Migrating an existing on-premise enterprise application to Windows Azure Cloud

Kulraj Singh Kohli & Saurabh Sharma

Industry Background:

We deliver digital transformation and technology services from ideation to execution, enabling clients to outperform the competition. We enable IT to move at the speed of business, leveraging emerging technologies and the efficiencies of Continuous Delivery to spur business innovation. Our major focus areas are data analytics, IT infrastructure, application development and maintenance. We have an employee base of around 8000 globally.

Migrating our employee performance application to the cloud:

We have an on premise deployed, employee performance recognition application which we are planning to migrate to the cloud. Migration is discussed using this system as an example for both Windows Azure, through Cloud services (PaaS) and virtual machines (IaaS) implementation models. The current architecture and deployment setup of this application:

· Is built with ASP.Net 3.5 and hosted in an on-premise data center. It can be accessed from the intranet (within organization) and the internet. The application relies on Microsoft Active Directory services to authenticate employees.

· Uses a standard Microsoft SQL Server 2008 database for storing application data.

· Communicates with other production databases within organization to fetch employee and other related data

· Using a linked server.

· Connects to the production databases using a service account.

· Stores the images uploaded to or created from the application using network file storage.

· Is hosted on single instance server

Reasons and analysis for moving to the cloud:

We are planning to make use of cloud services in order to cut cost of maintaining on-premise data centers and also we would want to make use of data processing and analytical services to make wise decisions related to employee performances, recognition and awards along with making better strategic decisions for rewarding our employees. This application will also help our HR team in assessing employee performances and calculating bonuses.

Working with the CFO:

A chief financial officer will definitely have questions while you are planning a cloud migration strategy. First thing the CFO would want the answers related to are the finances. If we are prepared to answer the questions appropriately then we might answer the biggest concern for him. As we know that the cloud gives us several ways of saving costs and the biggest of them is pay as you go pricing policy. On the other hand, when we are going for on-premise setup, we have to take care of a lot of licensing and premium paying plans which are a hassle for the CFO as well. A business can receive upgrades automatically and avoid the fuss of maintenance and management. This is the type of change a CFO needs to be aware of. He or she needs to think long term when planning a cloud move and decide which approach is best. With metered costs, the CFO can experience increased budget flexibility and work with the CIO to ensure successful migration.

The provider offers resources delivered as a service, and takes care of the purchase, storage, management and maintenance of the necessary infrastructure. This enables businesses of all sizes, in all industries, to take advantage of the latest technology without overspending, from startups to the biggest industry leaders.

Scalability leads to other benefits, including the possibility to reach customers across the globe and quickly bring them online, as well as minimizing energy consumption and excessive equipment.

Security is a huge concern to CFOs, and that's valid. It's frightening to trust your data in the hands of someone else. But think about it this way: a cloud provider relies on the ability to offer a more secure solution than an organization can provide itself. If we can give assurance related to security issues, another battle is won. So more or less it is good to have a CFO and our side and a thorough preparation to answer his expected concerns should be made in advance.

Goals and alignment with company's success goals:

Our cloud strategy primarily focuses on two aspects:

1. Cutting costs

2. Real time analytics

With the aforementioned two factors as we deal with the employee's sensitive data such as SSN, we would also want to focus on the features pertaining to security and compliance while opting for cloud service providers. We would also want to select cloud services from such a provider which has in-built APIs and easy to use platform as to leverage the cloud services and at the same time keep the costs in check. So, we have following factors to consider while devising the cloud strategy for our organization:

1. Security

2. Expertise and Resources

3. Managing Costs

4. Governance and Control

5. Compliance

Departmental objectives:

1. **Executive/Business:** Able to quickly deliver results, analytics for employee performance assessment, rewards distribution and HR analytics

2. **IT:** Operational simplicity and cost savings, access to various on-demand services, emerging tech adoption

3. **Other departments:** Shared access and collaboration, increased performance

We also perform SWOT analysis for considering whether moving to the cloud would be a right step for our organization or not:

Strengths: Cost cutting, easy maintenance, in-built APIs, speed, efficiency

Weaknesses: Training and new staff requirements might increase cost, security and compliance issue might also increase the burden

Opportunities: Data processing and analytics to increase clientele and capture market

Threats: Disruption of existing services, wrong selection of deployment model or cloud services or service provider may incur extra costs and little benefits

Cloud Migration Strategy

1. Assessing the current infrastructure:

We now need to assess our existing IT infrastructure, the applications we currently use, the resources, costs and other details. This will help us in making which applications are better suited for cloud and which one can be kept on the existing servers. So, as a grocery store chain we might be having some performance intensive applications on our local servers for calculations and inventory management. It would be wise to not migrate any performance intensive applications over cloud.

The other factors which we would like to consider:

· We would want to consider our current data storage needs, daily new data generated, current analytics performed, networking and expected SLAs.

· Current costs related to physical servers and server management.

· Hidden costs involved.

2. Choosing the right cloud deployment model:

Our next step towards building an effective cloud strategy is to determine how we want to deploy cloud within our organization, and we need to choose a deployment model which is right for us. As we know, there are various cloud deployment models available such as public, private, community and hybrid. Let us compare these models:

a. **Public Cloud:**

Advantages: Hassle free infrastructure management, high-scalability, low costs

Disadvantages: Compromised reliability, privacy and security concerns, the lack of bespoke services.

b. **Private Cloud:**

Advantages: Secure, high scalability, high reliability, bespoke development

Disadvantages: Costs (Not suitable for small companies)

c. **Community Cloud:**

Advantages: Reduced costs, improved security and reliability, ease of data sharing and collaboration

Disadvantages: High costs in comparison to public cloud, fixed storage and bandwidth limitations

d. **Hybrid Cloud:**

Advantages: Improved security and privacy, enhanced scalability and flexibility, reasonable price.

Disadvantages: Suitable when we can divide the data into mission critical and non-sensitive.

Solution: Our requirements are low costs, ease of setup and use, high data security and privacy, high reliability and high scalability and flexibility. Depending on these features, we believe that hybrid cloud will be a suitable option for our enterprise level solution.

3. Choosing the right type of cloud service:

Now as we have decided the deployment model, the next step will be to identify which type of cloud service would be an ideal fit for our requirements. The three commonly used service types are IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service).

SaaS: It allows people to use cloud-based web applications. Some of the most commonly used applications like Gmail, Office 365 and Google docs come under this category. Also, the Customer Relationship Management tools provided by vendors like Salesforce and Microsoft also come under this category. For our mid-sized grocery store, there can be many applications which we can use if we opt for this kind of cloud service model.

PaaS: This refers to the service platforms that provide runtime environments for developing, testing and managing applications. This service type is an ideal fit for developers but in our case, this might not be a good fit.

IaaS: This service provides basic computing infrastructure such as servers, storage and networking resources. It can act as a virtual data center. These services can be used to handle big data. We can install and use whatever operating systems and tools we like on the infrastructure we get. Popular IaaS providers include Amazon Web Services, Microsoft Azure, and Google Compute Engine.

An advantage of all the above-mentioned service types is that they follow pay as you use model of pricing which makes them cost effective

Selecting the right model based on our needs: A combination of PaaS and IaaS can be a good fit for our requirements. For computing needs, we will need virtual machines and, in that case, IaaS would also be required. So, for us a combination of IaaS and SaaS is required.

IaaS: It will provide us with virtual data centers, computing power and data analysis capabilities. It is widely used for data mining and analytics. This service model is also reliable, scalable and secure and requires almost negligible expenses on hardware infrastructure.

PaaS: The PaaS service model plays a crucial role in creating a customized software solution. The PaaS service platform will be providing an integrated development environment with all the necessary tools to create and deploy our application and will also help in continuous integration and changes to our application.

4. Choosing the right type of cloud service provider:

Next step will be to select an ideal service provider which could meet our cloud service deployment and cloud service type needs at the same time which is cost effective and provides prompt customer services and the correct set of SLAs. The popular vendors in the market include Amazon Web Services, Microsoft Azure and Google Cloud Platform. As we also want to perform analytics on our data to understand the shopping patterns of our customers, we would also keep that in consideration.

Microsoft Azure provides Azure stream analytics which is a powerful analytics platform. It does not require additional servers for performing analytics, supports SQL and also comes with machine learning capabilities and features. AWS also provides a wide range of analytics capabilities and supports various programming languages, open standard API's and fast processing capabilities.

We can choose any one of the above-mentioned service providers depending on the pricing and customer services provided.

For our purposes we concluded that the azure cloud will be good for our ASP.Net application. With Windows Azure, the focus is on the development, not the infrastructure. Key benefits of hosting applications include:

Azure include:
· Minimal focus required on the infrastructure.
· No need to buy / maintain any infrastructure.
· Easy scale-up and scale-out available in Pay-As You-Go model.
· Developer(s) having .Net skill can develop and migrate applications on Azure by learning Azure SDK.
· Windows Azure provides SLA 99.95% for the hosted applications.

5. Evaluating the readiness:

Several things should be considered while moving an application to Windows Azure. Major points that need to be addressed are:

- Application compatibility – analyze if the application is architecturally fit for Windows Azure before moving.
- External / internal dependencies – check if there are any external application dependencies and need to analyze and if those are accessible through Azure.
- Application class – verify how the application is classified in the business. Business critical and LOB applications demand high availability.
- Application integration – check whether candidate application is integrated with other on-premise applications and shared services.
- Database compatibility – analyze whether the existing database is best fit to migrate to Azure.
- Application maintenance / management – identify how the logs are maintained and where they are stored.
- Scalability / elasticity – identify whether the application design supports scalability as Azure supports it.
- Compliance requirements – check if there are enterprise compliance and regulations that govern whether the data can be moved / stored outside the enterprise's control.
- Cost - verify whether the moving application is cost effective for the enterprise.
- Security – clarify whether the same level of security can be provided after migrating to Windows Azure in terms of:
1. Data security
2. Authentication
3. Authorizations

6. Planning the migration:

a. Authentication and authorization model
Analyze and understand the current authentication mechanism in the application.

1. Check if the same authentication approach in the cloud application can be adopted (for instance, using forms-based authentication).

2. Explore Cloud based solutions for authentication. Utilize Windows Azure Active Directory Access Control (also known as Access Control Service or ACS) to authenticate users from identity providers, when they try to gain access to a web application. These ,include Microsoft, Google, Yahoo and Facebook.

3. Deploy Azure virtual private network to communicate with enterprise active directory. Use Windows Azure Active Directory with integrated on-premise organization active directory.

b. Interaction with other modules / applications

Web services: They can be converted to Azure WCF services, hosted either as a web role or worker role. They can be left as on-premise services and can be exposed through Azure service bus or Azure VPN.

Windows Services: They can be hosted as worker roles.

Native code: A managed wrapper can be created and deployed as part of an Azure package. It can be consumed from any Azure hosted service.

Third party / non-Microsoft dependency: Need to confirm if they can be consumed directly from Azure application.

c. Diagnostics support

Windows Azure diagnostics provides non-intrusive capture of diagnostic data and its subsequent data to the Windows Azure storage service. With WA diagnostics, one can:

- Implement custom logging and save the log information to Windows Azure storage tables.
- Push event logs to the diagnostics store.
- Push failed request logs to diagnostic store.
- Push performance counter data to diagnostics store.

d. Message queues

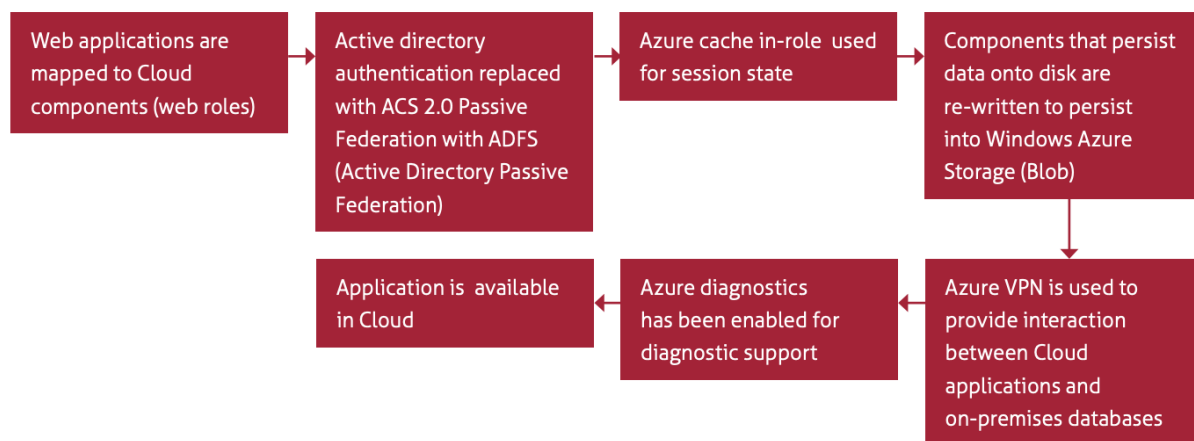Azure service bus topics / subscriptions can be used for message publish and subscribe model.

e. Configuration changes

If the application accesses any information from physical storage, it needs to be migrated to Azure storage / CDN / Windows Azure SQL database. Check for any hard-coded physical disk paths in the applications. Azure applications should not have any hardcoded physical disk or network access values. Ex: Application saves any information to local system / access information. Check for any third-party library or content references. They need to be included as part of the Azure package. Provide session and identify providers (ADFS / ACS information) in the web configuration file.

7. Executing the plan:

PaaS Migration

Web applications are mapped to Cloud components (web roles)	Active directory authentication replaced with ACS 2.0 Passive Federation with ADFS (Active Directory Passive Federation)	Azure cache in-role used for session state	Components that persist data onto disk are re-written to persist into Windows Azure Storage (Blob)
Application is available in Cloud	Azure diagnostics has been enabled for diagnostic support	Azure VPN is used to provide interaction between Cloud applications and on-premises databases	

1. Web Roles: Web applications are mapped to Cloud components

2. Active Directory Passive Federation: Active directory authentication replaced with ACS 2.0 Passive Federation with ADFS
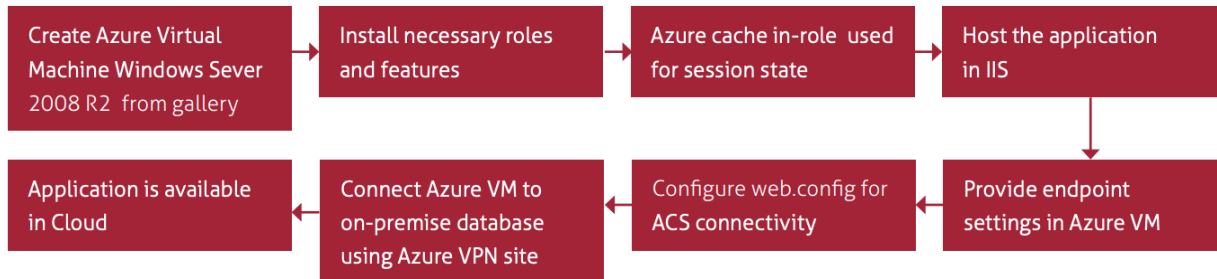
3. Session Management: Azure cache in-role used for session state

4. Blob Storage: Components that persist data onto disk are re-written to persist into Windows Azure Storage (Blob)

5. Azure VPN: Azure VPN is used to provide interaction between Cloud applications and on-premises databases

6. Azure Diagnostics: Azure diagnostics has been enabled for diagnostic support

IaaS Migration

Create Azure Virtual Machine Windows Sever 2008 R2 from gallery	→ Install necessary roles and features	→ Azure cache in-role used for session state	→ Host the application in IIS
Application is available in Cloud	← Connect Azure VM to on-premise database using Azure VPN site	← Configure web.config for ACS connectivity	← Provide endpoint settings in Azure VM

1. Azure VM: Create Azure Virtual Machine Windows Server 2008 R2 from gallery and then install necessary roles and features

2. Session Management: Azure cache in-role used for session state

3. IIS Hosting: Host the application in IIS

5. Endpoint Communication: Provide endpoint settings in Azure VM for communication with services

6. ACS connectivity: Configure web.config for ACS connectivity

7. Azure VPN: Connect Azure VM to on-premise database using Azure VPN site

8. Compliance requirements:

Regulations are in place to help companies improve their information security strategy by providing guidelines and best practices based on the company's industry and type of data they maintain. Non-compliance with these regulations can result in severe fines, or worse, a data breach. There are standards such as NIST and CIS controls, and compliances such as GDPR, CCPA, ISO and HIPPA which are applicable to various industries that we serve. But these compliances are not a blocker while migrating to the cloud. Azure provides the advantage of over 90 compliance certifications, including over 50 specifics to global regions and countries such as US, European Union, India and China etc. along with more than 35 compliance offerings specific to the needs of key industries, including health, government, finance, education, manufacturing, and media. Your emerging compliance needs are covered, too: Microsoft

engages globally with governments, regulators, standards bodies, and non-governmental organizations. Also, it provides the tools which simplifies and accelerates cloud compliance.

9. Experimentation in the Cloud:

Every organization has its own way of determining which projects get technology resources. Unfortunately, some organizations now treat the technology or IT department as a cost center and have pushed ideation too far away from those implementing it. Good ideas can come from anywhere, of course, and most technology professionals have a unique perspective that will surface when it comes to outside projects. This is especially true in our caseas we are just getting started with the cloud—the individuals using the cloud for their projects are in the best position to propose experiments that leverage capabilities that are unique to the cloud to benefit the business. So we must champion our team's proposals and position our staff to have an influence on which projects get invested in with the executive team.

10. Multi-Cloud approach:

We believe that migration to the cloud should be an incremental process. Hence, at the beginning we should not start with the multi-cloud approach. Rather than going with the multi-cloud approach at the beginning, a more sustainable long-term strategy to slowly move towards multi-cloud should be adopted. We believe that for a number of reasons. Following things are difficult when an organization is going for a multi-cloud strategy:

- Talent Management
- Cost Estimation, Optimization and Reporting
- Security Risks
- Operational Overhead

When we are successful in migrating to cloud with one vendor, then we should gradually start experimenting with other vendors as a part of our cloud strategy. Multi-cloud can be a boon for any organization as it provides a number of benefits such as:

- Innovation
- Managing Vendor Lock-in
- Negotiating Power
- Risk Mitigation
- Lower Latency

11. Limitations:

As we are migrating to cloud from the conventional model, we will be requiring that our technical staff is well equipped with the latest cloud computing skills. We will apply the following approaches to align our technical staff with our cloud migration plan:

· The first step is to perform a thorough analysis of your organization's current applications, infrastructure, skill sets, and resource and budget levels to get a better picture of the skills and capabilities you'll need to execute a successful migration to the cloud.

- Identify gaps in skills and resources, and create our staffing plan
- Meeting the gaps in skills investment in employee development
- Recruit new employees or partners for missing skills
- Create a culture of experimentation

References

SETH, S. (2019). 8 Best Cloud Storage Solutions for Small Business.

Retrieved from Investopedia: https://www.investopedia.com/articles/personal-finance/090715/8-best-cloud-storage-solutions-small-business.asp

When To Use A Multi-Cloud Strategy. (n.d.). Retrieved June 7, 2020, from https://cloudacademy.com/blog/when-to-use-a-multicloud-strategy/