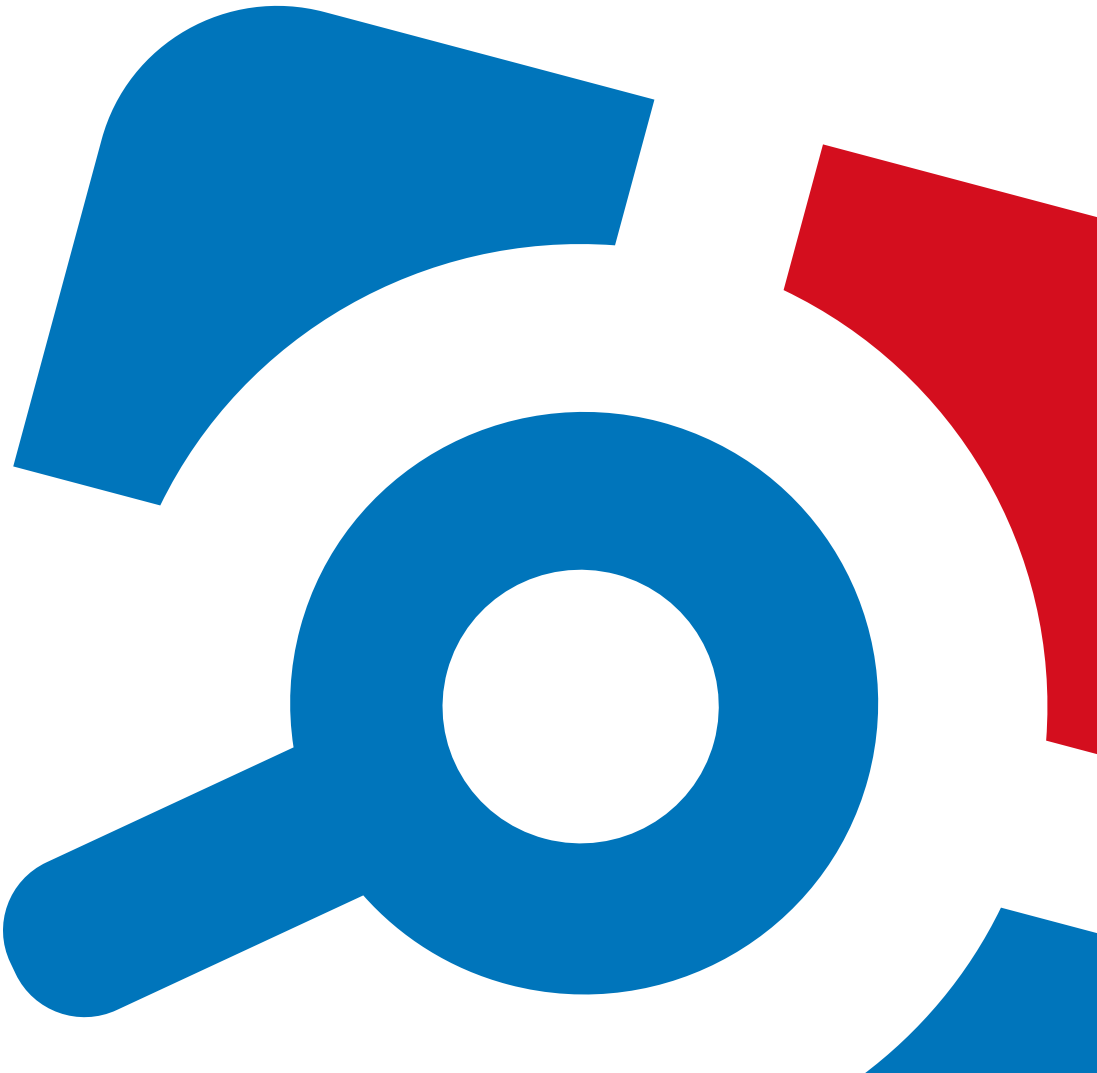
netwrix

Netwrix Auditor Add-on for Amazon Web Services

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 Amazon Web Services Overview

Amazon Web Services (AWS) provides a wide range of cloud-based services, including solutions and management tools for virtualization, data storage and hosting, private networking, relational and NoSQL databases, and many more. AWS CloudTrail is an internal tracking service that records AWS API calls. Companies leverage this information for analyzing user activity patterns and detecting potential threats. Unfortunately, collected audit data cannot be used for future reference: AWS CloudTrail stores events for 7 days allowing administrators and security analysts to review data for only short time periods.

Netwrix Auditor helps you gain complete visibility into Amazon Web Services user and service activity. The Netwrix Auditor Add-on for Amazon Web Services extends native AWS CloudTrail auditing and reporting possibilities. Aggregating data into a single audit trail simplifies activity analysis and helps you keep tabs on your hybrid cloud IT infrastructure. With Netwrix Auditor, AWS audit data is kept for much longer periods of time and always ready for review in easy-to-use search interface.

Implemented as a PowerShell script, this add-on automates the acquisition of Amazon Web Services CloudTrail logs and their transition to Netwrix Auditor. All you have to do is provide connection details and schedule the script for execution.

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

1. The add-on makes an AWS API call and collects activity events from AWS CloudTrail.
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.

   Currently, Netwrix Auditor processes details for the following AWS events (other events can be imported without details):

CreateGroup	CreateUser	CreateLoginProfile	CreateAccessKey
DeleteGroup	DeleteUser	DeleteLoginProfile	DeleteAccessKey
AddUserToGroup	RemoveUserFromGroup	UpdateLoginProfile	UpdateAccessKey

3. Using the Netwrix Auditor Integration API, the add-on sends the activity events 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.

2.1. Compatibility Notice

In Netwrix Auditor 9.0, Netwrix has updated API schemas. The scripts and add-ons designed for Netwrix Auditor 8.0 – 8.5 might become inoperable in Netwrix Auditor 9.6, while new add-ons designed for 9.0 and 9.6 cannot run at Netwrix Auditor 8.0 – 8.5.

Make sure to check your product version, and then review and update your add-ons and scripts leveraging Netwrix Auditor Integration API. Download the latest add-on version in the Add-on Store. For more information about schema updates, refer to Netwrix Auditor Integration API.

3. Use the Add-On

3.1. Prerequisites

Before running Netwrix Auditor Add-on for Amazon Web Services, 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 script will be executed	• Execution policy for powershell scripts is set to *"Unrestricted"*. Run **Windows PowerShell** as administrator and execute the following command: `Set-ExecutionPolicy Unrestricted` • The user running the script is granted the **write** permission on the script folder—the add-on creates a special .bin file with the last exported event. • AWS SDK for .NET is installed on your computer. Restart your computer after AWS SDK installation.
Amazon Web Services	• A trail is created in AWS CloudTrail. To gain complete visibility, Netwrix recommends to set **All** regions if you are using multiple regions in your environment. • AWS Access Key ID and Access Key are generated.

3.2. Define Parameters for Add-On

Before running or scheduling the add-on, you must define connection details: Netwrix Auditor Server host, user credentials, etc. Most parameters are optional, the script uses the default values unless parameters

are explicitly defined. You can skip or define parameters depending on your execution scenario and security policies. See Choose Appropriate Execution Scenario for more information.

First provide a path to your add-on followed by script parameters with their values. Each parameter is preceded with a dash; a space separates a parameter name from its value. You can skip some parameters—the script uses a default value unless a parameter is explicitly defined.

Parameter or switch	Default value	Description
AWSSDKInstallPath	'C:\Program Files (x86)\AWS SDK for .NET'	Assumes that AWS SDK for .NET is installed by its default path. To specify another location, provide a path in single quotes (e.g., 'C:\Program Files (x86)\My SDKs\AWS SDK for .NET').
ImportAllEvents	—	By deafult, only events with processed details will be imported. To import all events, set the switch during the add-on execution. **NOTE:** Importing all events makes audit data less human-readable.
NetwrixAuditorHost	localhost:9699	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).
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.
NetwrixAuditorPassword	Current user credentials	Unless specified, the script runs with the current user credentials. Provide a different password if necessary.

Parameter or switch	Default value	Description
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.

3.2.1. Update In-Script Parameters

1. Right-click a script and select **Edit**. **Windows PowerShell ISE** will start.
2. Navigate to the following lines:

```
$RegionEndpoint = "your AWS region endpoint"
$AccessKeyID = "your AWS access key ID"
$SecretAccessKey = "your AWS secret access key"
```

3. Update the following parameters:

Parameter	Description
RegionEndpoint	Provide an endpoint for your region, e.g., us-east-1 (N. Virginia). **NOTE:** If you use more than one region in your environment, run the script several times with different region endpoints. See Amazon regions and endpoints for more information.
AccessKeyID	Provide an AWS access key ID for your account. Access key is used to run requests to AWS SDK, CLIs, and API.
SecretAccessKey	Provide an AWS secret access key that works with your access key ID.

4. Save the script.

3.3. Choose Appropriate Execution Scenario

Netwrix Auditor Add-on for Amazon Web Services 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 Netwrix Auditor Add-on for Amazon Web Services Overview for more information.

Netwrix suggests the following execution scenarios:

Scenario	Example
The add-on runs on the Netwrix Auditor Server with the current user credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_Services.ps1`
The add-on runs on the Netwrix Auditor Server with the explicitly specified user credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_Services.ps1 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool`
The add-on runs on a remote computer. Data is written to a remote Netwrix Auditor repository with the current user credentials.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_Services.ps1 -NetwrixAuditorHost 172.28.6.15`
The add-on runs on a remote computer. Data is written to a remote Netwrix Auditor repository with the explicitly specified user credentials and monitoring plan name.	`C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_Services.ps1 -NetwrixAuditorHost 172.28.6.15 -NetwrixAuditorUserName enterprise\NAuser -NetwrixAuditorPassword NetwrixIsCool -NetwrixAuditorPlan Integrations`

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. Run the Add-On with PowerShell

To run the script with PowerShell

1. On computer where you want to execute the add-on, start **Windows PowerShell**.
2. Type a path to the add-on. Or simply drag and drop the add-on file in the console window.
3. Add script parameters. The console will look similar to the following:

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\AddOnUser> C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_Services.ps1 -
NetwrixAuditorHost 172.28.6.15
```

NOTE: If the script path contains spaces (e.g., `C:\Netwrix Add-ons\`), embrace it in double quotes and insert the ampersand (**&**) symbol in front (e.g., `& "C:\Netwrix Add-ons\"`).

4. Hit **Enter**.

Depending on the number of events logged by CloudTrail it may take a while. Ensure the script execution completed successfully. Every time you run a script, Netwrix Auditor makes a checkpoint with the last imported event. The next time you run the script, it will start retrieving new events.

NOTE: By default, CloudTrail keeps events for 7 days.

3.5. Automate Add-On Execution

To ensure you have up-to-date information about AWS user and service activity, Netwrix recommends scheduling a daily task for running the add-on.

To create a scheduled task

1. On the computer where you want to execute the add-on, navigate to **Task Scheduler**.
2. Select **Create Task**.
3. On the **General** tab, specify a task name, e.g., Netwrix Auditor Add-on for Amazon Web Services. Make sure the account that runs the task has all necessary rights and permissions.
4. On the **Triggers** tab, click **New** and define the schedule. This option controls how often audit data is exported from AWS CloudTrail and saved to Netwrix Auditor Audit Database. Netwrix recommends scheduling a daily task.
5. On the **Actions** tab, click **New** and specify action details. Review the following for additional information:

Option	Value
Action	Set to *"Start a program"*.
Program/script	Input *"Powershell.exe"*.
Add arguments (optional)	Add a path to the add-on in double quotes and specify add-on parameters. For example: `-file "C:\Add-ons\Netwrix_Auditor_Add-on_for_Amazon_Web_Services.ps1" -NetwrixAuditorHost 172.28.6.15`

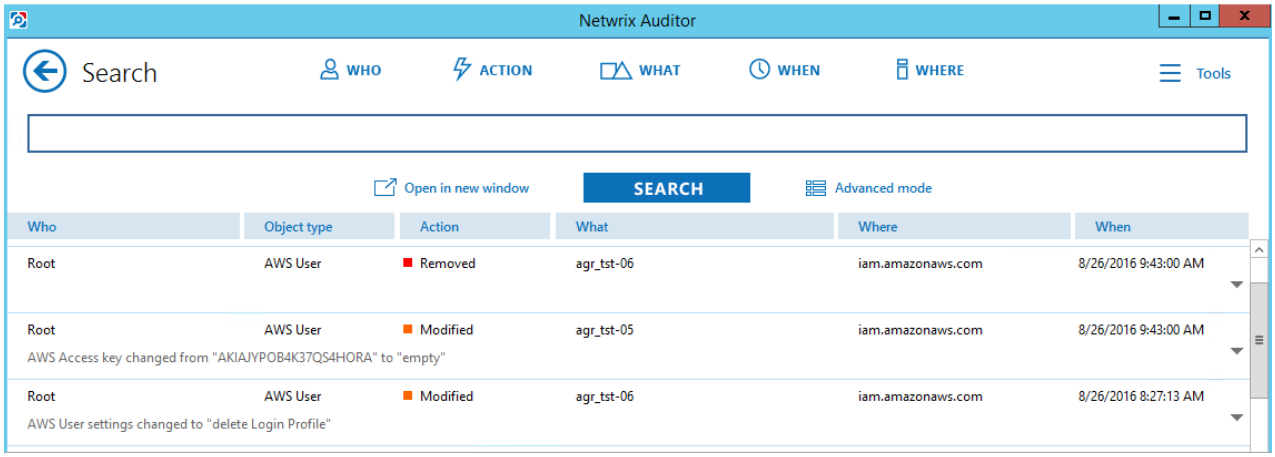
6. Save the task.

After creating a task, wait for the next scheduled run or navigate to **Task Scheduler** and run the task manually. To do this, right-click a task and click **Run**.

3.6. 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.



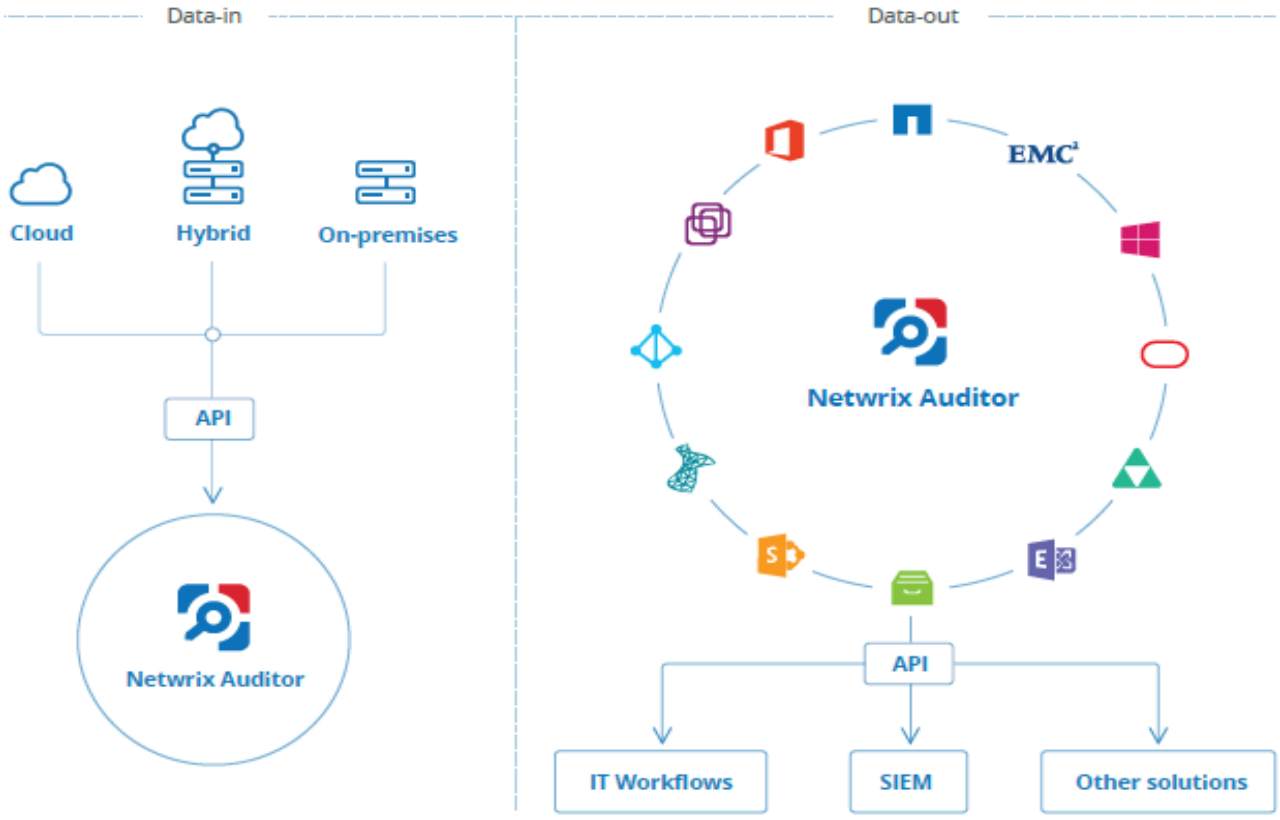
4. Netwrix Auditor Integration API Overview

Netwrix Auditor Add-on for Amazon Web Services 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.