VIEW POINT

NEXT-GENERATION CLOUD OPERATIONS: IMPORTANCE OF AGILITY AND SERVICE ASSURANCE

Abstract

How can companies determine the right balance between the need for speed and the necessity to stay up-to-date in cloud technologies, when business context changes every day? The answer lies in building agility and assurance across cloud operations from day one and not as an afterthought.

The fact is that as the nature of business changes, so does the complexity of a managed service model. Hence, today's organizations are in search of managed service providers (MSPs) who can offer business service assurance, while instilling agility as the new normal. When established players, such as Amazon Web Services (AWS), launch innovative services, organizations need to ensure that their chosen MSPs have the expertise and resources to on board new services cost-effectively. This paper compares the key differentiators between traditional, cloud native managed services, and summarizes the benefits gained by choosing the right MSP partner.

Infosys®
Navigate your next

Introduction

In today's digital age, businesses are expected to deliver everything 'as-a-service.' To achieve this, businesses are looking for newer ways to enable operational agility, improve service quality, and reduce administration overhead. Therefore, businesses must transform the way they procure, consume, and deploy cloud services to stay competitive. This requires adoption of leaner processes, bundling business operations and services, and enabling automation to reduce time-to-market (TTM).

In today's business environment, companies want to outsource their data centers, hosting, and managed services to specialized vendors who have strategic offshoring skills. They expect suitable vendors to provide business agility by allowing them to focus on their core business instead of spending time on undifferentiated heavy lifting of IT operations. Simultaneously, rapid advances in cloud-based technologies are driving them to choose service providers who can deliver continuous business service assurance instead of merely ensuring the availability of specific components.

Towards this goal, organizations must collaborate with MSPs who understand their business vision and can meet demands quickly. Having said that, it is important to underline the fact that such an alliance mandates a significant shift from lengthy processes that maintain traditional IT to a cloud-based model that drives automation. Further, to take advantage of new technologies and emerging trends, teams across both organizations must continuously experiment and build new capabilities and services. The key is to fail fast and fail cheap.

Challenges addressed by next-generation cloud MSPs

Organizations that continue to use traditional data center management solutions will struggle with inefficiencies due to limitations in defining, building, consuming, and administering services. Further, these solutions cannot incorporate automation capabilities, such as autoscaling, self-diagnosis, and automated creation or destruction of environments based on the business need.

Next-generation managed services for the AWS cloud cater to the present and future needs of businesses and improve usability for IT administrators and business users. The right solution bundles security, governance, and orchestration, thereby reducing total cost of ownership (TCO) and delivering outcome-driven services.

The following section details the key differentiators between traditional and next-generation MSPs for the AWS cloud.

Automation: Optimization and automation are two key levers used to reduce the cost of continuous delivery on the cloud. Organizations that use traditional managed services are trying to leverage automation to enable continuous improvement. However, these efforts often have a piecemeal approach, resulting in manually-driven and error-prone operations. On the contrary, in AWS, each service is exposed as an application programming interface (API). This allows MSPs to leverage infrastructure as code, and enable automation of operational actiivties such as provisioning, scaling, software installation, asset registration, resource allocation, alerting, and self-diagnosis of alerts / incidents. AWS services provide a range of options and techniques to achieve a DevOps (a clipped compound of development and operations) approach and native platform features, such as AWS CodeDeploy, Elastic Beanstalk, and OpsWorks. These services allow for seamless automation of enterprise service delivery processes and policies for continuous delivery.

Simplification of operations: When operating in a cloud environment, it is important to simplify processes and move away from the 'care and feed' approach that works well in traditional data centers. Operations teams need to leverage continuous automated monitoring, event logging, and real-time processing of data with new tool sets that are compatible with cloud technologies. This will enable businesses to progress from event-detection and enrichment to automated recovery and predictive analytics — to achieve optimal performance and the security of IT systems.

Visibility in usage and performance: Traditional managed services lack integration of tools and event sources that offer true insights into the solution. Without such visibility, organizations struggle to measure usage that validates costs. On the other hand, AWS offers pricing transparency at a granular level, thereby reducing complexity and cost. Further, cloud-based, MSP-driven solutions provide real-time information to key stakeholders about the status, utilization, and performance of workloads and service management.

Security enhancements: In the traditional managed services model, end-to-end security is owned by the service provider. Due to the increasing diversity of tools, security solutions have become complex and expensive. In the AWS cloud, security is a shared responsibility between AWS and customers through next-generation MSP offerings that address customers' requirements. Through AWS, security services, such as vulnerability management, encryption management, and firewall management have become a part of managed services. This will simplify security operations, allowing the MSP to leverage advanced tools and best practices for better cloud security and regulatory compliances.

Instead of merely deploying technology to maintain servers, the cloud-based managed services model enables self-service functionalities. This will engage end users to build services that streamline business operations. Simply put, the next-generation MSP takes complexity out of the equation to implement and manage the overall security setup.

Extreme skill differentiation: In the traditional data center model, organizations must employ resources with diverse skill sets in areas, such as server and storage management, network and firewall management, and perimeter security management. In the cloud world, infrastructure is delivered and managed through code. This reduces the need for employing engineers and architects with multi-domain skills and also allows maintenance tasks related to server hardware, hypervisor, and storage equipment management, to be managed through automation. Besides reducing the cost incurred by managing several technologies and personnel, this lowers dependencies on finding the right resource and enables MSPs to offer value-added services through extreme automation.

Achieving the right balance

A cloud-based managed services model requires continuous adoption and optimization of services as opposed to a traditional infrastructure based managed services model, as changes are less frequent in the latter. The chosen MSP should be able to customize the solution on a business-as-usual (BAU) basis and build continuously available technology and security stacks. This agility will help to achieve enhanced availability, near zero recovery time objective (RTO), recovery point objective (RPO), and other disaster recovery metrics.

Cloud service providers, such as AWS, are constantly innovating and launching new services. To maximize the potential of these new services, organizations need specialized MSPs who can continuously integrate capabilities and implement them to offer service assurance.

AWS has set a high standard across cloud managed services offered by partners to its customers. To obtain AWS MSP designation, partners must embrace and deeply understand the importance of DevOps in both internal operations and external engagements. They have responded to the power of automation for customers, and simply have looked at the world little differently. The AWS MSP program focuses on a core set of managed service capabilities that all AWS MSPs should possess, along with specific technical and business capabilities to further showcase their unique value to customers. The MSP should also have the ability to create a hybrid-architecture deployment and have detailed controls in place for data and operational security. It is important for next-generation MSPs to have a global presence with the right set of people and a software-based service delivery model to address the needs of the enterprise across all stages of cloud adoption.

Benefits of a next-generation managed services model

Finding the right MSP that provides service assurance through a next-generation managed services model can help enterprises:

- **Improve BAU operations:** With integrated processes, methodologies and frameworks, organizations benefit from higher operational transparency, agility, automation, and workload optimization without business disruption
- **Reduce the total cost of ownership:** With people plus software based tiered service delivery, enterprises have the freedom to select the best option based on the criticality of the business applications and types of service / support needed. They also gain flexibility in changing the service tier based on growing business requirements
- **Leverage pay-per-use:** Based on a pay-per-use model, such platform offers a range of payment options, instant scalability according to business needs, and adaptive pricing as cloud assets grow

Infosys Service Assurance Suite for the AWS cloud is a next-generation managed services offering that meets or exceeds the AWS MSP audited checklist requirements. It provides effective managed services through its centralized and multi-tenant platform to help enterprises procure, automate, orchestrate, secure, and manage AWS cloud resources.

In order to implement security controls and automate maintenance, we augment our offering through a continuous learning and certification program for our engineers and experts, including those managing security on the cloud. The Services we manage for the AWS cloud offers significant operational cost savings — the true measure of success for cloud adoption programs.

Conclusion

Organizations are looking for partners who can leverage cloud to deliver value across services rather than just managing it. While traditional IT support has a lights-on approach with standard operating procedures, managing systems on the AWS cloud is about more than merely maintaining components, but using the full capabilities of AWS.

The AWS Managed Services Program (MSP) is about utilizing cloud resources cost-effectively by constantly upgrading to new services that are launched from AWS. This model offers templates, code automation, orchestration, better security and governance, and visibility into usage analytics. With these capabilities, organizations can define new ways of consuming services, achieving significant cost savings, and improving business operational efficiency.

It is imperative for organizations to adopt a strategic approach when selecting an MSP to handle their business operations through AWS. The right MSP is one that can provide enhanced automation, a 360 degree view, and continuous monitoring with the ability to integrate new technologies into the service suite, thereby optimizing the consumption of resources.

The Infosys Service Assurance Suite addresses requirements of next-generation MSPs for the AWS cloud, enabling companies to accelerate cloud adoption across the enterprise.

About the Authors

Soma Sekhar Pamidi – Principal Technology Architect – Cloud, Infrastructure & Security, Infosys

Soma Sekhar Pamidi has 20+ years of experience in the area of Cloud and IT Transformation. In his current role, he is responsible for public cloud transformation practice developments & leads service delivery and teams of enterprise architects & principal consultants to acquire new clients/new businesses with existing clients and leads successful delivery of multiple large cloud & infrastructure transformation engagements.

Ashish Kumar – AVP and Global Sales Lead (AWS Cloud) – Cloud, Infrastructure & Security, Infosys

Ashish Kumar has 22+ years of experience in the areas of Cloud and IT Transformation. A trusted advisor and strategic partner to senior leaders at Fortune 500 enterprises to help improve their organizational effectiveness & efficiency. In his current role as AVP and Practice Leader for CIS Unit (Cloud, Infrastructure and Security) is responsible for driving business growth for AWS Cloud services (globally) and revenue growth for overall CIS services and solutions in the Americas (west) region.

For more information, contact askus@infosys.com

Infosys®
Navigate your next