借助自动化为特种作战部队添翼加速

对可扩展自动化的需求

手动执行的服务器配置与修补流程耗时冗长且容易出错。全球公共部门机构，包括特种作战部队（SOF），必须过渡到可扩展的自动化解决方案，以缓解这些问题。实现配置与修补自动化可避免人为错误、增强安全防护、加速新功能交付，并使工作人员能够专注于更具价值的任务导向型工作。采用包含红帽® Ansible® 自动化平台的全面解决方案，可实现所有硬件与软件产品的自动化配置和修补，将现有的供应商专用工具整合至统一界面。

手动防御流程的成本

即使网络升级已实现自动化，服务器、虚拟机（VM）和云资源的配置与修补往往仍需手动操作。这些手动操作会直接阻碍战略性防御目标的实现，具体表现为：

- 劳动密集型运维。重复性手动任务（例如置备 100 台新服务器或向 200 台虚拟机部署紧急安全补丁）会占用人员精力，使其无暇顾及关键战略举措，例如多域作战（MDO）联盟，这是北约为实现在 2030 年构建零信任网络安全框架而提出的重要计划。[1]
- 关键任务错误风险。升级与修补工作需遵循复杂的多步骤操作手册，这会大幅提升人为失误的概率，进而可能引发严重的安全漏洞，甚至导致系统故障。
- 专业技能的错位配置。若能将管理员从重复性任务中解放出来，投入更具创造性的工作，不仅能更充分发挥其专业能力，还能提振团队士气。

采用碎片化自动化的弊端

或许您的机构已实现部分手动流程的自动化，但仍希望加速推进进程。许多团队面临的一大挑战在于，大多数自动化工具仅适用于单一供应商的产品。对于 IT 团队而言，学习并管理多种工具（例如虚拟机、物理服务器和独立应用各有一套工具）并不现实。

另一个障碍在于，IT 团队需确保对自身流程的掌控权。面对如此之多的共享资源，每个团队确实需要关注如何防止人员和系统擅自更改流程，从而确保其资产的安全性和最佳性能。

1 *“NATO’s Bold Digital Leap: A SECURE Cloud-Empowered Alliance”（北约的数字化飞跃：构建安全的云赋能联盟），北约盟军转型指挥部，2024 年 12 月 9 日。*

开源自动化和编排解决方案

通过实现硬件和软件配置及修补的自动化，SOF IT 团队只需进行一次更改，之后即可轻松地将更改推送到所有或部分设备。若更改未达预期效果，将配置回滚至已知的可用状态也同样简便。

Ansible 自动化平台可助力 SOF 自动配置和修补所有硬件与软件系统，并编排高级工作流。对于任何硬件或软件产品，该平台能够自动执行可通过命令行界面（CLI）或应用编程接口（API）触发的任何操作。Ansible 模块可通过以下 3 种不同方式获取：

1. 从红帽生态系统目录下载模块。红帽与超过 60 家独立供应商合作，对 Ansible 模块进行验证和整合管理。这些模块以 Ansible 内容集的形式发布于红帽生态系统目录中。
2. 从软件和硬件供应商处获取模块。部分供应商会发布或提供用于管理其产品的 Ansible 模块。
3. 自主开发（DIY）。如果红帽或其他供应商未提供针对特定产品的模块，您可以自行编写。

Ansible 自动化平台有助于解决 IT 团队对配置与流程访问控制的顾虑。管理员通过 Ansible 自动化平台启动流程（例如修补服务器或升级软件）时，无需登录相关资产本身。Ansible 自动化平台将会调用该资产所属团队定义的操作指令。只有资产所属团队才能登录，从而避免配置偏移或权限提升等安全风险。

红帽 Ansible 自动化平台的 SOF 用例

限时网络访问

假设某一承包商需要 24 小时的系统访问权限，或者某个机器学习模型需要用 48 小时从外部源获取数据。这两种情况都需要打开防火墙端口。当前模式下，管理员需要设置一个提醒，以便在时限结束后关闭端口。但如果管理员没有看到提醒或正忙于其他任务，端口将保持开放状态，这会形成安全漏洞。借助 Ansible 自动化平台，管理员可在启动任务时预先设定其结束时间。

限时资源置备

团队有时需要在短时间内快速提升某项能力，例如为支持特种作战部队（SOF）任务而置备涉密云资源。如果管理员在任务完成后未能及时缩减资源规模，这种疏忽可能导致数周甚至数月的不必要开支。借助 Ansible 自动化平台，管理员可同时设定资源置备时间与释放时间。

事件响应

目前，安全团队需逐台设备处理威胁，例如应用补丁、关闭端口或移除用户。这些手动任务耗时费力，而且设备在等待处理期间会持续暴露于风险之中。借助 Ansible 自动化平台，可以一次性对所有存在漏洞的设备执行修复操作。

事件驱动型操作

通过与其他 SOF 系统集成，Ansible 自动化平台能够检测某一系统中的事件，并自动触发另一系统中预设的操作。下面是一些示例：

- **响应虚拟机请求。**构建一台虚拟机通常耗时不超过 10 分钟。但在许多组织机构中，从提出请求到投入生产，往往需要数周甚至数月时间。一个团队负责置备虚拟机，一个负责分配 IP 地址，还有一个负责安装操作系统（OS），另外还有其他团队负责安装应用程序。工作流中的每个步骤都会增加延迟。借助 Ansible 自动化平台，虚拟机请求会触发各团队预定义的流程，并按照指定顺序执行。虚拟机请求可在一天，甚至可能在一小时内完成交付。
- **通过基础架构即代码（IaC）自动置备服务器。**SOF 开发人员可能需要手动置备和管理服务器硬件、操作系统、存储及其他基础架构组件。然而，国防信息系统局（DISA）及其领导层指导方针鼓励向 IaC 转型，以提升效率并增强安全性。通过与 VMware 的虚拟化工具或 Amazon Web Services（AWS）、Microsoft Azure 等商业云平台集成，Ansible 自动化平台还能通过调用公开 API 来执行代码，从而自动置备服务器。
- **新团队成员入职。**您可以实现应用活动的自动化响应，以处理各类事件。例如，当员工入职系统中检测到新团队成员时，可触发自动化工作流，在相应的硬件和软件系统中创建帐户。相反，当检测到人员离开团队时，Ansible 自动化平台可自动存档或移除其帐户访问权限。同样，新增应用端点也可以触发自动化工作流，以调用防火墙规则、启动安全扫描或向相关团队通知服务可用性。

红帽 Ansible 自动化平台为 SOF 带来的优势

Ansible 自动化平台高效且易于采用，原因在于：

- **提供安全认证。**关于红帽 Ansible 自动化平台中自动化控制器的《安全技术实施指南》（STIG）的更多信息，可在 Ansible 内容集中查阅。
- **仅需少量培训或再培训。**全球 SOF 团队已广泛采用 Ansible 自动化平台，显著简化了其应用过程。
- **不依赖特定供应商。**运用 Ansible 自动化平台实现资产配置与修补的自动化。将实践从核心环境整合到战术边缘。

- **与现有工具相辅相成。**Ansible 自动化平台并非要取代现有的产品专用自动化工具，而是将其全部整合至统一界面，从而提升其价值。例如，使用 HashiCorp Terraform 实施 IaC 的团队可以通过 Ansible 自动化平台调用 Terraform 工作流，这与执行其他自动化任务的界面完全一致。

自动执行常规任务，加速 SOF 的现代化进程

自动化配置与修补虽是一项基础操作，却能为 IT 运维带来深远影响。借助红帽 Ansible 自动化平台，SOF 能够以同等人员规模管理更庞大的 IT 资产、缩短资源请求的交付时间、强化安全态势，并使工作人员能够将更多精力投入到 MDO 和零信任框架等高价值战略任务中。

了解更多

红帽与特种作战部队合作，提供任务关键型解决方案。如需了解更多详情，请联系红帽。

关于红帽

红帽通过一流的支持、培训和咨询服务，帮助客户跨环境实现标准化、开发云原生应用，并实现复杂环境的集成、自动化、安全防护和管理。

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编: 100020
8610 6533 9300

红帽官方微博

红帽官方微信

cn.redhat.com
#3134372_1225