CLOUD4C

ENSURING THE ROI FOR INNOVATION AND AGILITY IS ‘CLOUD’ AND CLEAR

CLOUD4C

Table of Contents

CLOUD4C

1. Overview

Today, cloud-based technologies have become the mainstay for businesses across verticals.

Gartner predicts that the global public cloud services market will grow 17.3% in 2019 to total $206.2 billion, up from $175.8 billion in 2018.

Hyperscale cloud services providers like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Alibaba Cloud attract many organizations with their flexible pay-per-use payments, easy scalability, elasticity, higher resiliency, and more. With all these features, the cloud is expected to deliver unmatched value (lower TCO), faster time-to-market, and better service quality compared with traditional IT offerings.

> The 2018 IDG Cloud Computing survey reports that "73% of organizations have at least one application or a portion of their computing infrastructure already in the cloud."

A report from IDC claims that AWS customers are able to achieve significant financial benefits including 94% reduction in unplanned downtimes, 51% lower cost of operations and a payback period of just six months.

It is also safe to say that, though the above stats are impressive, the narrative about the cloud's pervasiveness and its business benefits is not new. Business decision makers understand the cloud and its benefits quite well.

In a recent survey by CloudFoundary, three-fourths of the respondents claimed that they could comfortably explain PaaS to a colleague and around half of them could also explain containers.

Today, more and more organizations are embracing disruption and riding the next wave in technology banking on the cloud which provides them an agile platform for innovation and growth. However, even as organizations keep pace with technology, they can lose sight of the RoI of their cloud initiatives. Optimizing and managing resources in the cloud is today more challenging than it used to be. Cloud providers' race to the bottom is long over and optimizing cloud costs has become a big challenge. The ability to control cloud sprawl and manage cloud-native applications can provide huge operational efficiencies and strategic advantage to organizations. That's why businesses are more concerned about "how to make the most of the cloud." In this regard, hybrid and multi-cloud environments are becoming a preferred option.

The hybrid cloud market, which was worth $49.9 billion in 2018 is also expanding and is projected to be worth $91.74 billion by 2021.

> Every major organization is using around five clouds, and 81% of the enterprises have a multi-cloud strategy.
>
> RightScale

1.1
Why Organizations Choose Hybrid Clouds?

A Hybrid cloud setup uses a mix of private and public clouds. The private cloud could be either on-premise or a VPC (virtual private cloud) hosted elsewhere and may use multiple physical or virtualized servers. Hybrid clouds allow organizations to meet their varied requirements efficiently. Here are some of the reasons organizations prefer hybrid cloud models:

Technical Control

With hybrid IT, organizations can create an infrastructure that suits their specific business needs and have better control over their resources. For instance, they can give root access to select individuals and segment their network logically or physically as per their architecture preference. They can also avoid the multi-tenancy route and provision specific hardware to meet their application performance requirements.

Security and Compliance

Security and compliance are often cited as the main factors by organizations choosing private clouds over hybrid clouds. At the same time, organizations also want to make the most of public clouds. That's why most organizations choose a hybrid setup, putting their less critical workloads on public clouds and restricting mission-critical apps and sensitive data to private ones. This approach allows them to use dedicated servers and network devices that have security features to limit access.

Speed and Scalability

Hybrid setups can also help organizations reduce load times and improve data transfer speeds for their mission-critical applications by positioning their high-demand resources within their private network. Further, hybrid setups allow organizations to meet their cyclical demands or spikes with multi-tenant cloud servers that can be scaled up on demand.

In addition to the above factors, in recent years, there has been a curious trend favoring hybrid-cloud adoption with businesses moving some of their workloads (in some cases up to 50%) back from public to the private clouds.

One of the primary reasons for this shift is that many organizations have burnt their fingers with public cloud and now realize that it does not offer a silver bullet for every problem. Further, they are now able to distinguish which workloads are better suited to which environment.

80% of the IT decision-makers in an IDC survey reported that they migrated some of their applications/data from a public cloud to an on-premise or private cloud solution in 2018.

1.2
What is Driving the Multi-cloud Trend?

As organizations have the freedom to choose between multiple cloud providers based on their location, policies, and governance principles, they often exercise this freedom. For instance, in a typical enterprise, the IT department might choose to run its preferred ERP on virtual servers in its own data centers or a private cloud. On the other hand, it may run other workloads on Windows. At the same time, the sales and marketing department might be using AWS, while some of the teams in development might experiment with OpenStack. Here are some reasons why organizations prefer multi-cloud setups:

Cost and Performance Optimization

In a survey, respondents claimed that cost-optimization was the biggest motivator for

them adopting a multi-cloud strategy. A multi-cloud strategy gives organizations more bargaining power and allows them to cherry-pick specific cloud solutions at a lower cost. Further, a multi-cloud approach will enable them to meet their performance needs as some workloads run better on one cloud platform than they do on others.

Disaster Preparedness

In Feb 2017, AWS' massive outage in the US affected around 150,000 websites. This outage forced organizations to look beyond AWS and made a case for multi-cloud adoption stronger. While today, all cloud providers offer disaster recovery (DR) solutions with redundant copies in geographically dispersed data centers, by utilizing multiple cloud solutions organizations can add another fail-safe. It is unlikely that a DDoS attack or any other disruption would affect multiple cloud providers at the same time.

Latency and Compliance

In certain regions, a particular cloud provider may offer an edge over others with its edge locations (e.g., Alibaba Cloud in China). With multiple cloud providers, organizations can accelerate content delivery and combat latency issues. Moreover, organizations have to choose multiple cloud providers to deal with data localization or data residency laws.

It is understandable that organizations prefer hybrid and multi-cloud setups to meet regulatory compliances, reduce costs, gain higher resiliency and make use of the specific advantages that every cloud services provider offers. As a result, most organizations are starting to increase their reliance on a mix of multi and hybrid cloud strategies. However, hybrid and multi-cloud setups are not without their own set of challenges.

> By 2021, 98% of organizations plan to adopt multi-cloud architectures, but only 41% have a multicloud management strategy and just 38% have procedures and tools to operate a multi-cloud environment.
>
> IBM

In the following sections, we will discuss these challenges and explore some of the ways in which organizations can resolve these challenges.

CLOUD4C

CHALLENGES WITH MULTIPLE CLOUDS

2. Challenges with Multiple Clouds

In many ways, multi-cloud amplifies automation, migration, monitoring, security, and performance challenges that the traditional IT faces in handling their in-house setup or when working with a single cloud provider.

2.1 Multiple Portals

As every cloud provider offers self-service portals, administrators have to constantly shuffle between these portals for provisioning and management of resources. This complexity can also frustrate admins; for instance, different cloud providers have varying password strengths or authentication measures for identity and access management. Many times, to overcome this complexity, admins rely on simple passwords which are shared across the team. Needless, to say this is a big security lapse. Additionally, as the portals allow organizations to monitor workloads only on their infrastructure, it is possible for teams to lose sight of workloads running in private clouds or in-house setup. The fact that legacy monitoring tools do not support multi-cloud environments makes monitoring even more challenging. This can lead to configuration errors or oversights and can also prevent organizations from measuring their true RoI.

2.2 Migration & Application Deployment

Organizations often see commercial viability in migrating their core applications from their data centers to the cloud. However, the lift and shift approach doesn't always work. When shifting complex workloads out of their corporate data centers to a public cloud, very few organizations take the pain to re-architect their apps so that they could fully leverage the public cloud. Many times, organizations have to make substantial investments in redesigning to avoid performance and latency issues.

Over a period, an organization may find workarounds and solve these issues. However, difficulties can arise again when they try to scale or redeploy these apps to a different cloud platform. While orchestration tools and modern application deployment approaches can resolve these interoperability challenges, organizations often lack the expertise to undertake such initiatives.

2.3
Skills Crunch

To make the most of the multi-cloud strategy, organizations need to reduce their migration costs. This is possible only if they have the requisite skill-sets and readiness for containers that in theory can make applications more portable. They also need policies and tools that increase reliance on cloud neutral IaaS APIs and restrict usage of proprietary cloud APIs to access cloud services. However, most organizations do not have mature processes and IT skill-sets to take up such initiatives.

Cloud architects, engineers, developers, and DevOps professionals are in short supply. The problem becomes more acute when an organization has to manage multiple clouds. As organizations increase usage of IaaS, PaaS, and SaaS solutions, their requirement of technical skills and the vendor management burden also increases in the same proportion. At times, they have to wait for months before they get a staff with the right skill-set.

In a recent survey by OpsRamp, 94% of respondents from IT departments with 500 employees or more admitted that it is getting difficult to find the candidates with the right skills and experience for managing their cloud environments.

2.4
Security and Governance

In a multi-cloud environment, admins have to double check every critical service configuration and have to remain on toes to fix vulnerabilities in web application components. However, many organizations often lack visibility into where their data resides. Teams can quickly lose sight of their application components running across multiple clouds, some of which may be running in an unapproved environment. In highly regulated industries, this can also lead to severe penalties.

Organizations often also fail to monitor cloud services and SaaS applications that their employees use at their whim. Application layer threats and vulnerabilities pose a big challenge to enterprise security. They can also allow threat actors to initiate an attack from inside a corporate network. In certain cases, hackers can target misconfigured and unsecured cloud servers of an organization to mine cryptocurrency.

2.5
Cost Optimization

In multi-cloud environments monitoring applications is not simple and organizations can easily overprovision their resources. Moreover, it is not uncommon for developers to leave instances running when they aren't required. Also, as cloud platforms offer volume pricing organizations often end up paying a higher per-unit price for cloud infrastructure by spreading their workloads across multiple platforms. Organizations also fail to make the most of the spot pricing. Moreover, at times IT staff favors select cloud platforms for certain workloads, which end up becoming a default across the board. This approach can prove to be costly in the long run as organizations can save a lot by carefully distributing their workloads across different clouds. However, RoI optimization in a multi-cloud environment is a complex exercise, and very few organizations are able to do it right.

As highlighted by the RightScale survey report, security and cost optimization seem to be the most pressing challenges for organizations struggling with multi-cloud management.

There are multiple open source and commercial tools (e.g., Fog, CloudCheckr, Tangoe, Cloudability, etc.) available in the market which can help organizations solve their cost optimization challenges. However, their implementation is still low due to a range of reasons. For instance, certain open source tools have powerful capabilities but can cause information overload. Configuring and making these tools user-friendly to work with reduced noise is not easy.

As per RightScale 2018 State of the Cloud Report, Security is a challenge for 77 percent of respondents, with 29 percent seeing it as a significant challenge. Managing cloud spend is a challenge for 76 percent of respondents, while a smaller 21 percent see it as a significant challenge.

Some other commercial tools can help organizations in enforcing operational policy but have a cumbersome workflow. In fact, when it comes to security, many of the traditional on-premise monitoring and analytics tools are still in the process of capturing insights from the cloud and offer a varying degree of integration with cloud-based technologies. There is still some time before all these tools can unify every aspect of infrastructure, application, and cloud management and monitoring and start offering actionable intelligence with a higher degree of automation.

CLOUD4C

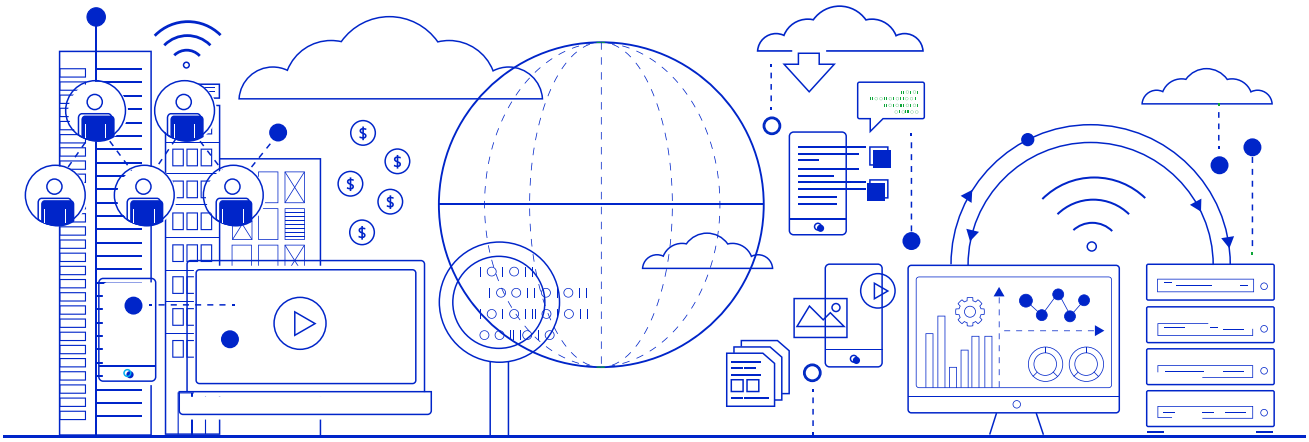
BEST PRACTICES

3. Best Practices for Managing Multiple Clouds

It is possible to solve multi-cloud management challenges with the right approach, using the right tools; there is an entire range of multi-cloud management platforms that help in provisioning and monitoring of services over a single pane of glass. However, these tools can further add a layer of complexity and many organizations have never used such tools. Further, organizations also lack a holistic strategy to implement multi-cloud. There is a need to improve the understanding of cloud technologies, overcome biases, and make informed decisions. We will discuss how organizations can follow the best practices in multi-cloud management to make the most of the opportunity.

3.1 Focus on Vendor Management

Organizations need to improve processes for managing multiple cloud vendors and negotiate on costs. To make the most of the multi-cloud opportunity, they need to assess their readiness for new technologies and understand the requirements for all the services. This groundwork will help them evaluate the pros and cons of multi-cloud architecture before they engage in any negotiations. However, not all decisions could be based purely on cost and organizations also need to take into account several performance and compliance issues into these negotiations. Once the negotiations are over, the organization should be able to make use of the multi-cloud environment as per their initial calculations. This requires strong governance to ensure teams access the right cloud service for the right purpose.



3.2
Update Security and Governance Policies

> Cloud computing ranks as the top risk concern for executives in risk, audit, finance, and compliance...at least 95 percent of cloud security failures will be the fault of the organization.
>
> Gartner

Security threats continue to grow in terms of sophistication, frequency, and impact. The threat exposure is only likely to grow with multi-cloud complexity. Therefore, it is vital for organizations to review and update their security and governance policies. In a multi-cloud environment, these policies become even more crucial. Multi-cloud environments increase the burden on IT teams responsible for security and governance. They need to adopt smarter tools and practices to reduce false positives in their complex distributed stack.

Organizations also need to realize that, though advanced security threats and zero-day vulnerabilities pose considerable risk, it is not always the most sophisticated attacks that cause major damage. Instead, social engineering attacks such as phishing and tailgating pose a more immediate threat. Further, most of the times organizations fail to put in place basic fail-safes like multi-factor authentication. Organizations should first try to fix such lingering issues and perform routine audits to improve their security posture.

As public cloud providers work in a shared responsibility model, organizations should ensure that every stakeholder and team member is aware of different security requirements. They should understand what part of their environment is covered by whom. Managing key controls (identity and access management) and security processes is critical for reducing potential risk.

3.3
Select the Right Cloud for Every Workload

Not all workloads perform equally well across all clouds. This means, in a multi-cloud environment, it is crucial for organizations to rely on data-based decisions and distribute workloads to different clouds taking into account their performance and costs. To make optimal use of cloud resources, they need to monitor their workloads and its environment in real-time. Additionally, tools like Live Optics can help organizations choose the correct deployment model (public/private/hybrid) for every workload.

Organizations also need to evaluate which types of apps are best suited for the cloud. They may consider prioritizing usage of multi-cloud for cloud-native applications which can harness the true potential of cloud with their modular, service-oriented architecture. On the other hand, they may consider VMware's vSphere-based Enterprise Hybrid Cloud for hosting their traditional monolithic apps. AWS also offers different kinds of solutions for different enterprise needs.

3.4
Make Multi-cloud API Management a Top Priority

Cloud provider offers APIs for different services. These APIs vary a lot as one moves from one cloud to another. For instance, the number of APIs needed to perform the same task, their performance, and latency differs. Cloud providers also have different limits on the number of API calls during a period. All this means that as an organization moves its application from one cloud to another, it may have to recalibrate it to suit the new environment.

Moreover, different cloud providers do not follow a single policy for API security and authorization. This means organizations have to get used to different frequency and types of API error messages. Keeping track of their updates is also crucial. Managing and integrating these APIs is crucial for seamless multi-cloud operations. Also, DevOps teams should analyze the differences between these APIs and how these difference would affect them in a multi-cloud environment.

3.5
Make Application Migration Seamless

Every application hosted on the cloud has several dependencies. Developers would never like to disturb a working application and shift it to another cloud and risk entering a dependency hell. However, migrating an application from one cloud to another can be unavoidable in certain cases. To ensure that all such migrations are seamless and less costly, developers should make sure that they have accounted for all IP addresses and service dependencies in advance. Further, using automation tools and abstraction techniques, such as the Adapter Design Pattern, can help organizations reduce their application migration worries and the costs associated with it.

3.6
Optimize VM Usage and Costs

It is a common knowledge that cloud providers charge more for their reserved instances than for on-demand instances. The size of a VM is another cost factor. Yet, organizations often fail to optimize the costs by choosing right-sized VMs. Developers often define and propagate a default configuration across the board. Organizations should ensure that this doesn't happen and every application is utilizing the right amount of OS and middleware components.

With Compute Engine, organizations can also explore preemptible VMs that come at heavily discounted prices. The catch is that these instances terminate after 24 hours. Google can also shut down the instances at any point it needs additional capacity for other workloads. However, many organizations use these instances for testing, quick batch jobs, and other fault-tolerant applications. With preemptible VM, organizations can up to 80% over standard GCE instances.

3.7
Evaluate Uptime Requirements

While every business wants to ensure high availability (HA), even the best of cloud providers have several hours of unscheduled downtime in a year. Organizations can ensure HA with active-active configuration, but it comes at a high cost, and many SMBs are often unprepared for these costs. Therefore organizations should carefully evaluate their uptime requirements, analyzing the service costs and comparing it with potential loss during downtimes. They need to answer if it would be more cost-effective to use multi-cloud for HA or can they rely on traditional manual redundancy processes.

3.8
Keep Tabs on Networking Fees

While all leading cloud providers offer free data ingress, data egress can cost a lot, especially if organizations have to move data between international locations. That's why tracking these data transfer costs in a multi-cloud environment is crucial. Enterprises often rely on chargeback and showback tools to monitor these costs and ensure every department is using cloud resources prudentially. Some hybrid cloud solutions can allow organizations to further reduce such costs by caching their active file data on-premises. This approach also makes access to the files quicker.

It is important to mention that many organizations have attempted a multi-cloud strategy that also encompasses their hybrid clouds. Logically, this integration could unify all types of resources, whether it is public or private cloud or their on-premise infrastructure. With this approach, organizations can better address their data residency and compliance issues with higher control. However, management of such a diverse environment is challenging and organizations should look forward to managed services providers for expertise and guidance.

On the other hand, in highly regulated industries, organizations should explore the community cloud service model. Community clouds help organizations leverage a highly secure and compliant hybrid environment that is built and managed on their behalf by the managed services provider.

CLOUD4C

MSP ROUTE

4. Explore the MSP Route

It is true that multi-cloud has become a de-facto strategy for higher performance, efficiency, and growth. However, multi-cloud is not a simple choice; in many cases IT teams and CIOs have it thrust upon them. As discussed, CIOs need to expand their IT capabilities and hire new employees with advanced skills to make the most of multi-cloud. They need to implement new policies and tools to manage complexity in their vast environment. Further, keeping tabs on different costs is not simple. All this complexity can make multi-cloud operations highly challenging. At times, organizations may have to spend more time fine-tuning their setup than focus on their real work.

In the absence of requisite know-how, organizations can make their technology stack more complex than it needs to be. They are also at risk of entering an endless counter-productive cycle of re-architecting and migrating applications and workloads. Therefore, it is crucial to identify gaps and assess readiness for multi-cloud adoption.

This is where a managed services provider can offer guidance and expertise in helping organizations look beyond the hype.

Mid-market enterprises looking for higher speed, efficiency, and automation are driving the demand for cloud managed services.

A managed services provider can help CIOs identify and plan several complexities, making sure that they have the right processes in place to manage a multi-cloud environment. They can help in managing the resources and controlling the costs. Moreover, managed service providers have to frequently deal with compliance requirements and are well versed with best practices, processes, and paperwork.

Globally, the market for cloud managed services is projected to reach $86.4 billion by the end of 2022, with strong growth (8.10% CAGR) in North America.

With their support, organizations can focus more on other critical areas, leverage the latest in technology, implement best practices and achieve a higher degree of automation. This can enable them to not only adopt the multi-cloud but also stay agile and explore new revenue opportunities with innovation.

CLOUD4C

5. About Cloud4C

Cloud4C is one of the leading global cloud and managed services providers offering multi-cloud management solutions and IT services on cloud platforms like Microsoft Azure, AWS, and Google Cloud. Our service portfolio comprises of private, public, and hybrid cloud, managed services, infrastructure as a service (IaaS), Security as a Service, DR as a service (DRAAS), and vertical-specific community clouds.

Cloud4C currently has 18 Centers of Excellence (CoEs) equipped with 1500+ skilled and certified experts who are addressing the needs of the enterprises by deploying cloud infrastructure that is compliant with country-specific privacy and data residency guidelines.

The company partners with large enterprises and global Independent Software Vendors in delivering applications to its end customers on its flagship community cloud platform. The cloud infrastructure is built on a robust architecture with high availability, disaster recovery and backup to provide zero data loss combined with near zero downtime. The company also specializes in multi-cloud platforms and collaborates with other global cloud providers to provide seamless client experience to its customers.

CLOUD4C

www.cloud4c.com

Let's Connect