



Fresh Mango's Guide to On-premises (physical) servers and Cloud servers

With remote working here-to-stay in one form or another, many businesses are questioning what kind of server solution they should have – On-premises or Cloud. Our guide highlights the main differences and the pros and cons of each approach.

On-Premises Servers vs Cloud Servers

The main difference between physical and cloud servers is their location: a physical server is located on-premises, a cloud server is situated in a remote location (which could be a data centre or a larger cloud infrastructure) and accessed remotely. Cloud servers can be dedicated or virtualised, in exactly the same way as On-Premises servers.

Pros and Cons

A physical server is the preferred option for performance-oriented scenarios. With the server located on your premises, data transfers are fast and server access is not broadband-dependent. Also, a physical server provides more control over your data (and data security). Sometimes, a physical server may be the only solution if your business operates specific line-of-business applications.

A cloud server removes any hardware and maintenance costs. It can be easily accessed from everywhere where you have an internet-connected computer. However, it – and therefore your business - is reliant on Internet broadband. The broadband will need to be fast, especially if you have many users or large files to edit. Also, it may not be possible to run certain applications on a full cloud environment.

Active Directory vs Azure AD

Active Directory is a critical component of a Domain Controller, a physical server that centrally manages users and computers on the network.

Azure AD is a full cloud solution that performs some of the same functions as Active Directory, but it is quite different – Azure AD does not replace Active Directory, but it represents an excellent alternative in several situations.

Pros and Cons

Active Directory is the best option for complex and large networks, with multiple users/departments and computers. It provides several tools to manage users and computers in details. Active Directory can manage every network component, including other servers.

For this reason, AD is the preferred solution if on-premises applications servers are required. Active Directory is not accessible from outside the network without configuring VPN access, and it requires a physical server environment.



Azure AD is the perfect solution for small networks, especially if newly provisioned. It provides a central management point for users, and limited control over computers. Azure AD also provides management for mobile devices.

Since Azure AD is a cloud service, it can be accessed from everywhere, but it is broadband-dependent. Azure AD can be integrated with other cloud services, such as Office 365 and OneDrive/SharePoint.

The main benefit of Azure AD is the possibility to have a single sign-on for different services and enable additional security measures (such as multi-factor authentication).

It is not possible to manage existing physical servers on Azure AD, and the system does not provide any options to manage different user departments, or fine-tune computer settings. In these scenarios, Active Directory is the preferred solution.

We hope that helps and do [contact Fresh Mango today](#) to discuss the next steps for your business server.