Picking the Right Cloud Provider for Your Application - Part 3

This lesson continues the discussion about picking the right cloud platform to host your app.

We'll cover the following

Consider multi-cloud deployment - Break down your architecture into modules

A multi-cloud deployment simply means do not put all your eggs in one basket. If you aren't an indie dev or a small startup and have a comparatively bigger service to deploy, you can consider deploying your application across multiple cloud platforms.

This is only possible if your application has a loosely coupled architecture consisting of several microservices. These services can be deployed across multiple platforms eventually having no single point of failure in terms of cloud platforms. We are not locked in with just one cloud vendor.

The upside of doing this is that the developers and the operations teams get familiar with different cloud platforms, including their intricacies, pricing models, etc... In the future, it becomes easier to bail out on a certain platform and transition to another since things don't have to be learned from scratch.

Also, if we have an exit strategy, a *Plan B*, in mind right from the time we deploy our service using the proprietary technology of a certain cloud platform, it would save us a lot of distress if we hit an impasse anytime in future.

A multi-cloud deployment serves us really well during these instances.

Security

For many businesses, security is a decisive factor when making the decision to migrate to the cloud or not. If we work in finance, military, healthcare, or other similar domains and have sensitive data, we should go through the security policies of the cloud vendor thoroughly.

This is the reason most companies prefer a hybrid cloud architecture. The sensitive data is stored on-prem and the rest goes out to the public cloud. Moving data, also known as *data in transit,* is vulnerable to security breaches.

Here is a checklist of questions with respect to data security that you should put before the cloud provider you pick to run your service:

- Is the cloud provider encrypting your data? Both at rest and in transit?
- Does the provider ensure that only authorized accounts have access to your data? By authorized accounts, here I mean the accounts of cloud engineers of the platform managing your data.
- Does it have a security marketplace with security products from different vendors in case you need it? How easy is deploying those tools on the platform?
- Does the cloud provider comply with security standards and certifications applicable to your business domain?
- What's the vendor's policy with respect to government legal requests for data?
- Has there ever been any major security breaches or failures in the past?
- How secure the data would be in case you implement a hybrid architecture and stream your data over to the cloud?
- Does the provider have a dedicated security team to resolve issues as soon as they are encountered?
- How are the data centers physically secured?
- How are the users authenticated? What is the process for preventing network intrusions?
- What are the data deletion policies?

Support

Support is another important factor to consider when giving business to a cloud vendor. Do they have a dedicated technical support team? What's the support policy? Is the support paid? If yes, what's the support pricing model?

Run a google search to get an insight into the market sentiment for a particular cloud provider.

Cloud marketplace

All the big cloud platforms have respective marketplaces that offer third party utilities, developer tools, solutions, and services to accelerate the development. Before writing a utility from the ground up, businesses generally look into the marketplace for that utility to save resources and time.

> You can visit the *AWS marketplace* and *Google Cloud marketplace* for details.

The cloud provider you pick should have an active third-party marketplace.