ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Cloud Application Deployment Mistakes and Solutions

S. Vimal Don Bosco[1], Dr. R.Latha[2], Dr. N. Prabakaran[3]

Research Scholar, Department of Computer Applications, St. Peter's University, Avadi, Chennai, India[1]

Prof.&Head of Department, Department of Computer Science and Applications, St. Peter's University, Avadi, Chennai, India[2]

Senior Vice Principal, St. Joseph College of information Technology, Songea, Tanzania[3]

ABSTRACT: In cloud deployment, simple mistakes are tormenting to the deployment. The user has to pay much importance to the deployment. It will move the performance and efficiency of the diligence. Many problems could not identify till now. If we do not see them, it will horrible to the cloud application. To find mistakes of cloud deployment, there are various methods available. But comparable to real time issue is more reasonable and effectible. The actual cloud deployment users are doing general mistakes. The given funding will help to cloud deployment user and minimize or reduce the problem while deploying applications on the cloud. Though this finding will help to increase efficiency and performance of cloud application. These findings relate to deployment tools, cloud model, security & network and compatibility, which are closely involved in deployment of cloud. The deployment tools are available and open to all in the network. Deployment tool may be daemon process or scheduler or like applications. It may have several representations. But deployment tools are doing a job in a particular manner towards to deployment of cloud with facing many issues. The cloud model will affects more deployments. If a private cloud may be less risky, but public or the hybrid cloud model will be a dangerous one. Open network may run to access on a mesh. While deploying source public or the hybrid cloud model needs to follow many steps carefully. While migrating the server to the cloud, users are really facing difficulties to migrate. In open network having less security and connectivity of the server may convene. In the compatibility view, cloud servers are not very compromising.

KEYWORDS: Deployment Tools, Cloud models, Migrate Servers to the cloud, Application Performance, Security and Networks and compatibility.

I. INTRODUCTION

The cloud application deployment is most considerable one in cloud activities. In that there are generally mistakes will have more impact to any problem. This investigation will help to the cloud deployment user get some clearance about to the deployment. The learning of the cloud deployment important to find a precise way to resolve many problems. The determinations are considered to be small or not a problematic, etc. But they are working to minimize the cloud application performance and efficiency. Findings will categorically help of the cloud deployment users. Some of the users may not have awareness about this discovery and significance. Cloud is not diminished. Cloud is a worldwide network of service provider. There are different tools, cloud models available in the market. But users are still facing many issues while deploying source on cloud servers. The deployment tool fixes for separate issues. The developer does not possess an adequate awareness of the cloud servers. At that place are various problem occurred while doing deployment.

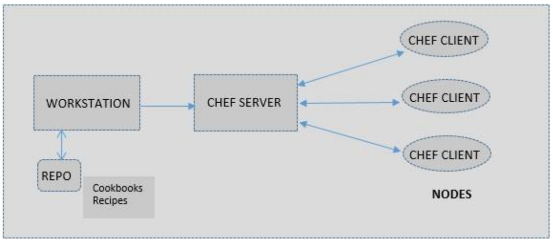
The cloud models are differentiated for user preferences and convenience. Only they are problematic to execute the maintenance and providing service to the users. The specific model of public cloud is always under risks to providing service in open networks. The server migration from out-of-date to cloud model will be more comfortable and flexible. In particular, point of migration may lead to worldwide access for application and services under risks. Performance of application of cloud will not be much efficient compared to traditional. They are many suspect on improving efficiency on a cloud. The efficiency always depends on network connectivity and security. If the network has less connectivity will not allow to increase efficiency. The connectivity is stable, then providing security will not satisfy. The compatibility view of the cloud application across the platform is not sensible.

II. DEPLOYMENT TOOLS

This chapter is going to discuss about organizations fail to do the upfront planning required to determine which apps are good candidate cloud application deployment.

Choosing tools which are used for the deployment in the cloud, it is playing an important role in the deployment. This will may distresses of the running applications. Their various platforms like UNIX, LINUX and WINDOWS etc. They are taking each specification provides the cloud base platform to access applications. If a tool is platform dependent, that will affect the deployment efficiency. Hence, choosing the tools for cloud application deployment major role. The platform independent application deployment tool is advisable to choose. They will not bear on running application performance. They are flexible to do application deployment across platforms.

In the network, there are a number of software available. They are providing a cloud environment to do the application operations. If we are choosing Chef Tool, for the cloud configuration management and deployment across the enterprises. The deployment model of chef tool.



Recipes	- It is used to configure software and deploy applications.
Cookbook	- They mean it is Database – MySQL
REPO	- It helps provisioning resources, manage recipes/cookbook, nodes and more.
Work Station	- It is computer configuration to sync with REPO.
Nodes	- Physical, virtual or cloud machine that is configured to be maintained by a chef.

This software presentation expressed, it is not a cross platform software. Users are using open source tools like MySQL. MySQL does not build efficiently and it may not support large project. Thus while choosing deployment software, we must consider like above points.

III. THE CLOUD MODEL

This chapter is going to discuss about organizations fail to pluck the correct cloud model private or public, for application deployment.

Applications can be deployed in private cloud or public clouds. Private clouds are on-premise clouds under the control of the IT organization that created them. They have more similarities with the traditional data center than public clouds. Public clouds are off-premises. The infrastructure of a public cloud is determined by the cloud provider and may present a much different look, feel than the traditional data center, or even a private, on-premises cloud. The mistake organizations make is failing to determine which applications are good fits for public clouds and which are the best suited to private clouds. Another common mistake is failing to determine the costs, long term and short term in deploying applications in each cloud model.

Before choosing a cloud model, Users have to follow basic steps.

- Understanding the different models of cloud
- Understand pros and cons of the models
- Choosing cloud service like SaaS, PaaS and IaaS.
- Cost, performance, security and flexibility
- Duration, we are going to use period.
- Choosing cloud model services that work for your business.

Public cloud services are available for anyone to subscribe to and use. The key benefit of a public cloud approach is one of scale – the cloud provider can potentially offer a better service at a lower cost because the scale of their operation means that they can afford the skilled people and state-of-the-art technology.

The public cloud model inherently provides service on demand. The cloud provider can dynamically reallocate resources as they are required. Spreading the service delivery across multiple locations also improves resilience. Local problems with power supplies, telecommunications, natural disasters, and so forth, can be managed more effectively when there are several data centers in multiple geographies.

Decreasing of the public cloud is the risks of compliance and data security. For example, data privacy laws in the EU mandate that personal data must be processed within defined guidelines. The cloud service, customer, which is the “data controller”, is responsible in law, and needs to ensure that these guidelines are adhered to. A large cloud providers have recognized this need and can offer compliant services. Sharing applications and infrastructure with unknown co-tenants can lead to concerns over data security and data leakage. There are standards and best practices for this, and it is essential to check that the cloud provider is externally certified as adhering to these.

The HMRC online tax filing service is a software-as-a-service with a public deployment model and this has been praised by the Audit Office, although it’s unclear whether it provides value for money.

A private cloud service is used exclusively by a single organization. The private cloud allows organizations to outsource the management of their IT infrastructure while retaining tighter control over the location and management of the resources. The price to pay for this is that the costs are likely to be higher because there is less potential for economy of scale, and resilience may be lower because of the limit on service resources available.

Isolation is one of the key techniques for ensuring security and, while in the public cloud applications and data exist in a shared environment, the private cloud offers greater isolation by dedicating resources to a particular customer.

A community cloud service is for the exclusive use of a specific community of organizations that have shared concerns (e.g. Mission, security requirements, policy, and compliance considerations). A community cloud provides many of the benefits of scale of the public cloud, while retaining greater control over compliance and data privacy.

Community cloud services already exist, but under a different name – for example NHSmail, the national email and directory service available to NHS staff in England and Scotland, an effective software-as-a-service with a community deployment model. As regards security, NHSmail is accredited to the government "restricted" status, and is the only NHS e-mail service that is secure enough for the transmission of confidential patient information.

IV. MIGRATE SERVERS TO THE CLOUD

This chapter is going to discuss about organizations tend to focus on “migrating” servers to the cloud versus deploying applications in the cloud.

When organizations decide to move from the traditional data center to a private cloud, the motivation is frequently server consolidation, which leads to improved server utilization and reduction in capital and operating expenses. The focus is not where it should be. The focus should be on deploying applications in the cloud. By focusing

DOI: 10.15680/IJIRCCE.2016. 0401073

on application deployment, enterprises will gain insight into the makeup of an application and management tools needed by the application in the cloud environment. This mistake fosters a number of other common mistakes.

Prioritized migration of process, applications and infrastructure a series of concerns must be addressed. Users Key amongst these are:

1. Agility
2. IT enables business transformation
3. Cost

There are other concerns to look into:

Security, reliability, resilience, availability, scalability.

Three steps to cloud selection:

1. What to migrate to the cloud?
   Applications, Processes (software) and Infrastructure.
2. When to migrate to the cloud?
   Non-core (ex-front office) and core (ex-new Product planning).
3. Which the cloud to migrate to?
   Private, public, community and hybrid.

V. APPLICATION PERFORMANCE

This chapter is going to discuss about failing to plan for changes in application performance in the cloud.

Deploying an application in a cloud may result in a performance level that is lower than the traditional data center because of the difference between the two. Organization administrators usually focus on CPU power, memory, disk storage, etc. when they think application performance. In the traditional data center, the application probably the only running on a server. The application is tuned on that server to reach to an acceptable performance level using physical server monitoring tools.

When an application is deployed in a cloud, it shares physical CPUs, physical memory, etc. on a single virtual host server with other applications in a virtual environment created by hypervisor software such as VMware ESXi or Xen. These applications are simultaneously contending for the physical resources of the virtual host server. Performance tuning of the application in the cloud begins in the new ecosystem.

Before an application is deployed in a cloud, users should create a baseline performance for the application that is satisfactory for fulfilling business needs. When the application is deployed in the cloud, users should examine its performance and compare it against the baseline performance, making adjustments until an acceptable performance level in the cloud is reached. To do this type of performance analysis, user will need performance monitoring tools that are working in virtual environments.

[7]With clouds, we're able to automate the process of dynamic resource allocation based on changing application demands. At the same time, a cloud, whether public or private, cannot make our applications run any faster. In fact, no transaction will execute more quickly in a cloud. Therefore, the wonderful flexibility users gain from cloud computing must be carefully balanced against the inherent need to be ever more aware of transactional efficiency.

The process of performance tuning remains much the same, with the addition of the metrics just discussed. But there is yet another layer of complexity added by the use of third-party services over which one has no control.

VMs to an application, which is simpler and more flexible than changing resource allocations, user do not want to over-provision. For example, adding a huge VM instance when we need 5% more power is overkill. Instead, increasing available hardware in small increments helps to maintain the advantages of flexibility.

The use of smaller, less power full VM instances has two logical consequences:

1. The number of instances per tier tends to increase, resulting in a very large number of tiers overall.
2. Elastic scaling can become necessary for each tier.

Cloud-deployed applications must be inherently scalable, which means:

- Avoiding all synchronization and state transfers between transactions. This limit sharing and requires a tradeoff in terms of memory and caching. For distributed data, we must use inherently-scalable technologies, which might disallow a particular SQL solution that we are used to.
- Optimizing the critical path so that each tier remains as independent as possible. Essentially, everything that is the response time-critical should avoid extra tiers. The best-case scenario is a single tier in such cases.
- Using queues between tiers to aid scaling. Queues make it possible to measure the load on a tier, the queue depth, which makes scaling the consuming tier very easy.

VI. SECURITY & NETWORK

This chapter is going to discuss about failure to understand that new tools are needed to monitor application performance, security and network traffic.

Some organizations fail to understand that tool worked in the traditional physical environment are not sufficient for the virtual environment of a cloud.
Monitoring tools help answer questions such as:

1. What is the performance for an application?
   Is application gaining access to computing and storage and bandwidth when we need?
2. What is the response time for storage devices that an application access?
3. Is my application being protected from intruders?

Virtualization has added a layer of abstraction to traditional monitoring. The user can no longer monitor performance just by looking at physical devices. Network operation teams have struggled to look through this abstraction to determine what actually happening in both virtual and physical levels is.

Because lots of traffic occurs within a hypervisor without making it to the physical network, you need tools designed to work in virtual environments. Physically-based monitoring tools do not see the traffic following among the virtual element, such as virtual servers, virtual routers, virtual switches, etc. Monitoring application performance and performance of the resources that surround and interact with an application in a cloud environment requires new tools designed for virtual environments. The same can be said for application security. Tools such as Catbird Network's Security are available for addressing security concerns by monitoring the traffic on virtual networks.

[8]Prioritize cloud security compliance will help to sort out the problem. New method of working demand new approaches security.

1. **Define problems early:** Cloud security is similar to solving a complex problem, and the best way to begin that is by clearing defining your objectives. Make a list of your security and compliance priorities and challenges, and start from there.
2. **Access control is essential:** One thing that is often forgotten when talking about cloud security concerns is that the location of your stored data is nowhere near as important as who has access to it. Establishing authorization and access controls — including implementing the principle of least privilege — is the best way to manage risk and limit the possibility of a breach.

3. **Priority vulnerability Testing:** Vulnerability testing is an important ally in cloud security management. The most rigorous testing your system undergoes, the better equipped user will be to design and implement proactive security controls.

The most considerable branches are below:

- **Data breaks**, which typically result from a flaw in an application's design or other vulnerability.
- **Data damage** as a result of a malicious attack, an accidental deletion or a physical problem in the data center.
- **Account hijacks**, including the use of phishing, fraud, or social engineering to obtain a user's private login information.
- **Insecure interfaces**, as cloud services depend on APIs to provide authentication, access control, encryption and other key functions. Vulnerabilities in these interfaces can increase the risk of a security breach.
- **Denial of service attacks**, in which a malicious actor prevents users from accessing a targeted application or database.
- **Cruel insiders**, such as employees or contractors, who use their position to gain access to private information stored in the cloud.
- **Mishandling of services**, which involves hackers who use the limitless resources of the cloud to crack an encryption key, stage a DDoS attack or perform other activities that would not be possible with limited hardware.
- **Insufficient due carefulness**, which is one of the most neglected threats against a cloud network. Failing to properly anticipate the risks of working in the cloud, or rushing the migration process, can expose organizations to considerable amounts of risk.
- **Shared vulnerabilities**, including platforms or applications accessed by different users in a multi-tenant environment. In these rare scenarios, even a single vulnerability can have monumental consequences.

VII. COMPATIBILITY

This chapter is going to discuss about failure to understand how an application fits into the big picture of cloud computing.

When an application is deployed in a cloud, just about everything associated with that application has been different. The performance is different, the monitoring tools are different, system management tools used to manage virtual servers are different, security is different, and act of deploying an application is different. These differences places a strain on the organization whose job is to manage the cloud, requiring changes to traditional processes for deploying managed application in a cloud environment.

Cloud vendor selection usually implies an infrastructure and ecosystem that can have a large effect on the deployment of applications in a cloud. Proper selection of vendor(s) and virtualization software, such as hypervisors, involves understanding how an application fits into the big picture of cloud computing, and determines, to a great extent, whether or not you can move application between private and public clouds to take advantage of the hybrid cloud model.

VIII. CONCLUSION

The several reasons may suggest to choose a cloud model. But the above factor could help to the buyer considerable points to get good cloud model and vendor. Most of the factors are effectible the application performance. They are really increasing the application deployment efficiency. The compatibility of the user is most important in every work of the cloud model. Platform independent will be an outstanding feature on a cloud. Some of the reasons may lead to problem in cloud network bandwidth, network connections and accessibility. While others have gone before the cloud model, make sure of the findings above. The findings are mentioning as mistakes in general deployment of the cloud, if users avoid those scenarios, it will be the better cloud model. The user has to give much importance for choosing deployment tools. Users should support to use deployment tools for deploying project in big applications like supply chain solutions. The user has to choose carefully cloud model by using the above findings.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Migration of the application from local server to cloud may cost reasonable, but about security side must be at risk. Application performance on cloud depends on bandwidth which we have in local to access applications. Above findings may increase application performance on a cloud. Insecurity and network side may occur problems. Prioritize precaution of the problem or ready for arrangement to face above findings. Cloud compatibility of application is more important, than only user can access application conveniently and efficiently. User before going for cloud above considerable findings will help to avoid issues or problems.

REFERENCES

1. Common mistakes in cloud application deployment July 2012 by Bill Claybrook, new Reiver Marketing Research
2. Navigating multi-cloud deployments remains a challenge by David Lucky on September 17, 2015, Cloud Computing, Hybrid IT
3. Overcoming complex multi-cloud management challenges by Paul Korzeniowski, April 2015
4. The Challenges of Cloud Security Deployments by Jude Chao on Oct 18, 2013, http://www.enterprisenetworkingplanet.com/
5. Deployment Tools, by Sanket Dangi on December 8, 2014 in cloud academy.
6. Cloud Choices by Mike Small on May 2012 in computer weekly.
7. Understanding application performance in the cloud by dynatrace on 2015. http://www.dynatrace.com/
8. How to Overcome Security issues in Cloud Computing by Don Carfagno on June 18, 2015 in blackstratus.

BIOGRAPHY

S.Vimal Don Bosco
Research Scholar, Department of Computer Applications, St. Peter's University, Avadi,
Chennai – 600 054