RED HAT ANSIBLE AUTOMATION USE CASES FOR TELECOMMUNICATIONS SERVICE PROVIDERS

OVERVIEW

71%

of service providers believe that process automation is the most important enabler of long-term operational excellence.[1]

INTRODUCTION

Red Hat® Ansible® Automation provides efficiencies for network infrastructure, operations, and business processes to facilitate and accelerate consumer, business, and mobile service delivery. Key automation use cases for service providers are discussed in the following sections.

NETWORK AUTOMATION

Network automation automates components required to deliver services, both managed and unmanaged, to businesses, consumers, and mobile devices. All services utilize the same network infrastructure, whether it is the datacenter, central office, or the edge. What differs are the specific hardware and virtual components, and locations of those components, that are involved in the actual service delivery. The following list provides examples of components involved in business, consumer, and mobile service delivery:

Service type:

- Business: vCPE, SD-WAN, vFW, vIPS, vLB
- Consumer: vBNG, vOLT
- Mobile: vEPC, vIMS, vPCRF

In addition to network components, many operating support systems (OSS) and business support systems (BSS) processes can be automated to simplify and optimize network management and maintenance. Automation is used so teams can focus on problem solving instead of individual device behavior, for example, command works on one device but not another. Service providers have tens of thousands of devices that are error prone and have access issues. Whenever a new service is deployed, automation can verify that the overall configuration is still valid rather than checking every individual configuration.

For network automation in a multivendor environment, playbooks control configuration—datacenter, wide area network (WAN)—and reduce configuration time and effort. The burden of dealing with intricacies of device-specific implementations is removed from operations and engineering, moving from predominantly node-by-node command line interface (CLI)-driven to application programming interface (API)-driven. APIs are either device-specific or standardized, e.g NETCONF, and work regardless of the underlying connection mechanism. Playbooks can orchestrate changes over a CLI connection and can move from CLI- to API-driven playbook over the life cycle of the device, adjusting naturally without having to retool at the operations level.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

redhat.com

[1] EY, "Digital transformation for 2020 and beyond," 2017. https://www.ey.com/Publication/vwLUAssets/ey-digital-transformation-for-2020-and-beyond/$FILE/ey-digital-transformation-for-2020-and-beyond.pdf

Automating service delivery and network management is as simple as having a playbook for the physical or virtual components involved. Ansible provides supported modules for thousands of devices across many of today's vendors. Playbooks provide abstraction of device-specific implementation details from network management, allowing you to focus on network configuration values.

Ansible functionality addresses key network provisioning use cases for service providers to:

- Integrate with IT service management (ITSM), for example, ServiceNow.
- Manage and configure physical router and switch appliances.
- Manage firewalls.
- Perform zero touch provisioning.
- Change multiple switching and routing platforms.
- Create backups of network equipment within a multivendor environment.
- Validate and audit compliance on multivendor equipment.
- Maintain and deploy software-defined networking (SDN) environments.
- Automate day 2 operations.

Automating legacy VNFs

As telecommunications companies continue to modernize their networks, they have to navigate the challenges that come with legacy systems, including legacy virtualized network functions (VNFs) that rely on local filesystem storage, single server implementations on which all the services run, and manually intensive installations and upgrades. Legacy VNF environments face multiple challenges:

- It is very difficult to automate the applications.
- The VNFs do not scale well.
- Monitoring is manual.
- There is no high-availability, and if a server goes down it has to be replaced manually.
- It is difficult to test and upgrade.

Ansible's power as a configuration management tool can help service providers automate the deployment of legacy VNFs as they shift more of their networks and infrastructure to network functions virtualization (NFV) and the cloud.

SECURITY AND COMPLIANCE

One of the key differentiators between Ansible and many other tools in the automation space is the security provided by its architecture. Installation of agents or other software on managed hosts is not required, allowing Ansible to effectively manage any device with secure shell (SSH). By default, Ansible manages remote machines over SSH, but can take advantage of APIs—for example, Arista EOS eAPI or Cisco NX-OS nxapi—or industry-standard protocols like NETCONF.

By not requiring dedicated users or credentials, Ansible respects the credentials that the user supplies when running. Similarly, Ansible does not require administrator access, providing additional security. Users with credentials that allow access to the control server or source control cannot push content out to remote systems, or otherwise command them, without also having credentials on remote systems. Similarly, by operating in a push-based model where only the needed code is passed to remote machines, remote machines cannot see or affect how other machines are configured.

Continuous monitoring of your multivendor network and infrastructure validates that it is operating as expected, prevents configuration drift, and maintains the ephemeral state of network devices. Red Hat Ansible Automation reads device state and configuration information for all network devices, compares the information to expected values, and reports conflicts and deviations. As a result, you can plan for remediation in the appropriate maintenance window. An assessment and electronic trail verifies compliance with regulations and corporate policies, and mitigates risk and exposure from end-of-life (EOL) or out-of-support components. External International Integrated Reporting Council (IIRC) reporting tools can create reports that detail the outcome of scheduled tasks, such as compliance checks and deployment. And with Red Hat Ansible Tower, you can schedule this validation process on a repeating basis to enforce security policies across all network devices, ensuring that your environment is audit-ready at all times.

Your state of compliance is impacted by anything and everything that is changed, as well as changes that are needed and not performed. Making an improper change and failing to install a recent security patch jeopardize compliance. In addition, all changes must be properly documented for a compliant audit trail. Automating and enforcing the proper change and documentation process is critical for a compliant network and IT environment.

While Red Hat Ansible Engine manages playbook execution, Red Hat Ansible Tower offers a centralized view of which playbooks have been executed in which environment, providing instant visibility and the necessary audit trail. Ansible can also tag resources and store a map of the resources' physical locations in a configuration management database. In addition, Ansible can apply device encryption to all machines that match given criteria, or execute a playbook that locates, eliminates, and documents the disposal of noncompliant data.

Ansible functionality addresses key security and compliance use cases for service providers, including:

- Standardizing and enforcing auditing and compliance.
- Maintaining firewall compliance.
- Centralizing all system-related changes.
- Upgrading driver and firmware.
- Automating remediation and patching of system vulnerabilities, such as Wannacry, Spectre, and Meltdown.
- Detecting system vulnerabilities and needed remediation by gathering Ansible facts and system event logs and exporting the information to system monitoring tools.

CLOUD AND INFRASTRUCTURE

Ansible allows you to model and manage your entire infrastructure as code, including bare metal and virtual machines, operating systems, hypervisors, middleware, and applications, regardless of whether they run in the cloud, in containers, or on site. This includes provisioning, application deployment, and workflow orchestration.

When provisioning, you define the configurations to be automatically deployed and enforced. Ansible automatically discovers infrastructure and uses the policies you define to configure, test, and deploy. By continuously and automatically remediating unplanned changes, Ansible ensures a known state with minimal errors and downtime. Ansible includes thousands of supported modules for automating the technologies in which you have already invested.

ANSIBLE AUTOMATES TECHNOLOGIES YOU USE

OVER 1,200 INTEGRATIONS

CLOUD	VIRT & CONTAINER	WINDOWS	NETWORK	CHAT	MONITORING
AWS	Atomic	ACLs	Arista	Email	Airbrake
Azure	CloudStack	Files	A10	HipChat	BigPanda
CenturyLink	OpenStack	Packages	Cumulus	IRC	Datadog
Digital Ocean	OpenShift	IIS	Bigswitch	Jabber	LogicMonitor
Google	RHEV	Regedits	Cisco	Rocketchat	Monit
OpenStack	VMware	Shares	Dell	Sendgrid	Nagios
Rackspace	**+more**	Services	F5	Slack	New Relic
+more		Configs	Juniper	Twilio	PagerDuty
		Users	Palo Alto	**+more**	Sensu
		Domains	OpenSwitch		StackDriver
		+more	**+more**		Zabbix
					+more

Figure 1. Red Hat Ansible Automation vendor integration examples

For applications, you can automate building, testing, and code deployment to any environment in your infrastructure with auditing and reporting for the entire process. This allows you to eliminate manual image building and script execution and focus on innovation. In addition, Ansible easily integrates with the majority of existing version control systems and many other tools right out of the box.

By modeling infrastructure as code, sequenced infrastructure and application deployments, regardless of where applications reside, are easily orchestrated and monitored from within Ansible Tower. Real-world application stacks involve many servers working together across multiple locations, and the order and timing of steps to be executed is critical. Steps can be limited, easily controlled with conditionals, and based on specified service and machine dependencies for compute provisioning, inventory, and networks workloads. Ansible is capable of easily deploying workloads to a variety of public and on-premise cloud environments, including cloud providers such as Amazon Web Services, Microsoft Azure, Rackspace, and Google Compute Engine, and local infrastructure such as VMware, OpenStack®, and CloudStack.

Ansible functionality addresses key cloud and infrastructure automation use cases for service providers:

- IT workflows
  - Integrating with ITSM, for example, ServiceNow
  - Building virtualized servers and maintaining virtual machines (VMs) in supported hypervisors
  - Managing and adding network interface cards (NICs) for VMs in supported hypervisors
  - Performing create, read, update, and delete (CRUD) operations for security groups and users in lightweight directory access protocol (LDAP), for example, active directory, internet download manager (IDM)
  - Provisioning and automating storage, including block and object, and databases, such as Oracle and MySQL
  - Facilitating extract, transform, and load (ETL) processes
  - Managing certificates
- Application delivery standardization
  - Building virtualized servers and maintaining VMs in supported hypervisors
  - Provisioning and automating storage, including block and object, and databases, such as Oracle and MySQL
  - Deploying and managing Kubernetes and Red Hat OpenShift® clusters

Ansible can also perform many other IT tasks, including talking to representational state transfer (REST) APIs. Playbooks can be written for very specific events and invoked at different times, working with any configuration management system and scripts that you might already have and using one simple language.

CONCLUSION

With thousands of devices, manual configuration and maintenance is no longer an option. Red Hat Ansible Automation allows you to quickly and easily add, remove, and configure physical and virtual devices and processes across service types and architectures. Applications can be automatically built, tested, and deployed, as can the processes that support and ensure consistent configuration, delivery, security, and performance of services across the entire network. For reliable management and deployment anywhere, anytime, Red Hat Ansible Automation is the clear choice.

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.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

NORTH AMERICA	EUROPE, MIDDLE EAST, AND AFRICA	ASIA PACIFIC	LATIN AMERICA
1 888 REDHAT1	00800 7334 2835	+65 6490 4200	+54 11 4329 7300
	europe@redhat.com	apac@redhat.com	info-latam@redhat.com