INTRODUCTION

Red Hat® Ansible® Automation automates not just traditional IT server and software installations, but expands automation to all IT infrastructure, including areas not covered by traditional IT automation tools. Ansible’s task-based, agentless nature makes it easily applicable to the networking space, and support is included with Ansible Automation for key automation vendors, including Arista, Cisco, and Juniper.

Ansible is minimal in nature, consistent, and highly reliable, with built-in security and a low learning curve for network engineers, operators, and managers. Red Hat Ansible Tower is an enterprise framework for controlling, securing, and managing Ansible Automation with a web user interface (UI) and representational state transfer (REST) application programming interfaces (APIs). Ansible Tower allows network teams to manage automation at scale, with control of how automation is deployed and used, and auditable knowledge about sources and automation outcomes.

ARCHITECTURE AND SECURITY

One of the primary differentiators between Ansible and many other tools in this space is its architecture. Ansible is an agentless tool that runs in a push model—no software needs to be installed on remote machines to make them manageable. Because many network devices do not allow applications or code to be executed on them, Ansible is a natural fit for network operators.

Ansible has numerous connection plug-ins that connect to IT infrastructure. For network automation, Ansible defaults to the secure shell (SSH) command line, but can take advantage of Network Configuration Protocol (NETCONF) and device APIs like Arista eAPI and Cisco Nexus NX-API. The transport method is separated from the automation, simplifying deployment of existing automation onto new device APIs.

Ansible Playbooks require an inventory to run against and credentials to use for logging in to network devices. Ansible Tower makes credential management almost effortless and adds security. Role-based access control (RBAC) means that credentials can be supplied to users to run jobs without access to the credentials themselves. Credentials can be SSH passwords, keys, tokens, or prompts.
Secure and standardize service provider networks

KEY SERVICE PROVIDER USE CASES
Ansible’s simple, task-based nature makes it uniquely applicable to a variety of network automation use cases, including:

**Device-centric network automation**
- Network device configuration
  - Backup and restore device configuration
  - Perform partial or holistic configuration management
  - Provide access control list (ACL) management
- Tactical operations on network devices
  - Upgrade network device operating systems
  - Perform network migration, testing, and configuration validation
  - Apply remediations to address common vulnerabilities and exposures (CVEs)

**Application-centric network automation**
- Software-defined networking (SDN)
  - Integrate Ansible with vendor specific controllers such as Cisco ACI, Cisco NSO, and Arista Cloudvision.

**Cloud-centric network automation**
- Deploy network connectivity between public clouds
- Deploy network connectivity between on-premise networks to any public cloud
- Perform configuration management for virtual private networks (VPNs) and Border Gateway Protocol (BGP) peering, such as Amazon Web Services (AWS) Direct Connect

Ansible supports integrations to existing business workflow management products, including Dynamic Host Configuration Protocol (DHCP), domain name system (DNS) and IP address management (IPAM), collectively known as DDI, and products such as InfoBlox, ServiceNow, and numerous other platforms across multiple vendors.

“[Automation with Ansible] provided us a quick time to deploy new customers. We started off with the first three customers that we deployed [taking] a couple weeks. The next 500 customers took 10 minutes, so we are very excited that we could get that level of automation.”

DON CLARK
DIRECTOR OF BUSINESS DEVELOPMENT, NEC
Currently, over 50 networking platforms are enabled by the Ansible Engine 2.7 release, including:

- A10 Networks
- Apstra AOS
- AVI
- Arista
- EOS
- Cloudvision
- Brocade Ironware
- Cisco
  - ACI
  - AireOS
  - ASA
  - ASA Firepower
  - IOS / IOS XE
  - IOS XR
- Meraki
- NSO
- NX-OS
- Cumulus Linux
- Citrix NetScaler
- Dell
  - Dell OS10
  - Dell OS9
- Dell OS6
- Extreme
  - EXOS
  - NOS
  - SLXOS
  - VOSS
  - Exoscale
- F5 Networks
  - BIG-IP
  - BIG-IQ
- Fortinet
  - FortiManager
  - FortiOS
- HPE ArubaOS
- Huawei CloudEngine
- Infoblox NIOS
- Juniper Junos
- Lenovo
  - CNOS
  - ENOS
- Mellanox ONYX
- MikroTik RouterOS
- NETCONF
- Netvisor
- Nokia
  - NetAct
  - SR OS
- Nuage Networks
- OpenSwitch (OPX)
- Open vSwitch (OVS)
- Ordnance
- Palo Alto Networks
- Pluribus Networks
- Radware
- Ubiquiti EdgeOS
- VyOS
ANSIBLE PLAYBOOKS AND ROLES

Ansible YAML Playbooks consist of plays that define automation across a set of hosts, known as the inventory. Each play consists of multiple tasks, that can target one, many, or all hosts in the inventory. Each task is a call to an Ansible module—a small piece of code for a specific task. These tasks can be simple, such as collecting useful network information like the software version on a target machine or backing up network configurations files. Tasks can also be complex, such as generating and managing entire network configurations or validating connectivity.

Ansible also supports encapsulating playbook tasks into reusable units called roles. The Ansible Galaxy community contains thousands of roles for customizing and building playbooks. Red Hat has written roles for agnostic configuration management, cloud management, and more, that are all fully integrated and ready to implement so network operators can quickly and easily adopt automation.

OPEN SOURCE ANSIBLE VERSUS RED HAT ANSIBLE AUTOMATION

Although the initial software download of community software is free, there are other factors that must be considered. In-house management and maintenance of community code can require dozens or even hundreds of changes to be incorporated each month due to community and internal activity. Every change that is made affects security and compliance. Consider your organization’s ability to handle these updates and security patches. In-house implementation of open source software requires ongoing resources and funds dedicated to support, maintenance, security, and compliance activities.

Red Hat Ansible Automation releases and updates are tested, hardened, and have predictable life cycles. Security patches are provided by the Red Hat Global Support Services team. Red Hat is uniquely positioned to offer holistic end-to-end IT support, from operating system (Red Hat Enterprise Linux®) to automation software (Ansible Automation) to dozens of vendor integrations (AWS, Cisco, Juniper, VMware, etc.), encompassing all your IT, network security, and compliance needs.

CONCLUSION

Red Hat Ansible Automation provides simple, reliable, and robust automation for any component in your network. Ansible Automation provides the support and expertise needed so you can focus on operating and growing your network.

Join Red Hat technical experts for a no-cost, one-day, hands-on Ansible network automation workshop. In the workshop, you will get a comprehensive overview of Ansible, dive into Ansible Tower, and learn how the two components work together. At the end of this workshop, you will have the skills to immediately implement Red Hat Ansible Automation and update and develop new playbooks.

Contact your Red Hat representative for more information.
LEARN MORE

Ansible Automation security examples

- Credential management in Ansible Tower
- OAuth2 documentation
- Integrations with CyberArk

Ansible network automation resources

This site contains video interviews with network engineering leaders, a directory of network integrations, and the form to request a free Red Hat Ansible Tower license.

Ansible Tower trial

Download the Ansible Tower trial for hands-on Red Hat Ansible Automation experience.

Github community

This community contains various repositories with detailed walk-throughs, including building an inventory report of network devices, Infoblox IPAM integration, workshop content, and more.

Ansible Module list

Provides vendor platforms supported by Ansible.

ABOUT RED HAT

Red Hat is the world’s leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.