RED HAT

Automation's vital role in securing cloud environments

The scale of today's IT operations demands an everything-as-code approach combined with automation

Mark Anderson
Red Hat

Government agencies are consistently being asked to "do more with less," and automation is critical to helping them succeed. When automation is used to handle repetitive processes, it frees up time for government employees to focus on being innovative and mission-focused — allowing for a true win-win situation.

Managing and securing a mix of on-premises systems and private or public clouds presents challenges that can be exponential. If agencies don't have a predictable path and pattern through which they execute in these environments, they could face major challenges. However, by utilizing an everything-as-code approach, with configuration as code being a core tenet, agencies can alleviate some potential burdens. It means thinking about how to approach operations in a way in which everything is configuration controlled, written down and executed as code without exception.

> Managing and securing a mix of on-premises systems and private or public clouds presents challenges that can be exponential.

When agencies do this, they can gain significant benefits, including the ability to log modifications to operations, compare and contrast against previous versions, and roll back to a previous version if an operation fails the testing process. In addition, agencies can replicate disparate environments and create a baseline and variances for use cases or needs for a specific cloud or on-premises environment. The approach also boosts agencies' internal collaboration capabilities, which can lead to more innovation.

A scalable, end-to-end automation platform

Another vital element of security is making sure the correct patches or mandates are deployed and upheld. Automation provides that consistency across the enterprise and allows agencies to track and monitor vulnerabilities and threats. With the use of a tool like Red Hat Ansible Automation Platform, all those activities can happen in one consistent interface. Red Hat's scalable, end-to-end platform can be used to configure systems, deploy software and orchestrate advanced workflows.

With Ansible, agencies can also set up proxy accounts that have limited access to specific environments to ensure no person has access to all systems, thereby reducing insider threats. Those proxy accounts allow organizations to add parameters around who has access to these systems and to track and maintain a log of who has scheduled and run updates. The latter capability can be vital when doing a root cause analysis of a security incident to provide necessary information for auditing purposes.

iStock

From on-premises to the cloud and out to the edge

Automation is not just for security and patching; it can be applied to a wide variety of situations. Expanding on the everything-as-code approach, agencies should also consider application development and deployment. Development is a good use case because the setup and configuration of environments, as well as the build and release processes, require getting code into different deployment environments.

In the past, developers might simply deploy code to a virtual machine, but now enterprise applications span environments from on-premises to the cloud and out to the edge. This is a significant amount of footprint to keep track of, and deployment scenarios become complex. Automation is vital because it allows for reuse and knowledge sharing at scale. It lessens the burden on the operations team because it can compartmentalize specific operations and checks, perform logging, and ensure that all lights are green on the way to production.

Red Hat Ansible Automation Platform simplifies the use of automation throughout the enterprise. It can check that specific application requirements or dependencies are in place and often hand off some operational coding to developers, thus facilitating better collaboration among agencies' development, security and operations teams. ■

Mark Anderson is an associate principal solutions architect at Red Hat and an experienced leader in enterprise systems development, consulting and data architecture.