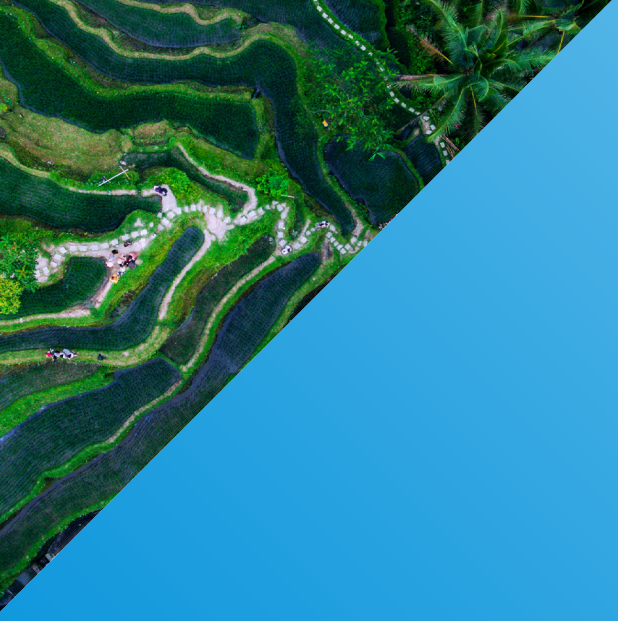


vmware® CLOUD™

The Enterprise Guide to Managing Multi-Cloud Operations

Mastering the scale and complexity of multi-cloud operations.

Contents

01 Overview

Many things have changed since Amazon launched AWS in 2006. Most organizations now have a substantial portfolio of applications running in the cloud.

As the number of applications running in the cloud has increased, so too has the complexity of managing these applications. And with most businesses leveraging multiple cloud environments, this complexity is heightened further.

The net of all of this is that the cloud is now a critical business resource that must be managed more strategically. It's no surprise then, that according to Forrester 86 percent of enterprises have adopted a multi-cloud strategy.[1]

With the growth in usage of the cloud and associated complexity, enterprises are now reaching a point where they are seeking to simplify their cloud operations. Many have created Cloud Centers of Excellence or Cloud Operations teams which are in charge of driving best practices in cloud operations across all of the enterprise's projects and clouds.

Enterprises are also taking a fresh look at the tools they use to manage these environments. As multi-cloud application architectures and multi-cloud operations become more the norm than the exception, finding solutions that provide a unified view and a single operating model across AWS, Azure, and Google is becoming a priority.

In this eBook, we'll explore the industry shifts driving multi-cloud adoption, the challenges enterprises face in this new paradigm, and how emerging practices and technology solutions can make optimized and consistent operations across multi-cloud environments a reality.

[1] **Forrester, Multi-cloud Arises From Changing Cloud Priorities, 2018**

02 The State of Public Cloud Operations

A Brief History of Public Cloud Adoption

DevOps teams were the first to embrace the cloud, seeking the ability to produce high-quality code at a faster rate than competitors. The public cloud supported this by delivering fast and easy access to resources, infrastructure as code, and well-defined APIs that could be easily embedded into Continuous Integration / Continuous Delivery (CI/CD) processes.

Developers and business leaders alike found a number of additional benefits of moving application workloads to the public cloud including:

- On-demand pricing and only paying for the resources they used
- OpEx rather than CapEx spending
- An ability to easily deploy applications to multiple geographic locations

Mission Critical and Multi-Cloud

For most companies, the portfolio of projects running in the cloud has moved from a few test and development and non-critical applications, to a large portfolio of revenue-generating, in-production applications.

As the profile of applications running in the cloud has changed and as cloud spending has surged, senior executives have realized public cloud usage can no longer be taken for granted. For most organizations, the use of public cloud is now intricately connected to business success.

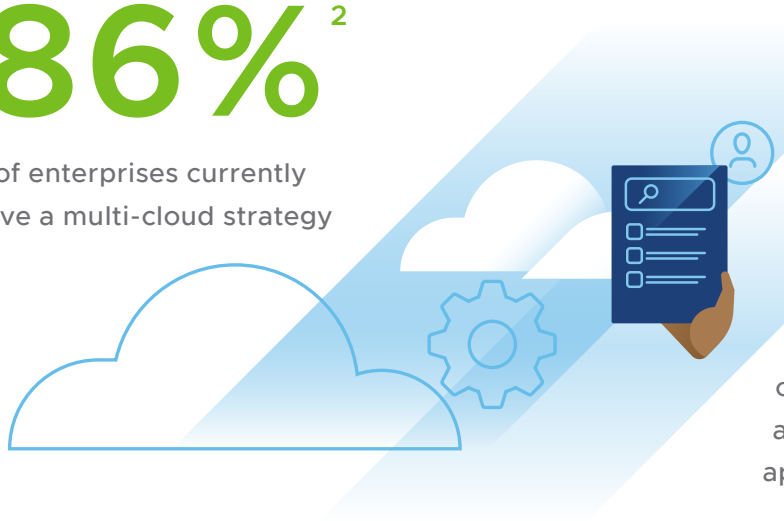
While adoption of multiple public clouds initially came about in an unplanned, ad-hoc fashion, senior executives now see the use of multi-cloud sourcing as a strategic imperative.

A multi-cloud strategy supports several important business objectives:

- **Protection against vendor lock-in:** Access to multiple clouds provides assurance that they can discontinue a relationship with one cloud provider and move its applications to another cloud with which they already have some operational experience.
- **The ability to leverage the unique strengths of each provider:** Multi-cloud strategies allow enterprises to choose the cloud with the most innovative or appropriate service to meet their specific application and customer needs.
- **Expanded geographic reach:** While the global footprints of all cloud providers are expanding, enterprises still often find that not all providers have a local presence in a particular market of interest. Working with multiple public cloud providers allows enterprises to bring capacity online exactly where they need it, when they need it.

86% [2]

of enterprises currently have a multi-cloud strategy



60% [2]

of enterprises plan to, or have already moved mission-critical applications to the public cloud.

[2] Forrester, Multi-cloud Arises From Changing Cloud Priorities, 2018

Cloud Maturity and Cloud Operations

When they first embraced development on the public cloud, application development teams weren't just writing code. Having left behind the data center and the centralized IT teams that managed operations, these teams became responsible for the significant task of managing cloud operations.

This included integrating resource management into CI/CD processes, keeping track of and optimizing resources and associated costs, and ensuring that applications and their environments were secure and compliant.

> Each new cloud provider introduces a unique operating model along with unique semantics, APIs and services.

As the number of applications these teams are developing in the cloud has increased, so has the scale and complexity of managing an ever-growing application portfolio.

This complexity is heightened further as more and more organizations begin to embrace multi-cloud operations because each new cloud provider introduces a unique operating model along with unique semantics, APIs and services.

Today, organizations are reaching an inflection point in how they think about managing this level of complexity. Increasingly, organizations want their development teams to put greater emphasis on producing features that drive revenue growth and increase customer acquisition and retention – and less on managing non-differentiated operational tasks.

As part of their evolving thinking, many organizations are beginning to staff Cloud Operations teams. These teams function as Centers of Excellence for public cloud operations, working across multiple application teams to improve the effectiveness of cloud operations.

These new teams are taking on a range of cloud operations tasks, including defining operational best practices, optimizing and managing cost, monitoring security and compliance, and troubleshooting application performance. They are a leveraged resource that often works with other teams to ensure that they have the necessary guardrails to proactively avoid operational issues across multiple domains.

Cloud operations teams are well positioned to handle the challenges associated with running cloud operations at scale. Challenges such as gaining visibility into where resources are being used and how efficiently they are being used and ensuring resources are properly configured to meet security, compliance and performance objectives.

03 Public Cloud Operations Challenges

Most organizations with a significant presence in the public cloud already struggle to effectively manage cost, implement consistent security and compliance, govern the use of cloud resources and ensure their portfolio of SaaS applications meet a broad range of business expectations. At the heart of this struggle are the twin challenges of scale and speed of change.

In the data center, the rate of change has traditionally been much slower than that of the public cloud. Generally, the number of users is fairly consistent and new services are deployed in a fairly predictable manner.

However, when organizations begin to operate in the public cloud, all of this changes. Even on a single cloud, the combination of a rapidly growing user base, hundreds of different services and a very high rate of change creates a situation where keeping up is extremely difficult.

Differences between cloud provider environments exacerbate this problem further when considering multi-cloud operations. As a result, most organizations lack the visibility and related control necessary to ensure cloud operations are both effective and efficient, which impacts in the following areas:

Cost Management

Many enterprises spend far more than they need on cloud resources. In fact, Gartner estimates that by 2020, organizations that lack cloud optimization processes will overspend by 40% in the public cloud.[3]

This is because organizations lack a holistic view and understanding of everything they are doing in the cloud, including what projects are running and how well resources associated with these projects are being managed. Lacking this detailed view, teams can't make clear and informed business decisions around where to optimize costs.

Cost challenges include:

- Inability to track and allocate costs by business unit
- Underutilized or zombie resources that could be resized or turned off
- Overuse of on-demand infrastructure instead of using discounted capacity reservations

Security and Compliance

Ensuring that applications and their environments are secure and compliant is a significant challenge for most organizations. The large number of accounts, applications, and objects that must be managed in a public cloud, combined with the high rate of change that characterizes the cloud, make it extremely difficult to ensure that resources are always properly configured. The fact that each cloud provider has its own unique security standards adds further complexity to the task of managing risk.

[3] Gartner, Predicts 2018: The Cloud Platform Becomes the Expedited Path to Value, 2018

The model for addressing application security and compliance is also changing. Organizations are seeking to adopt a much more proactive, "secure by design" approach.

In this model, security and compliance are addressed in every stage of the development cycle and then continuously audited once in production. The emerging paradigm also leverages a multi-disciplinary approach across security and development professionals.

> The combination of a rapidly growing user base, hundreds of different services and a very high rate of change creates a situation where keeping up is extremely difficult.

Security and compliance challenges include:

- Ensuring cloud resources continuously conform to the cloud provider, security, industry and regulatory configuration best practices
- Rapidly detecting changes to resource configurations, understanding the source of these changes and prioritizing risk mitigation based on application criticality
- Proactively integrating security and compliance requirements into CI/CD processes for early issue detection

Application Performance Troubleshooting

As the scale of operations in the cloud has grown, many teams struggle to rapidly troubleshoot SaaS applications built using microservices and containers. The amount of data that must be captured and analyzed for a modern app is much greater than that of a traditional application.

As a result, tools and practices built for an earlier age fall short in their ability to provide real-time insight into application performance.

Application performance troubleshooting challenges include the ability to:

- Quickly detect anomalies impacting cloud-native SaaS applications in production
- Easily see and correlate application performance trends
- Leverage intelligent alerting that is responsive to dynamic behavioral changes, impacting application performance

Resource Design and Governance

Teams developing apps in the cloud continuously build and deploy many different environments to support their application needs. Many of these are replicas or variants of previously built environments. To reduce repetitive, low value work and the errors associated with manual activity, organizations are looking for ways to automate the building and provisioning of resource templates.

[4] Gartner, Is the Cloud Secure, 2018

As multi-cloud operations become the norm, these templates must be able to abstract away differences between cloud providers so that environment definitions can be easily leveraged across more than a single cloud provider.

Resource design and governance challenges include:

- Maintaining a collaborative process to create or update environment templates to support application requirements
- Controlling which teams can use specific templates and where these templates can be deployed (for example, which availability zones or clouds can be leveraged for specific environments)
- Integrating the use of templates via APIs into CI/CD processes that support a fully automated development lifecycle

Who's Securing the Cloud?

Many cloud providers include stringent security policies in their offerings. However, there is a line where security becomes the responsibility of the enterprise and not the cloud provider. In many cases, users cause security lapses due to errors in security operations and management.

According to Gartner, 95% of cloud breaches through 2022 will be due to enterprise shortcomings.[4] CIOs must change their line of questioning from, "Is the cloud secure?" to, "Am I using the cloud securely?", and from there, build a strategy that ensures consistency, visibility and control over all operations.

04 Eight Critical Capabilities for Managing the Public Cloud

Visibility and Analytics

Broad visibility and data analytics across all of your public clouds is fundamental to success in the public cloud.

These capabilities enable enterprises to drive accountability, manage margins and do chargeback across the organization. They also allow organizations to track spending across multiple clouds and set budgets by any logical business grouping, whether it's a project, application, department or team.

Cost Optimization

The ability to optimize costs across multiple cloud environments is also a key capability that organizations should look for.

A solution should identify underutilized infrastructure, make recommendations on what adjustments can be made and report the ROI associated with making those adjustments. Multi-cloud solutions should also help organizations reduce cloud spend through the optimized use of Reservations.

Reservations – called Reserved Instances or Committed Use Discounts depending on the cloud platform – are upfront commitments made to consume resources from the cloud provider, in exchange for a discount.

While Reservations are one of the best ways to reduce spend in the public cloud, many organizations do not take full advantage of them because of the challenges in forecasting capacity needs and the complexity of managing them.

Ultimately, multi-cloud solutions should help enterprises save time and money by providing accurate recommendations and automated Reservation management.

CASE STUDY

Cox Automotive owns more than 25 brands globally, operating online and printed publications such as Kelly Bluebook and Autotrader.com

Typical of many enterprises, they have significant investments in both private and public clouds, running over 10,000 VMs across more than 50 data centers, and a sizeable footprint across both AWS and Google.

In 2017, Cox Automotive saved more than $2M on their cloud bills using **CloudHealth by VMware**. CloudHealth helped Cox Automotive improve application migration planning speed and accuracy, and to gain comprehensive visibility across their multiple public and private clouds.

Managing Resource Misconfiguration

Misconfigurations are currently the number one risk to applications and data in the public cloud. This problem was previously encountered when applications were built in the data center but is compounded in the public cloud due to the scale of operations. Because the public cloud supports very high levels of agility, configurations must now be changed more frequently.

The decentralized, low governance nature of the cloud also adds to misconfiguration risks. A multi-cloud solution should provide visibility into misconfigurations by continuously mapping service configuration relationships and movements in real time to reveal vulnerabilities across service layers.

Protecting Against Cross-Service Threats

Cross-service vulnerabilities exist in every cloud account and increase as cloud usage grows. Due to the interconnectedness of services within an environment, unintended vulnerabilities can be created from even minor changes.

This problem is exacerbated in a dynamic, always-changing environment. A multi-cloud solution should track and understand the relationships between services in real time, allowing enterprises to monitor and rapidly revalidate critical security configurations.

CASE STUDY

Each month, more than half a billion consumers view and share authentic opinions, questions and experiences about tens of millions of products in their network.

Bazaarvoice gives leading brands and retailers solutions that enable them to engage with consumers wherever they shop.

VMware Secure State helps Bazaarvoice address security and compliance concerns for their application portfolio running in the cloud by providing automated and continuous scans of all of their cloud accounts.

Bazaarvoice is integrating the use of VMware Secure State into their DevOps practices so they can proactively ensure that any code rolled out to production is secure and compliant by design.

High-Scale / High-Velocity Metrics Capture

App development teams often struggle to rapidly troubleshoot applications built with microservices and containers. Often, this requires capturing and analyzing metrics at levels of up to 1M points per second, which many enterprises can't achieve with their outdated monitoring tools.

Others use open source tools, however, these can't scale to deal with the data needs associated with large-scale SaaS applications. A multi-cloud solution must be able to address the high-velocity and high-scale demands of cloud-native applications.

Metric Correlation and Analytics

As part of ensuring application performance, multi-cloud solutions should include a wide array of analytical functions that support a team's ability to monitor code performance anomalies in production across their entire infrastructure and application stack.

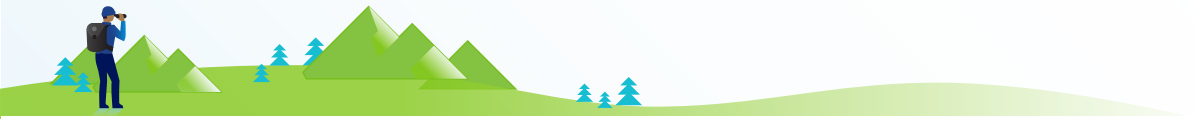
Out-of-the-box integrations with a broad ecosystem of technology solutions should be part of the solution as well. This allows the team to broaden their view of the forces that impact the performance of applications operating in the cloud.

CASE STUDY

Box is an enterprise content management platform providing a range of solutions; from sharing and accessing files on mobile devices to sophisticated business processes, like data governance and retention.

Today, more than 41 million users and 85,000 businesses – including 69% of the Fortune 500 – trust Box to manage content in the cloud.

Box collects more than 500,000 metrics per second on **Wavefront by VMware**. Hundreds of Box's developers use Wavefront to rapidly troubleshoot their SaaS applications. Box relies on Wavefront for key capabilities including; collecting metrics at scale, quickly building dashboards to help developers pinpoint performance issues, and sharing these dashboards for fast issue resolution.



Service Automation and Governance

In rapidly changing cloud environments, the only way to keep pace with the rate of change is to leverage automation. Multi-cloud solutions should provide enterprises with a centralized platform to manage cloud governance across multiple teams in an automated fashion.

You should be able to set policies that define best practices for configuration, cost and security and get alerted when policies are violated. This allows organizations to simplify daily cloud operations and proactively take actions related to cost spikes, tagging compliance issues, security vulnerabilities and more.

Cloud Agnostic Environment Templates

As public cloud operations become more multi-cloud, teams are finding it necessary to support the provisioning of resources across more than one cloud. This gives rise to a need for teams to work collaboratively to design version-controlled, cloud-agnostic blueprints (templates).

A multi-cloud solution should give developers easy access to resources using a declarative and iterative approach, treating infrastructure as code. At the same time, the solution should give Cloud Operations teams the ability to govern resource delivery across teams, environments and multiple clouds. Open and well defined APIs should make it easy to integrate resource delivery into CI/CD processes.

05 Conclusion

The increasing scale of public cloud usage within enterprise has given rise to a number of operational challenges – resulting in wasted time and money. Ensuring operations run efficiently should be a top priority for organizations looking to future-proof their cloud investments.

To meet this challenge, VMware has developed a portfolio of multi-cloud capable SaaS offerings to help enterprises overcome public and multi-cloud management challenges.

These solutions provide businesses with comprehensive visibility and necessary insights and tools, enabling businesses to optimize cost and resource usage, enforce consistent security and compliance standards, improve SaaS application monitoring and troubleshooting, and simplify resource governance and automation.

Together, this portfolio enables enterprises to simplify operations so they can take full advantage of the public cloud's benefits of agility, efficiency, and effectiveness.

These solutions provide businesses with comprehensive visibility and necessary insights and tools.

Managing public and multi-cloud operations doesn't have to be difficult. Visit the **Unify Multi-Cloud Operations** page on our website to discover how you can take full advantage of the benefits of multiple public clouds, without operational complexity.