

Skalierung von Spezialeinsatzkräften mit Automatisierung

Die Notwendigkeit skalierbarer Automatisierung

Manuelle Serverkonfigurationen und Patching-Prozesse kosten Zeit und sind fehleranfällig. Globale Organisationen des öffentlichen Sektors, darunter auch Spezialeinsatzkräfte (Special Operations Forces, SOF), müssen skalierbare Automatisierungslösungen implementieren, um diese Probleme zu mindern. Durch Automatisieren von Konfiguration und Patching können manuelle Fehler vermieden, die Sicherheit erhöht, die Bereitstellung neuer Funktionen beschleunigt und das Personal für wertschöpfende, geschäftsorientierte Aufgaben entlastet werden. Eine umfassende Lösung wie Red Hat® Ansible® Automation Platform kann die Konfiguration und das Patching von Hardware- und Softwareprodukten automatisieren und vorhandene anbieterspezifische Tools in einer einzigen, einheitlichen Oberfläche konsolidieren.

Die Kosten manueller Verteidigungsprozesse

Selbst wenn Netzwerk-Upgrades automatisiert sind, müssen die Konfiguration und das Patchen von Servern, virtuellen Maschinen (VMs) und Cloud-Ressourcen oft manuell durchgeführt werden. Diese manuellen Aufgaben behindern die strategischen Verteidigungsziele direkt durch Folgendes:

- ▶ **Arbeitsintensive Operationen:** Sich wiederholende manuelle Aufgaben, wie die Provisionierung von 100 neuen Servern oder das Anwenden eines dringenden Sicherheitspatches auf 200 VMs, halten Mitarbeitende von wichtigen strategischen Initiativen wie MDO-Alliance (Multi-Domain Operations) ab, einem Nato-Ziel für ein Zero Trust Framework für Cybersicherheit bis 2030.¹
- ▶ **Risiken durch missionskritische Fehler:** Komplexe, aus mehreren Schritten bestehende Anleitungen für Upgrades und Patches bergen ein hohes Risiko menschlicher Fehler, die zu erheblichen Sicherheitsschwachstellen oder zu einem kompletten Systemausfall führen können.
- ▶ **Fehlverteilung von Fachwissen:** Wenn sich Administratorinnen und Administratoren stärker auf kreative anstatt auf repetitive Aufgaben konzentrieren, können sie ihr Fachwissen besser nutzen und die Arbeitsmoral verbessern.

Nachteile einer inkohärenten Automatisierung

Vielleicht hat Ihre Behörde bereits einige manuelle Prozesse automatisiert, möchte aber den Fortschritt beschleunigen. Eine große Herausforderung für viele Teams besteht darin, dass die meisten Automatisierungstools spezifisch für das Produkt eines einzelnen Anbieters sind. Für IT-Teams ist es unpraktisch, mehrere Tools zu erlernen und zu verwalten – jeweils eines für VMs, physische Server und individuelle Anwendungen.

Eine weitere Hürde besteht darin, dass IT-Teams die Sicherheit benötigen, dass sie die Kontrolle über ihre eigenen Prozesse behalten können. Angesichts der Vielzahl gemeinsam genutzter Ressourcen liegt es im Interesse der einzelnen Teams zu verhindern, dass Personen und Systeme die Prozesse verändern, die den Schutz und die optimale Performance ihrer Assets gewährleisten.

Open Source-Lösungen für die Automatisierung und Orchestrierung

Durch die Automatisierung der Hardware- und Softwarekonfiguration sowie des Patchings können die IT-Teams von Spezialeinsatzkräften Änderungen einmalig durchführen und sie dann mit geringem Aufwand auf sämtliche oder einige Geräte übertragen. Wenn die Änderung nicht wie erwartet funktioniert, ist es genauso einfach, die Konfiguration in einen bekannten, funktionierenden Zustand zurückzusetzen.

Mit Ansible Automation Platform können Spezialeinsatzkräfte die Konfiguration und das Patching von Hardware- und Softwaresystemen automatisieren und fortschrittliche Workflows orchestrieren. Mit der Plattform lassen sich beliebige Aktionen automatisieren, die über eine Befehlszeilenschnittstelle (CLI) oder eine API für beliebige Hardware- oder Softwareprodukte initiiert werden können. Ansible-Module können auf 3 verschiedene Arten bezogen werden:

1. Herunterladen der Module aus dem Red Hat Ecosystem Catalog: Red Hat verifiziert und kuratiert Ansible-Module in Zusammenarbeit mit über 60 unabhängigen Anbietern. Diese Module sind im Red Hat Ecosystem Catalog als Ansible Content Collections verfügbar.
2. Erwerb von Modulen von Software- und Hardwareanbietern: Einige Anbieter veröffentlichen Ansible-Module zur Verwaltung ihrer Produkte.
3. Do-it-yourself (DIY): Wenn Red Hat oder ein anderer Anbieter kein Modul für ein bestimmtes Produkt bereitstellt, können Sie Ihr eigenes Modul schreiben.

Mit Ansible Automation Platform können IT-Teams ihre Bedenken hinsichtlich der Zugriffskontrolle für Konfigurationen und Prozesse beseitigen. Administrationsteams, die einen Prozess innerhalb von Ansible Automation Platform initiieren, wie etwa das Patchen eines Servers oder das Aktualisieren der Software, melden sich nie beim Asset selbst an. Stattdessen ruft Ansible Automation Platform die Aktionen auf, die von dem Team definiert wurden, das Eigentümer des jeweiligen Assets ist. Nur das Team, das Eigentümer eines Assets ist, kann sich auch anmelden. Dadurch werden Sicherheitsrisiken wie Konfigurationsdrift oder Berechtigungseskalation vermieden.

SOF-Use Cases für Red Hat Ansible Automation Platform

Zeitlich begrenzter Netzwerkzugriff

Stellen Sie sich vor, ein Auftragnehmer benötigt 24 Stunden lang Zugang zu einem System oder ein Machine Learning-Modell muss 48 Stunden lang Daten von einer externen Quelle aufnehmen. In beiden Szenarien müssen Firewall-Ports geöffnet werden. Heute müssen Admins eine Erinnerung festlegen, um die Ports nach Ablauf der Zeit zu schließen. Wenn das Administrationsteam die Erinnerung nicht sieht oder mit einer anderen Aufgabe beschäftigt ist, bleibt der Port geöffnet, was eine Vulnerability darstellt. Mit Ansible Automation Platform können Administrationsteams angeben, wann der Job enden soll, wenn sie ihn initiieren.

Provisionierung zeitlich begrenzter Ressourcen

Teams müssen manchmal eine Funktion für kurze Zeit hochfahren, beispielsweise die Bereitstellung von vertraulichen Cloud-Ressourcen zur Unterstützung eines Einsatzes von Spezialkräften. Wenn das Administrationsteam es versäumt, die Ressourcen nach Abschluss der Aufgabe herunterzuskalieren, kann diese Vernachlässigung über Wochen oder Monate zu unnötigen Kosten führen. Mit Ansible Automation Platform muss das Team sowohl die Zeit für die Provisionierung der Ressourcen als auch die Zeit für die Freigabe der Ressourcen eingeben.

Reaktion auf Sicherheitsvorfälle

Sicherheitsteams minimieren Bedrohungen derzeit für jedes einzelne Gerät, beispielsweise durch das Anwenden eines Patches, das Schließen eines Ports oder das Entfernen von Nutzenden. Diese manuellen Aufgaben sind arbeitsintensiv, und die Geräte bleiben während der Wartezeit anfällig. Mit Ansible Automation Platform können Sie die Maßnahme auf sämtliche anfällige Geräte gleichzeitig anwenden.

Eventgesteuerte Aktivitäten

Wird Ansible Automation Platform mit anderen SOF-Systemen integriert, kann es Events in einem System erkennen und dann automatisch definierte Aktionen in einem anderen auslösen. Hier finden Sie einige Beispiele:

- ▶ **Erfüllung einer Anforderung für eine VM:** Die Erstellung einer VM dauert in der Regel weniger als 10 Minuten. Allerdings kann es in vielen Organisationen zwischen der Anfrage und Produktion Wochen, manchmal Monate dauern. Ein Team provisioniert die VM, ein anderes weist eine IP-Adresse zu, ein weiteres das Betriebssystem und wieder ein anderes die Anwendungen. Die einzelnen Schritte im Workflow verursachen jeweils Verzögerungen. Mit Ansible Automation Platform löst eine Anfrage nach einer VM die Prozesse aus, die das jeweilige Team bereits definiert hat, und sie werden in der vorgesehenen Reihenfolge ausgeführt. Die VM-Anfrage kann in einem Tag, möglicherweise in einer Stunde, erfüllt werden.
- ▶ **Automatisierte Serverprovisionierung mit Infrastructure as Code (IaC):** SOF-Entwicklungsteams können Serverhardware, Betriebssystem, Storage und andere Infrastrukturkomponenten manuell provisionieren und verwalten. Die Defense Information Systems Agency (DISA) und ihre Führungsqualitäten fördern jedoch den Übergang zu IaC, um die Effizienz zu erhöhen und die Sicherheit zu verbessern. Bei einer Integration mit Virtualisierungstools von VMware oder kommerziellen Clouds wie Amazon Web Services (AWS) oder Microsoft Azure stellt Ansible Automation Platform den Server automatisch bereit, indem der Code mit den bereitgestellten APIs ausgeführt wird.
- ▶ **Onboarding eines neuen Teammitglieds:** Sie können die Anwendungsaktivität als Reaktion auf Events automatisieren. So könnte beispielsweise das Erkennen eines neuen Teammitglieds im Onboarding-System einen automatisierten Workflow zur Erstellung von Konten auf den entsprechenden Hardware- und Softwaresystemen auslösen. Umgekehrt kann Ansible Automation Platform, wenn festgestellt wird, dass eine Person ein Team verlassen hat, den Zugriff auf die Konten automatisch archivieren oder entfernen. Ebenso könnte das Hinzufügen eines neuen Anwendungsendpunkts einen automatisierten Workflow auslösen, um Firewall-Regeln aufzurufen, Sicherheits-Scans auszulösen oder Teams über die Verfügbarkeit von Services zu informieren.

Vorteile der Verwendung von Red Hat Ansible Automation Platform für SOF

Ansible Automation Platform ist effektiv und einfach zu implementieren durch:

- ▶ **Sicherheitsakkreditierung:** Weitere Informationen zum Security Technical Implementation Guide (STIG) für den Automation Controller in Red Hat Ansible Automation Platform finden Sie in den [Ansible Content Collections](#).
- ▶ **Minimales Training oder erneutes Training:** Ansible Automation Platform wird bereits von SOF-Teams weltweit verwendet, was die Einführung vereinfacht.
- ▶ **Anbieterunabhängigkeit:** Verwenden Sie Ansible Automation Platform, um die Konfiguration und das Patching eines Assets zu automatisieren. Integrieren Sie Praktiken von Ihrer Kernumgebung bis zum taktischen Edge.

- **Ergänzung vorhandener Tools:** Ansible Automation Platform ersetzt nicht die vorhandenen produktspezifischen Automatisierungstools, sondern vereint diese in einer Oberfläche und steigert so ihren Wert. So können beispielsweise Teams, die Hashicorp Terraform für IaC verwenden, Terraform-Workflows über Ansible Automation Platform aufrufen – also über die gleiche Oberfläche, die sie auch für andere automatisierte Aufgaben nutzen.

Automatisierung von Routineaufgaben für beschleunigte SOF-Modernisierung

Das Automatisieren von Konfiguration und Patching ist eine einfache Aktion mit nachhaltigen Auswirkungen auf IT-Abläufe. Mit Red Hat Ansible Automation Platform können SOF mit derselben Personalstärke eine größere IT-Umgebung verwalten, Ressourcenanfragen in kürzerer Zeit bearbeiten, ihre Sicherheitslage verbessern und ihren Mitarbeitenden mehr Zeit für hochwertige Initiativen wie MDO und das Zero Trust Framework geben.

Weitere Informationen

Red Hat arbeitet mit Spezialeinheiten zusammen, um missionskritische Lösungen bereitzustellen. [Kontaktieren Sie Red Hat](#), um weitere Informationen zu erhalten.



Über Red Hat

Red Hat unterstützt Kunden dabei, ihre Umgebungen zu standardisieren, cloudnative Anwendungen zu entwickeln und komplexe Umgebungen mit [vielfach ausgezeichnetem](#) Support, Training und Consulting Services zu integrieren, zu automatisieren, zu sichern und zu verwalten.

f facebook.com/redhatinc
% @RedHatDACH
in linkedin.com/company/red-hat

**EUROPA, NAHOST,
UND AFRIKA (EMEA)**
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549