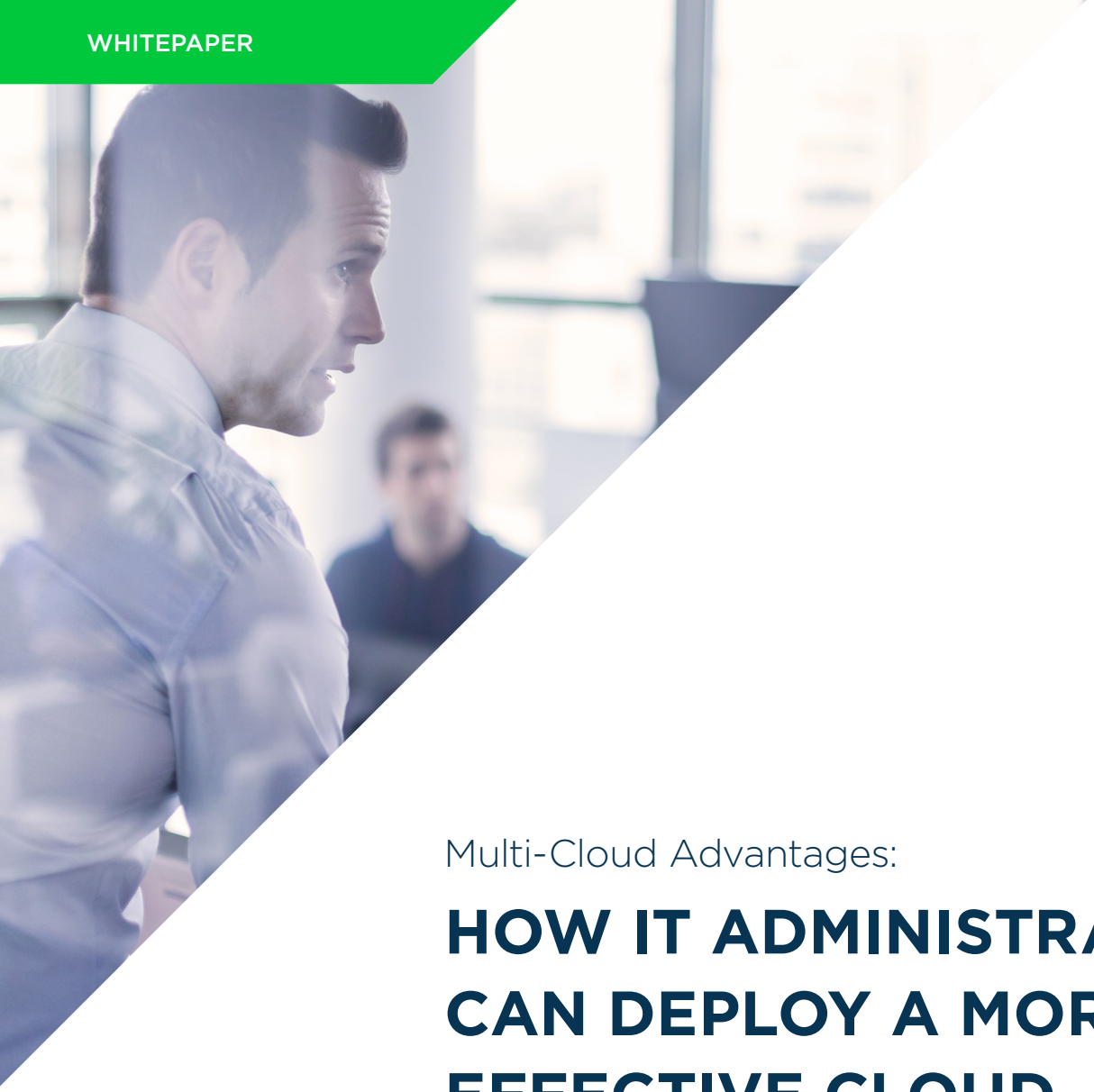
WHITEPAPER



Multi-Cloud Advantages:

HOW IT ADMINISTRATORS CAN DEPLOY A MORE EFFECTIVE CLOUD

Cloud Checkr

CONTENTS

1. Avoiding Lock-in With Multi-Cloud
2. Visibility
3. Accountability
4. Commercial-Grade management
5. Summary

OVERVIEW

As experience with cloud solutions grows, organizations of all sizes are realizing that various cloud services all have different advantages. The result is that cloud adoption is increasingly both hybrid and multi-cloud. Assigning a workload to the appropriate location has obvious economic advantages, but how can administrators efficiently manage a hybrid multi-cloud environment?

The simple approach to hybrid cloud computing is to rent everything from a single vendor. Microsoft is the primary example here, with both the Azure public cloud and the Azure Stack on- premises cloud designed to work together as a hybrid solution.

However, single-sourcing one's IT comes with risks. Clouds in general involve certain lock-in risks, but single-sourcing a hybrid cloud solution has a distinctly "Hotel California" feel: Workloads can check in to an ecosystem any time, but they are expected to never leave.

AVOIDING LOCK-IN WITH MULTI-CLOUD

The shift to a multi-cloud solution is aimed at countering this lock-in risk. Many organizations seek to manage on-premises clouds, service-provider clouds and the leading public clouds; they move workloads and data between all three. Organizations need to make sure they are observing regulatory standards regardless of where a workload or data exists; they also need to be constantly vigilant about costs.

Hybrid and multi-cloud approaches can help protect against an outage in any one cloud, but they should also help protect against changes in the economics or long-term legal viability of any given cloud provider. In short, organizations increasingly need the ability to walk away from a cloud provider entirely, not just handle a momentary outage.

This calls for a new breed of management solutions, one that can manage multiple clouds (and cloud types), and that helps organizations solve the intertwined problems of portability, availability, and cost.

VISIBILITY

Modern cloud management solutions need to provide organizations with visibility across different silos. Beyond the concept of a single pane of glass, visibility is critical to helping reduce cloud sprawl by allowing organizations to view resources that are duplicated in different silos.

A common inefficiency among organizations operating their own on-premises infrastructure is Virtual Machine (VM) sprawl—when the number of VMs in an organization exceeds the ability of administrators to effectively manage them. This is frequently due to the natural tendency not to delete unneeded VMs: It's much easier to focus on what has to be done than on cleaning up.

The same issue has spread to the cloud. Just as organizations found that they need to invest in tools, training and business practices designed to support a more purposeful and manageable VM lifecycle management, the same needs arise when dealing with clouds. While IT automation mitigates cloud sprawl most effectively, automation is impossible without first solving visibility.

Visibility reveals what workloads and data are where, and which workloads and data need to be where. With visibility into costs, optimal placement information for new workloads or data stores can be provided to administrators prior to instantiation. Eventually, that data can drive automation and boost efficiency.

ACCOUNTABILITY

Nobody wants to have to deal with different usernames and passwords to access different IT services. Organizations spend a great deal of time and money creating Unified Access Control (UAC) solutions, federating authentication systems, and otherwise trying to enable everyone to use a single user ID for everything. There are also reasons to embrace UAC that go beyond convenience: accountability, among others.

Clouds are predicated on the concept of self-service. One of the IT and business practices that clouds are explicitly designed to encourage is allowing application and service owners to create or subscribe to workloads and data as needed, without requiring approval from IT administrators.

The more people have access to an organization's cloud capabilities, the more important it becomes to track what they are doing, what they are spending, and what data they are accessing. Equally important is the ability to restrict what users can do in a granular fashion: It is important that all users be able to do what they need to do in the cloud, but only that which they need to do.

This concept of "least privilege" is so important that the European Union's new General Data Protection Regulation (GDPR) enshrines it into law. While UAC isn't strictly required to enforce least privilege, managing multiple accounts—and their various restrictions—for multiple users across multiple clouds very quickly becomes a nightmare.

UAC also underlies any sensible attempt to instrument the authentication system. UAC allows a user's actions to be monitored on all clouds, thereby enabling reporting on that user's activities as a single user. It also provides analytics and alerts of suspicious or dangerous behavior that might otherwise go undetected. (For example, deleting a workload or dataset from one cloud, and all of its backups across different clouds as well.)

UAC solutions can also be useful to enable best-practice checking, and to help automate IT auditing. Because of the deep integration between authentication and management, UAC is a must-have functionality for any effective hybrid multi-cloud management solution.

COMMERCIAL-GRADE MANAGEMENT

Cloud providers have attempted to address these problems by publishing Application Programming Interfaces (APIs), which allow administrators to command and control cloud solutions by writing applications or scripts. APIs are a fundamental aspect of IT automation. They make it possible for solutions like UAC to span multiple clouds.

For years, organizations have tried to solve these challenges by building an application that talks to APIs. As the features and functionality of clouds have grown more complex, and as the number of cloud organizations to interact with has grown, building such a solution in-house has become increasingly unmanageable.

The complexity of clouds has reached a point where commercial, hybrid, multi-cloud management is a necessity. Cloud vendors have the resources to dedicate a number of software engineers to increasing the functionality of the core management application, and to staying on top of the constantly evolving cloud APIs as well as the underlying features and functionality they entail.

SUMMARY

Virtualization made the lives of administrators easier by removing much of the daily focus on physical infrastructure. Server administrators could stop worrying about drivers and RAID arrays, and focus instead on the Operating System Environments (OSEs) for which they were responsible.

Cloud computing exists to remove the need to worry about OSEs and allow service owners to focus on the applications for which they are responsible. Service user scan spawn workloads from templates or sign up for Software as a Service (SaaS) solutions without needing the permission of IT administrators.

Incrementally, the variations and malfunctions of the underlying IT infrastructure are being abstracted away from service owners and end users. While someone, somewhere has to worry about dead hard drives, creating templates, and defining user profiles, infrastructure concerns are increasingly disconnected from the service consumer's experience.

That the service consumer's experience is now largely asynchronous of the IT infrastructure should not mean that organizations can simply forget about making that infrastructure usable. Whether the IT infrastructure you're dealing with is on premises, at a service provider, or somewhere in the public cloud, it has to be managed.

IT administrators are human too. There are real practical limits to how much administrators can manage before they too need advanced tools. Like anyone else, IT administrators need to abstract away what complexity is possible, and automate the automatables.

CloudCheckr helps you manage accounts across multi-cloud ecosystems, helping automate key tasks, manage UAC, and gain deeper visibility and control. Start your free trial today.

Need CloudCheckr for your organization? Learn more at **www.CloudCheckr.com**.

Cloud Checkr

342 N GOODMAN ST,
ROCHESTER, NY 14607

1-833-CLDCHCK

www.cloudcheckr.com