Scale special operations forces with automation

The need for scalable automation

Manual server configuration and patching processes are time-consuming and error-prone. Global public sector organizations, including special operations forces (SOF), must transition to scalable automation solutions to mitigate these issues. Automating configuration and patching avoids manual errors, strengthens security, speeds up delivery of new capabilities, and frees staff for higher-value, mission-focused work. A comprehensive solution including Red Hat® Ansible® Automation Platform can automate the configuration and patching of all hardware and software products, consolidating existing vendor-specific tools into a single, unified interface.

The cost of manual defense processes

Even when network upgrades are automated, configuring and patching servers, virtual machines (VMs) and cloud resources often remain manual processes. These manual tasks directly impede strategic defense objectives by creating:

- Labor-intensive operations. Repetitive manual tasks, like provisioning 100 new servers or applying an urgent security patch to 200 VMs, divert personnel from critical strategic initiatives, such as the Multi-Domain Operations (MDO) Alliance, a NATO ambition for a zero trust cybersecurity framework by 2030.[1]
- Mission-critical error risks. Complex, multistep instruction manuals for upgrades and patches introduce a high risk of human error, which can create significant security vulnerabilities or result in outright system failure.
- Misallocations of expertise. Refocusing administrators from repetitive tasks to more creative work is a better use of their expertise and a morale booster.

Disadvantages of using incohesive automation

Perhaps your agency has automated some manual processes but would like to accelerate progress. A major challenge for many teams is that most automation tools are specific to a single vendor's product. It is impractical for IT teams to learn and manage multiple tools—one each for VMs, physical servers, and individual applications.

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 changing the processes that keep their assets protected and performing optimally.

Open source automation and orchestration solutions

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 does not work as expected, reverting the configuration to a known working state is just as simple.

Ansible Automation Platform allows SOF to automate the configuration and patching of all hardware and software systems and orchestrate advanced workflows. It can automate 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 can be obtained in 3 different ways:

1. Download modules from the Red Hat Ecosystem Catalog. Red Hat verifies and curates Ansible modules, in collaboration with over 60 independent vendors. These modules are available in the Red Hat Ecosystem Catalog as Ansible Content Collections.
2. Acquire modules from software and hardware vendors. Some vendors publish or make available Ansible modules to manage their products.
3. Do-it-yourself (DIY). If a Red Hat or another vendor does not provide a module for a particular product, you can write your own.

Ansible Automation Platform helps address IT teams' concerns about access control for configurations and 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.

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 does not 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 neglect could incur unnecessary costs 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. These manual tasks are 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.

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. Here are some examples:

- **Fulfilling a request for a VM.** Building a VM typically takes less than 10 minutes. But, in many organizations, the time from request to production can be weeks, sometimes months. One team provisions the VM, another assigns an IP address, another the operating system (OS), 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, and they are executed in the designated order. The VM request can be fulfilled in a day, possibly an hour.
- **Automating server provisioning with Infrastructure as Code (IaC).** SOF developers may manually provision and manage server hardware, the OS, storage, and other infrastructure components. However, the Defense Information Systems Agency (DISA) and its leadership guidance encourages transitioning to IaC to increase efficiency and improve security. 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.

Benefits of using Red Hat Ansible Automation Platform for SOF

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

- **Offers security accreditation.** More information about the Security Technical Implementation Guide (STIG) for the automation controller in Red Hat Ansible Automation Platform can be found in Ansible Content Collections.
- **Requires minimal training or retraining.** Ansible Automation Platform is already in use by SOF teams worldwide, simplifying adoption.
- **Is vendor agnostic.** Use Ansible Automation Platform to automate the configuration and patching of an asset. Integrate practices from your core environment to the tactical edge.

- **Complements existing tools.** Rather than replacing existing product-specific automation tools, Ansible Automation Platform brings them all into 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.

Automate routine tasks to speed SOF modernization

Automating configuration and patching is a simple action with a lasting effect 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 in less time, strengthen its security posture, and give staff more time to work on high-value initiatives like MDO and the zero trust framework.

Learn more

Red Hat partners with special operations forces to deliver mission-critical solutions. Contact a Red Hatter for more details.

redhat.com
#3134372_1225