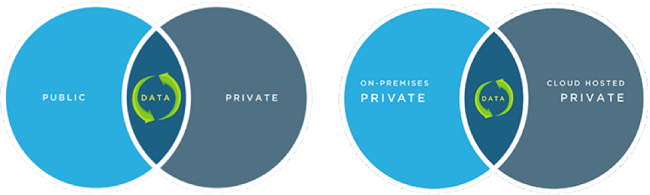
Defining Hybrid Cloud (vs. Multi-Cloud)

CONTENTS

WRITTEN BY HAROLD BELL
CLOUD SPECIALIST, NUTANIX

Hybrid clouds allow operators to perform a single task leveraging resources from two separate clouds. The key to remember is that hybrid combines the resources of two different clouds – could be two private, two public, or a mix of both. Referencing the Venn diagrams below, the overlapping space in the middle represents the encrypted, or "hybrid," layer.

WHAT DOES A HYBRID CLOUD ENVIRONMENT LOOK LIKE?



This middle ground between clouds provides a vital bridge for data transmission. It allows organizations to leverage cloud capabilities without compromising productivity or security.

Hybrid cloud infrastructure provides notable flexibility for organizations. You enjoy the secure access of on-premises resources while also having the rapid scale and elasticity of the public cloud. But what about environments that utilize both public and private cloud infrastructures if data isn't shared between them? How do we categorize this scenario?

A "multi-cloud environment" would be the right answer. These types of cloud environments differ from hybrids, as they suggest the presence and usage of many clouds without the guaranteed interoperability between them. According to Gartner, more than 70% of enterprises will be implementing a multi-cloud strategy by the end of this year.

One common misconception when comparing hybrid and multi-cloud infrastructures is that the two are mutually exclusive. The explicit definition of a multi-cloud environment, i.e. more than one cloud, suggests that a hybrid cloud model is also a multi-cloud model.

NUTANIX Xi Beam

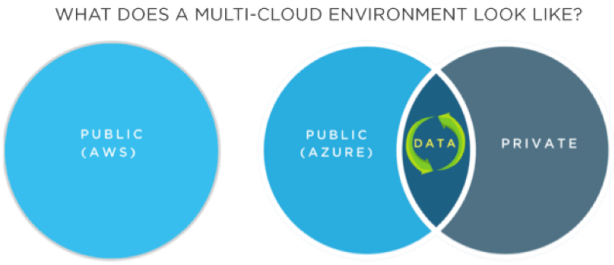
Cloud management made easy.

Easily identify and fix cloud security vulnerabilities and cost leaks in multi-cloud environments.

GET STARTED

nutanix.com/beam

However, the inverse is not always true. A multi-cloud configuration can be hybridized, but it can also exist without the need for individual clouds to talk to each other.



Enterprises are increasingly presented with business justifications for managing workloads amongst several cloud providers. Let's look at some of the management challenges in a multi-cloud world and how best to address them.

Multi-Cloud Management Challenges

Maintaining your multi-cloud environment that may consist of both on-premises and cloud-hosted infrastructure requires help. Major public cloud providers like AWS, Microsoft Azure, and Google Cloud Platform do have native cloud governance tools for their respective solutions. However, they neither offer a holistic view of your multi-cloud environment, nor the tools to drive efficiencies between providers. Essentially, they fail to provide the visibility and control that cloud operators require. Governance capabilities that are sufficient for the technology landscape of today require optimization of your entire cloud environment.

LACK OF VISIBILITY ACROSS CLOUD BOUNDARIES

IDC predicts that "by 2020, over 90% of enterprises will use multiple cloud services and platforms." However, the compromise is a loss of visibility and control over the cloud services that your engineering teams are consuming. When you have several cloud accounts across multiple cloud environments, not having a single pane of glass to provide you a holistic view of your spending patterns could lead to your budget blowing up and putting the timely delivery of your project in jeopardy.

LACK OF REAL-TIME OPTIMIZATION RECOMMENDATIONS

The elastic nature of on-demand instances in public cloud environments has been well suited for agile workloads. However, navigating the complexity of multiple options across a number of cloud accounts using a variety of services can be challenging. Variability in the use of cloud computing resources has pushed ownership of cloud cost management onto engineering teams. It's not a buffet where you can help yourself freely and someone else picks up the tab; engineering teams need to plan for and be accountable for the cloud resources they consume.

Unused public cloud instances, especially compute instances, or workloads running in the public cloud that are better suited for private cloud can result in large, unnecessary costs that could then start to weigh on the company's bottom line. Cloud operations teams may be unable to avoid cloud wastage without tools that help them analyze data granularly, identify the cost drivers quickly, and make intelligent recommendations to right-size cloud resources.

SHADOW IT (LACK OF CONTROL)

As cloud environments grow, the need to centralize control across multiple teams becomes critical. Cloud operators and business owners need a systematic way to map consumption to business units. If you are an IT manager or cloud architect, it's likely your engineering team forgot to turn off compute instances that they were no longer using. Or you have no idea who spun up what, but you are still paying at the end of the month.

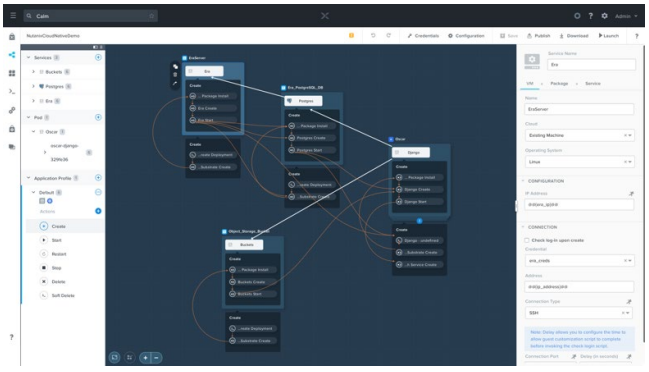
With that said, automation is required in order to address the lack of visibility, optimization, and control experienced by cloud operators. Specifically, a cloud management platform.

Critical Capabilities of Cloud Management Platforms and Tools

Gartner has recently begun research for their official classification of a Cloud Management Platform (CMP), as well as an updated Magic Quadrant. They officially define the CMP market as "tooling that enables organizations to manage multi-cloud (private and public clouds) services and resources." In the section below, we will highlight each of the critical capabilities, providing the official definition, and some best practices based on our experience.

PROVISIONING AND ORCHESTRATION

The tasks used to create, modify and delete resources and to orchestrate complex deployment and management operations.



Automating the entire lifecycle and orchestration process for quicker provisioning of applications. Screenshot: Nutanix Calm.

Proper application provisioning requires flexibility, scalability, and automation throughout the entire lifecycle. Your CMP should allow

you to fully automate the provisioning of hybrid cloud architectures, scaling multi-tiered and distributed applications across cloud environments. Orchestration tools help to automate tasks across different systems, giving you the freedom to deploy on the IaaS platform, hypervisor, and even container orchestrator of your choosing.

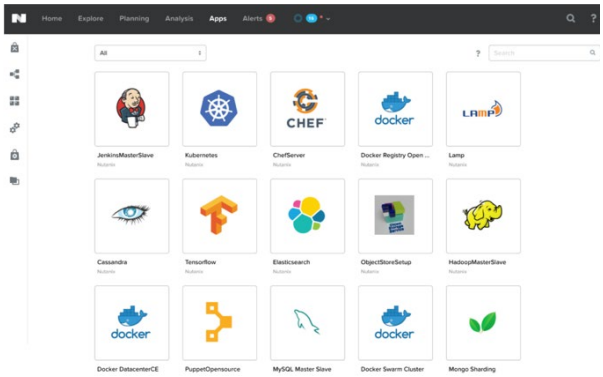
Additionally, it's critical to remember that while new applications might be completely cloud-native, existing applications are often too complex or costly to lift-and-shift to the cloud. This means that cloud-native only CMPs add to your operational overhead if they do not allow you to refactor your existing applications to make them cloud-ready. Look for end-to-end solutions that offer a single view of all of these cloud considerations with the flexibility to integrate with current and future provisioning tools to be sure you can always flex between clouds and provisioning strategies as needed.

SERVICE REQUEST

The tasks required to collect and fulfill requests from business users to access cloud services or deploy cloud resources.

Cloud management is an iterative process — in both improving the health of your environment and user experience. With that said, CMPs are evaluated on their ability to service requests from end users in a timely fashion. This could be inquiries on access to cloud services or requests for deploying new infrastructure resources.

When evaluating CMPs, your attention should be on how requests are serviced, the ease of use, and the presence of automation to deliver a self-service experience. One idea is that CMPs provide an internal marketplace that relies on pre-configured blueprints that can be used to configure various infrastructure components such as load balancers, databases, front-end servers, etc. Your application owners and developers can then request these blueprints from the marketplace as needed. DevOps teams in particular gain the freedom to operate quickly and efficiently on their own using existing blueprints without having to open tickets and wait for several weeks for IT to do it for them.



A self-service marketplace allows you to pick and choose the app components you need. Screenshot: Nutanix Calm.

INVENTORY AND CLASSIFICATION

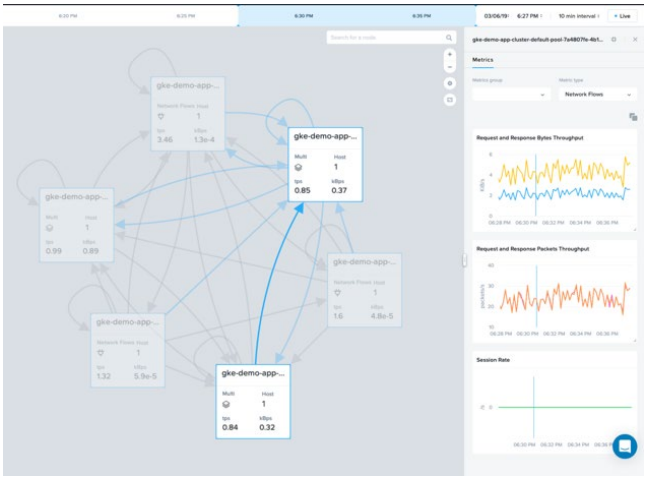
The ability to discover and maintain an inventory of cloud resources as well as the ability to monitor change and manage configurations.

There are many governance challenges that customers may face in a multi-cloud world. Governance comes from defining and enforcing policies and role management. This is where appropriately tagging cloud resources can help to enable automated tracking and control of cloud spend. Remember — you can't tag everything, but tag everything that you can.

Keeping a tight inventory of your infrastructure and cloud services consumed allows you to define and enforce multi-cloud budgeting policies that would provide warnings about overconsumption. A comprehensive inventory list that classifies resources by compute, storage, networking, analytics, etc., greatly enhances your capabilities to be proactive in how you handle migration, data transfer, and disaster recovery. If your CMP doesn't tell you what you are consuming in an easily digestible manner, you'll have a really hard time optimizing your consumption.

MONITORING AND ANALYTICS

The collection of performance and availability metrics, as well as the intelligence to analyze data, to prevent incidents or automate incident resolution.



A service dependency map and key application health metrics. Screenshot: Nutanix Epoch.

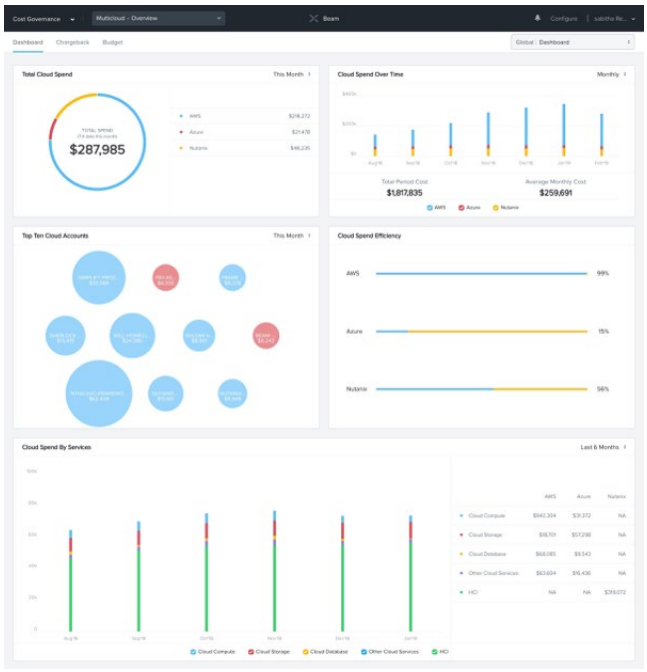
With the advent of containerization and serverless architectures, applications are rapidly going through a paradigm shift towards distributed architectures. Your CMP must have the ability to monitor the health of infrastructure, as well as distributed services, without relying on fragile code embedded techniques used by traditional application performance monitoring tools.

CMPs should allow you to monitor the "golden signals" of your application and service health including, but not limited to, through-

put, latency, and error rates at the service level without requiring code instrumentation. CMPs should provide cloud operations teams with powerful insights into events and service dependency maps that allows DevOps teams to quickly assess the impact of service downtime on other dependent services. Having a live map of your service and application interactions is invaluable for full-stack monitoring and performance analysis to eliminate bottlenecks and avoid costly outages.

COST MANAGEMENT AND RESOURCE OPTIMIZATION

The tasks needed to track and optimize spend on an ongoing basis as well as to align resource capacity to actual workload demand.



A multi-cloud Cost Governance dashboard. Screenshot: Nutanix Beam.

The elastic nature of clouds, especially public clouds, often leads to over-provisioning and unused resources. Industry leading analysts predict that by 2020, 80% of organizations will overshoot their cloud IaaS budgets due to a lack of cost optimization approaches. Providing global visibility, intelligent cost optimization recommendations, and policy-based automated control is a key pillar of CMPs that helps businesses realize the benefits of the cloud without blowing up their budgets.

Cost optimization capabilities in a CMP built for multi-cloud environments need to identify underused resources in real-time and also automatically downsize them when appropriate. For example, an extra-large size compute instance may be overkill for dev/test workloads. CMPs that identify such overprovisioned instances and automatically downsize them to a more appropriate size deliver more effective cost savings.

Similarly, your CMPs should allow you to configure automation policies that allow you to schedule on/off times for resources when they may not be needed — such as overnight or on weekends. They should also allow you to define and enforce multi-cloud budgeting policies that would not only warn about overconsumption before the cloud bills skyrocket.

CLOUD MIGRATION, BACKUP, AND DISASTER RECOVERY

The ability to replicate data to migrate workload, implement business continuity (BC) or disaster recovery (DR) architectures, or to protect data against accidental deletion or malicious activity.

Traditional DR services tend to be expensive and offer less-than-optimal recovery point and recovery time objectives. In a multi-cloud architecture, companies can use cheap, scalable public-cloud storage to keep snapshots of VMs and local disks. Sensitive data like customer financial history can be backed-up securely using private cloud storage.

CMPs need to streamline disaster recovery processes for business continuity of critical workloads. The ability to dynamically spin up testing environments and confirm the entire recovery process — without impact to your primary environment — is key. Eliminate the need for provisioning, configuring, and managing disparate cloud environments or multiple solutions for disaster recovery.

IDENTITY, SECURITY, AND COMPLIANCE

The tasks to manage and secure access to cloud services as well as enforcing a security configuration baseline.

A multi-cloud Security Compliance dashboard. Screenshot: Nutanix Beam.

A Dow Jones Customer Intelligence Study found that "68% of executives whose companies experienced significant breaches in hindsight believe that the breach could have been prevented by implementing more mature identity and access management strategies."

Remember, IT no longer has full control over the provisioning, de-provisioning, and operations of the cloud infrastructure. This decentralized ownership has increased the complexity for IT teams

to provide the compliance and risk management policies required to protect their businesses. Misconfiguration of network access controls tends to be one of the main reasons for most data governance vulnerabilities. Storage buckets with global read-write permissions and databases with publicly accessible ports are another ticking time bomb. CMPs that provide real-time, policy-based vigilance and remediation of such security vulnerabilities can help to secure your public cloud before data breaches occur.

Your security compliance policies need to scale with the scaling of your cloud deployments. Almost all enterprises that manage sensitive information need to adhere to regulatory compliance standards such as HIPAA, ISO, PCI-DSS, CIS, NiST, SOC-2, GDPR, etc. Pick a CMP that shows you the level of compliance with the regulatory policy framework that works best for your industry vertical, business function or geographic location. Continuously scan for and use policy-based remediation to validate your compliance with the regulatory policies so that you can pass audit checks confidently.

Conclusion

When it comes to selecting a cloud management platform, identifying a solution that scales with your cloud infrastructure is the key. This means you must evaluate how your CMP will fit in with a growing environment while delivering the level of visibility and control needed to enforce governance policies that directly influence performance, availability, security, capacity, cost, compliance, and disaster recovery.

Written by **Harold Bell,** Cloud Specialist at Nutanix

DZone
A DEVADA MEDIA PROPERTY

DZone communities deliver over 6 million pages each month to more than 3.3 million software developers, architects, and decision makers. DZone offers something for everyone, including news, tutorials, cheat sheets, research guides, feature articles, source code, and more. "DZone is a developer's dream," says PC Magazine.

Devada, Inc.
600 Park Offices Drive
Suite 150
Research Triangle Park, NC

888.678.0399 919.678.0300