Guardian and Central Management Console

Maintenance Guide

N2OS v25.0.0 — 2025-03-18

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction **5**
System overview 7
Core services 9
Chapter 2. Backup and Restore **11**
Scheduled backups 13
Do a full backup from a shell console 16
Do a full backup from the web UI 17
Schedule a full backup from the CMC web UI 18
Schedule a full backup from the Guardian web UI 20
Download a backup archive from the web UI 21
Delete a backup archive from the web UI 22
Upload a backup archive in the web UI 23
Do a backup of the environment from a shell console 24
Do a full restore from the web UI 25
Do a full restore from a shell console 26
Do a restore of the environment from a shell console 27
Chapter 3. Reboot and Shutdown **29**
Reboot or shutdown the system from the web UI 31
Reboot or shutdown the system from a shell console 32
Chapter 4. Software update and rollback **33**
Software updates and rollbacks 35
Do a software update from the web UI 37
Schedule a software update from the web UI 38
Do a software update from a shell console 41
Do a software rollback from a shell console 42
Chapter 5. Reset **43**
Do a data factory reset 45
Do a data factory reset with sanitization 45
Do a full factory reset with sanitization 47
Chapter 6. Miscellaneous **49**
Host-based intrusion-detection system 51
Action on log disk full usage 52
Generate a support archive file 53
Glossary 55

Chapter 1. Introduction

System overview

The Nozomi Networks solution includes partitions and a filesystem structure, along with core system services to help administer and maintain the solution in a production environment.

Table 1. Partition and filesystem layout

N2OS - First partition (/)	Main partition that includes a copy of the operating system. The operating system runs from this partition. Two different partitions deliver fast-switch between a running release and the new version.
N2OS - Second partition (/)	Partition that coordinates with the first partition to provide reliable update paths.
OS Configuration partition (/cfg)	Partition on which files are copied at the start of the bootstrap process. Contains low-level *operating system (OS)* configuration files, such as network configurations, shell admin users, etc
Data partition (/data)	Partition that contains all user data, such as learned configuration, user-imported data, traffic captures, and persistent database.

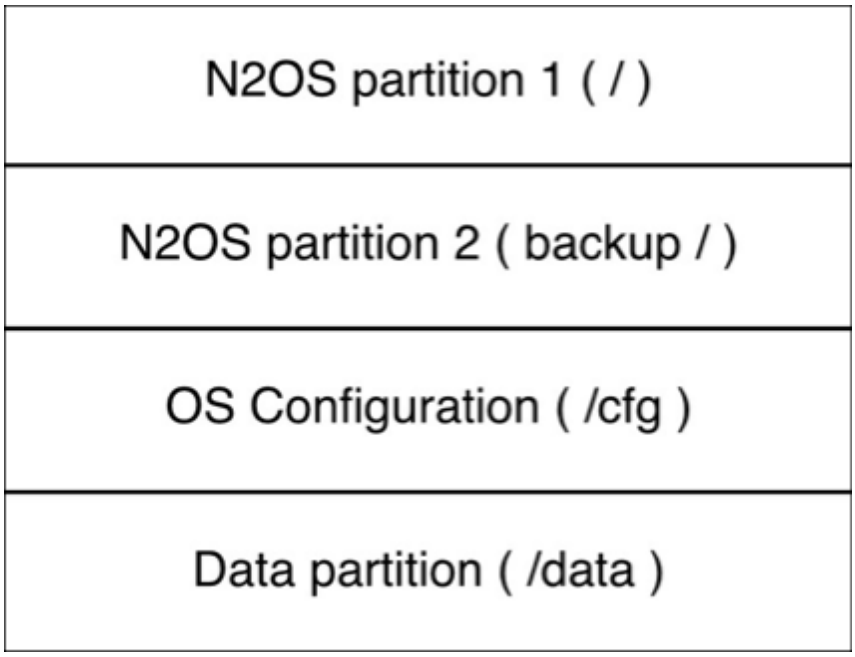


Figure 1. Partitions

The data partition includes these sub-folders:

- **cfg**: Includes all automatically learned and user-provided configurations. Two main configuration files are stored here:
  - **n2os.conf.gz**: For automatically learned configurations
  - **n2os.conf.user**: For additional user-provided configurations
- **data**: Working directory for the embedded relational database, used for all persistent data
- **traces**: Includes all traces, which are rotated when necessary
- **rrd**: Includes aggregated statistics, which is used for traffic, among others

Core services

The system services used for proper configuration and troubleshooting.

n2osids

The main monitoring process that can be controlled with:

```
service n2osids <operation>
```

`<operation>` can be either start or stop. After a stop, the service restarts automatically. This is true for every service. The log files start with `n2os_ids*` and are located under `/data/log/n2os`

n2ostrace

The tracing daemon that can be controlled with:

```
service n2ostrace <operation>
```

The log files start with `n2os_trace*` and are located under `/data/log/n2os`

n2osva

The asset Identification and Vulnerability Assessment daemon that can be controlled with:

```
service n2osva <operation>
```

The log files start with `n2os_va*` and are located under `/data/log/n2os`

n2ossandbox

The file sandbox daemon that can be controlled with:

```
service n2ossandbox <operation>
```

The log files start with `n2os_sandbox*` and are located under `/data/log/n2os`

nginx

The web server behind the web interface that provides a secure *hypertext transfer protocol secure (HTTPS)* service, and can be controlled with:

```
service nginx <operation>
```

Use of these services requires that you obtain permission using the `enable-me` command. For instance, the following commands allow you to restart the n2osids service:

```
enable-me
service n2osids stop
```

Several other tools and daemons are running in the system to deliver *Nozomi Networks Operating System (N2OS)* functionality.

Chapter 2. Backup and Restore

Scheduled backups

You can schedule full backups from the web UI.

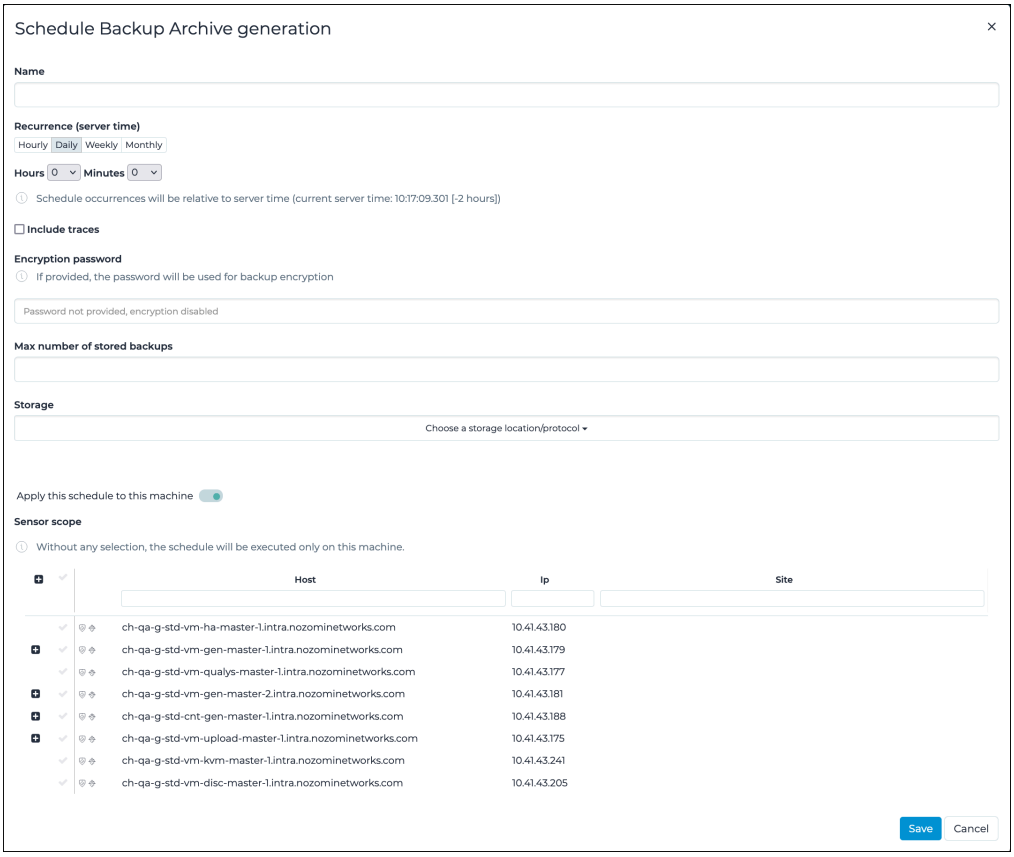


Figure 2. Schedule Backup Archive generation settings - CMC

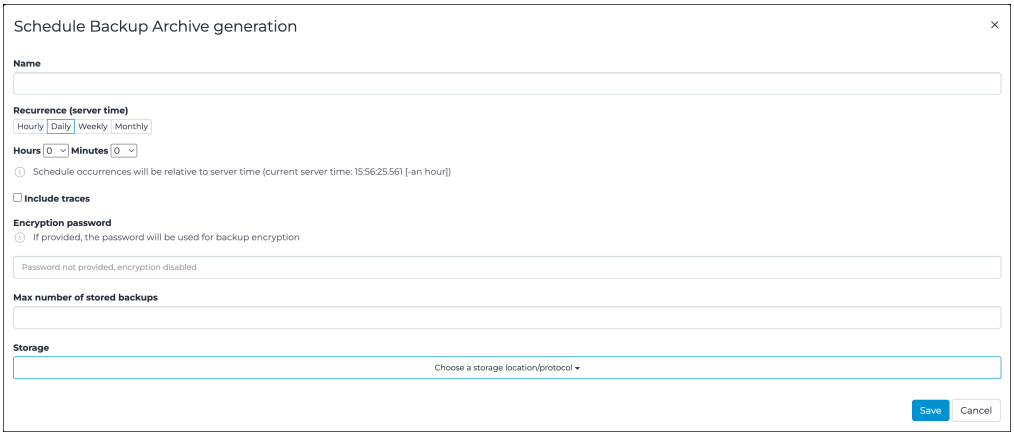


Figure 3. Schedule Backup Archive generation settings - Guardian

Recurrence (server time)

You can set how often the backups are saved. You can choose from:

- Daily
- Weekly
- Monthly

You can then set the hour and minutes for the time that you want the backup to occur.

Include traces

By default, traces are not included in backups. You can select the **Include traces** checkbox to include them. This option is also available for scheduled backups. Continuous traces are not included in the **Include traces** option.

Encryption password

If you enter a password in this field, users will be prompted to enter a password to do a backup or a restore.

Max number of stored backups

This field lets you enter a number to set the maximum number of backups that will be stored. When a new scheduled backup generates, the system confirms that the maximum number of backups will not be exceeded, and if needed, deletes the oldest backup.

Connection protocol

This dropdown lets you select a protocol to use for the connection. You can use a protocol to choose a remote location for storing backups, such as:

- *secure shell (SSH)*/ *secure copy protocol (SCP)*
- *file transfer protocol (FTP)*
- *server message block (SMB)*

Note:

SSH/*simple file transfer protocol (SFTP)* is not supported.

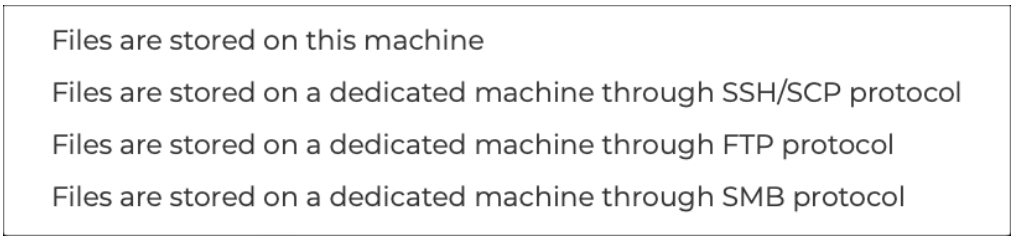


Figure 4. Connection protocols

Important:

The remote backup option that uses *SMB* is only supported for use with Microsoft *OS*s. Compatibility with third-party devices is not guaranteed. These devices might require additional configuration changes, including, but not limited to:

- Permission changes
- The creation of new network shares
- The creation of new users

Kerberos authentication is not supported.

Do a full backup from a shell console

You can do a full backup from the sensor shell console.

About this task

When you perform a full backup, only the following traces are retained:

- Those generated via **Request custom trace** (from **Other actions**)
- Those generated via **Request a trace** (from **Nodes and Links**)
- Those from **Alerts**

Procedure

1. Open a shell console.
2. To create a new backup, enter the command:

   ```
   n2os-fullbackup
   ```

3. Download the backup file.

   Note:

   For example:

   ```
   scp admin@<sensor_ip>:/data/tmp/
   <backup_hostname_date_version.nozomi_backup> .
   ```

Results

The backup file has been saved to the folder.

Do a full backup from the web UI

You can do a full backup from the web UI.

About this task

When you perform a full backup, only the following traces are retained:

- Those generated via **Request custom trace** (from **Other actions**)
- Those generated via **Request a trace** (from **Nodes and Links**)
- Those from **Alerts**

Procedure

1. In the top navigation bar, select 

   Result: The administration page opens.

2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. **Optional:** If necessary, in the **Generate Backup Archive** section, select the **Include traces** checkbox.
4. In the **Generate Backup Archive**, select **Download**.

Results

The backup file has been saved to your **Downloads** folder.

Schedule a full backup from the CMC web UI

You can schedule a full backup from the Central Management Console (CMC) web UI.

About this task

When you perform a full backup, only the following traces are retained:

- Those generated via **Request custom trace** (from **Other actions**)
- Those generated via **Request a trace** (from **Nodes and Links**)
- Those from **Alerts**

Procedure

1. In the top navigation bar, select 

   Result: The administration page opens.

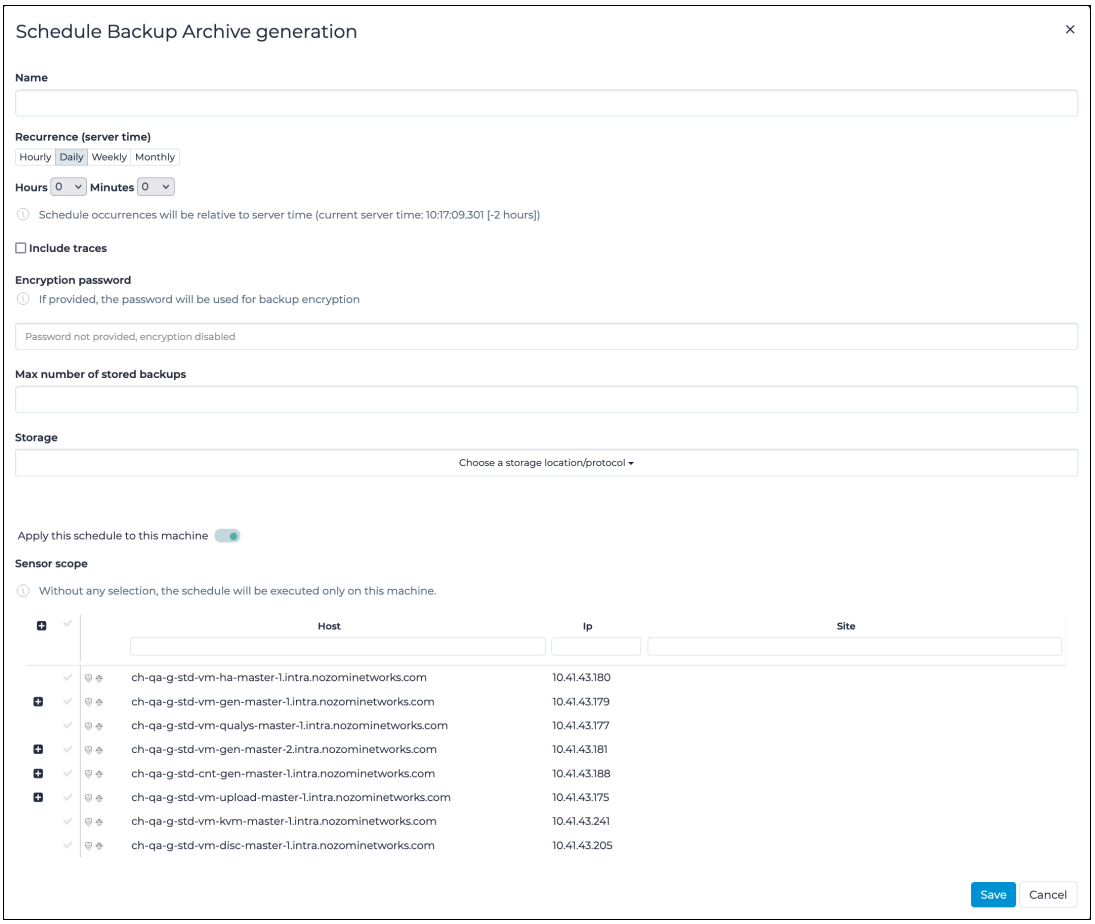
2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. In the **Schedule Backup Archive generation** section, select **Schedule backup**.

   Result: A dialog shows.

4. Select the settings as necessary.



5. If necessary, apply the schedule to downstream sensors.
    a. Select the **Apply this schedule to this machine** toggle to on.
    b. Select the applicable download sensors.
6. Select **Save**.

Results

The backup has been scheduled.

Schedule a full backup from the Guardian web UI

You can schedule a full backup from the Guardian web UI.

About this task

When you perform a full backup, only the following traces are retained:

- Those generated via **Request custom trace** (from **Other actions**)
- Those generated via **Request a trace** (from **Nodes and Links**)
- Those from **Alerts**

Procedure

1. In the top navigation bar, select 

   Result: The administration page opens.

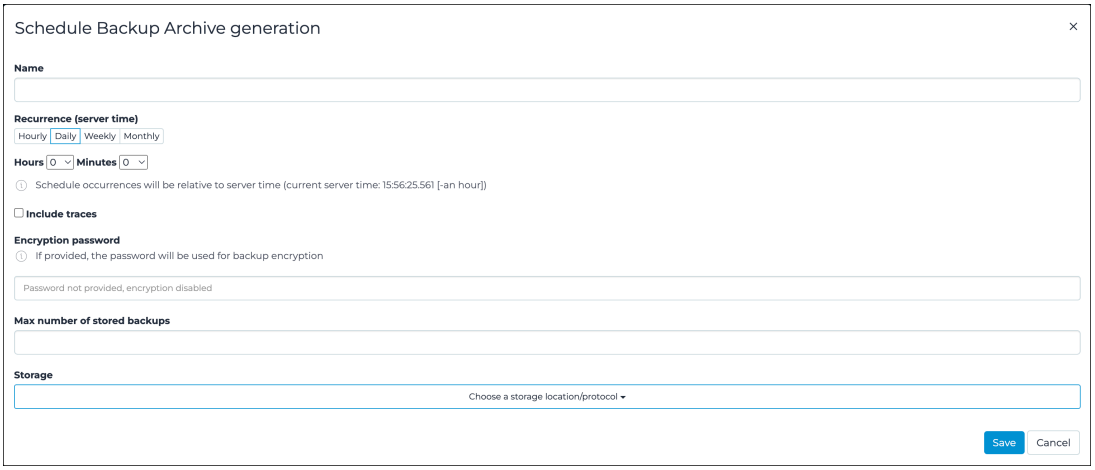
2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. In the **Schedule Backup Archive generation** section, select **Schedule backup**.

   Result: A dialog shows.

4. Select the settings as necessary.



5. Select **Save**.

Results

The backup has been scheduled.

Download a backup archive from the web UI

You can do a download a backup archive from the web UI.

Procedure

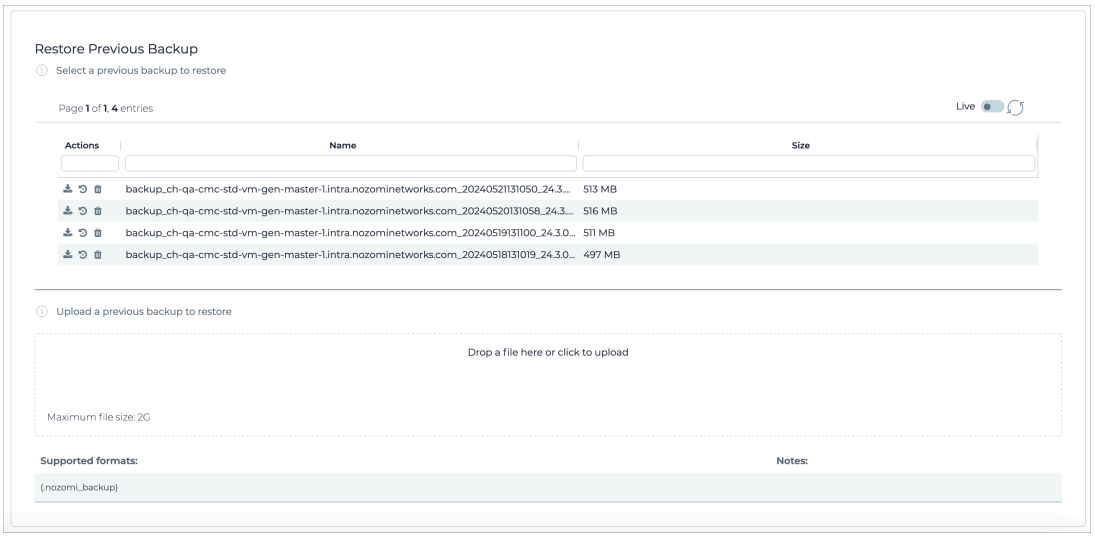
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. In the top right section, select **Restore**.
4. In the **Restore Previous Backup** section, find the applicable backup archive.



5. To the left of the required backup archive, select the ⬇ icon.

Results

The download of the backup archive starts.

Delete a backup archive from the web UI

You can do a delete a backup archive from the web UI.

Procedure

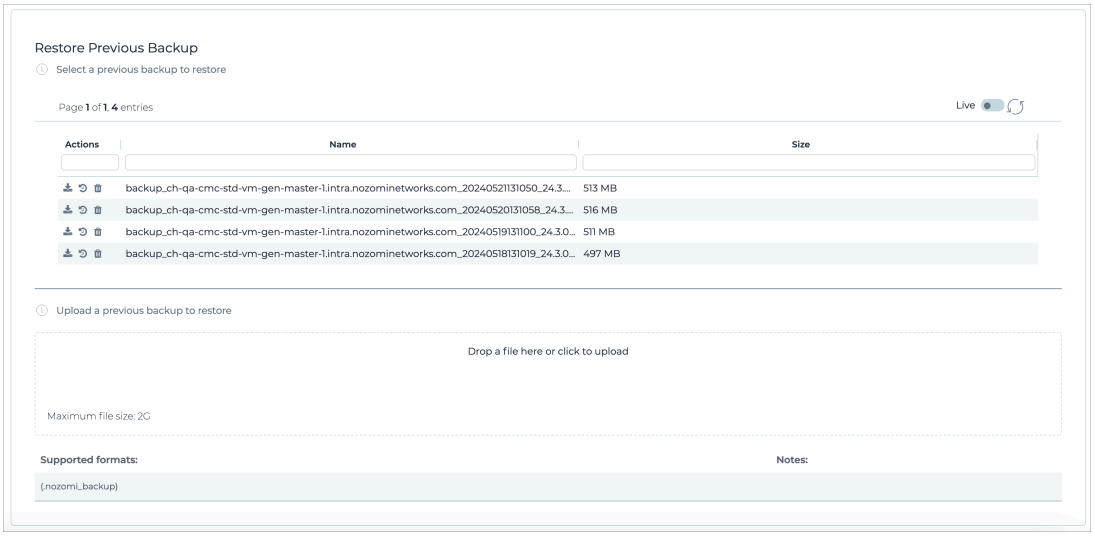
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. In the top right section, select **Restore**.
4. In the **Restore Previous Backup** section, find the applicable backup archive.



5. To the left of the required backup archive, select the 🗑 icon.

Results

The backup archive has been deleted from the disk.

Upload a backup archive in the web UI

You can do a upload a backup archive in the web UI.

About this task

It is possible to upload a backup archive from your local machine. For example, a backup that was previously created from the command-line, or downloaded from the Web UI.

Procedure

1. In the top navigation bar, select 

   Result: The administration page opens.

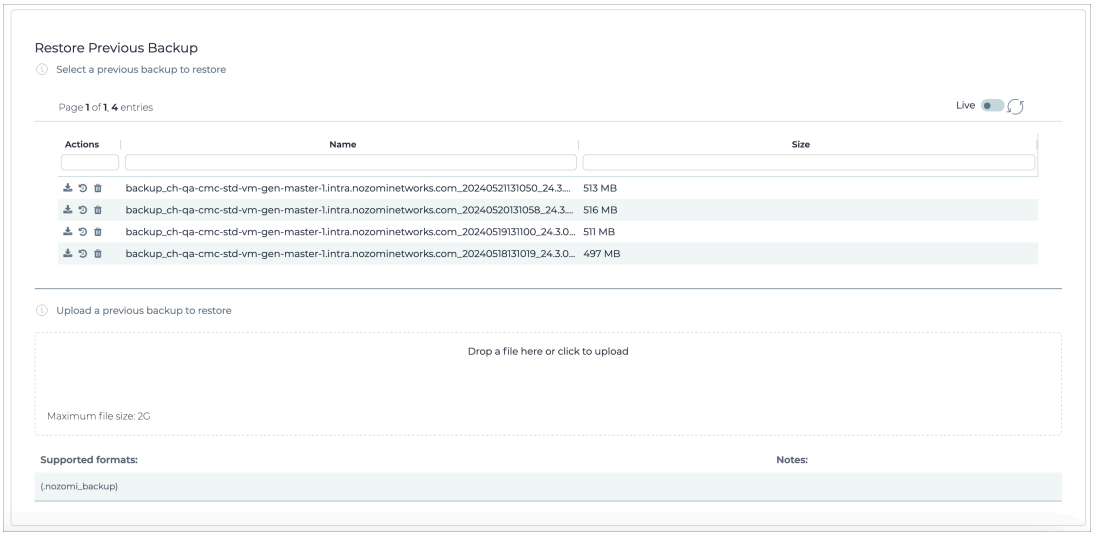
2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. In the top right section, select **Restore**.
4. Locate the backup archive file.
5. Choose a method to upload the backup archive file:

   Choose from:

   - Drag the backup archive file into the **Drop a file here or click to upload** field
   - Click in the **Drop a file here or click to upload** field and locate the file to be uploaded



Results

The backup archive file upload starts.

Do a backup of the environment from a shell console

You can do a backup of an existing environment from the sensor shell console.

Procedure

1. In the top navigation bar, select 

   Result: A menu shows.

2. In the **Settings** section, select **CLI**.

   Result: The **CLI** page opens.

3. In the CLI, enter the command:

   ```
   save
   ```

4. Copy the `/data/cfg` folder to a backup location.

Results

The environment backup has been saved in your backup location.

Do a full restore from the web UI

You can do a full restore from the web UI.

About this task

All automatically scheduled backups that exist on the disk will be listed in the **Restore Previous Backup** section.

Procedure

1. In the top navigation bar, select 

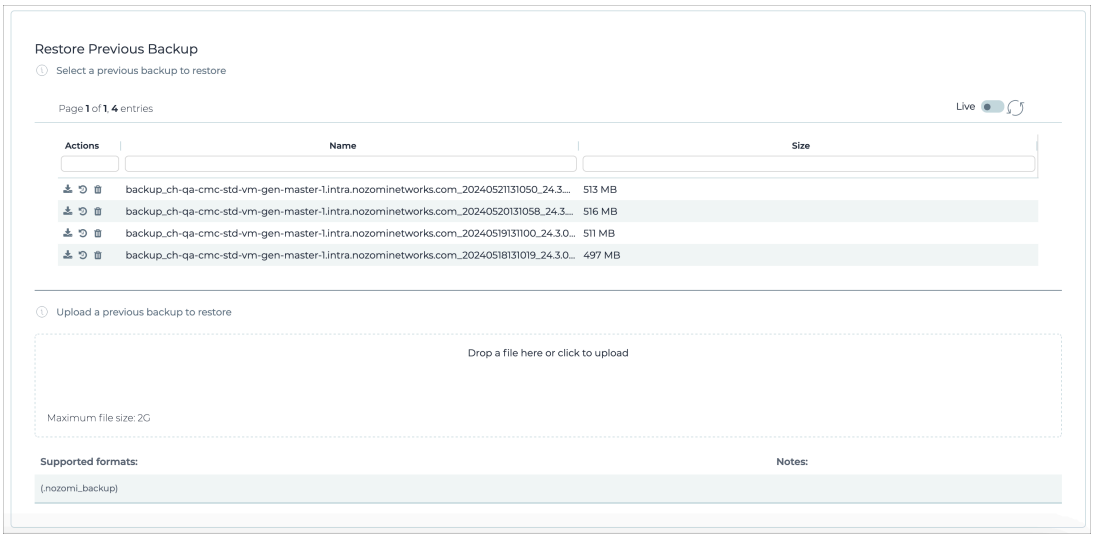
   Result: The administration page opens.

2. In the **System** section, select **Backup and restore**.

   Result: The **Backup and restore** page opens.

3. In the top right section, select **Restore**.

4. To the left of the required backup archive, select the  icon.



Results

The full restore process starts.

Do a full restore from a shell console

You can do a full restore from the sensor shell console.

Procedure

1. Open a shell console.
2. Locate the backup archive.
3. Use the *SFTP* or *SCP* to copy the backup archive to the `admin@<appliance_ip>:/data/tmp/<backup_hostname_date_version.nozomi_backup>` path of the sensor.

   Note:
   For example, enter the command:

   ```
   scp
    <backup_location_path>/<backup_hostname_date_version.nozomi_b
   ackup>
   admin@<appliance_ip>:/data/tmp/
   <backup_hostname_date_version.nozomi_backup>
   ```

4. In the shell console, enter the command:

   ```
   n2os-fullrestore /
   data/tmp/<backup_hostname_date_version.nozomi_backup>
   ```

   Note:
   You can use the `--etc_restore` option to restore the files from the `/etc` folder. This feature can be used with a backup produced from version 20.0.1 and newer.

Do a restore of the environment from a shell console

You can do a restore of the environment on an existing installation from the sensor shell console.

Procedure

1. Open a shell console.
2. Copy the saved content of the `cfg` folder to the `/data/cfg` folder into the sensor.
3. In the shell console, enter the command:

```
service n2osids stop
```

Results

The environment has been restored.

Chapter 3. Reboot and Shutdown

Reboot or shutdown the system from the web UI

You can reboot or shutdown the system from the web UI.

About this task

The reboot and shutdown commands are performed from the web UI. Alternatively, you can perform both commands from the shell console (inside an *SSH* session).

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **Operations**.

   Result: The **Operations** page opens.

3. Choose the action that you want to do:

   Choose from:

   - In the top left corner, select **Reboot**
   - In the top left corner, select **Shutdown**

Results

The system reboots or shuts down.

Reboot or shutdown the system from a shell console

You can reboot or shutdown the system from a shell console.

About this task

The reboot and shutdown commands are performed from a shell console (inside an *SSH* session). Alternatively, you can perform both commands from the Web UI.

Procedure

1. Open a shell console.
2. Choose the action that you want to do:

   Choose from:

   - To reboot the software, enter the command:

     ```
     enable-me
     shutdown -r now
     ```

   - To shutdown the software, enter the command:

     ```
     enable-me
     shutdown -p now
     ```

Results

The system reboots or shuts down.

Chapter 4. Software update and rollback

Software updates and rollbacks

You can update the Nozomi Networks software to a newer release, or roll it back to a previous release on physical or virtual sensors.

Before you do an update, or a rollback, Nozomi Networks recommends that you do a full backup.

Updates

You can use an update file to easily update Guardian sensors, *Central Management Console (CMC)*s, and Remote Collectors, and works for all physical and virtual deployments.

> **Note:**
> You need to use different update commands and procedures for container installations. For more details, see the **Container Installation** section in the **Installation Guide**.

You cannot update to a version that is more than one major version ahead of your current version. For example, you cannot update from version 23.0.0 to 25.0.0. Before you update a sensor, refer to the **Update** remarks topic in the **Release Notes**, which recommend update paths.

> **Important:**
> Manually scheduled updates apply regardless of whether the version is locked, or the update policy is disabled.

Updates will not occur if:

- In the *CMC*, the sensor is locked
- In the *CMC*, the sensor **Update Policy** is set to **Do not update sensors**
- The attempt to update a sensor returns this message: **Execution of the software update is taking longer than expected. Please wait for the process to finish or verify the status of the process by accessing the sensor via SSH. If this error persists contact Nozomi Networks Support for assistance.**

> **Note:**
> In certain cases, such as simultaneous human interventions, multiple concurrent `install_update` commands might have been issued. A new process has been implemented to prevent multiple instances of the `install_update` command from being executed simultaneously. If this new process is actively trying to prevent multiple, simultaneous updates while no update is actually in progress, it means the sensor's ability to update has been impacted. In this case, a rebooting of the sensor will disengage this process and will return the sensor's ability to update to a fully functional state.

Rollbacks

When you rollback to a release that was previously installed, all data is migrated back to the previous format.

Do a software update from the web UI

You can do a software update from the web UI.

Before you begin

You have downloaded the applicable update bundle that you want to use for the update.

Procedure

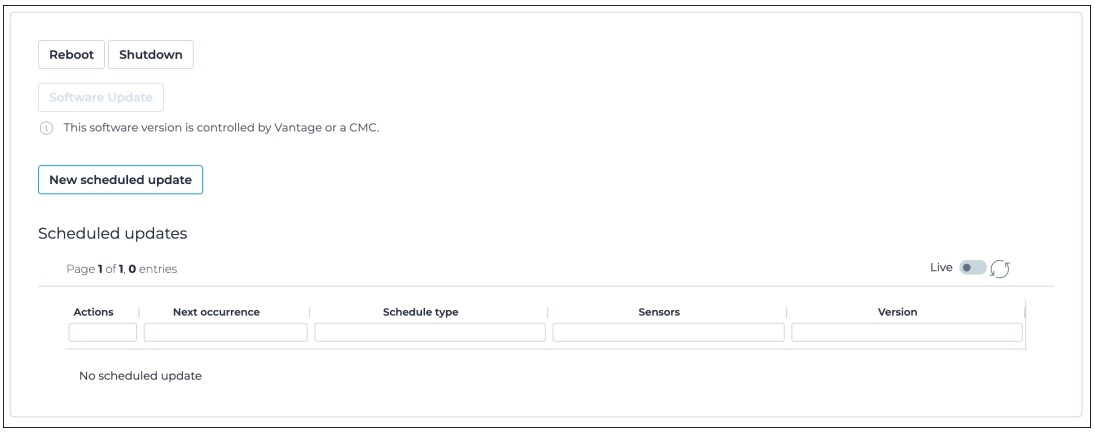
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **Operations**.

   Result: The **Operations** page opens.

3. In the top left, select **Software Update**.



   Result: A dialog opens.

4. Select the update bundle to use.

> **Note:**
> You should refer to **Release notes** of the new version to follow the correct update path.

   Result: The update bundle uploads.

5. Select **Proceed**.

Results

The update process begins. The update may take several minutes to complete.

Schedule a software update from the web UI

You can schedule a software update from the web UI.

Before you begin

You have downloaded the applicable update bundle that you want to use for the update.

Procedure

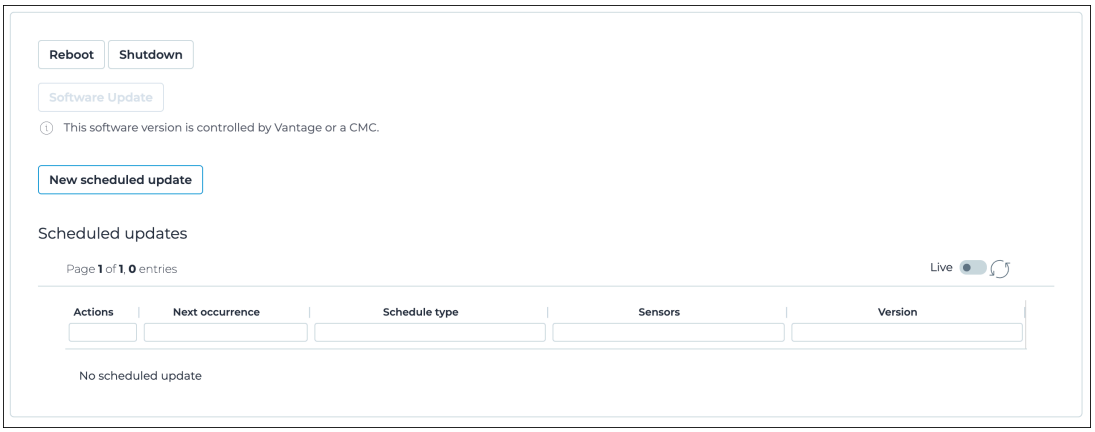
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **Operations**.

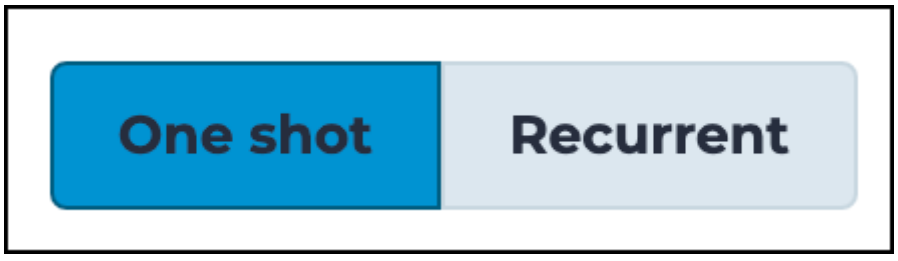
   Result: The **Operations** page opens.

3. In the top left, select **New scheduled update**.



   Result: A dialog opens.

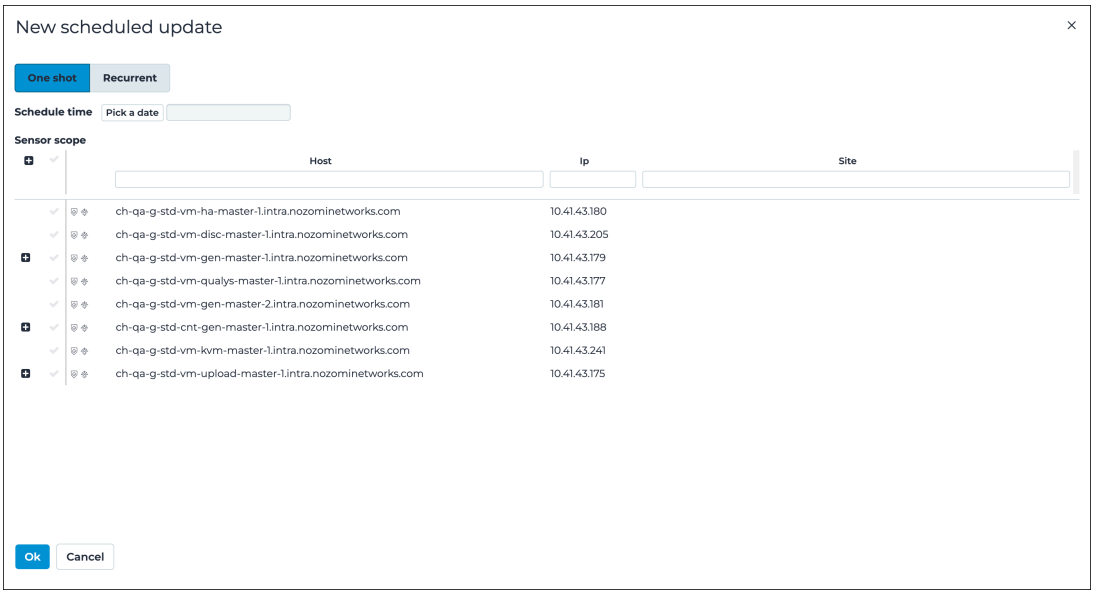
4. Choose an option:



   Choose from:

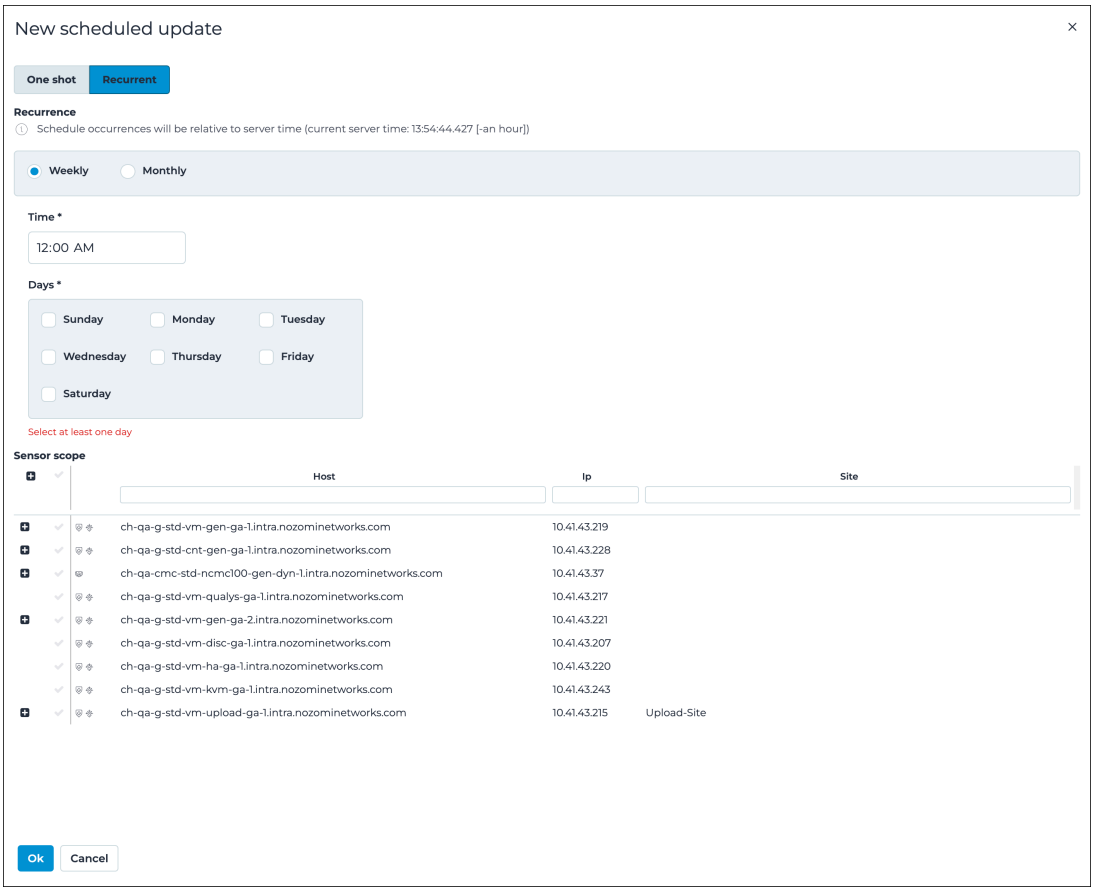
   - For a one-time update, select **One shot** and go to step 5 (on page 39).
   - For recurring updates, select **Recurrent** and go to step 9 (on page 40).

5. In the top left section, select **Pick a date**.



6. Select a date and time for the update.
7. From the list, select one, or more, sensors to update.
8. Select **Ok**.

9. Select a frequency:



Choose from:

- **Weekly**
- **Monthly**

10. In the **Time** field, set a time.
11. If you chose **Weekly**, in the **Days** field, select one, or more, day(s).
12. If you chose **Monthly**, in the **Days** field, select one, or more, date(s).
13. From the list, select one, or more, sensors to update.
14. Select **Ok**.

Results

The update has been scheduled.

Do a software update from a shell console

You can do a software update from a shell console.

Before you begin

You have downloaded the applicable update bundle that you want to use for the update.

Procedure

1. Open a shell console.
2. In the shell console, type `cd` and navigate to the directory where the `.bundle` file is located.
3. To copy the .bundle file to the sensor, enter the command:

   ```
   scp VERSION-update.bundle admin@<sensor_ip>:/data/tmp
   ```

   Note:
   You should refer to **Release notes** of the new version to follow the correct update path.

   Result: The update bundle uploads.
4. Enter the command:

   ```
   ssh admin@<sensor_ip>
   ```
5. To go to privileged mode, enter this command:

   ```
   enable-me
   ```

   Result: You can now perform system changes.
6. To start the installation of the new software, enter the command:

   ```
   install_update /data/tmp/VERSION-update.bundle
   ```

   Important:
   Make sure that you use the absolute path of the `VERSION-update.bundle`
   In the example above, the absolute path is `/data/tmp/VERSION-update.bundle`

Results

The update process begins. The update may take several minutes to complete.

Do a software rollback from a shell console

You can do a software rollback from a shell console. This can only be done once because only the previously installed version of the software is available for rollback.

Procedure

1. Open a shell console.
2. To go to privileged mode, enter this command:

   ```
   enable-me
   ```

   Result: You can now perform system changes.
3. To start the software rollback, enter the command:

   ```
   rollback
   ```

   Result: A dialog shows.
4. Select **y**.

   Result: The system starts to reboot.
5. Wait for the system to reboot.

Results

All configuration and historical data is automatically converted to the previous version, and no manual intervention is required.

Chapter 5. Reset

Do a data factory reset

You can erase the N2OS data partition to do a data factory reset to. The internet protocol (IP) configuration is kept, and the procedure is safe to execute remotely.

About this task

Important:
This procedure will cause the system to lose all its data. It will also reset enabled *SSH* public keys. Before you do this procedure, make sure that you have an admin password.

Procedure

1. Open a shell console.
2. Enter the command:

   ```
   n2os-datafactoryreset -y
   ```

   Result: The services are restarted with a fresh data partition.
3. If necessary, do the web console configuration in the **Installation Guide**.

Do a data factory reset with sanitization

You can use the U.S. DoD 5220-22M 7- pass scheme to completely erase the N2OS data partition and sanitize the disk space.

About this task

This process erases the N2OS data partition in accordance with the guidelines suggested in the NIST Special Publication 800-88 rev 1. Configurations such as network and console password settings are retained.

Important:
This procedure will cause the system to lose all its data. It will also reset enabled *SSH* public keys. Before you do this procedure, make sure that you have an admin password.

Procedure

1. Open a shell console.
2. Enter the command:

```
n2os-datasanitize -y
```

Result: The services are restarted with a fresh data partition.

3. Refer to the **Installation Guide** and do the web console configuration again.

Do a full factory reset with sanitization

You can use the U.S. DoD 5220-22M 7-pass scheme to erase data from a sensor, and clear disk space.

About this task

This process erases **ALL** data inside the sensor in accordance with the guidelines suggested in the NIST Special Publication 800-88 rev 1. All data and configurations (e.g., network and console password settings) are permanently deleted. The installed N2OS version remains the same.

Important:
This procedure will cause the system to lose all its data and configurations. The networking configuration will be reset to factory settings.

Procedure

1. Open a shell console.
2. Enter the command:

   ```
   n2os-fullfactoryreset -iknowwhatimdoing
   ```

   Result: The system reboots with a factory setup.
3. Refer to the **Installation Guide** and do the basic configuration again.

Chapter 6. Miscellaneous

Host-based intrusion-detection system

The internal Host-based intrusion-detection system (HIDS) sensors detect changes to the basic firmware image and note the change.

When a change is detected in the sensor's basic firmware image, a new event is logged in the system's audit log. It is also replicated in Vantage or the *CMC*.

You can change the default *host-based intrusion-detection system (HIDS)* settings to suit your security requirements.

Note:
This feature is not available in the container version due to the different security approach.

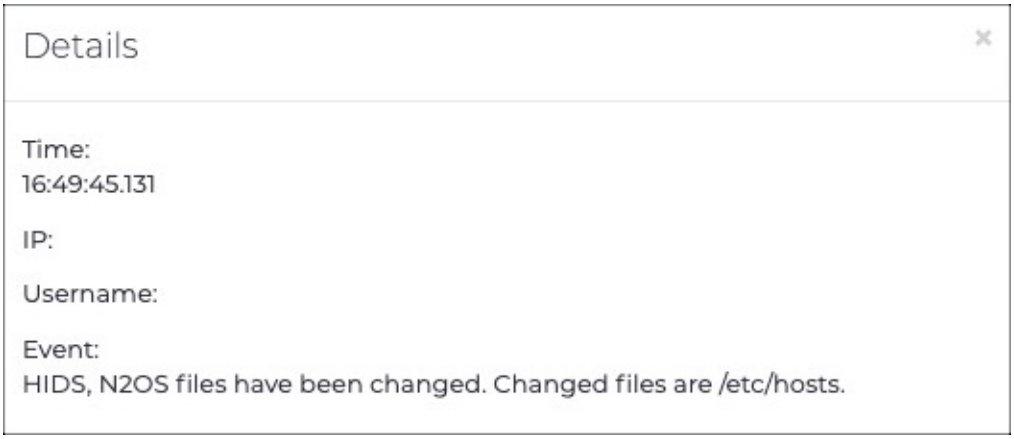


Figure 5. Host-based intrusion-detection system

Table 2. Host-based intrusion-detection system

Parameter	Default value	Description
hids execution interval	18 hours	HIDS check execution interval
hids ignore files	-	Coma separator list of files to be ignored by HIDS (ex: /etc/file1, /etc/file2)

Action on log disk full usage

There are several actions that you can take in order to preserve disk usage.

System log files are saved in a dedicated log partition and are automatically rotated in order to preserve disk usage. However, if a log partition becomes full, you might want to shut down the sensor.

To enable this feature, you can add the configuration key in the sensor shell console:

```
conf.user configure shutdown_when_log_disk_full true
```

Log emergency shutdown will also raise an alert in the sensor health log.

This feature is not available in the container version.

Generate a support archive file

Before you seek help from Customer Support, you should generate a support archive file.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

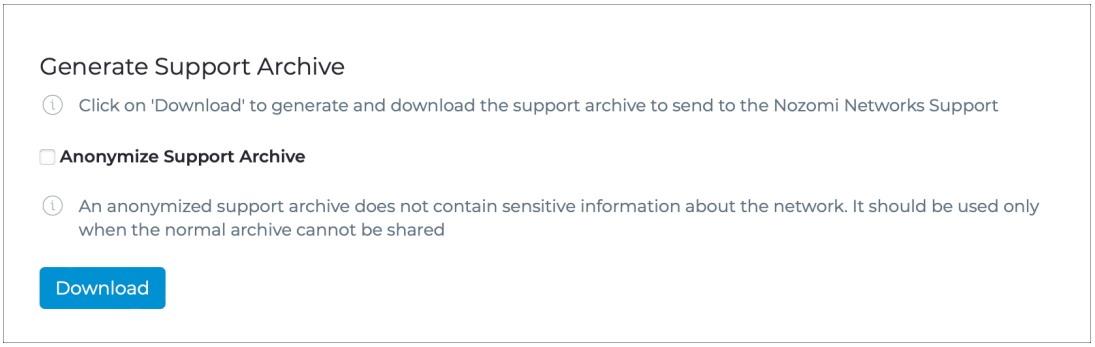
2. In the **System** section, select **Support**.

   Result: The **Support** page opens.

3. **Optional:** Select the **Anonymize Support Archive** checkbox to remove sensitive network information from the generated archive.

   > **Note:**
   > An anonymized support archive does not contain sensitive information about the network. It should be used only when the normal archive cannot be shared.

4. Select **Download**.

   Result: The support archive file starts to download in your browser.

5. Upload the file to the support case opened in the Nozomi Networks Support Portal.

Glossary

Amazon Machine Image

An AMI is a type of virtual appliance that is used to create a virtual machine for the Amazon Elastic Compute Cloud (EC2), and is the basic unit of deployment for services that use EC2 for delivery.

Amazon Web Services

AWS is a subsidiary of the Amazon company that provides on-demand cloud computing platforms governments, businesses, and individuals on a pay-as-you-go basis.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Assertion Consumer Service

An ACS is a version of the SAML standard that is used to exchange authentication and authorization identities between security domains.

Asset Intelligence™

Asset Intelligence is a continuously expanding database of modeling asset behavior used by N2OS to enrich asset information, and improve overall visibility, asset management, and security, independent of monitored network data.

Berkeley Packet Filter

The BPF is a technology that is used in some computer operating systems for programs that need to analyze network traffic. A BPF provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in the similar method to the sensor.

Central Processing Unit

The main, or central, processor that executes instructions in a computer program.

Certificate Authority

A certificate, or certification authority (CA) is an organization that stores, signs, and issues digital certificates. In cryptography, a digital certificate certifies the ownership of a public key by the named subject of the certificate.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

Command-line interface

A command-line processor uses a command-line interface (CLI) as text input commands. It lets you invoke executables and provide information for the actions that you want them to do. It also lets you set parameters for the environment.

Comma-separated Value

A CSV file is a text file that uses a comma to separate values.

Common Event Format

CEF is a text-based log file format that is used for event logging and information sharing between different security devices and software applications.

Common Platform Enumeration

CPE is a structured naming scheme for information technology (IT) systems, software, and packages. CPE is based on the generic syntax for Uniform Resource Identifiers (URI) and includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

Common Weakness Enumeration

CWE is a category system for software and hardware weaknesses and vulnerabilities. It is a community project with the aim to understand flaws in software and hardware and create automated tools that can be used to identify, fix, and prevent those flaws.

Configuration file

A CFG file is a configuration, or config, file. They are files that are used to configure the parameters and initial settings for a computer program.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

ESXi

VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS). Instead, it includes and integrates vital OS components, such as a kernel.

Extensible Markup Language

XML is a markup language and file format for the storage and transmission of data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

File Allocation Table

FAT is a file system architecture used in computers for managing disk space. It maintains a table to track the allocation of files on a disk, supporting efficient data storage, access, and management

File Transfer Protocol

FTP is a standard communication protocol that is used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture that uses separate control and data connections between the client and the server.

Fully qualified domain name

An FQDN is a complete and specific domain name that specifies the exact location in the hierarchy of the Domain Name System (DNS). It includes all higher-level domains, typically consisting of a host name and domain name, and ends in a top-level domain.

Gigabit per second

Gigabit per second (Gb/s) is a unit of data transfer rate equal to: 1,000 Megabits per second.

Gigabyte

The gigabyte is a multiple of the unit byte for digital information. One gigabyte is one billion bytes.

Graphical User Interface

A GUI is an interface that lets humans interact with electronic devices through graphical icons.

Graphics Interchange Format

GIF is a bitmap image format that is widely used on the internet.

High Availability

High Availability is a mode that permits the CMC to replicate its own data on another CMC.

Host-based intrusion-detection system

HIDS is an internal Nozomi Networks solution that uses sensors to detect changes to the basic firmware image, and record the change.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Identifier

A label that identifies the related item.

Identity Provider

An IdP is a system entity that creates, maintains, and manages identity information. It also provides authentication services to applications within a federation, or a distributed network.

Industrial Control Systems

An ICS is an electronic control system and related instrumentation that is used to control industrial processes.

Industrial Internet of Things

The IIoT is a name for interconnected devices, sensors, instruments, which are networked together with industrial applications. This connectivity allows for analysis and data collection, which can facilitate improvements in efficiency and productivity.

Internet Control Message Protocol

ICMP is a supporting protocol in the internet protocol suite. Network devices use it to send error messages and operational information to indicate success or failure when communicating with another IP address. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems.

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

Intrusion Detection System

An intrusion detection system (IDS), which can also be known as an intrusion prevention system (IPS) is a software application, or a device, that monitors a computer network, or system, for malicious activity or policy violations. Such intrusion activities, or violations, are typically reported either to a system administrator, or collected centrally by a security information and event management (SIEM) system.

JavaScript Object Notation

JSON is an open standard file format for data interchange. It uses human-readable text to store and transmit data objects, which consist of attribute–value pairs and arrays.

Joint Photographic Experts Group

JPEG, or JPG, is a method of lossy compression that is used for digital images. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality.

Lightweight Directory Access Protocol

LDAP is an open, vendor-neutral, industry standard application protocol that lets you access and maintain distributed directory information services over an internet protocol (IP) network.

Lightweight Directory Access Protocol Secure

LDAP over SSL or Secure LDAP is the secure version of LDAP.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Megabyte

The megabyte is a multiple of the unit byte for digital information. One megabyte is one million bytes.

National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Network Address Translation

NAT is a method of mapping an internet protocol (IP) address space into another one. This is done by modifying network address information in the IP header of packets while in transit across a traffic routing device.

Network Interface Controller

A network interface controller (NIC), sometimes known as a network interface card, is a computer hardware component that lets a computer connect to a computer network.

Network Time Protocol

The NTP is a networking protocol to synchronize clocks between computer systems over variable-latency, packet-switched data networks.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Nozomi Networks Query Language (N2QL)

N2QL is the language used in queries in Nozomi Networks software.

Open Virtual Appliance

An OVA file is an open virtualization format (OVF) directory that is saved as an archive using the .tar archiving format. It contains files for distribution of software that runs on a virtual machine. An OVA package contains a .ovf descriptor file, certificate files, an optional .mf file along with other related files.

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

Packet Capture

A pcap is an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Packet Capture Next Generation

A pcapNg is the latest version of a pcap file, an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Portable Document Format

PDF is a Adobe file format that is used to present documents. It is independent of operating systems (OS), application software, hardware.

Portable Network Graphics

PNG is a raster graphics file format that supports lossless data compression.PNG was developed as an improved, non-patented replacement for graphics interchange format (GIF).

Privacy-Enhanced Mail

PEM is a standard file format that is used to store and send cryptographic keys, certificates, and other data. It is based on a set of 1993 IETF standards.

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

Protected Extensible Authentication Protocol

PEAP is a protocol that encloses the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.

Random-access Memory

Computer memory that can be read and changed in any order. It is typically used to store machine code or working data.

Representational State Transfer

Representational State Transfer (REST) is an architectural style for designing networked applications. It uses stateless, client-server communication via standard HTTP methods (GET, POST, PUT, DELETE) to access and manipulate web resources represented in formats like JSON or XML.

Secure Copy Protocol

SCP is a protocol for the secure transfer of computer files between a local host and a remote host, or between two remote hosts. It is based on the secure shell (SSH) protocol.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

Secure Sockets Layer

A secure sockets layer ensures secure communication between a client computer and a server.

Security Assertion Markup Language

SAML is an open standard, XML-based markup language for security assertions. It allows for the exchange of authentication and authorization data different parties such as a service provider and an identity provider.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Server Message Block

Is a communication protocol which provides shared access to files and printers across nodes on a network of systems. It also provides an authenticated interprocess communication (IPC) mechanism.

Simple File Transfer Protocol

SFTP was proposed as an unsecured file transfer protocol with a level of complexity intermediate between TFTP and FTP. It was never widely accepted on the internet.

Simple Mail Transfer Protocol

SMTP is an internet standard communication protocol that is used for the transmission of email. Mail servers and other message transfer agents use SMTP to send and receive mail messages.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

Simple Text Oriented Messaging Protocol

STOMP is a simple text-based protocol, for working with message-oriented middleware (MOM). It provides an interoperable wire format that allows STOMP clients to talk with any message broker supporting the protocol.

Structured Threat Information Expression

STIX™ is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Supervisory control and data acquisition

SCADA is a control system architecture which has computers, networked data communications and graphical user interfaces for high-level supervision of processes and machines. It also covers sensors and other devices, such as programmable logic controllers (PLC), which interface with process plant or machinery.

Text-based User Interface

In computing, a text-based (or terminal) user interfaces (TUI) is a retronym that describes a type of user interface (UI). These were common as an early method of human–computer interaction, before the more modern graphical user interfaces (GUIs) were introduced. Similar to GUIs, they might use the entire screen area and accept mouse and other inputs.

Threat Intelligence™

Nozomi Networks **Threat Intelligence™** feature monitors ongoing OT and IoT threat and vulnerability intelligence to improve malware anomaly detection. This includes managing packet rules, Yara rules, STIX indicators, Sigma rules, and vulnerabilities. **Threat Intelligence™** allows new content to be added, edited, and deleted, and existing content to be enabled or disabled.

Transmission Control Protocol

One of the main protocols of the Internet protocol suite.

Transport Layer Security

TLS is a cryptographic protocol that provides communications security over a computer network. The protocol is widely used in applications such as: HTTPS, voice over IP, instant messaging, and email.

Uniform Resource Identifier

A URI is a unique string of characters used to identify a logical or physical resource on the internet or local network.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Uninterruptible Power Supply

A UPS is an electric power system that provides continuous power. When the main input power source fails, an automated backup system continues to supply power.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

Universal Plug and Play

UPnP is a network protocol that enables devices to automatically discover and communicate with each other using broadcast messages. While it facilitates easy device identification and connectivity, UPnP lacks robust authentication, making it vulnerable to unauthorized access in cybersecurity contexts.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

User Datagram Protocol

UDP is a lightweight, connectionless communication protocol used for fast, time-sensitive data transmission, such as video streaming, online gaming, and VoIP. UDP prioritizes speed and low latency over guaranteed delivery or error correction.

User Interface

An interface that lets humans interact with machines.

Variable

In the context of control systems, a variable can refer to process values that change over time. These can be temperature, speed, pressure etc.

Virtual DOM

A virtual DOM, or vdom, is a lightweight JavaScript representation of the Document Object Model (DOM). It is used in declarative web frameworks such as Elm, React, and Vue.js. It enables the updating of the virtual DOM is comparatively faster than updating the actual DOM.

Virtual Hard Disk

VHD is a file format that represents a virtual hard disk drive (HDD). They can contain what is found on a physical HDD, such as disk partitions and a file system, which in turn can contain files and folders. They are normally used as the hard disk of a virtual machine (VM). They are the native file format for Microsoft's hypervisor (virtual machine system), Hyper-V.

Virtual Local Area Network

A VLAN is a broadcast domain that is isolated and partitioned in a computer network at the data link layer (OSI layer 2).

Virtual Machine

A VM is the emulation or virtualization of a computer system. VMs are based on computer architectures and provide the functionality of a physical computer.

ZIP

An archive file format that supports lossless data compression. The format can use a number of different compression algorithms, but DEFLATE is the most common one. A ZIP file can contain one or more compressed files or directories.