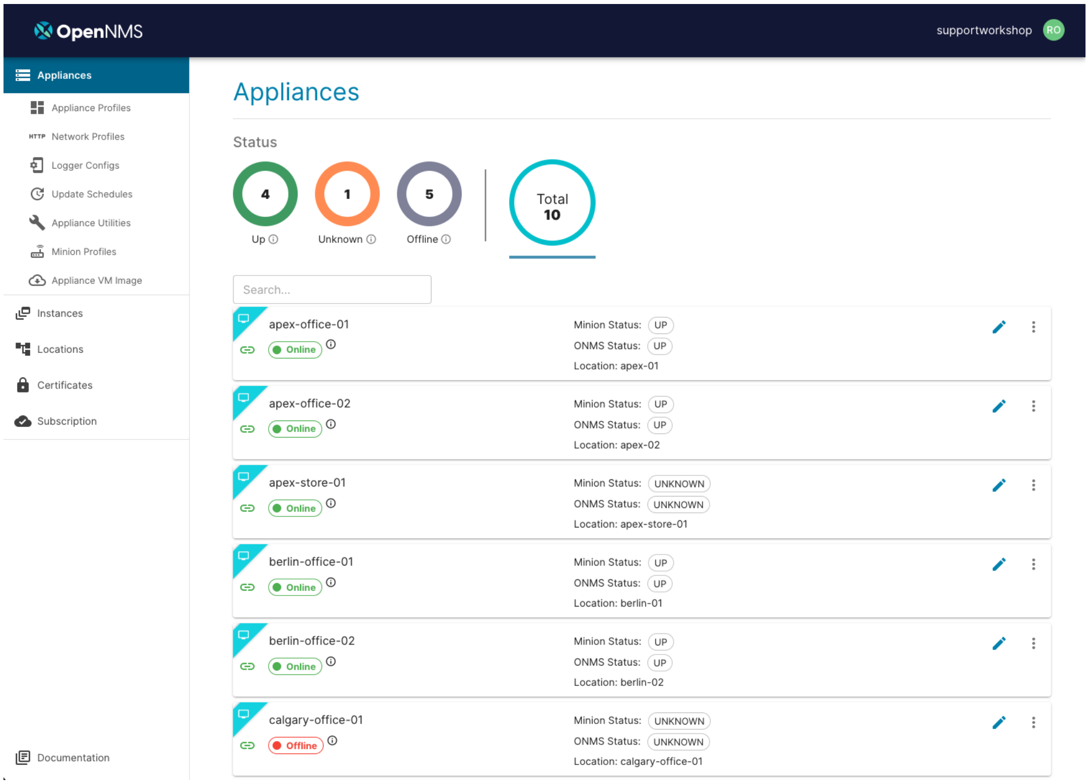
OpenNMS

Minion Virtual Appliance



Appliances

Status

4 Up · 1 Unknown · 5 Offline · Total 10

Appliance		Minion Status	ONMS Status	Location
apex-office-01	Online	UP	UP	apex-01
apex-office-02	Online	UP	UP	apex-02
apex-store-01	Online	UNKNOWN	UNKNOWN	apex-store-01
berlin-office-01	Online	UP	UP	berlin-01
berlin-office-02	Online	UP	UP	berlin-02
calgary-office-01	Offline	UNKNOWN	UNKNOWN	calgary-office-01

Cloud-managed distributed monitoring

The Minion Virtual Appliance is a virtual machine (VM) that helps organizations quickly, reliably, and securely deploy OpenNMS Minions. The OpenNMS Minion collects data from remote or adjacent private networks and sends them to OpenNMS Horizon or Meridian. It acts as both a proxy to process polling tasks and a receiver for SNMP traps, syslog messages, streaming telemetry and flow data. Install, configure, and deploy Minion Virtual Appliances using the OpenNMS Portal.

Automatic and scheduled updates

With the appliance, you never miss a release. The appliance checks regularly to ensure that OpenNMS and Minion versions match. If they do not, it upgrades the Minion Virtual Appliance so that it is synchronized with your OpenNMS core. Appliances automatically update on a schedule that you customize in the portal.

No complicated orchestration

Configure Minion Virtual Appliances from anywhere using the portal. Scripting not required: define profiles, policies, and self-signed certificates for TLS communication. Update schedules and manage subscriptions.

Currently, to update a self-managed Minion, users often write and maintain custom scripts to work with orchestration tools that schedule and manage containers. The Minion Virtual Appliance uses automatic and scheduled updates that you can configure directly in the portal.

High visibility and troubleshooting

Anyone on your team can log in to the OpenNMS Portal to view Minion and appliance logs, status, and statistics. View appliance status at a glance, identify issues, and troubleshoot your deployed Minion Virtual Appliances in one place.

Easy deployment

The OpenNMS Appliance Service makes it easy to deploy one or many Minions. Rather than traversing individual networks or VPNs, you can access the OpenNMS Portal from anywhere with internet access. Deploy a virtual appliance in a remote location or adjacent private network without needing to be physically at the location or install an operating system. Create customized configuration policies in the portal to ensure consistent settings across multiple appliances. The appliance REST API allows for programmatic deployment and configuration of many appliances at once.

Trusted security

The Minion appliance runs only cryptographically signed software, which helps defend against unauthorized code, such as malware or unapproved applications. Docker Notary technology signs our Minion software, and Ubuntu Core uses snap packages to sign operating system software.

Docker and Ubuntu snaps use containerization technologies to isolate and protect applications that run within the Minion appliance. This prevents applications from inadvertently or intentionally harming each other or the underlying Ubuntu/Linux Core operating system. These features make containerized software more secure, resilient, and stable than traditional software packages.

Updates to software used in Minion appliances can be automatically or manually initiated when new versions of Minion Docker images or Ubuntu snaps become available for download. Using the technologies described earlier, appliances install only cryptographically signed, OpenNMS-approved updates.

Our development and QA engineers are skilled in secure software engineering and testing techniques. OpenNMS also engages outside security assessment firms to test components in the Appliance Service and Minion images. Any security issues are prioritized for remediation, based on the associated risk, and then re-tested when a fix is implemented.

OpenNMS Minion Features

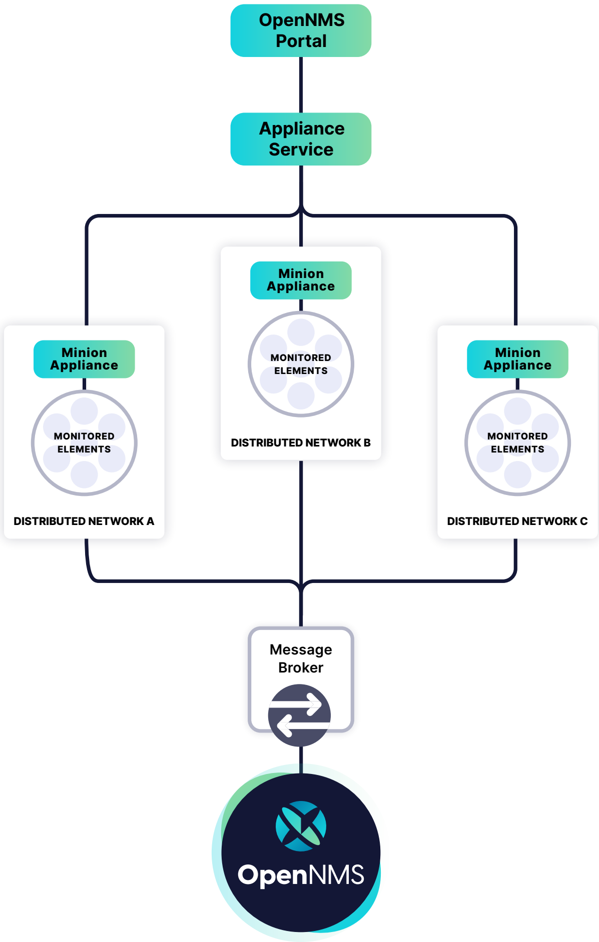
The Minion Virtual Appliance runs the Minion application in a cloud-managed environment, accessible from the OpenNMS Portal.

Minion features we love:

- distributed monitoring
- horizontal scaling of flow data
- compatibility with overlapping address spaces
- application perspective monitoring

How it works

A Minion Virtual Appliance is associated with a monitoring location where its Minion software monitors network infrastructure. The Minion communicates with the OpenNMS core through a Kafka or ActiveMQ message broker. The appliance itself communicates with the Appliance Service, which is hosted on Azure IoT Hub. Users configure, manage, and operate the Minion Appliance through the Appliance portal, accessed via web browser.



Architecture

The Minion Virtual Appliance is a virtual device that runs the Ubuntu Core (UC) operating system. UC is a version of Ubuntu optimized for IoT-native embedded systems that runs software packaged in snaps. It also runs Dominion, the component that manages the Minion, and makes the Appliance Service work.

OpenNMS Minion runs as a container on Docker (which itself is a snap). Snaps provide enhanced security and flexibility for software installation, upgrades, and rollbacks. The Minion Virtual Appliance obtains snap updates from the OpenNMS brand store (powered by the Ubuntu Snap Store). Only verified and approved software packages can be installed.

Snap updates are atomic: either the update is fully applied or it is rolled back. The system will always be in a consistent state. The system can recover from loss of network connectivity or power if an update is in progress.

Snap updates are optimized for network bandwidth: only binary deltas are transferred, not the entire snap.

The Minion Virtual Appliance communicates with the Appliance Service via Azure IoT Hub. The Appliance Service uses IoT Hub to relay system commands such as *update software, reboot*, and Minion configuration settings to the appliance. Likewise, the Minion Virtual Appliance uses IoT Hub to send status, events, logs, and statistics back for display in the portal.

Technical Requirements

Appliance minimum system requirements	2 vCPUs 4 GB RAM 15 GB disk space VMware 7.x
OpenNMS version	Horizon 29+ Meridian 2022+
Supported browsers for portal	Chrome 94+ Firefox 94+ Safari: 14+ Microsoft Edge: 94+
Firewall requirements	The Appliance Service uses Azure IoT Hub infrastructure and Ubuntu core with snap package management. You need to be able communicate with these public services and the OpenNMS infrastructure. For more details, see Security and Firewall Rules.