International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 02(II), April - June, 2021, pp 237-240

APPROACH FOR CLOUD MIGRATION JOURNEY FOR ORGANISATIONS: OVERCOMING CHALLENGES & LEVERAGING OPPORTUNITIES

Vivek Rastogi*
Dr. Harish Purohit**

ABSTRACT

Every day, traditional organisations are competing with digital counter parts that develop their business exclusively in the cloud. To fight this battle, companies are digitizing every area of their operations, looking for agility and insights from operations, data and analytics. This transformational effort includes migrating workloads to public cloud i.e. Amazon Web Services, Microsoft Azure and Google Cloud Platform, private cloud or hybrid clouds. There may applications which may not have been historically deployed as cloud-ready applications. This article is to discuss the, opportunities benefits and challenges of cloud computing.

Keywords: *Traditional, Companies, Workloads, Amazon, Applications.*

Introduction

The benefits of cloud computing have been spelled out extensively over a long time. Some of the stated benefits are closely related, and some of the benefits are

Key benefits offered by cloud solutions are scalability, reliability, cost optimisation, operational efficiency, ability to do rapid& flexible deployment without compromising security & compatibility.

Cloud solutions are massively scalable, and allow organizations to grow their users from a handful to hundreds virtually overnight. It only takes an order for additional subscriptions and a payment to the cloud service provider. Elasticity is similar and allows for a sudden change in cloud computing resources to respond to spikes in demand. Allone need to access a cloud service is a current subscription, a good Internet connection and an internet-enabled device (e.g. desktop, tablet, phone). Cloud service providers use redundant IT resources and a quick failover mechanism, and many of them offer a 24/7/365 and 99.9% uptime guarantee.

Cloud is cost-effective, since one uses the shared infrastructure of the cloud service provider via pay-as-you-go modes of payment. Cloud also enhances operational efficiency, since administrative tasks (e.g. software upgrades, storage increase, data backup) are off-loaded to the cloud service provider. Cloud service providers offer an ecosystem of ready-to-use services that can be rapidly deployed with simple migration and configuration.

Users may have the flexibility of choosing online or installed deployment of cloud applications. Some service providers even offer the flexibility of Public, Private and Hybrid Cloud. Cloud service providers take the security of their systems very serious to retain their customer base. They also keep their entire software stack updated and fully compatible to keep services up and running. Finally, cloud services can be expected to be compatible with a wide variety of mobile devices and web interfaces.

* Research Scholar, Department of Management, Shri Jagdish Prasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India.
** Associate Professor, Department of Commerce & Management, Shri Jagdish Prasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India.

The challenges of cloud computing are known, but easily brushed aside or overlooked. Key challenges with cloud are Internet connectivity, interoperability, data security and protection that you might have to deal with:

For working on cloud environment, one needs to have good Internet connectivity and a powered-up device to access the cloud. This can be a challenge in a developing economy like Kenya, particularly outside the urban centers. Accessing cloud services through public Wi-Fi could pose a risk, unless the necessary security measures are taken. For most subscription plans one must make a monthly or annual financial commitment. The service ceases once you stop payment, and in the worst case you might lose access to your business data.

Comparison

Compare this to buying a permanent software license, which needs to be maintained for good reason. Cloud service provider could have the best security certifications, but there's no guarantee that organisations won't lose data. Cloud service providers might even abuse client data in disregard of privacy concerns. Hackers are increasingly targeting cloud storage for their abundance of sensitive data.

Cloud requires a new thinking about computing, and adoption will fail if the culture doesn't change. Cloud buying decisions are increasingly made by functional managers and influenced by end-user requirements. Managing the requirements and delivering the envisioned benefits requires a high level of IT maturity. Some of existing applications might not be available as a cloud service. In addition, organisation has little control over the cloud services that's subscribed. Therefore, integration between services from different service providers and applications that run on your organization's infrastructure could present a real problem. Digital business infrastructure has become more complex spanning mainframe, client-server, virtualized, server less and hybrid cloud platforms that include containers and micro services. Yet the core responsibilities of IT to monitor and measure the infrastructure haven't changed. How does one achieve infrastructure visibility and insights into workloads when performance data spans diverse environments?

Challenges of navigating the cloud strategy aren't felt by IT alone. Security must ensure the posture of an infrastructure they no longer directly control and IT business partners must demonstrate the ROI of moving to "renting" instead of "owning" infrastructure. More than ever, it's critical to monitor performance across hybrid architectures with tools that collect and correlate data from every location. Multiple, fragmented monitoring solutions don't provide the visibility and intelligence to meet business, security and IT goals. As companies migrate to the cloud, end-to-end operational visibility is essential before, during and after the switchover to maintain insight into performance and address fears related to losing infrastructure control. It also eliminates finger pointing when KPIs are missed and when IT's reputation is on the line. And what does operational visibility look like in a hybrid cloud environment? It's an end-to-end view of infrastructure performance across application workloads and micro services, wherever they reside.

It provides the intelligence needed to monitor and measure KPIs to ensure a compelling user experience when infrastructure spans public and private domains. Before a cloud migration, it's important to measure the baseline user experience and performance, as well as define acceptable post-migration levels. Degradation in one performance area may be tolerated if it's balanced or offset by gains in another. To accurately validate a migration's success, the same monitoring tool should be used throughout the migration process.

Analysis

During a cloud migration, established performance metrics should be closely monitored. Variation from the baseline is an early indicator of trouble. A monitoring solution's dashboard and alerts will quickly identify these issues well before production, and save time and resources. A performance issue is better identified during a migration when it's easier to pause and make corrections. After a cloud migration, the same monitoring solution should be used to measure acceptable metrics and success. And continued use of the solution and dashboards, well after the switchover, is essential to ensure compelling customer journeys that cross on-premises and public cloud workloads.

From security perspective, getting the complete picture to protect your organization and your customer's. To maintain security in a hybrid cloud environment, organizations need an end-to-end view of user identity and behaviour at every application and database access point. This view shows unauthorized access, threat and attack locations and privilege changes. It also provides critical knowledge as entry points are spread more broadly across platforms and geographies.

When migrating to the cloud, security and IT teams are still responsible for the full protection of corporate data and customer information. And finger pointing and breach disputes aren't considered acceptable by business leaders. Technology teams must have a full view of security posture across hybrid architectures, respond quickly to vulnerabilities and threats, and produce timely audits. Adding workloads to a public cloud does increase the complexity of the security landscape. It extends the points of entry for hackers and adds cloud provider staff to the list of potential threats. So for comprehensive user activity monitoring across hybrid cloud architectures, it's key to have easy access to log files and end-to-end tools that collect, correlate and analyze suspicious behaviour.

New solutions highlight IT progressive approach to application security, enabling customers to deliver safe, frictionless, and modern digital experiences as consumers increasingly rely on applications, bolstering organisation technology leadership position in combining multi-cloud application security and delivery with bot mitigation and anti-fraud capabilities to guard against sophisticated threats. Log files and monitoring tools provide ample visibility and analysis into user activity. They track the identity of users who submit, modify and delete data, and the time when that event occurs. They also reveal unauthorized access attempts, simultaneous logins from disparate locations and changes to access privileges. They can even help spot inadvertent information changes.

Dashboards within cloud monitoring tools can help visualize user identity and access events, and create a foundation to analyze trends. Alerts and reports allow seamless transition from a reactive to proactive response. Also, some tools offer predictive analytics that provide security intelligence to obtain a comprehensive view of the cloud infrastructure and security posture. And many monitoring tools can help establish audit procedures and conduct compliance checks to ensure adherence to internal and industry standards. With audit trails, IT and security teams can rapidly troubleshoot threats before they become a cyber-security breach.

Migration to the cloud can offer huge cost savings by reducing server ownership and management. But if cost projections are incorrect, the entire cloud business case can be jeopardized. ROI can decline and break-even dates can lengthen — the blame placed on IT for inaccurate projections. True spend can vary substantially from even the best crafted budget.

Strong visibility and projections of cloud provider costs can address this concern. When applied to existing cloud workloads, monitoring tools help improve forecasts for the next set of migrated apps. Through usage and cost analysis, they reveal when workloads should be moved to the cloud or left on-premises until cost structures change.

Cloud monitoring analytics can optimize costs by signalling users to buy instances in advance at lower prices. By applying machine learning algorithms to the consumption data of existing workloads, IT can more accurately predict compute and adjust predictions based on expected spikes in demand. This yields better use of company assets and increases margins. Flawed forecasts, on the other hand, can place IT's reputation at risk and drive business teams to bypass recommendations and set their own purchase patterns without visibility provided by monitoring tools.

It's frustrating not knowing the source of an infrastructure performance problem or security threat, especially at the critical point of workload migration. Multiple, fragmented monitoring solutions add to this issue, providing a fragmented view of an already stratified infrastructure.

But a single monitoring solution that provides dashboards to multiple audiences from the same data can unify teams and make the transition to the cloud as seamless as possible. When managing a hybrid environment, the goals of IT, security and business teams will remain constant. For exampleThe KPIs IT will need to monitor the scale up/down of changing instances and workloads are the same for monitoring on-premises workloads — and IT will need to connect that data with application metrics for holistic monitoring.

Security will need a complete picture of the entire infrastructure, including all cloud nodes, transactions and users to ensure the security posture, and protect against potential threats. Business teams will need to know what has been deployed in the cloud, the usage, and if any devices are unpaired or orphaned in order to mitigate costs and demonstrate ROI. Having all three groups drawing analysis from one source prevents finger-pointing and eliminates silos.

More than ever, it's critical to monitor performance across hybrid architectures with tools that collect and correlate data from every location. A single end-to-end monitoring tool that traverses a hybrid cloud environment is beneficial to three separate teams — IT, security and expense management. But having all three teams unified on the same data is even more beneficial to the entire business.

Migration to the cloud can offer huge cost savings by reducing server ownership and management. But if cost projections are incorrect, the entire cloud business case can be jeopardized. ROI can decline and break-even dates can lengthen — the blame placed on IT for inaccurate projections. True spend can vary substantially from even the best crafted budget. Strong visibility and projections of cloud provider costs can address this concern. When applied to existing cloud workloads, monitoring tools help improve forecasts for the next set of migrated apps. Through usage and cost analysis, they reveal when workloads should be moved to the cloud or left on-premises until cost structures change.

Conclusion

When migrating workloads to the cloud, it's critical to monitor performance across hybrid architectures with tools that collect and correlate data from every location. • Don't wait to add end-to-end monitoring services until migration. Instead, secure a solution to establish a pre-migration baseline, mid-migration insights and post-migration success. • Only end-to-end monitoring solutions that easily collect public cloud provider log files can pinpoint vulnerabilities, threats and breaches. • Cost management tools offer current and historical instance usage and show unused resources. But it's critical to have full infrastructure economics for strong resource forecasts and intelligent migration decisions.

Cloud computing offers many tangible benefits, but one must be ready to deal with the challenges. These challenges can be overcome through proper migration strategy, investment (e.g. Internet connectivity) in key areas and continuous improvement. Going forward migration to cloud is a necessity and not a choice so organisations need to prepare themselves for the same.

References

1. Dr. Dekker M.A.C. and Livery Dmitri, "Cloud Security Guide for SMEs", SME version, Published by anise, April 2015, Page Number: 20-25
2. Subshell Kumar and Naval Kishore Dogma, "Cloud Storage and its Secure Overlay Techniques", Int. Journal of Engineering Research and Applications, Volume 4, Issue 4 (Version 5), April 2014, Page Number 33-37
3. SeenJay dip, "Security and Privacy Issues in Cloud Computing", Architectures and Protocols for Secure Information Technology Infrastructures, Published by IGI Global, Section 1, Chapter 1, 2014, Page Number 1 – 45
4. Sharma Rajang and Thrived Raj ender Kumar, "Literature review: Cloud Computing –Security Issues, Solution and Technologies", International Journal of Engineering Research, Volume No.3, Issue No.4, April 2014, Page Number 221-225
5. Sharma R and Dr. Kaswan B, Study of Cloud Based ERP Services for Small and Medium Enterprises (Data is Processed by Text Mining Technique), Revisits de System's de Informer coo da FSMA n. 13, 2014, Page Number 2-10
6. Sporty V, Maratha M. and Santos Kumar B., "A Survey on Data Storage and Security in Cloud Computing", International Journal of Computer Science and Mobile Computing, Volume 3, Issue 6, June 2014, Page Number 306-313.