Get started with compliance for AWS

Defining the need for hybrid cloud automation

A report looking at the state of cloud in today's business world[1] found:

- 80% of organizations have a hybrid cloud strategy.
- 77% of organizations identify managing multiple clouds as a challenge.
- Only 25% of organizations currently use a multicloud management tool.

Reduce hybrid cloud management complexity with automation

An automation platform designed for managing hybrid cloud environments—such as Red Hat® Ansible® Automation Platform—helps your organization orchestrate, operationalize, and govern its IT environments under a single set of processes, policies, and tools to improve consistency, scalability, and speed and reduce human error.

The set-up process for Ansible Automation Platform is simpler than ever now that it is available to purchase in the Amazon Web Services (AWS) Marketplace and ready to deploy directly within AWS.

Before settling into any technology or tool, it is important to first understand its basic functionalities, and Ansible Automation Platform is no exception. Red Hat's self-paced labs are a great way to learn the basics of Ansible Automation Platform and its functions.

Ensure hybrid cloud compliance with Ansible Automation Platform

A vital pillar of managing a hybrid cloud is compliance and using increased visibility in your IT environment to ensure all assets within it adhere to policies and regulations.

Using Ansible Automation Platform as a centralized, customizable management dashboard, your organization can conduct many simple, read-only automation use cases to provide insight into compliance and security of your assets and facilitate simplified remediation steps for concerns that are found—without the risk of production changes.

As a result, your organization can ensure compliance and security in a number of key areas across regions and clouds, including but not limited to enforcing identity and access management (IAM) policies, validating security groups and access control lists (ACL), tracking user activity, and more, while providing a common experience with existing cloud tools across public clouds.

Where to start with compliance use cases

Red Hat recommends all new users of Ansible Automation Platform follow a "crawl, walk, run" strategy. Through this strategy, you first try out simpler, less risky automation use cases that are able to deliver immediate value, before later moving into more complex use cases that provide long-term value.

There are many entry-level, read-only compliance visibility use cases, including:

- **Schedule automated compliance checks.** Ensure all assets within your AWS environment are compliant with all policies and relevant regulations by scheduling automated compliance and security checks. This can be done for a variety of services and assets from AWS by integrating with the platform's compliance and security tools. Learn which services and assets you can automate compliance and security checks on for AWS and how to access and manage schedules on Ansible Automation Platform.

[1] *"2022 State of the cloud report." Flexera, accessed March 2023.*

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

- **Unify permissions across clouds.** Providing a common experience across regions within a cloud environment is an essential step to streamlining and optimizing operations and a key aspect of ensuring compliance and security is followed in a consistent manner. Unifying permissions across regions is a vital piece of that process. Use automation to ensure IAM policies and ACLs are in alignment across your cloud and set up alerts to notify you when permissions overlap or conflict with one another. Learn how to retrieve inline IAM policies on AWS and gather IAM user facts on AWS.
- **Create automated support tickets.** Integrate Ansible Automation Platform with an IT service management (ITSM) platform, such as ServiceNow, to create automated support tickets whenever an asset is found to be out of compliance or not in accordance with security policies. This can be conducted in a read-only manner, whereby a ticket is automatically created but no remediation steps are triggered. As you gain confidence with automation processes, you can set up automated remediation steps that are enacted as soon as a ticket is created. Learn how to set up automated support tickets on ServiceNow.
- **Ensure assets are properly tagged.** Compliance processes within AWS rely heavily on assets being properly tagged. These tags serve as a way of identifying, sorting, finding, and taking action on assets. When these tags are properly applied, optimization measures—such as shutting down certain servers on weekends—can be implemented. By scheduling regular checks, for example, on an hourly basis, you can ensure that someone is alerted when an asset is found without adequate tagging to correct this issue. Learn about tags in AWS.

Although these use cases are a good starting point for your organization as it starts its automation journey, they are simply suggestions, and there are many more entry-level use cases you can explore in these interactive labs for Ansible Automation Platform.

Learn where to start with compliance on Ansible Automation Platform

Try Red Hat's self-paced compliance lab at no cost to learn more.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com