NOZOMI NETWORKS

RELEASE NOTES

Nozomi Networks Solution - N2OS

Table of Contents

N2OS 23.4.1

Updates in this Release - 23.4.1

Upgrade to 23.3.0 or 23.3.1 before 23.4.1 mandatory

Version 23.3.0 introduced a safer and more robust upgrade mechanism. In 23.4.1, this mechanism is leveraged to perform a sensitive operation that will keep the data in a more reliable and better-performing state. To upgrade 23.4.1 is therefore necessary to upgrade to 23.3.0 or 23.3.1 first.

Since the upgrade to 23.4.1 from 23.3.x requires to perform a full database dump to disk, make sure that the sensor has enough disk space before attemping an upgrade. The following command will show the size of the database.

```
psql -U n2os-dbms scadaguardian -c '\l+ scadaguardian'
```

Verify that the sensor's disk has enough free space to host a full copy of that size using the command `df -h /data`.

Rollback from 23.4.1 to a version earlier than 23.4.0

Due to a fundamental change in the system to improve security and ensure data safety, a rollback from version 23.4.1 to the previously installed version, if that previous version is 23.3.0 or 23.3.1, could present some technical difficulties if performed under certain circumstances. Under normal conditions it is prudent to backup a sensor prior to a version upgrade. During this upgrade, it is strongly recommeded to do so. In case of the need for a rollback after the installation, this functionality is provided in a best-effort fashion. Should the rollback procedure encounter unexpected difficulties, a fresh installation of the previously installed version followed by the restore of the backup will reestablish the previously working setup with the data intact. Rolling back from 23.4.1 to 23.4.0 will not present any particular difficulties.

Upgrade instructions for Container Edition

Due to architecture constraints, an operation that is necessary for the upgrade from 23.3.x to 23.4.1 cannot be automated within the Docker container, thus it is necessary to perform it manually before the upgrade. With the container on version 23.3.0 or 23.3.1 running, run the following command

```
docker exec -u 0 <CID> bash -c "pg_dump scadaguardian -U n2os-dbms | gzip
 -9 > /data/dump-upgradev"
```

where `<CID>` is the ID of the running container. When this command returns, stop the container running version 23.3.0 or 23.3.1 and start the container on version 23.4.0. The upgrade will complete automatically. If this command is not run manually, the upgrade will fail. No data loss will occur, but the container will not start.

Security fixes

- N2OS-14987 - Resolved CVE-2023-6916.
- N2OS-14994 - Updated software dependencies to address CVE-2023-6534, CVE-2023-6660, and CVE-2023-48795.
- N2OS-14999 - Resolved an HTML injection issue.
- N2OS-15016 - Resolved CVE-2024-0218.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Consolidation of data concerning MITRE ATT&CK®

N2OS exposes MITRE ATT&CK® related information in the alert properties `mitre_attack_for_ics` and `mitre_attack_enterprise`. The same information is also included in the legacy alert fields `mitre_attack_techniques` and `mitre_attack_tactics`, and in the legacy alert property `mitre_attack/techniques`. These legacy fields and properties are now deprecated and will be removed in a future version of N2OS.

Deprecation of STIX version 1

Nozomi Networks has supported STIX indicators versions 1 and 2 since N2OS 20.0.7. Version 1 uses XML representation and is now considered legacy, while version 2 uses JSON. Most threat intelligence information providers today deliver STIX content based on version 2. Nozomi Networks will in a future release remove the support for version 1 from N2OS. Those customers leveraging custom STIX rules based on version 1 are encouraged to transition to version 2. This transition will be necessary to maintain the level of protection currently supported by those custom STIX indicators, and can be performed using official and third-party tools.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.3.1 > 23.4.1

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.3.1, then to 23.4.1.

If you are on the release **22.6.2 or newer**:

- Upgrade to 23.3.1, then to 23.4.1.

If you are on the release **23.3.0** or newer:

- Upgrade directly to 23.4.1.

N2OS 23.4.0

Updates in this Release - 23.4.0

Upgrade to 23.3.0 or 23.3.1 before 23.4.0 mandatory

Version 23.3.0 introduced a safer and more robust upgrade mechanism. In 23.4.0, this mechanism is leveraged to perform a sensitive operation that will keep the data in a more reliable and better-performing state. To upgrade 23.4.0 is therefore necessary to upgrade to 23.3.0 or 23.3.1 first.

Since the upgrade to 23.4.0 requires to perform a full database dump to disk, make sure that the sensor has enough disk space before attemping an upgrade. The following command will show the size of the database.

```
psql -U n2os-dbms scadaguardian -c '\l+ scadaguardian'
```

Verify that the sensor's disk has enough free space to host a full copy of that size using the command `df -h /data`.

Rollback from 23.4.0 to previous version

Due to a fundamental change in the system to improve security and ensure data safety, a rollback from version 23.4.0 to the previously installed version could present some technical difficulties if performed under certain circumstances. Under normal conditions it is prudent to backup a sensor prior to a version upgrade. During this upgrade, it is strongly recommeded to do so. In case of the need for a rollback after the installation, this functionality is provided in a best-effort fashion. Should the rollback procedure encounter unexpected difficulties, a fresh installation of the previously installed version followed by the restore of the backup will reestablish the previously working setup with the data intact.

Upgrade instructions for Container Edition

Due to architecture constraints, an operation that is necessary for the upgrade to 23.4.0 cannot be automated within the Docker container, thus it is necessary to perform it manually before the upgrade. With the container on version 23.3.0 or 23.3.1 running, run the following command

```
docker exec -u 0 <CID> bash -c "pg_dump scadaguardian -U n2os-dbms | gzip
 -9 > /data/dump-upgradev"
```

where `<CID>` is the ID of the running container. When this command returns, stop the container running version 23.3.0 or 23.3.1 and start the container on version 23.4.0. The upgrade will complete automatically. If this command is not run manually, the upgrade will fail. No data loss will occur, but the container will not start.

Highlights

Network graph moved into the top-bar menu

The network graph is a key component of the Nozomi Network solution. It gives a bird's eye visibility of the entire network, and it offers extensive functionalities to filter, zoom and pan the view, or to use grouping and coloring to investigate a specific aspect or zone of the network. With version 23.4.0, the graph is no longer a tab of the network view, but it is now accessible directly under the navigation bar.

Support for UEFI devices

With this release, N2OS introduces full support for UEFI devices. This includes Amazon EC2 virtual machines and Siemens Ruggedcom APE in Legacy BIOS mode.

Base OS

- The database management software version has been updated. See the user manual for details and follow the N2OS upgrade paths strictly to avoid data corruption.
- Added support for leveraging the system backup and restore functionalities to enable data replication across data diodes.
- Network elements limits for N1000 and N750 appliances have been fixed according to the RAM available.

Reports and Integrations

- Additional description alert fields, whenever present, are now provided in the email body sent by the SMTP data integration.
- Guardian can now integrate with NetWitness to send alerts.

Protocols, Smart Polling and Arc

- The Zone filters feature is now out beta and ready for production use.
- Node points now have a source field indicating whether they come from Arc or Smart Polling.
- The nodeid_factory setting now works also for Arc, enabling for separation of nodes monitored by Arc and having duplicate addresses.
- Arc deployment now supports for automatic reboot of the target endpoints when a dependency installation requires it.
- The N2OS user is better warned on the absence of Arc bundles when attempting a deployment.
- The Arc deployment page is now more usable and shows the suitable Assets list instead of nodes list. Multiple nodes are automatically contacted per asset depending on credentials configuration.
- Added support for the Honeywell GLOFA-GM / Master Logic series protocol, including asset identification and properties extraction.
- Guardian can now detect Bosch Rexroth Nexo tools through passive detection and Smart Polling.
- Improved Honeywell Mercury support adding asset information, function codes and variables extraction.
- Improved support for Siemens CP devices via the LLDP protocol.
- Extended the SEL Telnet Smart Polling strategy to support to SEL RTAC devices.
- Asset information added through Asset Intelligence from the ONVIF protocol is now more reliable.
- Improvement of confirmed MAC address retrieval using passive SNMP traffic.
- Added support for IEC101 variable extraction when encapsulated into PSI Ketel protocol.

CMC, Remote Collector and AAA

- Names of locally created User groups at CMC level are no longer editable to grant for consistency to the previously propagated groups to downstream.
- Improved node synchronization between Guardian, CMC and Vantage.
- Improved asset synchronization between Guardian and CMC (all-in-one and multicontext).
- Improved deletion process for users and groups increasing security and flexibility. Please refer to the user manual for additional information.
- Improved data reset functionality for CMC all-in-one allowing users to effectively delete nodes, links and variables.
- Fixed an issue that prevented the CMC from synchronizing assets provided by downstream sensors when bulk synchronization is enabled and the CMC's upstream has disabled the synchronization of assets.
- Reduced the CPU usage for Guardians with multiple Remote Collectors connected.
- The Remote Collector Text-based User interface (`n2os-tui`) now allows to define inclusions to the traffic shaping configuration.

Contents and Detection

- Add the possibility to disable `node_cpe` generation per zone.
- Support JA3/JA3S signatures as part of Packet Rules to support the fingerprint of the TLS negotiation between client and server.
- CPE calculations can now be turned on/off for individual nodes and assets. When conflicting configurations are set at the node-level and an asset-level for the same device, asset configurations will have the higher priority.
- CVEs created by Guardian are now assigned an EPSS (Exploit Prediction Scoring System) score.
- Addressed a case where the `is_from_public` and `is_to_public` fields for some nodes were inconsistent due to a node's change of address.
- Largely improve the memory footprint of the Packet Rule Engine when loading tens of thousands of rules.
- Vendor names are now normalized by Asset Intelligence (e.g. "Siemens AG, Automations & Drives" becomes "Siemens") to provide a uniform experience. Please remark that queries and assertions relying on an exact match of the `vendor` and `mac_vendor` fields are impacted by this change and need to be reviewed.
- Improved the cooperation between Asset Intelligence and Threat Intelligence: assets enriched by AI are now processed by TI to enable for more accurate CVEs assignments.

Resolved issues

- N2OS-14390 - Improved the behavior of VI:NEW-FUNC-CODE alerts for Bacnet, identifying the right actors for serial or behind-backplane communications.
- N2OS-14528 - Resolved an issue that prevented certain query groups from being modified or deleted.
- N2OS-14926 - Improve the robustness of the IDS while reading the configuration file for complex property fields.
- N2OS-14933 - Improved the robustness of Sandbox when traversing deeply nested VBA macros.
- N2OS-14967 - Addressed a problem that prevented the Fortigate firewall integration from registering killed sessions in the database table.

Security fixes

- N2OS-14061 - Migration tasks can now be launched only by admin users.
- N2OS-14840 - Updated software dependencies to address CVE-2023-34058 and CVE-2023-34059.
- N2OS-14858 - Updated software dependencies to address CVE-2023-5369, CVE-2023-5370, CVE-2023-5941, CVE-2023-5978, and CVE-2023-5368.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Consolidation of data concerning MITRE ATT&CK®

N2OS exposes MITRE ATT&CK® related information in the alert properties `mitre_attack_for_ics` and `mitre_attack_enterprise`. The same information is also included in the legacy alert fields `mitre_attack_techniques` and `mitre_attack_tactics`, and in the legacy alert property `mitre_attack/techniques`. These legacy fields and properties are now deprecated and will be removed in a future version of N2OS.

Deprecation of STIX version 1

Nozomi Networks has supported STIX indicators versions 1 and 2 since N2OS 20.0.7. Version 1 uses XML representation and is now considered legacy, while version 2 uses JSON. Most threat intelligence information providers today deliver STIX content based on version 2. Nozomi Networks will in a future release remove the support for version 1 from N2OS. Those customers leveraging custom STIX rules based on version 1 are encouraged to transition to version 2. This transition will be necessary to maintain the level of protection currently supported by those custom STIX indicators, and can be performed using official and third-party tools.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.3.1 > 23.4.0

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.3.1, then to 23.4.0.

If you are on the release **22.6.2 or newer**:

- Upgrade to 23.3.1, then to 23.4.0.

If you are on the release **23.3.0** or newer:

- Upgrade directly to 23.4.0.

N2OS 23.3.1

Resolved issues

- N2OS-14817 - Addressed an issue that caused the files captured from the traffic to reside in the file system without being cleaned up, and to inhibit the processing by Sandbox.
- N2OS-14837 - Fixed a problem that prevented the FIPS version of the container edition from working correctly.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Upgrade path of future versions

N2OS 23.3.0 introduces improvements in the reliability of the upgrade process, which are instrumental to ensure that future upgrades are always smooth. For this reason, the upgrade path to future releases will require to install 23.3.0 or 23.3.1 first.

Consolidation of data concerning MITRE ATT&CK®

N2OS exposes MITRE ATT&CK® related information in the alert properties `mitre_attack_for_ics` and `mitre_attack_enterprise`. The same information is also included in the legacy alert fields `mitre_attack_techniques` and `mitre_attack_tactics`, and in the legacy alert property `mitre_attack/techniques`. These legacy fields and properties are now deprecated and will be removed in a future version of N2OS.

Deprecation of STIX version 1

Nozomi Networks has supported STIX indicators versions 1 and 2 since N2OS 20.0.7. Version 1 uses XML representation and is now considered legacy, while version 2 uses JSON. Most threat intelligence information providers today deliver STIX content based on version 2. Nozomi Networks will in a future release remove the support for version 1 from N2OS. Those customers leveraging custom STIX rules based on version 1 are encouraged to transition to version 2. This transition will be necessary to maintain the level of protection currently supported by those custom STIX indicators, and can be performed using official and third-party tools.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.3.1

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.3.1

If you are on the release **22.6.2 or newer**:

- Upgrade directly to 23.3.1

N2OS 23.3.0

Highlights

Alert deduplication

As we highlighted in the release notes of N2OS 23.2.0, a new feature prevents the creation of multiple identical alerts, symplifying the inspection of the alerts and reducing the stress to the system. This feature is now enabled by default and can be configured as detailed in the user manual.

Because configured data integrations including Nozomi alerts transmission will also be affected by the deduplication, Nozomi Networks recommends to check on the integrated endpoints configuration and logics accordingly.

Security improvements to SSH server

We have made significant security improvements to the configuration of our SSH server with the latest update. This includes updating the SSH protocols and ciphers that are accepted by the server to ensure better protection. Due to this update, ssh-rsa keys will no longer be accepted. If you are still using these legacy keys, we recommend uploading new ones before the upgrade.

If you require compatibility with legacy systems, you can switch your SSH configuration to legacy mode. Detailed instructions can be found in chapter 17 of the user manual.

Base OS

- It's now possible to restrict traffic shaping to some specified hosts. When configuring traffic shaping, it's now possible to use hostnames instead of IPs both when enabling it on specific hosts and when defining exceptions.
- Security of the database connection has been enhanced to ensure better protection during queries.
- Update FreeBSD to resolve CVE-2023-38408 and CVE-2023-3107.
- The optional configuration file `/data/cfg/database.yml` has been renamed and kept in the same folder just for backup reasons. This file is no longer necessary.
- Backups can now be encrypted. Users are prompted to fill in a password both to backup and restore.
- When performing backup/restoring a backup, the restored entity preserves its `.appliance-UUID` file for consistency.
- The CMC Web UI now shows an hyphen on the connected sensor's `license` field when the sensor is not licensed.

Reports and Integrations

- Open API: added ability to edit an alert note to the alerts endpoint.
- Kafka data integration: added a new option to generate a log file for troubleshooting issues.
- Improved the way sessions killed from the Fortinet FortiGate and Palo Alto Networks v10.1+ firewall integrations are stored. They used to be stored in the n2os.conf.user file, while now they are stored in the DB.
- Content Packs can now contain Playbooks, as well as optionally including the associated alert rules.
- Removed support for CheckPoint firewall integration in N2OS. The CheckPoint integration settings will not be restored upon rolling back from 23.3.0 to the previously installed version.
- Added support for sending firewall rules to Palo Alto Networks (PANW) Next-Generation Firewalls (NGFW) in `disabled` state, allowing PANW users to study and enable rules on the PANW environment and at their discretion.

- Open API Query endpoint: when using pagination, if the provided count value is higher than 10,000, no more than 10,000 items are returned. The maximum allowable page number is 1,000. Requests for pages beyond this limit will result in an error. Added API Best Practices section to the SDK User Manual.
- Cisco ASA Firewall integration now gives the user the ability to manage inactive policies.
- The Open API call `/api/open/sensors/resources` allows the user to retrieve the CPU usage, memory used, and disk used percentages.
- The DNS Reverse Lookup data integration now sanitizes the hostname before using it as a node label.
- MS endpoint configuration manager (SCCM) integrations: it is now possible to specify a custom port for the endpoint.
- To extract the local license information using OpenAPI, invoke the following OpenAPI command while using the credentials of an admin user `api/open/sensors/license`

Protocols, Smart Polling and Arc

- Improved expressiveness of the denylist syntax to allow the specification of port ranges. Also, the Windows' Carriage return characters `\r\n` are now interpreted correctly. The chapter 5 of the user guide contains more detailed explanations.
- Improved data source priority management for assets with Arc installed.
- Operating system (OS) node fields containing multiple different OS versions from old versions of N2OS are now cleaned up.
- Smart Polling is now able to poll SEL devices without performing authentication and therefore without requiring the device's password.
- The installation of Arc is now simplified through the management of dependencies. During manual deployments, the dependencies can be obtained from Guardian. During automatic deployments, the procedure installs the missing dependencies and details the result in the activity log. A dedicated `install_dependencies` command has been introduced to perform manual installation of dependencies. Note: Nozomi can only distribute the latest version of Sysmon. For Windows versions lower than 8.1, Sysmon needs to be manually replaced with a compatible version.
- When requesting a trace on elements extracted from tunnelled communication, the user is now prompted a message informing that the BPF filter is automatically built taking into account the tunnelled communication.
- Alerts on tunneled communications now correctly report the encapsulated source and destination IP addresses.
- The formatting style of Arc native alerts is now consistent with the rest of the system.
- Arc is now distributed also for 32-bits Windows systems, including support for automatic deployment from Guardian.
- The capture_device value has been made more expressive to disambiguate different natted Arc sensors.
- N2OS now supports the Honeywell Mercury protocol, including asset identification and variables extraction.
- Guardian can now extract iec104 variables from PSI-Ketel sessions.
- Improved handling of DHCP protocol to correctly assign node labels and confirm MAC addresses.
- Guardian can now detect the GE Healthcare Common Service Desktop web application through passive detection and Smart Polling.
- Guardian can now detect Bosch Rexroth WR21 HMI devices passively.
- The Smart Polling Tyan BMC HTTP(S) and Lanner BMC HTTP(S) strategies are now separated.
- Multiple Time Machines snapshots can now be loaded simultaneously in different browser tabs.
- Guardian now prevents to open more than 2 Time Machine snapshots to save on system performance, prompting the user to close the open snapshots when loading a new one.

CMC, Remote Collector and AAA

- Improved Guardian and All-In-One CMC's upstream asset synchronization management process by eliminating the use of the database.
- N2OS now authenticates with Vantage and other upstream appliances using token-based authentication.
- All-In-One CMCs are no longer constrained by the allowed network elements set for downstream sensors.
- The Remote Collector now uses the raw strategy to send traffic to the Guardian by default.
- The Remote Collector now offers a new strategy zraw, which uses compression and lowers the memory consumption on Guardian.
- Users can now select the Remote Collector communication strategy through the Guardian's sensors page in the WebUI.

Contents and Detection

- Introduced the new SIGN:DUALUSE-DETECTED alert type, with default risk set to 5. Updated the default risk for SIGN:PUA-DETECTED from 8 to 5. Introduced support for a Yara meta property called `nn_priority` (string) that the user can leverage to set a custom risk for alert types SIGN:MALWARE-DETECTED, SIGN:DUALUSE-DETECTED, SIGN:PUA-DETECTED triggered by the Yara rule containing it.
- Introduce support for negated PCRE options in packet rules.
- The vulnerabilities list now offers the possibility to filter for Known Exploited Vulnerability (KEV) items.
- Threat Intelligence can now perform an offline lookup of STIX indicators, using an on-disk database and thus reducing the memory consumption. Please refer to the User Manual for instructions to enable the feature. Note: XML STIX contents are not supported by the Database Provider; only custom contents are affected since all Update Service contents are deployed in JSON format.
- Added size sliders for all columns in the List tab of the Vulnerabilities page.
- Packet rules now implement the `multiplier` option for the `byte_math` and `byte_jump` options.
- Guardian now assigns End-of-Life CPEs to unmaintained versions of known software, giving higher visibility to outdated software components that could represent a threat for the environment.
- The level of recursion employed by Guardian when extracting macros from documents captured passively can now be configured, balancing detection abilities and preservation of system resources. The user guide contains details about this configuration option.
- Improved documentation for the commands that can be sent via the Command Line Interface to the VA service. NOTE: the legacy index and microsoft hotfixes engines have been deprecated and are no longer documented. They will be completely removed in a future version of N2OS.

Resolved issues

- N2OS-14186 - The visualization of dynamic Alert properties within the “More” card has been restored.
- N2OS-14225 - Addressed an issue that caused wrong sessions to be included in the CSV and Excel files downloaded from the asset details popup.
- N2OS-14239 - Fixed an issue that did not honour zones' custom Security Profiles during alert generation. Now when either zone has a security profile containing the alert type, the alert will be shown.
- N2OS-14293 - Addressed an issue affecting the persistence of a specific set of internal files.
- N2OS-14361 - Addressed an issue that caused the VA service to occasionally terminate abnormally when being stopped.
- N2OS-14379 - UTF-8 characters can now be used in the description and site fields of Guardians and CMCs.
- N2OS-14391 - Guardian no longer produces repeated alerts of type `VI:NEW-MAC`.

- N2OS-14408 - Addressed a false positive trigger of the multiple unsuccessful logins alert with the MySQL protocol.
- N2OS-14412 - Fixed an issue that prevented the Arc flag in the top black bar from being displayed when the license is expiring.
- N2OS-14428 - Addressed an issue that was causing the assets overview widget in the dashboard to link to the asset table with a wrong filter.
- N2OS-14469 - Addressed an issue affecting the enabling/disabling of alert deduplication via the CLI.
- N2OS-14483 - Addressed an issue that prevented the CheckPoint IoT data integration to work correctly due to connectivity incompatibilities.
- N2OS-14568 - The reload of Asset Intelligence is correctly triggered without a rematch upon the release of new contents.
- N2OS-14777 - Addressed an issue that prevented the configuration of Cisco ISE firewall integrations with certificates.

Security fixes

- N2OS-12936 - Users and open API keys are locked after reaching the failing attempt threshold
- N2OS-12963 - Added a process that ensures the proper use of an internal configuration file an additional layer of protection against accidental misconfiguration.
- N2OS-13239 - Check Point IoT Data Integration websocket is now accessible only if a corresponding Data Integration is configured.
- N2OS-13242 - Resolved CVE-2023-5253.
- N2OS-14188 - Updated SSH ciphers configuration and introduced new SSH profiles to improve compatibility with older systems
- N2OS-14270 - Updated WolfSSL FIPS library.
- N2OS-14587 - Updated Angular LTS library to version 1.9.3
- N2OS-14604 - Improved HIDS rules to avoid false positives.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Upgrade path of future versions

N2OS 23.3.0 introduces improvements in the reliability of the upgrade process, which are instrumental to ensure that future upgrades are always smooth. For this reason, the upgrade path to future releases will require to install 23.3.0 first.

Consolidation of data concerning MITRE ATT&CK®

N2OS exposes MITRE ATT&CK® related information in the alert properties `mitre_attack_for_ics` and `mitre_attack_enterprise`. The same information is also included in the legacy alert fields `mitre_attack_techniques` and `mitre_attack_tactics`, and in the legacy alert property `mitre_attack/techniques`. These legacy fields and properties are now deprecated and will be removed in a future version of N2OS.

Deprecation of STIX version 1

Nozomi Networks has supported STIX indicators versions 1 and 2 since N2OS 20.0.7. Version 1 uses XML representation and is now considered legacy, while version 2 uses JSON. Most threat intelligence information providers today deliver STIX content based on version 2. Nozomi Networks will in a future release remove the support for version 1 from N2OS. Those customers leveraging custom STIX rules based on version 1 are encouraged to transition to version 2. This transition will be necessary to maintain the level of protection currently supported by those custom STIX indicators, and can be performed using official and third-party tools.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.3.0

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.3.0

If you are on the release **22.6.2 or newer**:

- Upgrade directly to 23.3.0

N2OS 23.2.0

Highlights

Alert deduplication

The presence of a large numbers of nearly identical alerts causes stress to the system resources and impairs the usability of the alert system. Version 23.2.0 introduces a new feature that significantly improves the alert management by deduplicating these records. Alerts that represent the same event (or a repetition thereof) are grouped into a single record, keeping track of the amount of such events and their timestamp in new fields. The user is presented with a more effective summary of the anomalies and the resources of the system are preserved more efficiently.

The feature is disabled by default on all installations of 23.2.0, and can be enabled as explained in the user manual. An upcoming version of N2OS will enable this feature by default on all installations.

Because configured data integrations including Nozomi alerts transmission will also be affected by the deduplication, Nozomi Networks recommends to check on the integrated endpoints configuration and logics accordingly.

Detection of devices

As with every version of N2OS, 23.2.0 improves its ability to monitor the environment with the goal of providing an exhaustive asset inventory and an accurate assessment of the vulnerabilities.

N2OS can now detect Phoenix Contact WP 6000 devces through Smart Polling, BlueMark DroneScout through passive inspection, Type exacqVision Web Service, and Axis devices along with the installed add-on applications in both modes. Moreover, the asset inventory through passive detection of DICOM communication has been enhanced, as well as the identification of ABB 800xA controllers through the MMS protocol. Guardian can now also extract asset information from the inspection of server banners sent via FTP and HTTP protocols.

The asset information extracted from these sources is used to identify the vulnerabilities through Threat Intelligence.

Reports and Integrations

- The `type` field of nodes can now be updated through OpenAPI via the CSV and JSON endpoint imports.
- The percentage of used RAM for connected sensors is now available in the `info.mem_used_perc` field of the `appliances` data source within queries.
- The presentation of user groups in the configuration of reports group visibility is no longer limited to 30 entries.
- Updated Cisco ISE data integration to include node information updates upon change of state.
- The FireEye TAP solution has been retired and unsupported by the vendor for some time. Starting from this version of N2OS, all existing FireEye TAP integrations will stop working and new FireEye TAP integrations cannot be created. Please note that rolling back to a previous N2OS version after updating to version 23.2.0 may not restore FireEye TAP integrations configurations and data.

Protocols, Smart Polling and Arc

- The Import menu has now an option to select the CSV files separator character.
- Added support for the Cisco metadata transport layer.
- Added an elastic notification period for connected Arc sensors. The more Arc sensors are connected, the longer the notification period will be.

- Guardian now performs IP reputation checks through Threat Intelligence against the address seen in the traffic, including when the address is grouped through the `ipgroup` configuration.
- The asset details popup now shows source, confidence and granularity information about asset fields more consistently. This info is now presented also for the asset firmware.

CMC and AAA

- Improved resilience in the asset merging process of all-in-one CMCs.
- CMC now allows the users to disable the synchronization of reports from the connected sensors.
- Added support for logging in and importing Active Directory groups regardless of letter case difference between login username and Active Directory username. For example, if the domain name in the sensor's Active Directory configuration is `domain_name`, you can login and import groups with username `DOMAIN_NAME\user_name`.

Contents and Detection

- Guardian now allows to replay the traces with a specified throughput.
- The Guardian's packet rules engine will check only the inner payload for encapsulated traffic (e.g. transmissions using the CAPWAP protocol).
- The alert table now includes new columns to host source and destination custom fields with populated values as defined on a node basis.
- A new Asset type "Communication adapter" has been added. Also, the friendly name for "I/O" is now "IO" to help with searches.
- Added options for allowing local management of Threat Intelligence contents from downstream sensors.
- Improved the layout of the Alert detail view driving consistency in UI/UX
- The default value for the settings `max_attackers` and `max_victims` reported in the alert data for the applicable alert types is now 10.
- SIGN:CLEARTEXT-PASSWORD alerts are now raised only once per link.
- SIGN:NETWORK-SCAN alerts for ICMP are now raised at most once per day per source node.

Resolved issues

- N2OS-11592 - Addressed an issue that prevents importing a node type if a node already has a set operating system.
- N2OS-11770 - Traces are now correctly generated also in presence of GRE tunnelled traffic.
- N2OS-13629 - Addressed an issue affecting the ability to download individual traces for alerts.
- N2OS-13795 - Addressed an issue that prevented the creation of traces for alerts related to IP grouped nodes.
- N2OS-13960 - Addressed an issue that prevented the successful update of Threat Intelligence and Asset intelligence contents when passing through a proxy using Kerberos authentication.
- N2OS-14032 - Addressed an issue that was causing the assets page to show items belonging to a wrong Purdue model level when filtering by level.
- N2OS-14089 - Fixed an issue where some Asset last_activity_time was zero even if the associated nodes were active.
- N2OS-14093 - Addressed an issue with the SMTP forwarding data integration, which was not working when STARTTLS was unchecked.
- N2OS-14107 - Addressed an issue that prevented Asset Details page to load correctly.
- N2OS-14147 - Fixed an issue that caused alert rules to be incorrectly shown in the edit dialog.
- N2OS-14199 - Fixed an issue that prevented alert rules for playbook assignment from being saved correctly.
- N2OS-14207 - Fixed an issue that caused Smart Polling to connect to WinRM hosts to the wrong port when SSL was selected.

- N2OS-14212 - Only users with administration credentials are able to extract quarantined files using the API.
- N2OS-14243 - Fixed an issue that caused embedded Threat Intelligence contents to be loaded when a Threat Intelligence license is present.
- N2OS-14249 - Solved an issue that prevented the creation of reports when using a custom logo.

Security fixes

- N2OS-9865 - Addressed a vulnerability that allowed uploading a denylist file for a non-existing interface.
- N2OS-13206 - Fixed an issue that caused functional options within URL to be logged in case of download error when Threat Intelligence or Asset Intelligence contents are downloaded.
- N2OS-13750 - Improved the reliability of SSO login.
- N2OS-13789 - Updated FreeBSD
- N2OS-13821 - The interpreter for scriptable protocols has been upgraded from Lua5.3 to 5.4. Customers using scriptable protocols are recommended to consider the incompatibilities between these two versions of Lua, described in Chapter 8 of the Lua user manual: *https://www.lua.org/manual/5.4/manual.html*.
- N2OS-13933 - Upgraded WolfSSL library for FIPS to version 5.6.0.
- N2OS-14193 - Web interface passwords can now be hashed using the pbkdf2 sha512 algorithm; see the password policy chapter in the user manual for more details.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Check Point firewall integration End-of-Support

Nozomi Networks will end support for the current implementation in N2OS of the firewall integration with Check Point Gateway in the upcoming release.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.2.0

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.2.0

If you are on the release **22.6.2 or newer**:

- Upgrade directly to 23.2.0

N2OS 23.1.0

Highlights

UI Unification

Nozomi Networks is unifying the user experience across its products, including N2OS and Vantage. The goal is to make the interaction with our systems more consistent and to simplify the operations performed by the user.

N2OS 23.1.0 sets the new navigation bar by default. The new navigation bar was introduced in 23.0.0 and in Vantage at the same time. Its goal is to give a quicker access to the most used areas of the products. The old navigation bar can still be enabled through a toggle in the drop-down user menu. However, the old navigation bar will be removed in a future release.

The "Assets" page (previously "Asset view") has received graphical enhancements, as is the case also for the alert details dialog. The "Network view" and "Process view" pages have been renamed to "Network" and "Process" respectively. The favicon of the webinterface is now different for Guardian and CMC.

LACP and EtherChannel

Physical Guardian now supports Monitoring ports with Static EtherChannel, on an experimental basis, enabling link aggregation with "EtherChannel on mode" between N2OS and Cisco 9300 switches with firmware v17.6.3.

Physical Guardian and CMC sensors now support Management port with Link Aggregation Control Protocol LACP IEEE 802.3ad standard on an experimental basis, enabling Ethernet channels between N2OS and switches. Available for Cisco 9300 switches with firmware v17.6.3 and ARUBA 2530 switches with firmware vYA16.11.

Reliability Improvements

Versions 22.6.2 and 23.0.0 introduced important enhancements that improved dramatically the reliability and life span of our physical appliances, particularly Remote Collector. Version 23.1.0 continues this trend by implementing important updates to the range of supported hardware.

The memory management for the n2os_rc process has been improved, solving a few cases of crashes due to out-of-memory situations.

The version upgrade process has received stability improvements, solving a case in which multiple reboots were necessary to complete the update.

The data reset operation is now quicker and more reliable, including the feature that allows to play a trace with the "delete all data" toggle enabled, solving a case where this operation could timeout on machines with low resources.

Some filesystem directories have received performance and consistency improvements. Quarantined files are now kept in a RAM drive when the system host has sufficient memory. The traces are now kept in the /var/traces directory.

Support for RUGGEDOM sensors is reintroduced via the release N2OS 23.1.0. Full compatibility with the APE1808 platform has been restored. The recommended upgrade path is to upgrade to N2OS 22.6.2 and then immediately upgrade to N2OS 23.1.0, skipping N2OS 23.0.0, which does not support RUGGEDCOM and cannot be installed on these sensors.

More details can be found in the "Resolved issues" section of these release notes.

Base OS

- FIPS mode can now be enabled without a FIPS license to allow connection of new sensors to existing FIPS sensors. However, FIPS licenses are necessary to enable traffic monitoring on all FIPS sensors.
- Clarified supported disk types when installing a Virtual Machine (VM) and when adding a secondary disk to a VM. See "Installing the Virtual Machine (VM)" and "Adding a secondary disk to a Virtual Machine (VM)" in the N2OS User Manual for details.

Reports and Integrations

- N2OS now supports Fortinet FortiGate version 7.
- Improved the querying logic for data integrations by using pagination on all queries. Now, the sensor where the data integration is configured sends data in the order it is received.
- You can now change the margin between widgets in PDF reports.
- The IBM QRadar (LEEF) data integration now sends the appliance_site field of alerts.
- Previously, when a user added a widget to a report, N2OS returned them to the top of the page. Now, N2OS maintains its page position after the widget is added.
- Improved query type check for `uniq` and `where`, filtering out irrelevant parameters, and no longer treating irrelevant values as '0'. 'Never' is the only valid text value for `where` clause when using a timestamp.`
- Fixed an issue that allowed a user to re move all report pages, which left the report in an unusable state.
- If Time Machine Snapshots configuration files become corrupted, a diff between those snapshots will execute with stable behavior. It must be noted that if the configuration files are corrupted, Nozomi Networks cannot guarantee the fidelity of resulting diff between snapshots.

Protocols, Smart Polling and Arc

- Fields populated through passive detection now have a protocol information field. This field is visible in the asset details dialog through the information tooltips, and it is queryable through the `*:info` fields in the nodes and assets tables.
- N2OS can now extract asset information for WAGO devices using the HTTP protocol.
- N2OS now passively extracts Bently Nevada asset identification data, function codes, and hardware components.
- Added a Smart Polling Strategy for Bently Nevada devices.
- Guardian can now detect Ubisense DIMENSION4 UWB RTLS devices both through passive detection and Smart Polling.
- Guardian now supports the ubisense-uwb Ultra Wideband (UWB) protocol.
- Refined the import variables function to avoid an error, and requiring to map all the 3 primary keys to enable the import.
- Extended and refined the capabilities for Allen Bradley L5X project file imports.
- Improved support for CanBus (Controller Area Network) protocol.
- Added support for MVB (Multifunction Vehicle Bus) protocol.
- Introduced a new Smart Polling HTTP strategy for Lanner IPMI Card that includes Tyan BMC cards and other AMI MegaRAC SP-X implementations.
- Guardian can now extract network-related information about nodes from the DHCP protocol.
- Improved asset identification for the PSI KETEL protocol.
- The minimum interval between Time machine snapshots is now one hour.
- The Capture Device values populated for nodes discovered by Arc now show also the network interface by which traffic was found (e.g. arc[10.0.0.1@eth1]).
- Improved support for the CAPWAP (Control and Provisioning of Wireless Access Points) protocol by implementing the reassembly of fragmented messages.
- Improved the device module and firmware detection for Siemens S7 devices.

- Previously, Guardian alerted about extra tailing data in DNS packet. Now, extra tailing data in DNS packet is no longer considered a malformation and does not represent a potentially malicious action, so Guardian no longer alerts on this condition. Additionally, in both the HTTP and FTP protocols, we have lowered the frequency of `SIGN:PASSWORD:WEAK` and `SIGN:CLEARTEXT-PASSWORD` to a single instance per source node and destination node.

CMC and AAA

- Added support for multiple Active Directory and LDAP configurations.
- It is now possible to selectively propagate zones from Vantage downstream to specific sensors using the scope functionality
- Improved synchronization for reports files.
- Users and user groups are now propagated only to the sensors specified in the Allowed sensors filters of user groups.
- Improved the reliability of the file system synchronization.
- N2OS now limits the logging of output that comes from the binary syncing procedure. In addition, metadata discovery during binary syncing is now more efficient.

Contents and Detection

- Improved the performance of vulnerabilities recalculation for many node CPE changes.
- Minimized the risk of duplicate OS entries for Windows Operating Systems.
- CPEs that have reached the end of their life (EOL) and are loaded from Threat Intelligence contents, no longer generate or match obsolete CVEs.
- Guardian now supports the veeam-backup protocol. The rate of false positive packet rules and YARA rules detection related to Veeam backup solutions has been lowered.
- The LUA SDK now supports specific hooks for variables correlation. For more information, see the "Variables Correlation" section of the N2OS User Manual SDK.
- Users can now manage Sigma rules from the Threat Intelligence contents page. Sigma rules are actually in use only for installations with Nozomi Arc.
- CMC now sets the resolution status on vulnerabilities for which an installed hotfix has been found through Smart Polling or Arc.
- The vulnerabilities counter in the Asset View is now more accurate in case of assets made by multiple nodes.
- Increased the risk level assigned by Guardian to alert types SIGN:MALICIOUS-DOMAIN, SIGN:MALICIOUS-IP, SIGN:MALICIOUS-URL, and SIGN:PUA-DETECTED.

Resolved issues

- N2OS-12500 - In a previous release, the CMC did not include the usual retention parameter configuration options. Now, you can use the CMC to set the retention parameters for local report files, as well as for those synchronized from connected sensors.
- N2OS-12806 - Improved security checks for the download of exported files.
- N2OS-12893 - Fixed an issue that could prevent users from downloading support archives exceeding 1GB in size.
- N2OS-13046 - Fixed an issue that prevented some log to be updated after a backup was restored.
- N2OS-13291 - Fixed an issue in the Alert tuning table that prevented filter values from being properly reset.
- N2OS-13540 - Improved the structure of the hotfixes step for Smart Polling by dividing it into two chunks; retrieving additional hotfixes requires administration rights.
- N2OS-13645 - Fixed a data display issue in the Map Info panel.
- N2OS-13753 - N2OS now provides more information for failed SNMP polls.
- N2OS-13758 - N2OS can now read Mitsubishi MELSEC asset information from non-default IO modules.

- N2OS-13796 - Traces are now correctly retained when the `min_disk_free` option prevails over the `max_pcaps_to_retain` option.
- N2OS-13817 - Fixed a problem that prevented MIB files from being imported into Smart Polling.
- N2OS-13822 - Increased the timeout of the Sandbox when unzipping large files.
- N2OS-13864 - Google Chronicle data integration executes correctly.
- N2OS-13884 - Solved a problem that caused debug traces to take too much disk space.
- N2OS-13912 - Fixed an issue that lead to an IDS failure when Asset Intelligence searches for product names containing a curly bracket.
- N2OS-13962 - Fixed an issue that prevented the 'Focus On' feature to load the data of the target Guardian
- N2OS-14058 - Guardian now gives priority to asset information coming from Asset Intelligence over Smart Polling and Arc.

Security fixes

- N2OS-12937 - Hardened the Content-Security-Policy in use.
- N2OS-13725 - In Microsoft Windows environments, Arc is now deployed under C:\\Program Files\ \NozomiNetworks\\ .
- N2OS-13830 - Resolved CVE-2023-2567.
- N2OS-13910 - The AngularJS dependency was updated to a newer version.
- N2OS-14019 - Resolved CVE-2023-29245 and CVE-2023-32649.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release.

Check Point firewall integration End-of-Support

Nozomi Networks will end support for the current implementation in N2OS of the firewall integration with Check Point Gateway in an upcoming release.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.1.0

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.1.0

If you are on the release **22.6.2 or newer**:

- Upgrade directly to 23.1.0

N2OS 23.0.0

Updates in this Release - 23.0.0

This section discusses important changes in this **current** release that may require additional steps after this upgrade.

New product in the Nozomi solution: Arc

Nozomi Arc has been introduced as new product, including the needed support for N2OS. The N2OS user now can: install an Arc license both at CMC and Guardian level. Deploy Arc sensors automatically from the Arc > Arc deployment section. Manage the status and health of Arc sensors from the Sensors page. See data coming from Arc as part of the standard Network View, Asset View, and in a dedicated Node Points tab under the Arc menu. See what nodes were discovered by Arc via new values in the Capture Device field. Import an offline Arc data archive from the Import page. See alerts natively coming from Arc like SIGN:USB-DEVICE, SIGN:MALICIOUS-HID, and SIGN:SIGMA-RULE. See more contextual data on existing alert types involving nodes having Arc installed, such as the logged in users in such nodes.

Support for VMware ESXi

N2OS versions 23.0.0 and later do not support ESXi versions lower than 7.0. No deployments of Nozomi Networks virtual machines will be eligible for support on ESXi versions lower than 7.0. Additional information can be found in the release notes of version 22.6.2.

RUGGEDCOM sensors cannot support N2OS 23.0.0

N2OS 23.0.0 stability on RUGGEDCOM sensors doesn't match our quality standard. There's a probability the Sensor can remain stuck on reboot, because of this N2OS version 23.0.0 do not support RUGGEDCOM sensor. We are actively working with Siemens to resolve the current behavior as soon as possible. Additional information can be found in the release notes.

Palo Alto Networks End of Life

Because Palo Alto Networks versions 8.1, 9.0, and 10.0 have reached their end of life, Nozomi does no longer support this product in version 23.0.0 and higher. Nozomi supports and recommends Palo Alto Networks implementation version 10.1 or higher. For details, please see Palo Alto Networks community post: *https://live.paloaltonetworks.com/t5/blogs/prepare-for-end-of-life-pan-os-and-migrate-to-latest-pan-os/bc-p/462398#:%7E:text=PAN-OS*

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release.

Check Point firewall integration End-of-Support

Nozomi Networks will end support for the current implementation in N2OS of the firewall integration with Check Point Gateway in an upcoming release.

Highlights

- When viewing a snapshot in Time Machine, the Live toggle is no longer displayed.
- Guardian no longer stores alerts that are not visible under the currently selected security profile. The previous behavior (i.e., invisible alerts are kept in the database, but hidden) can be restored by using the `conf.user configure alerts save_invisible_alerts true`.
- The N2OS User Manual's "Remote Collector" chapter now includes instructions for setting the time zone.
- The Updates & Licenses page now shows whether the base and FIPS licenses were provided by Vantage.
- The N2OS User Manual now includes details about both SSH transfer options; also clarified that the example uses the SCP command.
- Fixed an issue that caused memory footprint spikes when cleaning up database entities for retention.
- The N2OS User Manual's "Queries" chapter now describes more suffix modifiers; see the "Basic Operators" section.
- The WinRM Smart Polling strategy can now retrieve vendor, model, and BIOS serial number.
- The N2OS User Manual SDK's section about sec_profile_visible now also describes incidents.
- Added the capability of specifying the TCP ports that SmartPolling uses to poll SSH servers.
- Playbooks are now introduced also in N2OS. Users can: create playbooks using markdown syntax, associate them to specific alerts, edit them also from the alert instance, and manage them both from Guardian and from the CMC as the rest of alert tuning.
- Smart Polling can now actively scan Sewio UWB devices, gather their information, and generate the corresponding CPEs.
- When closing alerts as changes using a table filter, Guardian now indicates that the action will only affect learnable alerts (VI alerts).
- The Graph's clustered layout is no longer a "beta" feature.
- The Smart Polling supported strategies have been re-organized and enabled for better Progressive Mode plans automatic configuration.
- Improved the behavior of two services: Reduced the volume of log entries generated by the n2osjobs service; now, only task runs that perform a change log their execution. Reduced the interval on which the rrdcached service writes data to disk.
- Improved the documentation about changing a password. See the N2OS User Manual for details.
- Improved the mapping for custom OIDs in the Smart Polling SNMP strategy.
- Added the ability for users to switch between the previous and the new UI navigation bar.
- The N2OS login page has been redesigned.
- Smart Polling now supports Progressive SNMP strategies.
- N2OS now manages Arc licenses for a cumulative number of sensors.
- Smart Polling can now autonomously poll nodes through UPnP using progressive mode.
- Smart Polling in Time Machine no longer displays execution-related UI elements.
- Improved the robustness of trace handling when N2OS is operating under load.

Base OS

- The N2OS User Manual lists the CPU vendors that Nozomi supports for cloud-based N2OS deployments.
- The Open Virtual Appliance (.OVA) files used to deploy Guardian, CMC, and Remote Collector in virtualized environments have been updated. For Guardian and Remote Collector the default virtual RAM allocation has been updated. The ESXi has been updated to version 7.0, the Virtual Hardware has been updated to version 17, the settings for OS compatibility have been updated to FreeBSD version 13 or later, and the SCSI controller has been updated to LSI Logic SAS.
- Updated the version of FreeBSD from 12.3 to 13.1.
- The N2OS User Manual now includes VMware deployment restrictions.
- Improved the performance of Time Machine's diff operation.
- Optimized the usage of working memory by reducing the number of web server workers.

- Users can now specify netmasks in denylists.
- Improved the detection of parallel Time Machine diff jobs.
- Minor improvements in Time Machine GUI
- Removed the `additional_rails_environment_variables.yml ''` file from the configuration directory because it isn't needed.
- By default, Time Machine now creates snapshots only from VI alerts. For details on customizing this behavior, see the N2OS User Manual.
- Reduced the repetition of error messages in Remote Collector logs.
- Time Machine now stops computing diffs with large results when the changes involve too many network elements. This threshold is configurable. See the N2OS User Manual for details.
- When importing .CID files, N2OS now imports the firmware version.
- Fixed an issue that caused N2OS to deadlock when receiving frequent ARP packets.
- Improved the handling of internal processes to optimize memory consumption.
- Updated OpenSSL to resolve CVE-2023-0286, CVE-2023-0215, CVE-2022-4450, CVE-2022-4304.
- Restored the availability of the PLC node type. This type can now be assigned again to the nodes.

Integrations

- When Guardian is integrated with Palo Alto Networks firewalls, commits are now sent only when the firewall configuration is changed.
- Nozomi has ended support for Palo Alto Networks firewalls versions lower than 10.1. More information is present in the "Current updates" section above.
- The User Manual SDK now explains the meaning of granularity and confidence as they relate to nodes mac_address:info.
- Added the record_created_at column to the following query sources: alert, audit_log, health_log, node_cves, captured_logs, report_files, node_cpes, node_cpe_changes, assertions, node_points, captured_urls and link_events. This column is populated with the timestamp when the corresponding record was created on the appliance.
- When using the N2OS SDK, the sign_in API endpoint now receives key_token as parameter.

Protocols

- Improved the accuracy of asset information extracted through the ONVIF protocol.
- N2OS now supports the SCPI (Standard Commands for Programmable Instruments) protocol, and the VXI-11 protocol.
- N2OS now supports the PSI Ketel protocol.
- N2OS now protects patients health information (PHI) inside HL7 protocol.
- Improved MAC address detection in IPv6 networks thanks to NDP protocol decoding.
- Guardian now detects the LDAP protocol on port UDP/389.
- An imprecise detection on EtherNet/IP implicit has been removed.
- Improved support for the HSR (High-availability Seamless Redundancy) protocol.

CMC and AAA

- Clarified the distinction between stale connections and sensor health in the N2OS User Manual.
- The N2OS User Manual now describes how the local default admin of Web UI is re-created after reboot (as an intended behavior) to make sure that a user cannot mistakenly delete it.
- In the "Network view", under the "Links" sub menu of CMCs configured as "all-in-one", the category "Appliance hosts" has been added to the list of columns of available information. The "Appliance hosts" category shows all sensors monitoring the nodes that form the Link.
- Improved the reliability of alerts synchronization.
- Improved the robustness of the synchronization process.
- Asset synchronization between sensors and all-in-one CMCs has been improved by using an optimized version of the asset information instead of the full asset database.

- Implemented an enhanced synchronization procedure that prevents a possible deadlock when synchronizing assets.
- When N2OS detects migration errors during an update, the propagation of the update package to all connected sensors will stop. Once all migration errors are resolved, the update package will be propagated to all connected sensors.
- Guardians now synchronize asset custom fields with CMC.
- Documentation and User Interfaces of Nozomi On-Premise and Cloud solutions have been updated to reflect the new naming nomenclature for all sources of network information that are not data integrations and/or API connections.
- Fixed an issue that could prevent the propagation of scheduled updates. Now, the UI only shows scheduled updates involving the sensor itself or the downstream connected sensors.
- Fixed an issue with the deletion of zone configurations via the clear sensor data button available in the Sensors page. In previous versions, zone configurations were deleted from the CMC only after the next restart of the IDS, while now they are deleted when the action is triggered.

Contents and detection

- Sandbox can now process larger files than previously; the limit is now the size of the `/var/sandbox` tmpfs partition. For details on configuring the size of this folder, see the N2OS User Manual.
- The old Asset Intelligence engine has been dismissed in favour of the new, more flexible and powerful one.
- N2OS now utilizes multiple Sandbox processes to handle high volumes of traffic.
- The Health page now includes a metric displaying the size of the decompressed archives in Sandbox.
- N2OS now recognizes Windows Server 1903.
- The partition size for Sandbox tmpfs is now configurable. For more information, see the N2OS user manual.
- Asset Intelligence can now enrich also the Vendor field. This enables for a more harmonized set of Vendors values across different detections. For example, having initially two original detection mechanisms yielding values "ABB Global Services Limited", and "ABB", they will both be updated to the "ABB" polished value. Check your existing queries to update them accordingly if needed.
- When the sandbox queue is about to become overloaded, N2OS now pauses the unzipping of files and archives in order to avoid the overload.
- Fixed an issue in the Threat Intelligence page that prevented users from disabling STIX indicators.
- By default, Vulnerabilities computation is disabled on new Guardians connected to Vantage or CMC. This behavior can be customized using the 'va cve enable' configuration option described in the user manual.
- Improved the memory efficiency of the jobs Update Service task.
- Fixed an issue in the Vulnerabilities page that caused a delay in the presentation of the data.
- VA no longer loads CVE files when CVE matching is disabled.

Resolved issues

- N2OS-11838 - Fixed an issue that prevented user from exporting `help XXX` queries.
- N2OS-11878 - Fixed an issue that prevented generated reports from displaying for users with limited permissions.
- N2OS-12272 - Fixed an issue that prevented some alerts related to YARA rules from being raised when a trace is replayed using its timestamps.
- N2OS-12685 - The `byte_test` option for Packet Rules now takes `operator !` into account at every call.
- N2OS-12714 - Updated the N2OS User Manual to clarify the meaning of the Is Suspended flag.
- N2OS-12724 - Fixed a display issue that prevented a button from appearing when the report widget text field was empty.
- N2OS-12758 - Fixed an issue that caused queries on node_cves ID to return a syntax error.

- N2OS-12820 - Zone configurations received by downstream appliances are now correctly removed from the CMC when the Zone configurations option in the Synchronization settings is disabled.
- N2OS-12941 - INCIDENT:NEW-NODE no longer shows entries with 00:00:00:00:00:00 as the MAC address.
- N2OS-13030 - The IPv6 **fe80::ffff:ffff:ffff:ffff** IP is no longer marked as an Asset.
- N2OS-13055 - Fixed an issue on CMC that caused outdated data to be loaded when focusing on a Guardian.
- N2OS-13227 - Fixed an issue that caused the wrong IP Source to be written to the syslog when a brute force attack was detected.
- N2OS-13244 - Fixed an issue that caused some alerts rules to be applied even after their deletion. Alert rules are no longer applied after they are deleted.
- N2OS-13465 - Fixed an issue that prevented the use of the CLI rule setting the machine limits' variables quota.
- N2OS-13481 - Mute rules with an expiration date will not shadow other tuning rules if expired.
- N2OS-13565 - Previously, when there were two or more saved queries, if a user clicked "See in editor" or "To assertion," the selected query wasn't displayed. Now, N2OS correctly populates the corresponding field with the selected query.

Security fixes

- Updated the version of AngularJS to address CVE-2022-25844 and CVE-2022-25869.
- Better parsing of time machine timestamps
- Upgraded to WolfSSL FIPS library 5.5.4.
- Updated rack to version 2.2.6.3 to address CVE-2023-27530.
- Resolved CVE-2023-24015.
- Resolved CVE-2023-22378.
- Resolved CVE-2023-22378.
- Resolved CVE-2023-22843.
- Resolved CVE-2023-23574.
- Resolved CVE-2023-23903.
- Resolved CVE-2023-24471.

Update Path Recommendation

If you are on a **20.x** release - version support for these versions has ended as of the release date of 23.0.0.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2 > 23.0.0

If you are on the release **21.9.0 or newer**:

- Upgrade to 22.6.2, then to 23.0.0

If you are on the release **22.6.2 or newer**:

- Upgrade directly to 23.0.0

N2OS 22.6.3

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Support for VMware ESXi

N2OS versions 23.0.0 and later will not support ESXi versions lower than 7.0. No deployments of Nozomi Networks virtual machines will be eligible for support unless they leverage the right ESXi and Nozomi Networks version combination as listed below:

- N2OS v23.x and Host ESXi v7.0
- N2OS v22.x and Host ESXi versions earlier than v7.0

Additional information:

1. All ESXi releases lower than version 7.0 reached the end of their General Support in the Fall of 2022.
2. The lowest version of ESXi supported by its vendor is version 7.0.
3. All users and 3rd parties must avoid using ESXi versions lower than 7.0 unless they have a special agreement with the vendor.
4. N2OS release version 22.6.x is the last N2OS release line to support ESXi versions lower than ESXi 7.0.
5. N2OS release version 23.0.0 will be the first N2OS release to be supported only by ESXi version 7.0 and higher (and virtual hardware version 14 or higher).
6. N2OS release version 23.0.0 is scheduled for General Availability in the second quarter of 2023.

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Palo Alto Networks End of Life

Because Palo Alto Networks versions 8.1, 9.0, and 10.0 have reached their end of life, Nozomi will end support for this product in an upcoming release. To prepare for these changes, Nozomi recommends that you migrate your Palo Alto Networks implementation to 10.1 or higher. For details, please see Palo Alto Networks community post: *https://live.paloaltonetworks.com/t5/blogs/prepare-for-end-of-life-pan-os-and-migrate-to-latest-pan-os/bc-p/462398#:%7E:text=PAN-OS*

Base OS

- Upgraded FreeBSD to a newer version.
- The AngularJS dependency was updated to a newer version.

Resolved issues

- N2OS-13607 - Fixed an issue that prevented non-administrative users from viewing generated Asset reports.

Security fixes

- Upgraded FreeBSD to a newer version.
- Resolved CVE-2023-2567.
- The AngularJS dependency was updated to a newer version.
- Resolved CVE-2023-29245 and CVE-2023-32649.
- Updated actionview to version 6.1.7.3 to address CVE-2023-23913.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.6.3

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.3

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.6.3

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.6.2

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Support for VMware ESXi

N2OS versions 23.0.0 and later will not support ESXi versions lower than 7.0. No deployments of Nozomi Networks virtual machines will be eligible for support unless they leverage the right ESXi and Nozomi Networks version combination as listed below:

- N2OS v23.x and Host ESXi v7.0
- N2OS v22.x and Host ESXi versions earlier than v7.0

Additional information:

1. All ESXi releases lower than version 7.0 reached the end of their General Support in the Fall of 2022.
2. The lowest version of ESXi supported by its vendor is version 7.0.
3. All users and 3rd parties must avoid using ESXi versions lower than 7.0 unless they have a special agreement with the vendor.
4. N2OS release version 22.6.x is the last N2OS release line to support ESXi versions lower than ESXi 7.0.
5. N2OS release version 23.0.0 will be the first N2OS release to be supported only by ESXi version 7.0 and higher (and virtual hardware version 14 or higher).
6. N2OS release version 23.0.0 is scheduled for General Availability in the second quarter of 2023.

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Palo Alto Networks End of Life

Because Palo Alto Networks versions 8.1, 9.0, and 10.0 have reached their end of life, Nozomi will end support for this product in an upcoming release. To prepare for these changes, Nozomi recommends that you migrate your Palo Alto Networks implementation to 10.1 or higher. For details, please see Palo Alto Networks community post: *https://live.paloaltonetworks.com/t5/blogs/prepare-for-end-of-life-pan-os-and-migrate-to-latest-pan-os/bc-p/462398#:%7E:text=PAN-OS*

Highlights

- The Health page no longer displays the discarded URLs count when the capture url feature is disabled.
- Fixed an issue that affected the behavior of shortcuts on query autocomplete.

Base OS

- Improved performance of Remote Collector. These changes result in a significant decrease in memory consumption and CPU usage and better overall reliability.
- Updated OpenSSL to address CVE-2023-0286, CVE-2023-0215, CVE-2022-4450, and CVE-2022-4304.

- Improved the robustness of N2OS against abnormal amounts of ARP packets.
- Reduced the repetition of error messages in Remote Collector logs.
- Enhanced the diagnostics information about the sensor's disk that is sent upstream.
- Updated the MAC vendors list.
- Enabled remote collector system board hardware watchdog.
- The N2OS boot sequence is now more resilient to serial port noise.

CMC and AAA

- Serial number and machine_id of physical appliances are now sent to CMC and Vantage
- Fixed an issue that caused the update bundle to be repeatedly downloaded when automatic installation was disabled.

Contents and detection

- Improved the accuracy of asset information extracted through the ONVIF protocol.

Resolved issues

- N2OS-12684 - Fixed an issue that prevented an asset's report from being produced.
- N2OS-12940 - Fixed an issue that prevented users from saving empty filters when configuring a report’s filters.
- N2OS-13061 - Fixed an issue that prevented the rendering of graphical saved queries.
- N2OS-13068 - Fixed an issue that prevented N2OS from saving reports.
- N2OS-13078 - Fixed an issue that caused a blank page to appear after login.
- N2OS-13194 - SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS are now correctly persisted.
- N2OS-13219 - Fixed an issue that prevented link bulk actions from taking effect.
- N2OS-13288 - Fixed an issue that prevented N2OS from saving user groups updates.
- N2OS-13333 - Fixed an issue that could prevent startup of the container version of the Remote Collector.
- N2OS-13391 - Fixed an issue that prevented non-administrative users from exporting queries and assets.
- N2OS-13503 - Solved a problem that prevented the refresh button and live toggle switch of saved queries from working correctly.

Security fixes

- Resolved CVE-2023-22843.
- Resolved CVE-2023-22378.
- Resolved CVE-2023-23574.
- Resolved CVE-2023-24471.
- Resolved CVE-2023-24015.
- Resolved CVE-2023-23903.
- Resolved CVE-2023-24477.
- Resolved CVE-2023-22378.
- Updated Rails to version 6.1.7.2 to address CVE-2022-44566.
- Updated globalid, nokogiri, and rack to address CVE-2023-22799, CVE-2022-44570, CVE-2022-44571, CVE-2022-44572, and GHSA-2qc6-mcvw-92cw.
- Updated the moment.js library, the diff library, and the jquery-ui library to address CVE-2022-24785, CVE-2022-31129, and CVE-2022-31160.
- Updated rack to address CVE-2023-27530.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.6.2

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.2

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.6.2

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.6.1

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Support for VMware ESXi

N2OS versions 23.0.0 and later will not support ESXi versions lower than 7.0. No deployments of Nozomi Networks virtual machines will be eligible for support unless they leverage the right ESXi and Nozomi Networks version combination as listed below:

- N2OS v23.x and Host ESXi v7.0
- N2OS v22.x and Host ESXi versions earlier than v7.0

Additional information:

1. All ESXi releases lower than version 7.0 reached the end of their General Support in the Fall of 2022.
2. The lowest version of ESXi supported by its vendor is version 7.0.
3. All users and 3rd parties must avoid using ESXi versions lower than 7.0 unless they have a special agreement with the vendor.
4. N2OS release version 22.6.x is the last N2OS release line to support ESXi versions lower than ESXi 7.0.
5. N2OS release version 23.0.0 will be the first N2OS release to be supported only by ESXi version 7.0 and higher (and virtual hardware version 14 or higher).
6. N2OS release version 23.0.0 is scheduled for General Availability in the second quarter of 2023.

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Palo Alto Networks End of Life

Because Palo Alto Networks versions 8.1, 9.0, and 10.0 have reached their end of life, Nozomi will end support for this product in an upcoming release. To prepare for these changes, Nozomi recommends that you migrate your Palo Alto Networks implementation to 10.1 or higher. For details, please see Palo Alto Networks community post: *https://live.paloaltonetworks.com/t5/blogs/prepare-for-end-of-life-pan-os-and-migrate-to-latest-pan-os/bc-p/462398#:%7E:text=PAN-OS*

Resolved issues

- N2OS-13027 - Addressed an issue affecting the performance of physical Remote Collectors.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.6.1

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.1

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.6.1

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

  Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.6.0

Correction to Release Notes

N2OS Release versions 22.5.0 and 22.5.1

Original Release Notes Excerpt:

In Release 22.2.0, plans for upgrading our Operating System (OS) from v12.x to v13.x were announced. The timeframe for the OS upgrade has changed, and it is not scheduled to take place earlier than the Fall of 2023.

Even though the OS upgrade timeframe has changed, customers are encouraged to keep in mind that a key implication of the OS upgrade is the loss of compatibility and support for ESXi versions lower than 7.0. Therefore, it is crucial that customers continue making plans to upgrade all virtual environments used to host Nozomi Networks virtual appliances to ESXi 7.0. No deployments of Nozomi Networks virtual appliances will be eligible for support unless they leverage the right ESXi and Nozomi Networks version combination as listed below:

- *Nozomi Networks OS v13.x and Host ESXi v7.0*
- *Nozomi Networks OS v12.x and Host ESXi versions earlier than v7.0*

Errors:

The timeframe for the OS upgrade has changed, and it is not scheduled to take place earlier than the Fall of 2023.

Corrections:

The timeframe for the OS upgrade has changed, and it is tentatively scheduled to take place in the first quarter of 2023.

Additional information:

1. All ESXi releases lower than version 7.0 reached the end of their General Support in the Fall of 2022.
2. The lowest version of ESXi supported by its vendor is version 7.0.
3. All users and 3rd parties must avoid using ESXi versions lower than 7.0 unless they have a special agreement with the vendor.
4. N2OS release version 22.6.0 will be the last N2OS release to support ESXi versions lower than ESXi 7.0.
5. N2OS release version 22.6.0 is scheduled for General Availability in December 2022.
6. Security patches and bug fixes will continue to be added to N2OS release version 22.6, in the form of patch releases.
7. N2OS release version 23.0.0 will be the first N2OS release to support only ESXi version 7.0 or higher (and virtual hardware version 14 or higher).
8. N2OS release version 23.0.0 is tentatively scheduled for General Availability in the first quarter 2023.

Updates in this Release - 22.6.0

This section discusses important changes in this **current** release that may require additional steps after this upgrade.

Changes to alerts, protocol and table names

In 22.6.0, we have updated the names of selected table fields and values, as described below. These changes may require user intervention to adapt saved queries, assertions, custom reports, alert rules,

and data integrations scope to the new names. In some cases, the impacts of these changes may extend beyond N2OS to include other systems such as 3rd party tools leveraging integrations into N2OS to extract information of the monitored endpoints.

Release 22.5.2 included tools to assist you in identifying where adjustments are needed, and version 22.6.0 includes tools to help migration to the new names. For more information and guidance, please visit the Knowledge Library available on the Nozomi Customer Support Portal.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization

Field in scope	Current	New	Description/ Rationale
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

For more information, see the "System, Migration Tasks" section of "User Interface Reference" chapter of the N2OS User Manual.

Updates in Upcoming Releases

This section discusses important changes in **future** releases that may require additional steps during upgrade.

Support for VMware ESXi

N2OS versions 23.0.0 and later will not support ESXi versions lower than 7.0. No deployments of Nozomi Networks virtual machines will be eligible for support unless they leverage the right ESXi and Nozomi Networks version combination as listed below:

- N2OS v23.x and Host ESXi v7.0
- N2OS v22.x and Host ESXi versions earlier than v7.0

Additional information:

1. All ESXi releases lower than version 7.0 reached the end of their General Support in the Fall of 2022.
2. The lowest version of ESXi supported by its vendor is version 7.0.
3. All users and 3rd parties must avoid using ESXi versions lower than 7.0 unless they have a special agreement with the vendor.
4. N2OS release version 22.6.x is the last N2OS release line to support ESXi versions lower than ESXi 7.0.
5. N2OS release version 23.0.0 will be the first N2OS release to be supported only by ESXi version 7.0 and higher (and virtual hardware version 14 or higher).
6. N2OS release version 23.0.0 is scheduled for General Availability in the second quarter of 2023.

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Palo Alto Networks End of Life

Because Palo Alto Networks versions 8.1, 9.0, and 10.0 have reached their end of life, Nozomi will end support for this product in an upcoming release. To prepare for these changes, Nozomi recommends that you migrate your Palo Alto Networks implementation to 10.1 or higher. For details, please see Palo Alto Networks community post: *https://live.paloaltonetworks.com/t5/blogs/prepare-for-end-of-life-pan-os-and-migrate-to-latest-pan-os/bc-p/462398#:%7E:text=PAN-OS*

Migration tasks in 22.6.0

Version 22.6.0 introduces helper tools, called **Migration Tasks**, to make use of new features or adapt to new changes. Please refer to the N2OS User Manual for more information about these tasks. This section describes the migration tasks introduced in 22.6.0.

Data Model Updates

As explained in section *Updates in this Release - 22.6.0* on page 37, version 22.6.0 introduces name changes to the data model to better describe the alert names, CVEs, and protocols. The **Data Model Updates** migration task performs automatic updates to user-defined contents, such as alert rules, data integrations, saved queries, assertions, and reports to comply with the name changes.

The changes will result in better understanding for ease of use.

Legacy Credentials Import Tasks

Version 22.6.0 introduces a **Credentials Manager**, which can be used to securely store passwords and other sensitive information used by Guardian to access hosts through Smart Polling, or decrypt encrypted transmissions detected passively. This migration task can migrate existing credentials from Smart Polling plan configurations to the new credentials manager, thus enhancing the maintainability of this kind of sensitive data.

Running this migration task is not necessary to ensure that Smart Polling works correctly in the new version, but it will organize the credentials in a more controlled way.

Highlights

- Administrators can now add a Smart Polling license from the Updates & Licenses page.
- The Report tables now display as many rows as are returned; previously, N2OS limited these results to the first 1,000 rows.
- Fixed an issue that prevented users from exporting large numbers of vulnerabilities. Now, an export is only made available for download when it's fully written to disk.
- A Migration Task dedicated to importing credentials into Credentials Manager has been added.
- Content packs now support Dashboards.
- Improved the completeness of alert-related traces.
- Updated the definitions of 'time' and 'created-time.' See the User Manual SDK details.
- Improved performance of the dashboard's Situational Awareness widget when handling a large number of links and nodes.

Base OS

- User can now enrich the assets in their asset inventory by extracting the firmware/software version from imported IEC 61850 .CID project files.
- Added an option that allows a CSV file to overwrite previously imported (or manually edited) field values.
- Guardian can now be configured as a VXLAN Tunnel End Point (VTEP) and can receive and process VXLAN encapsulated traffic.
- Fixed an issue regarding FIPS mode persistence after upgrade; this issue only affected the container version of N2OS.
- Optimized disk usage and reduced disk aging by improving the write policy for gathering metrics.
- In addition to deleting all data, the `n2os-datafactoryreset` and `n2os-fullfactoryreset` commands now also delete and recreate the file system. This enables users to address file system corruptions.
- Added more details about the actions available for assets to the "Asset View" section of the N2OS User Manual.

Integrations

- Users who integrate with Palo Alto Networks firewall versions 10 and above can now create block link policies based on configurable alert type. Since this new option works on the IP level, block link policies are triggered as long as the following fields are populated for the relevant alerts: ip_src, ip_dst, transport_protocol, and port_dst

- The DNS Reverse Lookup data integration now overwrites existing nodes labels, according to data sources, granularities, and confidence priorities.
- Improved latency of the Data Integration task for executions that don't send out any message. Now, the Kafka integration only flushes messages on socket close when needed, which is when actual messages are enqueued during task execution.

Protocols

- Improved the detection of Pelco cameras as well as the CPE generation for HTTP servers.
- Introduced support for Mac-in-mac encapsulation protocol (IEEE 802.1ah).
- Improved DeltaV asset information, function codes and variables extraction. N2OS now supports all Emerson DeltaV UDP ports. N2OS now extracts Emerson Charm I/O Card asset information. N2OS now extracts Emerson DeltaV devices primary and secondary interfaces as properties.
- Now, SIGN:UNSUPPORTED-FUNC in the Modbus context is raised only once for each function code between two given nodes.

CMC and AAA

- Improved nodes merging in certain High Availability scenarios.
- The replication of alert rules in High Availability (HA) configuration has been improved for increased consistency between the primary and secondary CMCs. Alert rules can be managed from either the primary or the secondary CMCs and now all changes will be replicated across both CMCs. Notes: Users who experience any sustained alert rules discrepancies between the primary or the secondary CMCs after this update should connect to the secondary (HA) CMC using SSH, access the Database using this command `psql -U n2os-dbms scadaguardian` and delete all alert rules using this command `delete from alert_rules ;` Next, users should connect to the primary CMC using SSH, access the Database using this command `psql -U n2os-dbms scadaguardian` and restart the replication using this command `update alert_rules set replicated = false;` This will initiate a new replication from the primary CMC to the secondary CMC and will eliminate any discrepancy in the alert rules between the primary and secondary CMCs
- Documented the conditions when the appliance will not automatically update. See the N2OS User Manual for details.
- Added documentation of the behavior of the primary group on the Active Directory server, and described why it is not visible in the Nozomi Networks Operating System (N2OS). See the N2OS User Manual for additional details.
- Updated the N2OS User Manual to better describe user privileges needed to connect and integrate with Active Directory.

Contents and detection

- Improved the performance of synchronization for the node_cpes table.
- Hotfixes in Asset Details are now presented with more details, separating minimum and latest hotfix.
- Asset Intelligence is now empowered by more robust matching logics at the N2OS level, and the new logic are now enabled by default.
- N2OS now detects Windows 22H2 versions.
- N2OS now searches VBA and XLM filetypes for malicious content.

Resolved issues

- N2OS-12338 - Fixed an issue that prevents zones import if no other options other than the name and subnet are specified.
- N2OS-12532 - Fixed an issue that prevented N2OS processes from restarting when disabling environment synchronization on the CMC.
- N2OS-12515 - Fixed a parsing issue that affected the PDF output of reports.

- N2OS-12568 - The Network graph is now capable of displaying and handling large amounts of nodes.
- N2OS-12139 - N2OS now preserves links information when restoring a backup on a different appliance.
- N2OS-12585 - Fixed a UI issue that prevented applied filters from being displayed in scheduled reports after the user left the page.
- N2OS-12479 - Fixed the sort order of query results when they were sorted by a numeric extended field.
- N2OS-12603 - Addressed a limitation that would cause issues with the startup and shutdown process of an internal software service if started and stopped several times within an extremely short period of time.
- N2OS-12649 - Fixed an issue that prevented the web server from starting up or shutting down correctly.
- N2OS-12609 - Fixed an issue that caused SP WinRM strategies to fail when `$historyCount` was zero.
- N2OS-12083 - Updated the N2OS User Manual to indicate that passwords have a 12-character minimum.

Security fixes

- The Checksum calculation is now performed using SHA256; previously, MD5 was used.
- Updated the WolfSSL FIPS library to version 5.5.3.
- Upgraded software dependencies to resolve CVE-2022-23514, CVE-2022-23515, CVE-2022-23516, CVE-2022-23517, CVE-2022-23518, CVE-2022-23519, and CVE-2022-23520.
- Upgraded Ruby to resolve the vulnerability CVE-2021-33621.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.6.0

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.6.0

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.6.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.

- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

  Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.5.2

Correction to Release Notes

N2OS Release versions 22.5.0 and 22.5.1

Original Release Notes Excerpt:

In Release 22.2.0, plans for upgrading our Operating System (OS) from v12.x to v13.x were announced. The timeframe for the OS upgrade has changed, and it is not scheduled to take place earlier than the Fall of 2023.

Even though the OS upgrade timeframe has changed, customers are encouraged to keep in mind that a key implication of the OS upgrade is the loss of compatibility and support for ESXi versions lower than 7.0. Therefore, it is crucial that customers continue making plans to upgrade all virtual environments used to host Nozomi Networks virtual appliances to ESXi 7.0. No deployments of Nozomi Networks virtual appliances will be eligible for support unless they leverage the right ESXi and Nozomi Networks version combination as listed below:

- *Nozomi Networks OS v13.x and Host ESXi v7.0*
- *Nozomi Networks OS v12.x and Host ESXi versions earlier than v7.0*

Errors:

The timeframe for the OS upgrade has changed, and it is not scheduled to take place earlier than the Fall of 2023.

Corrections:

The timeframe for the OS upgrade has changed, and it is tentatively scheduled to take place in the first quarter of 2023.

Additional information:

1. All ESXi releases lower than version 7.0 reached the end of their General Support in the Fall of 2022.
2. The lowest version of ESXi supported by its vendor is version 7.0.
3. All users and 3rd parties must avoid using ESXi versions lower than 7.0 unless they have a special agreement with the vendor.
4. N2OS release version 22.6.0 will be the last N2OS release to support ESXi versions lower than ESXi 7.0.
5. N2OS release version 22.6.0 is scheduled for General Availability in December 2022.
6. Security patches and bug fixes will continue to be added to N2OS release version 22.6, in the form of patch releases.
7. N2OS release version 23.0.0 will be the first N2OS release to support only ESXi version 7.0 or higher (and virtual hardware version 14 or higher).
8. N2OS release version 23.0.0 is tentatively scheduled for General Availability in the first quarter 2023.

Upcoming updates

Changes to alerts, protocol and table names

In 22.6.0, we will update the names of selected table fields and values, as described below. These changes may require user intervention to adapt saved queries, assertions, custom reports, alert rules, and data integrations scope to the new names and structures. In some cases, this impact may extend beyond N2OS to include other systems' integrated endpoint logics.

Release 22.5.0 includes tools to assist you in these interventions. For more information and guidance, please visit the Knowledge Library available on the Nozomi Customer Support Portal.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields

Field in scope	Current	New	Description/ Rationale
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Highlights

- The outdated connection status message caption reading "API connection error" has been adjusted to read "Slow connection". This new message caption accurately represents the current status of the condition of the connection into the Guardian's web user interface..

Contents and detection

- Reduced Guardian's RAM consumption when a large number of STIX indicators is loaded.

Security fixes

- Resolved CVE-2022-4259.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.5.2

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.5.2

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.5.2

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on

disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.

- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.5.1

Upcoming updates

Changes to alerts, protocol and table names

In 22.6.0, we will update the names of selected table fields and values, as described below. These changes may require user intervention to adapt saved queries, assertions, custom reports, alert rules, and data integrations scope to the new names and structures. In some cases, this impact may extend beyond N2OS to include other systems' integrated endpoint logics.

Release 22.5.1 includes tools to assist you in these interventions. For more information and guidance, please visit the Knowledge Library available on the Nozomi Customer Support Portal.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods

Field in scope	Current	New	Description/ Rationale
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Base OS

- Clarified the text for the auto logout toggle switch tooltip.
- Improved the Time Machine user interface to provide better operability and intuitiveness.

Contents and detection

- Sandbox is now able to disable the analysis of files resulting from the unzipping of compressed archives based on their advertised file extension.

Resolved issues

- N2OS-12429 - Fixed the generation of XLSX reports, which was not working correctly in 22.5.0.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.5.1

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.5.1

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.5.1

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.5.0

Upcoming updates

Changes to alerts, protocol and table names

In 22.6.0, we will update the names of selected table fields and values, as described below. These changes may require user intervention to adapt saved queries, assertions, custom reports, alert rules, and data integrations scope to the new names and structures. In some cases, this impact may extend beyond N2OS to include other systems' integrated endpoint logics.

Release 22.5.0 includes tools to assist you in these interventions. For more information and guidance, please visit the Knowledge Library available on the Nozomi Customer Support Portal.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods

Field in scope	Current	New	Description/ Rationale
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Highlights

- Users can now add images to Reports using the new Image Widget.
- Renamed RTU_ID to Namespace in the process view.
- Fixed an issue that prevented the query help command from showing all of a table's fields in some cases.
- Improved the look and feel of the import section.
- N2OS now sanitizes data retrieved from the Smart Polling Powershell strategy before inserting it into the PostgreSQL database.
- You can now execute Log4j detection via Smart Polling on older Windows 7 systems with limited Powershell capabilities.
- The CMC now contains a new tab under Appliances that displays a graph of the topology of the connected appliances (1 level down from the CMC). On the graph, the color of the CMC and connected appliances' icons represent their current health. The colors and their meanings are as follows: Green is for good health, Orange is for average health, Red is for poor health, and Black is used when an appliance is unreachable. Please note that if connected appliances (1 level down from the CMC) have other appliances connected to them (2 levels down from the CMC), the "worse" health out of all connected appliances will be the health represented by the appliance (1 level down from the CMC). Additionally, the color of the links between the CMC and the appliances (1 level down from the CMC) represent the current status of the connection. The colors and their meanings are as follows: Green is for good connection, and Black is for stale connection.
- Documented import options for IEC61850 (SCL files), Triconex, Allen Bradley, and Honeywell TDS platforms. See the N2OS User Manual.
- Added documentation describing Smart Polling progressive mode. See the N2OS User Manual.

Base OS

- Improved the performance of the Time Machine functionality in Guardian.
- Purdue levels are now assigned to a broader set of asset types.
- Fixed an issue that sometimes caused the failed login message to report an incorrect IP address.

- Assets deletion is now correctly synchronized to CMC and Vantage.

Integrations

- Added support for IPv6 addresses for the Palo Alto V10 firewall.
- The N2OS OpenAPI now supports importing Threat indicators.
- N2OS now supports SMTP forwarding with empty username and password.
- Introduced New Data Integration for Google Chronicle.
- You can now specify the shared firewall service name when configuring a Barracuda firewall integration.
- Added in-product documentation for Microsoft Endpoint Configuration Manager (WinRM RPC) Data Integration.
- Improved documentation of the asset_id field. See the N2OS User Manual SDK.

Protocols

- Guardian now supports de-encapsulation from the HP-ERM encapsulation protocol.
- CVEs are now generated for some Honeywell Experion devices.
- Yokogawa Vnet/IP function codes support has been extended.
- N2OS now uses the MCU version as the reported firmware version for Avalue Renity ARTEMIS UWB Smart Polling Detection.
- Improved detection of potentially malicious operations applied through the EtherNet/IP protocol.
- N2OS now displays the correct Windows version for deltaV workstations.
- N2OS now sets the correct DeltaV controllers label.
- Fixed an issue that caused a a false positive alert about empty request path for the EtherNet/IP protocol.
- Introduced garbage collection of obsolete protocol connection (.pcn) files Please note: 1) We added a new GC process to clean out old/outdated Connection Manager files stored in the /data/cfg/connections folder; and 2) Only 2 protocols use this process: Profinet and Ethernet/IP.

CMC and AAA

- Appliances now send their asset count to the upstream appliance.
- Administrators can now edit and delete zones that are created in the local appliance even when the propagation policy for zones is local only.
- Improved the reliability of alerts synchronization between Guardian and CMC.
- Administrators can now edit and delete zones that were created in the local appliance, even when the propagation policy for zones is upstream only.
- Fixed an issue that caused duplicate records of the health_logs, alert_event, alert_events_alerts, audit_items, node_cpe_changes, and telemetry_events tables; note that this issue only occurred when the CMC was configured in High Availability mode.

Contents and detection

- The default Security Profile is now Medium. After first run this can be changed in the Administration Settings.
- Added performance and load information about the sandbox service in the Health page.
- Improved the responsiveness of Sandbox during startup and when the directory for the extracted files is full.
- Users can globally disable Alert and Sandbox engine contents if/when needed.
- Users can manually configure the types of files, and the type of traffic that are analyzed in the search for malware.
- Sandbox now presents improved statistics on the number of processed and discarded files.

- Improved the web UI by unifying and simplifying the Hotfix and Patches tabs.
- Previously, the High Load badge for Sandbox was displayed based on an absolute metric. Now, it is displayed based on the relative load of the application.

Resolved issues

- N2OS-12112 - Sandbox now clearly reports the number of files being dropped due to various network and system reasons.
- N2OS-12046 - Fixed an issue that prevented users with Health group permission from accessing the Services tab in the Health page.
- N2OS-12137 - Fixed a retention mechanism issue regarding continuous traces.
- N2OS-12068 - Fixed an issue in the evaluation of the state of the appliances in cases when of two CMCs connected in High Availability.
- N2OS-12205 - Fixed an issue affecting communication between a Guardian and a CMC in High Availability mode when the primary goes down.
- N2OS-12052 - Improved the export UI by removing an unhelpful component that showed the number of items and pages.
- N2OS-12201 - Fixed an issue that caused CMC to display a second, redundant Smart Polling page.
- N2OS-12368 - Fixed an issue that caused upgrade problems when custom asset types with apostrophe (') characters were used.
- N2OS-12041 - Fixed an issue that prevented user define closing reasons to appear when single alerts were closed.
- N2OS-11588 - Updated the N2OS User Manual to clarify that, in Phase 1 initial setup of Guardian, the prompt for the admin password applies only to virtual Guardians, and not physical appliances.
- N2OS-12276 - Removed incorrect documentation details regarding the configuration of retention of quarantined files.

Security fixes

- Upgraded to Puma 5.6.4 to address CVE-2022-24790 and CVE-2022-23634.
- Updated FreeBSD to version 12.3-RELEASE-p7 to resolve CVE-2022-37434.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.5.0

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.5.0

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.5.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add

a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.

- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.4.0

Upcoming updates

Changes to alerts, protocol and table names

In 22.6.0, we will update the names of selected table fields and values, as described below. These changes may require user intervention to adapt saved queries, assertions, custom reports, alert rules, and data integrations scope to the new names and structures. In some cases, this impact may extend beyond N2OS to include other systems' integrated endpoint logics.

Release 22.5.0 includes tools to assist you in these interventions. For more information and guidance, please visit the Knowledge Library available on the Nozomi Customer Support Portal.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods

Field in scope	Current	New	Description/ Rationale
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

FireEye TAP End-of-Support

Because FireEye TAP (Threat Analytics Platform) has reached its end of life, Nozomi will end support for this product in an upcoming release. The first step of end-of-support will remove the ability to create new FireEye TAP integrations.

Highlights

- The N2OS web UI is now available in Simplified Chinese.
- Improved the Remote Collector health status when nodeid_factory is configured.
- N2OS now supports licenses generated with AES SHA256.
- Improved communication on the data channel between Remote Collectors and Guardian, especially when many Remote Collectors send data at the same time. Please note: Remote Collector and Guardian must have the same version number. Remote collectors at versions prior to 22.4 can't communicate with Guardians at version 22.4 and above.
- Introduced a new Smart Polling strategy to poll BACnet devices and obtain asset information.
- N2OS now raises running status alerts based on polled information by the Siemens S7 Smart Polling strategy.
- Added USB-port details to the N2OS User Manual. See "Additional Settings" in the Installation chapter.
- Updated the N2OS User Manual to clarify that only the following traces are retained with a full-backup: 1. those generated via Request custom trace (from Other actions) 2. those generated via Request a trace (from Nodes and Links), and 3. those generated from Alerts.
- Introduced a new Smart Polling operational mode, called Progressive Mode. When enabled, it automatically creates plans on behalf of the user based on the information acquired from the passive module. For example, a Linux machine is automatically polled by the `ssh` strategy. For now, the functionality is included only for strategies that don't require credentials.

Base OS

- Rockwell Harmony RSX and RSH files can be directly imported. More information such as Serial Number, Device ID and Product Code is now also extracted.
- Introduced new healthcare asset types.
- Added a shell command `n2os-import-project-file` that can be used to manually import configuration files that are too big to upload via the UI.
- Improved the detection of migration errors.

- Fixed an issue that affected the migration of custom asset_types from `n2os.conf.gz` to the database.

Integrations

- N2OS now supports a new data integration for Microsoft Endpoint Configuration Manager that queries the CM Database for values in these views: v_GS_OPERATING_SYSTEM, v_GS_NETWORK_ADAPTER_CONFIGUR, v_Add_Remove_Programs, and V_GS_Quick_Fix_Engineering.

Protocols

- N2OS now passively detects Moxa NPort devices.
- N2OS now supports the DICOM protocol. N2OS currently detects roles, function codes, protocol version, and process variables.
- N2OS now extracts the serial number of DeltaV devices.
- N2OS now provides passive and active detection of RTLS-UWB for Artemis Avalue Smart Retail Solutions devices.
- Improved support for the MMS/61850 protocol via the ability to extract the complete Data model from imported SCD files; variable names now follow the complete 61850 syntax.

CMC and AAA

- Upon user login, N2OS now reads the user's groups from the AD server and updates the user's N2OS groups to match.
- N2OS now supports the bulk deletion of zone configuration.
- During synchronization, the CMC now sends the appliance mode (either multi_context or all_in_one) to the upstream appliance.
- The LDAP user integration now uses the memberOf, isMemberOf and groupMembership attributes in addition to the gidNumber attribute to retrieve the groups a user belongs to. Also, upon user login, the mapping between the user and the user groups that the user belongs to is refreshed and updated from the LDAP server.
- CLI and Custom CLI actions now provide a more reliable execution statuses in case of errors.
- Downstream appliances no longer send synchronization calls to upstream appliances for tables that are not supported by the upstream appliances.

Contents and detection

- Asset Intelligence is now empowered by more robust matching logic at the N2OS level. The new logic is disabled by default; we recommend enabling it for testing.

Resolved issues

- N2OS-12178 - Fixed a problem that caused the IDS service to be killed at startup time upon loading of large configurations, thus causing the application become unresponsive.
- N2OS-12199 - Fixed an issue that prevented the ThreatIntelligence page from displaying the list of installed STIX indicator files.
- N2OS-11636 - STARTTLS is now enabled by default for the SMTP Forwarding data integration.
- N2OS-11480 - Fixed an issue that prevented the All and None selection buttons from functioning properly when more than 20 zones were selected.
- N2OS-11836 - Fixed an issue that prevented Guardian from sorting alert rules in the correct order.
- N2OS-11700 - Administrators can now set password policies via the CLI.

- N2OS-11471 - Fixed an export issue that occurred when users navigated away from the Alerts page.
- N2OS-11659 - Fixed an issue that prevented assets autocomplete from working on CMC or Guardian when no nodes were loaded in memory.
- N2OS-11739 - The CMC identity provider can now be configured from the CLI.
- N2OS-12064 - Improved the web UI's resilience when handling null values.
- N2OS-12080 - Fixed an issue that prevented the Product Lifecycle Status column from appearing in the assets list even when selected by the user.

Security fixes

- Updated FreeBSD to address CVE-2022-23089, CVE-2022-23090, and CVE-2022-23091

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.4.0

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.4.0

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.4.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.3.0

Upcoming updates

Changes to alerts, protocol and table names

In an upcoming release, we will update the names of selected table fields and values, as described below. These changes may require user intervention to adapt saved queries, assertions, custom reports, alert rules, and data integrations scope to the new names and structures. In some cases, this impact may extend beyond N2OS to include other systems' integrated endpoint logics.

Before releasing these changes, Nozomi Networks will provide tools and guidance to ensure a smooth transition to assist you in these interventions.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods

Field in scope	Current	New	Description/ Rationale
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

Highlights

- Smart Polling now detects General Electric D400 devices.
- N2OS now supports the FirmwareChange alert for the VnetIPProtocol.
- The N2OS reporting engine now supports Chinese, Japanese, and Korean characters when generating PDF files.
- Fixed an issue that caused false positive Teardrop alerts.
- In order to enforce the minimum free disk trace that is set, continuous traces now check for available disk space every time a new segment starts.
- Smart Polling's MELSOFT strategy now retrieves the firmware version for Mitsubishi GOT devices from the external SD card.
- Query results are now sorted in the order specified by the `select` command.
- The WinRM Smart Polling Strategy now correctly handles backslashes for Active Directory accounts.
- Queries using the `uniq` command now support specific field names.
- The positions of nodes in the graph now stay fixed when in 2D Purdue view.
- Improved the stability of firmware extraction for the S7 Smart Polling Strategy for devices consisting of multiple racks and slots.
- The S7 Smart Polling strategy can now extract the module information, serial, status, and firmware version for the modules on the same rack as the polled node.
- Improved concurrency handling in the S7 Smart Polling strategy.
- You can now specify the interval at which individual assertions are checked (valid values range from 10 seconds to 1 day); the default is 10 seconds.
- Improved the performance and memory usage of the queries `bucket` command when executed on a data source residing in the database.
- Introduced the concept of 'Related node' for Incidents where the object can be either a source or a destination.

Base OS

- N2OS can now extract device modules information from Siemens S7 Plus traffic.

  Improved the parsing of Siemens AML files to support importing device submodules.
- For SNMP monitoring purposes, added the ability to return n2os-version from the `UC-SNMP-MIB::extOutput.0` query.

- Added the possibility to use the node label as Device ID for nodes belonging to a specific zone. This helps the asset consolidation for networks where a label represent a unique device.
- N2OS now provides feedback details when you import nodes and variables. In addition, import is validated against the Denylist; N2OS prevents import if validation fails.
- Administrators can now configure a set of live traffic labels transformations that harmonize the labels to create a uniform label format. Such transformations can be configured at the global level or per protocol.
- Node custom fields are now stored in the database.
- Updated the WolfSSL FIPS library to version 5.3.0.

Integrations

- N2OS now supports the Barracuda Networks firewall. The integration supports nodes blocking and links blocking policies.
- The OpenAPI now supports authentication with bearer tokens. OpenAPI keys can only be assigned to local users.
- Improved the authentication mechanism used by the Cisco ISE data integration:

  Admins can now provide a 3rd party CA certificate that N2OS uses for SSL peer verification of the Cisco ISE endpoint during authentication.

  Added a new parameter named `client name` that N2OS uses as the user name with pxGrid during authentication to avoid conflicts when the Cisco ISE data integration is configured on multiple N2OS appliances.

Protocols

- Extended the support for IEC 61850 MMS to extract more process variables when sent via an Information Report.
- Improved the HTTP passive detection of Fanuc devices and the corresponding generation of CPEs.

CMC and AAA

- Updated configuration documentation about LDAP. See the Users chapter in the N2OS User Manual for details.

Contents and detection

- Improved handling of out-of-order packets, especially in relation to packet and YARA rules. In addition, quarantined sandbox files are now moved (rather than being copied) from the analysis folder.
- Improved the management of Windows KB contents.
- N2OS now passively detects Siemens SINAMICS Drives and returns vendor, product name, and firmware version.
- Improved IP fragmentation to correctly handle TCP flags for packet rules.
- The Sandbox process is now configurable. See the N2OS User Manual for details.
- N2OS now writes messages to the Sandbox logs when YARA rules are matched.

Resolved issues

- N2OS-11644 - N2OS now generates CPEs from the Ethernet/IP Smart Polling strategy.
- N2OS-11609 - Fixed a parsing issue that affected the PDF output of reports.
- N2OS-11611 - Fixed an issue that caused learned nodes to toggle in presence of DHCP traffic.

- N2OS-11596 - Fixed an issue that prevented the user from adding a note to a trace in the "Upload traces" page.
- N2OS-11713 - Fixed an issue that caused zones configured as upstream on a Guardian and CMC to remain active even after they were deleted from the CMC.
- N2OS-11653 - Improved the identification of the ONVIF (Open Network Video Interface Forum) protocol.
- N2OS-11645 - Fixed an issue with Guardians in HA mode that could prevent the CMC from managing alerts provided by downstream appliances.
- N2OS-11860 - Fixed a migration issue related to asset types execution policies.

Security fixes

- Updated the Nokogiri parser to address CVE-2022-29824.
- Updated the Nokogiri parser to address CVE-2022-29181.
- Updated a dependency to address CVE-2022-30123 and CVE-2022-30122

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.3.0

A rollback from a version newer than 20.0.7.7 to 20.0.7.7 is not supported.

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.3.0

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.3.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.2.1

Upcoming updates

In the near future, we are going to update the names of some table fields and values, as described in this table.

The updates are intended for use in N2OS, including saved queries, assertions, custom reports, alert rules, integrations scope. In the case of an integration, changes may apply also outside N2OS, i.e. on the integrated endpoints logics.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization

Field in scope	Current	New	Description/ Rationale
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

Resolved issues

- N2OS-11655 - Fixed an issue that caused VLAN tagged traffic to be discarded on Intel network interfaces.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.2.1

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.2.1

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.2.1

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.

N2OS 22.2.0

Upcoming updates

In the near future, we are going to update the names of some table fields and values, as described in this table.

The updates are intended for use in N2OS, including saved queries, assertions, custom reports, alert rules, integrations scope. In the case of an integration, changes may apply also outside N2OS, i.e. on the integrated endpoints logics.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization

Field in scope	Current	New	Description/ Rationale
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

Highlights

- Service n2osjobs is now automatically restarted on a Remote Collector's TUI.
- Added new functionality for tracking extended network statistics over time. The new fields last_1hour_bytes, last_1day_bytes and last_1week_bytes can be queried for 1 hour, 1 day, and 1 week, similar to the existing 5, 15, and 30 minute increment fields. The feature must be enabled in the feature Control Panel first, then in the Zones configuration tab. Check the User manual for important configuration details.
- Added `help [query_source]` commands in order to show the description of each field in the source.
- Added an `assertion_element_monitoring` setting that enables assertion alerts to re-trigger when the alert is closed but the assertion still fails. New alerts are also triggered for new elements that contribute to the failure of an already-failing assertion.
- In Smart Polling, you can now import MIBs that have been renamed.
- You can now configure the site, description, and compression strategies for the Remote Collector from the TUI.
- N2OS now validates the syntax of the JSON when you import a dashboard from a JSON file.
- Improved resiliency and usability when importing malformed MIBs. Also improved the UX/UI for the SNMP Smart Polling plan.
- Improved the visualization of alert details.
- Improved timeout handling for the SNMPV3 SP strategy.
- Fixed an issue that caused flickering links when the Graph was paused.
- In the 3D Graph Purdue Model graph, fixed an issue that caused blurry text and red arrows under specific view angles.
- Improved the active detection of asset data through Mitsubishi protocols.
- In the N2OS User Manual's License section, updated the license status description and related behavior that occurs when a base license expires or exceeds the node limit.

Base OS

- You can now collect the list of from/to ports used by links for a specified set of protocols.
- You can now import a CSV file with new variables or update the variables' label, unit, scale, and offset fields.
- Improved support for our upcoming appliance model NS20. The `n2os-hwinfo --psu` command now returns the status of PSU.
- Updated the list of embedded MAC addresses' vendors.
- Made minor visual improvements to the administration page's side navigation panel.

Integrations

- Improved handling of alerts in peak conditions (that is, more than 300 alerts every 5 seconds) for the following data integrations: CEF, Cisco ISE, QRadar (LEEF), ServiceNow, SMTP forwarding, SNMP Trap, Splunk, and FireEye.
- The FortiGate v6 firewall integration now supports VDOM in transparent mode as well as the ability to send policies in disabled status.
- Updated the N2OS User Manual SDK to clarify that an authenticated Nozomi user must belong to a group with Queries and exports permission in order to execute api/open/query.

Protocols

- Improved the creation of CPEs for the ENIP protocol; it is based on the inference of the existence of multiple devices behind a gateway-like device.
- N2OS now supports the CIP Security protocol.
- N2OS now supports the Honeywell CDA protocol. Variables support for Honeywell DSA protocol has been deactivated. Links previously detected as DSA may now be detected as CDA.
- Added support for the Honeywell FSC-DS protocol.

CMC and AAA

- Smart Polling node points, plans, executions and status information are now synchronized from Guardian to CMC. The synchronization of these entities is disabled by default, but it can be enabled from the Tuning tab of the Administration -> Synchronization settings menu. Only node points produced after the synchronization was enabled are sent from Guardian to CMC. The retention of these objects can be configured.

  CMC has a new Smart Polling page. Smart polling plans configured in underlying Guardians, their execution status and the polled nodes are displayed in this page. This information is diagnostic only. It is not possible to make changes to plans and to add, remove or execute plans.

  CMC now shows Software and Hotfixes tabs for assets. These tabs are populated with the information extracted from Smart Polling plans as it occurs in Guardian.
- Updated the N2OS User Manual to clarify filter restrictions: in CMC Multicontext, if a user belongs to multiple groups, and at least one group is non-admin with restrictions on appliances, nodes, or zones, then the most restrictive filter is applied to the user.
- Documented the ports and protocols required to access Vantage. For details, see the N2OS User Manual.
- Added improved and expanded the N2OS User Manual section about High Availability. Please see the user manual for details.

Contents and detection

- N2OS now correctly computes Windows CPEs versions for 20H2, 21H1, and 21H2.
- Refined the behavior of the alert type VI:KB:UNKNOWN-PROTOCOL, inhibiting the ones for links having unknown protocols ("other", "tcp/xx") without any payloads.
- Administrators can now disable the generation of CPEs, and therefore CVEs, for selected nodes.
- Improved the generation of SNMP CPEs for Hirschman devices with long product names.
- Improved the performance of application CPEs generation in N2OS VA.

Resolved issues

- N2OS-11569 - If an appliance is synchronized with an upstream CMC or with Vantage, and a proxy has been configured in the synchronization settings, the same proxy is also used to download Threat Intelligence and Asset Intelligence updates from the upstream appliance.

- N2OS-11275 - Addressed an issue that prevented saving changes to the configuration of the internal firewall.
- N2OS-11449 - Fixed an issue that affected node labels that included spaces.
- N2OS-11510 - The Dahua Smart Polling detection strategy has been integrated with the creation of the related node points.
- N2OS-11328 - Fixed a version migration issue related to asset types.
- N2OS-11323 - Fixed an issue that prevented users from disabling the "Generate Assets From IPv6 Nodes" option.
- N2OS-11247 - Improved the user experience of the upload pcaps feature in cases when multiple pcaps are replayed.
- N2OS-11440 - Assets with multiple IPs no longer display Smart Polling duplicated statistics.
- N2OS-11340 - Fixed an issue with reports exported to CSV and Microsoft Excel formats.
- N2OS-11554 - Fixed an issue that caused the following configuration settings to be invalidated after the appliance was configured to synchronize with Vantage: `cmc bulk_sync`, `cmc send_bundle_without_updating`, `cmc sync send_only_visible_alert`.
- N2OS-11273 - Improved the resilience of n2os_ids when handling corrupted saved sessions.
- N2OS-11326 - Fixed an issue that caused the bulk report mail to be re-sent when both SMTP relay and SMTP server were configured to send on-demand and scheduled reports.
- N2OS-11332 - Fixed an issue in which closing alerts from the table could result in the closure of other alerts unintentionally.
- N2OS-11454 - Fixed an issue that prevented the legend from displaying in the 'Alerts flow over time' dashboard widget.
- N2OS-11262 - N2OS now ensures that packet rules with the 'http_header' specification do not match outside the header.
- N2OS-11439 - Fixed an issue in the handling of queries using `day_hour`. Be careful when accounting for daylight saving time. Use `day_hour_utc` when absolute precision is desired.
- N2OS-11559 - Fixed an issue that caused malformed zone definitions in the configuration file to prevent upgrade to newer versions of N2OS.
- N2OS-11288 - The Guardian UI now correctly displays the source and destination node for assertions involving `node_cves`.
- N2OS-11491 - Fixed an issue when generating CPE versions for the MySQL protocol.
- N2OS-11345 - Improved learning of Links in the network view.
- N2OS-11369 - Updated the definition of a variable in the N2OS User Manual.

Security fixes

- Updated a dependency to address CVE-2022-28739.
- Removed the `X-Runtime` response header and normalized the login response time. In addition, messages about users being locked are not longer enabled by default. To enable them, run the `conf.user configure authentication paranoid_mode false` CLI command, followed by a unicorn restart via `service unicorn stop`.
- Removed an invalid and non-functional sign up page from the N2OS log in screen.
- Updated a dependency to address CVE-2018-25032.
- Updated FreeBSD in order to resolve CVE-2018-25032, CVE-2022-23088, CVE-2022-23086, CVE-2022-23087, CVE-2022-23084, and CVE-2022-23085.
- Updated a software dependency to resolve CVE-2021-44906.
- N2OS now supports FIPS (Federal Information Processing Standards) with a FIPS-140-2 approved cryptography module. For more information, please see the N2OS User Manual.
- Upgraded N2OS to FreeBSD 12.3.

Update Path Recommendation

If you are on a **19.x** release - version support has ended as of March 1st, 2022

- Please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.2.0

If you are on a **21.x older than 21.9.0**:

- 21.x > 21.9.0 > 22.2.0

If you are on the release **21.9.0 or newer**:

- Upgrade directly to 22.2.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
            docker exec -d <CID> \
            bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /
data/dump-updatev"
```

  Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.
- To restore a backup made from a version < 19.0.5, perform restore process in a version < 20.0.0, then execute update.

N2OS 22.1.0

Upcoming updates

In the near future, we are going to update the names of some table fields and values, as described in this table.

The updates are intended for use in N2OS, including saved queries, assertions, custom reports, alert rules, integrations scope. In the case of an integration, changes may apply also outside N2OS, i.e. on the integrated endpoints logics.

Field in scope	Current	New	Description/ Rationale
alerts: type_id	SIGN:TCP-MALFORMED	SIGN:NET-MALFORMED	This type also covers malformed items outside of TCP
alerts: type_id	SIGN:FIRMWARE-CHANGE	SIGN:FIRMWARE-TRANSFER	The type describes a firmware transfer not necessarily related to a change
alerts: type_id	SIGN:PROGRAM-DOWNLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	SIGN:PROGRAM-UPLOAD	SIGN:PROGRAM-TRANSFER	Different definitions of download/upload coexist in the OT/IT world
alerts: type_id	VI:NEW-SCADA-NODE	VI:NEW-NODE (existing)	The current name is obsolete. The added value of the differentiation with VI:NEW-NODE is not relevant
alerts: type_id	SIGN:SCADA-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:NETWORK-MALFORMED	SIGN:MALFORMED-TRAFFIC	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:SCADA-INJECTION	SIGN:PROTOCOL-INJECTION	Removed differentiation between OT and IT protocols
alerts: type_id	SIGN:TCP-SYN-FLOOD	SIGN:TCP-FLOOD	Removed differentiation between TCP SYN and other TCP floods
alerts: type_id	VI:NEW-LINK	VI:NEW-LINK-GROUP	Name harmonization
alerts: type_id	VI:NEW-PROTOCOL	VI:NEW-LINK (existing)	Name harmonization

Field in scope	Current	New	Description/ Rationale
alerts: type_id	NEW-PROTOCOL-APPLICATION	VI:NEW-LINK (existing)	Name harmonization
alerts: type_id	NEW-PROTOCOL-CONFIRMED	VI:NEW-LINK-CONFIRMED	Name harmonization
node_cves: resolved_reason	resolved_reason	minimum_hotfix, latest_hotfix	Name correctness, as well as articulated the concept into 2 separated fields
Honeywell FSC DS protocol	honeywell-sis	honeywell-fsc-ds	Name correctness for links and sessions

Highlights

- You can now disambiguate traffic coming from different Remote Collectors using the site property of each appliance.
- Smart Polling logs no longer include clear text passwords.
- Added source information to the label field.
- Improved support for Mitsubishi Q Series, iQ-R Series, GOT1000 Series, and GOT2000 Series in Smart Polling.
- Fixed an issue during restore that resulted in the removal of network elements after a backup was restored to a different machine.
- The container edition of N2OS now supports the Backup/Restore feature.
- Removed the **Environment Information** dashboard widget from the list of available widgets for dashboards of CMC's operating in Multi-context mode. This widget is only intended to be used for CMC's operating in All-In-One mode.
- Enhanced the `n2os-tui` with a new section that controls bandwidth throttling.
- Queries that operate on the database json fields (that are in memory) now support the main arithmetic operators, such as sum.
- Improved the update message in the Appliance pane for container Remote Collectors.
- Documented the query syntax for comparing fields. For example: `links | where from_zone == $to_zone | select from_zone to_zone`. For details, see the N2OS User Manual.

Base OS

- Added support for upcoming appliance model NS1.
- Added support for upcoming appliance model NS20.
- Improved the resilience of certain update migration paths.
- Introduced two new lock files, n2os.conf.user.lock and n2os.conf.gz.lock, which are stored in the same folder as other configuration files (/data/cfg). These the lock files are used to improve the consistency of configuration files when they are updated.

Integrations

- Add transparent mode support to Fortigate v6 firewall integration.

Protocols

- Improved the detection of SIEMENS SIPROTEC 5 devices
- Improved the asset detection capabilities for devices speaking IEC 61850 and ABB Relion devices

- If a device has multiple network interfaces and sends information about its interfaces via the Foundation Fieldbus protocol, as in the case of Honeywell controllers with FTE (Fault Tolerant Ethernet), this information is now used to avoid duplicate IP address alerts and node renaming operations. Note that this feature depends on the availability of network interface information on the Foundation Fieldbus protocol, which may not be available depending on the context.

CMC and AAA

- During synchronization, the interval between data merge tasks is the now same as the synchronization interval. For example, if synchronization is set to an interval of one hour, the merge task also occurs at hourly intervals.
- Improved the synchronization of assets assets in certain bulk delete cases involving HA.

Contents and detection

- Guardian can now generate CPEs and match CVEs for the LS-XGT protocol.
- Introduce active and passive support for the detection of Dahua Thermal Cameras
- Threat Intelligence now checks all available licenses when upgrading contents via a manual update.
- Added further improvements to passive and active detection of Schneider-Electric/APC PDUs.
- Fixed an issue that prevented the quarantine folder from having the corresponding file for certain alerts related to transferred files.

Resolved issues

- N2OS-10769 - Added a check for duplicated zones during zone configuration import. Also fixed an issue related to importing zone configuration properties.
- N2OS-10868 - Fixed an Asset Inventory report generation problem for assets containing multiple IP addresses.
- N2OS-10914 - Fixed an issue that prevented the correct removal of zones from a user group.
- N2OS-10961 - Fixed an issue that prevented the the security profile from being used properly in widgets based on alerts source.
- N2OS-11093 - Fixed an issue that prevented the deletion of a user that was propagated from the upstream appliance when its user group was changed to a one that was not propagated.
- N2OS-11038 - Improved parsing of the MAC vendor information for assets actively monitored by Guardian resulting in increased accuracy of MAC vendor information and merging of active assets that are shared upstream to a Central Management Console (CMC)
- N2OS-11117 - Fixed an issue when querying captured_urls
- N2OS-11124 - Fixed an issue related with the `expand` and `group_by` query keywords
- N2OS-11052 - Fixed a graphical issue related to the "Overview" widget in reports.
- N2OS-11056 - Fixed an issue related to closing the custom query window.
- N2OS-11196 - Fixed an issue that created a non-existent node when a node delete rule was executed.
- N2OS-10112 - Corrected the title of the Trend Micro TXOne EdgeIPS section of the user manual so it matches the Guardian web UI.

Security fixes

- Updated a dependency to address CVE-2021-30560.
- N2OS now detects Lanner devices.
- Updated a dependency to address CVE-2022-23633.

Update Path Recommendation

If you are on a release older than **19.0.11 (version support has ended)**

- 19.x > 20.0.0 > 20.0.7.7 > 21.9.0 > 22.1.0
- **Note:** please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.1.0

If you are on a **21.x**:

- 21.x > 21.9.0 > 22.1.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
        docker exec -d <CID> \
        bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /data/
dump-updatev"
```

  Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.
- To restore a backup made from a version < 19.0.5, perform restore process in a version < 20.0.0, then execute update.

N2OS 22.0.0

Highlights

- Improved the alert and trace retention mechanisms by adding advanced retention options.
- Smart Polling now detects Log4J on Windows and Unix machines.
- Port scan incidents can now be configured in terms of the minimum alerts to be triggered and the maximum time interval for the detection.
- Support for Mitsubishi Q Series, iQ-R Series, GOT1000 Series, GOT2000 Series in Smart Polling
- Guardian can now import SNMP MIBs through the GUI.
- Adding Content Pack functionality. The user can now export a single file containing groups of Reports and Queries, and then import it on another machine, resulting in the same items appearing in the target system.
- Added the advertised header length and the actual length to the UDP low layer validation alert.
- Improved Guardian's reliability when generating traces for alerts triggered by packet rules.
- Restructured the UX/UI of the administration pages, as well as updating the tab navigation inside all the pages of the web application.
- Fixed minor consistency issues in the ordering of the Links and Sessions table columns.
- Improved the S7 Smart Polling strategy.
- The N2OS SDK User Manual now correctly lists the `value` field of `node_points` table as deprecated; instead of this deprecated field, please use the `content` field.

Base OS

- Improved the audit log by adding Zone Configuration activities.
- The remote collector may now run within a Docker instance on the ARM64 architecture. This allows for greater flexibility in deployments and unique orchestration for users deploying the remote collector. To utilize this platform, there is a new folder within the GA release build called ‘N2OS_Container_RC_ARM’. This folder contains the necessary docker files, install scripts, and the content required to build the docker image. For advanced configuration details, licensing, pairing with Guardian, and insights into the full utilization of the remote collector on docker, please see the N2OS User Manual for full details.
- Improved syntax checking for the CLI. The new CLI command `find_cmd` lets users search the list of available commands.
- Added is_from_public and is_to_public fields to Session.

Integrations

- Improved the in-product documentation for the ServiceNow data integration.
- Added `traces` and `continuous traces` retention sections in GUI.
- Improved the serialization of information concerning sessions being killed by firewall integrations.
- The N2OS User Manual now calls out the features that require Guardian to be in protecting/strict mode.

CMC and AAA

- Improved nodes merging. For each node, the CMC provides a list of appliances from which it receives the node data.
- Improved RBAC granularity: added new options to view and make changes in the Threat Intelligence section; also added an option to view in the Audit section.

- Added a new RBAC permission that restricts API queries to specific tables. RBAC for the "Query and Export" permission has been extended to consider "View" permissions. Previously, if the "Query and Export" permission was enabled, users could query any API endpoint. Now, users can only query API endpoints they have permission to "View". This applies to the following: Assets, Vulnerabilities, Trace requests, Link events, Captured urls, Alerts, Process, Appliances, Threat Intelligence, Sessions, Reports, and Health information This new permission is granted retroactively to users who previously had access via the broader permission. If the user had "Query and export" permission before, the new permission and the rest of the "View" permissions are enabled automatically. This ensures backwards compatibility without enabling providing access to data that was previously unavailable.
- CMCs and Guardians now properly handle the Retry-After response received from Vantage. As a result of such responses, the synchronization process is paused until Vantage becomes available once again.
- The N2OS User Manual now provides configuration instructions for HA.

Contents and detection

- N2OS now supports defragmented payloads for HTTP packet rules.
- N2OS now supports passive detection of Schneider/APC PDUs.
- Smart Polling now supports Schneider PDU active detection.
- Improved the VA vulnerabilities recalculation performance.
- Improved packet rules documentation by expanding upon the syntax and semantics of packet rules. Please see the N2OS User Manual.

Resolved issues

- N2OS-8026 - Fixed an issue that prevented Guardian from deleting the CPEs of deleted nodes.
- N2OS-11071 - Fixed a regression in the SNMPV3 SP strategy where password fields were grayed out.
- N2OS-10871 - Smart Polling is no longer installed in connected appliances if their Relative Version Locked option is enabled.
- N2OS-10977 - Fixed an issue that prevented execution of the n2os-diskfull-emergency script.
- N2OS-10976 - Fixed an issue that caused the health logs to be exported as empty Excel or CSV file.
- N2OS-11012 - Fixed an issue that could cause time synchronization issues on appliances running on Hyper-V.
- N2OS-11014 - Fixed an issue that prevented scheduled local backups from being created.
- N2OS-11082 - Fixed an issue that prevented the download of the support archive in the container edition.
- N2OS-11142 - Fixed an issue that prevented the download of locally stored backups.
- N2OS-10958 - Fixed an issue in which graph icons could sometimes appear with an anomalous border.
- N2OS-10082 - Fix and issue that caused an empty path request to raise a false positive alert for EthernetIP.
- N2OS-10980 - Fixed an incorrect query example in the N2OS User Manual. The arrays example now correctly includes expand parents.

Security fixes

- During login, if matching against the gid number does not produce any result, LDAP login is now performed case insensitive.
- Fixed a security issue concerning the upload logo function in reports.
- Updated the version of FreeBSD to resolve CVE-2021-29632.

Update Path Recommendation

If you are on a release older than **19.0.11 (version support has ended)**

- 19.x > 20.0.0 > 20.0.7.7 > 21.9.0 > 22.0.0
- **Note:** please see update remarks of 20.0.0 (listed below for convenience).

If you are on a **20.x release older than 20.0.7.7**:

- 20.x > 20.0.7.7 > 21.9.0 > 22.0.0

If you are on a **21.x**:

- 21.x > 21.9.0 > 22.0.0

20.0.0 update remarks

- If upgrading from a version < 18.5.9 see update remarks of 19.0.0.
- Version 20.0.0 introduces SSH key based authentication and blocks SSH password login for the `root` user. SSH password login is allowed only when using the `admin` user. If you are upgrading from version 18.5.9 to version 20.0.0, or if you don't use the admin user yet, you'll need to add a SSH key using the WebGUI in order to be able to login. Refer to the user manual for more information about how to configure SSH keys.
- Ensure enough space is available in `/data` before update execution. As a rule of thumb check that the appliance has at least 15% of free disk space or at least 5GB free. To perform an exact check use the `n2os-db-stats` command to gather the database size and check that the free space on disk is bigger that the sum of all the tables. The update process can take a long time, depending on the amount of data and the complexity of the system, but it generally takes less than a few minutes.
- To update a Docker container edition a manual database dump is mandatory:

```
        docker exec -d <CID> \
        bash -c "pg_dump scadaguardian -U n2os-dbms | gzip -9 > /data/
dump-updatev"
```

  Where <CID> is the container id of your current running container. After dump execution stop old container and start the new one.
- To restore a backup made from a version < 19.0.5, perform restore process in a version < 20.0.0, then execute update.