Hybrid IT Strategy

Benefits, Use Cases, and Risks

General Services Administration

Federal Acquisition Service, Cloud PMO

February 2016

Table of Contents

I. EXECUTIVE SUMMARY

When agencies find that they cannot migrate all IT infrastructure including legacy, applications or data to the public cloud, a blend of public and private cloud may be considered. Cloud Service Providers (CSPs) refer to this as a hybrid cloud. Migration to hybrid cloud should be done if tangible benefits may be achieved. Migrating to a blend of public and private cloud may help agencies sufficiently protect sensitive or classified data and still demonstrate compliance with OMB's "Cloud First" policy.

To ensure proper justification of cloud migration, agency CIOs may wish to seriously consider the use case for the workload of the application and comparing it to the option of leaving software running as is or migrating to a combination of private and public cloud infrastructure. Agency CIOs should ensure they identify the operational and business benefits of implementing a hybrid cloud and build the business case [1] to support their strategy.

II. DISCUSSION

a. What is a Cloud and what Cloud Strategy is Best?

As defined in NIST Special Publication 800-145, a cloud is a commercially provided IT service that must possess five essential characteristics such as on-demand self-service, resource pooling, rapid elasticity, measured service, and broad network access.

Federal IT stakeholders may wish to consider their cloud strategy, roadmap, and respective cloud deployment status. Secondly, stakeholders are encouraged to

[1] A study by several IT analytic firms found that major CSPs offering Infrastructure as a Service (IaaS) typically cost more than CSPs offering Private Cloud services once they reach about $7,000 in cost per instance. Research studies also found that if operations require 24x7x365 availability, it may be more cost-efficient to only host IT environments in a private cloud unless a CSP offers significant volume discounting.

consider whether the agency wishes to move all data and applications to the public cloud, the private cloud, or a split between the two to achieve the best degree of agility, elasticity/scalability, and availability in addition to the best protection of any sensitive data.

Government IT leaders should know before contracting with a vendor whether they want a public, private, or hybrid cloud. A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model with a greater number of computing resources that may be provisioned to meet varying workload demand than other delivery models, and may cost less than public clouds.

In a private cloud model, scalability and self-service are featured characteristics not unlike the public cloud, yet private cloud carries a proprietary architecture. Contrary to public clouds, which deliver services to multiple organizations, a private cloud has computing resources dedicated to a single organization. However, many internally designed and implemented private clouds fail as they are often unable to scale or meet growing security requirements.

In a hybrid cloud model, orchestration exists between public and private clouds. Agencies can run mission-critical workloads or sensitive applications on the private cloud while using the public cloud for high volume workloads that must scale on-demand. Acquisition stakeholders should carefully consider the inherent functions of their agency when selecting a cloud type to ensure an appropriate level of policy and governance. Implementing a hybrid model may require a fine balancing of security, achievable compliance levels, accessibility, computing and financial resources. However, hybrid models can leverage cloud management platforms (CMPs) to ease the burden of balancing security and thereby ensure optimum benefit and control is exerted. CMPs can also help identify and manage the prevalence of shadow IT, and is often deployed in SaaS instances.

b. Use Cases and Benefits of Hybrid IT

By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options. For example, an enterprise can deploy an on-premises private cloud to host sensitive or critical workloads, but use a third-party public cloud provider,

such as Google Compute Engine, to host less-critical resources such as test and development workloads. To hold customer-facing archival and backup data, a hybrid cloud could also use Amazon Simple Storage Service (Amazon S3). A software layer, such as Eucalyptus, can facilitate private cloud connections to public clouds, such as Amazon Web Services (AWS).

Hybrid cloud is particularly valuable for dynamic or highly changeable workloads. For example, a transactional order entry system that experiences significant demand spikes around the holiday season is a good hybrid cloud candidate. The application could run in a private cloud, but leverage public cloud computing resources (for additional cost) when computing demands spike. To connect private and public cloud resources, this model requires a hybrid cloud environment.

Another hybrid cloud use case is big data processing. A company, for example, could use hybrid cloud storage to retain its accumulated business, sales, test and other data, and then run analytical queries in the public cloud, which can scale to support demanding distributed computing tasks. In comparison, a private cloud, may not always have the scalability necessary to handle the workload needed to achieve an agency's desired results, measurable objectives, or business goals.

Many agency cloud environments are still evolving. However, most large agencies are using a mix of private and public commercial clouds for a variety of workloads, such as email and collaboration, content management, test and development, big data analytics and even security. Hybrid IT solutions offer the benefit of Cloud Storage Gateways which may also help agencies store data where rapid elasticity is valued. Finally, a hybrid IT strategy relieves agencies of the burden of retaining trained staff to manage data centers or on premise application hosting environments. CSPs take on that responsibility, or enable the customer to control the network at the SaaS or PaaS level.

When moving forward, achieving the ability to virtualize the network is the first step. Virtualization, a means of partitioning servers and operating systems to share computing resources and applications across multiple users, has expanded throughout the infrastructure, from computer to storage to the network layer. Virtualizing the network is a critical next step toward the evolution of the hybrid cloud, according to Doug Bourgeois, Vice President of End-User Computing with VMware U.S. Public Sector. Virtualization at the network layer allows managers to disconnect the application from the physical network. Once complete, the entire business application can be

moved across a unified management control point. “You can actually migrate from datacenter to datacenter,” said Bourgeois.

Policies can also be applied at the network layer to give business applications specific priorities. For example, a credential-checking app used at border crossings or in airports should always be running, so it would have higher priority than a human resource management app. If there is a disruption of services, apps can be navigated around problems to maintain service levels via a unified management plane. A hybrid cloud can allow agencies to seamlessly manage applications and data across multiple clouds and on premise platforms.

Bottom line, CIOs may find the hybrid cloud strategy a formidable choice in deployment model after the benefits are realized, especially the ability to handle dynamic workloads while still protecting the most sensitive data in the private cloud.

c. Risks of Hybrid IT

Hybrid clouds may become normal practice among federal agencies, however, the challenge will be interconnecting multiple clouds to work as a seamless whole. There is always the risk of agencies building cloud silos – an email in one cloud, office automation in another, test and development in yet another cloud. These clouds may not be interconnected and use different sets of management tools. Cloud service brokerage (CSB) technology, which connects a diverse set of users to a marketplace of cloud service providers could provide the unified management necessary to prevent silos.

To mitigate the risks of cyber incidents, hybrid IT or hybrid cloud strategies should ensure security is designed from the ground up. Most CSPs have the ability to continually invest in security whereas in legacy government network administrators cannot. Additionally, CSB and CMP technology may be able to offset workload handling and provisioning issues in the hybrid cloud by running SaaS discovery tools to inform the administrator of what is already using elements of the public cloud.

III. RECOMMENDATIONS FOR BUILDING A HYBRID CLOUD

■ Ensure cloud use aligns with the agency's business goals. Business goals and objectives should determine the proper cloud strategy or deployment model to pursue. CIOs and senior leadership should identify which of the cloud attributes they most readily need or want at the outset of planning, and ensure financial, performance, risk and business outcome metrics are appropriately aligned. When discussing with leadership, CIOs may also wish to take a "coaching" approach in getting senior leadership to understand what is required of them. Cloud migration involves significant organizational change. The government or agency CIO must, at the earliest possible stage, engage the senior leadership and other disciplines in the debate. New skills for staff and management, organizational procedures and processes around risk management and emergency planning, all of which can add cost, as well as absorb staffing effort, will be new requirements.

■ Build a private cloud with a hybrid cloud model in mind. Many agencies have built private clouds without thinking about hybrid, which resulted in the cost and labor of modifying those clouds to more closely resemble a hybrid configuration.

■ Ensure the necessary staff and skill sets are available to support cloud acquisition, migration of applications, automation tool (e.g., CMP) operation, contract monitoring, and vendor management.

■ Agencies should interconnect the clouds they utilize, and build actual network connections between them. In order to create interconnected multiple clouds, federal managers and industry experts believe that they must tie them together in a unified management plan that lets organizations use the same toolsets and security profiles. Leverage CMPs and CSBs as needed.

■ Extract the environment from the physical systems and network via virtualization.

■ Migrate applications and services to the hybrid cloud.

■ Establish a unified management control point to extend management and security policies across the hybrid cloud. Agency managers should practice "context-aware IT", where the level of assurance of the data defines the required level of trust. They have to look at who are the users, what data are they accessing, where they are and where the data is located. Valuing information is important in determining the risk associated with moving beyond the data center to the cloud.

- Ensure an exit strategy exists for off-boarding applications or transitioning them to the next cloud integrator or vendor. Verify SLAs cover transition of data, applications, and software to prevent “lock-in” issues. CIOs should ensure cloud service offerings are interoperable to ensure applications and data can be on and off-boarded.

- Build a strategic plan for hybrid cloud services, including the expected road map for services (and corresponding processes and automation) and end states.

- Modify the strategic plan constantly based on gained knowledge, new customer requirements, changes in service use, changes in cloud infrastructure technologies and changes in the cloud computing provider market.

- Invest in hybrid cloud not only to deliver a rapid return on investment, but also to enable sourcing model and architectural evolution over time (including off-premises and public cloud models.

■

REFERENCES

1. Hybrid Cloud Definition – Techtarget.com http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud
2. Techtarget.com – Cloud Computing http://searchcloudcomputing.techtarget.com/definition/cloud-computing
3. NIST SP 800-145, NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
4. NIST SP 500-292, NIST Cloud Computing Reference Architecture, Sept 2011 http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
5. OMB 25 Point Implementation Plan to Reform Federal Information Technology. December 2010 https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf
6. Hybrid cloud strategy needs unity from the start. Federal Times: http://archive.federaltimes.com/article/20140728/FEDIT03/307280003/Hybrid-cloud-strategy-needs-unity-from-start
7. Is There a Point Where Private Cloud Is Cheaper Than The Public Cloud. Network World. http://www.networkworld.com/article/2825994/cloud-computing/is-there-a-point-where-a-private-cloud-is-cheaper-than-the-public-cloud.html
8. Security Issues: Public vs Private vs Hybrid Cloud Computing. International Journal of Computer Applications (0975-8887) Volume 55-No.13, October 2012 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.245.1453&rep=rep1&type=pdf
9. Gartner. “When Building a Private Cloud, Start Big, Think Small”. Bittman, Thomas J. November 2013. http://www.gartner.com/document/2629234?ref=sendres_email
10. Gartner. “Key Skills Needed for Successful Deployment of Cloud Computing in Government”. Cannon, Neville. April 2014. http://www.gartner.com/document/2720817?ref=sendres_email
11. Gartner. “Government Cloud Benefit Realization Starts with Business Alignment”. Cannon, Neville. December 2015. http://www.gartner.com/document/3176020?ref=sendres_email