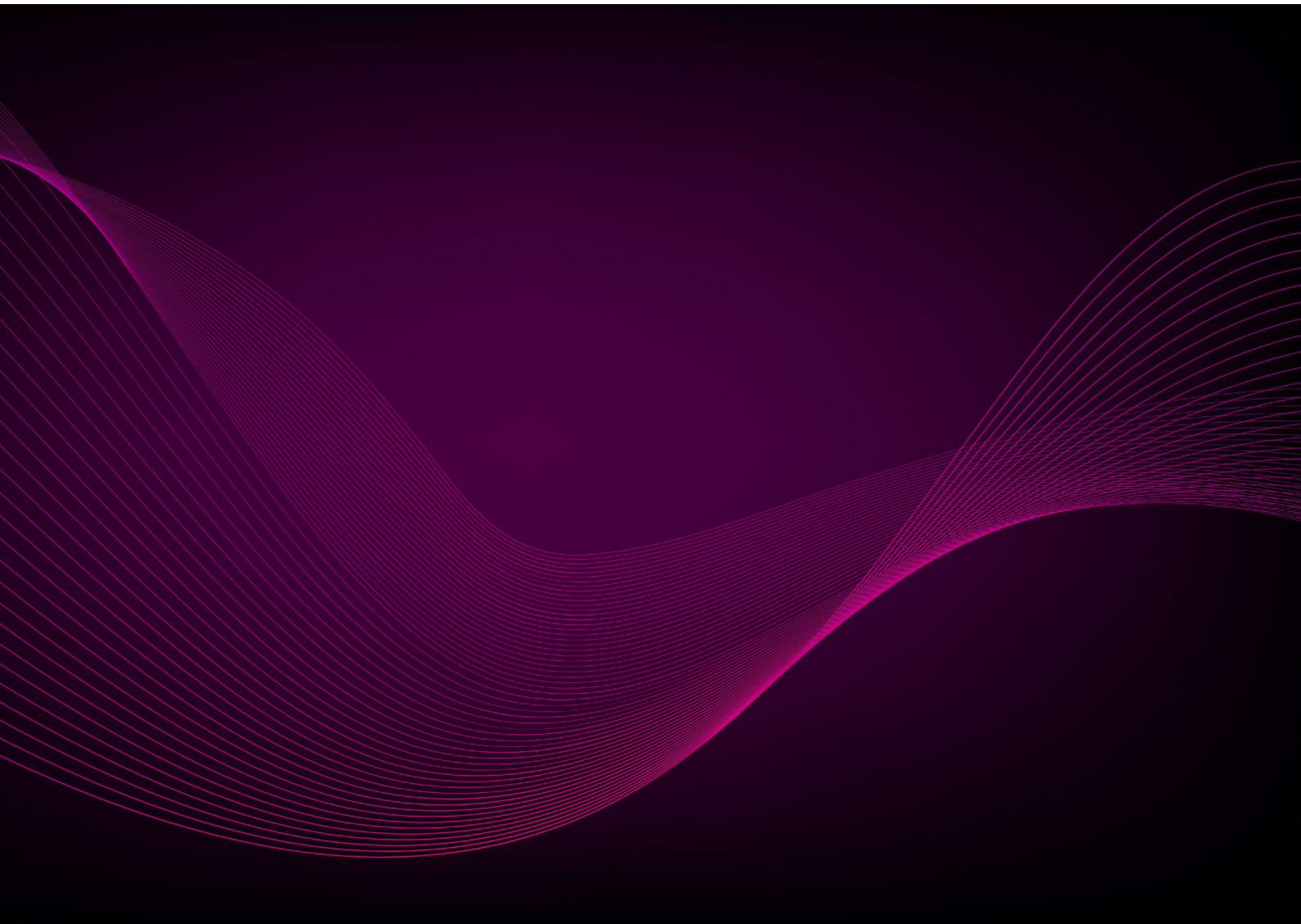
CAPCO | DIGITAL

# MULTI-CLOUD:
## THE WHY, WHAT AND HOW OF PRIVATE-PUBLIC CLOUD SETUPS AND BEST PRACTICE MONITORING



# INTRODUCTION

Banking, as any business, is complex, and there are many choices and decisions to be made – all the time. Underlying many businesses today is expensive technology which adds to the endless decision complexity. When mapping their IT strategy, companies need to evaluate opportunities and challenges presented by cloud technology, and many businesses find themselves with a mixed private and public cloud setup. This whitepaper explores important issues with multi-cloud scenarios, with a focus on the monitoring of multi-cloud solutions.

# WHY DO COMPANIES ARRIVE AT MULTI-CLOUD SCENARIOS?

The uptake of cloud technology by large, high-profile global companies, its popularity within IT departments, its promise of 'almost free' (or at least low cost) and the rise of cloud-based solutions have predictably forced companies to scrutinize and reconsider their traditional legacy systems and setups.

Every significant company must develop a cloud strategy defining if and how they should move their existing setup to the cloud. They will likely start the transformation process implementing a private cloud solution on on-premises infrastructure to achieve a scalable and more manageable system.

However, as business activities expand, it becomes inevitable that the need for more computing resources or external software services grows to the point where the company faces a dilemma – expand the private cloud resources or acquire resources and services from a public cloud provider. Companies must consider compelling arguments linked to the benefits of public cloud use. Once a company starts to utilize a public cloud provider, the result is a hybrid-cloud solution, a combination of private and public cloud services. A complete cut-over to public cloud is rarely possible as some IT infrastructure usually needs to remain on-site or in a private environment.

There are many benefits of using a public cloud, like the flexibility in deploying new environments within minutes or quick reaction to peak workloads, to name just a couple. This results in better employee experience and efficiency. The quicker you can deploy and scale the quicker people can get to projects using cloud. Public cloud providers offer solutions that enable quick business transformation journeys and faster go-to-market requirements.

Computing resources have become a commodity. Businesses are aware of the fact that they cannot differentiate solely based on technological maturity linked to the usage of their infrastructure. Public cloud providers are generating and offering more and more new cloud based and cloud native services that reinforce technological innovations and modernization. Adopting these companies' services brings additional value to businesses.

Public cloud providers have also already addressed many regulatory and legal requirements and continue to do so. This is paving the way for a broader adoption of cloud services – increasingly also in highly regulated industries.

Driven by these very compelling arguments many companies will chose to expand their private cloud infrastructure with public cloud offerings. This results in an ever-increasing number of multi-cloud setups.

# MULTI-CLOUD COMBINES THE BEST OF BOTH WORLDS

The scenario described above results in the use of multi-cloud solutions as there are compelling arguments and regulatory restrictions to retain some of the application landscape in a private cloud infrastructure.

**Private cloud:**

- **Security aspects, regulatory and legal requirements:** Certain systems and data registers may not be placed into a public cloud environment. Possible reasons are constraints regarding geographical placement and the required physical access (e.g. emergency infrastructure, co-location requirements, bandwidth, data restrictions).
- **Financial aspects:** For example, the hardware that is already owned and still not depreciated (and software if it cannot be reused) can be used for running a private cloud design.
- **Services or functionalities:** Some services cannot be provided by a public cloud provider or are uneconomical to adapt for a public cloud scenario (e.g. legacy and custom built applications).

**Public cloud:**

- **Scalability:** Complete flexibility to react to resource needs instantly without requiring oversized hardware for everyday business.
- **Dynamic creation of environments:** Development and test activities benefit from unrestricted and automated creation and destruction of environments on demand.
- **Innovative services:** Bringing in and leveraging innovative, external cloud-based services is easy.
- **Evaluation and proof of concept (POC):** Evaluation of products in cloud setups is very easy and can usually be done without financial commitments outlasting the duration of a POC.

These examples show why a multi-cloud solution is often used, as it is necessary for companies for compliance reasons and they can also get the best of both worlds. However, even though a multi-cloud solution can bring considerable benefits for a company, it also brings inherent risks, specifically with monitoring.

# CURRENT AND TARGET STATE OF MULTI-CLOUD MONITORING: Q&A ON THE MOST IMPORTANT ASPECTS

**How do customers currently manage their multi-cloud environments? What is still left in their legacy infrastructure management landscape?**
On the one hand, public cloud providers offer dedicated monitoring solutions like AWS CloudWatch, Azure Monitor or GCP's operations suite. Monitoring of legacy infrastructure and private cloud domains, on the other hand, is dominated by on-premises hosted products such as Zabbix, Nagios or Dynatrace. Both options are usually combined with third party cloud and local services used for application monitoring. The use of distinct and isolated monitoring solutions however, comes with operational risks and difficulties linked to the management of multi-cloud workloads.

**What are the current challenges with multi-cloud management and their effect on resource usage?**
The challenges related to monitoring multi-cloud solutions include **operational factors** such as:

- The support and operations teams must manage multiple monitoring platforms – this has a direct impact on resource utilization.
- Non-standardized monitoring frameworks result in different monitoring specifics. When used in parallel, the different metrics and threshold levels lead to confusion and loss of control. This can result in non-compliance with Service Level Agreements (SLAs).
- Building a central event management system, an IT Service Management (ITSM), with ticketing or emailing and multiple monitoring solutions linked to it using webhooks creates complex integration overhead.
- The lack of a centralized visualization interface results in an increased need of resources.
- The lack of dependency links between the different monitoring solutions obstructs a holistic view. A raised alarm is followed by complicated and time-consuming processes of incident troubleshooting and problem root-cause identification. It is expensive and prone to missing out important factors that may significantly contribute to the issue's origination.
- The lack of dependency information can lead to wrong decisions by operations engineers because a metric or an alarm cannot be put into the context and thus loses meaning. The consequence is an increased risk of service unavailability with the potential of system-wide crashes.
- Meeting end-to-end business and customer SLAs becomes more challenging as the dependencies between systems monitored by different solutions are not taken into account.

Even though this is just a short non-exhaustive list of challenges, they need to be addressed.

**What should be the target state of multi-cloud monitoring? How does this effectively support customers on their journey (innovation, transformation, digitalization) with a hybrid cloud solution?**

An ideal and solid multi-cloud monitoring system needs to have attributes of high availability and centralization. A quick win might be to choose a Monitoring-as-a-Service (MaaS) solution where a predefined, preconfigured, and scalable monitoring service is hosted in a public cloud. Solutions from all major monitoring providers can be found as instantly deployable services within public cloud providers' marketplace sections.

Another solution consists of creating and managing your own centralized monitoring system installation where either your local infrastructure or private/public cloud hosted infrastructure stack supports performance monitoring of infrastructure and application layers. Additional attributes include a fully customizable visualization interface and flawless compatibility with mobile

platforms as a must. Finally, a wide support of API and webhook connectivity options towards mostly used and popular ITSM tools is an important attribute to facilitate an effective alert/event management.

The decision to choose between MaaS or own installation of monitoring solution should follow the standard cloud service adoption approach and analysis. It should consider factors already mentioned: regulatory requirements, company's infrastructure standards, availability, capacity of internal computing, human resources, willingness to invest and modernize, number of monitored services as well as employee skillset and prior experience linked to legacy monitoring solutions.

**What is a typical approach of implementing a multi-cloud monitoring solution?**

The generic approach of implementing a new multi-cloud monitoring solution should contain the following steps and milestones:

- Identify the pain points and missing information that would protect the business.
- Together with relevant business units determine what needs to be monitored. Outline how they benefit.
- Select a suitable monitoring solution based on requirements.
- Set up an implementation strategy - MaaS or own installation.
- List metrics, key performance indicators (KPIs) to monitor and events to log.
- Develop an incremental implementation strategy based on criticality and value.
- Deploy the solution for a trial run and setup alerts for high priority events and metrics. Establish and test connections to external tools used as part of the ITSM and initiate business reporting.
- Check the functionality and reliability of the new monitoring system in a redundant setup of the 'old' and the newly deployed solution. Confirm that the new solution is reporting events correctly.
- Complete the setup of metrics monitoring and event logging.
- Control the metrics for accuracy and tune thresholds to the desired targets.
- Decommission legacy monitoring systems.

### How to choose the right multi-cloud solution

There are many solutions on the market, and it is difficult to make the right choice. During the selection process, you should consider the following questions:

- What type of monitoring are we seeking?
  The most common types are network and security, infrastructure availability and capacity, application performance and availability, web performance and user interaction monitoring, business performance metrics (e.g., the number of processed documents, transactions, sales results, etc.).

- What is the preferred management technology and required information granularity?

  – Agent monitoring – typically designed for a specific platform and vendor, can collect more detailed information.

  – Agentless monitoring – uses standardized protocols and log analysis. In general, ready-to-deploy solutions are hosted in private/public clouds and usually have great built-in agentless monitoring possibilities.

- How many devices and applications are to be monitored?

- What is the company's licensing strategy? Would it rather invest, rent, or use an open-source solution, potentially contributing own development to implement specific functionalities?

- How likely is the IT landscape to grow and will the scope for monitoring need to be extended? Is the candidate solution flexible enough to support the growth strategy?

### What is the right adoption and implementation strategy?

Regarding the adoption and implementation strategy, it is important to also consider some factors that are in favour of a MaaS solution. Generally, product licensing is already included in the operational costs, so there is no need to procure additional software licenses. Ready to use tools can be deployed instantly and provide flexibility in terms of features testing and creation of POCs.

Additionally, MaaS providers offer support 24/7. SaaS solutions allow more time to focus on business demands rather than worrying about the effort needed for monitoring maintenance and reliability, as well as offering the quick adoption of new services, components, and assets into the monitoring solution.

### How to establish quick wins

By selecting and implementing a suitable multi-cloud monitoring solution, one of the earliest benefits a company can profit from is the possibility to review and manage the system utilization patterns. This allows for optimal resource allocation and manging the running costs effectively. The resulting increased availability of services, greater performance and cost transparency, as well as reduced critical incidents will improve business experience and strengthen relationships between IT operations and business.

If a business runs a correctly and purposefully set-up multi-cloud monitoring solution, it will provide additional and significant benefits to different business areas:

**FinOps:**
Unmanaged utilization and deployment of new services using public providers can become very expensive. Monitoring is necessary to avoid cloud cost leaks.

**SecOps:**
Early alerting and effective response to security threats results in decreased costs linked to security issues. This will improve the security of applications and network layers in the long run.

**CloudOps:**
Simple and effective scaling when needed, either manually or automatically, using resource scaling scripts triggered by events, optimizes service availability and ensures positive end-user experience.

**DevOps:**
Embedding monitoring into the early stages of the DevOps cycle helps DevOps engineers to identify and fix issues at a much earlier stage. That way they can achieve and maintain optimal application performance.

# CONCLUSION

Many companies are running workloads, applications, and systems in a distributed landscape with a combination of public cloud providers, private clouds and legacy on premises infrastructure. Without the right solution, the monitoring of all these environments can become a useless overhead in the best case and a danger to the business in the worst.

Therefore, we regard a multi-cloud monitoring solution as an important infrastructure item in this scenario. Implementing multi-cloud monitoring will require investment, but it is a crucial step towards operating a stable business and achieving lower total costs.

Monitoring systems are 'behind the scenes' technology and are often only thought of when systems fail. Subsequently, getting investment and interest from the business can be challenging.

However, **all business stakeholders need to be involved** in the discussions about monitoring solutions, so that their needs and requirements are understood and considered. That way they can also appreciate the value monitoring brings for them and how it facilitates effective growth and profitability for the overall business.

## HOW CAN CAPCO HELP?

Capco has worked on cloud migration projects and projects introducing the required operating and governance models across the financial sector. We bring the experience and innovative drive to introduce this technology in the current regulatory and control driven environment.

We maintain strong partnerships with industry leading cloud providers (GCP, AWS, Azure) and leverage these for cutting edge solutions and capabilities, delivered by our accredited cloud consultants, architects and engineers. Moreover, we work with our clients to increase their cloud skills and capabilities through integrated training and change delivery.

At Capco, regulatory compliance consulting for financial firms is a key expertise we are known for. We help our clients to navigate the regulatory challenges that come with cloud transformations and to align solutions accordingly.

Getting your organization ready for sustainable platform transformations is at the heart of our proposition. Contact us to find out more about our high impact approach to cloud consulting that delivers everything you need to drive cloud uptake and benefits realization.

## AUTHORS

**Florian Nemling,** Senior Consultant
florian.nemling@capco.com

**Alan Benson,** Managing Principal
alan.benson@capco.com

## CONTACT

**Michael Feiler,** Executive Director
M +49 17 2698 7299
E michael.feiler@capco.com

## ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, Xing, LinkedIn and Instagram.

## WORLDWIDE OFFICES

### APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

### EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

### NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

### SOUTH AMERICA
São Paulo

**WWW.CAPCO.COM**

CAPCO | DIGITAL