ENTERPRISE AUTOMATION

INNOVATION IN GOVERMENT

TECH SPOTLIGHT SERIES

Security is the number one area of use for enterprise open source software in IT organizations today.

(State of Enterprise Open Source, 2020)

Obtain a **146% ROI** and three month payback with a foundation for building and operating enterprise automation.

(Forrester, 2018)

Reduce unplanned downtime by **53%** with a foundation for building and operating enterprise automation

(IDC, 2019).

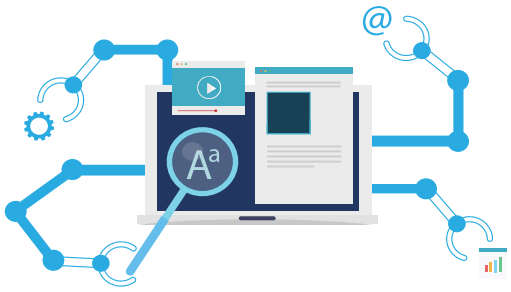
RESOURCES

Automation Made Easy with Red Hat's Jason Ritenour

Automating Government IT Operations

Red Hat Ansible: Security and Compliance Automation

Transforming Federal Agencies with Automation



TECHNICAL SUMMARY

Federal government agencies require robust IT and software capabilities developed to carry out their agency-specific missions and day-to-day operations. However, software development within government organizations comes with a unique set of challenges due to security and compliance regulations. While necessary, the compliance requirements can quickly turn into roadblocks to developing new IT solutions within the federal space, slowing down modernization and burdening developers with a large amount of time-consuming extra work.

Automation of these repetitive, required tasks is emerging as one way to make software development easier for government agencies. However, the process is still full of challenges, including having to work with a specific vendor or cloud provider and the complexity of programming and managing the automation capabilities.

Red Hat gives federal agencies a scalable, enterprise-wide automation solution with the Ansible Automation Platform. Ansible goes above and beyond other automation tools with its intuitive graphical user interface for simple management and vendor-agnostic tooling that makes it easy to switch cloud providers if needed. The platform empowers developers to automate mundane tasks, freeing up their own time to focus on what really matters.

THE CHALLENGE

Numerous standards and requirements, including the Common Criteria for Information Technology Security Evaluation, Federal Information Processing Standards (FIPS) compliance, and the Defense Information System Agency (DISA)'s Security Technical Implementation Guides (STIG), all ensure government networks and software are encrypted and secure. The software development process within federal agencies is frontloaded with setting up and ensuring compliance, creating barriers that developers have to address before and during the software development life cycle.

For example, to ensure DISA STIG compliance, an agency's operating system has to be configured in such a way that it meets the vast STIG requirements which include dictating how the hard drive should be formatted, the strength of passwords, and other technical implementation details. It's up to the agency to scan their system to ensure that all components are meeting the criteria—a largely manual and tedious process.

Red Hat | carahsoft.

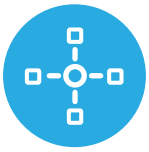
SOLUTION

Automating compliance

Ansible's IT automation capabilities serve as a force multiplier for federal government developers, allowing them to achieve compliance while focusing on more critical tasks. Red Hat Ansible platform helps ensure end users' applications and IT environments become and stay certified with major federal security requirements and provides developers tools to seamlessly facilitate security mitigation, scans, and remediations.

Ansible can be used to initiate a scan of a system and find any components that need to be remediated to remain compliant—a process that normally takes developers several days that can now be conducted in a matter of hours.

The platform's user interface, Ansible Tower, gives users a visual way to manage all the moving pieces. It includes features expected of enterprise-wide solutions, such as corporate single sign-on capabilities, role-based access control, and workflow management.



Utilization across the enterprise

Ansible is a powerful tool for a wide variety of uses—while one organization might use it exclusively for provisioning and managing their network devices, another might not use that capability at all and instead rely on it for application deployment or managing the software development life cycle.

The platform is ubiquitous in its ability to automate nearly anything within an organization, including security scanning, compliance, and remediation. Ansible can also be used for the management of hardware devices within the IT enterprise, whether that's storage, appliances, firewalls, or security appliances.

Flexibility across environments

The Ansible platform can be easily adjusted to handle agency-wide changes in cloud providers, vendors, and policies. Instead of building out programs and software specific to one vendor, Ansible can be used to write a generic script to provision a server for a specific vendor that can be easily switched if something changes.

Like many Red Hat products, Ansible is made more valuable through the community built around the product. A robust repository constantly updated by both users and vendors provides insights into innovative ways the tool can be used to automate operations, providing further flexibility and reducing the labor of developing those solutions.

ENSURE COMPLIANCE THROUGH AUTOMATION

Free up developers' time and keep applications secure with Red Hat Ansible Automation Platform. To learn more about Red Hat, visit **www.facebook.com/redhatinc**, on Twitter at **@RedHatGov**, or at **www.linkedin.com/company/red-hat**.

CONTACT US **RedHat@carahsoft.com** • **877-RHAT-GOV** • **www.carahsoft.com/redhat**

Red Hat | carahsoft.