Automation improves resilience for special operations forces

Automating configuration and patching avoids manual errors, strengthens security posture, and makes better use of resources

> "We are desperate to use automated manual processes. It pains me to watch humans spend 2.5 hours programming a server."
>
> **Joe Tragakis**
> Director of Communications Systems and Chief Information Officer, U.S. SOCOM[1]

Executive summary

Manually configuring and patching servers is time-consuming and error-prone. Special operations forces (SOF) can improve security posture and cyber resilience by scaling automation with Red Hat® Ansible® Automation Platform. Automating configuration and patching avoids manual errors, strengthens security, speeds up delivery of new capabilities, and frees staff time for higher value, mission-focused work. Ansible Automation Platform can automate configuration and patching of all SOF hardware and software products. Rather than displacing existing vendor-specific automation tools, it increases their value by making them all accessible through a single interface.

Manual processes come at a cost to the mission

Even if you have already automated network configuration and upgrades, manual processes may still dominate when configuring and patching servers, virtual machines, and cloud resources. Manual configuration and patching impedes the mission because:

- **It is labor-intensive.** Provisioning 100 new servers requires entering the configuration 100 times. An urgent security patch for 200 virtual machines (VMs) needs to be applied 200 times. That time is better spent on higher-value activities such as multi-domain operations (MDO) and meeting the 2027 deadline for the zero trust cybersecurity framework.
- **It is error-prone.** Some upgrades and patches come with 10-page or even 100-page instruction manuals. Neglecting to complete step 47 in a 120-step process can create security vulnerabilities or cause an outright failure.
- **There are much better uses of IT administrator time.** Refocusing administrators from repetitive tasks to more creative work is a better use of their expertise and a morale booster.

Tasks to automate with Red Hat Ansible Automation Platform

- Patching
- Software upgrades
- Initial configuration
- Day 2 operations like reconfiguring or integrating with new systems

Barriers to automation

Perhaps your organization has automated some manual processes, but would like to accelerate progress. A major blocker for many teams is that most automation tools are specific to and work only with the vendor's product. It's impractical for IT teams to learn and manage dozens of tools—one each for VMs, physical servers, individual applications, a single vendor's network devices, etc.

Another barrier is that IT teams need assurance that they can maintain control of their own processes. With so many shared resources, each team is rightly concerned about preventing people and systems from deliberately or inadvertently changing the processes they've carefully built to keep their assets secure and performing optimally.

1 *Special Operations Command Seeks Automation, Modernization, AFCEA, February 29, 2023.*

Solution: open source automation and orchestration

By automating hardware and software configuration and patching, SOF IT teams can make changes once and then push the changes to all or some devices with little effort. If the change doesn't work as expected, reverting the configuration to a known working state is just as simple.

With Red Hat Ansible Automation Platform, SOF can automate configuring and patching of all hardware and software systems and orchestrate advanced workflows. Ansible Automation Platform automates any action that can be initiated from a command-line interface (CLI) or application programming interface (API), for any hardware or software product. Ansible modules are available from 3 sources:

1. Red Hat curates Ansible modules, in collaboration with over 60 independent vendors, and makes them available in the Red Hat Ecosystem Catalog as Ansible Content Collections.
2. Some vendors publish Ansible modules to manage their products.
3. If a vendor doesn't provide a module for a particular product, you can write your own.

Ansible Automation Platform addresses IT teams' concerns that someone from another team will alter their configurations or processes. Administrators who initiate a process from within Ansible Automation Platform—for example, patching a server or upgrading software—never log into the asset itself. Instead, Ansible Automation Platform invokes the actions defined by the team that owns the asset. Only the team that owns an asset can log into it, avoiding security risks like configuration drift or privilege escalation.

Companion tools are pre-integrated

Every Red Hat product release is validated to work with other Red Hat products, saving the time and expense of integrating multiple tools and maintaining those integrations. Use Red Hat Ansible Automation Platform with:

- Red Hat Enterprise Linux®
- Red Hat Advanced Cluster Management for Kubernetes
- Red Hat Advanced Cluster Security for Kubernetes
- Red Hat OpenShift® Data Foundation Essentials
- Red Hat Application Foundations
- Red Hat Quay, a container image registry

SOF use cases for Red Hat Ansible Automation Platform

Time-limited network access

Imagine that a contractor needs access to a system for 24 hours or that a machine-learning model needs to ingest data from an external source for 48 hours. Both scenarios require opening firewall ports. Today, administrators need to set a reminder to close the ports after the time has expired. If the administrator doesn't see the reminder or is busy with another task, the port remains open—a security vulnerability. With Ansible Automation Platform, administrators can specify when the job will end when they initiate it.

Provisioning resources for a limited time

Teams sometimes need to ramp up a capability for a short time—for example, provisioning classified cloud resources to support a special operations forces (SOF) mission. If the administrator neglects to scale down resources after the mission is completed, this could incur unnecessary costs, possibly for weeks or months. With Ansible Automation Platform, the administrator enters both the time to provision the resources and the time to release them.

Incident response

Security teams currently mitigate threats device by device—for example, applying a patch, closing a port, or removing users. That's labor-intensive, and devices remain vulnerable while waiting their turn. With Ansible Automation Platform, you can apply the action to all vulnerable devices at once.

Our credentials

Red Hat is the #2 overall contributor to Cloud Native Computing Foundation (CNCF) projects like Kubernetes.[2]

We represent our customers in key communities, advocating for new capabilities and fixing issues. Using our software to build applications gives SOF organizations early access to the latest innovations in security and performance.

We meet compliance guidelines and standards required for the intelligence community, including FIPS 140-2 and 140-3, Secure Technical Implementation Guidelines (STIG), and more.

Event-driven activities

When integrated with other SOF systems, Ansible Automation Platform can detect events in one system and then automatically invoke defined actions in another system. Here are some examples:

Fulfilling a request for a VM. Building a VM typically takes less than 10 minutes. But the time from request to production can be weeks, sometimes months. The reason is that one team provisions the VM, another assigns an IP address, another the operating system, and still others the applications. Each step in the workflow adds delay. With Ansible Automation Platform, a request for a VM triggers the processes that each team has already defined, executed in the correct order. The VM request can be fulfilled in a day, possibly an hour.

Automating server provisioning with infrastructure as code (IaC). Today, SOF developers may manually provision and manage server hardware, the operating system, storage, and other infrastructure components. However, Defense Information Systems Agency (DISA) and leadership guidance are encouraging transitioning to IaC to improve efficacy, efficiency, and security.[3] When integrated with virtualization tooling from VMware or commercial clouds such as Amazon Web Services (AWS) or Microsoft Azure, Ansible Automation Platform provisions the server automatically by executing the code using the exposed APIs.

Onboarding a new team member. You can automate application activity in response to events. In one example, detecting a new team member in the onboarding system could trigger an automated workflow to create accounts on the appropriate hardware and software systems. Conversely, when detecting that a person has left a team, Ansible Automation Platform could automatically archive or remove access to their accounts. Similarly, the addition of a new application endpoint could trigger an automated workflow to invoke firewall rules, trigger security scanning, or notify teams of a service availability.

Why Red Hat Ansible Automation Platform for SOF

Ansible Automation Platform is effective and simple to adopt because it:

- **Has a STIG.** A Security Technical Implementation Guide (STIG) for the automation controller in Red Hat Ansible Automation Platform is available for download at the Department of Defense (DoD) Cyber Exchange.
- **Requires minimal training.** Ansible Automation Platform is already in use across special operations forces, simplifying adoption.
- **Works with any vendor's products.** Use Ansible Automation Platform to automate configuration and patching of any asset. Modules for more than 60 products are available in our Ansible Content Collections. We curate the content and verify that it's legitimate.
- **Complements existing automation tools.** Rather than replacing existing product-specific automation tools, Red Hat Ansible Automation Platform brings them all onto the same interface, increasing their value. As an example, teams using Hashicorp Terraform for IaC can invoke Terraform workflows from Ansible Automation Platform, the same interface they use for other automated tasks.

2 *Kubernetes Project Journey Report*, Cloud Native Computing Foundation, June 8, 2023.

3 *The Armed Services Wish List for Hybrid Cloud Security*, GovCIO Media and Research, December 6, 2022.

Summary: Automate routine tasks to accelerate special operations modernization

Automating configuration and patching is a simple action with a big impact on IT operations. With Red Hat Ansible Automation Platform, SOF can manage a larger IT estate with the same number of personnel, fulfill requests for resources more quickly, strengthen its security posture, and free staff to work on high-value initiatives like MDO and the zero trust framework.

Learn how Red Hat partners with special operations forces to deliver mission-critical solutions at redhat.com/SOF.

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

redhat.com
#639669_0124