Red Hat

6 reasons to automate Policy as Code for better compliance

Managing governance, risk, and compliance (GRC) across IT solutions is essential for most organizations—especially when artificial intelligence (AI) is in use—but policy enforcement can impact the developer experience, create cross-functional friction, and slow application development. Automation can help address those challenges. Discover 6 key benefits of using automated Policy as Code (PaC) for GRC practices.

1 Boost confidence in critical application compliance

Whether GRC policies are internally or externally mandated, organizations need consistent, defined ways to make certain these practices are implemented throughout operations, from development and test to production and ongoing life cycle management.

By building policies into your infrastructure and Ops as Code (OaC) models, you can feel more confident that your teams are operating within compliance guidelines.

Consider the benefits of being able to automatically:

- Apply cloud resource control checks without manual coding or other manual steps.
- Check for environment-specific policy compliance using specific rules, such as managing use of a firewall port.
- Shorten post-issue root cause analysis cycles.

2 Improve developer productivity

Development teams are under pressure to deliver projects and applications that spur innovation, increase efficiency, and create business value. It is important to apply GRC criteria to these deliverables, but doing so can be frustrating for development teams that need to operate at the speed of the business.

Automated PaC allows developers to:

- Use self-service capabilities so that new environments are automatically provisioned and aligned to policies.
- Add business or security rules automatically, without manual approval.
- Control who is able to complete a specific task, such as creating a cloud instance, based on specific access criteria.

3 Operate consistently at any skill level

Most organizations have a workforce with a range of skill levels. By using automation as part of an Infrastructure as Code (IaC) or OaC model, you can:

- Codify operational knowledge in automation projects so that staff at every skill level operate consistently and within compliance policies.
- Automatically implement the right policies for the right environment, from multiclouds to on-premise to the network edge.
- Mitigate risks, such as errors that result in downtime, security vulnerabilities, and non-standard configurations.

4 Expedite auditing, reporting, and analysis

Auditors and assessors face challenges when working with teams to validate policy adherence. Teams must make time to work with assessors, which can lead to extended working hours and low morale. Cross-functional team collaboration suffers when the process is manual and time-consuming.

Automated PaC can reduce these burdens by:

- Reducing the demand for operations teams to generate manual audit reports.
- Giving assessors the ability to independently report on and evaluate existing policy alignments.
- Eliminating friction points so cross-functional teams can instead collaborate to deliver IT applications and services.

5 Instill compliance across the entire life cycle

To be effective, compliance policies must apply to applications and underlying infrastructure across the entire life cycle, including Day 0, Day 1, and Day 2 operations. Automation can help ease the application of these policies for each key role, including:

- Developers creating automation that, by default, includes applicable policies in provisioning and in test and validation.
- Operations teams validating their solutions using event-driven automation to reapply a standard configuration to a drift scenario.
- Security teams attaching specific criteria to cloud instance creation to help reduce risk across development, test, and production environments.
- Assessors or auditors reporting on the current implementation of policies and identifying gaps.

6 Control cloud costs

Organizations are looking for ways to manage and contain the cost of cloud resources, while also maintaining a focus on security. Automated PaC can help deliver on cloud security mandates while managing costs. Consider these examples:

- Developers can create or use self-service to request a cloud instance; the maximum size of this instance can be predetermined to help control costs.
- Cloud operations administrators can receive notifications if cloud billing exceeds a certain threshold.
- Security professionals can include compliance policies that specify acceptable parameters to help teams work more efficiently.

Learn more

Explore this page to learn more about the benefits of automating PaC.

Watch a webinar

Watch the Automating Policy as Code webinar to discover how to use Red Hat® Ansible® Automation Platform to implement PaC operations.

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	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1 www.redhat.com	00800 7334 2835 europe@redhat.com	+65 6490 4200 apac@redhat.com	+54 11 4329 7300 info-latam@redhat.com

redhat.com