Cloud Migration – Making a Flawless Path

Puneet Pardasani[1], Ameya Parkar[2]

[1]Vivekanand Education Society's Institute of Technology,
Hashu Advani Memorial Complex, Collector Colony, Chembur East, Mumbai, Maharashtra 400074

[2]Vivekanand Education Society's Institute of Technology,
Hashu Advani Memorial Complex, Collector Colony, Chembur East, Mumbai, Maharashtra 400074

Abstract: *When a business decides it's time to implement the cloud, there are many questions that need to be answered. Businesses need to have a full understanding of the reasons for a move to the cloud, all while managing the different steps to making it happen. With this research paper we try to create a flawless path toward Cloud Migration.*

Keywords: Cloud Computing, Cloud Migration, Migration Pitfalls, Migration Difficulties.

1. Introduction

It has been said that nothing is easy. Moving our solutions to cloud environments and just expecting to benefit from all the potential advantages won't work. It's dangerous to undertake cloud migrations because cloud environments differ significantly from other environments. Cloud Computing comes with a set of risks and challenges that we need to understand clearly to determine whether exactly to what extent we require cloud-based computing.

2. To Cloud or Not To Cloud

Which business applications should you migrate to the Cloud?

With cloud computing becoming a new trend in the computer business, the key decision – makers must understand the various benefits and pitfalls of moving their applications to a hosted environment. Most applications would certainly benefit in some way from cloud migration in terms of improved performance through put or security. On the other hand, some applications fail to gain expected benefits than others. Earlier the trend was to move all the existing application and solutions to the cloud. This attitude is changing after learning from applications which stand to gain lower benefits. Identifying which applications should be migrated to the cloud is the next logical step.

The Three Factors to consider during this decision

- Cost of Effort

Migrating a solution to a cloud enables your organization to a more productive path, the move will likely yield a high return on investment. This move would be right for your business. "Cost of effort is equal to the value of the time that would be saved eventually". This is rightly said when a cloud application or solution is saving your high amount of time.

- Economic Gain

The actual economic gain behind migration of a solution to a cloud is that it is cost-effective. If an operation will consume resources from effectively after its migration to the cloud, then it's a good move for the organization.

- Agility

In the cloud world, agility could simply mean efficient and quick operation. This final point is our benchmark to pick application migration. By moving a specific application to the cloud wouldn't result in increased speed or performance, it is not worth the move. Choose the ones that would provide "time savings and performance improvements".

3. Business Pitfalls to Look For

3.1 Starting with Zero Experience

Like every the organization is different from one another, hence every migration would be carried out differently. A proper understanding and knowledge of the current infrastructure is necessary before the migration is carried out. Such knowledge can only be gained by a dedicated staff. The staff fully understands the current needs and can rightly advise on the platforms and services the organization needs to adopt. The level of understanding needed when evaluating future cloud needs is directly related to a present understanding of infrastructure limitations. If a business does not fully comprehend a problem, they will not be able to recognize a solution. Seamless migration is next to impossible. Even with the best planned approach, there would cases over which the people won't have any control. The best step to make is to fully focus on what is known, and things which can be predicted. By choosing the right external and internal expertise, an organization can begin to offset for the coming migration hazards while being able to properly measure its need.

3.2 Choosing a Wrong Cloud Environment

When evaluating the different needs of the company, one should define a set of priorities. The failure to properly do so can cause a lot of complication at the later stage. The most common mistake a company makes is not buying the right cloud service for their business needs. Buying a cloud service itself is complicated, for which the key persons of the company should undergo a proper discussion followed by a

final decision. We usually see that the companies end up spending for service which they don't require, this affects in losing control and agility.

An organization should come up with many questions like – Would the hybrid cloud be better in case if the private cloud may not be able to facilitate sudden surges in application usage in spite of its security? How much control does the business want over the cloud? What levels of security are acquired?

3.3 Choosing the Wrong Cloud Provider

In terms of meeting a company's needs, adequate security and ability of handling the size and scope of the project the company should choose their right cloud provider. Especially for huge companies it is a persistent work. Down the line, cost, level of security and accessibility of data are not fully enough for confirmation of a cloud vendor. On big area of thought is Support, which is most important in terms of the working relation. A weak or bad relation will hinder, disrupt and finally cause harm to the business.

4. Technical Difficulty

4.1 IP Addressing

A new cloud environment will obviously have new public and private IP networks. This makes things little problematic. The problem occurs with those services and applications that are dependent to, or connected with old networks. Due to this some of the web servers may fail to reach the database or some other services which they would need as a support. The cloud provider's migration tool would not identify your old network connections and rebind them with fresh new interfaces.

4.2 Configuration Management

We can now manage application configuration on the servers with the help of tools like Chef, Puppet, and SaltStack. Usually, companies use moving services to a cloud as an opportunity to refresh some of their components. Components like newer OS, better network, etc. The existing configurations may need to be manually taken care of, if they are incompatible with the newer versions. You need a cloud partner who can identify these important components and point out their configurations to you. What migration tools fairly do is capture disk images and export them to a target cloud environment. This approach works quite well for basic applications, but fails multi-tier complex enterprise applications

4.3 Data Transport and Synchronization

With image migration, you will be doing a one-time export of your server image. This approach works fine for development or test environments, but typically unacceptable for production as the data is always changing constantly. If data or image synchronization options are not powerful, it might lead to application outrage. Your migration plan should incorporate several facets of data replication and synchronization.

4.4 Load Balancing

Complex load-balancing policies can be problematic when moving applications to the cloud. Do the current load balancers perform SSL offloading? If yes, how will the tool capture and move the SSL certificates, change its old IP address to the new IP address. They even need to preserve existing health checks and move them to the cloud. For all this you need to have expertise and understanding of the application flow, along with a good migration plan which involves a compatible load-balancing technique.

4.5 Firewall security policies

During migration of a service we need to capture, translate and move firewall security policies. Depending on what type of policy is currently carried out, it may turn out to be complex or even incompatible with the target cloud provider's network. A security engineer can translate the security policy, considering changing networks, both private and public.

4.6 Domain Name System

After the identification of the DNS changes, the tools alone will not allow you to 'redirect' to direct production traffic to the new destination. For this internal DNS has to be taken into consideration. You need to have a plan of action to move to a global DNS service, incorporate it into your migration plan, and finally a team capable of executing on that plan.

4.7 Security

In cloud environments, especially in public cloud environments, there needs to be a wider knowledge of security and risk among all team members than the earlier non cloud environments. This is because we will be putting data in an environment that would stand outside of our control range. It's within the control of a third-party cloud provider. We may have some level of control, but we don't have complete control. In traditional environments, there was one security specialist who would take care of the necessary security and respond to attacks and threats. This went fine because, in those traditional environments, the security concerns were more isolated. There may be exposure to outside attackers or vulnerabilities because it is not a fully controlled environment. There needs to be a great understanding of what security implications may come out of certain decisions and certain ways that we use data and applications in a cloud environment.

We' are delivering a solution on an environment that we have limited control. We may be using virtualized IT resources that share and that are hosted by physical IT resources accessed by multiple different cloud consumers. Those IT resources are residing on the same physical server. If this physical server is attacked or compromised, it can impact all those IT resources. The attacker can do anything once he has access to any of the IT resources. He can blow it down or he can even

access secured data or misuse it. The attacker may be one of the cloud consumers who have access to the virtualized IT resource. You may even say 'I want this physical sever just for me, while no other cloud consumer can access it.' However we need an amount of trust in how the cloud provider manages security controls and what measures they undertake to guarantee safety of our IT resource.

Choose the right cloud partner after the satisfactory assurance. After you have moved to a cloud environment, in the very next future you must not discover that our environment is vulnerable or has been under attack and that we have already lost data or either stolen. And that it happened due to inadequate security measures of the cloud provider and not due to you. Then we come up with the conclusion that we want to move away, which now brings us to a state where we started from.

4.8 Mobility

When we move our data and our solutions and other types of IT assets into a cloud, we are moving them into a really distinct environment, it is often to the cloud provider. For the cloud to work the way as we want it to, it should be able to take advantage of all the IT resources that vendor gives. We need to design the system, in a way that it is distinct to the cloud vendor's environment. We're migrating legacy systems into the cloud, we now have to invest in integration testing to make sure everything is working the way it has worked on-premises traditionally.

It's not just about the technology and the right function of our IT resource on the cloud environment. It's also about budget and impact and timeline and effort. We have to understand these things before we sign the cloud provisioning agreement with the cloud provider.

5. Conclusion

It is important to keep in mind that cloud migrations are not an all-or-nothing proposition. Organizations do not have to go "all in" with cloud migrations. In most cases, it will make sense to move certain services to the cloud while continuing to operate others on-premises.

Cloud migrations are a hands-on process, so enterprises need to have solid knowledge of the latest terms and technology. And because cloud computing is a rapidly evolving area of IT, its evolution brings new terminology for enterprises to learn. The above pitfalls and decision making parameters will prepare enterprises for their cloud journey and help to ensure a successful migration.

References

[1] Thomas Erl, "Cloud migration strategy: Consider portability, security, overall risk" searchcloudapplications.techtarget.com [Online] Available: http://searchcloudapplications.techtarget.com/feature/Cloud-migration-strategy-Consider-portability-security-overall-risk. (General Internet site)

[2] Brien Posey, "To cloud or not to cloud: What's your cloud migration strategy?" searchcloudapplications.techtarget.com [Online] Available: http://searchcloudcomputing.techtarget.com/feature/To-cloud-or-not-to-cloud-Whats-your-cloud-migration-strategy. (General Internet site)

[3] David Vogel, "Cloud Migration: Five Pitfalls and Considerations" datapipe.com [Online] Available: https://www.datapipe.com/blog/2013/12/04/cloud-migration-pitfalls-considerations/. (General Internet site)

[4] Not-Available, "Which Business Applications Should You Migrate to the Cloud?" glowtouch.com May 26, 2015 [Online] Available: http://www.glowtouch.com/which-business-applications-should-you-migrate-to-the-cloud/. (General Internet site)

[5] Not-Available, "Why Seamless Cloud Migration is Almost Impossible?" glowtouch.com June 2, 2015 [Online] Available: http://www.glowtouch.com/which-business-applications-should-you-migrate-to-the-cloud/. (General Internet site)

Author Profile

[1]**Puneet Pardasani** is currently pursuing his Master's degree in Computer Application from Vivekanand Education Society's Institute of Technology, Chembur, Mumbai. During the year 2008-2011 he studied his bachelor's degree in Information Technology from S.M.Shetty College of Science, Commerce & Management, Powai, Mumbai.

[2]**Ameya Parkar** is currently an Assistant Professor at Vivekanand Education Society's Institute of Technology, Chembur, Mumbai. In the year 2008 he completed his Master's degree in Computer Application from MET - Mumbai Education's Trust Institute of Computer Science, Bandra, Mumbai.