Hybrid Cloud Orchestration

Edwin Sturrus MSc and Olga Kulikova MSc

Those readers who have cloud computing on their radar might have noticed a growing hype around the term "hybrid". It is becoming another fuzzword and, like the term "cloud", doesn't represent a new technology solution so much as a new way of deploying and managing IT environments. In general, going for a hybrid cloud simply means using different cloud deployment models simultaneously – they could include public, community, or (virtual) private cloud deployment models.

E. Sturrus MSc
is security advisor at
KPMG Advisory N.V.
sturrus.edwin@kpmg.nl

O. Kulikova MSc
is security advisor at
KPMG Advisory N.V.
kulikova.olga@kpmg.nl

Few IT professionals resist acknowledging the benefits of hybrid cloud. Why limit yourself to only one cloud model? Why not combine the best of all worlds and harvest the economic pay-as-you-go benefits of public clouds, and at the same time keep the enterprise-critical workloads under the "control" of a private cloud? That is exactly the tendency we see now within organizations – leveraging both private and public computing – which is in line with Gartner's estimation that "nearly three fourths of large enterprises expect to have hybrid deployments by 2015" ([Gart13a] (Thomas Bitttman)).

In this article we will cover the main reasons why organizations end up with a mix of cloud environments. Then we outline security concerns arising from the shift towards hybrid, and propose a solution framework for successful cloud management, which is now often referred to as "orchestration".

Moving to Hybrid Cloud

Regardless of what route an enterprise may choose – to employ just one private and one public cloud to keep things simple, or to go with a strategy involving multiple public clouds – practice shows that the horizon is already "cloudy" and enterprises have their data processed by a variety of different cloud service providers. Most of the time this is the result of easily accessible cloud offerings on the market, where a given department (e.g., marketing, HR) can purchase a cloud offering with one click for their specific business needs. Sometimes this happens because IT requirements for certain applications or data cannot be met by one specific provider, so the company has to add another one.

In general, there is a common motivator behind all of the different cloud usage scenarios: enterprises are looking for choice and adaptability, to be able to run their resources in the places where it makes the most sense; that means involving multiple cloud service providers (CSPs) instead of just one. Organizations usually cite the following reasons when deciding on their cloud strategy and whether to involve multiple CSPs or keep data in a private cloud:

- Cost benefits of certain providers;
- Reliability and performance benefits;
- Speed of deployment;
- Storage location (e.g., jurisdictions with different data protection laws);
- Security, risk and control reasons;
- Off-the-shelf, ready-to-use SaaS solutions.

For example, there could be many reasons for keeping data in the on-premise cloud platform. Some organizational workloads can be so unique that it would not be possible to shift it to the public cloud, or at least not

feasible from a cost-benefit perspective. Also, in certain jurisdictions, regulations still do not allow certain applications and data to leave the enterprise boundaries without a proper assurance from the CSP side, which many current providers cannot provide in full. As such, companies must keep their most critical data in-house. On the other hand, the motivation to shift to a public cloud can include accessing additional computing power for certain applications during peak seasons, which public CSPs can provide. Or, multiple CSPs for similar operational tasks may be an option for organizations that are afraid of locking themselves into a single cloud solution. Such lock-in can happen, for example, when a customer starts using a vendor's APIs that are not supported by any other cloud provider, which makes shifting to another provider a painful task.

Eventually, as more companies see the benefits of hybrid clouds mentioned above, the answer to the question of whether "to go hybrid or not" will be increasingly positive. Next, further questions will arise, such as to what extent should companies diversify in terms of hybridity? How should they integrate and manage multiple clouds? Also, what are the consequences in terms of enterprise security?

Security Concerns

Hybrid cloud security will take center stage, as there will not be a single solution for it, considering the unique approaches to "going hybrid" adopted by each organization. No matter how many CSPs get involved, it cannot be assumed that once the services and data are shifted to the cloud, security becomes the sole responsibility of the CSP. The amount of responsibility assumed by the enterprise usually varies depending on the cloud service model (IaaS, PaaS, or SaaS), the sensitivity of the data and assets put in the cloud, and the security maturity of the CSP.

In order to secure a hybrid cloud an enterprise should start with a complete understanding of what the enterprise's desired level of control is. It is important to determine that desired outcome before taking any hybrid initiatives. The desired level of control is easy to grasp when there is a clear understanding of the importance of the assets and data to be shifted to the cloud, and what the consequences could be of establishing connections with the third parties.

Once the boundaries of control are defined, an enterprise can start developing strategies to stay secure, which will

Case Study: Hybrid Cloud Orchestration

A large organization in the energy sector wanted more elastic and pay-as-you-go IT services, in order to reduce costs and make the organization more agile. Therefore the strategic decision was made to move most of their IT assets, such as services and data, to the cloud. For this organization losing confidentiality, integrity or availability of their business critical information would have a major impact on the organization itself and its stakeholders, potentially to the level of going out of business. As a result, the organization spent a lot of effort on maturing their IT security and specifically defining their security requirements and controls regarding the different classified types of data and services. In principle, any type of service or data was allowed to move to a public or private cloud as long as the required security requirements and controls were met. However, for the most confidential data and services, the defined security requirements were strict. Examples are: the infrastructure has to be a non-shared physical infrastructure, there has to be complete network isolation, all connections must be encrypted, all backups must be encrypted and access should go through IPSec VPN. Besides that, public cloud services have to be provided from inside the European Union. When taking into account the security offerings of the various cloud service providers in the market, the organization determined that their security requirements for the most confidential data cloud could not always be met in a public cloud. Therefore, specific services and data had to remain within the organization itself, in order to meet all the security requirements. This drove the organization to the decision to opt for a hybrid option and secure its most confidential data and services within the on-premise private cloud.

In order to stay in control of where the classified information was being sent outside the private cloud environment, the organization had to obtain a complete overview of their existing cloud services. The organization was aware that multiple cloud services were used by employees, without being onboarded, allowed and controlled. Examples such as TeamViewer or Evernote were in use by employees, even though these services were prohibited. In order to get a full overview of the cloud services in use, a scan on the network was performed: collecting logs from firewalls, proxies, and gateways over a period of time. Later this data was analyzed with a commercial tool to make sure that majority of cloud services used by employees were captured.

After that, the organization performed a risk assessment of the discovered cloud services based on the

result in sound security policies covering the cloud, as well as security and compliance mandates. This way, a variety of security issues and topics can be timely addressed by enterprises, such as:

- **Security of data in motion.** Enterprises will have to develop or establish secure interfaces with the CSPs, to ensure end-to-end security of data flows between corporate infrastructure and the public clouds. Securing the data flow can be accomplished, for example, by using SFTP or HTTPS, or by routing all connections from and to the CSP through VPN ([CSA11]).
- **Security of data at rest.** Enterprises will need to think about the ways to protect their data residing in the cloud from unauthorized access. Encryption solutions and a well-thought-out approach to identity and access management will be required to protect data at rest. It will also be important to understand where data is going to be stored and make it part of the agreement with CSPs, as they might shift data here and there, for example to their own third-party providers, without making enterprises aware of that. An organization will also need assurance that, in case of contract termination or bankruptcy of the CSP, the company's data will be fully migrated or destroyed.
- **Enhanced visibility.** Enterprises will need to consider how to demand better visibility of their public cloud resources, and thereby improve their ability to monitor and analyze aspects like access to enterprise data. Better visibility also means receiving timely and sophisticated overviews of security incidents in the cloud, e.g., via security dashboards. Integration of information streams from multiple public clouds will also require management's attention, to make sure that the enterprise has complete oversight of all public cloud services it uses.
- **Cloud service brokerage.** Gartner also estimates that by 2015 20% of all cloud services will be consumed via internal or external cloud service brokerages ([Gart13b] (Thomas Bittman)). Cloud Service Brokerage happens when an internal team or external third party acts as an intermediary between the consumer of a cloud computing service and the CSPs. Organizations will need to examine whether or not this will result in new security issues (e.g., cloud service brokerage being an additional point of exposure), or is it actually creating enhanced security by establishing a single solid security policy with that brokerage.

Organizations need to find the way to manage the described mix of cloud environments without losing control over security requirements. With a clear overview of already employed clouds and their risk, as well as the organizational future vision on clouds, the orchestration processes around them had to be defined to create and maintain sustainable cloud solutions.

The orchestration framework was populated with the processes of selection, on-boarding, governance and monitoring of clouds. These processes were aligned with the organizational security requirements and controls, for each different classified type of information, considering the roles and functions of the stakeholders and the business units involved. This enabled the organization to maintain the desired level of control of the cloud services that were used and are to be on-boarded in future, without losing the flexibility and fast adoption rate of cloud computing, by keeping the on-boarding process flexible and easy.

To conclude, in order to reap the benefits of hybrid cloud, organizations have to increase the focus on security and control. As more clouds come into play, each having its own specifics and rules, it can become a burdensome task for organizations to implement controls and govern different environments. Cloud orchestration framework is required to facilitate the process and establish centralized control over multiple clouds.

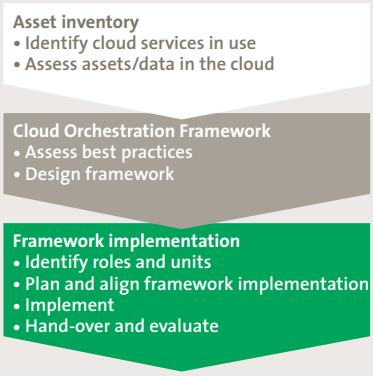

Figure 1. **Orchestration Framework Implementation.**

trol over them and thereby increasing the chance of security incidents. At the same time, the effort to be in control should not exceed organizational goals of being agile, reducing IT costs and other benefits when moving to a hybrid cloud. In order to find and maintain a good balance between the enterprise control over the cloud and its trust in the CSPs, so-called cloud "orchestration" is required.

Cloud Orchestration Framework

We view orchestration as an organizational ability to develop business cases, analyze and mitigate risks and govern IT services [KPMG11]. In relation to hybrid cloud computing, organizations need to be able to define their cloud strategy with respect to multiple cloud providers, determine requirements, select solutions, follow on-boarding procedures, govern and monitor existing and newly deployed services. The framework to coordinate all of these processes is called the cloud orchestration framework. The following focus areas of cloud orchestration can be distinguished:

- **Cloud business-case** – the process of designing a solid business case, or strategy, for using the cloud service(s), including requirements for specific cloud use-cases. The requirements can be imposed both on the organization itself as well as on the CSPs.
- **Cloud selection** – the process of selecting the preferred cloud service provider, based on a set of predefined assessment criteria. Assessment activities can include going through checklists together with the CSPs, reviewing third-party assurance reports, or, if possible, conducting on-site audits.
- **Cloud on-boarding** – the process of on-boarding a cloud service in a consistent, efficient, secure and compliant manner. A special attention is on migration of enterprise mission critical workloads during the on-boarding process, which should not impact the confidentiality, integrity, and availability of the enterprise data.
- **Cloud governance** – the process of optimizing the benefits of hybrid clouds, which includes management of multiple service providers, demand and purchase control, the integration of processes and technology, and the termination of the cloud service.
- **Cloud monitoring** – the process of monitoring existing cloud services against the organization's security policies and agreed SLAs, as well as periodically analyzing logs and discovering "shadow" third party cloud services adopted by the enterprise employees.

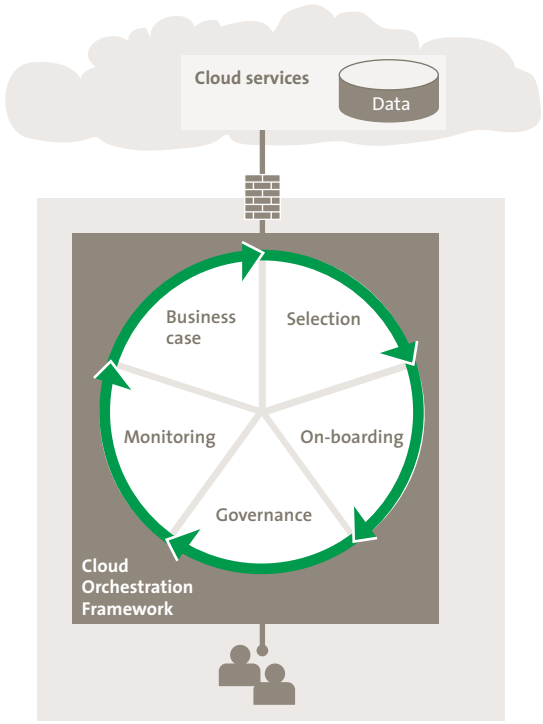

Figure 2. **Cloud Orchestration Framework.**

Further reading

[KPMG11] KPMG, 2011, "Orchestrating the New Paradigm. KPMG's Business Guidelines to Cloud Computing and Beyond," available at http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Cloud%20Paradigm%20Art.pdf

[Gart13a] Gartner, 2013, "Private Cloud Matures, Hybrid Cloud Is Next," available at http://www.gartner.com/document/2585915

[Gart13b] Gartner, 2013, "Hybrid Cloud Is Driving the Shift From Control to Coordination," available at https://www.gartner.com/doc/2592815

[CSA11] CSA, 2011, "Security Guidance for Critical Areas of Focus in Cloud Computing," Version 3.0. available at https://cloudsecurityalliance.org/research/security-guidance/

About the author

E. Sturrus MSc is security advisor at KPMG Advisory N.V. in the Netherlands. He has been involved in multiple IT-security-related engagements, such as IT GRC, Identity and Access Management, Cloud Computing, PKI Audit and IT Audit. Before he started working for KPMG, Edwin studied Economics and Informatics at Erasmus University in Rotterdam. He wrote his Master's thesis on Cloud Computing and Identity and Access Management.

O. Kulikova MSc is security advisor at KPMG Advisory N.V. in the Netherlands. She advises companies on Information Risk Management, Cyber Defense strategies, Cloud Security, Identity and Access Management, and PKI. Olga also performs IT assurance and certification audits for various clients in Europe and abroad.
Prior to joining KPMG, Olga completed a MSc in Technology Management at TU Delft University, the Netherlands, in conjunction with Carnegie Mellon University, USA, with a focus on Information Security and Privacy.