



What Causes Server Downtime and How Can It Be Reduced?

A server is a piece of hardware or software on a computer that offers information, resources, and software to other systems. Your company's vital information is stored on servers, which act as a single central system from which it can be accessed, shared, or managed. Since servers are used to deliver constantly needed services, they will always be ON. Therefore, since servers are an essential component of business operations, consider what would happen if one went down for even a brief period. Unplanned server downtime has a direct negative impact on a company's productivity and revenue. Thankfully, we can put in place a set of best practices to avoid such unanticipated server downtime

Let's take a quick look at server load before discussing server downtime to understand why it's important to monitor server load.

What is a server Load?

The strain on the server will increase as the server load increases. Therefore, it is always recommended to keep the server load level within the acceptable range for optimal server performance.

Many variables affect server load, with distributed denial-of-service (DDoS) attacks being the most frequent culprit. A DDoS attack overloads the server with many requests, causing it to crash. Your company may sustain severe damage as a result. Therefore, if you see that your server's load is peaking and worrying you, think about getting in touch with a [server management company](#) to identify and fix the problem.

How Can Server Downtime Be Reduced?

Let's now talk about the best practices for reducing server downtime. It should be noted that it is not at all possible to completely prevent server downtime.

Human Mistakes

According to numerous studies, human error is the main reason for server downtime.

According to a study done by computerweekly.com, human error accounts for about 75% of all downtime.

Therefore, data centers and companies need to make sure that only authorized individuals can access the server and make changes. The likelihood of errors can be decreased by properly documenting the routine tasks that must be completed.

Protect Yourself from Cyberattacks

An additional significant factor in server downtime is cyberattacks. Cyberattacks, particularly DDoS attacks, can affect servers. For businesses, being the target of a DDoS attack can be disastrous. DDoS attacks flood servers with many requests, causing the server to become overloaded and crash.

One of the simplest ways to prevent a DDoS attack is to add redundancy to your infrastructure by distributing your servers across various data centers with a good balancing system. But it appears that implementing an anti-DDoS hardware and software module is the most efficient. On top of the installed hardware, anti-DDoS software helps filter out malicious traffic. One of the easiest and most economical methods is this one. Other ways to stop a DDoS attack include anti-DDoS hosting and an anti-DDoS firewall.

Have an Uninterrupted Power Supply (UPS)

Your server's power supply can be maintained with the aid of a reliable uninterrupted power supply (UPS) system. Additionally, UPS aids in reducing power peaks and averts unanticipated surges that could damage your system.

Plan frequent backups

Hardware failures on servers are frequent and can occur at any time. As a result, it is always advisable to regularly back up server data so that you can quickly restore it in the event of an emergency. Your business data is safe and secure with regular backups. Without a backup, it would be impossible to recover data from hardware that had been damaged, costing your company important data. There are numerous types of backup solutions with varying scopes on the market. Choosing the best option based on your needs and requirements is always the best course of action.