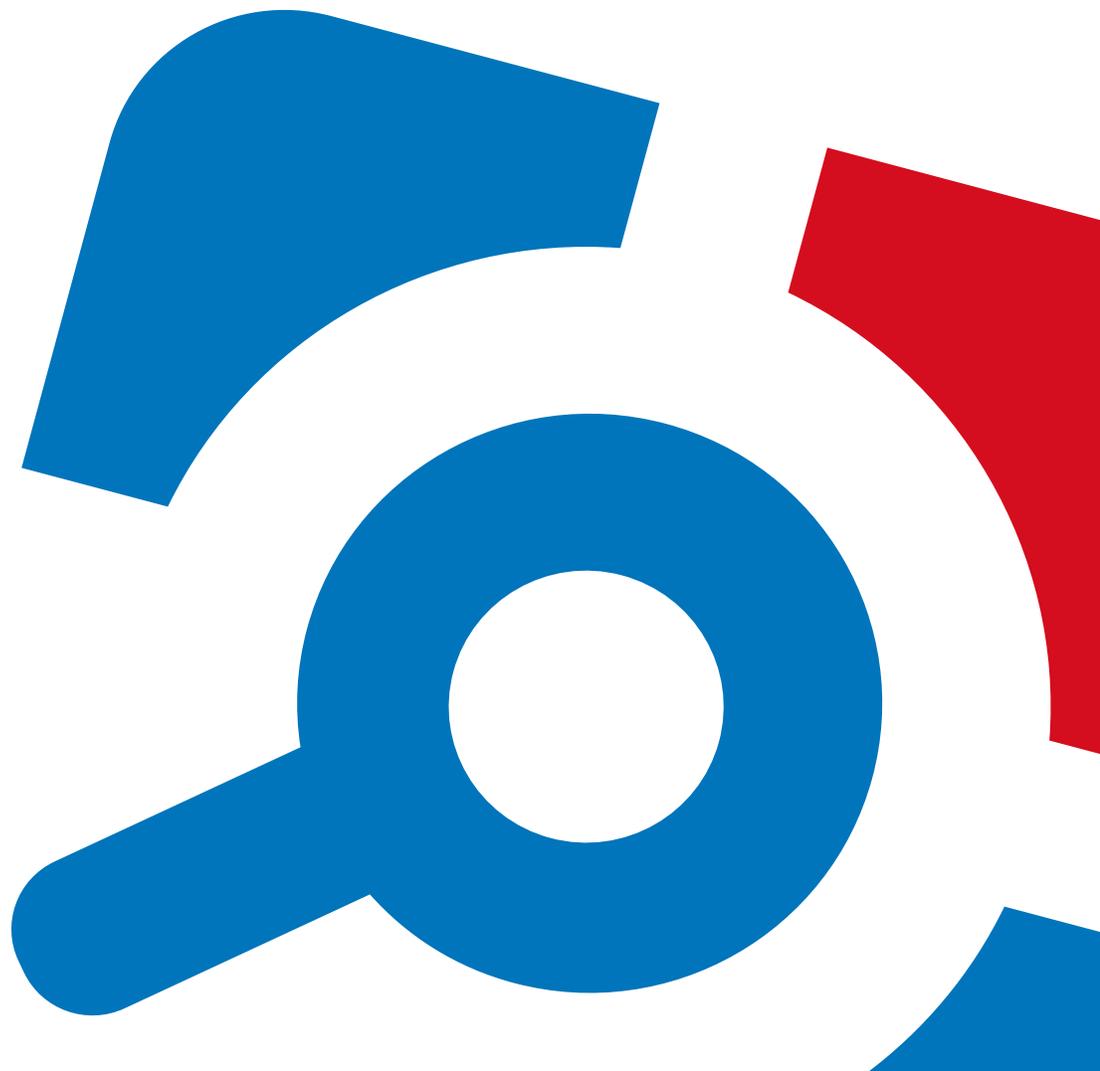netwrix

Netwrix Auditor

Virtual Appliance and Cloud Deployment Guide

Version: 9.6
6/15/2018

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. Overview

In addition to traditional on-premises deployment, Netwrix Auditor now offers new deployment options that can speed time-to-value by getting you up and running in less than 15 minutes. The following additional deployment options are available:

- **Virtual appliance**—If you run a Microsoft Hyper-V or VMware vSphere, you can deploy Netwrix Auditor as a virtual appliance. Virtual appliance is a VM image file with installed Netwrix Auditor and enabled auto-audit (User Activity monitoring for localhost). The following configuration options are available:

  - Generalized Windows Server 2012 R2, 180-day evaluation version, and Microsoft SQL Server 2014 Express with native Reporting Services installed.

  - Generalized Windows Server 2016, 180-day evaluation version, and Microsoft SQL Server 2016 Express with native Reporting Services installed.

  Navigate to the Netwrix website at https://www.netwrix.com/virtual_appliances.html and start the Virtual Appliance Download Manager.

  Review the following for additional information:

  - Virtual Deployment

- **Cloud deployment**—If you have an active AWS or Azure Marketplace account, you can deploy Netwrix Auditor in the cloud. The Netwrix Auditor virtual machine image consists of Windows Server 2016 and Netwrix Auditor. The image also contains Microsoft SQL Server 2016 Express with native Reporting Services installed.

  Review the following for additional information:

  - Cloud Deployment

2. Virtual and Cloud Deployment

2.1. Virtual Deployment

This section explains how to import a virtual machine with installed Netwrix Auditor to your virtual environment.

Review the following for additional information:

- Requirements to Deploy Virtual Appliance
- Import Virtual Machine from Image to VMware
- Import Virtual Machine from Image to Hyper-V

2.1.1. Requirements to Deploy Virtual Appliance

This section provides the software requirements and represents the default hardware configuration for the virtual machine where Netwrix Auditor virtual appliance is going to be deployed. Refer to the following sections for detailed information:

- Software Requirements
- Hardware Configuration

NOTE: The requirements below are sufficient for evaluation purposes only. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on the requirements for installing Netwrix Auditor in production environments.

2.1.1.1. Software Requirements

The table below lists the minimum software requirements for the virtual appliance deployment:

Virtual Environment	Requirements
VMware	- VMware: ESXi 5.1, 5.5, 6.0, 6.5 - Workstation: 11 and 12
Hyper-V Server	- Windows Server 2012 - Windows Server 2012 R2

2.1.1.2. Hardware Configuration

When deploying Netwrix Auditor virtual appliance, a pre-configured virtual machine is created. The table below contains the default hardware configuration of the VM where Netwrix Auditor virtual appliance is going to be deployed:

Parameter	Value
Common	
Processor	4 cores
RAM	16 GB
HDD	100 GB
VMware only	
Total Video Memory	16 MB
Network adapter	vmxnet3
Other	Check and upgrade VMware tools during power cycle.

2.1.2. Import Virtual Machine from Image to VMware

1. Connect to your VSphere Client and select **File → Deploy OVF Template**. Then follow the instructions in the table below:

Step	Description
Source	Browse for the folder that contains the Netwrix Auditor virtual appliance template.
OVF Template Details	Review information on this template.
Name and Location	Select a name for the new virtual machine if you do not want to use the default name *"Netwrix Auditor"*. NOTE: The name must be unique within the inventory folder and may contain up to 80 characters including spaces.
Resource Pool	Select a resource pool to deploy Netwrix Auditor virtual appliance.

Step	Description
Storage	Select destination storage.
Disk Format	Netwrix recommends to select the **Thin Provision** option to save your disk space.
Network Mapping	If you have multiple networks on your ESXi Server, select the **Destination** network for a new virtual machine.
Ready to Complete	Review your virtual machine settings. Click **Finish** to exit the wizard.

2. Select the newly created virtual machine and click **Power On**.

2.1.3. Import Virtual Machine from Image to Hyper-V

1. On your Hyper-V server, unzip the Netwrix Auditor virtual appliance package to the specified location.

2. Navigate to **Start** → **All Apps** → **Hyper-V Manager**.

3. In the **Hyper-V Manager**, navigate to **Actions** → **Import virtual machine** and follow the instructions of the wizard. Review the table below for more information.

Step	Description
Locate Folder	Browse for the folder that contains extracted Netwrix Auditor virtual appliance.
Select Virtual Machine	Select **Netwrix Auditor**.
Choose Import Type	Choose the import type that best suits your needs.
Choose Network Type	Select a virtual switch.
Summary	Review your virtual machine settings. Click **Finish** to exit the wizard.

NOTE: If your Hyper-V server runs Windows Server 2012, instead of importing a virtual machine, select **New virtual machine**. Proceed with the wizard: set startup memory to 4096 MB, specify your network switch, and select **Use an existing virtual hard disk** option—NetwrixAuditor.vhdx disk (located in *NetwrixAuditor-hyperv\Netwrix Auditor\Virtual Hard Disks*) to this machine.

4. The newly created virtual machine named **Netwrix Auditor** will appear in the list of virtual machines. Right-click and select **Start**.

2.1.4. Configure Virtual Appliance

Follow the steps below to configure your virtual appliance with Netwrix Auditor.

1. Once you connect to the virtual appliance, you will find out that Windows Server 2012 R2 installation is almost complete. On the **Settings** page, specify a password for the built-in administrator account. Then re-enter your password. Click **Finish**.

2. Log in to the virtual machine.

3. The **Windows PowerShell** opens and automatically runs the script. Press any key to read the license agreement and then press `Y` to accept it. Then you will be prompted to configure the virtual machine. Press **Enter** to start.

Step	Description
Rename virtual machine	Specify a new name for the virtual machine (e.g., `NA-Server`).
	NOTE: The computer name must be properly formatted. It may contain letters (a-z, A-Z), numbers (0-9), and hyphens (-), but no spaces and periods (.). The name may not consist entirely of digits and may not be longer than 15 characters.
Configure network	• Select `Y` to use DHCP server to configure network settings automatically. • Select `N` to configure required parameters manually. In this case, you will be prompted to set up IP settings manually.
Join computer to the domain or workgroup	*To join to a domain* Select `Y`. Specify the fully qualified domain name to join (e.g., `corp.local`). Then, specify domain administrator name and password. NOTE: For your convenience, the account specified will be added to the local **Administrators** group and set as account for collecting data from the target systems. *To join to a workgroup* Select `N`. Specify the local administrator name and credentials. NOTE: For your convenience, the account specified will be set as account for collecting data from the target systems.
Add additional input	Select `Y` if you want to specify additional input languages unsing the

Step	Description
languages	**Language** window. Select N to proceed with English.
Configure SQL Server	The shell script automatically configures SQL Server instance. The **sysadmin** server role on SQL Server instance is granted automatically to the **BUILTIN\Administrators** group.

In the example below, review how the shell script configures the new VM:

4. When the script execution completes, you will be prompted to reboot the virtual machine for the changes to take effect.

5. After reboot, log in to the virtual machine using the domain administrator credentials (for appliances joined to domain) or local administrator credentials (for appliances joined to workgroup).

   For the first time, Netwrix Auditor client starts automatically. Later, you can always run it from the **Start** menu or launch it by double-clicking the Netwrix Auditor shortcut on the desktop. The product

will automatically start configuring self-monitoring—the first monitoring plan is configured to track User Activity on your server.

NOTE: Do not close the Netwrix Auditor Virtual Appliance Configuration window until the self-monitoring configuration completes. Otherwise, you will have to create a monitoring plan manually.

2.2. Cloud Deployment

Try playing around with Netwrix Auditor to see how it helps you enable complete visibility with enhanced cloud deployment options:

- **Amazon Marketplace**—Discover Netwrix Auditor if you have an active AWS account.

  NOTE: Consider that this section describes evaluation steps to investigate the Netwrix Auditor functionality and it does not contain detailed instructions on how to use and configure Amazon services and instances. Refer to AWS Documentation for more information.

- **Windows Amazon Marketplace**—Discover Netwrix Auditor if you have an active Microsoft account.

2.2.1. Configure AWS Instance

1. Log in to the **AWS Management Console** and navigate to **Amazon EC2** launch wizard.

2. Select Netwrix Auditor in the software list and launch the instance. Refer to Launching an AWS Marketplace Instance section for detailed instructions on how to use instances.

   For your convenience, you can rename instance, e.g. *"Netwrix Auditor"*.

3. The instance may take a few minutes or more to launch. Although your **Instance State** is *"running"*, it may be unavailable. You can check the image health in two ways:

   - Right-click the instance and select **Instance Settings → Get Instance Screenshot** and review image current state.

   - Right-click the instance and select **Instance Settings → Get System Log**. Empty log means that your image is still being prepared.

   Wait until the **System Log** contains the `Windows is Ready for Use` message and connect to the instance.

4. In the **Connect To Your Instance** dialog, select **Get Password** next to **Password**.

5. Select your Key Pair file and click **Decrypt Password**. See Amazon EC2 Key Pairs and Windows Instances for more information on Key Pairs.

6. Copy the password. Consider that this password will be used to connect to the instance where the product is going to be deployed. It will also function as a service password for Netwrix Auditor and SQL Server and Reporting Services. You can always reset it later upon Netwrix Auditor deployment

completion.

7. Select **Download Remote Desktop File** and launch the **Remote Desktop Connection** window by clicking the downloaded RDP file.

8. In the **Windows Security** dialog, provide the password you have copied on the step 6 and log on to the instance.

2.2.2. Configure Azure Marketplace VM Instance

1. Log in to the **Microsoft Azure Marketplace** and navigate to **Virtual machines**.

2. Select Netwrix Auditor image in the software list.

3. Select **Create VM** and complete the following fields:

Option	Description
Name	Specify the name for the new Virtual machine. For example, *"NetwrixAuditor"*.
VM disk type	Select disk type that meets your business needs
User name and password	Specify credentials to log on the new Virtual machine. This account will be granted the **Global Administrator** role in Netwrix Auditor.
Subscription	Select your Azure subscription type
Resource group	In the list of resource groups, assuming you have some applicable assets in your Azure subscription, you should see a list of resource groups. You can use one of your configured resource groups or create the new one.
Size	Browse for required sizes and VM features. Refer to Netwrix Auditor Installation and Configuration Guide for minimal hardware requirements to deploy Netwrix Auditor.
Settings	Configure the following virtual machine settings, if needed: • High availability • Network • Extensions • Auto-shutdown • Monitoring

Option	Description

Summary—Review your Netwrix Auditor image configuration.

4. Wait until deployment completes. The image may take up to 10 minutes to deploy.

5. Once the image has been deployed successfully, select **Go to resource** on the right pane.

6. Navigate to **Virtual machines** and make sure that your Netwrix Auditor image status is "*Running*".

7. Select **Connect**—The Remote Desktop File will be downloaded automatically.

8. In the **Windows Security** dialog, provide the Netwrix Auditor Global Administrator credentials you specified on the step 3 and log on to the instance.

2.2.3. Netwrix Auditor Deployment

Connect to the instance where Netwrix Auditor is going to be deployed. The **Windows PowerShell** opens and automatically runs the script.

1. In the **Netwrix Auditor Deployment configuration** wizard, review computer name and domain to which the computer is joined. Enter Y if you are all right with the default parameters and go to Step 3 to complete deployment.

2. If you want to rename the computer and join it to another domain or workgroup, follow the additional steps below:

    -   Enter N to open the **System Properties** dialog.

    -   Modify computer parameters at your convenience.

    -   Restart the computer.

    -   Re-establish RDP connection to the instance where Netwrix Auditor is being deployed.

        When completed, you will be taken to the step 1.

3. The shell script automatically configures SQL Server instance. The **sysadmin** server role on SQL Server instance is granted automatically to the **BUILTIN\Administrators** group.

For the first time, Netwrix Auditor client starts automatically. Later, you can always run it from the **Start** menu or launch it by double-clicking the **Netwrix Auditor** shortcut on the desktop.

For the first run, you need to specify the password to connect to Audit Database:

1. In Netwrix Auditor client, navigate to **Settings → Audit Database**.

2. Click **Modify** under **Default SQL Server Settings** and provide the password you have decrypted during AWS instance configuration.

2.3. What Is Next

Now you can evaluate Netwrix Auditor functionality. Review the table below for more information.

To...	Run...	Get more info
• See a list of audit settings • See a list of rights and permissions required for data collecting account	—	Netwrix Auditor Installation and Configuration Guide
• Create a monitoring plan • Review data collection status • Configure the Long-Term Archive and the Audit Database settings • Assign roles and delegate control	Netwrix Auditor client	Netwrix Auditor Administration Guide
• Browse data with interactive search • Review diagrams • Generate reports • Configure report subscriptions • Create alerts	Netwrix Auditor client	Netwrix Auditor Intelligence Guide

If any errors occur, please contact Netwrix technical support.