

Multi-cloud management

Unified governance-based approach to multi-cloud

Just when it seemed like we are getting the hang of using and managing one cloud, along comes “multi-cloud”. In this article, we will explore recent multi-cloud trends and the associated complexities managing multiple clouds (vendors) as a unified (single-pane-of-glass) governed cloud. Furthermore, we will recommend strategies and tactics for organizations to deal with the presented complexities and prepare themselves for the inevitable future.



Harish Bharadwaj
is Senior Manager, Digital Transformation at KPMG.
bharadwaj.harish@kpmg.nl



Alexandre Ferreira Gomes
is Senior Consultant, Digital Transformation at KPMG.
ferreiragomes.alexandre@kpmg.nl



Olga Kulikova
is Senior Manager, Cyber at KPMG.
kulikova.olga@kpmg.nl

AWS WENT MULTI-CLOUD. WAIT, WHAT?

December 1st 2020 was an interesting day in the world of cloud. Amazon Web Services (AWS) announced two new services, Elastic Container Service (ECS) Anywhere and Elastic Kubernetes Service (EKS) Anywhere, slated for 2021 launch. Although they are primarily aimed at managing applications and containers on private data centres, Amazon quietly confirmed that each service works on any infrastructure, be it on private data centre, or Microsoft Azure or Google Cloud. It seems that AWS, like all of us, has come to terms with, albeit somewhat, the inevitability of multi-cloud in the future.

For too long, multi-cloud seemed like a solution in search of a problem. But as cloud providers have begun to differentiate between themselves with specialized offerings, companies are beginning to realize that each provider has its own advantages and disadvantages. AWS may be leading Google Cloud Platform (GCP) with EC2, but App Engine may be preferable to AWS Elastic Beanstalk. And as companies become more experienced and gain further expertise in cloud, they are no longer feeling intimidated by the concept of adopting another cloud platform.

Multi-cloud, as the term indicates, is used primarily in IaaS and PaaS context when companies decide to use two or more platforms such as Amazon Web Services (AWS), Microsoft Azure or GCP to place their workloads (in computer science terminology, workload refers to the amount of work that software imposes on the underlying computing resources). Traditionally, people have tried to drive a distinction between multi-cloud and hybrid cloud, which meant a combination of on-premise, private infrastructure and public cloud infrastructure. But for an integrated cloud strategy, where both hybrid and multi-cloud components are expected to co-exist, it is extremely important not to separate hybrid cloud setups at the start of the definition (which can also be applicable to certain SaaS setups, as many of them can be used for similar purposes and use similar management capabilities). It is worth mentioning that the complexity associated to the maintenance of these setups is likely to increase when compared to more traditional setups, given the additional number of services to be managed and the intricacy to coordinate and maintain all the infrastructure and cloud environments.

WHAT IS DRIVING MULTI-CLOUD?

The factors that are ratcheting up the move to multi-cloud can be classified broadly into two different buckets:

1. **Intentional** – Deliberate, structured designs aiming to benefit from best-of-breed services, avoid vendor

lock-ins, reduce risks and achieve the desired operational agility.

2. **Situational** – Typically, as a result of acquisitions, geographical limitations, legacy infrastructure, organizational complexities, low maturity, service envy, Shadow IT or, sometimes, a combination of multiple factors.

Historically, most organizations have ended up inheriting multi-cloud issues (situational), rather than intending to adopt multi-cloud in a deliberate and structured manner (intentional). But multi-cloud is inevitable. IDC ([IDC19]) predicts that by 2022 “the top 4 clouds will be the destination of choice for 80% workloads (Amazon, Microsoft, Google, IBM currently), while lock-in will be avoided through multi-cloud and cloud native approaches to achieve portability”. With this, IDC also expects that “90% of European 500 organisations will have a multi-cloud management strategy that includes integrated tools across private and public clouds by 2024” and that “By 2024, 90% of Global 1000 Organizations will have a multi-cloud management strategy that includes integrated tools across public and private clouds”.

YES, IT IS HARDER THAN IT LOOKS

Most architects concur that it is at least twice as hard to migrate from on premise setups than it is to migrate between clouds. But companies constantly underestimate multi-cloud by treating cloud as a collection of servers to run containers on and citing the eventual move to containers (Docker, Kubernetes etc.) as a solution to all their problems. While basic primitives such as Virtual Machines, Containers and Storage exist in all big cloud providers, adoption of multi-cloud should simply not be equated to just these commonly used components. Even for containers, platform lock-in issues crop up. Whether it's the use of managed cloud container services such as Azure Kubernetes Service or augmenting Containers with AI services, serverless functions, IAM policies etc., containers too are tied intrinsically to platforms and their capabilities.

Some of the challenges for adopting a multi-cloud strategy:

- The only services that can potentially be adopted are the lowest common denominators, which are typically the basic primitives. Every service offering that is higher order (secondary services such as security groups, load balancers etc) is unable to be utilized natively as they all work differently across cloud providers. For example, when we create an EC2 instance on AWS, we also tend to create Elastic IPs, Auto Scaling Groups, Network / Application Load Balancers, etc.
- These additional / higher order services therefore end up requiring customized solutions, which in turn,

add a lot of new complexity. There is a fine balance between managing complexity and valued benefits.

- Cross-cloud deployments are complex and require manual efforts and multi-domain expertise
- Spreading spend across cloud providers simply reduces negotiating power.

CHAOS CONTROL

Despite the enormous complexities involved, the needs of an average organization are so diverse that they will not be able to resist the temptation of being multi-cloud. Recognizing this as unavoidable, there are things that IT Organizations can do to prepare, govern and ensure that they are ready for multi-cloud. Even when the adoption of multi-cloud is situational, the following steps are still applicable and should be taken into consideration as soon as possible.

1. Adopt an intentional strategy, architecture and operating model

Right off the bat, IT organizations should actively define a multi-cloud strategy, a set of governance and architecture principles, think about the changes that will be required in the operating model and which blueprints should be in place. It is better to be intentional than being stuck with an uncomfortable situation – and it is also better to re-think your path sooner than later.

The *target operating model* is an overall ecosystem that allows companies to embark on a path for achieving their strategic vision on the basis of different priorities, principles and starting points.

2. Perform a comparison and assessment of cloud providers

Even though many cloud services may appear to be similar or comparable across different cloud providers, looking into the details is likely to be a worthwhile investment and will also be a continuous endeavour. A thorough investigation of the benefits and main competencies of each cloud provider is therefore a must when it comes to defining a multi-cloud strategy. Cloud providers should be compared and classified based on what they may offer to your business and classified per technology, line of service, potential for innovation, or any other key criteria for the business. Real-life use cases should be developed and taken into consideration at this stage, to substantiate the analysis with meaningful examples, which are recognized by the business and can be tested when starting the deployment of the workloads.

3. Create a workload placement methodology

Organizations should build an explicit workload placement decision tree (see Figure 2, a sample Cloud Hosting Analysis Framework which takes into account performance, cost, regulations, geographical restrictions, internal policies, etc.) to guide application and infrastructure teams to determine whether the workloads should be placed on the cloud, which cloud the workloads should live on and how they are integrated with the rest of the portfolio.

Figure 2 provides a simple example of the type of analysis that KPMG uses to help its clients perform, enabling well-informed planning of where (and why) each workload should be placed. This assessment is rec-

Figure 1. KPMG operating model framework as a holistic method ([Koni18]).



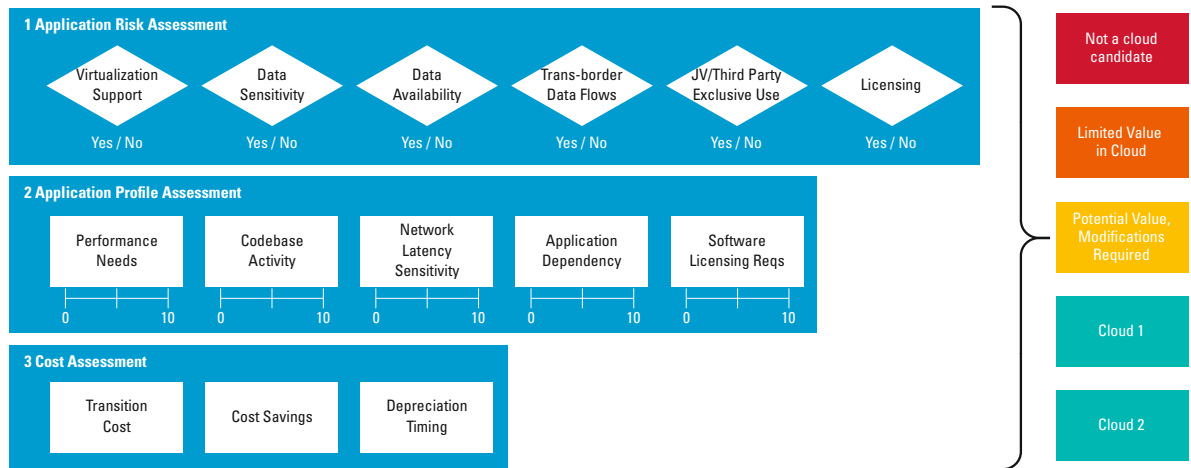


Figure 2. Sample Cloud Hosting Analysis Framework.

ommended to be on an application level and responds to three levels:

- The application risk assessment explores the limitations of each application or workload (e.g. due to data privacy-related legislation or licensing reasons).
- The application profile assessment is focused on more technical and performance aspects (e.g. dependency of other applications or latency requirements).

- The cost assessment looks at the financial aspect of a potential migration (e.g. the investments required to perform a migration and the ROI).

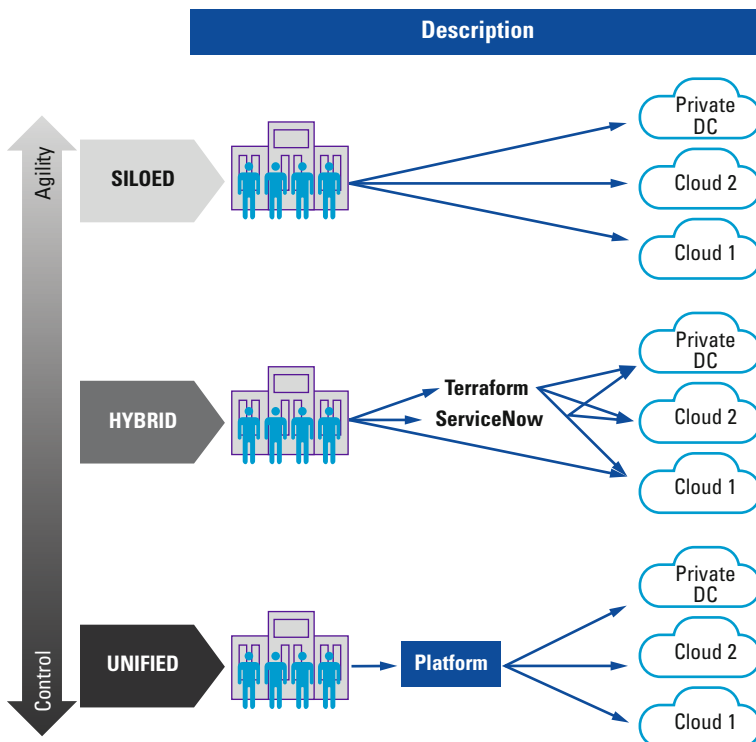
4. Determine a multi-cloud tooling strategy

Siloed management, whereby each cloud is managed independently of the others, provides a greater level of agility than a unified management strategy, which typically makes use of a cloud management platform or a cloud services broker. This approach enhances the ability to access new features and services as and when they are released by the vendors, which is an advantage. However, it is important to keep in mind that each cloud requires its own set of specialists, which may involve additional costs.

Yet another approach is to manage all clouds using a single service (typically through a managed services provider). While this provides a single-pane-of-glass on most aspects of the different clouds being used, it normally also means a slower exposure to new cloud technologies.

The industry leading practice is to establish a unified management capability across all the environments and utilize a hybrid tool setup. Most cloud providers typically provide technical and management tooling, although they are limited to their respective environments. The key to success is establishing a common management layer across identity, security, service management and operations automation, similar to a single-pane-of-glass, for all in scope environments. Figure 4 shows some of the capabilities required and the split of the scope of responsibilities entailed by different operators.

Figure 3. Cloud management approaches.



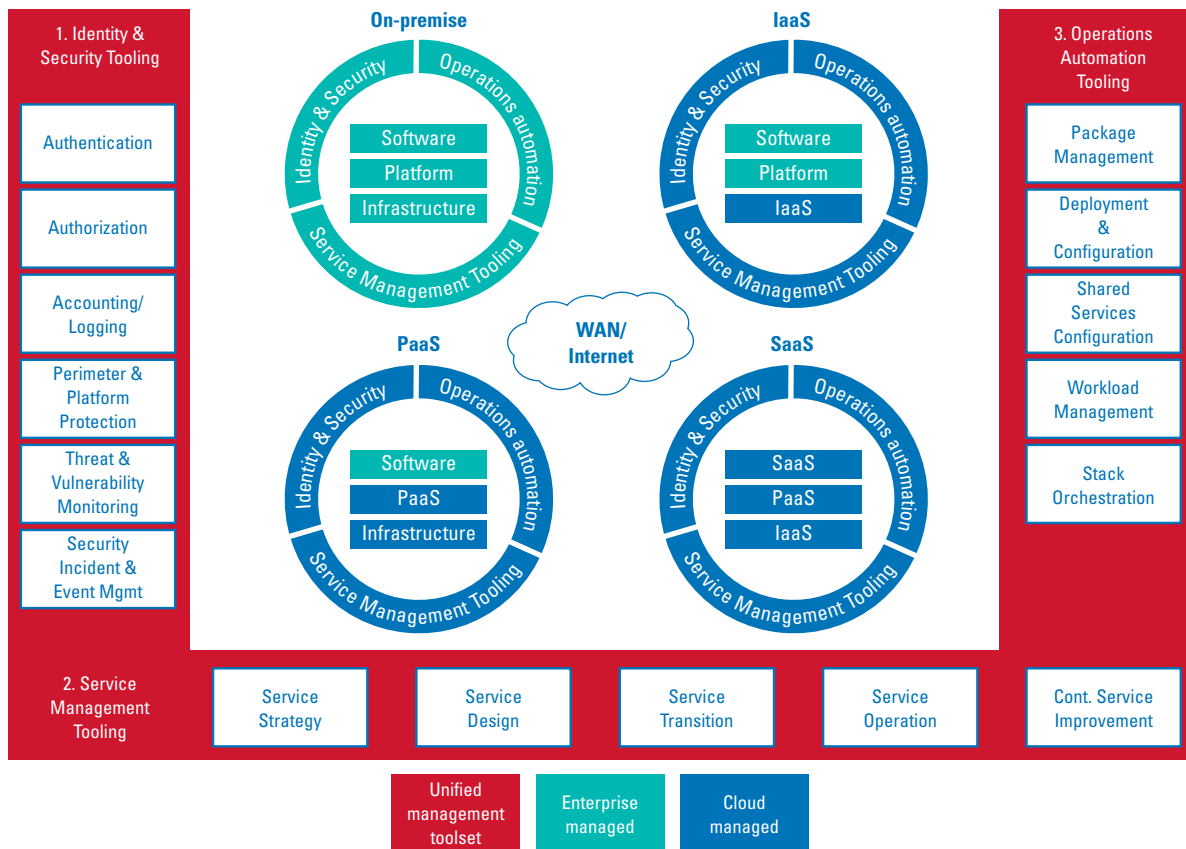


Figure 4. Sample unified cloud management capabilities.

CONCLUSION

Multi-cloud increasingly proves itself to be the correct end game, even AWS thinks so! Multi-cloud, if tapped correctly, can provide huge advantages in agility, flexibility, performance and cost effectiveness amongst other benefits. While lingering concerns about multi-cloud are understandable, a plethora of technologies

such as Containerization, Kubernetes, OpenStack are making life easier. It is, however, up to the companies, who have no choice but to change their approach and evolve their services to either gain a competitive edge or risk falling behind.

References

- [Boul19] Boulton, C. (2019, 3 October). Multi-cloud strategy: Pros, cons and tips. Retrieved from: <https://www.cio.com/article/3441856/multi-cloud-strategy-pros-cons-and-tips.html>
- [Harv20] Harvey Nash / KPMG (2020). *Harvey Nash / KPMG CIO Survey 2020: Everything changed. Or did it?* Retrieved from <https://home.kpmg/xx/en/home/insights/2020/09/harvey-nash-kpmg-cio-survey-2020-everything-changed-or-did-it.html>
- [IBM20] IBM Cloud Education (2019, 5 September). Multicloud. Retrieved from: <https://www.ibm.com/cloud/learn/multicloud>
- [IDCr9] IDC (2019). IDC FutureScape: European Cloud 2020 Predictions. Webcast, January 21, 2020. Retrieved from: <https://www.uk.idc.com/trends/european-futurescape-2020>
- [Konir8] Koning, T. de, et al. (2018). The CIO journey to agility. *Compact* 2018/2. Retrieved from: <https://www.compact.nl/articles/the-cio-journey-to-agility/>

About the authors

Harish Bharadwaj heads the Products and Services Management service line and is Senior Manager, Digital Transformation at

KPMG. He has been at the forefront of Products Management, Agile, Cloud, DevOps and IT Service Management for the last 14 years and brings extensive knowledge and experience in helping clients better ideate, architect, develop, and manage their solutions (products and services) throughout the lifecycle.

Alexandre Ferreira Gomes is Senior Consultant Digital Transformation at KPMG. He supports his clients in their digital transformation journeys and focuses on architecture- and infrastructure-related questions. He feels comfortable bringing business and IT together to realize the full potential of each organization, enabling well-thought and sustainable improvements on how people, processes and technology interact with each other.

Olga Kulikova MSc is Senior Manager Digital Transformation at KPMG. She helps KPMG clients with their information risk management, identity and access management (IAM), cloud transformation and IT assurance programs. Her passion is helping companies realize value in their large-scale transformation and innovation programs without introducing security and privacy risks. Olga is a Certified Cloud Security professional (CCSP) by (ISC)2.