Best Practices Guide for Cloud Migration

BEEVA

Avda. de Burgos 16D
[28036] Madrid
hablemos@beeva.com
www.beeva.com

BEEVA

Hoja de Control

Realizado por	Fecha
Angel Lorigados	2015/12/12
Aprobado por	**Fecha**

1.1. Control de Versiones

Versión	Motivo del Cambio	Responsable del Cambio	Fecha del Cambio
1.0			
2.0			
2.1			
2.2			
2.3			
2.4			
2.5			
3.0			

1.2. Anexos

Documento	Descripción

BEEVA

2. Objective

A poor migration strategy can be responsible for costly time delays, data loss and other problems on your way to success modernizing your infrastructure into the cloud.

To help avoid all this problems we offer this guide in order to be help and reference for future migrations from on-premise sites to the cloud.

The idea is not provide deep and boring documentation but highlight the roadmap to success in the migration.

BEEVA

3. Description

The primary technological goal of any cloud migration project is to transfer an existing compute resource/application from one on-premise environment to another in the cloud, as quickly, efficiently, and cost effectively as possible.

This is especially critical when considering a migration to a public cloud; considerations must include security controls, latency and subsequent performance, operations practices for backup/recovery and others.

For many companies, the initial pull to cloud based services is primary the lower cost – especially since the repeated infrastructure upgrades are no longer required.

However many companies find themselves staying on cloud operations for other strategic reasons like improving productivity, move more swiftly and focus on business transformation related activates not just technical activities. We have had not one client move from the cloud back to on premise solutions.

BEEVA

4. Best Practices

To help in the above premises, this is a selection of the best practices available from the Blueprint to the Cultural Change.

4.1 Blueprint

Before migration is always recommended to map out the requirements to the right blueprint of the current premise and operations because it can happen that the client doesn't fully understand what they have on premise today and the features they need to be migrated.

Make sure of what functions/ features of your applications are most used in your on premise solutions and make sure that you rank them from the most used to the least used before starting.

4.2 Time Planning

Another important part of migrating process is to calculate how long the migration will take, and which are the key parts to transition first because you never want the business to suffer any longer, or any losses, in a drawn out transition.

Start with the features that are not the most popular, then after you have mastered those, work your way up to the most frequently used. Also, make sure that you build an emergency exit into your project plan.

If things don't work out as expected in the cloud, you should have a way to dial back to your on premise solution, just in case, without affecting your business.

4.3 Availability & Resiliency

To be effective on a cloud infrastructure, the application architecture needs to be addressed for multiple points of failures.

Though a lift and shift approach it should be strongly be evaluated re-factoring or re-architecting options before deciding on an approach to be carried out, and even more will be required a strategy to follow several testing cases to provide quality to the final result.

4.4 DNS/URL/IP Management

Legacy applications within an enterprise are often accessed by business users via internal intranet URL. This URL common name and DNS management in a typical enterprise would have evolved over the last couple of decades into a complex setup, the management of which is often eased by having a centralized server cluster.

Running out of IP addresses is also not uncommon. When you migrate an application to the cloud (private or public), the DNS entry rewiring often ends up as a nontrivial exercise. Multicloud or hybrid-cloud scenarios make this even more complex, careful planning and network design is of utmost importance.

4.5 Security & Access Management

A server farm infrastructure typically provides for a centralized security access mechanism like webseal or forefront plug-ins tied into the corporate active directory or LDAP.

Many of the applications leverage this without any application specific security checks or balances in place. In this case the cloud can be a very secure place, but it will only be as secure as the application is, so it is very important to check security here in all cases.

4.6 Governance and Security

Managers often push back on cloud migration due to unfounded beliefs that the cloud is unsecured. IT should ascertain exactly what their security and governance needs are for a specific application and find a cloud provider according to the exact need for that app.

The cloud is always secure in origin because always exist a responsibility sharing agreement between the customer (the way security is implemented) and the service provider (secure infrastructure).

Major security problems are always related to the way the security tools, methods, politics and strategies are deployed in both networks and applications.

4.7 Monitoring & Alerts

The workflow of many operations & production support teams start with the monitoring alerts typically in place for these enterprise server clusters.

Alert centralized tools do the server monitoring with a customized solution to inform the right teams and stakeholders.. Again, the application is often unaware of the surrounding support structures that exist to keep it

up and running, so before migrating to the cloud it is capital to deploy mechanisms to monitor the services and not only the servers.

4.8 Server Sprawl

Sometimes data centers have poor hardware resource utilization, poor system and software level security and wasted energy. Migration and deployment models available are designed to avoid this server sprawl.

Though the public cloud players have some very good tooling in place, private clouds or hybrid clouds may be a different story. Often, organizational inertia and existing team structures will try to enforce legacy deployment models to the cloud, but is highly recommended to analyze and create new ones if required.

4.9 Licensing

Server sprawl could also be caused by licensing issues because multiple applications could share the same license, whereas it would be a substantially different cost model when going to individual servers – however small the server is.

If this forces a legacy deployment model onto the applications, it may be worthwhile to consider re-platforming to open source tools.

4.10 Certificate Management

Many enterprise applications are self-signed, usually using an in-house certificate authority solution. This is also integrated with internal DNS and URLs.

Cloud migration is an opportunity for the applications to ‘grow-up’ and be first world citizens.

4.11 Production Support

It is not uncommon for legacy applications to require direct database access or admin access for production support or business operations requirements.

It is recommended that when migrating such applications to the cloud, both application access and network access are important parameters to consider and evaluate properly in order to implement the right solution.

4.12 Disaster Recovery (DR)

Apart from being highly available (HA), many enterprise applications have centralized DR plans and processes in place.

Cloud migration provides an opportunity to tier the applications based on service levels and DR profiles, and develop application specific deployment models.

4.13 Partners

An important part of transitioning successfully is choosing the right vendor according to their reliability, security metrics and certifications. If the provider is too small they may not last, if they are too big, you may not be their priority. It is capital to ensure that vendor has full range of capabilities that your business requires.

Do you have vendors, partners, clients that are accessing your on premise solution today? Review in deep how they can access that resources in a cloud solution and get the cloud services provider to do a full analysis of the current premise based infrastructure, especially with the customized functionalities adapted to the existing premise system that need to be migrated to the new cloud solution.

4.14 End User Adoption

Once the business has migrated fully to cloud based operations, it's crucial to shift the focus to end user adoption. Cloud based technology offer greater features and flexibility than premise based.

Many companies fail to leverage these benefits and continue their new cloud operations in the same manner as their earlier premise solution.

4.15 Cultural Change

Recognize and prepare for the change: cultural changes and general operational changes to how things work. Be open-minded as change can be hard, but worth it on the other side.

The positive side to all of this change is that final customer should always be accompanied throughout the whole process. Remember that the cloud is always a relationship, not merely a product.

BEEVA

5. Common Mistakes

In order to complete this document we are going to provide some more information related to common mistakes when deploying migrations to the cloud.

Perhaps the best approach is to complete the migration process by deploying the previous best practices from the beginning to the end and try to avoid all the following common mistakes.

Good luck with all of your migrations!.

5.1 Expenses

The first major mistake that enterprise makes when moving their IT operations on-premise to the cloud is not understanding the total cost of the process.

There are several complex metrics that must be used when determining if a migration of an application or project to the cloud is actually saving the company money.

This is why it is highly recommended to invert time in measure the actual cost versus future cost on the cloud.

5.2 Security & Governance

Another common mistake is plunging into the cloud without considering the security and governance standards that must be met.

Always is up to the IT department to balance and follow up the proposal of accessibility and security in the IT infrastructure when migrated to the cloud.

5.3 Priorice

Prioritizing what applications (and in what order) are needed to be moved to the cloud is an important goal.

Not everything needs to be moved into the cloud. Managers should look for applications that can be moved to the cloud in a cost-effective way, without sacrificing usability and security.

By taking it on a case by case basis, special care can be taken for every specific applications in order to choose the best option.

5.4 Reusing

Legacy applications can have an architecture that is the exact opposite of cloud-native applications.

By simply doing a lift and shift to the cloud, these applications could become less available or more unstable, so is also highly recommended to evaluate and deploy a new version of the application for the cloud.

Luckily, in many cases the application refactoring that is required to fully leverage the cloud is only incremental compared to the lift and shift model. Often, a new deployment architecture will be sufficient to address the challenges. But simply lifting & shifting: i.e. replicating the legacy architecture in the cloud is a recipe for disaster.