NetOps Automation platform

opengear

Vendor-Neutral Automation of Network Operations Workflows

The Opengear NetOps Automation™ platform provides a solution for automation of NetOps workflows, enabling the management of the network from a central location, and eliminating the need for human intervention on the data center floor or at the edge of the network.

Leveraging the Lighthouse 5 software platform with the presence and proximity of Opengear management appliances, it uses an open architecture to sequence and coordinate actions; ensure physical security at untrusted sites; manage configuration and image files; and manage and run distributed container applications.

Built as a general-purpose management system, the NetOps Automation platform employs technology components used by the largest hyperscale service providers. It is packaged for enterprises who want to focus on their core competencies - innovating and prototyping new business models - as opposed to committing their resources to engineer automation systems from scratch.

Agile Architecture

Opengear's NetOps Automation utilizes standard tools such as Ansible, Docker and Git to allow rapid development of modules as new challenges appear. The first module available on the platform is a Secure Provisioning application targeting automation of the initial provisioning, configuration management, re-provisioning and disaster recovery of remote infrastructure. Additional modules will become available as the system evolves.

git docker ANSIBLE RESTful API GET PUT POST DELETE

System Components

The Opengear NetOps Automation solution includes the following elements:

- Lighthouse 5 Software
- NetOps Provisioning Module License for Lighthouse 5
- OM2000 Management Appliances
- Resilience Gateway or IM7200 Console Servers (optional, depending on network architecture)

Provisioning Module

The Secure Provisioning Module leverages the new Opengear OM2000 appliances to implement automated provisioning of remote infrastructure at scale:

1 Upon landing at the remote site, a management appliance is able to “call home” over existing IP connectivity or an out-of-band channel, even if the production network is not yet available. The appliance has embedded physical security to ensure the firmware, configuration and VPN keys have not been accessed or tampered with.

2 Relevant image, configuration and script files are automatically pushed from Lighthouse at the central location to the Opengear edge appliances. The appliances become zero-touch provisioning servers to bring up all other network devices at the remote location without local human intervention.

3 During normal operation, the system provides out-of-band emergency access and readiness for disaster recovery, maintenance, outages, and device failures. All files are kept up-to-date at the location where and when needed.

Features & Benefits

Orchestration Capabilities
Automate any NetOps workflow, with improved infrastructure scalability, security and availability

Container Applications
Central management of distributed applications running at the core and edge of the network without need for additional hardware

File Repository
Central management and distribution of firmware, configuration and script files to remote locations

Out-of-Band Cellular Connectivity
Uninterrupted automation of workflows prior to availability of production IP network and during network outages

Trusted Platform Module (TPM)
Embedded physical security ensuring firmware, configuration integrity and secure storage of VPN keys, even when deployed at untrusted locations

Vendor-Neutral Architecture
Use consistent workflows to provision and manage networking devices from Cisco, Juniper, Arista, Huawei, Aruba, Cumulus, Pica, white boxes, etc.

More Information

NetOps capabilities are currently available as beta product to a select group of customers and will be generally available in Q4 2018. To obtain additional information or become a beta-user, please visit: https://opengear.com/NetOps