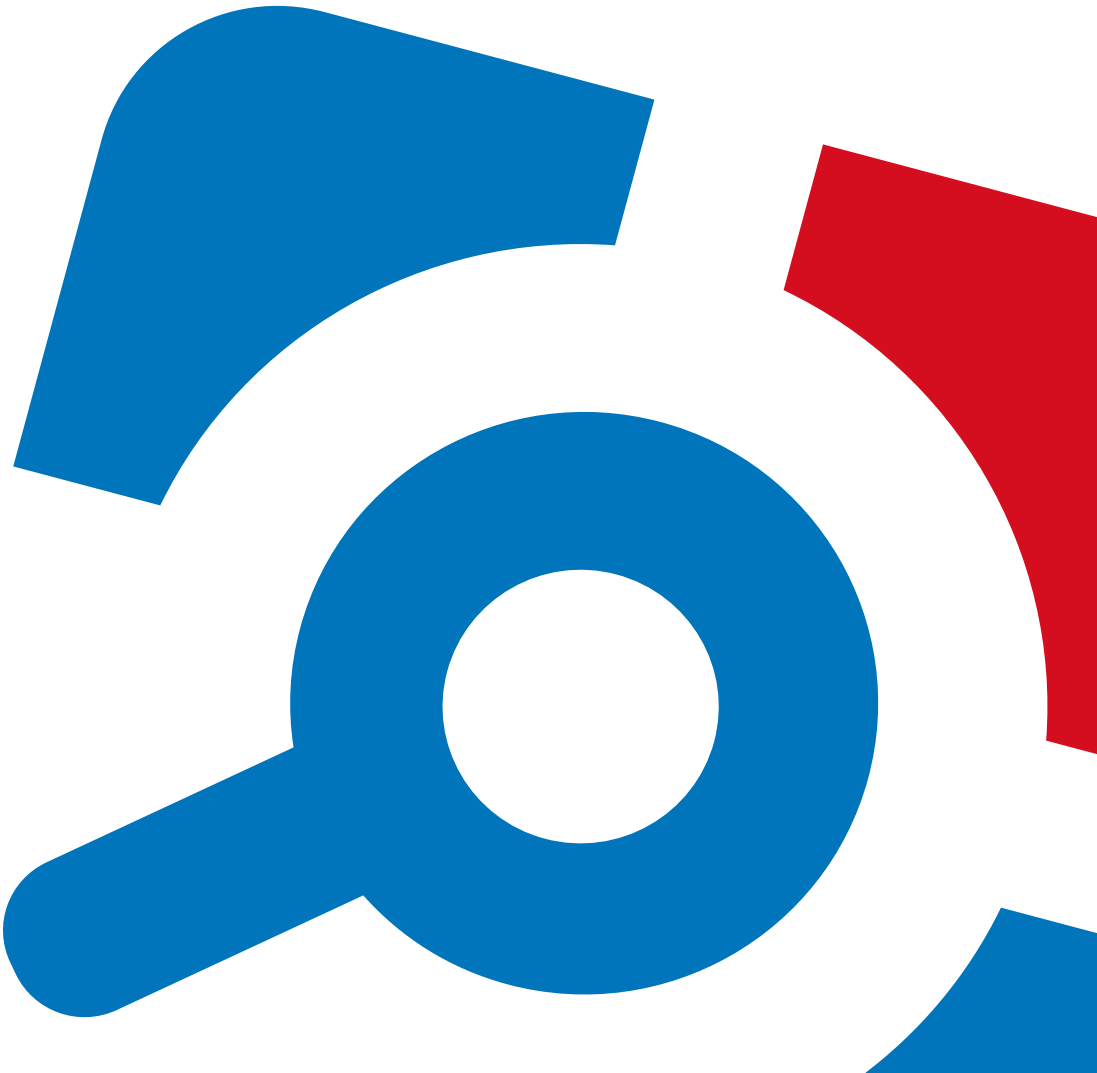
netwrix

Netwrix Auditor Add-on for Nutanix AHV

Quick-Start Guide

Version: 9.9
9/23/2020



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
4. Add-on delivery package 8
5. Before you start 9
   5.1. Prerequisites 9
   5.2. Accounts and rights 9
   5.3. Considerations and limitations 10
   5.4. Upgrade path 10
6. Deployment scenarios 11
   6.1. Example 1 11
   6.2. Example 2 11
7. Deployment procedure 13
   7.1. Step 1: Prepare Netwrix Auditor for data processing 13
   7.2. Step 2: Configure message forwarding for Nutanix Prism 13
   7.3. Step 3: Download the add-on 15
   7.4. Step 4: Configure add-on parameters 15
   7.5. Step 5: Register the add-on 18
8. Working with collected data 19
9. Maintenance and troubleshooting 20
10. Appendix. Object types and activities monitored on Nutanix Prism 21

1. About this document

This guide is intended for the first-time users of Netwrix Auditor add-on for Nutanix AHV. 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 assumes that you have Netwrix Auditor installed and configured in your environment. For Netwrix Auditor installation scenarios, data collection options, as well as for 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 AHV is a virtualization platform within the Nutanix Enterprise Cloud architecture. It provides facilities for VM deployment, operation and centralized management. Nutanix AHV is a fully integrated component of the Nutanix Enterprise Cloud.

Virtualization teams, Managed Service Providers and other IT professionals need to detect who does what in the Nutanix Hyperconverged infrastructure. For that, a unified audit trail is required, supporting detailed Nutanix monitoring and effective response to changes.

For that purpose, you can use a specially designed Netwrix Auditor add-on for Nutanix AHV that supports audit for Nutanix AHV and Nutanix Prism/Element. The add-on works in collaboration with Netwrix Auditor, supplying data about operations on your Nutanix AHV 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:

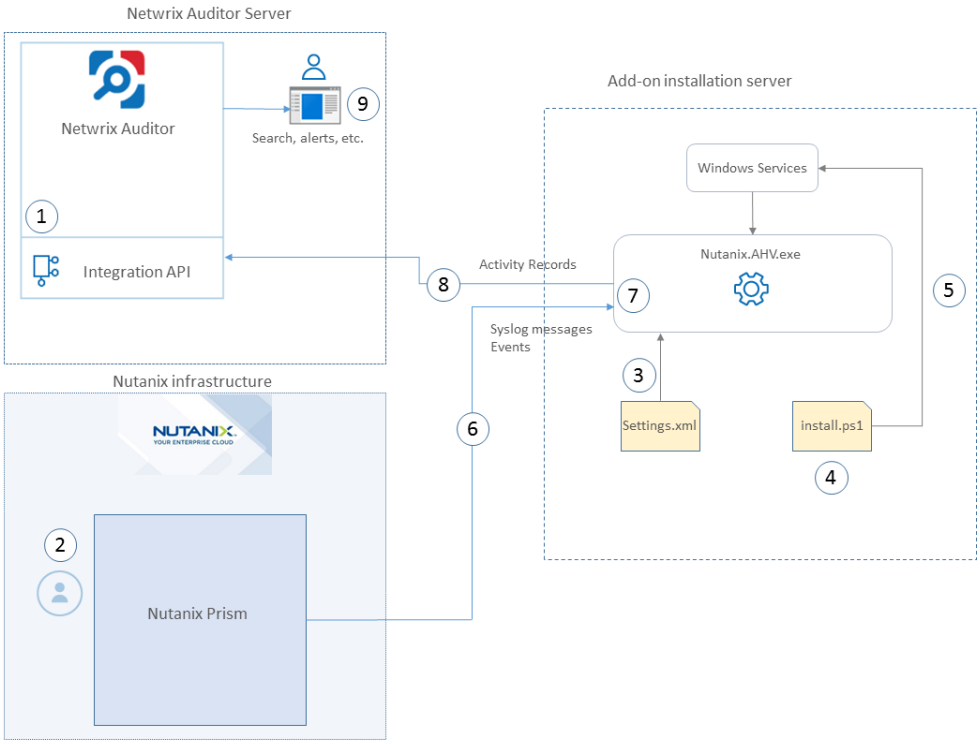
- Gain a high-level view of the data you store
- Detect unauthorized activity that might threaten your data

2.1. Compatibility notice

Netwrix Auditor add-on for Nutanix AHV is compatible with Nutanix AOS 5.11 and with Netwrix Auditor 9.9 and later.

3. How it works

The add-on is implemented as a Syslog service that collects activity data from Nutanix infrastructure 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 Prism Central/Element and configures Syslog server (IP, port, etc.).

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

4. The administrator selects the deployment scenario and runs the **install.ps1** PowerShell script file to deploy and configure the add-on components on the target server.

5. In particular, the script deploys and starts **Netwrix Auditor Add-on for Nutanix AHV** Windows

Service— this is the main add-on component, responsible for audit data collection and forwarding.

6. The add-on starts collecting and forwarding activity data from Nutanix Prism server: it listens to the specified UDP port and captures designated Syslog event messages and also collects activity data using Nutanix REST API.

   NOTE: Syslog event data communication is performed using UDP version of Syslog protocol. Default list of events supported out-of-the box is provided in the Appendix. Object types and activities monitored on Nutanix Prism.

7. The add-on processes the incoming Syslog messages and activity data collected using Nutanix REST API into Netwrix Auditor-compatible format (Activity Records). Each Activity Record contains the **Who-What-When-Where-Action** information (that is, initiator's 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 second.

   NOTE: For more information on the Activity Record structure and 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

4. Add-on delivery package

Netwrix Auditor add-on for Nutanix AHV delivery package is a ZIP archive comprising several files, including configuration and executable files listed in the table below.

File name	Description
Install.ps1	PowerShell script that creates windows service to execute add-on.
Settings.xml	Contains parameters for the add-on service operation.
setNutanixCredentials.ps1	Allows you to change user name or password for accessing Prism Central.
Netwrix.Nutanix.IntegrationService.exe	Main add-on component, responsible for audit data collection from Nutanix AHV.
Netwrix_Auditor_Add-on_for_Nutanix_AHV_Quick_Start_Guide.pdf	This document.

5. Before you start

5.1. Prerequisites

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

Where	Prerequisite to check
Netwrix Auditor Server side	1. Netwrix Auditor version 9.9 or later. 2. Netwrix Integration API and Audit Database settings are configured properly in Netwrix Auditor. See Configure Integration API and Audit Database. 3. The **TCP 9699** port must be open on Windows firewall for inbound connections. 4. 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.
The machine where the add-on will be installed	1. Any of the following Windows OS versions: • Windows Server 2012 R2 (or later) • Windows 8.1 (or later) 2. The **UDP** port must be open on Windows firewall for inbound connections. 3. .NET Framework versions 4.5 or later
Nutanix Prism server	Nutanix AOS 5.11

5.2. Accounts and rights

It is recommended to create a dedicated account for running **install.ps1** and **Netwrix Auditor Add-on for Nutanix AHV** (main service of the solution). 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.

This service account requires the **User Admin** role in Nutanix Prism. You will be prompted for the corresponding set of credentials when you run the **install.ps1** script (see Steps 4 and 5 of the Deployment procedure). User name and password for connection to Nutanix Prism server will be then encrypted and stored in the solution configuration.

5.3. Considerations and limitations

- By default, the add-on is targeted at a single Nutanix Prism Central/Element server.
- Netwrix add-on must be deployed in the same subnet as Nutanix Prism Central/Element server.
- Please be aware that monitoring of actions performed on the add-on installation server is not supported.

5.4. Upgrade path

To upgrade from versions released earlier than August 2020, do the following:

1. Stop and remove the **Netwrix Auditor Add-on for Nutanix AHV** service.
2. Download and unpack the new add-on package to the same location as the earlier version.
3. Run the **install.ps1** PowerShell script file from the new add-on version on the target server.

6. Deployment scenarios

Netwrix Auditor add-on for Nutanix AHVcan run on any computer in your environment, except for the machine where your Nutanix Prism Central/Element runs. Depending on the deployment scenario you choose, you will need to define a different set of parameters.

Possible deployment options are as follows:

1. Add-on running on the same machine as Netwrix Auditor Server.
2. Add-on running on the remote machine.

6.1. Example 1

- The add-on runs on the Netwrix Auditor Server.
- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>
https://172.28.6.19:9699/netwrix/api/v1/activity_
records</NetwrixAuditorEndpoint>
<NetwrixAuditorUserName/>
<NetrixAuditorPassword/>
```

NOTE: Configuration parameters **NetwrixAuditorUserName** and **NetrixAuditorPassword** are not required.

- **PrismIP** parameter in **DataCollection** section should contain the IP address of Nutanix Prism server.

```
<PrismIP>172.22.6.14</PrismIP>
```

NOTE: You will be prompted for the corresponding set of credentials (user name and password) when you run the **install.ps1** script (see steps 4 and 5 of the Deployment procedure). Credentials for connection to Nutanix Prism server will be then encrypted and stored in the solution configuration. Consider that user account should have the **User Admin** role in Nutanix Prism.

6.2. Example 2

- The add-on runs on the Netwrix Auditor Server with the explicitly specified user credentials, or on the remote machine.
- Configuration parameters to specify in **settings.xml** (sample values):

```
<NetwrixAuditorEndpoint>
https://172.28.6.19:9699/netwrix/api/v1/activity_
records</NetwrixAuditorEndpoint>

<NetwrixAuditorUserName>SecurityOfficer
</NetwrixAuditorUserName>

<NetwrixAuditorPassword>NetwrixUser
</NetwrixAuditorPassword>
```

- Also, specify the name of **Data Collection Server** (Nutanix Prism server):

```
<DataCollectionServer>NutanixServer</DataCollectionServer>
```

Netwrix recommends to create a special user account with permissions to access Netwrix Auditor Server and Nutanix server.

7. Deployment procedure

7.1. 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 *MonitoringPlan* and *MonitoringPlanItem* attributes in the add-on configuration parameters. See **Step 4** below for details.

7.2. Step 2: Configure message forwarding for Nutanix Prism

To provide for interaction and data flow between Nutanix Prism and Netwrix Auditor add-on for Nutanix AHV, you should set up the add-on installation server as a remote Syslog listener for Nutanix Prism. For that remote Syslog server, you will need to specify the IP address and port for inbound messages. Depending on Nutanix Prism server you are using (Element/Central), follow the related procedure below.

Procedure for Nutanix Prism Element

If you are using Nutanix Prism Element, do the following:

1. Connect to a Controller VM (or Nutanix Prism) by SSH or via web console and execute the `ncli` command.

NOTE: IP address of the Controller VM can be found in Nutanix web console under **Settings** > **General** > **Configure CVM**.

Alternatively, you can download and install the *ncli* (Nutanix command-line interface) on any server in your infrastructure, as described here, and connect to a Controller VM in your cluster.

2. By default, the remote Syslog listening server is enabled. Disable it temporarily until you configure a new remote Syslog listener. For that, run the following command in ncli:

   ```
   ncli> rsyslog-config set-status enable=false
   ```

3. Create a remote Syslog server — a remote server that will operate as a Syslog listener, receiving the Syslog messages from Nutanix server. In the integration solution deployment, it will be the add-on installation server. Run the following command in *nlci*:

   ```
   ncli> rsyslog-config add-server name=<CustomServerName> ip-
   address=<RemoteIP> port=<Port> network-protocol=udp
   ```

   here:

   - `CustomServerName` — remote server that will receive the syslog messages (i.e., server on which the add-on will be deployed)
   - `RemoteIP` — remote server IP address
   - `Port` — Destination port number on the remote server

   To ensure the server was created successfully, review the list of servers. For that, run the following command:

   ```
   ncli> rsyslog-config ls-servers
   ```

   NOTE: The server will be added to the cluster automatically.

4. Instruct the AUDIT module of Nutanix solution to forward its log information to the new remote syslog listener, and specify the logging level. For that, run the following command:

   ```
   ncli> rsyslog-config add-module server-name=<CustomServerName> module-
   name=AUDIT include-monitor-logs=false level=notice
   ```

5. Finally, enable syslog forwarding to remote server:

   ```
   ncli> rsyslog-config set-status enable=true
   ```

   NOTE: This syslog server will be added to the cluster automatically.

Procedure for Nutanix Prism Cenral

First, provide the new remote Syslog server settings to Nutanix Prism server that will forward Syslog messages. For that, do the following:

1. Log in to Nutanix Prism Central.
2. Select **Settings→ Email and Alerts→ Syslog Server**.
3. Click **Configure Syslog Server**.

4. Enter remote Syslog server settings you specified at Step 2:
   - **Server Name** — name of the remote server.
   - **IP Address** — server IP address.
   - **Port**— port for incoming messages
5. Select **UDP** as communication protocol.
6. Click **Configure**.

Next, for the most detailed logs to be sent to remote Syslog server, set the logging level in Prism to *5* (*Notice*):

1. Select **Data Source** and click **Edit**.
2. Select **Audit** module and select **5 - Notice** level.
3. Finally, click **Save**.

7.3. Step 3: Download the add-on

1. Download the distribution package from the Netwrix website.
2. Unpack it to a folder on the computer where you plan to deploy the add-on.

7.4. Step 4: Configure add-on parameters

Open the add-on folder and edit the **settings.xml** file to configure the add-on parameters:

Parameter	Default value	Description
	NetwrixAuditorIntegration	
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

Parameter	Default value	Description
		server name followed by the port number (e.g., WKS.enterprise.local:9999). **NOTE:** Do not modify the endpoint part (/netwrix/api . . . .)
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.
DateTimeFormat	yyyy-MM-ddTHH:mm:ssZ	Netwrix Auditor time format. By default, set to zero offset.
MonitoringPlan	—	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.
MonitoringPlanItem	—	Unless specified, data is not associated with a specific plan and, thus, cannot be filtered by item name.

Parameter	Default value	Description
		Specify an item name. **NOTE:** Make sure to create a dedicated item in Netwrix Auditor in advance.
UserName	Current user credentials	Credentials to access Netwrix Auditor server. 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.
Password	Current user credentials	Unless specified, the service runs with the current user credentials. Provide a different password if necessary.
ARsNumberAtTime		Maximum number of Audit Records that can be sent to Netwrix Auditor at a time.
ARsSendingPeriodicity		Periodic time inteval for sending Activity Records (in seconds).
PauseWhenSendingFailed		Pause after a failed attempt to send Activity Records (in seconds).
DataCollection		
ListenUDPPort	514	UDP port for receiving incoming Syslog messages. **NOTE:** Make sure that this port is not used by any other add-ons or applications (for example, Netwrix Auditor for Network Devices); otherwise specify another port here.
PrismIP		IP address of Prism Cental server.
UserName		Credentials to accessing Prism Central. **NOTE:** Manual configuration is not

Parameter	Default value	Description
		required. This parameter will be configured automatically by **install.ps1** script. If you need to modify it later, use **setNutanixCredentials.ps1** script from the add-on package.
Password		Credentials to accessing Prism Central. **NOTE:** Manual configuration is not required. This parameter will be configured automatically by **install.ps1** script. If you need to modify it later, use **setNutanixCredentials.ps1** script from the add-on package.
StateUpdatingPeriodicity		Periodic time interval for updating state of clusters (in seconds).
EventsReadingPeriodicity		Periodic time interval for reading events (in seconds). Target endpoint: */api/nutanix/v2.0/events*
PageLength		The number of objects loaded with one request.
ShortTermFolder		Short term folder for collected data (full or local path).

NOTE: If you modify parameters in the **settings.xml** file, remember to save the changes and then restart the **Netwrix Auditor Add-on for Nutanix AHV** service for them to take effect.

If you need to change user name or password for accessing Prism Central, you should run **setNutanixCredentials.ps1** script that will prompt you for the new credentials (see step 5 below). Then restart the Netwrix Auditor Add-on for Nutanix AHV service for the changes to take effect.

7.5. Step 5: Register the add-on

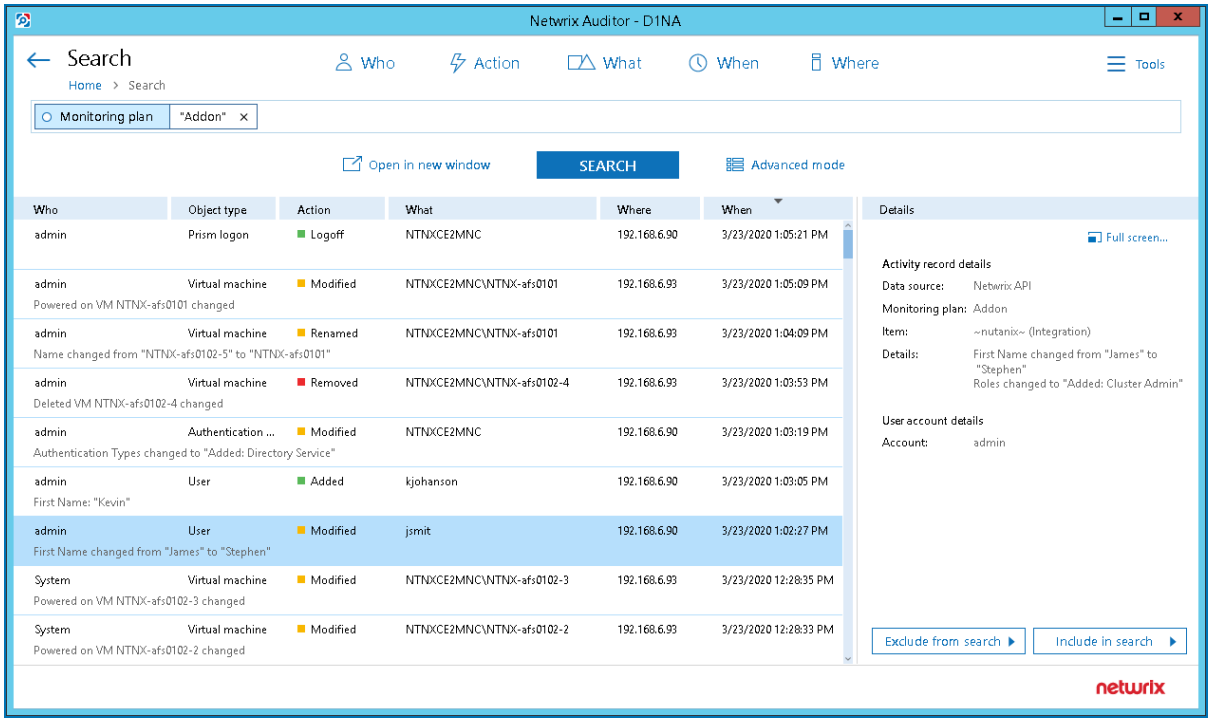
Run the **install.ps1** PowerShell script to register the add-on service. You will be also prompted to specify credentials for accessing Nutanix Prism Central. These credentials will be encrypted and used for secure communication. If you need to modify them later, use **setNutanixCredentials.ps1** script from the add-on package.

8. 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.

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

9. Maintenance and troubleshooting

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** .

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

Currently, the add-on supports only one Prism installation (Central or Element). To monitor more than one Prism Central/Element, you can copy the add-on to another folder, configure **settings.xml** as described in this document and modify **install.ps1** to rename the service:

1. Deploy one more add-on instance to the server where the first add-on instance is already installed. Be sure to use a different installation folder.
2. Open **settings.xml** and configure the new add-on instance to work with the second Prism server.
3. Open **install.ps1** for the new add-on for edit.
4. Modify the default service name:

   ```
   $name = "enter_new_name"
   ```

5. Save and then launch the updated **install.ps1** file.

10. Appendix. Object types and activities monitored on Nutanix Prism

Review a full list of object types and activities monitored on Nutanix Prism with Netwrix Auditor add-on for Nutanix AHV.

Object	Action	Property
Virtual Machine	Create/Delete Clone Migrate Rename State change (Power off/on, Pause etc.) Restore from snapshot Hardware Configuration change	Name MAC Address VLAN Name Connection State Number Of Processors Cores Per Processor Memory Size (MiB) Disk Size (Bytes) Host IP
Host (Node)	Add/Remove	IP
Local User	• Create/Delete • Properties change • Roles change • Log in/out • Password Change	• Username • First Name • Last Name • Email • Language • Roles
Authentication Configuration	• Authentication type change	• Authentication Types