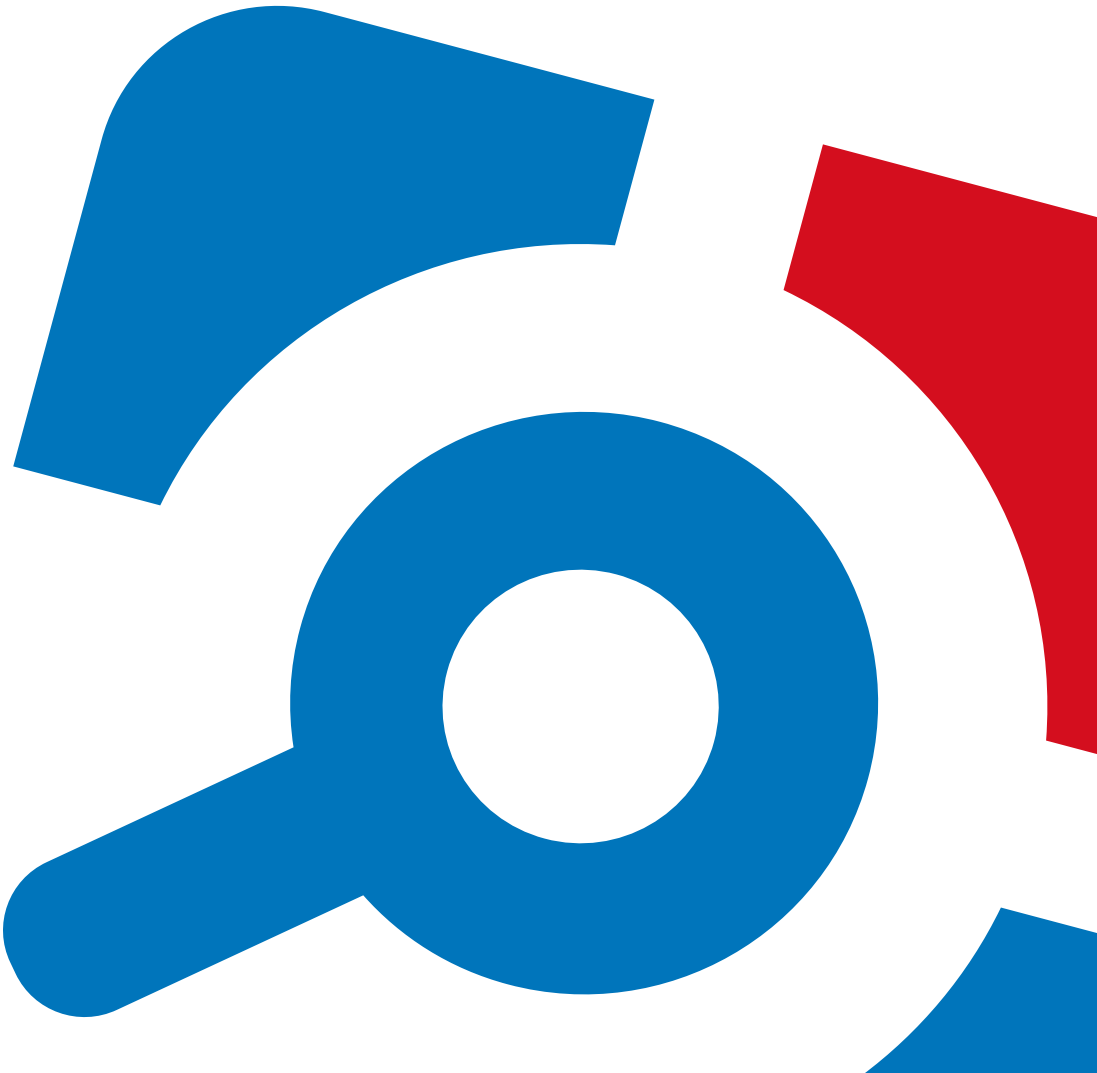
netwrix

Netwrix Auditor Add-on for Hyper-V SCVMM

Quick-Start Guide

Version: 9.9
3/16/2020



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

This guide is intended for the first-time users of Netwrix Auditor add-on for Hyper-V SCVMM (Microsoft System Center Virtual Machine Manager). 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:

- Deploy the add-on and configure its parameters
- Run 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.

Microsoft System Center Virtual Machine Manager (SCVMM) is a solution for configuring and managing virtualized infrastructure components across on-premises, service provider, and the Azure cloud environment. These components include virtualization servers, networking components and storage resources.

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

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

Major benefits:

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

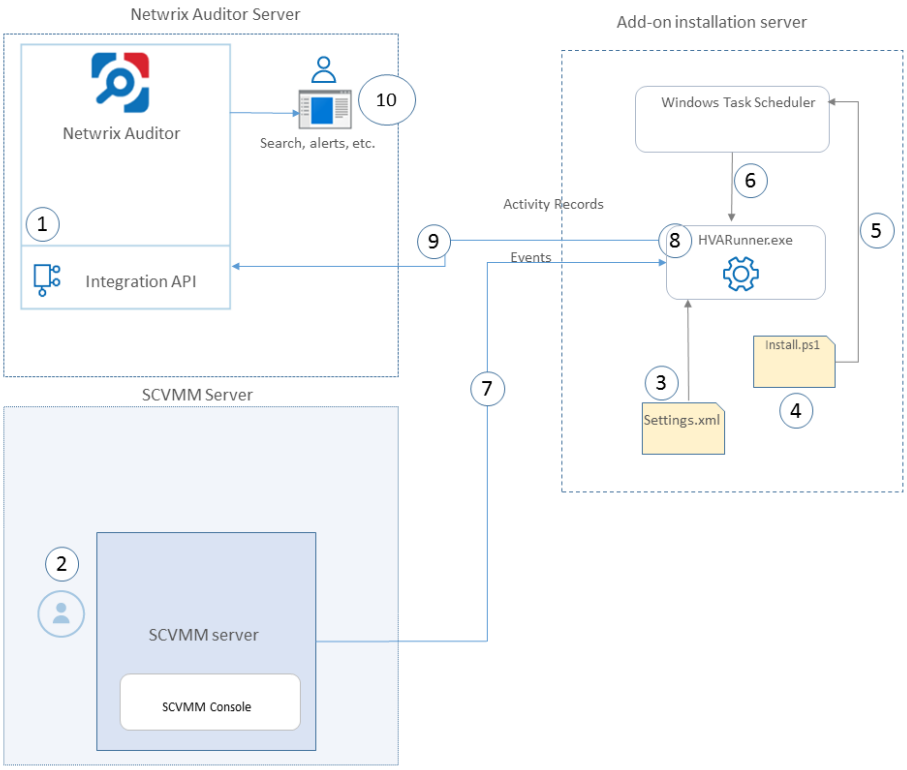
2.1. Compatibility Notice

Netwrix Auditor add-on for Hyper-V SCVMM is compatible with:

- Microsoft System Center Virtual Machine Manager 2019 and 2016
- Netwrix Auditor 9.9 and later

3. How It Works

The add-on is implemented as a stand-alone application that collects activity data from Virtual Machine Manager 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 or item name.

2. On SCVMM side, the IT administrator prepares a dedicated user account for accessing SCVMM server. This account requires administrative rights.
3. Then the IT administrator opens **settings.xml** configuration file and specifies the necessary parameters for add-on operation, including Netwrix Auditor server settings, etc.
4. The IT administrator selects the deployment scenario and runs **install.ps1** PowerShell script file to deploy and configure the add-on components on the target server.
5. This script creates a Windows scheduled task that will run periodically (every 15 minutes) to collect

audit data from VMM server.

NOTE: Default list of the events supported out-of-the box is provided in the Appendix A. Monitored SCVMM Events.

6. The add-on component **HVARunner.exe** starts collecting activity data from VMM. Data communication is performed using TCP protocol.
7. The add-on processes this data 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).

   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.
8. The add-on uses Netwrix Auditor Integration API to send the Activity Records to Netwrix Auditor Server, where this data becomes available for search, reporting and alerting.
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 Hyper-V SCVMM delivery package is a ZIP archive comprising several files, including DLLs, configuration and executable files. The latter ones are listed in the table below.

File name	Description
install.ps1	PowerShell script that installs the add-on components and creates a scheduled task for data collection.
settings.xml	Contains parameters for the add-on service operation.
HVARunner.exe	Main add-on component, responsible for audit data collection from SCVMM.
Netwrix_Auditor_Add-on_for_Microsoft_SCVMM_Quick_Start_Guide.pdf	This document.

4. Before You Start

4.1. Prerequisites

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

Where	Prerequisite to check
Netwrix Auditor Server	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.
Add-on installation server, i.e. the machine where the add-on will be installed	1. The **TCP 5985** port must be open on Windows firewall for inbound connections. 2. NET Framework 4.5 or later.
Microsoft System Center Virtual Machine Manager	SCVMM versions: • 2019 • 2016
Virtualization hosts	• Microsoft Hyper-V (hardware and nested-virtualization) • VMware ESXi

4.2. Accounts and Rights

It is recommended to create a dedicated account for running the add-on.

This account should have the following minimal rights and permissions:

- **Administrator** role in SCVMM
- **Contributor** role in Netwrix Auditor (see Role-Based Access and Delegation for more information)

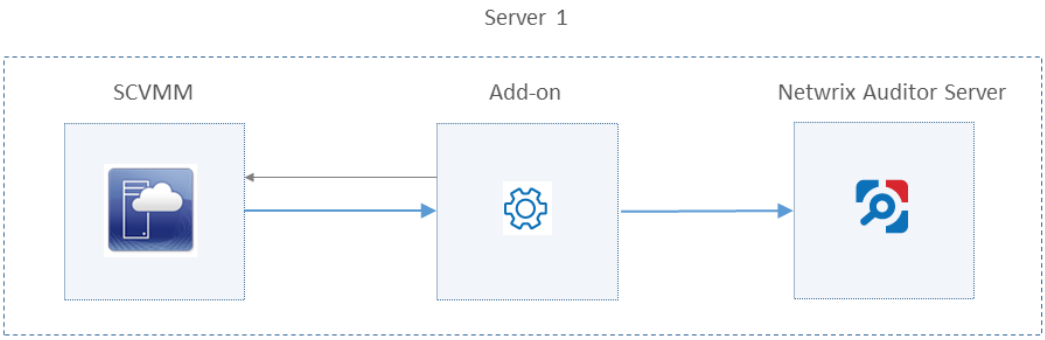
4.3. Considerations and Limitations

- By default, the add-on is targeted at a single SCVMM server.
- If Netwrix Auditor server becomes unavailable for some time, the add-on will reset the last data collection and will run it anew during the next scheduled interval.

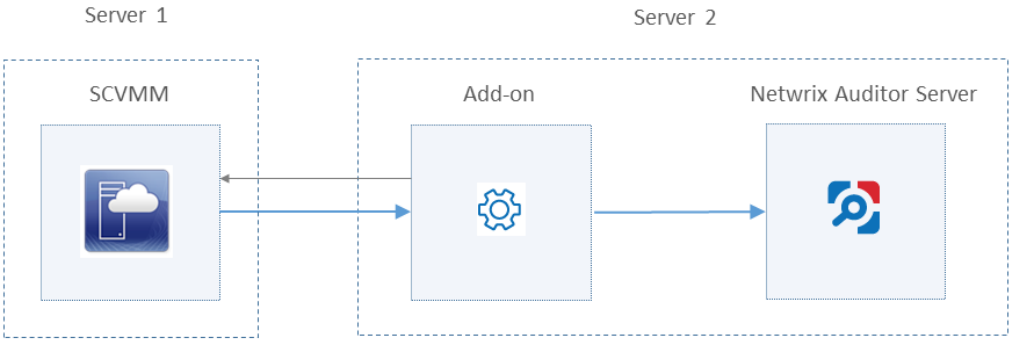
5. Deployment Scenarios

Netwrix Auditor add-on for Hyper-V SCVMM can be deployed 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. Also, consider different SCVMM deployment scenarios. Possible deployment options are as follows (here it is assumed that the add-on is installed together with Netwrix Auditor server):

1. Add-on running on the same machine as SCVMM server (with Management Console):

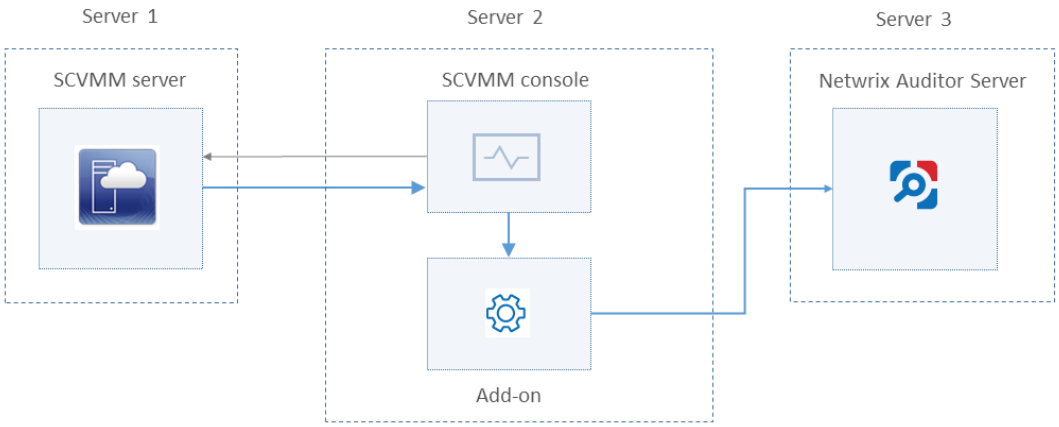


2. Add-on and SCVMM server (with Management Console) running on different machines:



   In this scenario, the account used to access SCVMM server must be a member of the *Remote Management Users* local group on the SCVMM server.

3. Add-on running on the same machine as SCVMM Management Console; SCVMM server running on the remote machine:



In this scenario, make sure to specify SCVMM server address in the **DataCollectionServer** parameter (not the machine where SCVMM console runs) in the **settings.xml** configuration file. See the table below and also the Appendix B. Add-on Parameters.

Depending on the deployment scenario you choose, you will need to define a set of the add-on parameters. Several examples are provided below.

NOTE: In the certain scenarios you may need to configure not all parameters but only some of them.

5.1. Examples

5.1.1. Example 1

- The add-on runs on the Netwrix Auditor Server.
- The *System* account is used to launch the add-on via Task Scheduler (default configuration).
- 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.

5.1.2. Example 2

- The add-on runs on the Netwrix Auditor Server with the explicitly specified user credentials.
- 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>
```

5.1.3. Example 3

- The add-on runs on the machine with SCVMM.
- The *System* account is used to launch the add-on via Task Scheduler (default configuration).
- Configuration parameters to specify in **settings.xml**:

```
<DataCollectionServer/>

<DataCollectionUserName/>

<DataCollectionPassword/>
```

NOTE: Credentials for **Data Collection Server** (that is, SCVMM) are not required.

5.1.4. Example 4

- SCVMM and/or Netwrix Auditor run on the machines other than the add-on server.
- In this case, the corresponding set of credentials (for **Data Collection Server** and/or **Netwrix Auditor**) must be specified explicitly.
- 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>

<NetrixAuditorPassword>NetwrixUser</NetrixAuditorPassword>

<DataCollectionServer>SCVMMServer</DataCollectionServer>

<DataCollectionUserName>SCVMMAdmin</DataCollectionUserName>

<DataCollectionPassword>Password</DataCollectionPassword>
```

6. Deployment Procedure

6.1. 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 *NetwrixAuditorPlan* and *NetwrixAuditorPlanItem* parameters in the **settings.xml** file. See Appendix B. Add-on Parameters for details.

6.2. Step 2: Download the Add-On

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

6.3. Step 3: Configure Parameters for Data Collection

In the add-on folder, open the **settings.xml** file and configure the add-on parameters for data collection, as listed below.

NOTE: For the full list of configuration parameters, refer to Appendix B. Add-on Parameters.

Parameter	Default value	Description
DataCollectionServer	(empty)	Specify SCVMM server to collect data

Parameter	Default value	Description
		from. You can use IP address, FQDN or NETBIOS name. For *localhost*, leave this parameter empty.
DataCollectionUserName	(empty)	Specify user account that will be used for data collection from SCVMM server. To use the account currently logged in, leave this parameter empty. Make sure the account has administrative rights on that server (see Accounts and Rights section).
DataCollectionPassword		Specify user account password.
ShortTermFolder	*ShortTerm*	Specify path to the short-term archive (Netwrix Auditor working folder). You can use full or relative path.

Save the **settings.xml** file. New configuration settings will be applied automatically at the next data collection.

For the full list of parameters, refer to Appendix B. Add-on Parameters.

6.4. Step 4: Register Windows Scheduled Task

Run the **install.ps1** PowerShell script from the add-on folder. It will configure and register a Windows scheduled task that will run periodically every 15 min to retrieve audit data from SCVMM.

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

- If you cannot see collected data in Netwrix Auditor, check the following:
  - Add-on account has sufficient rights to access SCVMM and Netwrix Auditor.
  - 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**.
  - If you configured a dedicated monitoring plan, make sure data source monitoring is enabled.
  - Verify the parameters you provided in **settings.xml**.
- If you need to monitor more that one SCVMM, then you can do the following:
  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 SCVMM server.
  3. Open **install.ps1** for the new add-on for edit.
  4. Modify the default scheduled task name:

     ```
     $name = "NetwrixAuditor Add-on for Microsoft SCVMM"
     ```

  5. Save and then launch the updated **install.ps1** file.
- If you need to modify the task schedule, you can do the following:
  1. Open **install.ps1** for edit.
  2. Modify the default scheduled task schedule:

     ```
     $task.Triggers.Repetition.Interval = "PT15M"
     ```

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

NOTE: Alternatively, you can use Windows Task Scheduler.

- If the solution was deployed using the third scenario (that is, SCVMM server and add-on are running on different machines), then the following error may be written in the solution log:

The WinRM client cannot process the request.

See also Deployment Scenarios

If the authentication scheme is different from Kerberos, or if the client computer is not joined to a domain, then HTTPS transport must be used or the destination machine must be added to the **TrustedHosts** list. To configure this list, use **winrm.cmd**.

NOTE: Computers included in the **TrustedHosts** list might not be authenticated. To get more information about their settings, you can run the following command:

```
winrm help config
```

For details on remote troubleshooting and authentication issues, see this Microsoft article.

To work around, add the remote SCVMM server to the **TrustedHosts** list on the machine were the add-on runs. For that, use the following commands:

```
winrm quickconfig
Set-Item WSMan:\localhost\Client\TrustedHosts -Value "ServerNameOrIP"
```

here:

`ServerNameOrIP` – SCVMM server name or IP address.

9. Appendix A. Monitored SCVMM Events

Review a full list of the events that can be monitored using the add-on.

Object Type	Reported Action	Reported Properties
Virtual Machine	• Create/Delete • Clone • Migrate • Rename • Create/Delete Checkpoint • Hardware Configuration change	• Name • Checkpoint Name & Description • Number Of Processors • Memory Size (Allocated, Max) • VHD Location, Max size • Network Name • Switch Name
Hypervisor (Host)	• Create/Delete • Move • Hardware Configuration change • State change	• Name • Number Of Processors • RAM Memory Size • Host Disk Capacity
Host Cluster	• Create/Delete • Move	• Name
Host Group	• Create/Delete • Move • Rename	• Name
Private Cloud	• Create/Delete • Rename	• Name
VM Network	• Create/Delete • Rename	• Name
User Role	• Rename	• Name

Object Type	Reported Action	Reported Properties
	• Add/Remove Members • Add/Remove Scopes • Permissions change	• Scope • Permissions • Members

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.

Parameter	Default value	Description
	NetwrixIntegration	
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). **NOTE:** Do not modify the endpoint part (/netwrix/api . . . .)
NetwrixAuditor CertificateThumbprint	NOCHECK	Netwrix Auditor Certificate Thumbprint Property. Possible values: • `AB:BB:CC.`—Check Netwrix Auditor Server certificate thumbprint identifier.

Parameter	Default value	Description
		• NOCHECK—Do not check Netwrix Auditor certificate. Make sure to select this parameter if you plan to specify servers by their IP.
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.
NetwrixAuditorUserName	Current user credentials	Unless specified, the add-on runs with the current user credentials. If you want the add-on to use

Parameter	Default value	Description
		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 add-on runs with the current user credentials. Provide a different password if necessary.
	DataCollection	
DataCollectionServer	(empty)	Specify SCVMM server to collect data from. You can use IP address, FQDN or NETBIOS name. For localhost, leave this parameter empty.
DataCollectionUserName	(empty)	Specify user account that will be used for data collection from SCVMM server. To use the account currently logged in, leave this parameter empty. Make sure the account has administrative rights on that server (see Accounts and Rights section).
DataCollectionPassword		Specify user account password.
ShortTermFolder	*ShortTerm*	Specify path to the short-term archive (Netwrix Auditor working folder). You can use full or relative path.

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