

What is Failover and Why is it Important?

We rely so much on our systems these days that there's a surprising amount of server space that we'd simply couldn't operate without.

This is most often realised with occurrences like hardware malfunctions or, more maliciously, DDOS & other cyber attacks. In these instances, thorough failover and Disaster Recovery plans become literal life-savers in real time. But what exactly is failover and why is it so important?

Let's find out.

What is failover?

Failover is a shorthand for a backup server that lets effective service continue without any noticeable difference on the front end. It's used for 'high-availability' systems that must continue to run in order for operations to continue.

When set up properly, there should be no reduction in traffic, no downtime, and no change for the user. However, depending on the exact machines in the network, there might be fractional reductions in availability for exceptionally high-load systems in the few microseconds it takes to switch over to the backup system.



Why is failover important?

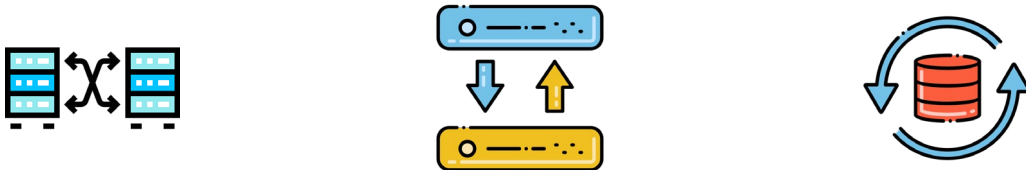
To put it in oversimplified terms: when you depend on a life support machine, you'd be in trouble if it stopped working.

In practice, what businesses today depend on is not only that their websites remain accessible so that customers can find information, contact, and pay the business, but also that they're able to accept payments properly, show the right information from databases, and so on.

Depending on the business or organisation, the reasons for a particular machine becoming inactive can be various: from simply needing to be temporarily turned off to be updated, to a hardware malfunction, to a purposeful cyber attack.

It's also a great way to be able to run updates to systems, test them, and revise them in real time, without having to account for total system shutdown.

Failover protocol, then, serves as a key component to enable continuous uptime.



There are numerous ways to set up failover, and the most effective method depends on the individual scenario; each business will have different resources available and different goals for failover.

The usual method is to have multiple machines that broadcast a Virtual IP address (VIP). This means that requests go to the same network. These machines are themselves tethered in a Primary/Secondary/Tertiary priority order so that any requests are first directed to and routed through the primary machine to whatever information is requested. When that machine becomes unresponsive, requests then flow through the secondary machine, and so on.

This switchover to the backup happens in fractions of a second, so isn't enough to be disruptive. When updating, for example, it allows for the updating of the secondary machine, which is then switched over to be the primary machine once updates are deemed to be stable. The other machines then duplicate that primary one.



Should I implement failover?

Absolutely! While the cost sheet may sometimes appear discouraging, being able to have a backup system for your vital services can solve a lot of headaches and, in many regulated industries, is actually a requirement for cyber safety certification.

If you have any questions, [get in touch](#). We'd be glad to advise on anything cyber! Discover more about [our failover solutions here](#).