CHANGE MANAGEMENT IN AWS HYBRID ENVIRONMENT

Change management in AWS Hybrid Environment is more than just a checklist item. It's about harmonizing the apparently conflicting DevOps goals of performing rapid iterations and fast release cycles while maintaining infrastructure availability. In hybrid cloud environments, IT assets become programmable resources and automation toward continuous integration, delivery, deployment and release allows DevOps organizations to meet customer demands iteratively. The inflexibility and constraints of finite infrastructure resources are eliminated and traditionally siloed functional groups within Devs, Ops and QA are empowered to perform changes within highly automated environments.

Failure to manage changes in the cloud can cause cascading repercussions that reverberate across the internal organization as well as the wider customer-base. This AWS outage incident is a prime example where a developer accidently deleted a piece of code that affected how the infrastructure balanced IT workloads between applications and the underlying hardware. Several AWS customers faced 4.5 hours of outage – a significant loss considering the cost of downtime for large enterprises averages nearly $700,000 per hour!

(This tutorial is part of our AWS Guide. Use the right-hand menu to navigate.)

Change Management – The Definition

Change management refers to procedures applied to the changes in order to ensure smooth transition and desired outcomes. In the discipline of IT service management, the concept refers to controls, procedures and standardized methods applied to changes associated with IT service assets and configurations.

The goal of ITSM change management is to reduce IT infrastructure incidents while responding to changing business requirements of the IT services. Ideally, all changes should be thoroughly evaluated, tested and authorized within controlled environments. As a result, unplanned outages, unauthorized changes and project implementation delays are avoided.

This BMC guide on ITIL Change Management provides detailed overview of the framework, best practices, strategies and processes involved in making change management work for your organization. For now, we shall explore what makes change management different in AWS hybrid cloud environment and the associated best practices:

Taking Care of Change Management in the AWS Hybrid Environment

With the introduction of AWS stack into the IT infrastructure, organizations need to integrate several controlled change and configuration management practices based on new security, audit and compliance requirements of the hybrid cloud infrastructure. The significance of these requirements enhances when the AWS stack is used for production environments considering its impact on IT operational and change management processes.

Consider the case of audit and compliance to HIPAA regulations that require visibility into data processes and changes that take place at the infrastructure level. A right set of solutions will be required to provide visibility into the AWS stack in the same way as traditional on-premise firewall. These solutions should accurately analyze and understand the security stance that protects your data. The visibility capability should encompass all security rules that protect data across each AWS instance, in context of mapping between multiple security groups that span across on-premise and AWS cloud infrastructure.

The ability to search and analyze different security protections across the hybrid stack will be equally important to provide holistic compliance reporting. Once that information has been taken care of, organizations also need the ability to perform changes to security group rules that take place in the hybrid infrastructure. Again, changes to individual instances or their mapping to specific security groups can have a ripple effect on how data is protected across the hybrid infrastructure and how compliance is maintained.

In context of DevOps, many configuration changes take place automatically and therefore, proactive alerting and monitoring of those events is critical to perform appropriate security procedures or improvements. In addition to AWS tools such as CloudWatch and CloudTrail that automate the process of tracking and reacting to these changes, tools such as BMC can augment these change management capabilities for specific audit and compliance requirements related to the AWS hybrid stack including PCI, HIPAA and SOX.

From an infrastructure perspective, DevOps teams need to consider the following concepts as the new approach toward change management in AWS hybrid environment:

- Managing Amazon Machine Images: When AWS virtual appliances are created, updated or patched, AWS can launch new user permissions, device mapping and configurations as predefined and programmatically. The associated configuration management agents can be used to track the resulting impact on compliance, security stance and performance of the infrastructure.
- Automatic vs Manual Configurations of Instances and OS: When the instance is launched, it can be automatically configured at launch or incorporate manual configuration changes later. This

capability is particularly important considering the need to maintain consistent change management policies within the scalable and automated cloud instance provisioning systems. The same requirement holds for OS credentials. How do you govern changes to OS credentials when new server images are launched or terminated?

- Managing Applications as Homogeneous Workloads: The AWS hybrid infrastructure environment allows organizations to decouple applications from the underlying infrastructure. As a result, DevOps organizations can de-conflict changes between application iterations and infrastructure in terms of code releases, time and frequency of the releases. The instances can then be automatically and dynamically provisioned depending upon the existing usage demand and predictable usage patterns. For instance, users can dynamically add servers to autoscale groups for improved application management.
- Configuring OS Firewalls to Monitor Instances: As explained earlier, organizations must monitor and manage changes in OS firewall configurations to identify anomalous or unauthorized changes. Ideally, internal configuration management solutions can integrate AWS instance related changes without necessitating substantial modifications.
- Infrastructure-Aware Applications: Change control and infrastructure management are two distinct and independent processes in traditional infrastructure environments. It takes several independent infrastructure changes to perform individual deployments, and then the infrastructure tends to remain static until the next deployment change. With the introduction of the AWS stack, infrastructure changes can take place dynamically based on usage demand to support the varied business and technical functions of the application. Change management therefore becomes an ongoing process since infrastructure changes happen rapidly and with high frequency. As such, all changes should be tracked back to specific user stories. This approach ensures that the unused instance resources are terminated and therefore don't add to the cost when they are not required or running.
- Automation and AWS Service Discovery: Managing change in traditional infrastructure environments requires organizations to understand the complex nature of the underlying resources. With AWS Service Catalog, organizations can provision resources without having to deal with the complexity involved. As a result, the change management process improves significantly. DevOps teams can apply predefined service templates based on organizational policies and auto-approve instances and the resulting known changes as provisioned from the AWS Service Catalog. Since not all required services may be included in the Service Catalog portfolio, organizations may need to enforce strong policies and rules through automation to rapidly facilitate approved infrastructure changes – such as issuing alerts when AWS Lambda instances are launched without tags. Essentially, automation of change management processes will be critical to effective change management in AWS hybrid environments.

In context of DevOps, this list is not exhaustive. Change management is not just a tooling practice but also part of the culture and processes. Technology capabilities around automation and proactive monitoring should empower organizations to manage changes before they impact users. Change management capabilities should match and capitalize on the flexibility and scalability of AWS hybrid infrastructure to improve delivery pipelines, eliminate impactful incidents before they occur and make the IT infrastructure operate smoothly. All of this should be done in a repeatable and automated format as much as possible to ensure that DevOps processes align with changing customer requirements for application availability, performance and security.