RELEASE NOTES

LIGHTHOUSE

VERSION 25.04.0

INTRODUCTION

This is a recommended production release for Lighthouse. Please check the Lighthouse User Guide for instructions on how to upgrade your Lighthouse.

DEFINITIONS

Production release: A production release contains new features, enhancements, security fixes and defect fixes.

Patch release: A patch release contains only security fixes or defect fixes for high priority issues.

KNOWN ISSUES

- Session timeout warnings are not currently shown before the user is logged out for inactivity. A fix to provide a prompt as per accessibility guidelines is planned in an upcoming release. [IM-17507]
- When disabling the only non-root admin user, a warning around ensuring another admin user exists first is not always shown. Please ensure another admin user exists before proceeding with the action. [IM-16471]
- Due to a current limitation in Lighthouse, once a subscription is upgraded to either a Core or Enhance, the node filter will no longer return nodes with criteria that matches any NetOps module. It is recommended to push the disable NetOps module templates using the node filter before applying the new subscription. If the subscription has already been applied, it is recommended to push the disable NetOps module templates to all nodes by clearing the node filter and selecting all when pushing config templates. Users may also navigate to the Nodes page and use the “Template Run Status” column to determine which have had Netops templates pushed to them. [IM-17457]

DEPRECATION NOTICE

- Support for DSA-signed SSH keys is being deprecated and will be removed in a future version of Lighthouse.
- Support for the following APIs are being deprecated.

Deprecated Endpoint	Replacement Endpoint
/interfaces GET	/system/network GET
/interfaces/:id GET	/system/network/:lighthouse_id GET
/interfaces/:id PUT	/system/network/:lighthouse_id PUT
/system/external_endpoints GET	/system/network GET
/system/external_endpoints POST	/system/network/:lighthouse_id PUT
/system/external_endpoints/:id GET	/system/network/:lighthouse_id GET
/system/external_endpoints/:id PUT	/system/network/:lighthouse_id PUT
/system/external_endpoints/:id DELETE	/system/network/:lighthouse_id PUT
/system/hostname GET	/system/network/:lighthouse_id GET
/system/hostname PUT	/system/network/:lighthouse_id PUT

25.04.0 (April, 2025)

This is a production release.

Migration Guide

- Lighthouse 25.04.0 introduces support for configuring an external certificate authority (CA).
  - An external CA can only be configured on a deployment that does not have any Opengear devices or secondaries enrolled.
- This release introduces port session management functionalities enabling administrators with the ability to view/terminate active serial port connections from Lighthouse for all nodes, including third party devices, enrolled into Lighthouse. For this feature, a new role permission Port Management has been added under the Nodes and Configuration permission group with the following settings:
  - `FULL ACCESS`: The user can view and terminate serial sessions.
  - `READ-ONLY`: The user can only view the list of Lighthouse initiated serial sessions.
  - `DENY`: The user cannot see the active serial sessions, nor can they terminate any sessions.

  By default, the:
  - `Lighthouse Admin` role is set to `FULL ACCESS`
  - `Node Admin` role is set to `READ-ONLY`
  - `Node User` role is set to `DENY`
  - `Reporter` role is set to `READ-ONLY`

Features

- **External Certificate Authority support** [IM-17445] Lighthouse now supports integration with external certificate authorities for certificate issuance using the Simple Certificate Enrollment Protocol (SCEP) and revocation using the Online Certificate Status Protocol (OCSP). This enhancement addresses customer requirements for compliance, interoperability, and improved security by allowing organisations to manage certificates through their preferred CA.
  Supported external certificate authorities include:
  - Venafi Trust Protection Platform
  - Microsoft Active Directory Certificate Services

  The external CA integration does not currently support certificate renewals and rollover. It is recommended to set your certificate validity to greater than a year. This will be addressed in a following release.

- **Serial Port Connection Status** [IM-17496] This release introduces centralized visibility and control over active serial port sessions across all nodes (Opengear and third-party) enrolled in Lighthouse. It enables administrators and network engineers to monitor, filter, and terminate serial port connections via Lighthouse across multiple nodes.

- **Cell Failover and Health Observability Enhancements** [IM-17822] [IM-17863] Enhanced visibility of nodes in cellular failover mode from the Lighthouse dashboard and across multiple pages. These improvements ensure that failover status is communicated through visual indicators and filtering options available to help users detect failover conditions at scale and take action, if necessary.

Enhancements

- Updated the `cert_manage` CLI command to only run as root or using sudo. [IM-16675]

- Updated the `cert_manage` CLI command to output the number of certificates either scheduled or processed for renewal. [IM-16510]
- Added progress bar to `cert_manage` CLI. [IM-16458]
- Limited the user password to less than 512 characters. [IM-16791]
- Improved the documentation for POST and PUT endpoints for smart groups. [IM-17897]
- Improved the error message to explain node enrollment failure when the user's group contains node or port filters. [IM-14641]
- Added the script `/usr/bin/pre-upgrade_checks.sh` to help assess Lighthouse readiness for upgrade. [IM-15808]
- Improved the Lighthouse upgrade checks to ensure the dependent has enough space for a database dump. [IM-17352]
- Improved robustness of back-end worker processes. [IM-17897]
- Updated the configuration authentication templates to allow LDAP over SSL configuration for NGCS devices. [IM-17502]
- Updated node backup and firmware upgrade cron jobs to use UTC timestamps, ensuring consistent scheduling regardless of local timezone settings. [IM-17832]
- Improved logging of failed conman start/stop commands. [IM-17768]
- Improved the accessibility of the stepper component on the Template and Firmware Upgrade pages. [IM-17506]
- Improved the focus indicator contrast when the light color theme is active. [IM-17509]

Security Fixes

- Updated OpenSSH to 9.9p2 to fix CVE-2025-26465 and CVE-2025-26466 [IM-17835]

Defect Fixes

- Fixed handling of duplicate entries in conman configurations. [IM-17723]
- Fixed the support script `generate-graphs.sh` for generating status history charts. [IM-17774]
- Fixed a tooltip issue that prevented users from moving the mouse pointer onto the text. [IM-17510]
- Fixed a layout issue where long node names caused a horizontal scroll bar to appear on the node details page. [IM-17508]
- Fixed an issue where node firmware upgrade jobs were scheduled incorrectly if local timezone was set to anything other than UTC. [IM-17144]
    - Note: Jobs on affected Lighthouses prior to this update must be cancelled and rescheduled to ensure accurate scheduled times.
- Fixed an issue where netops modules do not show in the UI when using a legacy license. [IM-17797]
- Fixed an issue where the Console Gateway SSH Address could not be updated with a hostname value. [IM-17227]
- Fixed an unexpected 429 error when bulk approving nodes. [IM-14996]
- Fixed an issue where MTU could not be set for network interfaces via ogconfig-cli. [IM-18032]
- Fixed an issue where Lighthouse would show incorrect user name "???" in the logs when ogconfig-cli was used to enable logging. [IM-17858]
- Resolved an issue where users assigned the same node filter, but different port filters can only see ports that overlap. [IM-10930]
- Resolved an issue where the Smart Management Fabric navigation bar item was not highlighted on the Lighthouse OSPF settings page. [IM-17814]
- Resolved an issue where users were able to delete node and port filters that were linked to user groups. A warning message now shows. [IM-13663]
- Resolved an issue where the "SSH Port" for external link specified under network settings was incorrectly treated as an internal SSH port. [IM-17929]

24.12.2 (April, 2025)

This is a patch release.

Enhancements

- Added SSH key authentication as an alternative to password authentication when enrolling third party nodes. [IM-17908]
- Improved data handling from a node during config retrieval. [IM-17886]
- Added the ability to set the default metric for each interface connected to Lighthouse. [IM-17717]

Defect Fixes

- Fixed an issue where NGINX was reloading constantly in the background due to unused enabled IPv6 automatic connections on Lighthouse. [IM-17819]
- Fixed an issue that could cause an upgrade to fail and roll back. [IM-17798]
- Fixed an issue where remote port logs from nodes can cause rsyslogd to crash. [IM-17752]
- Resolved an issue where error messages for the node filter fields were not being read out with screen reader software. [IM-17511]

24.12.1 (February, 2025)

This is a patch release.

Defect Fixes

- Fixed an issue with Cell Health Connectivity Check not working correctly with IPv6 addresses. [IM-17658]
- Fixed an issue on the Network Settings page not displaying Secondary Lighthouse's run time status data correctly. [IM-17574]
- Resolved a display issue on the Lighthouse OSPF Settings page when a description is not set for Secondary Lighthouses. [IM-17672]
- Fixed an issue with Node Backup frequency converting weeks to days incorrectly. [IM-17544]
- Fixed an issue that allowed roles to be deleted while assigned to groups and groups to be deleted while assigned to local users. [IM-16564]
- Fixed an issue to prevent the users and groups configuration templates from being created with duplicate groups. [IM-16342]
- Resolved an issue with the dynamic setting for the number of concurrent API connections on upgrade boot. Any other boot was not affected. [IM-17642]
- Fixed an issue where unexpected Cellular Health data would result in unwanted errors in the Lighthouse logs. [IM-17631]
- Ensured Lighthouse upgrades are rolled back when invalid nginx configuration is found. [IM-17472]

24.12.0 (December, 2024)

This is a production release.

Migration Guide

- This release comes with added functionality to support multiple network interface connections. It is strongly recommended to follow the migration guidelines on our support portal if your deployment is already running additional network interfaces. Skipping the migration steps when upgrading with a second network interface connection may result in exposing Lighthouse on undesired networks or loss of access to Lighthouse. It is important that these steps are done before upgrading.

- The Network Interfaces and Network Settings pages have been consolidated into a single page called Network Settings. This change impacts Role-Based Access Control permissions as follows:
  - Obsolete Permissions:
    - "Network Interfaces" permission previously controlled access to the Network Interfaces page.
    - "Admin and Subscriptions" permission previously controlled access to the Network Settings page.
  - New Permissions:
    - Access to the consolidated **Network Settings** page is governed by a newly introduced permission called "Network Settings", with the following default settings for built-in roles:
      `Lighthouse Admin: Full-Access, Reporter: Read-Only, Node Admin/Node User: Deny`.
      All custom-created roles will be set to `Deny`.
    - While upgrading to 24.12.0 please note that built-in roles will automatically inherit the new "Network Settings" permission as specified above. All custom-created roles will not receive the new permission by default. These roles must be manually updated to ensure proper access control for the Network Settings page.

Features

- **Subscription Changes** [IM-16965]

  Enterprise Edition and Automation Edition subscription including NetOps modules will reach their End-of-Life, making way for Opengear's new commercial model with two new subscription types. Learn more about the changes. This Lighthouse release introduces support for the two new subscription types:
  - Lighthouse Core as a replacement for the Enterprise Edition subscription.
  - Lighthouse Enhance as a replacement for the Automation Edition subscription.
  - Evaluation mode now offers Lighthouse Enhance as the trial subscription.
  - The duration of evaluation mode has been increased from 30 days to 90 days.
  - Node filters now come with an option to filter nodes running NetOps modules.
  - Three new **Disable NetOps** templates provided to cleanup NetOps infrastructure running on OM1200, OM2200 and CM8100.

- **Smart Management Fabric (SMF) Enhancements** [IM-16657]

  Introduced advanced SMF capabilities, resolving routing limitations and improving multi-instance network management for enterprise deployments.
  - Extended **OSPF functionality for networks connected to Lighthouse**, to enable

devices on the management subnet to connect directly to Lighthouse and access devices on networks connected to Opengear Nodes through routed IP.
    - Added support for **multiple network interface connections**, allowing you to specify connections as “reserved” for Lighthouse OSPF configuration.

- **Centralized Network Settings Management for Primary and Secondary Instances** [IM-16657]

  Enhanced user experience to streamline network settings management for multi-instance administration. The new **Network Settings** page allows you to centrally manage hostnames, multiple interface connections, direct access port configurations, and external network addresses for all instances, including secondaries.

- **Custom Login Message** [IM-16099]

  This release introduces support for administrators to configure and display a custom login message on the Login page and login via CLI. The message can include hyperlinks within the text.

Enhancements

- Added the ability to show/hide unmasked password. [CDM-1251]
- Enhanced the search functionality on the Ports page to support searching by node name. [IM-14917]
- Enhanced local syslog storage to be more robust. [IM-16024]
- Added the ability to tag a single resource on the Resource page. [IM-14931]
- Enhanced the View Group Details page to show the filters associated with the user group. [IM-15191]
- Disabled NetOps related services when not in use. [IM-17075]
- Updated the background image on the Login and Password Reset pages. [IM-16919]
- Improved cleanup of SSH authorized keys added by or for remote-only users.[IM-16150]
- Added the ability to tag multiple resources on the Resource page. [IM-15704]
- Improved error message when tagging a non-existent resource. [IM-15568]
- Displayed number of user groups associated to a filter on the: [IM-15197]
    - Resource Filter page and Delete Resource Filter modal.
    - Port Filter page and Delete Port Filter modal.
- Database transfers for secondary upgrades and replication between primary and secondary lighthouses are now compressed. [IM-17351]

Security Fixes

- Upgraded Docker to 25.0.3 for CVE-2024-24557 and Go to 1.22.6 for CVE-2024-24790. [IM-17147]
- Fixed CVE-2015-9542. [IM-16121]
- Upgrade waitress to 3.0.1 to fix CVE-2024-49769. [IM-17337]

Defect Fixes

- Fixed an issue where nodes would never enroll if they were approved too quickly. [IM-17187]
- Fixed a bug where the CRG proxy buttons were incorrectly enabled when SMF was disabled. [IM-17186]
- Fixed an issue that caused OGCS nodes without modems to log SignalStrength errors in the logs when cellular health checks are enabled. [IM-17045]
- Fixed an issue where node-command logs were attached to support reports, leading to

errors due to dangling symlinks. [IM-17044]
- Resolved an issue with including log files in the configuration backup. [IM-17042]
- Fixed an issue where node-info, node-command, node-copy did not process repeated switches correctly. [IM-17040]
- Fixed an issue where SNMP values were reported incorrectly due to service startup order. [IM-17031]
- Resolved an issue where pending nodes were not being listed following an upgrade. [IM-16774]
- Fixed an issue where not all permitted CSR key lengths were supported. [IM-16604]
- Resolved a bug where on support report download, the success message was being shown before the download was complete. [IM-16487]
- Fixed an issue where customers could not upgrade Lighthouses when two tags with the name “Bundle” where specified for an enrollment bundle. [IM-15948]
- Fixed an issue where dependent Lighthouses would attempt to enroll nodes via API. [IM-15580]
- Fixed input length validation on several API. [IM-15419]
- Fixed ‘Console Shell’ access permissions to assign the correct permissions. [IM-14601]
- Resolved an issue where the SHA1 signed cert was being overwritten on upgrade. [IM-17009]
- Resolved a race condition that caused issues with upgrading Secondary Lighthouses from version 24.06.1 to 24.06.2 [IM-17523]
- Fixed an issue to ensure the subscription bar graph uses the Lighthouse system time not the user’s local time [IM-17422]

24.06.2 (September, 2024)

This is a patch release.

Enhancements

- Third-party nodes can now be added as resources for HTTP, HTTPS, and SSH access after they are enrolled in Lighthouse with Smart Management Fabric (SMF) enabled.
- Added additional screen reader navigation landmark.
- Improved link differentiation.
- Added form field labels to aid form comprehension.
- Improved password validation feedback for remote authentication.
- Removed large decorative icons from empty tables.

Security Fixes

- Patched python to fix CVE-2024-7592.
- Patched expat to fix CVE-2024-45490, CVE-2024-45491 and CVE-2024-45492.

Defect Fixes

- Resolved accessibility limitations regarding keyboard and screen reader support.
    - Fixed screen reader navigation, icon, status, warnings, table header and tool tip announcements.
    - Fixed job filter announcements.
    - Fixed focus order for tables and modals.
    - Fixed role definition for tool tips, no longer buttons.
    - Corrected link navigation announcements.
- Disabled 3rd party node Web UI access links from dashboard and nodes pages.
- Allowed scrollbar buttons to be accessed on the local terminal page.
- Fixed refreshing template status updates.
- Allowed mixed case ‘yes’ confirmation for Backup and Restore and Factory reset pages.

24.06.1 (August, 2024)

This is a patch release that supersedes the 24.06.0 release. Please refer to the 24.06.0 release notes section below for the full list of features and fixes.

Security Fixes

- Updated Libarchive to 3.7.4 to fix CVE-2024-37407
- Patched Wget to fix CVE-2024-38428

Defect Fixes

- Fixed an issue where Filters (Smart Groups) were not being migrated correctly when upgrading to 24.06.0.
- Fixed an issue where Lighthouse Web Service failed to start when a DNS server was not configured.
- Resolved an issue on the Resources page where the SSH Access button in the SSH connection modal did not prompt users for their preferred client when using Firefox.
- Updated the RAML documentation to remove unused fields from the Connected Resource Gateway API examples.
- Fixed an issue where the Lighthouse menu pane was overlapping with the main page content.

24.06.0 (July, 2024)

This is a production release.

The Lighthouse User Interface (UI) has been re-architected for an enhanced user experience. This release replaces the Ember UI fully with React. It brings a new color and design scheme, better organization of functionality to improve workflow, clearer indication of form errors, and other improvements. Additionally, it adds auto-refresh capabilities to the UI, presenting real-time data display to the user.

Please refer to the Lighthouse User Guide for more information on the changes in this release.

Features

- **Connected Resource Gateway**

  Connected Resource Gateway (CRG) is a feature that allows users to build and manage a catalog of resources in Lighthouse, that are within the Smart Management Fabric (SMF) discovered networks. CRG allows clientless network access to these resources (via SSH, HTTP, HTTPS proxy), leveraging the IP connectivity enabled by our SMF infrastructure.

  CRG, like SMF, is available as part of the Lighthouse Enterprise Automation Edition subscription and requires Opengear appliances running firmware version 23.10.4 or higher.

- **Resource Tagging**

  Resource Tags is a feature that allows unique identification of serial ports and resources using tags. It improves the ability to separate and tie batches of ports or resources to relevant user groups.

  NOTE: The 'Port Tags' feature has been renamed to 'Resource Tags' in the UI and API, expanding its functionality to cover both Serial Ports and Resources.

Enhancements

- Added support for Certificate Management.
  Certificate Manager enables automatic renewal of Node and other VPN certificates used to authenticate Lighthouse. The `cert_manage` CLI command may be used for additional configuration.
- Added support for AWS Lighthouse to allow login on IPv6-only subnets, enabling access for instances without public IPv4 addresses or any IPv4 addresses. For IPv6-only deployments, ensure the following instance-specific settings are configured:
  - Metadata access: enabled
  - Metadata transport: enabled
  - Metadata version: V1 and V2 (token optional)
- By default the root account is disabled on an AWS image, for new installs. A new account lhadmin has been provided for initial configuration.
- By default, root login is disabled over SSH on an AWS image, for new installs. Existing AWS installs are unaffected, but could leverage the security enhancement.
  For scripts that need to be run by a root user, a Lighthouse admin may `sudo` to assume root permission.
- By default, password authentication is disabled over SSH on an AWS image, for new installs. Existing AWS installs are unaffected, but could leverage this.
- Enhanced error handling for duplicate users created on the Users page.
- Enhanced debugging capability by adding additional logs for upgrades.

- Enhanced the robustness of Multiple Instance Primary/Secondary replication resync scripts.
- Historical system stats are now included in support reports, providing a comprehensive view of system performance over time, and aiding support capabilities.
- Implemented a new script that runs daily and attempts to re-enroll nodes that have previously failed on a secondary Lighthouse. The `retry_secondary_node_enrollments` script can also be manually executed at any time.
- Improved input validation in the Configuration Backup feature to address a vulnerability.
- Improved input validation in the Configuration Restore feature to prevent a potential server error.

Security Fixes

- A number of critical and high Javascript related CVEs have been resolved with the UI upgrade to React. The addressed CVEs include: CVE-2022-2421, CVE-2023-26136, CVE-2023-37466, CVE-2023-37903, CVE-2023-45133, CVE-2021-23424, CVE-2023-45133, CVE-2023-46234, CVE-2022-21222, CVE-2022-38900, CVE-2021-23337, CVE-2022-21213, CVE-2020-7792, CVE-2021-3803, CVE-2022-25883, CVE-2023-32695, CVE-2023-26115.
- Enhanced security by using File Key Encryption to encrypt the database at rest.
- Hardened API security by limiting cookie authentication.
- OpenSSL patched to include fix for CVE-2023-6129.
- Updated glibc to include fix for CVE-2023-0687.
- Updated gnutls to include fixes for CVE-2024-0553 and CVE-2024-0567.
- Updated libuv to include fix for CVE-2024-24806.
- Updated libxml2 to include fix for CVE-2024-25062.
- Updated MariaDB from version 10.7.8 to 10.11.6.
- Updated nginx to include fix for CVE-2023-44487
- Updated OpenSSH from version 8.9p1 to 9.8p1 to include fix for CVE-2024-6387.
- Updated perl to include fix for CVE-2023-47100
- Updated python3-cryptography from version 41.0.6 to 42.0.5 to include fix for CVE-2023-50782.
- Updated redis from version 7.0.13 to 7.0.15 to include fix for CVE-2023-41056.
- Updated runc from version 1.1.4 to 1.1.12 to include fix for CVE-2024-21626, CVE-2023-28642, CVE-2023-27561.
- Updated sqlite3 to include fix for CVE-2023-7104.

Defect Fixes

- Addressed a security vulnerability by isolating sensitive authentication processes, strengthening Brute Force Protection mechanisms, and reducing the risk of unauthorized access to Lighthouse.
- Fixed an issue where a user who was previously locked out still appears as locked out after the lockout timer expires.
- Fixed an issue where an AWS Lighthouse instance would not start when using AWS metadata v2 (IMDSv2) only.
- Fixed an issue where certain configuration files in /etc/ were not replaced correctly during system upgrades and migrations.
- Fixed an issue where invalid port filters could be created.
- Fixed an issue where node configuration changes, such as serial port label updates, were not reflected on a secondary Lighthouse promoted to primary.
- Fixed an issue where running outdated configurators potentially leads to incorrect configurations.
- Fixed an issue where Smart Group (Node filter) or Port Filter queries that are exactly 255 characters long prevent Lighthouse from being upgraded.
- Fixed an issue with failed script templates triggering unexpected behavior for subsequent

script runs.
- Fixed an issue with upgrades failing due to usernames with backslashes (such as domain) in the passwd or shadow files.
- Resolved a bug with access control filters so they are fully enforced.
- Resolved an issue where users without SSH permissions could still reach nodes through SSH jump.
- Resolved an issue where all serial port sessions initiated from Lighthouse were incorrectly reported as “root” on the console server. Sessions now display the correct Lighthouse user who initiated them.
- Resolved an issue where large support reports were not being generated.
- Resolved errors being generated by race conditions during node enrollment. Additionally, this also fixes an issue related to AWS Lighthouse failing to upgrade from version 23.10.2 to 24.02.0.
- Restricted permissions on config files used in Azure deployments.
- Updated RAML documentation for the Bundles endpoint to include ‘tier’ as a required item in the example.

24.02.1 (May, 2024)

This is a patch release.

Defect Fixes

- Resolved an issue where all serial port sessions initiated from Lighthouse were incorrectly reported as “root” on the console server. Sessions now display the correct Lighthouse user who initiated them.
- Fixed an issue where upgrading from LH 23.10.2 to 24.2.0 would fail with an error related to subnet size in certain deployment scenarios.
- Fixed an issue where certain configuration files in /etc/ were not being replaced correctly during system upgrades and migrations.
- Updated RAML documentation for the Bundles endpoint to include ‘tier’ as a required item in the example.
- Fixed an issue with upgrades failing due to usernames with backslashes (such as domain) in the passwd or shadow files.
- Number of config push workers are now dynamically allocated based on system resources to improve performance in larger deployments.
- Fixed an issue with failed script templates triggering unexpected behavior for subsequent script runs.
- Enhanced the robustness of Multiple Instance Primary/Secondary replication resync scripts.
- Fixed an issue causing some upgrades on AWS deployed Lighthouses to rollback.
- Added support for AWS Lighthouse to allow login on IPv6-only subnets, enabling access for instances without public IPv4 addresses or any IPv4 addresses. Additionally, this also fixes an issue related to AWS Lighthouse failing to upgrade from version 23.10.2 to 24.02.0. For IPv6-only deployments, ensure the following instance-specific settings are configured:
    - Metadata access: enabled
    - Metadata transport: enabled
    - Metadata version: V1 and V2 (token optional)
- Addressed a security vulnerability by isolating sensitive authentication processes, strengthening Brute Force Protection mechanisms and reducing the risk of unauthorized access to Lighthouse.
- The upgrade process now includes a check to detect if a CA certificate with a SHA-1 signature is in use, and if so, halt the upgrade. In case the upgrade is essential despite the SHA-1 certificate warning, a mechanism has been provided to override this check. However, overriding is not recommended.
- Fixed an issue where a cron script could run outdated configurators, potentially leading to incorrect configurations in certain cases.
- REST API connection limit is now dynamically increased at boot based on system resources, enhancing performance and availability.
- Fixed an issue where node configuration changes, such as serial port label updates, were not reflected on a secondary Lighthouse promoted to primary.
- Historical system stats can now be included in support reports, providing a comprehensive view of system performance over time, and aiding support capabilities.

23.10.3 (May, 2024)

This is a patch release.

NOTE: This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and upon an upgrade to this version will cause a loss of the VPN to the nodes. Please refer to Lighthouse VPN Certificate Upgrade Failure for additional details.

Defect Fixes

- Addressed a security vulnerability by isolating sensitive authentication processes, strengthening Brute Force Protection mechanisms and reducing the risk of unauthorized access to Lighthouse.
- The upgrade process now includes a check to detect if a CA certificate with a SHA-1 signature is in use, and if so, halt the upgrade. In case the upgrade is essential despite the SHA-1 certificate warning, a mechanism has been provided to override this check. However, overriding is not recommended. Instead a solution has been provided, please refer to Lighthouse VPN Certificate Upgrade Failure for additional details
- Fixed an issue where a cron script could run outdated configurators, potentially leading to incorrect configurations in certain cases.
- REST API connection limit is now dynamically increased at boot based on system resources, enhancing performance and availability.
- Fixed an issue where node configuration changes, such as serial port label updates, were not reflected on a secondary Lighthouse promoted to primary.
- Historical system stats can now be included in support reports, providing a comprehensive view of system performance over time, and aiding support capabilities.

24.02.0 (February, 2024)

This is a production release.

Features

- Smart Management Fabric

Smart Management Fabric (SMF) is a dynamic routing-based IP access solution integrated into Opengear's Network Resilience platform.

This update enhances Lighthouse, offering a unified management framework with a routed IP connectivity overlay, facilitating quick and efficient remote infrastructure access and provisioning. It serves as a cornerstone for automation and monitoring, providing a reliable solution for everyday operations and challenging situations.

SMF is available as part of the Lighthouse Enterprise Automation Edition subscription, and requires Opengear appliances running firmware version 23.10 or higher. For complete usage details, refer to the Lighthouse User Guide.

Security Fixes

- Updated the Cryptography package from 41.0.3 to 41.0.6 to include a fix for CVE-2023-49083.
- Patched OpenSSH 8.9 to include fix for CVE-2023-48795.

Defect Fixes

- Fixed an issue where users authenticated via Security Assertion Markup Language (SAML) can not see web terminal links on the Ports page.
- Fixed an issue to give sudo access only to groups with roles that have shell access. Prior to this change, the netgrp group always provided sudo access regardless of the role. This is no longer the case.
- Removed default LighthouseAdmin permissions from the netgrp group. Netgrp now requires privileges to be configured explicitly. This change only affects new Lighthouse deployments or Lighthouses that have been factory reset.
- Fixed an issue that allowed users to create Port Filters named "New Port Filter".
- Improved detection of failures during upgrade, which is used to trigger a rollback.
- Updated the Roles UI to show a warning when Node Backup permissions are selected without Nodes & Devices (Base) permissions. Also ensured the Node Backup page is available on the sidebar only to users with Nodes & Devices (Base) permission.
- Fixed issues that prevented SAML Identity Provider (IDP) metadata configuration from being updated.
- Added missing /system/time REST API endpoint.
- Fixed an issue where some template push jobs were being re-run if Lighthouse was restarted soon after pushing templates to prevent jobs being queued that would never be processed.
- Fixed an issue where subscription expiry was calculated based on client system time. It now uses Lighthouse system time.
- Resolved an issue with services being terminated on status check via the CLI command.
- Fixed an issue where the Two-Factor Authentication (2FA) input box in the UI was hidden but autofilled for users authenticated via Remote Authentication Dial-In User Service (RADIUS).
- Fixed an issue where the SSL certificate was not being restored correctly from the configuration backup.

- Resolved an issue where after config restore on the primary, dependent instances show incorrect node information via Simple Network Management Protocol (SNMP).
- Fixed an issue where bad Network Time Protocol (NTP) configuration was causing high CPU utilization.

23.10.2 (January, 2024)

This is a patch release that supersedes the 23.10.1 release. Please refer to the 23.10.1 release notes section below for the full list of features and fixes.

NOTE: Before installing Lighthouse 23.10.2, it is necessary to upgrade any currently installed NetOps modules to the latest version 4.4.4, as Yocto has been upgraded. Failure to do so would have an impact on Secure Provisioning deployments. For instructions on upgrading NetOps, refer to the NetOps upgrade instructions.

Defect Fixes

- Resolved a potential serial console issue in Azure deployments.

23.10.1 (November, 2023)

This is a production release that supersedes the 23.10.0 release. Please refer to the 23.10.0 release notes section below for the full list of features and fixes.

NOTE: Before installing Lighthouse 23.10.1, it is necessary to upgrade any currently installed NetOps modules to the latest version 4.4.4, as Yocto has been upgraded. Failure to do so would have an impact on Secure Provisioning deployments. For instructions on upgrading NetOps, refer to the NetOps upgrade instructions.

Defect Fixes

- Fixed an issue with the migration of NTP configuration data when upgrading from older versions of Lighthouse.
- Fixed a database constraint issue around User and Group templates, that caused a migration error when trying to upgrade Lighthouse.

23.10.0 (October, 2023)

This is a production release.

NOTE: Before installing Lighthouse 23.10.0, it is necessary to upgrade any currently installed NetOps modules to the latest version 4.4.4, as Yocto has been upgraded. For instructions on upgrading NetOps, refer to the NetOps upgrade instructions.

Features

- Added support for network traffic mirroring to enable the integration of Lighthouse with an enterprise Intrusion Detection System (IDS).

Enhancements

- Improved the Port Tagging feature to enhance its functionality and user experience.
  - Advanced filter dropdowns for Port Filters now show the name of the applied filter after it has been saved.
  - Users are now able to filter for tags containing apostrophes or quotes on the 'Manage Port Tags' page.
  - Smart Group and Port filter fields are now disabled for users who do not have edit permissions for Smart Groups, ensuring appropriate access control.
  - Manage Ports page enables users to filter ports by Configuration status (Configured/Unconfigured/All).
  - Added the ability to sort Ports table by columns under Monitor>Nodes> Node details.
  - Fixed an issue where create port tag modal would not handle errors correctly until next load of the modal.
- Improved Accessibility
  - Added keyboard navigation accessibility on side menu bar on smaller width screens.
  - Improved screen readabilty of the 'Add node' link as well as 'System and Subscription' and 'Help' menus.
  - Fixed order of focus when tabbing through on a reduced page size.
  - Ensured the UI on the enrollment bundle page now responds correctly to very high zoom levels.
  - Fixed a keyboard navigation issue where the focus didn't correctly return to the opening element when the modal was closed.
  - Fixed a keyboard navigation issue where the focus didn't lock to dropdown menus accessed from the navbar.
  - Fixed accessibility issues in the node firmware upgrade UI.

Defect Fixes

- Resolved a critical issue that was causing a dependent's upgrade process to be repeated recurrently, if the upgrade took too long. More time is now allowed for the upgrade process to complete, and if the dependent's upgrade fails, automatic retries are no longer performed. Users have the option to manually retrigger the upgrade if required.
- Fixed an issue to show the availability of the disk space correctly on the Node Firmware Upgrade page.
- Updated the Web UI to allow Services: HTTPS Certificate to use larger number of bits when generating a Certificate Signing Request (CSR).
- Improved the node-command functionality to ensure that arguments are correctly passed to the node. The new argument `-e` or `--exact` has been added to allow details to be passed to the node exactly. This is particularly beneficial when executing ogcli commands on console servers, enabling the passing of the double-quote character, mirroring the input on

the node.
- Resolved an issue that could arise when simultaneously enrolling two nodes, resulting in the assignment of the same serial number to both certificates. This scenario caused connectivity issues when un-enrolling one device, because the shared serial number would be added to a deny list preventing further connections for the other device.
- Resolved an issue where restoring a configuration backup to a fresh Lighthouse resulted in OpenVPN connectivity disruptions for nodes and dependents.
- Users and Groups templates were limited to 32-character group names, causing incompatibility with Lighthouse groups and console server groups, which allow names of up to 60 characters. We have now enhanced the templates to fully support 60-character group names.
- Fixed an issue with the Users and Groups template editing which was allowing the deletion of all groups and applying the changes whereas the creation of a new template mandates the inclusion of at least one group.
- Resolved an issue with the ‘Use as template’ functionality for user groups where it was not retaining the assigned smart group and port filter information.
- Fixed issues with removing and re-adding node tags.
- Fixed a problem with smart groups where altering the criteria was causing issues with the search functionality.
- Added user input validation for mandatory parameters in HTTPS Certificate and Remote Authentication pages.
- Fixed an issue to prevent the use of ‘New Smart Group’ as the name for a Smart Group to ensure better clarity and organization.
- Fixed an issue where node cell interface status change was not reflected accurately on Lighthouse.
- Included the Docker subnet in the list of conflicting VPN addresses to prevent any overlap with the Lighthouse VPN range.
- Resolved an issue to fix ordering by ‘Status’ in the Jobs table.
- Fixed authentication issues in the operation of the ‘netgrp’ group and ensured remote groups are retrieved when they should be.
- Fixed an issue where the node filter ignores the status when applying a smart group filter.
- Ensured the button to approve a node enrollment is visible but disabled when the subscription is expired.
- Addressed an issue with the processing of cellular health data, where it was failing to handle erroneous data for non-cellular devices resulting in inaccuracies in the cell health dashboard and status updates.
- Resolved an issue to ensure that manually deleting subscriptions will no longer lead to the unintentional deletion of enrollment bundles and their associated nodes.
- Resolved an issue where the dashboard node count occasionally displayed inaccurate values.
- Fixed an issue where some HTTP security headers were not present on all URLs (Content-Security-Policy, X-XSS-Protection, X-Content-Type-Options, Strict-Transport-Security).
- Resolved an issue to ensure SSH and web terminal links on Ports/Console Gateway pages are only displayed to users who have permissions to access the port.
- Fixed an issue where node backup start times are off by the Lighthouse timezone offset.
- Fixed an issue where the hostname was not updating in `/etc/hosts` when changes occurred, such as when the user set it to a new name or when the Lighthouse becomes a dependent instance.
- Fixed an issue where the SNMPv3 Auth/Priv passwords would not be updated correctly when the SNMP service is already running.
- Changed the default hashing of user passwords to use SHA512 (from SHA256).
- Fixed an issue where cell interface addresses would be incorrectly reported in the web UI in some cases.

- Enhanced ping and traceroute tools with full-featured implementations.
- Addressed an issue with Smart Groups where filtering nodes by firmware version was providing incorrect results.
- Increased the maximum length of LDAP Base DN and Bind DN fields to 512 characters.
- Fixed an issue where node firmware upgrade scheduling didn't correctly calculate UTC time.
- Fixed an issue where disabling TLS v1.2 on Lighthouse or on the Operations Manager for the node would prevent remote web UI proxy from working.
- Resolved an issue related to editing multiple enrollment bundles, where attempting to edit the second bundle would result in the page not loading.
- Addressed an issue in which the initial push of a configuration template displayed a success message, even while the process was still running.
- Fixed an issue that would result in multi-selected port tags not being cleared correctly.
- Removed an unused field 'plaintext_password' from the 'users' table and the 'lighthouse-encrypted-backup.sh' script.
- Resolved an issue related to a GET request made to the default_subscription REST API, where it incorrectly attempted to modify data on dependent instances.
- Fixed an error that occurred when enrolling third-party nodes without providing a name.
- Resolved an issue with Smart Groups filtering to display the status of nodes correctly on a dependent Lighthouse.
- Ensured content is displayed on the Config Backup page when clicking Download Backup.
- Disabled the usage of the Enter key for toggling checkboxes, thereby enforcing the use of the spacebar for this operation to maintain a consistent user experience.
- Fixed an issue with firmware selection in the Firmware upgrade modal that occurred when clicking 'Cancel' and then returning.
- Resolved an issue where disabled users were not automatically logged out.
- Streamlined the Smart Group filtering options for string parameters, restricting to 'equals' and 'not equals' only.
- Fixed an issue on the Local Users page when re-selecting a group.

Other

- Removed the CLI tool '`port-tags`'.
- Removed Zapier Zap Integration and Event Notifications following the discontinuation of Zapier support from the previous release.
- Upgraded the Yocto version to Kirkstone.
- Upgraded Python to 3.10.

23.04.1 (July, 2023)

This is a patch release.

Defect Fixes

- Resolved a significant performance issue encountered during an upgrade migration, especially for configurations with many node ports.
- Addressed an issue related to replication when restoring a configuration backup into a primary Lighthouse in a Multiple Instance setup.
- Rectified a memory leak that was occurring when pushing script templates to nodes.
- Fixed an issue to prevent unnecessary re-queuing of configuration push jobs.

23.04.0 (April, 2023)

This is a production release.

Features

- Added Serial Port Tagging support:
  - Allow unique identification of serial ports using tags
  - Improved ability to seperate and tie batches of serial ports to relevant user groups
  - Improved search filters based on serial ports

Enhancements

- Added bulk node approval REST API
- Added bulk node unenrollment REST API
- Added support for proxies in curl
- HTML user manual accessible from Lighthouse
- Improved webUI cookie security
- Improved handling of invalid JSON in request body for all relevant REST APIs
- Removed identifying information in web requests
- Updated Cellular Health Check to use OpenVPN port for Connectivity Test on OM1200, OM2200 and CM8100

Defect Fixes

- Fixed external endpoint population when there's no DHCP address
- Fixed issue with node config template workers interacting with job queue system
- Fixed config validation issues that could prevent successful upgrades
- Fixed an issue where external endpoint addresses could be applied out of order
- Fixed an issue where a read-only (View) icon has the label Edit, which was read out by screen readers
- Fixed an issue where Lighthouse was not handling long group names on enrolled nodes
- Fixed UI issue when creating and editing bundle tags with empty values

Other

- Removed support for Zapier

22.11.2 (January, 2023)

This is a patch release.

Defect Fixes

- Fixed issue where an upgraded Primary Lighthouse sometimes can’t upgrade a Secondary Lighthouse to the same revision.
- Fixed issue where a Primary Lighthouse can be upgraded when a Secondary Lighthouse is currently upgrading or has failed an upgrade.

22.11.1 (November, 2022)

This is a patch release.

Defect Fixes

- Fixed issue where the User Interface was being cached and reverting to a previous state after Lighthouse upgrades on Firefox
- Fixed issue where node enrollments weren’t being counted against Licenses correctly

22.11.0 (November, 2022)

This is a production release.

Features

- Added Mix n Match Subscription support:
  - Allowing up to 2 Subscriptions to co-exist on a Lighthouse to leverage feature sets on different nodes
  - Improved functionality and support for adding and viewing Subscriptions
  - Subscription Assignment system to allow nodes to leverage features from applied Subscriptions

Enhancements

- The Jobs page now has the ability to filter jobs by status (All, Success, Failed, Pending)
- Hardened Secondary Lighthouse upgrading process when encountering upgrade failures
- Improved node-info function to attain node connection states, reflecting what is present on the Lighthouse Dashboard - For further info use the command “node-info -h” in the CLI
- Cellular Health failover status reporting has been improved to be more consistent
- Improved reporting of SIM status when cellular interface is disabled
- Improved node VPN connection processes during Lighthouse start-up
- Improved handling of OGCS cell health response when the modem is rebooting (due to changing SIMs)
- Removed support for old, no-longer-recommended ssh encryption functions
  - Note that these changes do not get applied to upgrading systems
  - To manually apply this change, follow Migration For Outdated SSH Ciphers

Defect Fixes

- Fixed issue where deleting smart groups and managed device filters would delete attached groups. Users now see an error message blocking the process until groups are detached
- Fixed issue where Lighthouse upgrades were failing when users that exist have smart_group_ref unset
- Fixed issue with node upgrade sometimes not displaying firmware filenames correctly
- Fixed issue where pmshell access was missing for users with a managed device filter but no smart group filter (ie. “All Nodes”)
- Fixed issue where skip to main content accessible button did not work for NetOps pages
- Fixed IP address range validation for LHVPN range setting
- Fixed issue where editing group templates can duplicate groups
- Fixed issue where SNMP traps for secondary replication were misaligned with MIBs
- Fixed an issue where cellular IP addresses for NetOps Console Servers would persist after the cellular connection went down
- Fixed certain scenarios for when NetOps Console Servers did not show up on the cell health dashboard
- Fixed issue where non-admin user couldn’t see support report option
- Fixed the permission for read only users to edit smartgroups
- Fixed issue with LDAP configuration validation where the LDAP Bind DN field could not be left blank
- Fixed issue where the Search field on the port logs page was missing
- Fixed issue where external end points for IPv6 were not being populated automatically on Azure Instances
- Fixed issue where you could not drag and drop multiple files onto the Node Firmware file manager

- Fixed issue where Node ID parameter was not part of the free text search

22.Q1.2 (September, 2022)

This is a patch release.

Enhancements

- Accessibility improvements to raise standards of keyboard and screen reader support
- Minor interface and input changes to improve user experience and flow when accessing parts of the UI

22.Q1.1 (August, 2022)

This is a patch release.

Enhancements

- Managed Device Filter parameters can now be combined using AND or OR in the Web UI

Defect Fixes

- Fixed intermittent multi-instance replication issue during upgrade
- Fixed a post-upgrade issue to 22.Q1.0 for remote authentication of groups with upper case characters
- Fixed logging into the Lighthouse UI using 2FA
- Fixed an issue affecting upgrades with a large number of nodes
- Fixed an issue which could result in user sessions being incorrectly logged out when the system is processing multiple requests for the same session

22.Q1.0 (June, 2022)

This is a production release.

Features

- Support for UI driven node firmware upgrades
- Support for CM 8100 nodes

Enhancements

- Accessibility improvements:
  - Improved keyboard navigation
  - Styling changes for focus items
- Increased the timeout for secondary Lighthouse upgrades
- Enhanced performance with better task prioritization
- Improved config validation error messages
- Improved network error handling
- Improved node backup error handling
- Expanded managed device filters support from smart groups to all nodes
- User can be enabled or disabled using ogpasswd without needing to change their password

Defect Fixes

- Resolved issues with events service that could cause it to stop
- Fixed issue where the ‘root’ user could be removed from the ‘admin’ group

21.Q4.2 (March 2022)

This is a patch release.

Defect Fixes

- Fixed issue where NetOps deployments could lose access to node information if the root user was disabled on non-azure deployments
- Fixed issue where NetOps deployments could lose access to node information on the Azure platform due to the root user being disabled
- Fixed an issue which could result in user sessions being incorrectly logged out when the system is processing multiple requests for the same session
- Fixed an issue where a node in the Lighthouse database with an unknown firmware version caused an upgrade to fail and rollback
- Fixed an issue where any users with Unicode characters in their description field could cause users to be locked out of Lighthouse
- Fixed a problem where usernames containing a full-stop/period caused an upgrade to fail and rollback
- Fixed a problem where a misconfigured node serial port could cause an upgrade to fail and rollback
- Fixed issue with missing serial port mode when config retrieving OM devices, this could cause an upgrade to fail and rollback

21.Q4.1 (February 2022)

This is a patch release.

Enhancements

- Enhanced Authentication logging for Lighthouse users logged in with SAML
- Improved Support Report information including AWS Targets
- Improved Monitor Nodes page to now apply user group managed device filters
- Improved node cell health status logic for more clear communication
- Adjusted colour scheme for Node Dashboard
- Disabled SSH links for Lighthouse users logged in using SAML

Defect Fixes

- Fixed issue where node upgrade command did not allow multiple nodes to be selected
- Fixed issue where smart groups did not allow more than 18 entries of criteria
- Fixed issue in RADIUS setup stopping save changes after port field selection

21.Q4.0 (December, 2021)

This is a production release.

Features and Enhancements

- WebUI SAML support added for Single Sign-on Identity Providers: Azure AD, Okta, and OneLogin - Review the 21.Q4 manual for setup instructions.
- Connected ports now displayed on Quick Search page with sorting and free text search support.
- Performance improvement for pmshell load times when the Lighthouse has a large number of nodes/ports.
- Improved failover login behaviour when using high latency remote AAA authentication.
- Lighthouse now detects and prevents duplicate enrolment attempts during node enrolment.
- Added additional support for FQDN usernames when using remote AAA authentication.
- Additional help/error messages added for when the user's browser is using a stale cache of the Web UI.
- Improved the error messaging for issues with 2FA token challenges.
- Added additional integrity checking to the creation of tags for enrolled nodes from bundles.
- Updated the error checking/reporting around LDAP CA certificates.
- Removed a number of static key ciphers from use by the WebUI and node proxies.

Defect Fixes

- Fixed the missing use of the hostname in the syslog for certain system messages
- Fixed refresh issue when accessing node proxies via saved hyperlinks in the Web UI.

21.Q3.0 (September, 2021)

This is a production release.

Features and Enhancements

- Node-upgrade CLI utility improvements and support for Operation Manager series devices
- Improved display of information and upgrade results
- CLI arguments and options preserved for backwards compatibility
- Additional arguments/options:
    - —firmware-file for selecting a specific firmware image instead of specifying a directory to search through
    - —product for selecting nodes by product family
    - —verbose for displaying log information (but not as much as with –debug)
- Added password verification when performing user changes for local Lighthouse users
    - This is applicable for Lighthouses configured to only use local auth
- Usernames including “.” characters can now be used in Lighthouse
- Content Security Policy header has been implemented
- Updated the WebUI display for third party/digi passport nodes to show the node address
- Added support for a configurable remote AAA timeout value via the ogconfig-cli tool
    - Once your AAA auth has been set, use “ogconfig-cli auth.timeout #” to set the timeout in the CLI
- Improvements to Cell Health handling and display of the Failover status for nodes
- Added script to support for bulk-unenrolling of nodes - please contact support if you wish to utilize this script
- Added additional system status information to the Lighthouse support report
- Enabled support for the Carrier Grade NAT IP range (RFC 6598, 100.64.0.0/10) for LHVPN tunnels to Nodes

Defect Fixes

- Fixed an issue in which the default static IPv4 address was left in External Network Address list when the associated network interface is disabled
- Fixed issues with the smart group node-id search that had previously resulted in incorrect results when using the abbreviated id form (i.e. 1 instead of nodes-1) or viewing the results on the Console Gateway page
- Fixed an issue in which the “read_write” SNMP community field could not be cleared once set
- Fixed an issue with generic third party nodes which resulted in the port labels being assigned to the incorrect ports

21.Q2.1 (July, 2021)

This is a patch release.

Defect Fixes

- Fixed issue where Lighthouse couldn’t receive firewall zone data from OM series devices on 21.Q1
- Fixed issue where Lighthouse could use incompatible upgrade files
- Fixed issue where multiple instance enrollment via alternate port still sends traffic to port 443

21.Q2.0 (June, 2021)

This is a production release.

Features and Enhancements

- Upgraded Yocto version to Dunfell
- Deprecated Python 2 in favor of Python 3 on Lighthouse
- Improved monitoring and error notifications for Multiple Instance Lighthouses
- Improved upgrade process and flow for Multiple Instance Lighthouses
- Improved enrollment and unenrollment process of nodes on Lighthouse
- Improved performance of cellular health reporting on Lighthouse
- IMEI, IMSI and ICCID reported for cellular health on UI and through REST API
- Added node ID and port ID to Lighthouse system logs
- Added sorting support through REST API for smartgroups endpoint
- Added sorting support through REST API for jobs endpoint
- Added sorting support through REST API for nodes endpoint
- Improved REST API backward compatibility
- Added MI diagnostics to support report
- Added versions support for Hyper-V powershell install script

Defect Fixes

- Fixed Lighthouse CVE issues
- Fixed issue with free text search not working for IP Addresses on node pages
- Fixed SSL problems with self-signed certs in web UI on Big Sur chrome
- Fixed issue where in 20.Q4.0 third party (Avocent) nodes can't connect with pmshell
- Fixed issue with multiple instance Lighthouse enrollments when the replication_user already exists
- Fixed cross site scripting vulnerability for script templates
- Fixed issue where rest_api_log process was logging with incorrect hostname
- Fixed issue with Lighthouse memory usage info in SNMP (slab memory)
- Fixed issue with enrollment bundle template ordering not being saved
- Fixed issue with LDAP configuration changes not getting saved
- Fixed issue with 7008 configuration not getting updated on Lighthouse
- Fixed issue where LDAP does not fall back to local authentication on failure
- Fixed issue where node-related redis keys are not deleted when node is unenrolled
- Fixed issue where Lighthouse console_gateway API doesn't always return address used for SSH links
- Fixed issue with RADIUS sending incorrect Service-Type
- Fixed issue where changing the node VPN on the Primary instance in a MI cluster does not check for vpn conflicts
- Fixed issue where Lighthouse generates invalid engine ID for SNMPv3
- Fixed issue with cell health when communicating with an OM device that has no modem
- Fixed issue where a user cannot deploy Azure Lighthouse without Public IP Address
- Fixed issue where hitting a node proxy URL when not logged in gives a 401 screen
- Fixed issue where Enrollment Token cannot contain special characters
- Fixed issue where port label with '%' breaks web terminal page
- Resolved Enrollment bundle UI issue for adding Netops modules
- Fixed issue where lh-client-connect script is too slow
- Fixed issue where Lighthouse on AWS becomes unresponsive after upgrading and then factory resetting

20.Q4.2 (May, 2021)

This is a patch release.

Defect Fixes

- Added storage of Azure configuration parameters to allow persistence after factory reset
- Fixed issue where Node Backup may be disabled after upgrading to 20.Q4.0, if it was configured on 20.Q3.0
- Fixed issue where replication on secondaries may be interrupted after promoting a secondary to primary
- Fixed issue where debugging log messages were being logged after enabling remote syslog
- Fixed issues with MI and node enrollment in various firewall configurations (combinations of NAT, external endpoints, alternate ports, etc.)
- Improved log handling of node config retrieval to not log spurious data
- Improved memory footprint by disabling some services if not enabled (eg. Zapier event notification)
- Improved memory usage by cleaning up database entries for old configuration updates
- Improved upgrade process in hosting configurations with non-standard device names (eg. /dev/vda, /dev/xvda)

20.Q4.1 (April, 2021)

This is a patch release.

Defect Fixes

- Fixed issue where remote syslog may debug log user credentials
- Improved framework logging handling of errors
- Added sanitization of framework logging stack traces
- Improved reliability of rollback process on failed upgrade
- Fixed handling and validation of custom HTTPS certificates
- Fixed issue with REST API endpoints fail when trailing slash specified
- Improved sanitization of REST API logging when non-standard content-type specified

20.Q4.0 (January, 2021)

This is a production release.

NOTE: This release includes major changes that can break NetOps functionality on Lighthouse. As such, it is highly recommended to upgrade NetOps modules to the latest version. (If the version of NetOps modules on Lighthouse does not match the required criteria, a banner is displayed on UI prompting the user to update the modules.)

Features and Enhancements

- Added ability to combine multiple smart group search conditions using logical 'OR'
- Updated default TLS version on Lighthouse to 1.2 and made it configurable using ogconfig-cli
- Improved Lighthouse security
- Improved Lighthouse user experience and usability
- Upgraded EmberJS to 3.16 LTS release
- Added static code analysis for security vulnerabilities
- Added granular group roles and permissions
- Upgraded Yocto version to Zeus
- Added capability to store and display console serial port logs
- Removed non inclusive language from Lighthouse code
- Added version checking for config restore
- Added node name to node backup file names
- Added support for ordering node tables by connection status
- Added capability to cleanup logs when disk is filling up
- Added warning banner to be displayed if NetOps modules are not compatible with this release of Lighthouse

Defect Fixes

- Fixed issue where cellular connectivity test does not work with alternate API port
- Fixed issue where node upgrade commands fail with LUA error
- Fixed issue where secondary Lighthouse nodes receive varying IP addresses on boot
- Fixed issue where Lighthouse sets default switch type to private on HyperV
- Fixed issue with multiple license handling on Lighthouse
- Fixed Lighthouse Zapier integration to add tags to events. If users are running Lighthouse Zapier app privately, please update with the latest packages
- Fixed issue where Azure Lighthouse could not be deployed without assigning public IP address

20.Q3.0 (August, 2020)

This is a production release.

NOTE: To support the improvements required for disk management, this version of Lighthouse requires a new 20.Q3 virtual machine to be deployed and a configuration backup and restore from at least 20.Q2.0 onto the new virtual machine. From this release onwards, the supported upgrade path will be from the last major release (or patch release of that major release) only. This will generally be from the previous quarter.

Features and Enhancements

- Add improved UI for viewing consolidated Node and Port information
- Add support for system notifications, with Zapier as the initial integration. More information can be found in this FAQ article; https://opengear.zendesk.com/hc/en-us/articles/360048367371
- Add support for more effective and extendable disk management in Lighthouse, utilising LVM
- Add UI for viewing results of system tasks, currently supported are registrations, enrollments, and configuration retrieval
- Add support for enrolling Digi Passport devices
- Improved REST API performance and stability

20.Q2.1 (July, 2020)

This is a patch release.

Defect Fixes

- Fixed Web Terminal problems (sometimes not loading properly or restarting)
- Fixed issue with spurious SNMP server restarts on secondary Lighthouses
- Fixed issue with SNMP not reporting node information accurately after restarting some system services
- Fixed issue with some Cell Health SNMP traps being sent, regardless of status change
- Fixed issue with log file partitions filling up due to excessively large log files
- Fixed issue with slow Web UI responsiveness if the private VPN range is changed from the default
- Fixed issue with incorrect response codes to console servers during enrollment with many parallel enrollments
- Fixed issue with many parallel enrollments becoming bottlenecked and timing out
- Fixed issue with config retrieval job failures on nodes with poor connectivity

20.Q2.0 (May, 2020)

This is a production release.

Features and Enhancements

- Add support for implementing password policies for users
- Add logging capability for CLI and REST API
- Improved UI look and feel
- Improved performance for node registration and enrollment process
- Improved REST API performance and stability
- Improved formatting for remote syslog messages
- Improved reporting of cellular health for nodes
- Improved reporting of issues during node communication for enrollment and config retrieval

Defect Fixes

- Fixed session creation when system is under high load
- Fixed some memory leak issues when system is under high load
- Fixed enrollment for some ACS Classic configurations

20.Q1.0 (February, 2020)

This is a production release.

NOTE: The minimum required RAM for Lighthouse is now 8GB from this release.

Features and Enhancements

- Add support for IPv6
- Add support for different remote authentication methods (eg. RadiusLocal, RadiusDownLocal, LocalRadius, etc.)
- Improved security - limit web server information exposure, and add cross-site scripting protection
- Improved UI look and feel (including Ember 3.12 upgrade)
- Improved REST API performance and scalability
- Updated base operating system distribution (new versions of many opensource packages, security fixes, etc.)

Defect Fixes

- Fixed two-factor authentication with SSH
- Fixed issue booting on ESXi (older hardware without DRNG random number entropy support)
- Fixed support for node cell health status and IP address display
- Fixed serial console gateway using delimiters and SSH pubkey together
- Fixed issue where promoted secondary Lighthouse instances can’t enroll future secondary Lighthouses
- Fixed permissions issue when administrators try to delete syslog server configuration from Lighthouse
- Fixed various UI bugs (display, input field validation, etc.)
- Fixed issue with web terminal session remaining when UI logs out
- Fixed intermittent config server sync error when using many secondary lighthouses (causing failed web logins)
- Fixed issue with node backups not being visible between different version installs

19.Q3.3 (October, 2019)

This is a patch release.

Defect Fixes

- Fixed Netops Web UI support on upgrade
- Improved Multi-Instance processes to allow for slower networks/systems
- Improved configuration validation routines

19.Q3.2 (September, 2019)

This is a patch release.

Defect Fixes

- Fixed handling of large queues of system configuration updates

19.Q3.1 (September, 2019)

This is a patch release.

Defect Fixes

- Fixed issue with web terminal sessions persisting over reboots
- Fixed problems preventing secondary Lighthouse enrollment over alternative HTTPS ports
- Fixed problems with 3rd party nodes getting removed during secondary lighthouse promotion
- Fixed issue where many rapid node config updates could fill the disk
- Fixed issue where a high number of database updates used more disk than necessary
- Fixed issue with secondary Lighthouses in AWS not upgrading cleanly

19.Q3.0 (July, 2019)

This is a production release.

Features and Enhancements

- Add support for multiple secondary Lighthouse instances
- Added numerous improvements to multi instance upgrades
- Added numerous improvements to multi instance node enrolments
- Add support for deploying Lighthouse on AWS
- Add support for backing up and restoring Lighthouse configuration
- Add support for backing up managed node configuration (requires Console Server v4.6+)
- Add support for remote authentication using LDAPS
- Add node-id in the node list display in Lighthouse UI
- Add support for SSH links to nodes via node-id
- Add support for displaying third party nodes in node-info on CLI
- Improved Licence expiry banner display
- Improved node status dashboard widget links to more useful filtered list of nodes
- Improved SNMP traps sent for node connection/disconnection

Defect Fixes

- Fixed an issue where Lighthouse was reporting negative time in “Last Changed” field
- Fixed an issue with memory management of ogconfig-srv
- Improved processes around node connection while adding dependant secondary Lighthouse instances
- Fixed Lighthouse not listening correctly on alternative enrollment port

19.Q2.2 (June, 2019)

This is a patch release.

Defect Fixes

- Fix issue with many (> ~500) 3rd party console servers where some would not start up correctly
- Fix potential upgrade issue from versions pre-5.3.0 under certain circumstances

19.Q2.1 (June, 2019)

This is a patch release.

Defect Fixes

- Fix issue with multiple overlapping config retrieval operations occasionally crashing
- Improve speed of configuration for large numbers of 3rd party nodes

19.Q2.0 (May, 2019)

This is a production release.

Features and Enhancements

- Add support for Azure deployment
- Add ability to upgrade multi-instance Lighthouse deployments using a provided script
- Add license expiry warnings. Expired licenses will put Lighthouse into a read only operational mode
- Licenses are now uploaded as a file
- Lighthouse now supports retrieval and reporting on cellular health status for enrolled nodes
- Updated base operating system, new versions of many opensource packages
- Fixed potential vulnerability in web terminal
- Add ability to filter nodes by connection status
- Add script to set static IP (for support assistance)

Defect Fixes

- Scalability improvements for third party enrollment
- Fix issues where sudoing as root may not grant the expected permissions
- Fix issue where it was not possible to search by internal VPN address
- Fix issue where secondary lighthouses could lose their network configuration upon enrollment

5.3.0 (February, 2019)

This is a production release.

Features and Enhancements

- Add support for adding a secondary Lighthouse for the purpose of redundancy and failover
- Add support for changing the IP range to use for the internal Lighthouse VPN
- Add support for applying authentication templates to OM22xx devices
- Add support for applying user and group templates to OM22xx devices
- Third party node authentication settings can now be modified using the REST API
- Improved network validation
- Updated base operating system, new versions of many opensource packages

Defect Fixes

- Fix display error in ogconfig-cli where references displayed the wrong target path
- Fix authorization error for users with short usernames

5.2.2u1 (December, 2018)

This is a patch release.

Defect Fixes

- Improved performance for script template push to OpenGear console server
- Improved reliability of authentication

5.2.2 (September, 2018)

This is a production release.

Features and Enhancements

- Upgrade OpenSSH to 7.7p1
- Add OM22xx Operations Manager enrollment support and basic management
- Add support for running NetOps Automation Modules
- Add Secure Provisioning module for NetOps Automation
- Add expect to the Lighthouse CLI for custom scripting
- Add MOTD banner post-login that displays IP address information
- New deployments include a secondary drive for NetOps Modules. Upgrades of existing deployments will need to manually add this disk.
- Update the Web UI to use Ember 2.16
- Add support for running Docker containers on Lighthouse

Defect Fixes

- Improve handling of node's cellular addresses (requires console servers to be version 4.4 or above)
- Fix an rare incorrect authentication failure in the REST API
- Fix incorrect error when on script template PUT REST API endpoint
- Fix spurious log messages when connecting via SSH as an Admin user
- Fix incorrect error when invalid address entered into Authentication template UI
- Fix /system REST API endpoints being visible by Node Admin users
- Fix incorrect error when invalid arguments passed to node-copy cli
- Fix syslogd not restarting if the process exits
- Fix references in ogconfig-cli displaying with off-by-one indices

Security Fixes

- CVE-2017-17080
- CVE-2017-16830
- CVE-2017-16831
- CVE-2017-16832
- CVE-2017-17123
- CVE-2017-16828
- CVE-2017-17125
- CVE-2017-17122
- CVE-2017-17124
- CVE-2017-17121
- CVE-2017-16829
- CVE-2017-16827
- CVE-2017-16826
- CVE-2018-5390
- CVE-2018-5391
- CVE-2018-6323

5.2.1u1 (July, 2018)

This is a patch release.

Defect Fixes

- Fixed snmpwalk not listing all nodes.
- Fixed upgrade to 5.2.1 failing when LDAP auth is configured.

5.2.1 (June, 2018)

This is a production release.

Features and Enhancements

- The following endpoint namespaces have been modified in v3 of the REST API, so v1, v1.1, and v2 have been deprecated and will no longer be updated. As the endpoint's functionality has changed, there may be changes required to user programs utilising the REST API. Refer to the REST API documentation for v3 for example request/response bodies. Deprecated endpoints since 5.2.0u1:
- /v2/auth
- /v2/templates In general, prefer the latest version of the REST API (v3) in your own programs as this ensures the latest functionality is available.
- Add SNMP MIBs for Lighthouse 5.
- Add support for SNMP TRAP/INFORM messages on node connection status changes.
- Improve password handling in ogconfig server.
- Add support for Google Compute Engine deployment.
- Extend functionality for User and Group templates.
- Allow node users to have rights limited to specific ports on nodes.
- Add support for Console Gateway SSH links to use specified external address.
- Add support for exporting syslog to remote server.
- Add support for LDAP ignore_referrals.
- Default LHVPN timeout reduced to 60 seconds, and added config option to allow custom value.
- Changed sidebar ordering for sub-elements.
- Add support for configuring number of nodes/ports per page.
- Web UI pop-ups can now be closed by hitting escape and submitted by pressing enter.

Defect Fixes

- Fixed warning bar not showing when licence limit is exceeded.
- Fixed third party nodes causing a config sync error.
- Fixed UI allowing duplicate external endpoints.
- Fixed deleted template appearing on UI.
- Fixed DOM error on Remote Authentication page.
- Fixed success message not showing on bundles page.
- Fixed race condition with script templates.
- Fixed error when disabling enrolment only REST API port.
- Fixed Cisco 2900 failing if MOTD set.
- Fixed error on REST API Port endpoint.
- Fixed memory leaks in REST API.
- Fixed pmshell crashing if columns set to 1.
- Fixed third party node config sync error.
- Fixed rare segfault when deleting users.
- Fixed core daemons from having multiple instances.
- Made delete icon in web-ui consistent.
- Fixed error when editing Authentication templates.

5.2.0u1 (April, 2018)

This is a patch release.

Defect Fixes

- Fix issue with session IDs

5.2.0 (March, 2018)

This is a production release.

Features and Enhancements

- The following endpoint namespaces have been modified in v2 of the REST API, so v1, and v1.1 have been deprecated and will no longer be updated. As the endpoint's functionality has changed, there may be changes required to user programs utilising the REST API. Refer to the REST API documentation for v1.1 for example request/response bodies. Deprecated endpoints since 5.1.1u1:
- /v1.1/auth
- /v1.1/search
- /v1.1/nodes/smartgroups
- /v1.1/ports
- /v1.1/support_report
- /v1.1/services/console_gateway In general, prefer the latest version of the REST API (v2) in your own programs as this ensures the latest functionality is available.
- Large performance improvements across the board, allowing for larger numbers of nodes to be used on a single Lighthouse instance
- Updated base operating system, new versions of many opensource packages
- Add support for Hyper-V deployment
- Add support for configuring an enrollment-only HTTPS REST API endpoint
- Add managed device filters to UI and REST API
- Add search support in ogconfig-cli
- Make Console Gateway SSH links use the configured External Network Address
- Add a syslog entry when a new local user is created
- Add support for mounting additional filesystems for bulk file storage
- Add link to download the user manual
- License body is now hidden from UI
- Add human readable format for uptime in support report
- Add SNMP service and reporting
- Add log rotation to /var/log/wtmp

Defect Fixes

- Manually installed SSH keys are no longer breaking shell access
- Fix multiple issues caused by nodes with duplicate names
- Disable TCP timestamps
- Use SHA512 instead SHA1 in certificate generation
- Deleting a CSR now removes it from the SQL database
- Fix a failure with Avocent 3rd-party enrollments when using non-default serial port settings
- Fix issues with AAA logins and add more error reporting
- Fix crash in ogadduser when referencing a non-existent group
- Fix Administration/System button not responding in IE11
- Fix uncommon error message in syslog when unenrolling 3rd party nodes
- Fix upgrade issues that could occur from 5.1 to 5.1.1u1
- Fix lhadmin users not being able to run node-command
- Fix last successful config push losing status
- Fix lack of copy/paste in the Web Terminal

5.1.1u1 (December, 2017)

This is a patch release.

Defect Fixes

- Fix for a critical issue that prevented nodes being enrolled or coming back online after a system reboot in some circumstances.

5.1.1 (December, 2017)

This is a patch release.

Features and Enhancements

- The following endpoint namespaces have been modified in v1.1 of the REST API, so v1 has been deprecated and will no longer be updated. As the endpoint's functionality has changed, there may be changes required to user programs utilising the REST API. Refer to the REST API documentation for v1.1 for example request/response bodies.
- Deprecated endpoints:
- /v1/nodes
- /v1/system
- /v1/auth
- /v1/bundles
- /v1/users
- /v1/groups
- /v1/templates In general, prefer the latest version of the REST API (v1.1) in your own programs as this ensures the latest functionality is available.
- (Breaking change) AAA groups are now case-sensitive when mapping to local group authorization. This will only effect AAA groups that use capital letters.
- Change node names to be automatically synchronized to console server's hostname (needs CS firmware 4.1.1)
- Add support for pushing templated bash scripts to nodes (needs CS firmware 4.1.1)
- Add support for configuring a CLI session expiry
- Add Smart Group support to node-command and associated tools
- Improve performance of our REST API
- Improve usability of our Console Port Access page
- Add more examples to our REST API documentation
- Add ability for AAA-users to be defined locally without password
- Allow local user group names to contain more special characters
- Add netgrp user group that will contain all AAA users, allows for default permissions for AAA users
- Default netgrp permissions to Lighthouse Admin
- Add support for templates to be associated with bundles for automatic configuration application on enrollment
- Add information about current user to top bar in UI
- Add vmxnet3 driver for better VMWare virtualization support
- Add reporting about configuration template push status to node details
- Change default Lighthouse VPN MTU to be 1400
- Add ability to change the MTU for the Lighthouse VPN
- Add REST API endpoint to expose current firmware and API versions
- Add better node status reporting in the UI
- Update our HTTPS ciphers and protocols to comply with Mozilla Server Side TLS Recommended guidelines
- Add command line support for scheduling cron jobs

Defect Fixes

- Fix assorted authorization issues
- Fix issues caused when date is set to the past
- Fix failing configuration synchronizations causing enrollment to fail
- Fix inconsistencies in node terminology in the UI

- Fix crashes in ogconfig-cli
- Fix excess incorrect failure messages in syslog during successful enrollment
- Fix syslog error messages during unenrollment of 3rd party console servers
- Fix rare issue where the preflight check would list no nodes
- Fix browser window title incorrectly persisting after leaving console gateway page
- Fix ability to disable the root user
- Fix incorrect pmshell error message when no nodes selected
- Fix system details popover incorrectly sticking on screen
- Fix TACACS authentication hang when duplicate remote groups were discovered
- Fix ability for console servers with _ in hostnames to be enrolled
- Fix TTY parsing for Cisco 2900 3rd party console servers
- Fix incorrect usage information for node-upgrade
- Fix issue where long-lived LH5 instances would stop responding to REST API requests
- Fix TACACS Login authentication
- Fix Web Terminal copy and paste issues
- Fix rare configuration retrieval failing on node descriptions
- Fix configuration template pushes that raise errors never being marked as complete
- Fix remote AAA Lighthouse Admin users being unable to delete templates
- Fix Web UI Proxy when LH5 is being an external DNAT rule
- Fix user UID conflicts after switching from remote to local authentication schemes
- Fix memory leaks in configuration backend
- Fix memory leaks in our REST API
- Fix the disable multiple button not working on the Users page
- Fix left side bar inconsistencies
- Fix missing error messages when trying to add 3rd party nodes with more than 400 serial ports
- Fix enrollment breaking when secure HTTPS ciphers are configured on the console server
- Fix enrollment failures if remote node has portshare password set
- Remove autorefresh on Preflight and Template push pages

5.1.0 (August, 2017):

This is a production release.

Features and Enhancements

- (Breaking change) The Lighthouse OpenVPN connection now runs on UDP. This means Lighthouse 5.1.0 is only compatible with Opengear Console Servers version 4.1.0+.
- Add functionality for pushing configuration templates to groups of Opengear devices. Currently supported are Group and AAA templates.
- Add node-upgrade command line utility.
- Add system upgrade to the web UI. Users are able to upload a new system image or provide a URL where the file is hosted.
- Add license restrictions to the Lighthouse. Without a license, the Lighthouse is in evaluation mode with a limit of 5 enrolled nodes. Users can purchase licenses that increase that limit and give access to enroll third party devices.
- Add automated migration for configuration when upgrading to new Lighthouse versions.
- Add support for specifying multiple endpoints to access a Lighthouse device (from an Opengear Console Server) and custom ports on the Lighthouse that will listen for incoming requests.
- Add device support for non-Opengear devices (known as third party devices) with native configuration support for: – Avocent ACS 6000 & 8000 – Avocent Classic – Cisco ISR2921
- Add Console Gateway page with responsive searches over devices' serial ports
- Improved pmshell command line utility.
- Improved the config cli for manipulating Lighthouse configuration (ogconfig-cli).
- Improved the speed and stability of the configuration server and REST API.
- Improved the Web UI for usability.
- Improved configuration validation and feedback to client.
- Improved RAML documentation for the REST API.

Defect Fixes

- Users are redirected correctly after logging in.
- Fixed some stty issues around remote CLI sessions.
- Improved feedback when user attempts to access commands without suitable permissions.
- Free text search with multiple terms
- SSH custom delimiter parsing
- Disabling an interface could cause other interfaces to go down
- Group names can now contain a dash
- Console Gateway conventions are now adhered to for specifying username and port labels
- Improved shutdown & restart times
- Fixed enrollment of Console Servers with ports in Serial Bridging and Terminal Server mode
- Hostname and system time will now change in syslog when the system is updated
- A user's home directory will now be deleted when the user is deleted
- REST requests proxied via the Lighthouse to the Console Server will now be forwarded correctly by the Lighthouse
- Fixed an enrolment failing to complete if a node was approved too early in the registration stage. A node can now be approved at any point without breaking the enrollment.

5.0.0 (April, 2017):

This is a production release.

NOTE: This is a ground up rewrite of Lighthouse.

Features and Enhancements

- Add modern HTML5 Web UI
- Add streamlined user and groups mechanisms
- Add secure OpenVPN connections to remote nodes
- Add REST API for external integration and control of LH5
- Add HTML5 local web terminal
- Add HTML5 Console Gateway terminals
- Add 'Smart Groups', a way to group managed nodes through saved searches over their configuration and associated searchable tags
- Add support for searchable tags to be added to managed nodes
- Add a quick search bar at the top of every UI page that lists managed nodes
- Add initial and on-going synchronization of node serial port configuration, avoiding the need to 'Retrieve Managed Devices'
- Add streamlined enrollment methods via DHCP ZTP, USB, or Web UI
- Add consistently validated configuration backend
- Add tab-completable config cli