# Technical challenges for DevOps Engineer position

## Basics

> General

1. What is the role of AWS/Azure/GCP in DevOps?

AWS/Azure/GCP are cloud providers and provide services which are ready to use. There is no setup required or software to install. We can worry less about setting up, installing, and operating infrastructure and focus more on core product. We can automate manual tasks or processes such as deployments, development & test workflows, container management, and configuration management easily and fast also. We can scale up and scale down also very easy based on the requirement.

### One more benefit is Pay-As-You-Go.

2. How will you approach a project that needs to implement DevOps?

To implement DevOps for any project first I will understand the current architecture and manual tasks which are happening in project. After that make I clear plan and architecture after discussion with team which should satisfy agile principles.

Below Steps will follow for any Project which Requires DevOps implementation.

1. Check Impediments
2. Infrastructure readiness and install software's using Iac
3. Break the DevOps pipeline into tasks and start work on that.
4. After implementation of each task, enable that in DevOps pipeline

If we follow above steps and method, we can implement successful DevOps in very less time.

3. Mention some of the core benefits of DevOps.

The core benefit of DevOps is we can avoid discrepancy between development and ops team. Along with that below advantages we can achieve using DevOps.

* Continuous software delivery.
* Less complexity to manage.
* Increase **productivity** of business and IT teams.
* Improved operational support and faster fixes.
* Collaborative working.

4. What are the different phases in DevOps?

DevOps process is all about agility and automation. Each phase in the DevOps lifecycle focuses on closing the loop between **development** and operations and driving production through continuous **development**, **integration**, **testing**, monitoring and feedback, delivery, and **deployment**.

5. Explain the concept of branching in Git.

**Ans:** Branching in GIT is that you can create your own branch and jump between those branches. It will allow you to go to your previous work keeping your recent work intact.

A standard branching strategy is required for every project which helps to maintain code very easily and help developers to maintain their working code without impact on continuous delivery branch.

Based on branching strategy we can have different kind of branches like, feature, development, release, hotfix and master.

6. What is a merge conflict in Git, and how can it be resolved?

**Ans:** A ‘conﬂict’ arises when the commit that has to be merged has some change in one place, and the current commit also has a change at the same place. Git will not be able to predict which change should take precedence.

To resolve the conﬂict in git, edit the ﬁles to ﬁx the conﬂicting changes and then add the resolved ﬁles by running “git add” after that to commit the repaired merge, run “git commit”. Git remembers that you are in the middle of a merger, so it sets the parents of the commit correctly.

> Security

1. What is DDoS attack? How do you deal with it?

**Ans:** A distributed denial-of-service (DDoS) attack is one of the most dangerous things on the internet. If any website is being brought down by hackers means it has become a victim of a DDoS attack a victim of a DDoS attack. In short, this means that hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic.

Below are the symptoms of DDoS attack.

* The website is responding slowly.
* The website is unresponsive.
* The user has problems accessing the website.
* Internet connection issues if you are a target.

**Precautions to avoid DDoS attack:**

1. Configure firewalls and routers:

Firewalls and routers should be configured to reject bogus traffic and you should keep your routers and firewalls updated with the latest security patches.

1. By adding captcha, we can void DDoS attack.
2. The earlier a DDoS attack in progress is identified, we should notify your ISP provider as soon as possible to determine if your traffic can be re-routed. Having a backup ISP is also a good idea.
3. The best way to ensure that your organization reacts as quickly and effectively as possible to stop a DDoS attack is to create a playbook that documents in detail every step of a pre-planned response when an attack is detected.

2. What are the benefits of having Policy management?

**Ans:** Policy management is used to control network environments and protect organizations against evolving threats.

Since organizations will have more people and more devices, they seek ways to automate tedious and repetitive tasks, simplify operations, and identify inconsistencies that could leave them vulnerable to attack. Network security policy management helps in gain visibility across distributed environment, and then organize and standardize these policies to improve business security.

Network security policy management streamlines security policy design and enforcement. It applies rules and best practices to manage firewalls and other devices more effectively, efficiently, and consistently.

3. How HTTPS is different from HTTP?

**Ans: HTTPS** is **HTTP** with encryption. The only difference between the two protocols is that **HTTPS** uses TLS (SSL) to encrypt normal **HTTP** requests and responses. As a result, **HTTPS** is far more secure than **HTTP.**

4. What TCP and UDP vulnerabilities are you familiar with?

**Ans:** I have experienced with below TCP and UDP vulnerabilities:

* 1. DNS Spoofing
  2. Port scanning
  3. DNS Spoofing

5. Explain OAuth

**Ans:** OAuth is an open-standard authorization protocol or framework that provides applications the ability for “secure designated access. OAuth is about authorization and not authentication, It doesn’t share password data but instead uses authorization tokens to prove an identity between consumers and service providers. It approves one application interacting with another on your behalf without giving away your password.

Facebook apps are a good OAuth use case example. Say you’re using an app on Facebook, and it asks you to share your profile and pictures. Facebook is, in this case, the service provider: it has your login data and your pictures. The app is the consumer, and as the user, you want to use the app to do something with your pictures. You specifically gave this app access to your pictures, which OAuth is managing in the background.

6. What types of firewalls are there?

**Ans:** A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through

* Packet-filtering firewalls
* Circuit-level gateways
* Stateful inspection firewalls
* Application-level gateways (a.k.a. proxy firewalls)
* Next-gen firewalls
* Software firewalls
* Hardware firewalls
* Cloud firewalls

**> Additional features**

**\*\*Not\*\* required but would be great additional questions to answer**

1. Add to your plan how you would handle User Authentication

**Ans:** For any applicaton Json Web Token is best method to authenticate between multiple parties.

Once the Authentication server verifies the user’s credentials, it will create a JWT and sends it to the user. The app now gets this JWT and allows the user access to its data

Along with that we can use Oauth with active directory and MFA also be better approach.

2. How would you approach Microservice deployments using Azure?

**Ans:**

AKS is best service is to deploy micro service in azure, below steps we can take to deploy microservice in azure.

* Pods
* Services
* Ingress for routing and load balancing
* API gateway

3. How would you deploy API's in Azure and how would you ensure they are secure?

API’s can be deploy in private AKS and we can secure those using Vnet with subnets configured & Defined Azure network security groups as per the requirement.