PATH TO CLOUD MIGRATION

Chethan Nagaraj
Dell EMC
chethan.nagaraj@dell.com

Abstract

Today's business are moving their applications to the cloud to increase uptime, agility, scalability, enhance end user satisfaction, disaster recovery etc. But, how do you migrate your existing applications which are already running in your data center? This article guides you in migrating applications in the existing environment to the cloud platform.

We explain the motivating factor for cloud migrations, possible benefits, risks involved in cloud migrations, cloud security, identifying an application, whether it is the right candidate for cloud migration, and guidelines for selecting the right cloud provider.

The aim is to provide a practical reference for enterprise business decision makers analyzing and considering application migration to cloud computing. It includes a list of steps along with guidance and strategies that consider both business and technical requirements.

Table of Contents

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell EMC's views, processes or methodologies.

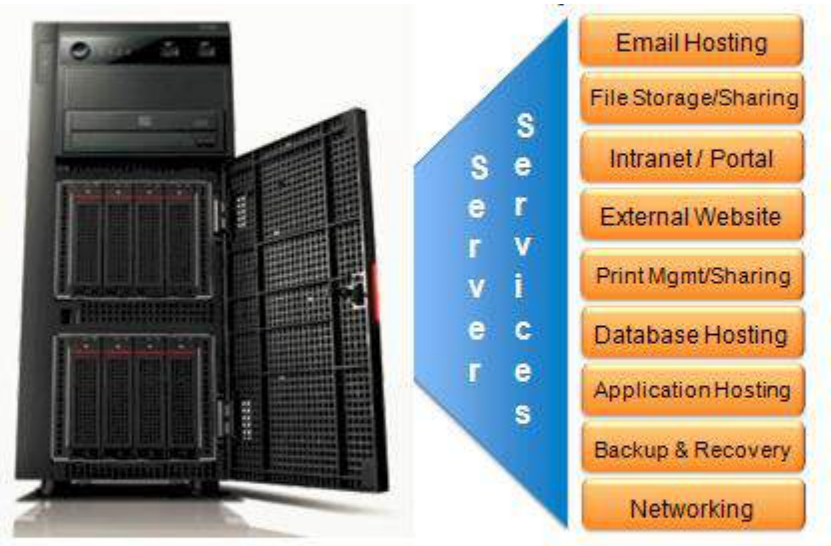
Introduction

Many enterprise applications and customer demands are serviced from cloud computing technologies. Today, cloud computing is one of the major technologies in the IT industry where you access resources as a service on demand through the internet. Cloud computing is not just for startups but also for established enterprises like Twitter having their applications built on cloud platform and service providers like Dell EMC and Amazon are attracted to cloud-based services which is considered superior to traditional data centers in terms of cost and technical dimensions.

Many enterprises intend to move their applications to cloud platform. Though Cloud may not be an alternative for all kind of hitches, it can definitely overcome difficulties related to scalability, performance, and operational and financial issues. But internal migration would require careful planning and attention. It is important that enterprises consider both positive and negative aspects of the migration. Issues related to cloud security due to multi-tenant environment, unexpected cost, applications re-work to suit cloud, and lack of planning are a few of these concerns.

Regardless of whether you are migrating your existing data center to cloud for the first time or you are migrating from one cloud to another, what really matters is understanding the process involved so we don't end up creating unnecessary problems. It is also important to realize that cloud is not a solution for all our problems and not all applications are suitable to run in cloud. Hence, we need to identify whether it suits our organization and the right candidate within to move.

Traditional Server Responsibilities



1. Need: Are there services lacking in the current infrastructure which cloud services can fulfill?

2. Costs: What would be the cost of cloud services when compared to current expenses?

3. Accessibility: Are there accessibility issues when employees are working from home or working in the field?

4. Control: What type of control is needed regarding security, accessibility, or configuration or customization for the current applications?

5. Support: What kind of support required? i.e. on-site, 24/7, etc.

6. Regulatory Compliance: Are there any regulatory compliance issues that should be taken into account related to access, control, security, data transmission, etc.?

Factors motivating for data migration

Some of the factors for cloud migrations include:

1. Cost savings by lowering CapEx and OpEx
2. Reduced maintenance
3. Efficient resource utilization
4. Unlimited scalability
5. Improved responsiveness
6. Higher availability
7. Broader reach
8. Business agility and flexibility
9. Easier access

Some cloud computing characteristics

1. **Measured service**: A key feature where you pay only for the amount of data used saving cost as you don't need to buy resources if not using. Lesser data usage equals less money, more data usage, pay more. Resource consumption can be controlled, managed, monitored, and reported exhibiting transparency between service providers and consumers.
2. **Rapid elasticity**: The ability to scale resources up and down based on business demands is more suitable for applications which are more dynamic in nature. For example: There may be a need for more resources at the end of the financial year for large transactions; rapid elasticity fulfills this demand my dynamically adjusting the back-end infrastructure corresponding to the requirements and lessening when not demanded.
3. **Scalability**: Applications that desire scattering workload over collective servers benefit by automated scalability feature that meets performance.
4. **Resource pooling**: Cloud enables pooling resources and presenting to more than one customer through multi-tenant layout utilizing same physical platform by allotting and withholding resources according to company's needs.
5. **On-demand service:** Resources such as compute, storage, and network are provisioned during run time without affecting the current operations.

Types of Cloud Migrations

1. **Replace:** This type of migration replaces one or more legacy application with service providers. Least used, it requires certain components to be re-configured to work with cloud stack. It is used to overcome shortcomings by using migration layer functionalities.
2. **Partially Migrate:** In this type of cloud migration, organizations would migrate a few applications implementing particular cloud functionalities.
3. **Migrate the entire application:** In this type of migration, entire applications are migrated to cloud platform encapsulated in a virtual machine. This migration may not require any changes to applications migrating; instead, it helps move applications 'as-is' into cloud.

Challenges in Cloud Migrations

1. **Sensitive Data:** Data migrations to cloud might contain business sensitive data, which require safeguarding at the highest level. Even though every cloud provider guarantees data security, there may be a possibility of data loss or leakage, placing sensitive data is put at risk. Data leakage would result in business damage in terms of cost or its reputation.
2. **Data Security:** The biggest threat in the IT industry is data protection. It's always recommended that the process of migration be carried out by experts regardless of cost because we are putting sensitive data at risk when migrating from physical environments to cloud. *(We will discuss this topic later)*
3. **Portability:** Data portability is very important. It is required to move the data from one platform to another without any modifications.
4. **Cost and time:** Cloud migrations require sufficient time and cost, counting the resources required for the task. Companies be compelled to bear the expenses. Specifically, cost would include sufficient bandwidth requirements and time for transferring data to cloud. This depends on the amount of data we migrate.
5. **Adoptability:** The challenges involved in implementing new policies or systems is the transition period. The team should understand new process and adapt.
6. **Interoperability:** The term refers to "systems capability to communicate with each other". The ability is in the code written that can adapt with multiple cloud providers.

Identifying the right candidate for cloud migrations

Enterprises may not migrate all of their data into cloud. Instead, they identify the applications meeting their needs in terms of performance, cost, etc. Also, not all applications are suitable for cloud. Identifying the right candidate is crucial. Applications may be good or bad depending on whether the meet the purpose and also their adaptive nature.

Good Candidates for Cloud

- ✓ Applications that are not frequently used but when used require significant resources to run. Claiming resources only when required helps reduce excessive cost involved in having their own infrastructure.

- ✓ Suppose you are starting a new branch office in some remote location, which needs additional IT staff for different time zone. Instead of investing in the infrastructure, an application running in the cloud serves the need.
- ✓ Newly developed applications can be tested in cloud platform before being implemented in your IT infrastructure. This helps in smoother transition without any flaws.
- ✓ Web hosting and internet-based customer services can be outsourced to cloud which provides the back-end server support for the applications.
- ✓ Companies who are willing to keep a copy of their production as a backup can look upon cloud as an alternative compared to traditional methodologies such as tape backups.
- ✓ Companies that requires a distributed server system and storage for application to run. Cloud helps create larger resource pool, with efficient system and storage utilization.

Bad Candidates for Cloud

- × Applications with sensitive data involve higher risk when exposed to cloud, especially in multi-tenant platform. These types of applications require higher security framework. Legal opinion would be an added benefit before committing applications to cloud.
- × Performance-sensitive applications which currently run in the company's private networks and users are not ready to compromise any sort of functioning. It is very difficult to maintain consistent network performance for cloud services.
- × Application running on legacy hardware. There are applications which can run on only specific hardware and migrating these applications might require re-work on coding to suit the new platform which would be very time consuming and expensive.
- × Applications requiring a larger database may not be best suited as there might be performance issues in accessing the data from cloud.
- × Vender lock-in situations that require applications to run on specific hardware.

Considerations for Cloud Migration

Migration is a process where applications are re-deployed on newer platforms and infrastructure. This process involves staging the backend infrastructure within the given cutoff data with the help of IT staff. If the application is compatible with the new platform, then application re-coding is not required.

In the case of cloud migrations, applications running in their physical infrastructure are moved to the target cloud platform. Target clouds can Private, Public, Hybrid or a combination of multiple clouds.

Steps for successful migration:

1. **Identifying the right candidate:** The first step is to identify the right candidates in terms of Technical and Business criteria. It reduces the cost. Agility is the key factor for application migrations.

IT services is another criteria where cloud services has an advantage over traditional methodologies. Previously, provisioning would take weeks or months; now, it is done in a few minutes with a few clicks.

Customers are offloading operations and management to cloud service providers, increasing the performance and scalability. Private cloud in enterprise private cloud can provide similar services.

2. Type of Cloud to choose

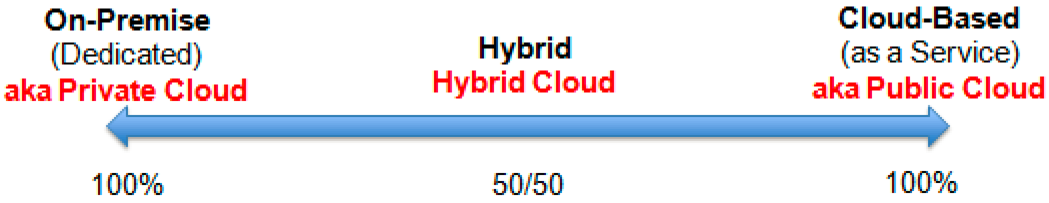
Software as a Service: SaaS eliminates the need of provisioning both application and infrastructure. As the name suggests only software are services, not the hardware.

Platform as a Service: PaaS helps in migrating application that are written using the standard software like Java, Microsoft, .Net for testing or developments purposes.

In PaaS, the service provider manages the platform where applications are running. The application platform might be shared over one or more customers managed by the cloud provider themselves. Some applications may not be supported in PaaS platform that require application changes.

Infrastructure as a Service: The initial step is to check the compatibility of the application with the cloud hardware and operating system (OS). For example: Application running on x86 platform requires similar hardware on the target side or else it requires re-work.

3. Choosing the right Cloud offering: This depends on the services we are looking for. Cloud types such as Private, Public, and Hybrid have their own benefits.



Public Clouds are suited for insensitive data providing highly scalable environment with pay-as-you-use model. While public clouds might not be suited for sensitive data like financial sector due to lack of control and multi-tenancy, data archiving would be a good reason to choose public clouds.

Cloud providers are completely responsible for any kind of maintenance.

Private Clouds are implemented within customer premises. Since it is implemented on-premises, management remains the company's responsibility. Performance and security is taken care of by the company itself. It is more expensive compared to public clouds but provides better security. Data are more customizable and chances of data conflict are minimized compared to multi-tenancy environment in public clouds.

Hybrid Cloud is the combination of Private and Public cloud. The combination can be used as a cloud tiering where the mission critical, sensitive data can be moved to private cloud while data achieving, backup, etc. can be moved to public cloud.

4. Application Evaluation Criteria: 'Scale-up' architecture can benefit from more resources by adding more CPU or memory to a single node or server. In contrast, 'Scale-out' architecture helps spread applications across multiple nodes scaling horizontally.

'Scale-out' architecture can take advantage of the pay-by-usage concept where resources can be increased or decreased by adding/removing nodes based on resource demand.

'Scale-up' architecture can also be an advantage in today's advanced technologies where CPU and memory can be added dynamically.

5. Data Transfer: Since clouds are internet-based most of the data transfers are done through internet. Internet connections in small and medium range business would be very slow and take more time to transfer even just a few GB's of data.

The other option is to ship the hard drives to cloud providers in order to overcome the bottlenecks of online transition. Cloud venders can deploy the customer's application on physical hardware which is closest to the customer's location. This can make a big difference in response time.

6. Data Storage and Location: If the data is very large, storage cost for these data would be very expensive. Shared resource or centralized databases are more effective compared to individual virtual machine files.

Licensed software used in cloud would contradict the terms of a license or may invoke special clauses that may not apply elsewhere. It's important to check the license or consult a legal opinion before signing any agreement.

7. Service Level Agreements: Service Level Agreements (SLA) defines the amount of performance or availability the service provider guarantees to the customers and outlines the consequence if they fail to deliver.

8. Upgrade and Maintenance: Service providers are responsible for updating their systems from time to time to protect against security breaches and by also providing new features to consumers running their applications on it with the latest patches. This should not interrupt the application running. Vendors should schedule the maintenance period with a completion deadline.

9. Software architecture: The architecture in cloud where data will be moved will be different form the architecture of the physical platform where applications are running currently. Questions need to be asked about the type of platform required – i.e. a cluster environment or Hadoop installed instances for big data analytics for better service. Does it require a distributed database or a single large database instances to handle all the traffic?

Cloud Security

1. Easier Access:

Cloud services are easily accessible by consumers within few clicks which is one of the main attractions of cloud service. However, it also invites hackers who can introduce acts like unsolicited emails and malware to crack passwords, etc. and expose sensitive data.

2. Shared Resources:

Cloud service providers use multi-tenant environment to support more customers through sharing resources from a single platform. This is achieved by allocating resources to multiple users and preventing them from accessing other user's data with proper policies. However, if the attacker is able to hack the underlying infrastructure, all the user's data will be easily exposed. Techniques for hacking may be various methods like exploiting a vulnerability of the hypervisor, breaking out the virtual machine (VM) sandbox, etc.

3. Inside Attacks:

Since service providers have full access to all customer data, it is important to implement security measures preventing them from viewing/accessing the customer's private data.

4. Loss of Data:

Backing up the data stored on cloud would be important in case there is accidental deletion of data, hard drive failure, or data modified by the attacker. Backing up the data would enable quick recovery of data when situations arise.

5. Data Breach:

Since a single physical hardware is used to share resources across multiple users, there is a possibility of one virtual machine accessing the resources reserved for another virtual machine. It is popularly known as side-channel attacks, in which processor and memory are stolen from other users.

6. Account Security:

It is best to use a two-factor authentication wherever possible. It prevents hacking accounts by sending SMS messages to the user's phone alerting about the unauthorized access.

7. Denial of Service (DoS):

Cloud services can be disrupted by the attacker by issuing the Denial of Service attack. It can be done in various ways through shared resources like CPU, RAM, network bandwidth, disk space, etc.

8. Lack of understanding:

Enterprises should invest in educating its users before moving into cloud, because there's nothing worse than a company not knowing what it is getting itself into. Service providers and Enterprises should agree on their roles and responsibilities. For example: If services providers are not backing up the data, enterprises should.

9. Data Protection and Data Portability:

If there is a need to switch between cloud service providers, we need to address the issues related to data protection and movement. Data stored in the previous cloud provider has to be deleted once it has been moved to new service provider, without leaving any trace of data.

What if a service provider does not return the data? It's always better to use an established, recognized service provider who has been in business a while.

10. Vendor Lock-in

Before signing the agreement it is important to sign the contract with a clause that allow customers to move their data to any other service provider whenever needed. This might be required when customers are not satisfied with the current services or might require other providers for any other reason. Contracts containing such clauses prevent service providers from restricting the customer to choose only their services.

Best Practice

Just Data Migration:

This would be the right choice for Tier 1 and 2 applications. There cannot be any downtime for Tier 1 applications, for example when invoking replication. Replication itself is a complex and detailed subject. The key is to identify the size of the data, the rate of change, and the bandwidth required between source and target. As a general rule, if rate of change is greater or equal to the chosen bandwidth, the migration would fail. That's because rate of change refers to the data coming in and bandwidth refers to the channel where data are carried to reach the target. The channel should obviously be greater than the rate of change for successful migration.

Machine replication:

This involves stack migration, best suited for Tier 1 and Tier 2 applications which can sustain certain downtime. There might be huge data for migration but requires very less configuration. Stack migration would be best when moving to internal private cloud. Since you have plenty of bandwidth to move around, you will be able to move the entire stack.

Physical to Virtual (P2V) Migration:

Typically used for Tier 2 and Tier 3 applications which are not virtualized. The concept involves taking the physical app and virtualizing it. Tools like P2V convertor from VMware ease the process of converting physical machines to virtual machines. In this option there is no need for replication. Instead, after being virtualized, applications are shipped to the cloud provider to run.

Disaster Recovery:

Many companies treat it as Disaster Recovery (DR) scenario. Setting up something similar to their physical environment, they choose to replicate the entire stack from point A to point B then choose to failover.

Knowing the Data Gravity

Data gravity should be taken into consideration when moving Tier 1 applications from a physical data center to private or public cloud. You need to evaluate the weight of the data in the app considering for migration, as there is no easy way to shrink down the data. In a high transaction company or high transaction application there would be huge data to replicate.

Another important aspect of pre-migration plan is to determine how connected the application is which is migrating or what impact it has on other applications running. If there are more applications tightly coupled to the application you are migrating then cloud might not be an option for that application or at least only for that application.

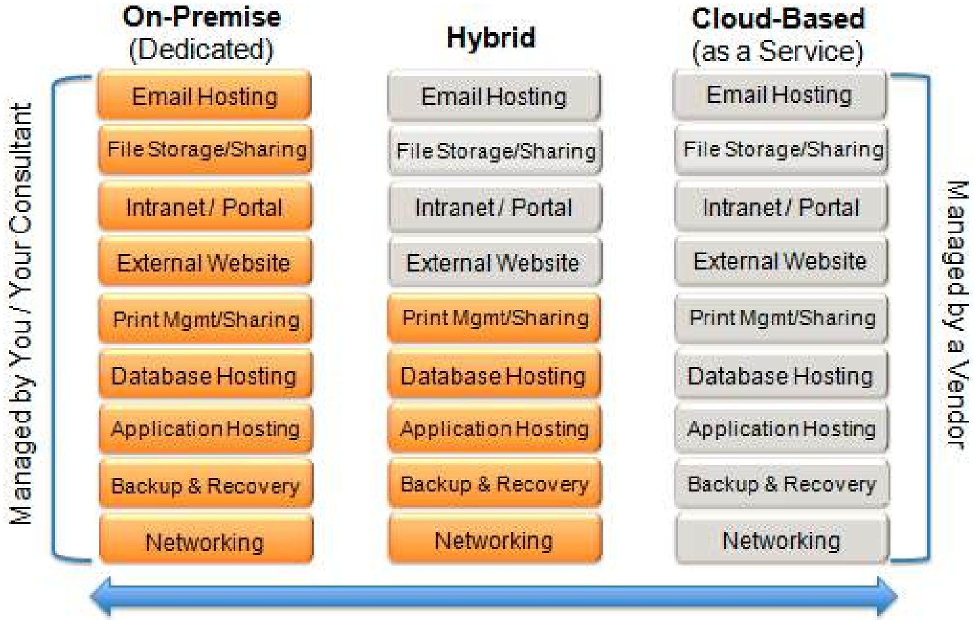
Identify your application connections

If applications which are planned to be moved contain data that are accessed by other application, all applications must be moved as well. If two or three applications are tightly coupled then you need to move all three to cloud. Otherwise, a cloud-hosted application accessing a physical server could experience latency.

Similarly we should also identify the applications which are sensitive to latency problems. This should be a consideration when deciding whether to move it or not. It's very important to understand the nature of the application.

The strategy for each application won't be the same for everyone.

Cloud Migration Strategy



On-Premise (Dedicated)	Hybrid	Cloud-Based (as a Service)
Email Hosting	Email Hosting	Email Hosting
File Storage/Sharing	File Storage/Sharing	File Storage/Sharing
Intranet/ Portal	Intranet/ Portal	Intranet/ Portal
External Website	External Website	External Website
Print Mgmt/Sharing	Print Mgmt/Sharing	Print Mgmt/Sharing
Database Hosting	Database Hosting	Database Hosting
Application Hosting	Application Hosting	Application Hosting
Backup & Recovery	Backup & Recovery	Backup & Recovery
Networking	Networking	Networking

The above model helps in understanding the cloud strategy. It answers all the questions and helps in proper justifications behind every decision regarding each need. This information will be handy, supporting all your demands once you begin communicating with the vendors.

Important checklists that help in transition

1. **Considering application or data:** As discussed above, not all data are suitable for migration. Mission-critical data, legacy applications and sensitive data such as customer account details in a financial sector may not be suited for cloud. To take advantage of cloud computing without compromising performance customers can opt for private, public, or hybrid cloud services for their data center migration.

   Public cloud works on the concept of multi-tenancy that means more than one customer are served from a single underlying platform through sharing resources. With auto-scaling, resources scale up and down based on the requirement. It is also important to analyze the resources required for each application. Increasing utilization demands higher bandwidth and may hinder application performance.

2. **Evaluate Cost:** Cost saving is one of the main advantages of moving to cloud compared to building, operational and maintenance expenses of traditional IT. But without proper analysis of the resources required to run applications, cost would increase as the usage increases. Mobile applications which randomly increase and decrease resource consumption yields would better benefit compared to larger Oracle databases which are expensive to run in cloud. There are metering services that help monitor expenses.

3. **Security:** It's important to take precautions against security breaches, disaster recovery, failover, failback, etc. If you are prepared to bear additional expenses there are many tools and services for extra security.

4. **Governance:** Governance needs a tweak to accommodate cloud migration policies. This is because pre-migration governance does not work post-migration. There would be little responsibility for the local IT team and more on service providers. Hence there is more dependency on cloud providers. It is also important to choose the right service provider with a proper contract and validate that the provider certificates are up-to-date.

5. **Cloud-to-Cloud Migrations:** Cloud migrations need not be only from physical environments to cloud; they can also be from one cloud service provider to another service provider. It can also be from private to public cloud services. Many third-party tools help in migrations.

   Before migrating to another cloud provider there is need to test applications, OS, network and more including additional manual labor expenses.

6. **Auditability:** Auditing helps in monitoring the data compliance as per the contract. Auditing can be conducted by a third party or by the customer itself. Companies that require greater audits would usually opt for private clouds.

7. **Service Levels:** Service levels should be clearly defined in the service contract. If any discrepancy, the customer has every right to question the provider.

8. **Cloud and Law:** Companies are bound by the law related to data privacy which prevents data from crossing its boundaries. Hence few countries will be able to use cloud services if they comply with the law.

9. **Subcontractors:** Public cloud providers many times outsource the project to subcontractors. In that case the contract terms and conditions apply to them as well. A Cloud provider should also disclose the details of its subcontractors.

Conclusion

In this article we have discussed all possible technical and business aspects of cloud migration. A fair idea has been provided about the challenges, risks, advantages, and disadvantages of cloud migrations. Any complex task can be made smoother with proper planning and taking pre-cautions about the risk involved. We have only described an overview about the contents. There are more detailed explanations if you explore on each mentioned topic.

Every business environment differs which makes each decision unique and cannot be compared to others. There is no one generic solution for all questions. Strategy for each business will be different as per its needs.

References

https://www.nten.org/article/cloud-server-yes-it-can-make-sense-to-have-both/

Dell EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” DELL EMC MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.