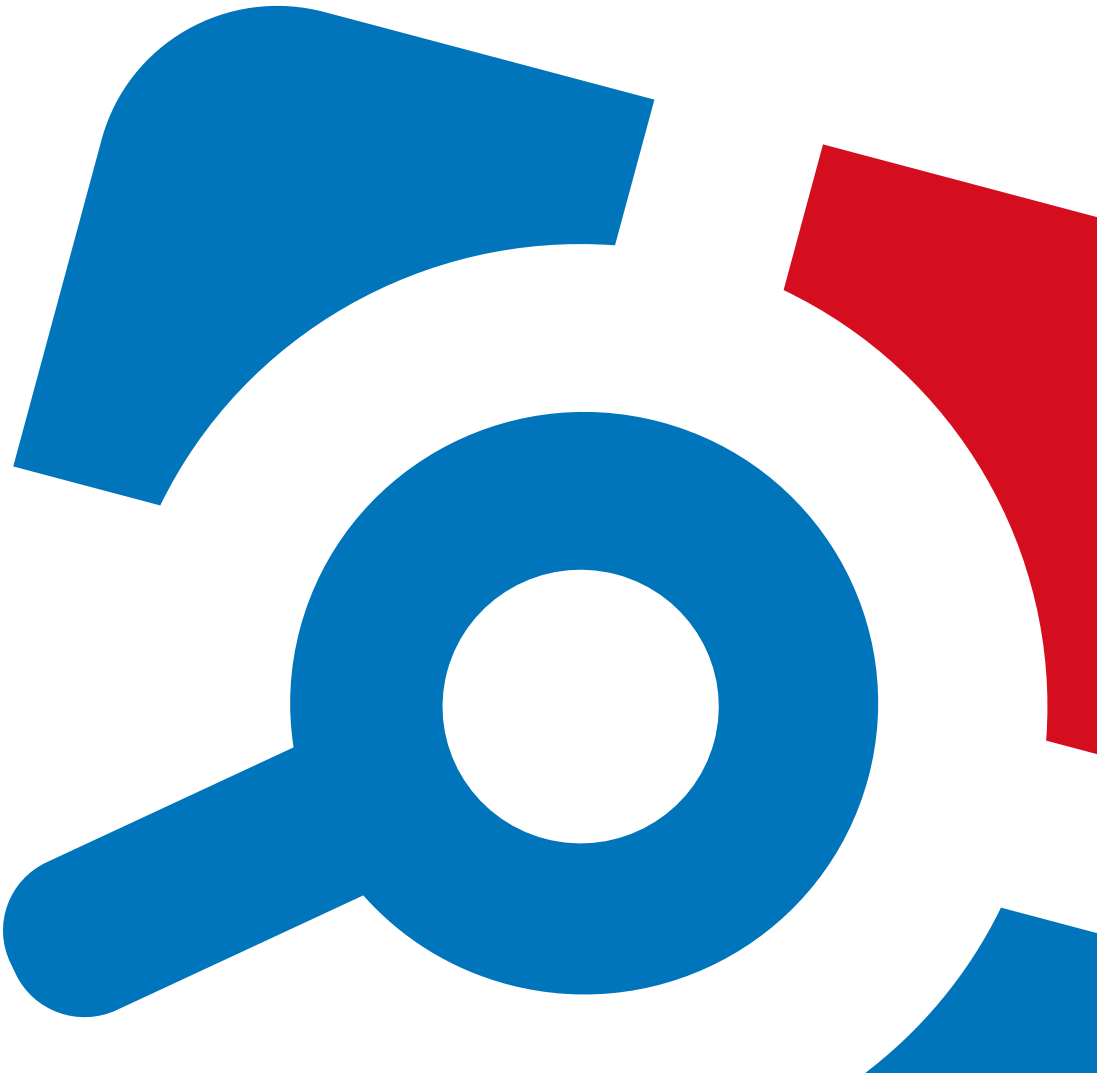
netwrix

Netwrix Auditor Add-on for Nutanix Files

Quick-Start Guide

Version: 9.8
5/28/2019



Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Microsoft, Active Directory, Exchange, Exchange Online, Office 365, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

Table of Contents

1. About This Document 4
2. Solution Overview 5
   2.1. Compatibility Notice 5
3. How It Works 6
   3.1. Add-on Delivery Package 7
4. Before You Start 9
   4.1. Prerequisites 9
   4.2. Accounts and Rights 10
   4.3. Considerations and Limitations 10
5. Deployment Procedure 11
   5.1. Step 1: Prepare Netwrix Auditor for Data Processing 11
   5.2. Step 2: Create a Nutanix Files User and Obtain Server Settings with NCLI 11
   5.3. Step 3: Download the Add-On 12
   5.4. Step 4: Configure Add-on Parameters 12
   5.5. Step 5: Configure Interaction and Data Flow 13
   5.6. Step 6: Install the Add-on 14
   5.7. Step 7: Register Add-on Server 14
6. Deployment Scenarios 15
7. Working with Collected Data 16
8. Maintenance and Troubleshooting 17
9. Appendix A. Monitored Events 18
10. Appendix B. Add-on Parameters 19
11. Appendix C. Add-on Internal Parameters 25

1. About This Document

This guide is intended for the first-time users of Netwrix Auditor add-on for Nutanix Files. It can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Install the add-on and configure its parameters
- Execute the add-on
- Review data collection results

NOTE: The add-on works only in combination with Netwrix Auditor so this guide covers a basic procedure for running the add-on and assumes that you have Netwrix Auditor installed and configured in your environment. For installation scenarios, data collection options, as well as detailed information on Integration API, refer to the Online Help Center and product documentation:

- Netwrix Auditor Online Help Center
- Netwrix Auditor Installation and Configuration Guide
- Netwrix Auditor Integration API Guide

2. Solution Overview

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Nutanix Files (former known as Nutanix Acropolis File Services (AFS)) is a file storage solution built upon the Nutanix Enterprise Cloud architecture. It provides facilities for VM storage and file storage, offering centralized management and enterprise storage features for unstructured data, including user profiles, departmental shares and home directories, as well as application logs, backups and archives. Nutanix Files is a fully integrated component of the Nutanix Enterprise Cloud Platform.

To control who does what in the IT infrastructure that includes Nutanix Files storage system, organizations need to monitor file activity on Nutanix Files. A typical case is when a user has renamed a directory at the top level, and other users are unable to locate their files anymore. Thus, IT specialists require a way to monitor, search and get notifications on certain file activity so that they can take corrective measures.

For that purpose, you can use a specially designed Netwrix Auditor add-on for Nutanix Files. It works in collaboration with Netwrix Auditor, supplying data about file operations on your Nutanix Files to Netwrix database. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost-effective, and helps you keep tabs on your IT infrastructure.

Major benefits:

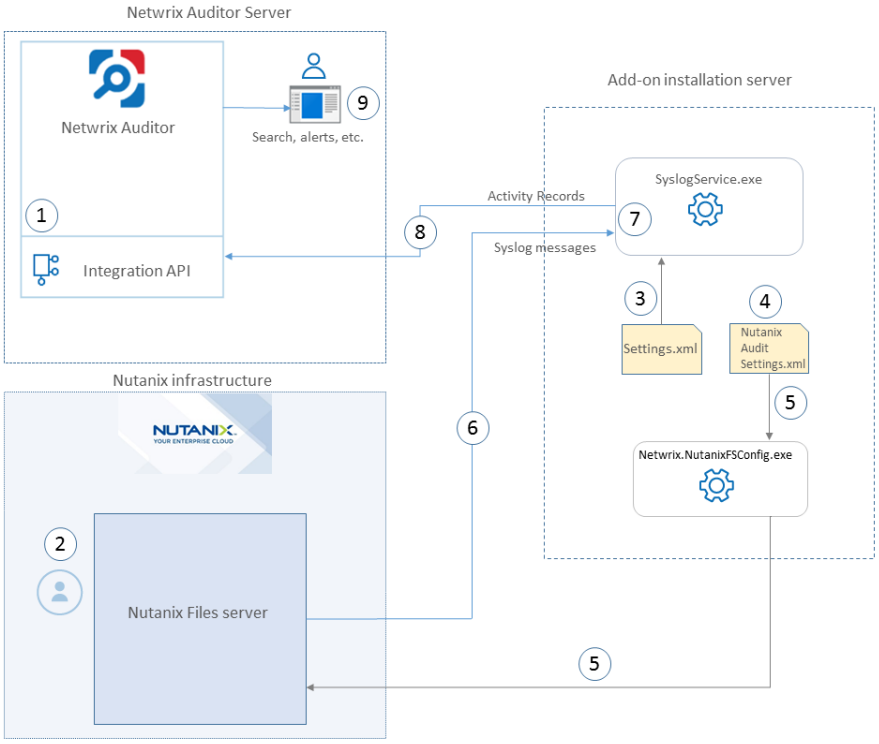
- Gain a high-level view of the data you store
- Detect unauthorized activity that might threaten your data

2.1. Compatibility Notice

Netwrix Auditor add-on for Nutanix Files is compatible with Nutanix Files 3.0, 3.2, 3.5 and with Netwrix Auditor 9.7 (build 9.7.3939) and later.

3. How It Works

The add-on is implemented as a Syslog service that collects activity data from Nutanix Files storage and sends it to Netwrix Auditor using Netwrix Auditor Integration API.



On a high level, the solution works as follows:

1. An IT administrator configures Netwrix Auditor Integration API settings to enable data collection and storage to Netwrix database for further reporting, search, etc.

   NOTE: It is recommended to create a dedicated monitoring plan in Netwrix Auditor and add a dedicated item of ***Integration*** type to it — then you will be able to filter data in reports and search results by monitoring plan/item name.

2. On Nutanix side, the IT administrator prepares a dedicated user account for accessing Nutanix Files server.

3. Then s/he opens **Settings.xml** configuration file and specifies the necessary parameters for add-on operation, including Nutanix Files server as the source of Syslog messages, Netwrix Auditor settings, etc. The add-on will operate as a Syslog listener for Nutanix Files server.

4. The add-on installation server is treated as a *partner server* for Nutanix Files. To configure interaction and data flow between Nutanix Files server and its partner server, the administrator uses **NutanixAuditSettings.xml** configuration file. There s/he needs to:

- Specify Nutanix Files server and partner server (i.e. add-on installation server) that will interact.
- Specify events and changes on the certain file share(s) the add-on will listen to.

NOTE: Default list of events supported out-of-the box is provided in the Appendix A. Monitored Events. You can edit the configuration to change the types of captured events.

5. The administrator runs the **Netwrix.NutanixFSConfig.exe** utility that registers the add-on on Nutanix Files server, communicating interaction parameters to that server (via REST API).
6. The add-on starts collecting and forwarding activity data: it listens to the specified TCP port and captures designated Syslog messages. Data communication is performed using TCP version of Syslog protocol.
7. The add-on processes these Syslog messages into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the **Who-What-When-Where-Action** information (that is, user account, time, action, and other details).
8. Using Netwrix Auditor Integration API, the add-on sends the activity records to Netwrix Auditor Server that writes them to the Audit Database and Long-Term Archive. Data is sent periodically, by default every 5 seconds.

   NOTE: For more information on the structure of the Activity Record and the capabilities of the Netwrix Auditor Integration API, refer to Netwrix Auditor Integration API Guide.
9. Users open Netwrix Auditor Client to work with collected data:
   - Search for file changes using certain criteria
   - Export data to PDF or CSV files
   - Save search results as reports
   - Subscribe to search results
   - Configure and receive alerts

3.1. Add-on Delivery Package

Netwrix Auditor add-on for Nutanix Files delivery package is a ZIP archive that includes the following files:

File name	Description
Install.cmd	Command file that installs and enables Netwrix Syslog service.
NutanixAuditSettings.xml	Configuration file used to set up interaction and data flow between Nutanix Files and Netwrix add-on.
Netwrix.NutanixFSConfig.exe	Registers the add-on installation server on the Nutanix Files server and communicates interaction parameters to that

File name	Description
	server. This file must be co-located with **NutanixAuditSettings.xml** that contains interaction parameters.
Netwrix.NutanixFSConfig.exe.config	Configuration file intended mainly for internal use, in particular, to enable extended logging (turned off by default).
Nutanix-v3.5.xml	Contains rules for processing Nutanix events. Intended mainly for internal use.
Settings.xml	Contains parameters for the add-on service operation.
SyslogService.exe	Netwrix Auditor add-on for Nutanix Files service – main add-on component, implemented as a Syslog service.
SyslogService.exe.config	Add-on configuration data.
Netwrix_Auditor_Add-on_for_ Nutanix_Files_Quick_Start_ Guide.pdf	This document.
Release_Notes.pdf	Release Notes file.

4. Before You Start

4.1. Prerequisites

Before you start working with Netwrix Auditor add-on for Nutanix Files, check the prerequisites listed in the following table:

Where	Prerequisite to check
The Netwrix Auditor Server side	1. Netwrix Integration API and Audit Database settings are configured in Netwrix Auditor Server settings. See Configure Integration API and Audit Database. 2. The **TCP 9699** port must be open on Windows firewall for inbound connections. 3. User account under which data will be written to the Audit Database requires the **Contributor** role in Netwrix Auditor. See Role-Based Access and Delegation. **NOTE:** Alternatively, you can grant it the **Global administrator** role, or add that account to the **Netwrix Auditor Administrators** group. See Netwrix Auditor Administration Guide for more information.
The machine where Netwrix Auditor add-on for Nutanix Files will be installed	1. The **TCP 9898** port must be open on Windows firewall for inbound connections. 2. Any of the following .NET Framework versions must be installed: • 4.6 • 4.5 • 4.0 • 3.5 SP1
The machine where **Netwrix.NutanixFSConfig.exe** will be launched	1. Any of the following Windows OS versions: • Windows Server 2012 R2 (or later) • Windows 8.1 (or later) 2. .NET Framework 4.5 or later
Nutanix Files (former Nutanix AFS server)	Version 3.0, 3.2, 3.5.

4.2. Accounts and Rights

It is recommended to create a dedicated account for running **install.cmd** and **SyslogService.exe** (Netwrix Auditor add-on for Nutanix Files service). The service will connect to Netwrix Auditor Server using this account, so at least the **Contributor** role in Netwrix Auditor is required for it. See Role-Based Access and Delegation for more information.

4.3. Considerations and Limitations

- Currently, auditing is only available for SMB file shares.

NOTE: Auditing for NFS file shares in not supported due to known limitations.

- Netwrix add-on must be deployed in the same subnet as Nutanix Files.
- In case Netwrix Auditor add-on for Nutanix Files service (SyslogService.exe) that runs remotely is unable to receive all generated events (that is, event queue is full), then Nutanix Files server performance for regular file operations may decrease.
- Currently, not every detail about permission and attribute changes may be provided by Nutanix Files, so they cannot be reported by Netwrix Auditor.
- Please be aware that monitoring of actions performed from partner server (the add-on installation server, i.e. the macine where *SyslogService.exe* will run) is not supported in the current version of Nutanix Files auditing API.

5. Deployment Procedure

5.1. Step 1: Prepare Netwrix Auditor for Data Processing

In Netwrix Auditor client, go to the **Integrations** section and verify Integration API settings:

a. Make sure the **Leverage Integration API** is switched to **ON**.

b. Check the TCP communication port number – default is **9699**.

NOTE: For more information, see Configure Integration API Settings.

By default, activity records are written to ***Netwrix_Auditor_API*** database which is not associated with a specific monitoring plan.

NOTE: Optionally, you can create a dedicated monitoring plan in Netwrix Auditor. In this case, data will be written to a database linked to this plan. Target it at Netwrix API data source and enable for monitoring. Add a dedicated item of ***Integration*** type to the plan for data to be filtered by item name. For more information, see Netwrix Auditor Administration Guide.

In such scenario, you will need to specify this monitoring plan in the *naplan* and *naplanitem* attributes of the *AcceptList* > *Address* configuration parameters. See Appendix B. Add-on Parameters for details.

5.2. Step 2: Create a Nutanix Files User and Obtain Server Settings with NCLI

To provide for interaction and data flow between Nutanix Files and Netwrix Auditor add-on for Nutanix Files, you will need to specify user credentials for accessing Nutanix Files server that will execute REST API calls. It is recommended to create a dedicated user account for that purpose.

Do the following:

1. Download and install the *ncli* (Nutanix command-line interface) on any server in your infrastructure, as described here.
2. Start the utility and establish a *ncli* session by the following command:

   ```
   ncli -s management_ip_addr -u 'username' -p 'user_password'
   ```

   here:

   - `management_ip_addr` - the IP address of any Nutanix Controller VM in the cluster
   - `username` - user name to access that VM; if not specified, *admin* (default name) will be used

- `user_password` - password to access that VM

3. Run the `fs list` command in *ncli* to get the list of Nutanix Files servers.
4. Locate the name of Nutanix Files server you want to audit; locate and save the following server parameters to a text file:
   - **Uuid** - Nutanix Files server ID
   - **Network type: Internal** > **IP Pool** - pool of IP addresses for communication with internal networks
   - **Network type: External** > **IP Pool** - pool of IP addresses for communication with external networks

   NOTE: You may have one IP address or IP range in these pools; in the latter case it is recommended to write down every separate address that belongs to the corresponding range.

   For example, if an **IP Pool** for **Network type: Internal** looks like *172.28.23.81 - 172.28.23.84*, you should write down the following addresses: *172.28.23.81, 172.28.23.82, 172.28.23.83. 172.28.23.84*.
5. Finally, create a new user and specify credentials that will be used to access this Nutanix Files server. For that, run the following command in *ncli* :

   ```
   fs add-user uuid=<fs_uuid> user=<username> password=<password>
   ```

   here:
   - `<fs_uuid>` - Nutanix Files server ID (Uuid)
   - `<username>` - user name
   - `<password>` - password

5.3. Step 3: Download the Add-On

1. Download the distribution package **Netwrix_Auditor_Add-on_for_Nutanix.zip**.
2. Unpack it to a folder on the computer where you plan to deploy the add-on.

5.4. Step 4: Configure Add-on Parameters

1. Open the add-on folder and edit the **Settings.xml** file to configure the add-on parameters:
   a. Modify the *<Address>* parameter.

   It defines the IP addresses of possible syslog events sources. The add-on will only collect and process events from these sources. As it must process the events from the Nutanix Files server, enter all IP addresses from the IP pools that you saved at Step 2: Create a Nutanix Files User and Obtain Server Settings with NCLI .

NOTE: If you have configured a dedicated monitoring plan targeted at Netwrix API data sourceSee "Deployment Procedure"

b. Specify Nutanix Files server time zone. For example:

```
<Address tstimezone="Pacific Standard Time">1.2.3.4</Address>
```

NOTE: To display the list of time zones available for the machine, you can run **install.cmd** on that machine using the `showtimezone` parameter:

```
install /showtimezone
```

For default list of time zones, refer to Microsoft documentation.

2. Save the **Settings.xml** file.

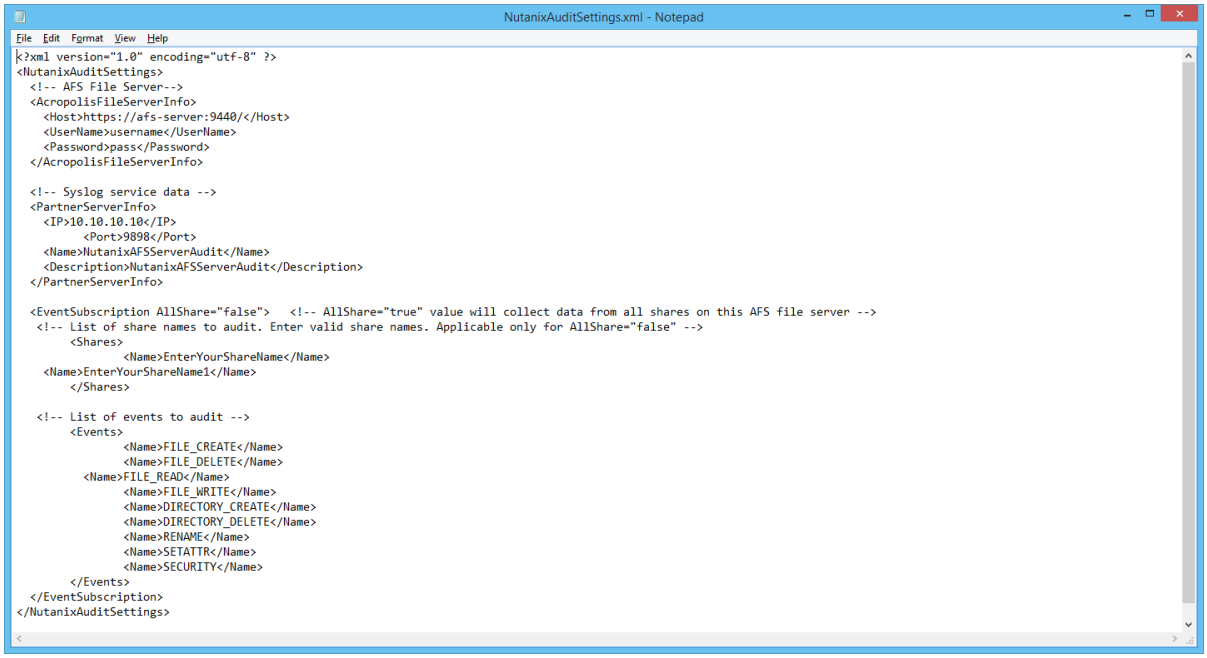
If you later need to modify parameters in the **Settings.xml** file, remember to save the changes and then restart Netwrix Auditor add-on for Nutanix Files service (*SyslogService.exe*) for them to take effect.

NOTE: For the full list of parameters, see the Appendix B. Add-on Parameters in this guide.

5.5. Step 5: Configure Interaction and Data Flow

Edit **NutanixAuditSettings.xml** file to configure interaction and data flow between Nutanix Files and the add-on. Do the following:

1. Specify Nutanix Files server that will be audited (you saved its UUID at Step 2: Create a Nutanix Files User and Obtain Server Settings with NCLI).
   For that, in the *AcropolisFileServerInfo* section of configuration file specify the following parameter values:
   - **Host** — enter the URL of Nutanix Files server
   - **UserName** and **Password** — enter the credentials of Nutanix Files user you supplied at Step 2: Create a Nutanix Files User and Obtain Server Settings with NCLI .
2. Specify the server that will receive Syslog messages from Nutanix Files server, process them and forward to Netwrix Auditor server. This will be the add-on installation server (the machine where *SyslogService.exe* runs). It is recognized by Nutanix Files as a *partner server*. So, in the *PartnerServerInfo* section specify the parameters of the add-on installation server:
   - **IP** and **Port** — enter IP address and communication port of the add-on installation server.
   - **Name** — enter name of the add-on installation server. Description is optional.
3. Specify the file shares whose changes you want to track using syslog messages. For that, go to the *EventSubscription* section and specify the following:
   - To get messages on changes to all shares, set *AllShare="true"*.
   - To get messages on changes to specific share, enter the share name in the **Name** parameter under *Shares*.
4. Save the configuration file.



If you later decide to modify parameters in the *Events* section, consider that you will have to unregister the add-on installation server and then register it again, as described below.

5.6. Step 6: Install the Add-on

Run **Install.cmd** file from the add-on folder.

This command installs the add-on and configures a Windows firewall inbound connection rule to allow connections via default port **9898**.

NOTE: If you plan to change this port, then remember to do it in the following files:

- **Install.cmd** (otherwise, you will have to open the necessary port on Windows firewall manually)
- **Settings.xml** — modify *<ListenTcpPort>*
- **NutanixAuditSettings.xml** — modify *<PartnerServerInfo><Port>*

5.7. Step 7: Register Add-on Server

Now you need to register add-on installation server as a partner server of Nutanix Files server and communicate interaction parameters to that server. Run the following command:

```
Netwrix.NutanixFSConfig.exe –register
```

The add-on will start collecting activity data and forwarding it to Netwrix Auditor.

NOTE: Events originating from partner server (that is, add-on installation server) will not be registered.

To unregister, run the following command:

```
Netwrix.NutanixFSConfig.exe –unregister
```

6. Deployment Scenarios

Netwrix Auditor add-on for Nutanix Files can run on any computer in your environment. For example, you can run the add-on on the computer where Netwrix Auditor is installed, or on a remote server. Depending on the deployment scenario you choose, you will need to define a different set of parameters.

Netwrix suggests the following scenarios:

Scenario	Example: Parameters updated in default Settings.xml
The add-on runs on the Netwrix Auditor Server with the current user credentials.	`<Address>172.28.4.15</Address>` `<Address>172.28.3.18</Address>`

The add-on runs on the Netwrix Auditor Server with the explicitly specified user credentials.	`<NetwrixAuditorUserName>SecurityOfficer </NetwrixAuditorUserName>`
	`<NetwrixAuditorPassword>NetwrixUser </NetwrixAuditorPassword>`
	`<Address>172.28.4.15</Address>`

The add-on runs on a remote computer. Data is written to a remote Netwrix Auditor repository with the current user credentials.	`<NetwrixAuditorEndpoint> https://172.28.6.19:9699/netwrix/api/v1/activity_ records</NetwrixAuditorEndpoint>` `<Address>172.28.4.15</Address>`

The add-on runs on a remote computer. Data is written to a remote Netwrix Auditor repository with the explicitly specified user credentials.	`<NetwrixAuditorEndpoint> https://172.28.6.19:9699/netwrix/api/v1/activity_ records</NetwrixAuditorEndpoint>`
	`<NetwrixAuditorUserName>NetwrixUser </NetwrixAuditorUserName>`
	`<NetwrixAuditorPassword>NetwrixIsCool </NetwrixAuditorPassword>`
	`<Address>172.28.4.15</Address>`

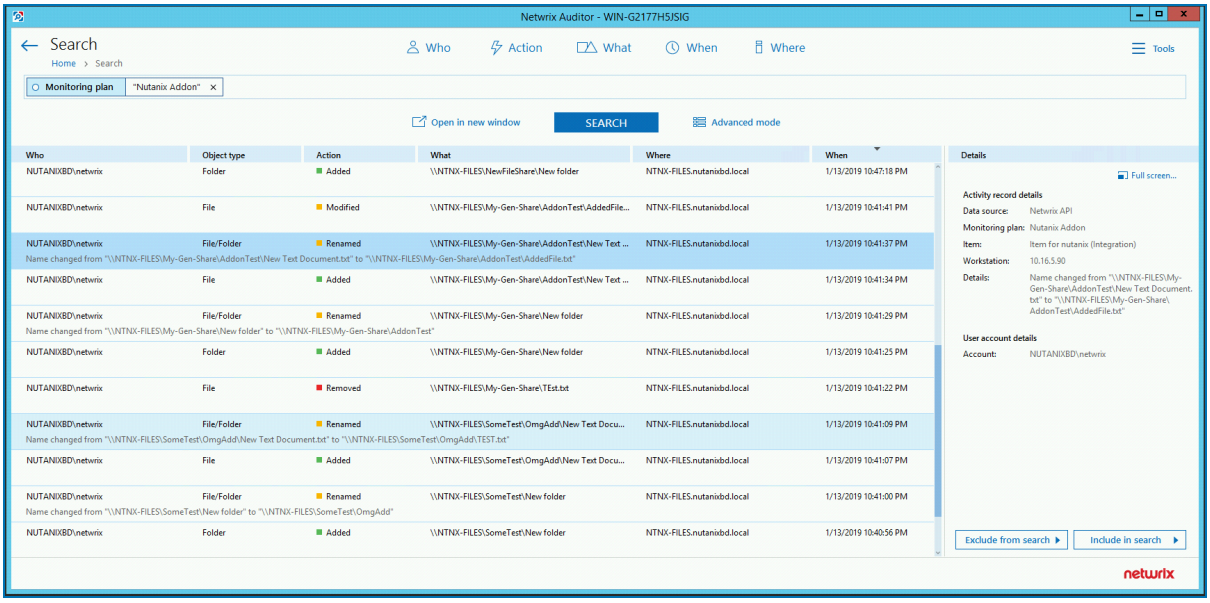
For security reasons, Netwrix recommends running the script with current user credentials (skipping user credentials). Create a special user account with permissions to access Netwrix Auditor Server.

7. Working with Collected Data

To leverage data collected with the add-on, you can do the following in Netwrix Auditor:

- Search for required data. For that, start Netwrix Auditor client and navigate to **Search**. After specifying the criteria you need, click **Search**. You will get a list of activity records with detailed information on who did what in the reported time period.

NOTE: You might want to apply a filter to narrow down your search results to the **Netwrix API** data source only.



- Also, you can click **Tools** in the upper-right corner and select the command you need. For example:
  - If you want to periodically receive the report on the results of search with the specified criteria, click **Subscribe**. Then specify how you want the report to be delivered – as an email or as a file stored to the file share.
  - To create an alert on the specific occurrences, click **Create alert**.
  - To export filtered data to PDF or CSV, click **Export data**.
- You can also configure and receive alerts on the events you are interested in.

See for more information, see Netwrix Auditor User Guide and Online Help Center.

8. Maintenance and Troubleshooting

Netwrix Auditor add-on for Nutanix Files operations are logged into the **SyslogService.txt** file. This file is located in the same folder as **SyslogService.exe.**

To change the add-on logging level, use the **LogLevel** parameter in the **Settings.xml** file.

- It is recommended that before the first run you set this parameter to `debug`. This will facilitate operations tracking and possible problem solving.
- After that it is strongly recommended to re-set this parameter to `error` (default value) to prevent the uncontrolled log growth.

If you cannot see collected data in Netwrix Auditor, check the following:

1. Service account has sufficient rights to access Netwrix Auditor.
2. In Netwrix Auditor settings, go to the **Integrations** section and make sure the **Leverage Integration API** is switched to **ON**. Check the communication port number – default is **9699**.
3. If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
4. Verify the parameters you provided in **Settings.xml** and **NutanixAuditSettings.xml**.

Also, remember that events from partner server (add-on installation server) are not collected.

9. Appendix A. Monitored Events

Netwrix Auditor add-on for Nutanix Files supports monitoring for the following syslog events:

Event	Description
FILE_CREATE	A new file was created.
FILE_DELETE	A file was deleted.
FILE_READ	Read operation was performed for a file.
FILE_WRITE	Write operation was performed for a file.
DIRECTORY_CREATE	A new directory was created.
DIRECTORY_DELETE	A directory was deleted.
RENAME	File or folder name was modified.
SETATR	File or folder attribute was modified.
SECURITY	File or folder permission set was modified (successful changes only).

10. Appendix B. Add-on Parameters

To configure the add-on parameters, you need to edit the **Settings.xml** file in the add-on folder. You must define connection details: Netwrix Auditor Server host, user credentials, etc.

Most parameters are optional, the service uses the default values unless parameters are explicitly defined (*<parameter>***value***</parameter>*). You can skip or define parameters depending on your execution scenario and security policies.

Parameters in **Settings.xml** can be grouped as follows:

- General parameters that affect add- on execution. They are listed in the table below.
- Settings for a certain event source (within the *Source* section) that can override general settings.
- Internal parameters that should not be modified in most cases. They are listed in Appendix C.

Parameter	Default value	Description
General parameters		
ListenTCPPort	9898	Specify TCP port for listening incoming syslog events.
NetwrixAuditorEndpoint	https://localhost:9699/netwrix/api/v1/activity_records	Netwrix Auditor Server IP address and port number followed by endpoint for posting Activity Records. Assumes that the add-on runs on the computer hosting Netwrix Auditor Server and uses default port 9699. If you want to run the add-on on another machine, provide a name of the computer where Netwrix Auditor Server resides (e.g., 172.28.6.15, EnterpriseNAServer, WKS.enterprise.local). To specify a non-default port, provide a server name followed by the port number (e.g., WKS.enterprise.local:9999).

Parameter	Default value	Description
		NOTE: Do not modify the endpoint part (/netwrix/api . . . .)
NetwrixAuditor CertificateThumbprint	NOCHECK	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `Empty`—Check Netwrix Auditor certificate via Windows Certificate Store. • `AB:BB:CC.`—Check Netwrix Auditor Server certificate thumbprint identifier. • `NOCHECK`—Do not check Netwrix Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use another account to connect to Netwrix Auditor Server, specify the account name in the DOMAIN\username format. **NOTE:** The account must be assigned the **Contributor** role in Netwrix Auditor.
NetwrixAuditorUserPassword	Current user credentials	Unless specified, the service runs with the current user credentials. Provide a different password if necessary.
NetwrixAuditorDateTimeFormat	yyyy-MM-ddTHH:mm:ssZ	Netwrix Auditor time format. By default, set to zero offset.
NetwrixAuditorPlan	—	Unless specified, data is written to **Netwrix_ Auditor_ API** database and is not associated with a

Parameter	Default value	Description
		specific monitoring plan. Specify a name of associated monitoring plan in Netwrix Auditor. In this case, data will be written to a database linked to this plan. **NOTE:** If you select a plan name in the add-on, make sure a dedicated plan is created in Netwrix Auditor, the **Netwrix API** data source is added to the plan and enabled for monitoring. Otherwise, the add-on will not be able to write data to the Audit Database.
NetwrixAuditorPlanItem	—	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name. Specify an item name. **NOTE:** Make sure to create a dedicated item in Netwrix Auditor in advance.
EventStorePath	—	Select where to store temporary files of syslog messages before the add-on sends them to Netwrix Auditor Server. **NOTE:** Netwrix recommends not to store these files out of the service directory.
LogLevel	error	Specify logging level: • none • info • warning

Parameter	Default value	Description
		• error (used by default) • debug
WriteCriticalIssues ToEventLog	0	Instructs the add- on to write important events (like service start or critical issue) not only to its own log but also to Netwrix event log. • 1=yes • 0=no (default)
Parameters within SourceList		
You can specify parsing rules for each specific event source and define parameters to override general settings, such as time zone, default plan name, etc.		
NetwrixAuditorPlan	—	When specified, overrides the general settings.
NetwrixAuditorPlanItem	—	When specified, overrides the general settings.
DefaultTsTimezone	—	Define the time zone of syslog events. By default, set to zero offset (UTC).
AppNameRegExp	—	Define a custom regular expression pattern to retrieve the application name from your syslog messages. Unless specified, RFC 3164/5424 format is used. If you provide a pattern for application name, this name will be used to determine what rule file will be used to parse syslog messages. The pattern you provide here must match the application name in your custom rule file.
AppNameGroupID	—	Define application name value by Group ID only if messages are not formatted in accordance with RFC 3164/5424. Otherwise, leave the default value.

Parameter	Default value	Description
RuleFileList PathFile	nutanix-v1.xml	Specify paths to XML file(s) with regular expression parsing rules. You can create a custom file or use rules provided out of the box. Currently, the **nutanix-v1.xml** rule file is shipped with this add-on. You can specify several rule files. The service will check if the AppName parameter in the first rule file matches the AppNameRegExp and AppNameGroupID regular expression in this file. If not, the service will proceed to the next rule file.
AcceptList Address	—	Specify a list of IP addresses of syslog events sources. The service will collect and process events from these sources only. **NOTE:** Events collected from any other source will be ignored. The Address parameter may be followed by optional attributes that override parameters specified above: • naplan— A name of associated monitoring plan • naplanitem— A name of associated item • tstimezone— Timezone for Nutanix Files For example: `<Address naplan="NFSmonitoring" naplanitem="NFS" tstimezone="GMT StandardTime">172.28.3.15 </Address>`

NOTE: Remember to save **Settings.xml** after editing is complete.

After you modify parameters in the **Settings.xml** file, remember to save the changes and then restart Netwrix Auditor add-on for Nutanix Files service (SyslogService.exe) for them to take effect.

11. Appendix C. Add-on Internal Parameters

Internal parameters listed in the table below are intended for performance tuning. In most cases the default values should be used.

Parameter	Default value	Description
EventsFromMemoryFirst	1	Instructs the add-on to save events to temporary storage only if there is no free space in queues: • 1=yes • 0=no
ConcurrentSend	-1	Specifies number of threads for concurrent forwarding of events to Netwrix Auditor. Default value is -1 (switch off concurrent forwarding).
ListenTcpAddress	0.0.0.0	Defines destination IP address. In case of multiple network cards, you can specify certain IP address here to listen to its messages only.
SenderSleepTime	30	Specifies retry interval in seconds to send messages to Netwrix Auditor (30 - 3600 seconds).
TaskLimit	8	Specifies number of threads and queues for concurrent handling of events.
QueueSizeLimit	1000	Specifies maximum number of events to keep in queue before saving to temporary storage or sending to Netwrix API.
QueueTimeLimit	5	Specifies the length of timeout before events from queue (not full) are saved to temporary storage or sent to Netwrix API: From 5 to 300 - timeout in seconds. -1—disable timeout.