IT automation in government

Gain more time for innovation that supports your mission

Potential barriers to automation

- Resistance to learning another tool
- Insecure scripting practices
- Reluctance to maintain internally developed automation scripts
- Limited integration with different vendors' devices, applications, and clouds
- Concern that other IT teams will modify carefully developed processes
- Resistance to change

Maximize productivity by minimizing the time spent on repetitive IT tasks

Manual activities consume a large portion of the workweek for government IT teams, at the cost of innovation. Deploying a server or storage can take 1-3 days per person. After provisioning, every device and application requires time-consuming Day 2 activities such as rebooting, security patching, and configuration changes.

Manual IT activities impede government efficiency because they are:

- **Time-consuming:** Patching is especially burdensome. An urgent patch may need to be applied individually to each of 200 virtual machines (VMs). Besides completing patch installation, administrators must also identify and resolve dependencies, coordinate with the networking and application teams, bring down application servers 1 by 1 to maintain service-level agreements (SLAs), and reconfigure load balancers to drain traffic from the server being patched. More time is spent acquiring the skills and tools for each operating system or application being patched.
- **Error-prone:** Many IT teams manually upgrade and patch systems, sometimes following processes with dozens or hundreds of steps. Neglecting to complete any step in these processes correctly can lead to security vulnerabilities or cause outright failure.
- **Neglected:** Unapplied security patches–omitted accidentally or as a tactical decision by busy IT teams–leave government entities vulnerable to attack. According to a study by the Ponemon Institute, 57% of attacks could have been prevented with an existing security patch.[1]
- **Inefficient:** The best use of IT talent is innovation to support your mission, not repetitive activities.

Automation can help IT teams solve these challenges. The time saved by automating one manual task can be used to automate additional tasks or improve software and infrastructure operations in support of your mission.

Bring the benefits of enterprise IT automation to the public sector

Government IT teams can use Red Hat® Ansible® Automation Platform to automate and orchestrate actions across diverse hardware and software products, including infrastructure, network devices, security information and event management (SIEM) systems, edge devices, private and public clouds, and IT service management (ITSM) systems.

Ansible Automation Platform provides end-to-end automation across IT processes and tasks, whether configuring systems, deploying patches and other software, or orchestrating advanced workflows. The platform can be deployed on premise or to your choice of cloud providers, including Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform, with managed versions available to further simplify deployment and operation.

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

[1] *Ponemon Institute and Adaptiva. "Managing risks & costs at the edge." 13 July, 2022.*

Simplify Ansible Automation Platform adoption with hands-on training

Teams can build their Ansible automation skills with In-person and virtual training such as:

- Red Hat Enterprise Linux Automation with Ansible (RH294)
- Network Automation with Red Hat Ansible Automation Platform (DO457).

Part of the platform, Ansible Content Collections are packages of reusable modules, plug-ins, playbooks, and roles for automating IT tasks, such as patching a database or configuring a switch, following a consistent structure in a single portable format. Many of these collections are certified by Red Hat, but IT organizations can also write their own Ansible content to address unique requirements or use cases. Automation tasks can then be executed by administrators in a single step—and reverted to the original configuration just as efficiently.

Designed for complex enterprise environments, Red Hat's automation technology meets the robust requirements of government IT, including:

- **Provides low barrier to entry:** Ansible Automation Platform is used throughout the public and private sectors, so skilled talent is widely available. Unlike traditional code, Ansible content uses human-readable language that is simple to write and read, with self-documenting capabilities. All IT teams—compute, storage, networking, operating system, and application—use the same platform and language.
- **Simplifies security and governance.** Given the number of systems and amount of data that automation code affects, it is critical to verify that code is from a legitimate source. Ansible Automation Platform can centrally store all automation content, whether developed in-house or by third parties. IT teams can select the option to not execute automation content from any source unless it has been digitally signed.
- **Complements existing automation tools:** Rather than replacing existing, product-specific automation tools, Ansible Automation Platform links them to multiply their value. For example, a team using Hashicorp Terraform in an infrastructure as code (IaC) approach can invoke Terraform workflows from Ansible Automation Platform.
- **Integrates with IT systems popular in government:** Compatible with solutions including ServiceNow for ITSM, Splunk for SIEM, and Dynatrace for software observability, Ansible Automation Platform helps IT teams orchestrate their processes for observation, decision making, change management, and configuration management.
- **Gives each team control over its own configurations and processes:** The team that controls an asset also controls access to that asset, helping prevent security risks like configuration drift or unauthorized privilege escalation. For example, an administrator who initiates a process from within Ansible Automation Platform, such as patching a server or upgrading software, does not receive privileged access. Instead, Ansible Automation Platform invokes the actions defined by the team that owns the related asset.
- **Clears the path to authority to operate (ATO):** Red Hat participates with government entities to provide guidance for a straightforward path to ATO. A Security Technical Implementation Guide (STIG) for the Ansible Automation Platform automation controller—the platform's management interface—is available for download from the Department of Defense (DoD) Cyber Exchange STIGs Document Library.

Address common government automation use cases with Ansible Automation Platform

Patching and configuration changes. These tasks can be automated with little effort for a rapid return on investment (ROI).

Provisioning compute or storage resources. In an IDC study, 93% of organizations used more than 1 public cloud provider.[2] As a single tool to provision resources both on-premise and in public clouds, Ansible Automation Platform helps to reduce complexity.

Managing VMs. Use Red Hat OpenShift® Virtualization to run VMs alongside containers on Red Hat OpenShift. Then use Ansible Automation Platform to automate Day 2 VM operations, such as configuration changes, patching, and rebooting. Ansible Automation Platform also simplifies automation of VMware vSphere operations.

Creating self-healing services. Use Event-Driven Ansible, a feature of Ansible Automation Platform, to monitor for defined conditions and respond by executing automated actions. If one node in a cluster stops responding, for instance, Ansible Automation Platform can automatically restart services.

Providing time-limited network access. For example, if a contractor needs access to a system for 24 hours, administrators must close firewall ports after that set time has passed. But if the administrator misses the reminder they set, the port remains open, creating a security vulnerability. With Ansible Automation Platform, administrators can be prompted to enter the ending time when they set up the job, and the ports will automatically be closed at the specified time.

Provisioning limited-time resources. Government IT teams sometimes need to ramp up cloud capability for a short time—for example, in preparation for healthcare open enrollment, tax filing, or military campaigns. But retaining those resources after they are no longer needed can make cloud costs add up fast. With Ansible Automation Platform, the administrator can be prompted to enter the time to release resources during provisioning.

Supporting incident response. Today, government IT security teams typically mitigate threats device by device by applying a patch, closing a port, removing users, and similar approaches. But manual incident response is labor-intensive, and the last device to be remediated remains vulnerable longer than the first. With Ansible Automation Platform, security teams can apply actions to all vulnerable devices at once, with no wait.

Establishing event-driven processes. When integrated with other government systems, Ansible Automation Platform can detect events in those systems and automatically invoke the appropriate action. Examples include fulfilling a VM request initiated through an IT ticketing system, automating server provisioning with IaC, creating accounts for new hires on hardware and software systems, or restoring connectivity between an application server and database.

Success stories: Government IT automation in action with Ansible Automation Platform

A central IT team for a large U.S. city

Before: Patching each of 90 Oracle high availability (HA) servers took 2 hours, and creating Domain Name System (DNS) records took 8 hours. Two Oracle database administrators and one Linux® engineer were on call during the change window, often over the weekend.

Get started with IT automation

- Begin by automating a time-consuming process, then use the reclaimed time to automate other processes. Good starting projects include server provisioning, patching, firewall configuration, and user account creation.
- Review the ticketing system to identify other manual tasks that frequently interrupt IT operations teams.
- Organize hackathons, where different IT teams come together to automate manual processes to meet mission goals.
- Create an automation user group where personnel can share knowledge.

[2] *IDC. "IDC MarketScape: Worldwide Multicloud and Hybrid Cloud Management with Automation 2024 Vendor Assessment." Doc#US52084624, May 2024.*

With Ansible Automation Platform: Server patches take 81% less time, typically less than 45 minutes each. With 90 servers, the IT team saves 112.5 hours per patch—the equivalent of 2 weeks of work time for a full-time employee. Time to create DNS records dropped by 97%, from 8 hours to 15 minutes. In addition, IT staff are no longer required to be available over the weekend.

A law enforcement agency

Before: The agency rebuilt 25 Linux VMs each month, taking 1-2 days of work time for 4 people.

With Ansible Automation Platform: Automated Linux VM rebuilds now take just 30 minutes of time for a single staff member. As a result, the agency has recaptured 1,500 salaried employee hours annually. Service levels have improved because the IT team can fulfill most requests to restore applications in less than a day.

A system integrator working with a major federal government agency

Before: The system integrator received 3-4 daily requests to reboot VMs. With each request, a VMware vCenter administrator had to abandon the current task for 15 minutes to log in, reboot the VM, and enter the activity in the ticketing system.

With Ansible Automation Platform: Requests are fulfilled automatically, freeing up 45-60 minutes daily for the administrator.

Get started with government IT automation

- Discover the top 5 benefits of IT automation for the public sector.
- Sign up for a no-cost trial of Red Hat Ansible Automation Platform.

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