Brought to you by: CIO FROM IDG

THE 'GOTCHAS' OF MULTI-CLOUD MANAGEMENT

Unforeseen challenges can blunt cloud benefits

"MANY ORGANIZATIONS FAIL TO UNDERSTAND THE SPECIALIZED SKILLS AND EXPERIENCE NECESSARY TO ADDRESS THE DATA/SYSTEMS INTEGRATION, APPLICATION PERFORMANCE MANAGEMENT AND VENDOR MANAGEMENT CHALLENGES ASSOCIATED WITH A MULTI-CLOUD DEPLOYMENT STRATEGY."

JEFF KAPLAN::MANAGING DIRECTOR THINKSTRATEGIES, INC.

Managing multi-cloud environments is challenging enough. Some of the obstacles are well known—silos, security, and the need for a unified view among them. There's another dimension, however: the challenges that you cannot anticipate, or that are not widespread, but still can hold back cloud potential. We asked cloud industry leaders to reveal the most common, yet unforeseen multi-cloud management challenges.

From time to time, IT needs a sanity check to remind us that technology isn't the goal—business outcomes are the prizes to pursue. Taking that step back to think about overall strategy can pay dividends when managing a multi-cloud environment.

"The challenge in taking a multi-cloud strategy from paper into practice is that success requires the company [to] have a strategic IT vision," says Diana Nolting, product analyst at Bluelock. "This vision should balance the right menu of options for workloads while maintaining security, compliance, connectivity, and visibility into the entire environment."

Strategy takes planning, another hidden challenge for multi-cloud management, especially when trying to avoid overspending and over provisioning. "It is critical to truly embrace the advantages of cloud scalability and to only use what is truly needed," according to Michael Sheehan, senior manager of content marketing at Riverbed Technology. "This requires careful forecasting and planning to ensure that infrastructure isn't 'over purchased' just in case."

IT's long-standing quest to reduce complexity can be foiled by a cloud initiative. "It's important to have a partner you trust to work with any planning, implementation, and management of multi-cloud environments as these can be extremely complex," says Sheehan.

INTO THE WEEDS

Some of the "unforeseen" challenges are hidden in the weeds, which our experts address. Let's get into the weeds:

- "Effectively distributing, rotating, and de-provisioning secrets such as SSH keys, service account passwords, and application passwords that are used in DevOps environments is one of the more challenging, yet obscure issues that companies face in multi-cloud environments," points out Kayne McGladrey, director of information security services at Integral Partners.
- "Connecting together two public cloud provider networks is straightforward," says Eric Leach, VP, product management, at Apcera. "What's really hard is getting your on-prem network securely connected (usually with VPNs) to a public cloud. Automating and operationalizing this is probably the biggest challenge."
- "Billing and accounting can be a real hassle depending on the organization and how [it manages] vendor contracts," says Will Kelly, technical writer. "Accounting also has to work through variables in billing, so expect some pushback from your friends in accounting."

- David Geer, technology content consultant, points out that "there is a lack of standardization from one cloud provider to the next, with different providers using various products and their unique proprietary solutions. This creates complexities in managing two or more cloud deployments."

DON'T OVERLOOK DATA AND SKILLS

Tim Crawford, CIO strategic advisor at AVOA, makes the case. "Two key issues are common: Split skillsets, which lead to architectural issues. The second is split data, which leads to increased integration challenges."

Data gets "split" thanks to the need to move it around among cloud and on-prem environments. "I believe that migration is one of the main challenges," says cloud computing expert Rick Blaisdell. "Moving your applications from a public, private, or hybrid cloud to a multi-cloud environment must be carefully planned to ensure that your results meet your expectations."

Riverbed's Sheehan elaborates: "Of top concern is the cross-communication between clouds. That is to say, how VMs [virtual machines] attach to LANs and WANs as well as the networking between clouds to ensure a secure communication. To that end, security of cloud environments must be a top concern as well to ensure fast and secure communications between clouds as well as corporate networks and data centers."

Skills can also be a hidden challenge. "Many organizations fail to understand the specialized skills and experience necessary to address the data/systems integration, application performance management, and vendor management challenges associated with a multi-cloud deployment strategy," says Jeff Kaplan, managing director of THINKstrategies Inc.

The skills question has an interesting twist: It's not just technical expertise that can be a challenge; it's the skill set needed to work with multiple cloud vendors. Kelly points out that "different management portals and various features can challenge teams who lack members with multi-cloud vendor experience."

MULTI-CLOUD, MULTIVENDOR SECURITY AND COMPLIANCE

The "multi-cloud vendor experience" makes "coming up with that 'single pane of glass' view of your environments" challenging, says Ed Featherston, VP and principal architect at Cloud Technology Partners. "Every vendor has their own set of tools that provide great visuals to their environment. Being able to see across the hybrid clouds transparently to facilitate management is being worked on by variety of vendors, but [they're] not quite there yet."

That means, says Blaisdell, "It might be pretty hard to ensure compliance in a multi-cloud environment as some adherence measures adopted on one platform might not be the best for the other one." And, says Kelly, "Each cloud provider handles it differently."

"The biggest challenge is figuring out how to translate existing policies that govern security, access, and even performance to a cloud environment," says Lori MacVittie, principal technical evangelist at F5 Networks. "Organizations that use different services in different clouds to handle these critical components can run into obstacles trying to make sure they're consistently implemented."

And don't forget about disaster recovery, says Bluelock's Nolting.

"Multi-cloud deployments, by default, increase environment complexity, making successful disaster recovery plans for an entire environment harder to execute than plans leveraging a single cloud—which many companies don't consider in advance," she says. "When an enterprise needs to recover services after a disruption, they may have cloud-native applications that resume automatically in a new zone, but those need to be recovered alongside and connected to incumbent technologies like managed private cloud-hosted databases or a physical AIX system. Disaster recovery plans (and the testing and certification of those DR plans) become even more critical as the complexity of a business's environment increases."

KEY TAKEAWAYS

Let's finish with some key points made by Theo Lynn, professor of digital business at DCU Business School, who puts forward the "forest for the trees" argument.

"While industry has responded to the need for managing the complexity of multi-cloud deployment, the focus of such service providers tends to [concentrate] on operational management.

"As a result, both migration and deployment planning to optimize the cost of resource acquisition and usage remain issue[s] that [are] often inadequately considered or not at all. Migration plans are either too strategic or too technical," Lynn says. "This is complicated by lack of standardization in terms of interoperability, SLAs, and pricing schemes."

Finding that sweet spot between "too strategic or too technical" is key. Until standards and interoperability are sorted out, IT leaders should:

- Have a strategic plan for cloud deployments.
- Pay attention to the "weeds:" things like SSH keys, compliance policies, networking, and billing.
- Focus on data and data migration.
- Be ready to address skills and training.