The top three public cloud pitfalls

And how to avoid—or fix—them with a hybrid, managed cloud services approach

Introduction

The public cloud offers tantalizing benefits for organizations with digital transformation projects. With on-demand resources and self-service tools, it's among the most efficient options. To get customers in the virtual door, more resources and tools are being released, bundled, and often offered with attractive incentives.

Without proper planning, insight, and skills, however, these public cloud benefits are not always in reach.

Many companies run into unanticipated problems as they move their workloads to the public cloud and expand their cloud usage over time. Performance issues can stall a cloud transition, security and compliance issues can lurk quietly in the background, and cost issues can quickly escalate. Due in large part to these challenges, one out of every three enterprises has repatriated at least a portion of its applications or data from public clouds in the past year .[1]

Fortunately, repatriation isn't always necessary.

With a hybrid approach that combines public cloud resources with experienced, managed cloud services, companies can avoid or extricate themselves from the following pitfalls.

Pitfall #1: Performance issues

Taking a "lift and shift" approach is one of the biggest and most common missteps companies make as they transition to the public cloud, leading to a variety of performance problems.

Because of the inherent differences between on-premises and public cloud environments, attempting to mirror the two isn't practical. When workloads are simply pushed to a public cloud, existing problems typically persist and new problems often crop up.

Almost any application can perform well in the public cloud, but it requires careful evaluation, configuration, rightsizing, and capacity planning. It also demands a deep understanding of the underlying cloud environment.

[1] 451 Research, Voice of the Enterprise: Cloud Transformation—Organizational Dynamics 2017

In many ways it's a matching game, determining the right cloud resources for each and every workload. With an overwhelming amount of options, models, and tools, which vary by cloud provider, these determinations take time, analyses, and expertise.

The first step is understanding the requirements and dependencies of each application. Is the traffic steady or bursty? Because averages won't suffice, how high are the peak loads and when do they occur? How does the application interact with clients? How does it share data? How is it accessed? Does it have compliance requirements? Answers to these questions will lead to a more targeted evaluation of public cloud resources.

An application with high I/O throughput that has been running on spinning disks, for example, may not perform as smoothly in a public cloud environment that utilizes a different type of disk. An application that uses legacy protocols may not perform well over a public cloud's wide area network (WAN). Additionally, applications with very large files or local data transfers may need additional resources, like a caching appliance, to perform as expected in the public cloud.

Simply put, public cloud environments are different than on-premises and colocation environments, and they need to be configured and managed in a different way. Avoiding performance problems requires upfront planning and analysis, careful decision making and configuration, and ongoing management and optimization—on a workload-by-workload basis.

Pitfall #2: Security issues

While performance problems are generally noticeable and commonly appear after an application has been moved to the public cloud or after a change has been made, security and compliance problems can arise at any time and often linger silently. Many of them are accidental and unseen—until it's too late—due to a lack of understanding about the roles and responsibilities of the cloud provider and customer in protecting applications and data.

Security spans three key vectors: platform, applications, and users. While public cloud providers deliver security and compliance for the underlying platform, it is the customer's responsibility to secure the application, its traffic, and its accessibility. Therefore, placing an application in a secure, compliant public cloud doesn't mean the application itself is secure or compliant.

13 Biggest Challenges When Moving

Your Business to The Cloud

Before they can reap the benefits of cloud technology, companies will first have to move there successfully. This process is often fraught with a variety of challenges, from insufficient planning to obsolete technology and more.
Members of the Forbes Technology Council recently outlined the biggest hurdles a business might have to overcome when moving to the cloud:

1. Getting it right
2. People and processes
3. Having a defined strategy and business objectives
4. Getting over the psychological barriers
5. Time, cost, and security
6. Not getting caught up in the hype
7. Change management
8. Dependable technology infrastructure
9. Accurately estimating the costs
10. Modifying the architecture of cloud services
11. Translating security posture to the cloud environment
12. Determining whether to lease or own
13. Connecting legacy systems with cloud applications

Forbes Article - 13 Biggest Challenges When Moving Your Business To The Cloud

concerto
cloud services

Companies must have people, processes, and rules in place to protect their applications and data, with a distinct focus on administrative practices, user behavior, and access control. It is far too easy to misconfigure an application or the underlying public cloud resources—particularly external gateways and firewalls—in ways that accidentally create unwanted access points, compliance gaps, or other security vulnerabilities. While most companies are concerned with attacks and breaches from the outside, the vast majority of security and compliance problems are caused internally, many of them the result of human error.

Securing applications and data in the public cloud is a multidimensional activity. It requires platform configuration, software tools, processes and controls, and workforce training—all of which are outside the purview of most public cloud services. Additionally, each workload will need to be evaluated and secured based on the criticality of the application, the value of the data it contains, its compliance parameters, and user accessibility requirements. Once applications are secured in the public cloud, they will need to be actively monitored. Because security vulnerabilities and compliance gaps are easily and often accidentally created, specialists will need to regularly review logs and traffic for suspicious activity.

Pitfall #3: Cost issues

One of the public cloud's most alluring benefits is also its greatest conundrum: Cost. While cost reductions are the primary driver for public cloud migrations, a survey from IDG Enterprise revealed many companies are struggling to keep their public cloud expenses under control .[2] There are a number of reasons for steep, escalating, or unexpected costs.

Many services—such as disaster recovery, two-factor authentication, intrusion detection, and encryption for data at rest—are typically not included in standard pricing. Replicating data in different regions and moving data out of the public cloud can result in unanticipated fees. Costs associated with e-commerce and database workloads can rapidly increase along with user, transaction, and data volumes. The bandwidth requirements of content delivery applications—especially those that feature video—can be exceedingly expensive. What is economical in the beginning can quickly snowball as public cloud usage and data volumes grow. Plus, most organizations don't take advantage of the cost reduction opportunities at their disposal.

Many companies overprovision their cloud resources, purchasing excess capacity that goes unused. Some are not aware of cost saving options—such as spot or reserved instances—that require longer commitments but can lower the monthly bill by 30 to 40 percent. And others don't leverage the elasticity of the public cloud, purchasing full capacity for sporadic or bursty workloads.

Attaining and maintaining a grip on public cloud costs comes down to visibility, strategy, and diligence. Companies need in-depth capacity planning and they need to architect their cloud environment on a workload-by-workload basis, balancing price, performance, security, and resiliency. Because public cloud pricing models frequently change, companies need to closely monitor their cloud usage and costs over time and make adjustments when needed.

[2] *CIO Article - Why Controlling Public Cloud Costs is so Difficult and What to do About it*

CIO: The three main reasons public cloud costs escalate

With public cloud initiatives moving beyond early-stage, it's time for companies to get serious about optimizing and controlling their use of cloud resources and, in so doing, cutting unnecessary public cloud costs. To do this, they must leverage services and tools that can provide hard data about their cloud deployments, and help them navigate through the jungle of public cloud service and pricing options.

1. DevOps-led cloud deployments

Most of the early generations of public cloud initiatives have been led by DevOps teams whose main objectives have been speed of development and quality of solution, not cost control. In the classic three-way tradeoff of products, you can achieve two of three objectives—speed, quality, and low-cost—but not all three. All too often, low cost has been the odd-man out. With a "better-safe-than-sorry" attitude, many DevOps teams have purchased more cloud capacity and functionality than their solutions required.

2. Complexity of public cloud offerings

As public cloud platforms such Microsoft Azure and Amazon Web Services (AWS) have matured, their portfolios of service options have grown dramatically. For instance, AWS lists nearly 150 "products" grouped under 20 different categories (e.g. compute, storage, database, developer tools, analytics, artificial intelligence, etc.). That portfolio makes for well over 1 million different potential service configurations.

3. Lack of analysis tools and operational visibility

In yet another affirmation of the truism that "you can't improve what you can't measure," companies have found they don't have good visibility into how much infrastructure their cloud apps actually need to deliver the required functionality and service levels. Without services or tools that provide such analysis, companies can't hope to choose the best options, right-size existing public cloud deployments, or to remove "deadwood" cloud apps that never got removed as DevOps teams have moved on to build new cloud solutions.

Three public cloud offers to help you launch your digital transformation

1. **Receive the first 90 days of Microsoft Azure for free!**
   New workloads qualify for up to $15,000 in free services from Concerto, and large projects can qualify for even more.

2. **Get three more years of Windows Server or SQL 2008 security!**
   Migrate your Windows Server or SQL 2008 workloads to Microsoft Azure and you'll receive critical security updates for three years after end of life.

3. **Reduce AWS or Azure overspend by 20% or more, or our services are free!**
   Overspending on current AWS or Azure environments? Put the risk on us. If we don't reduce your spend by 20% or more, our services are free.

Learn more about these Azure Promotions here, or contact us at 813.327.7408 or info@concertocloud.com to schedule a personalized consultation with our Cloud Advisory Team.

About Concerto Cloud:

Concerto Cloud Services provides fully managed private, public and hybrid cloud solutions. A cloud pioneer, Concerto was built on a rich legacy of application expertise, innovation and a relentless pursuit of service excellence. Concerto is a trusted advisor to customers and partners seeking to make IT easier, manage risk and reduce operational challenges.

A Hybrid, Managed Approach

Microsoft Azure and AWS offer world-class public cloud platforms, toolsets, and resources, but they require a great deal of time, effort, and expertise to get the most out of them and to avoid the aforementioned pitfalls.

Concerto Cloud Services helps companies do just that. Our fully managed private, public, and hybrid cloud solutions are built on a rich legacy of application expertise, innovation, and service excellence. Compared to a do-it-yourself, trial-and-error approach, we can optimize your cloud resources and expenses upfront and then manage them over time to make your IT operations easier, more efficient, more secure, and more cost effective.

- Deployment and migration services designed to speed the success of Microsoft Azure and AWS environments
- Ongoing management focused on controlling costs, boosting performance, and increasing security
- Integration with Concerto private cloud and on-premises solutions
- Tier 1 Cloud Solution Provider for Microsoft Azure and Office 365
- Azure Expert Managed Services Provider

concerto
cloud services