EVENT PROCEEDINGS REPORT

IDC BREAKFAST BRIEFING WITH IBM: ADDRESSING CLOUD IMPLEMENTATION CHALLENGES

Sponsored by: IBM

Chris Morris Raj Mudaliar

March 2012

IN THIS DOCUMENT

This Event Proceedings document provides an overview of the latest cloud trends and issues that were presented and discussed at a recent breakfast hosted by IDC and IBM on the morning of 8 March 2012 in Sydney. This breakfast was by invitation only and attended by 13 participants comprising CIOs, IT executives and service providers from a cross-section of businesses from Financial Services, Government, Education, Media, Engineering Services and Pharmaceuticals

Over the course of breakfast, attendees took part in a lively discussion on the key cloud implementation challenges faced by their organisations. Chris Morris, Associate Vice President for Cloud Services research, IDC Asia/Pacific, facilitated the discussion.

Note: The names of the participating companies have not been divulged for confidentiality reasons.

SITUATION OVERVIEW

The dominant themes that emerged at the breakfast briefing reflected the early cloud adoption stage common to most attendees. At the forefront of the cloud discussion were risk management and the real challenges posed to enterprises wanting to actualise the potential benefits of cloud services. Enterprise risk around network security, protecting data sovereignty, maintaining data privacy and data control were all cited as the bigger influences whilst evaluating workload migrations to the public cloud.

There was general acknowledgement that traditional enterprise risk assessment processes had not yet been rigorously applied in the initial phases of cloud adoption and new service delivery models.

Most of the participants agreed that both a private cloud and a hybrid model of private and public cloud are the future forms for delivery of IT infrastructure services, core business applications (e.g., enterprise resource planning), storage and storage management. Pure public cloud deployments are currently being used, or planned for use, to deliver less critical business applications like email, collaboration and horizontal business processes (e.g., payroll).

IDC Australia, Level 20, 8-20 Napier Street, North Sydney, NSW 2060 www.idc.com

Another interesting aspect of the discussion was around how social media platforms like Facebook, Twitter and LinkedIn are forcing enterprises to think differently and driving momentum for change, especially in sectors like education which are more exposed to the Gen Y audience. This has been further exacerbated by the proliferation of smartphones and media tablets at an unprecedented rate and soon poised to rival PCs and notebooks as the dominant end-user device.

For enterprises, it is inevitable that they must now formulate policies around bring you own device (BYOD) for employees, as well as develop clear strategies for mobility to enable access to enterprise applications anytime and anywhere. Although the impact of these new technologies varies from industry to industry, what is becoming obvious is that these changes are here to stay and depending on the maturity of the sector, it is only a matter of time the consumerisation of IT permeates every industry.

CHALLENGES FOR CLOUD MIGRATION

Some of the main challenges identified at the event was around workload migration to the cloud and are summarised as the following:

- **Security** – CIOs expressed concerns that this area has still not been fully addressed, but acknowledged that as global security standards are established, cloud service providers will continue to enhance their offerings to make them more robust and comprehensive.

- **Integration** – Firing up a server is easy once the correct processes and standards are in place, but it is the standardisation and integration with the back-end processes which are critical. This means undertaking a sometimes complex process of enterprise change involving people, culture and processes, which is far more difficult than the technology change.

- **Control of Data** – Unstructured data is increasing at a phenomenal rate within organisations. For example, in knowledge industries like pharmaceuticals, there are huge investments made in R&D. In such cases, issues like classification of data crossing over borders have huge legal implications and have yet to be addressed in a holistic manner.

CLOUD SERVICES – AN IDC PERSPECTIVE

(Based on IDC's ongoing research of the Cloud Services Market in Australia since 2009 and key findings from IDC's APEJ Cloud End-User Survey, April 2011)

While the market has been initially dominated by software-as-a-service (SaaS) cloud solutions, that trend has changed over the last 12 to 18 months as more robust infrastructure-as-a-service (IaaS) solutions became available from an expanded range of providers, and most recently, the platform-as-a-service (PaaS) offerings gained momentum. A major driver of the IaaS market has been the entry of telcos with their IaaS services, as well as the penetration of Virtual Private Cloud (vPC) services from IT infrastructure vendors, IT SPs and telco SPs.

IDC's 2011 APEJ Cloud End-User Survey estimates that APEJ spending on vPC will exceed that of public cloud IaaS by the end of 2013. The drivers of this trend include:

- Lingering mistrust of public cloud security.
- Public cloud performance concerns, especially for network latency, which are accelerating regional datacentre investments and a proliferation of vPC offerings from telcos as well as IT vendors and IT SPs.
- Pure private cloud has proven to be overly expensive in terms of budget, time and resources. Experience from early private cloud adopters has been that they are not able to meet their ROI targets without very large upfront capital investments.

Main Implementation Challenges

Key factors inhibiting cloud adoption include concerns about security, performance, availability, cost uncertainty, ability to bring cloud systems and information back in-house, as well as lack of integration and portability standards. IDC research shows that, by far, the greatest inhibitors to public cloud services adoption are security or privacy concerns and performance availability concerns (for example, latency on retrieval is a problem for email). If vendors fail to demonstrate steady improvements in addressing these concerns, or worse, if there is a significant number of high visibility failures, these inhibitors could seriously retard growth rates. Suppliers are, and will continue to be, very focused on bringing solutions to market that mitigate these concerns.

Public versus private

Hybrid portfolios with options for both public and private deployments, as well as combinations of both models, will be the preferred way forward. Ultimately, however, public cloud services will be more pervasive than private clouds, as most new solutions will be developed for public cloud platforms. Also, public cloud SPs will have significantly lower unit costs than many private datacentres, making it tougher for private datacentres to justify retaining systems in-house, where there is no compelling argument otherwise (e.g., security or privacy). The largest public cloud SPs will provide a level of security and availability comparable to most private datacentres because they will have greater resources (as shared SPs) than most customers.

Cloud Service Orchestration

Over the last 12 to 18 months, the more aggressive push of enterprise IT leaders with "trusted brands" into the cloud services market has begun to change the market significantly. "Enterprise grade" capabilities – in the areas of manageability, security, availability and legacy/private system integration are now sought and expected from cloud SPs. The first-generation pure-play cloud leaders – such as Amazon and Google – have evolved and expanded their offerings to counter the market entrance and trusted brand of established IT SPs such as HP, IBM, CSC and Fujitsu. Orchestration of cloud services, which refers to the integrated automation of provisioning, monitoring and management of the cloud services, is now a critical area of capability and only adequately provided by those cloud SPs which have invested in IT service management processes, people and tools. Without cloud orchestration services, much of the value of cloud services can be lost as the need for manual processes to take on the orchestration function removes much of the cloud advantage.

An ongoing challenge mentioned as part of the larger debate about cloud security management that is common to many multi-sourced solutions including cloud services is user identity management across multiple service sources. This is a challenge that is not unique to cloud, and moving to a single sign-on environment poses several challenges and needs to be addressed at the enterprise architectural level.

FUTURE OUTLOOK

The availability of public IT cloud offerings with higher levels of security, availability and reliability has already begun to change the direction of the development of next-generation on-premises systems. Early experience has shown that private cloud implementations can prove to be too difficult for all but the most well-resourced IT organisations, and apart from the potential for the use of externally hosted "virtual private clouds", there is also an emerging appetite for drop-in cloud appliance solutions that can remove the time-consuming configuration and test steps of such projects. These pre-configured and pre-tested hardware or software stacks are cloud-aware solutions and architected using private datacentre topologies and equipment skewed toward much heavier WAN (DC-to-cloud) traffic expected in a cloud-enabled datacentre.

This "cloudifying" of private datacentres will not just impact datacentre hardware, as virtually all enterprise-focused ISVs will introduce next-generation versions of their on-premises software that is architected for the cloud model (multitenant architecture, accessible via services portal, greater scalability, granularity and usage monitoring/metering).

Public cloud offerings are also driving demand for cloud-based solutions which aggregate individual cloud services to form IT service solutions in areas such as backup, file/data management and security that allow organisations to leverage public cloud services in conjunction with internal systems.

ESSENTIAL GUIDANCE FOR THE CIO

IDC recommends that event participants and CIOs consider the following key areas whilst developing and formulating their cloud strategy.

- The CIO has to understand risk management, not just from a traditional perspective but from a new approach which reflects knowledge and awareness of threat management. Governance, risk and compliance are now more critical in managing the overall process for successful business transformation.
- Enterprises must allow time to gain a good understanding of the cloud service offering from both the technical and commercial aspects. The cloud brings new elements to IT service delivery which, if not addressed at the start of the project, could destroy the value of their benefits.
- Even with the standardised offerings available from the cloud, the IT team must invest time in planning from the earliest stage and – if necessary – work with an experienced partner who is able to advise and navigate potential obstacles which could add risk to the project's successful delivery.