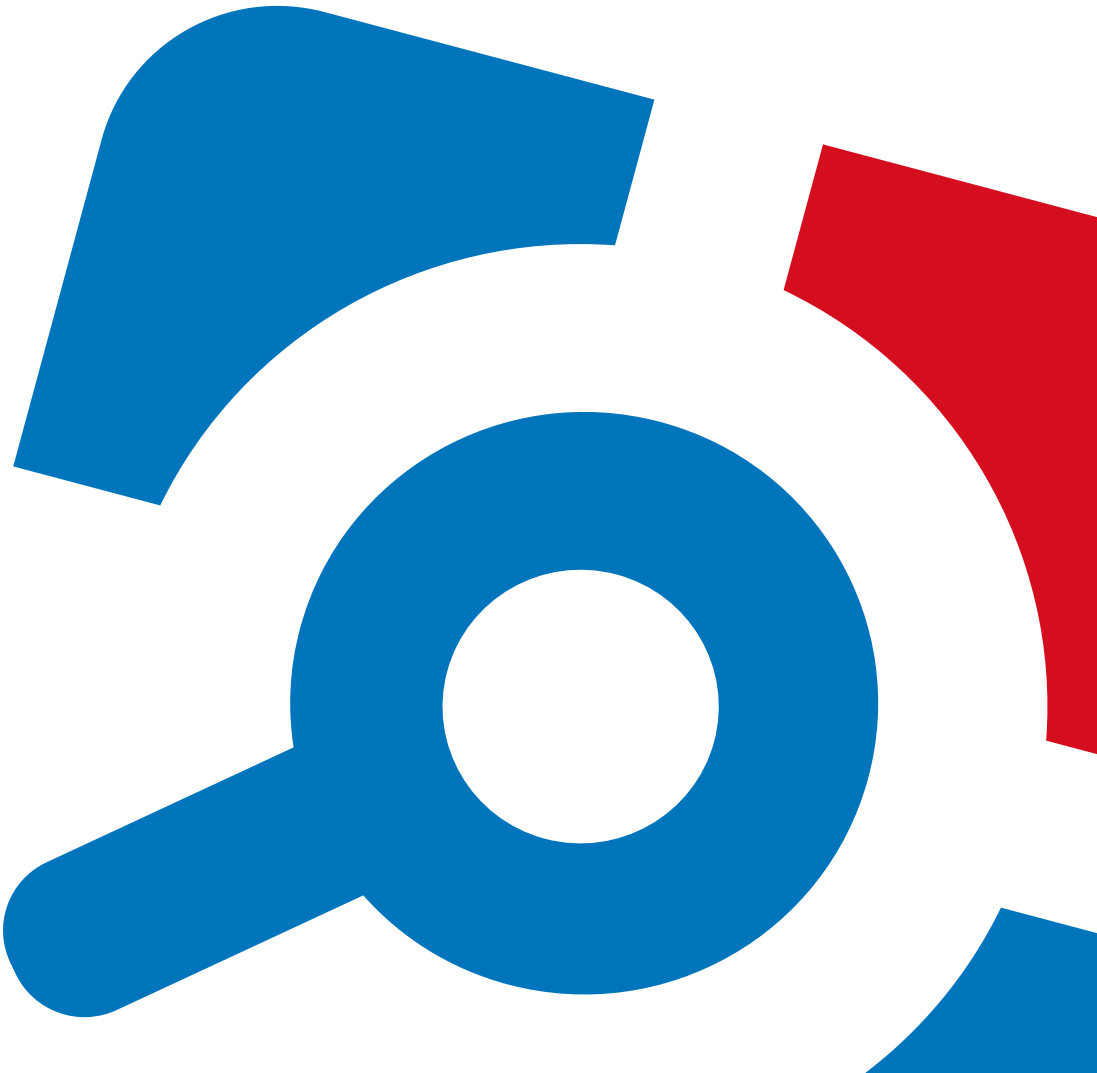
netwrix

Netwrix Auditor Add-on for Generic Linux Syslog

Quick-Start Guide

Version: 9.6
5/8/2018



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. Introduction

This guide is intended for the first-time users of Netwrix Auditor Integration API add-ons. 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:

- Define add-on parameters
- Execute the add-on
- Review 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:

- Netwrix Auditor Installation and Configuration Guide
- Netwrix Auditor Administration Guide
- Netwrix Auditor Integration API Overview

1.1. Netwrix Auditor 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.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

Major benefits:

- Detect insider threats—on premises and in the cloud
- Pass compliance audits with less effort and expense
- Increase productivity of IT security and operations teams

2. Netwrix Auditor Add-on for Generic Linux Syslog Overview

The add-on works in collaboration with Netwrix Auditor, supplying data about activity on your Linux-based devices. Aggregating data into a single audit trail simplifies analysis, makes activity monitoring more cost effective, and helps you keep tabs on your IT infrastructure.

Implemented as a service, this add-on facilitates the data transition from Linux-based systems to Netwrix Auditor. All you have to do is provide connection details and specify parsing rules. The parsing rules provided out of the box are generic and Netwrix encourages you to extend the list of parsing rules and create rules specific to your Linux devices.

On a high level, the add-on works as follows:

1. The add-on listens to the specified UDP ports and captures designated Syslog messages.

   Out of the box, messages from Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu 16 are supported. For other distributions, deployment of rsyslog package may be required. You can edit the add-on configuration to extend the captured message list.

2. The add-on processes these events into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the user account, action, time, and other details.

3. Using the Netwrix Auditor Integration API, the add-on sends the activity records to the Netwrix Auditor Server, which writes them to the Long-Term Archive and the Audit Database.

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 Overview.

3. Collect Events with Service

3.1. Prerequisites

Before running Netwrix Auditor Add-on for Generic Linux Syslog, ensure that all the necessary components and policies are configured as follows:

On...	Ensure that...
The Netwrix Auditor Server side	• The Audit Database settings are configured in Netwrix Auditor Server. • The TCP 9699 port (default Netwrix Auditor Integration API port) is open for inbound connections. • The user writing data to the Audit Database is granted the **Contributor** role in Netwrix Auditor. Alternatively, you can grant the **Global administrator** role or add the user to the **Netwrix Auditor Administrators** group. In this case, this user will have the most extended permissions in the product.
The computer where the service will be installed	• The UDP 514 port is open for inbound connections. • .Net Framework 3.5 SP1, 4.0, 4.5, or 4.6.
The target syslog-based platform	The Syslog daemon is configured to redirect events. The procedure below explains how to configure redirection: **NOTE:** Red Hat Enterprise Linux 7 and 6, SUSE Linux Enterprise Server 12, openSUSE 42, and Ubuntu 16 are supported out of the box. For other distributions, deployment of rsyslog package may be required. • On Red Hat Enterprise Linux 7: 1. Open the **/etc/rsyslog.conf** file. 2. Add the following line: `auth.*;authpriv.* @name:514;RSYSLOG_SyslogProtocol23Format` where `name` is a FQDN, NetBIOS name or IP address of the computer where Netwrix Auditor Server is installed. For example: `auth.*;authpriv.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format`

On...	Ensure that...

3. Launch the **RHEL** console and execute the following command: `service rsyslog restart`.

- On Ubuntu 16:

1. Navigate to the **/etc/rsyslog.d/50-default.conf** file.
2. Add the following line: `auth.*;authpriv.* @name:514;RSYSLOG_SyslogProtocol23Format`

   where `name` is a FQDN, NetBIOS name or IP address of the computer where Netwrix Auditor Server is installed. For example:

   `auth.*;authpriv.* @172.28.18.25:514;RSYSLOG_SyslogProtocol23Format`
3. Launch the **UBUNTU** console and execute the following command: `service rsyslog restart`.

3.2. Define Parameters

1. Navigate to your add-on package.
2. Edit the **Settings.xml** file.

   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 (`<paramenter>value</parameter>`). You can skip or define parameters depending on your execution scenario and security policies. See Choose Appropriate Execution Scenario for more information.

   Parameters in **Settings.xml** can be divided as follows: general parameters that affect add-on execution, settings for a certain event source (within the Source tag) that can override general settings, and internal parameters that should not be modified.

   NOTE: Do not modify parameters unless they are mentioned in the table below.

Parameter	Default value	Description
General parameters		
ListenUdpPort	514	Specify UDP port for listening incoming syslog events.
NetwrixAuditorEndpoint	https://localhost:	Netwrix Auditor Server IP address and

Parameter	Default value	Description
	9699/netwrix/api/v1/activity_records	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). **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

Parameter	Default value	Description
		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 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.

Parameter	Default value	Description
LogLevel	error	Specify logging level: • none • info • warning • error (used by default) • debug
SenderSleepTime	600	Specify retry interval in seconds to send messages to Netwrix Auditor (30 - 3600 seconds). -1— Disables message sending (used for debugging).
Parameters within SourceList		
You can specify parsing rules for each specific event source and define parameters to override general settings, such as timezone, 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.

Parameter	Default value	Description
		Otherwise, leave the default value.
RuleFileList PathFile	genericlinux.xml	Specify paths to XML files with regular expression parsing rules. You can create a custom file or use rules provided out of the box. Currently, the following rule files are shipped with this add-on: • **genericlinux.xml**—for syslog 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 example: `<Address naplan="Linux monitoring" naplanitem="RedHat" tstimezone="GMT StandardTime">172.28.3.15 </Address>`

3. Save **Settings.xml**.

NOTE: Every time you edit the **Settings.xml** file, restart the service, otherwise the product will ignore your changes.

3.3. Choose Appropriate Execution Scenario

Netwrix Auditor Add-on for Generic Linux Syslog runs 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 execution scenario you choose, you have to define a different set of parameters. See Define Parameters for more information.

Netwrix suggests the following execution 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 Netwrix Auditor Server.

3.4. Deploy the Service

1. On the computer where the service is going to be deployed, create a new folder (e.g., **Netwrix Auditor add-on**) and copy the contents of the add-on package.

2. Run the **install.cmd** file. The file deploys and enables the **Netwrix Auditor Syslog Message Processing Service**.

The service collects activity data and sends it to Netwrix Auditor every 10 minutes by default.

3.5. See Results

1. Start the Netwrix Auditor client and navigate to **Search**.
2. Click **Search**.

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

3.6. Expand List of Gathered Events

Based on the activity you get, you may want to adjust the processing rules, add other relevant events, etc. To do that, copy and edit the file with processing rules, and then restart the service.

Contact Netwrix Support to order custom files with regular expression parsing rules for your syslog event sources.

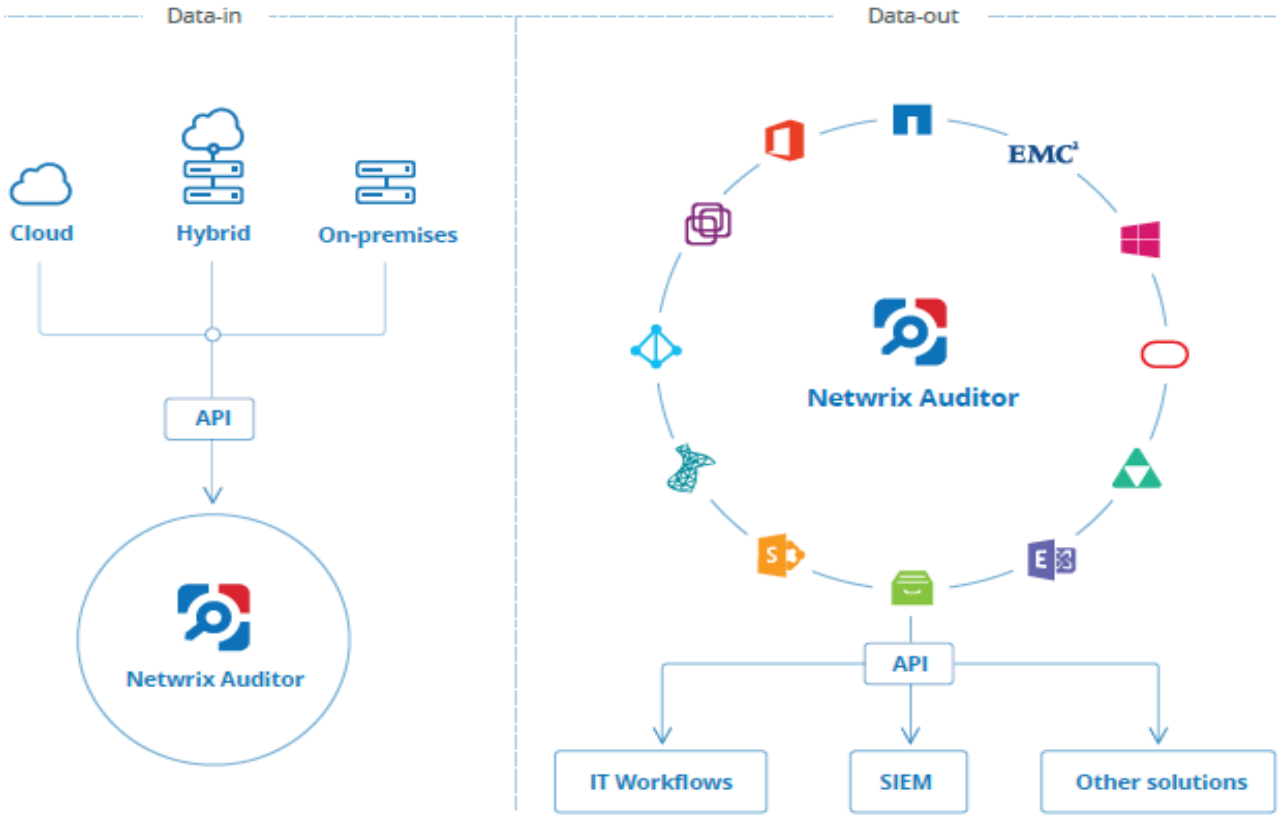
4. Netwrix Auditor Integration API Overview

Netwrix Auditor Add-on for Generic Linux Syslog leverages Netwrix Auditor Integration API. Although you can always use the add-on as is, but Netwrix encourages customers to create their own integration add-ons. The add-ons created based on Netwrix Auditor Integration API capabilities are easily tailored to your specific environment and business requirements.

Netwrix Auditor Integration API—endless integration, auditing and reporting capabilities.

The Netwrix Auditor Integration API provides access to audit data collected by Netwrix Auditor through REST API endpoints. According to the RESTful model, each operation is associated with a URL. Integration API provides the following capabilities:

- **Data in**: Solidify security and meet regulatory compliance standards by enabling visibility into what is going on in any third-party application.
- **Data out**: Further automate your business processes, IT security and operations workflows by enriching third-party solutions with actionable audit data.



Netwrix Auditor Integration API operates with XML- and JSON-formatted Activity Records—minimal chunks of audit data containing information on *who* changed *what*, *when* and *where* this change was made. XML format is set as default.

With Integration API you can write Activity Records to the SQL Server-based Audit Database and access audit data from remote computers. Also, Netwrix prepares add-ons—sample scripts—to help you integrate your SIEM solutions with Netwrix Auditor.

Netwrix does not limit you with applications that can be used with Integration API. You can write RESTful requests using any tool or application you prefer—cURL, Telerik Fiddler, various Google Chrome or Mozilla FireFox plug-ins, etc.

See Netwrix Auditor Integration API Guide for more information.