HOW TO MOVE SAP® TO MICROSOFT AZURE:
CONSIDER THESE 5 KEY POINTS

Interfaces, Interfaces, Interfaces

Migrating your SAP landscape to Azure could impact how your SAP systems talk to your other business systems. Make sure your interfaces and system connections are well-documented; you'll need to reconfigure these. Often due to staff changes or documentation challenges, interfaces may not be recorded. Explain in detail when the interfaces run, how they transfer data, and where they transfer to. Look for permissions, drive shares, external services such as FTP/SFTP/Email, and ensure all those details are recorded. Diagrams help immensely!

Networking

Your SAP systems will be moved onto new network addresses. This will impact how your SAP systems talk to each other. Get your network topology up-to date! It's possible that your existing systems are on IP addresses that could clash with the reserved addresses in the public cloud. Most IT organisations will have detailed lists of these addresses; make sure they are up-to-date, and also include all the systems that are on the periphery of your SAP systems.

Micro-segmentation

Have you split your SAP landscape into different networks? Are your Sandbox, Development and QA environments separated out? If not, migrating to Azure is a good time to start thinking about it. The security departments within businesses are putting pressure on business units that run SAP to ensure that they are as secure as possible. These SAP systems are often the core of your business, and have a very high impact should a security breach occur.

Micro-segmentation is where you split out and separate different sections of your landscape into their own networks and put security policies in place to aggressively control data flow in and outside those systems. Retrofitting fine grained micro-segmentation to an existing SAP landscape can be very time-consuming, with high business impact. With cloud migrations, the move to Suite on HANA and S/4HANA creates the opportunity to implement this on the target side. Going from a flat network structure to a fine-grained security topology is a journey that you need to think about; this should be a core focus for your migration.

Security

Have you anonymised your non-production landscape? Cloud security models are shared ownership. There have been numerous reports of the last couple of years of data being exposed to the public. Care must be taken when configuring your storage, especially during migrations to ensure that data is transferred encrypted and that the permissions are secure. Take a look at the data itself and anonymise as much of your non-production data as you can. Trimming down your non-production data will reduce your attack surface, and combined with anonymisation will greatly reduce your exposure.

Cost optimisation

The costs when running in the public cloud can be high, especially when running HANA. Have you thought about reducing the size of your production and non-production landscape? HANA is an in-memory database which can cause a significant increase in IT budget spend. Over the last 10 years, the cost of running IT infrastructures has dropped due to server innovations. It can be an uncomfortable conversation between the business and the IT stakeholder when you explain that HANA = more expensive systems. By reducing your database size, you will reduce the size of the system that needs to run it. This will decrease the cost of running it. Reducing the data in your production and non-production landscape will make the business case to migrate to the public cloud much more feasible. Data from your production database can be archived and stored in a non-HANA platform that can be much cheaper to run.

EPI-USE Labs can help you with your move to Microsoft Azure.
Contact us at **epiuselabs.com | sales@labs.epiuse.com**

EPI-USE Labs is a member of the groupelephant.com family