TGIX

4 Pitfalls of an Undermanaged AWS Environment

How to avoid the most common expense, management, and security risks in AWS cloud

An In-the-Trenches Viewpoint

Table of Contents

4 Pitfalls of an Undermanaged AWS Environment

4 Pitfalls of an Undermanaged AWS Environment

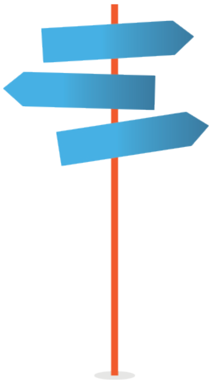
How to avoid the most common expense, management, and security risks in AWS cloud

Cloud computing offers significant advantages, amongst which are elastic scalability, agility, and a pay-as-you-go model. As cloud adoption rates pick up and cloud footprints increase for organizations, there are a set of unique but predictable issues that start emerging, which if left unchecked can lead to increased expenses, management headaches, and security risks down the road. It's not uncommon for a sense of disillusionment to creep in as you struggle to manage your environment and control costs, especially while hearing stories of other businesses that are striking big wins in the cloud. In reality these stories are about a small subset of organizations that plan their growth and run a tight, managed environment with the help of a trained team of cloud professionals; however, a majority of organizations choose to strike out on their own initially and run into issues with spiraling expenses, chaotic manual management, and even security risks.

Over the years, we have seen numerous companies taking a quick, self-managed path to the cloud, making the same mistakes and running into the same set of issues. At the end of the day, the very benefits of cloud computing, if not properly managed, can lead an environment to quickly become chaotic, insecure and costly. So, what exactly are these pitfalls? Here are the 4 critical ones that we have spotted from our engagements with a variety of clients that initially built and managed their own AWS infrastructure prior to engaging us as their AWS partner:

Pitfall 1:

Getting Stuck with Uninformed, Sub-Optimal Architecture Choices



AWS continues to release new services at a breakneck speed. This fast pace of innovation results in a large number of what can seem like duplicative, and sometimes confusing, architecture choices. Where is something replaced vs. optional? What services are contraindicated? How do you know which to choose? Businesses without deep and constantly updated cloud expertise on hand, and with limited planning and pressing deadlines, can end up making technology decisions that are less than optimal. The resulting environment becomes needlessly complex, doesn't effectively use new services and features, and fails to meet all the business goals and expectations. In such cases, security, availability, and scalability are all compromised. Businesses that don't adapt quickly get sucked deeper into the rabbit hole.

In the case of one particular client, a growing healthtech organization, the in-house engineering team implemented an older strategy for their multi-account VPC architecture, which led to issues that significantly impacted their DR capabilities. Testing the DR failover and failback functions became a needlessly complex, time-consuming, and costly chore, jeopardizing their HITRUST regulatory compliance certification. Tgix's cloud engineers helped rearchitect the network infrastructure with reusable scripted CloudFormation templates, ensuring a standard and consistent VPC design as per AWS's current best practices – and furthermore automated their DR testing to ensure that ongoing compliance requirements were met and maintained.

Pitfall 2:

Missing Out on Cost Savings Opportunities

AWS, like most other cloud vendors, offers a number of opportunities for cost savings to its customers. From Cost Savings Plans and Reserved Instances to using Autoscaling technologies, there are many tools in this proverbial bag of tricks that can create significant cost optimizations when implemented correctly. Additionally, there are companies such as NetApp (with their Spot tool suite) that specialize in providing continuous optimization for all cloud operations. Indeed, operating in the cloud without a plan and paying "on-demand" rates to AWS for resources consumed all but ensures that you'll overpay. Environment sizing and budgeting, along with cost optimization strategies, need to be determined for each workload at the onset, and businesses that fail to do so will continue to be frustrated by budgets out of control until they can intelligently manage their costs.

A not-for-profit organization that we work with in New York City figured that they had mastered this problem through a judicious use of Reserved Instances. When costs started spiraling up in their non-production environments (where Reserved Instances were not an effective strategy), they appeared to have exhausted their options and turned to us. Through our proprietary offering that automatically controls uptime for key resources, we were able to quickly reduce the EC2 and RDS spend by more than 75% across the environment.

Pitfall 3:

Failure to Control the Environment Sprawl

Most organizations take a phased approach with their cloud adoption strategy, incrementally moving different workloads or environments into the cloud. Unless this process is closely managed and controlled through standardization, automation, and configuration management tools, it can quickly lead to disparate hybrid environments, where everything from access control mechanisms to application stack versions are out of sync. Furthermore, ownership of resources

and responsibilities start becoming fuzzy across the environments. The end result is a chaotic infrastructure that is difficult to manage, costly to maintain, and eventually requires a forklift to upgrade.

A client of ours in the publishing industry had a multitude of web media properties under their corporate umbrella, running on a variety of different platforms. The original cloud migration was supposed to consolidate the workloads and standardize under a unified platform strategy. Due to a lack of planning and proper management, the infrastructure eventually spread across multiple isolated AWS accounts with different owners and policies, leading to inconsistencies across the different environments and high levels of frustration. Several new initiatives were delayed until core production environments went through a complete re-architecture and upgrade process (which we managed and led), a side benefit of which was the accurate tagging of all resources and deprecation of many unused / unclaimed instances, saving substantial direct (no longer paying for extraneous instances) and indirect (management and constant questions over inconsistent resources) costs as well as reducing overall complexity and security risks.

Pitfall 4:

Lack of Production Systems Discipline

The DevOps paradigm presents tremendous advantages in terms of speed, efficiency, automation, and accuracy, but there are significant downsides too if the right controls are not put into place. The benefits come from rigorous systems development and controls; if development teams have unfettered access to company-wide data and resources then the environment can quickly turn into an insecure and unmanageable mess. Environments that don’t enforce a “production systems mindset” often use the latest development tools and technologies but unfortunately fail with critical product systems controls and functions such as logging, monitoring, or backups. AWS provides a plethora of technologies, but without the right team and discipline to configure the tools and manage the environment the technologies themselves won’t protect you.

A SaaS firm had their security compromised and engaged us to review their environment and operations. Our investigations uncovered the precise issues mentioned above. Every one of their development staff had root or admin access to the cloud platform and production systems, leading (unsurprisingly!) to passwords being compromised. This can happen even if the individuals involved are not deliberately being bad actors — which is why appropriate controls and governance are critical. We were able to help this organization contain the breach and restructure their environment to support both growth and security.

Key Indicators You Might Need More DevOps Expertise

- Do you have an uncontrolled AWS environment with multiple accounts, mysterious instances with no owners, and unpredictable costs?
- Are your costs spiraling out of control despite your accurate forecasting and diligence in right-sizing the environment?
- Does it take an inordinate amount of time to initiate customized instances every time you need to scale, test, or deploy?
- Do you wonder if there are better ways to optimize, secure and manage your environment?

4 Critical Areas for Optimal Management

1. Make the right architecture and tooling choices to effectively use new services and features, reduce complexity, and meet business goals and expectations whilst maintaining availability, and scalability.
2. Implement continuous optimization across all your cloud operations to minimize costs without adversely impacting performance.
3. Grow thoughtfully and strategically to mitigate environment sprawl that can create a chaotic infrastructure that is difficult to manage, costly to maintain, and eventually requires a forklift to upgrade.
4. Implement a Product Systems Mindset with rigorous systems development and controls to minimize management overhead and, more importantly, maintain security.

Overcoming these pitfalls is essentially an exercise in creating an overall better architected and managed environment. Once you recognize that a problem exists, it is not difficult to remediate as our clients have found out.

TGIX

Tgix is a certified Advanced Consulting Partner with AWS and has work with many organizations on their regulatory compliance issues, secure cloud architectures, and providing ongoing managed support.

Contact us for a complimentary evaluation of your current network and security architecture in AWS.

W: tgix.com
P: 212-918-5000
E: info@tgix.com