How to Build a Cloud Computing Infrastructure: 7 Key Steps

Cloud computing is becoming an increasingly popular option for businesses of all sizes. By implementing a cloud computing infrastructure, businesses can improve their efficiency and agility while reducing costs.

Building a cloud computing infrastructure can seem like a daunting task, but it doesn't have to be. By following these 7 essential steps, you can build a cloud computing infrastructure that's right for your business.

In this blog post, we will outline the essential steps for building a cloud computing infrastructure. We will also discuss the components that are necessary to create a successful cloud strategy. Let's get started!

1. Define your business needs and goals

Before a business can implement a cloud computing infrastructure, it needs to carefully define its needs and goals. These needs and goals can be evaluated by asking questions such as:

- What types of workloads will be moved to the cloud?
- How many users will need to access shared cloud resources?
- What are the performance and availability requirements?
- How much data needs to be stored, and how often will it need to be accessed?

Once these needs are understood, the next step is to identify which cloud deployment model – public, private, or hybrid – is best suited for the business.

Finally, the cloud service provider must be selected and the infrastructure put in place. There are a number of different cloud computing providers, each with their own unique offerings. It is important to compare and contrast these options in order to find the best fit for the business.

By taking the time to answer these important questions upfront, businesses can ensure that their cloud computing infrastructure is deployed in a way that meets their specific needs.

2. Choose the right cloud platform

Determining which cloud platform is the best fit for a business can be difficult. There are a variety of cloud providers – including those offering private cloud, hybrid cloud and public **cloud services**. Each of these providers comes with their own set of features and pricing models.

More importantly however, the needs of each business vary, making it important to select a platform whose cloud computing services meet the specific requirements of the business. So, with such a variety of options to choose from, how can a business select the right cloud platform?

One way to narrow down the choices is to consider the cloud computing infrastructure offered by each provider. For example, if a business needs a scalable and highly available infrastructure, then a provider that offers these features should be at the top of the list. Another consideration is the price model. Some cloud providers charge by the hour, while others have monthly or annual subscription plans. Once again, it is important to select a plan that fits the budget and needs of the company.

Finally, it is also important to consider customer support when selecting a cloud platform. After all, even the best cloud platforms can experience downtime or other issues. When problems do arise, it is crucial to have access to 24/7 customer support in order to get the issue resolved as quickly as possible.

3. Set up your virtual infrastructure

Once the cloud provider has been selected, businesses can begin to migrate their existing data and applications to the cloud infrastructure. Migrating data and applications can be a bumpy ride, so here are a few insider tips to make the **data migration** process go smoothly:

- **Take inventory of what you need to migrate**

This will help you determine which cloud provider is a good fit, and what kind of migration tools you'll need.

- **Establish a timeline and business case for the migration**

This will help you get buy-in from stakeholders and ensure that the project stays on track.

- **Check the cloud technology included with your cloud provider**

Finally, consider using a cloud platform that offers built-in migration tools. This can save you time and money in the long run.

4. Configure security and networking

Cloud computing architectures are highly secure, but you'll need to take steps to protect your data. When configuring security and networking for a cloud computing infrastructure, there are a few important factors to consider.

First, you need to make sure that all data is properly encrypted. This will help to protect sensitive information from being accessed by unauthorised users.

Second, you need to ensure that the network is properly configured. This includes setting up firewalls and implementing robust authentication and authorisation controls in order to ensure that only authorised users have access to the network and its sensitive data.

Finally, you need to make sure that the **cloud computing** infrastructure is properly monitored. This includes monitoring for unusual activity and keeping an eye out for any potential security threats, especially if you are using public cloud computing. Security threats can sometimes present as a disadvantage of cloud computing, but generally the positives outweigh the negatives. Find out more **advantages and disadvantages of cloud computing**.

5. Configure your storage solutions

When configuring storage solutions in a cloud computing infrastructure, it's important to consider the needs of your applications and workloads. For example, if you're running a cloud-based database, you'll need to ensure that your storage solution can provide the required performance and capacity for both your operating systems and your data storage, especially if you're a business with a large data set. If you need more information about **where data is stored in cloud computing**, we've got the perfect blog.

You'll also need to consider issues such as data redundancy and security. Fortunately, there are many different storage solutions available for cloud environments, so you should be able to find one that meets your specific needs.

Once you've selected a storage solution, you'll need to configure it appropriately for your cloud infrastructure. This process will vary depending on the solution you've chosen, but in general, you'll need to create storage accounts and set up replication and security. By taking the time to properly configure your cloud-based storage solution, you can help ensure that your applications and workloads have the resources they need to run smoothly.

6. Deploy your applications

Businesses will also need to deploy their applications to the cloud infrastructure. This can be done using a platform-as-a-service (PaaS) solution or by manually provisioning virtual machines (VMs) and other resources.

In the cloud, applications are hosted on a network of remote servers, which are accessed over the internet. When deploying applications in a cloud computing infrastructure, it's important to consider the below factors which can help with successfully deploying applications in the cloud:

First, make sure that your application is compatible with the cloud platform you're using. Not all applications are well suited for cloud deployment, so it's important to do your research upfront.

Second, create a detailed plan for how you will deploy your application. This should include both the technical aspects of the deployment as well as any business or organisational considerations.

Third, test your application thoroughly before deploying it to the cloud. This will help to ensure that there are no unforeseen issues when you go live.

Finally, be prepared to scale your application according to demand. Cloud deployments can often experience spikes in traffic, so it's important to have a plan in place for how you will handle increased demand.

Additional tips to abide by include:

Balance workloads between multiple servers: In order to avoid overloading a single server, it is important to distribute workloads evenly across multiple servers. This will help to improve performance and reduce the risk of outages.

Use automation tooling: Automation can help to speed up the process of provisioning and configuring servers. This can save time and money when deploying applications in the cloud.

Once your applications are up and running, you'll need to monitor them closely to ensure that they are performing as expected. This includes monitoring application logs, tracking performance metrics, and setting alerts for when issues arise.

7. Manage and monitor your cloud environment

Cloud computing infrastructure can be a complex and ever-changing landscape. To ensure that your cloud infrastructure is running smoothly, it's important to have a cloud infrastructure management plan for monitoring and managing your cloud environment. Here are some tips:

First, create a cloud management strategy that outlines your goals and objectives for the cloud. This will help you prioritise tasks and make sure everyone on your team is on the same page. Make sure to also define clear roles and responsibilities for those who will be working with the cloud infrastructure.

Next, establish governance policies and procedures for how the cloud infrastructure will be managed. This can include things like who has access to the cloud, what kinds of changes can be made, and how changes will be tracked.

Next, set up a cloud monitoring system that tracks key performance indicators (KPIs) such as uptime, response times, and resource utilisation. This will give you visibility into how your cloud infrastructure is performing and identify areas for improvement.

Finally, establish a process for regularly reviewing your cloud infrastructure and making changes as needed. This might include adding new features, adjusting resource allocation, or scaling up or down as needed. By having a plan in place for managing and monitoring your cloud infrastructure, you can keep it running smoothly and avoid any unexpected surprises.

To conclude

Cloud computing is becoming an increasingly important part of business, and many businesses are looking to build their own dedicated cloud infrastructure. If you're one of

Log monitoring

Collect log data across applications, cloud services, and on-premises to monitor, analyze and troubleshoot performance and security issues before they impact users.