Best Practice

Quickly migrating apps into the Cloud.

Four measures to make business critical applications available via Azure.

Campana Schott

Many companies operate applications that are critical to their business in their own computer center. But in times of crisis, limited accessibility leads to challenges. The four measures described below make it possible to quickly migrate business applications into the Cloud.

There are good arguments for providing critical applications in the company's own premises: data sovereignty, control and established processes for configuration and management. But in exceptional situations - for example if many employees are working from home - this setup can lead to significant challenges.

For example, when systems can only be accessed by VPN or in the company's own network for security reasons. But many companies have not set up VPN connections for all of their employees, or such connections only come with a limited bandwidth.

Often, the Internet connection in the home office reduces app performance because some client/server applications are optimized for network access and require a lot of bandwidth. In addition, certain applications can only be used remotely via terminal servers. This can have a negative impact on the efficiency of employees working from home, if they cannot copy and edit documents on their desktop, for example.

Therefore large-scale remote access means that applications must be made available via the Cloud. The Azure platform provides companies with a multitude of options for the short- or medium-term migration of apps. The following four measures are recommended:

1. Short-term solution: Azure Reverse Proxy

Many critical, web-based applications such as purchase order systems can only be accessed in the company's network, because they run in the Intranet. Microsoft's Azure AD Application Proxy offers a simple solution for making available on-premises web applications through the Azure AD Portal. Users are authenticated through Azure AD and the user context is forwarded to the on-premises web application.

The on-premises systems are then made available in a VPN without dial-in but can still be made secure using Azure's security functions. To access the on-premises systems, Azure builds a secure tunnel on an application proxy connector. The required adjustments for the on-premises system environment are minimal. For example, companies can quickly reverse the adjustments after the crisis situation has passed. The cost of migrating in both directions is relatively low

2. Short-term solution: Interaction through the Cloud

Often, employees working from home who access company systems are no longer able to perform certain work or approval processes, or they are no longer able to do so within the required time frame. To accelerate these processes, companies often only need to simplify one single step (e.g. approval signature) for their employees.

Through the platforms Azure/O365/D365, Microsoft provides gateway components for this purpose. They can be used to migrate individual interaction steps from on-premises systems into the Cloud. With the help of Power Platform components, these solutions can be made available independent of the device, i.e. in equal measure for cellular phones, tablets and PCs. Here too, on-premises gateway components create a secure connection to the end points in the Cloud.

Rapid implementation and almost no required adjustments to existing processes avoid interruptions in the existing workflows. In this way, approval steps in particular can be provided without a VPN connection, and employees are able to react more quickly even outside of the company's network. The cost of such an implementation is also low, as only single process steps are adjusted.

3. Short-term solution: Lift & Shift

Client/server solutions in particular often exchange large volumes of data, which puts considerable stress on the company's Internet connections. These processes frequently involve special applications in specific departments, such as documentation systems. Usually, they are hosted via on-premises VM systems.

Azure also enables the hosting of VMs. This means that on-premises applications can be easily migrated by migrating the VMs. Companies benefit from access and direct authentication via Azure. In this way, a VPN is no longer required as the Azure network is also available as an option (and depending on the connection). This relieves the pressure on company Internet connections and improves access performance. The VMs remain in the domain, i.e. in the company's operating processes. The cost for the rapid VM migration to Azure can be kept to a minimum because only few adjustments must be made to the existing architecture.

4. Medium-term solution: Migration of apps based on Azure components

In the medium term, it pays to convert existing solutions on the basis of Azure components, in order to take greater advantage of the benefits offered by the Cloud. By the latest after the short-term conversion, companies should begin to adjust their applications accordingly, so they can benefit from the advantages of accessing applications via scalable Cloud architectures.

Options include a direct migration from? on-premises applications, as well as a gradual redesign according to Lift & Shift.

The solution architecture is based on tailor-made Azure components. They enable server-less and micro-service architectures.

The advantages of this solution are:

- Easy scaling, particularly during high peak times
- No fixed operating costs for components, instead costs are based on inquiries/expected useful life
- Reduction in access rate for the company network

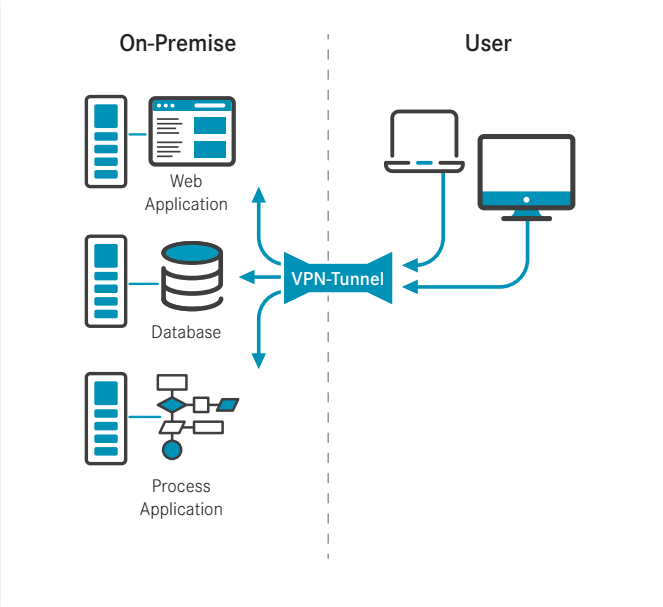

Illustration 1: Corporate solutions are accessed via a central VPN access

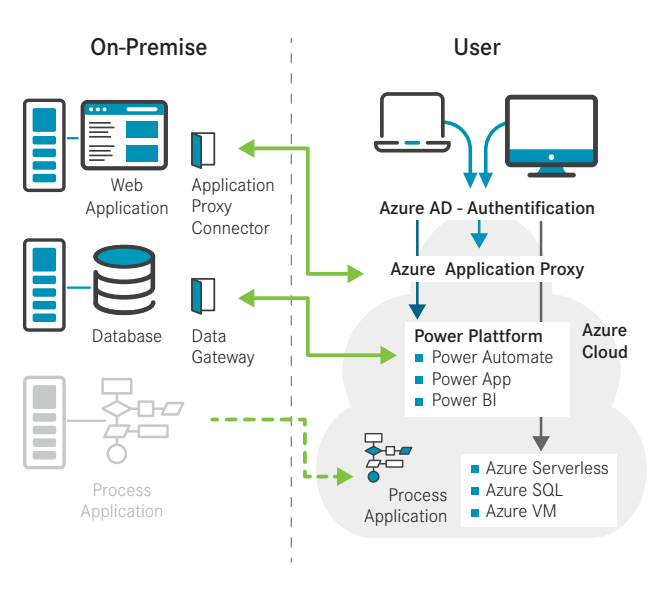

Illustration 2: Cloud-based applications allow access without a VPN connection

These are the advantages of Azure:

Overall, the benefits for the companies that are able to quickly provide critical applications via Azure are as follows:

- Authentication from the Cloud using Azure AD, which also simplifies the roll-out of multi-factor authentication
- Azure as a platform comes with an extremely high security standard and can be made even more secure with additional security features. Attacks on the Azure infrastructure are permanently averted by Microsoft specialists.
- Simple scaling through the use of Azure server-less components or adaptive architectures
- No investment in hardware, so that transitional solutions can be reversed easily

Conclusion

In times of crisis, companies must act quickly to provide short-term solutions for remote access with the same standard of performance. But in the medium term, they should also begin to implement the Cloud migrations that are anchored in their IT strategies. If you require assistance, feel free to direct your inquiries to your contact person at Campana & Schott. Our consultants provide integrated support services to IT departments – from IT strategy and Business Continuity to the implementation of solutions and change management for employees.