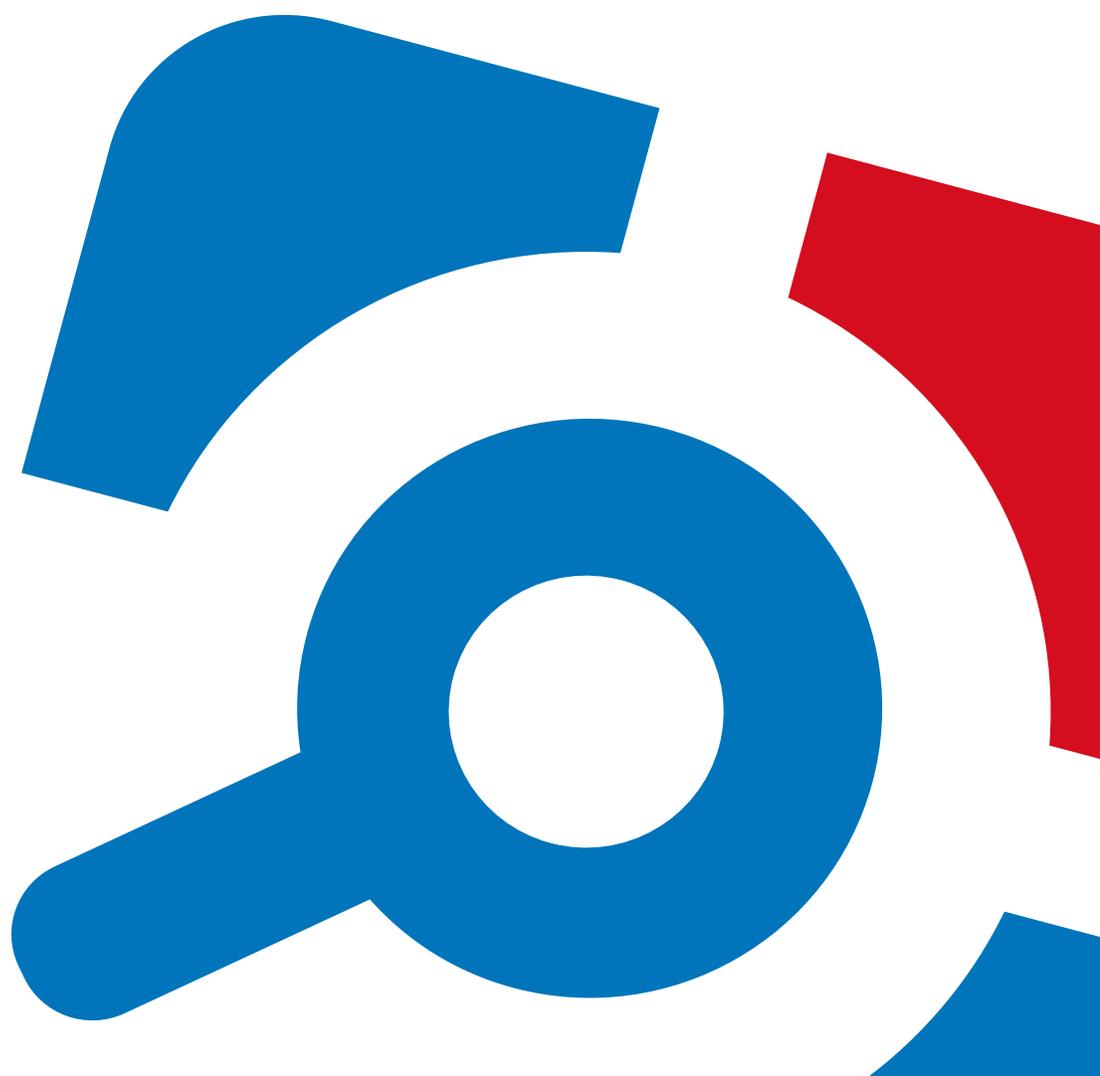# Netwrix Auditor

## Virtual Appliance and Cloud Deployment Guide

Version: 10
12/29/2021

**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. Virtual and Cloud Deployment

# 1.1. Overview

In addition to on-premises deployment, Netwrix Auditor offers the deployment options that can speed time-to-value by getting you up and running in less than 15 minutes. These are:

- **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. The image is also configured to use Microsoft Edge as a default web browser.

  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:

  - Available Configurations
  - 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, and configured to use Microsoft Edge as a default web browser.

  Review the following for additional information:

  - Cloud Deployment

**NOTE:** You can also add Netwrix Auditor Virtual Appliance to the Content Library of your VMware Cloud on AWS SDDC and then deploy this Virtual Appliance to the cloud-based ESXi host, following the steps described in this guide. In this deployment scenario, Netwrix Auditor will be able to work with other VMs running on that ESXi host.

# 1.2. 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

## 1.2.1. Available Configurations

The following virtual appliance configurations are available:

| Guest OS | SQL Server |
| --- | --- |
| Generalized Windows Server 2016<br><br>(180-day evaluation version) | Microsoft SQL Server 2016 Express Edition, with native Reporting Services installed |
| Generalized Windows Server 2019<br><br>(180-day evaluation version) | Microsoft SQL Server 2016 Express Edition, with native Reporting Services installed |

### 1.2.1.1. Considerations and Limitations

- Consider Microsoft limits for evaluation versions of Windows Server. You have 10 days to complete online activation, otherwise your Windows evaluation license expires, and Netwrix Auditor virtual appliance will shut down every hour. Provide a valid license key for Windows Server, or go to Microsoft Licensing Activation Center to register your license online. Refer to Microsoft article for more information: Evaluation Versions and Upgrade Options for Windows Server. Also, you can register you license by phone. See Microsoft Licensing Activation Centers worldwide telephone numbers for more information.

- Microsoft SQL Server Express Edition is only recommended for evaluation, PoC or small deployments. For production deployment planning in bigger environments, refer to requirements and recommendations listed in SQL Server and Databases section.

## 1.2.2. Requirements to Deploy Virtual Appliance

This section lists supported virtualization platforms and default hardware configuration required for the virtual machine where Netwrix Auditor virtual appliance will be deployed.

**NOTE:** The requirements below are sufficient for evaluation purposes only. Refer to Prerequisites and System Requirements for deploying Netwrix Auditor in production environments.

### 1.2.2.1. Supported Platforms

The table below lists supported virtualization platforms for the virtual appliance deployment:

| Virtual Infrastructure | Supported Version |
|---|---|
| VMware vSphere | • VMware server: ESXi 7.0, 6.7, 6.5, 6.0<br><br>• VMware workstation: 11 and 12<br><br>NOTE: You can also add Netwrix Auditor Virtual Appliance to the Content Library of your VMware Cloud on AWS SDDC and then deploy this Virtual Appliance to the cloud-based ESXi host, following the steps described in this guide. |
| Microsoft Hyper-V | • Microsoft Windows Server 2019<br><br>• Microsoft Windows Server 2016<br><br>• Microsoft Windows Server 2012 R2 |

## 1.2.2.2. Virtual Machine Hardware Requirements

When deploying Netwrix Auditor virtual appliance, a pre-configured virtual machine will be created from the template. Below is the default hardware configuration for the VM where you plan to deploy Netwrix Auditor virtual appliance:

| Parameter | Value |
|---|---|
| **Common** | |
| Processor | 4 cores |
| RAM | 16 GB |
| HDD | • Local Disk (C:) 100 GB<br><br>• Data (D:) 300 GB |
| **VMware only** | |
| Total Video Memory | 16 MB |
| Network adapter | vmxnet3 |
| Other | Check and upgrade VMware Tools during power cycle. |

# 1.2.3. Import Virtual Machine from Image to VMware

1. Connect to your vSphere infrastructure using **vSphere Web client**, right-click the object you need (datacenter, ESXi host, VM folder or resource pool) and select **Deploy OVF Template**.

   **NOTE:** If you are running VMware 6.0, connect to vSphere using the on-premises **vSphere client** and select **File → Deploy OVF Template**.

2. 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 (optional; default name is *"Netwrix Auditor"*).<br><br>**NOTE:** The name must be unique within the Inventory folder; it may contain up to 80 characters including spaces. |
| **Resource Pool** | Select a resource pool to deploy Netwrix Auditor virtual appliance. |
| **Storage** | Select the destination storage. |
| **Disk Format** | To optimize the disk space, it is recommended to select **Thin Provision**. |
| **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 complete the wizard. |

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

# 1.2.3.1. Deploy Netwrix Auditor Virtual Appliance to VMware Cloud on AWS

1. Import the **NetwrixAuditor.ova** file to a Content Library of VMware vSphere, as described in this VMware article: Import Items to a Content Library.

2. Start the **New Virtual Machine...** wizard.

3. On the **Select a creation type** step, select **Deploy from template**.

4. On the **Select a template** step, select **NetwrixAuditor** from your ContentLibrary.

5. Proceed with the wizard: select name and folder, resources and storage for the VM.

# 1.2.4. 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. |

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

# 1.2.5. Configure Virtual Appliance

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

1. For Windows Server, the EULA will be displayed in the **License terms** page; read and accept the agreement.

2. Next, specify a password for the built-in administrator account. Then re-enter your password. Click **Finish**.

3. Log in to the virtual machine.

4. The **Windows PowerShell** opens and automatically runs the script. Press any key to read the license agreement and then press Y to accept it.

5. 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`). <br><br> **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. |
| **Add additional input languages** | Select `Y` if you want to specify additional input languages. <br><br> Select `N` to proceed with English. |
| **Configure network** | <ul><li>Select `Y` to use DHCP server to configure network settings automatically.</li><li>Select `N` to configure required parameters manually. In this case, you will be prompted to set up IP settings manually.</li></ul> |
| **Join computer to the domain or workgroup** | *To join a domain* <br><br> Select `Y`. Specify the fully qualified domain name to join (e.g., `corp.local`). Then specify domain administrator name and password. <br><br> **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. <br><br> Domain Users group will be removed from the local **Users** group after the machine with the appliance joins the domain. <br><br> The script is starting to test your domain controller: by NETBIOS name first, then by DNS name and finally, using an IP address. If at least one of the tests is successful, the computer will be added to a domain. In case of failure, you will be prompted to do one of the following: <br><br> 1. Re-try to joint to the selected domain. In this case, the script uses the DNS name of your domain controller. <br><br>     **NOTE:** The name must be resolved. <br><br> 2. Continue with Workgroup. See the procedure below on how to join the computer to a workgroup. <br><br> 3. Cancel and Return to Main Menu. Select if you want to cancel the domain join and re-configure the machine. Press **Enter** |

| Step | Description |
|------|-------------|
| | and repeat menu section. You will return to <u>step 5</u>. |
| | *To join 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. |
| **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.

   **NOTE:** Do not close the Netwrix Auditor Virtual Appliance Configuration window until the product configuration completes.

# 1.3. 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.

**NOTE:** You can also add Netwrix Auditor Virtual Appliance to the Content Library of your VMware Cloud on AWS SDDC and then deploy this Virtual Appliance to the cloud-based ESXi host, following the steps described in this guide. In this deployment scenario, Netwrix Auditor will be able to work with other VMs running on that ESXi host.

# 1.3.1. 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.

# 1.3.2. 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.<br><br>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:<br><br>• High availability |

| Option | Description |
|---|---|
| | <ul><li>Network</li><li>Extensions</li><li>Auto-shutdown</li><li>Monitoring</li></ul> |

**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.

## 1.3.3. 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.

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

If any errors occur, please contact Netwrix technical support.