now if you cancel this, it might result in corrupt terraform state. How would you debug this issue?

What is a lag in read replica of a database ?

SET-32

Are you aware of Backtrack option in AWS Aurora ? How does it help?

What is branch protection in GitHub ?

SET-33

How does the kubernetes scheduler quickly assign worker nodes for the pods ? Explain the internal working of kubernetes scheduler

Please explain how you create your dashboard for monitoring services in your current

project ?

SET-34

Can you explain how "terraForm plan" and "terraForm apply" happens when using CI/CD

to provision a AWS/GCP infrastructure in your current project?

Can we control resource utilization per namespace in Kubernetes ?

SET-35

We have a commit that was pushed to main Branch.We don't want it now, We have to quickly remove this commit to avoid it getting deployed in production.Can you show us how do you do it ?

46.Docker

Question 1 : What is the best use case of dockerhub webhook integration.

Question 1 : What is cron & how does it work in Linux ?

================================================================================================Free Devops Interview Questions and Answers ===========================

===================================================================================

Check out pdf : F:/Interview PDFs/Udemy\_Interview/

SET-1

Explain the need of cloudtrail in AWS. Do you use it in current project ? What are some cons with using cloudtrail

You have a docker host (EC2instance), which contains 6 docker containers running.

If you restart the EC2 instance, will the Docker containers also be restarted automatically ?

SET-2

What are some key DevOps KPI's (key performance indicator) that you monitor in your team today ?

What is difference between git fetch & git pull ?

SET-3

What is the secret engine you have used in your organization and how does it help ?

What is git log ? What information in git log helps you ?

SET-4

Can we write docker-compose file in JSON ? If yes will the below command work fine or will fail ?

docker-compose -f docker-compose.json up

What is AWS Aurora ? What kind of RDS do your project use ? Speak a bit about database failure with respect to Aurora

SET-5

What is controller & agent in jenkins ?

What is local & remote artifact ? Which one is commonly used in organisations & why ?

SET-6

How do you handle security in jenkins ?

What is livenessProbe ? why is it used ? Also whats failure Threshold ?

SET-7

How is your jenkins setup done/managed ?

Have you come across tmpfs mounts in docker ?

SET-8

The developer from your team is complaining of connection drop to database.Explain how will you investigate this & provide solution if any

SET-9

How is secret engine used in your organisation ?

SET-10

What are 3 different types of cloud network connectivity ?

SET-11

Can you share 3 different sonarqube quality checks that you have come across ?

https://askdevops.notion.site/Docker-Network-Interview-Question-08339d842491490f840bfd351105462a

===================================================================================================== INTERVIEW QUESTIONS FROM PDF ====================================

====================================================================================

Describe branching strategies you have used ?

I have worked on Git which is distributed version control system. DVSC is independent on central server to store project files.

how do you revert a commit that has already been pushed and made public?

1.Remove or fix the bad file in a new commit and push it to the remote repository

git commit -m “commit message”

2.undo all changes that were made in the bad commit

git revert <name of bad commit>

How do you squash last N commits into a single commit?

git reset –soft HEAD~N &&

git commit

What is Git bisect? How can you use it to determine the source of a (regression) bug?

Git bisect is used to find the commit that introduced a bug

first we start git bisect using

git bisect start

Then we mark current commit as a bad commit , coz here our app crashesh

git bisect bad

From logs we get the good commit at which our app was working fine previously

git log

We use bisect again to check if app is working fine. If it works fine we go for this commit & if its not working we mark this as bad commit & again from git log we try new commit as a good commit.

git bisect good commit-id : check if app is working, if its not working try below

git bisect bad : this will check out another one check if it is working

git bisect reset - we will go to commit before git bisect start

If app is working fine & we want to revert the changes

git bisect good > copy commit-id

git show commit\_id\_of\_above\_good

git revert commit-id\_of\_above\_good > add message > wq

What is Git rebase and how can it be used to resolve conflicts in a feature branch before merge?

It merge another branch into the branch where you are currently working, and move all of the local commits that are ahead of the rebased branch to the top of the history on that

branch.

How do you configure a Git repository to run code sanity checking tools right before making commits, and preventing them if the test fails?

How do you find a list of files that has changed in a particular commit?

How do you setup a script to run every time a repository receives new commits through push?

How will you know in Git if a branch has already been merged into master?

git branch –merged lists

git branch -no–merged lists

SYSTEMS-MANAGER :

AWS-CLI IAM S3 VPC ELB CLOUDWATCH CLOUDTRAIL RDS DYNAMODB

ELASTIC-BEAN-STALK ROUTE53 LAMBDA-FUNCTIONS CLOUDFRONT CLOUDFORMATION CODE-PIPELINE CODE-BUILD

CODE-DEPLOY CLOUD-MIGRATION ECR ECS EKS AWS-TERRAFORM

Login to AWS account

Code Commit

Create codecommit repo

Create iam user with codecommit policy

Generate ssh keys locally

Exchange keys with IAM user

Put source code from github repo to cc repository and push

Code Artifact

Create an IAM user with code artifact access

Install AWS CLI, configure

Export auth token

Update settings.xml file in source code top level directory with below details

Update pom.xml file with repo details

Sonar cloud

Create sonar cloud account

Generate token

Create SSM parameters with sonar details

Create Build project

Update codebuild role to access SSMparameterstore

Create notifications for sns or slack

Build Project

Update pom.xml with artifact version with timestamp

Create variables in SSM => parametersore

Create build project

Update codebuild role to access SSMparameterstore

Create Pipeline

Codecommit

Testcode

Build

Deploy to s3 bucket

Test Pipeline

=============

**LOGIN TO AWS ACCOUNT**

**CODE COMMIT**

1.Create codecommit repo - vprofile-maven-repo > Public upstream: maven-central-store > This account > Domain: visualpath. We see 2 repositories one for maven-central-store used to store dependencies

2.Create iam user with codecommit policy – vprofile-arti-admin > AWSCodeArtifactAdminAccess > Copy Access & Secret Access key. On Gitbash aws configure & run command export CODEARTIFACT\_AUTH\_TOKEN=`aws codeartifact get-authentication-token --domain visualpath –domain-owner <account\_id> --query authorizationToken –-output text`. Run echo $ CODEARTIFACT\_AUTH\_TOKEN

3.Generate ssh keys locally

4.Exchange keys with IAM user

5.Put source code from github repo to cc repository and push

**CODE ARTIFACT**

Create an IAM user with code artifact access

Install AWS CLI, configure

Export auth token

Update settings.xml file in source code top level directory with below details

Update pom.xml file with repo details

SONAR CLOUD

Create sonar cloud account

Generate token

Create SSM parameters with sonar details

Create Build project

Update codebuild role to access SSMparameterstore

CREATE NOTIFICATIONS FOR SNS OR SLACK

BUILD PROJECT

Update pom.xml with artifact version with timestamp

Create variables in SSM => parametersore

Create build project

Update codebuild role to access SSMparameterstore

CREATE PIPELINE

Codecommit

Testcode

Build

Deploy to s3 bucket

TEST PIPELINE

Lift & shift Migration

Cost saving abhishek

Monitoring by promethues

CICD with jenkins