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.

© 2019 Netwrix Corporation.

All rights reserved.
# Table of Contents

1. Introduction ........................................................................................................... 5  
   1.1. Netwrix Auditor Features and Benefits ............................................................. 5  
2. Prerequisites and System Requirements ............................................................... 6  
   2.1. Supported Data Sources .................................................................................. 6  
   2.2. Requirements to Install Netwrix Auditor ......................................................... 6  
      2.2.1. Hardware Requirements ............................................................................. 6  
      2.2.2. Software Requirements ............................................................................. 7  
3. Review Components Checklist ............................................................................. 9  
   3.1. Configure Data Collecting Account .................................................................. 9  
4. Configure NetApp Filer for Monitoring ................................................................. 11  
   4.1. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring ........ 11  
      4.1.1. Prerequisites ............................................................................................. 11  
      4.1.2. Configure ONTAPI Web Access ................................................................. 12  
      4.1.3. Configure Firewall Policy .......................................................................... 13  
      4.1.4. Configure Event Categories and Log ......................................................... 14  
5. Install the Product ............................................................................................... 18  
6. Monitoring Plans .................................................................................................. 20  
   6.1. Create a New Plan ............................................................................................ 20  
      6.1.1. Settings for Data Collection ....................................................................... 20  
      6.1.2. Default SQL Server Instance .................................................................... 21  
      6.1.3. Database Settings ..................................................................................... 22  
      6.1.4. SMTP Server Settings ................................................................................ 24  
      6.1.5. Email Notification Recipients .................................................................... 24  
      6.1.6. Monitoring Plan Summary ......................................................................... 24  
   6.2. Add Items for Monitoring ................................................................................ 25  
      6.2.1. NetApp ...................................................................................................... 25  
7. Make Test Changes .............................................................................................. 27  
8. See How Netwrix Auditor Enables Complete Visibility ....................................... 28
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1. Review an Activity Summary</td>
<td>29</td>
</tr>
<tr>
<td>8.2. Review Overview Dashboard</td>
<td>30</td>
</tr>
<tr>
<td>8.3. Review the All Changes Report</td>
<td>31</td>
</tr>
<tr>
<td>8.4. Browse Data with Intelligence Search</td>
<td>31</td>
</tr>
<tr>
<td>9. Related Documentation</td>
<td>35</td>
</tr>
</tbody>
</table>
1. Introduction

This guide is intended for the first-time users of Netwrix Auditor for NetApp. 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 and configure Netwrix Auditor
- Create a monitoring plan to start auditing NetApp appliances
- Launch data collection
- See how Netwrix Auditor enables complete visibility

**NOTE:** This guide only covers the basic configuration and usage options for auditing NetApp appliances with Netwrix Auditor. For advanced installation scenarios and configuration options, as well as for information on various reporting possibilities and other product features, refer to Netwrix Online Help Center.

1.1. Netwrix Auditor Features and Benefits

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, Active Directory Federation Services, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, Nutanix Files, network devices, SharePoint, Oracle Database, SQL Server, VMware, Windows Server, and User Activity. Empowered with a RESTful API, 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

To learn how Netwrix Auditor can help your achieve your specific business objectives, refer to Netwrix Auditor Best Practices Guide.

Netwrix Auditor for NetApp detects and reports on all changes made to NetApp Filer appliances both in cluster- and 7-modes, including modifications of files, folders, shares and permissions, as well as failed and successful access attempts.
2. Prerequisites and System Requirements

This section lists the requirements for the systems that are going to be audited with Netwrix Auditor, and for the computer where the product is going to be installed.

To learn about Netwrix Auditor licenses, refer to the following Netwrix Knowledge Base article: Netwrix Auditor Licensing FAQs. To learn how to install a license, refer to Licenses.

To learn about ports and protocols required for product operation, refer to Protocols and Ports Required for Netwrix Auditor.

To learn about security roles and permissions required for product operation, refer to Configure Netwrix Auditor Service Accounts.

2.1. Supported Data Sources

The table below lists systems that can be monitored with Netwrix Auditor for NetApp:

<table>
<thead>
<tr>
<th>Data source</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp</td>
<td>• NetApp ONTAP 9.0 – 9.6 (CIFS configuration only)</td>
</tr>
<tr>
<td></td>
<td>• NetApp Clustered Data ONTAP 8.2.1 – 8.2.3, 8.3, 8.3.1, 8.3.2 (CIFS configuration only)</td>
</tr>
<tr>
<td></td>
<td>• NetApp Data ONTAP 8 in 7-mode (CIFS configuration only)</td>
</tr>
<tr>
<td></td>
<td>• NetApp Data ONTAP 7 (CIFS configuration only)</td>
</tr>
</tbody>
</table>

2.2. Requirements to Install Netwrix Auditor

This section provides the requirements for the computer where Netwrix Auditor is going to be installed. Refer to the following sections for detailed information:

- Hardware Requirements
- Software Requirements

2.2.1. Hardware Requirements

This section provides rough estimations of the resources required for Netwrix Auditor PoC or evaluation deployment. Consider that actual hardware requirements will depend on your monitored infrastructure, the number of users in your environment, and activities that occur in the infrastructure per day.
The metrics provided in this section are valid for clean installation on a server without any additional roles or third part applications installed on it. The use of virtual machine is recommended.

Below you can find rough estimations, calculated for evaluation of Netwrix Auditor for NetApp. Refer to [Netwrix Online Help Center](https://www.netwrix.com/support/online-help-center/) for complete information on the Netwrix Auditor hardware requirements.

You can deploy Netwrix Auditor on a virtual machine running Microsoft Windows guest OS on the corresponding virtualization platform, in particular:

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV

Note that Netwrix Auditor supports only Windows OS versions listed in the **Software Requirements** section.

<table>
<thead>
<tr>
<th>Hardware component</th>
<th>Starter, evaluation, or small environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>100 GB—System drive</td>
</tr>
<tr>
<td></td>
<td>100 GB—Data drive (Long-Term Archive and SQL Server)</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>Minimum 1280 x 1024</td>
</tr>
<tr>
<td></td>
<td>Recommended 1920 x 1080 or higher</td>
</tr>
</tbody>
</table>

### 2.2.2. Software Requirements

The table below lists the software requirements for the Netwrix Auditor installation:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server OS:</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2012</td>
</tr>
<tr>
<td>Windows Desktop OS (64-bit):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Windows 10</td>
</tr>
</tbody>
</table>
## 2. Prerequisites and System Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8.1</td>
<td></td>
</tr>
<tr>
<td>.NET Framework</td>
<td>.NET Framework 4.5 and above.</td>
</tr>
<tr>
<td>Installer</td>
<td>Windows Installer 3.1 and above</td>
</tr>
</tbody>
</table>
3. Review Components Checklist

To speed up the evaluation process, Netwrix recommends you to ensure that the following services and components are up and running prior to the Netwrix Auditor installation.

<table>
<thead>
<tr>
<th>Service or component</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and target systems or servers that work as your data sources</td>
<td>Test connectivity to your data source. Make sure you can access it by its NetBIOS and FQDN name from the computer where you intend to install Netwrix Auditor—use the nslookup command-line tool to look up domain names. Domain controllers must be accessible as well.</td>
</tr>
</tbody>
</table>
| SQL Server with Reporting Services (or Advanced Services) 2008 or higher | Supported SQL Server versions are listed [here](#). Consider maximum database size in different versions. Make your choice based on the size of the environment you are going to monitor, the number of users, and other factors. Remember that maximum database size in Express editions may be insufficient.  
**NOTE:** Although Netwrix Auditor provides a convenient way to download SQL Server 2014 Express edition right from the product, it is recommended to deploy SQL Server instance in advance.  
If installed separately, remember to test SQL Server connectivity. |
| Test account | Netwrix recommends you to create a special account with extensive privileges. This account should have sufficient permissions to:  
- Collect audit data. See [Configure Data Collecting Account](#) for more information.  
- Access data stored in the SQL Server instance:  
  - The account must be assigned the Database owner (db_owner) role and the dbcreator server role.  
  - The account must be assigned the Content Manager role on the SSRS Home folder.  
- Make test changes in your environment. |

3.1. Configure Data Collecting Account

This service account is used to collect audit data from the data source items; it is specified during the monitoring plan creation.
Netwrix recommends creating a special service account for that purpose. Depending on the data source your monitoring plan will process, the account must meet the corresponding requirements.

**NOTE:** The information in this section is outside the quick-start guide scope and is provided for reference only. For detailed instructions on how to configure the data collecting account to access your audited platform or application, see [Netwrix Auditor Online Help Center](#).

<table>
<thead>
<tr>
<th>Data source</th>
<th>Required rights and permissions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp</td>
<td><a href="#">For NetApp Auditing</a></td>
</tr>
</tbody>
</table>
4. Configure NetApp Filer for Monitoring

You can configure your file shares for monitoring in one of the following ways:

- Automatically when creating a monitoring plan. If so, your current audit settings will be periodically checked by Netwrix Auditor and adjusted if necessary.

  **NOTE:** To use this option for NetApp Clustered Data ONTAP 8 or ONTAP 9, make sure that audit configuration has been created (with `vserver audit create` command) for the target system; enabling audit configuration is optional. See [Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring](#) for more information.


4.1. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Monitoring

To configure Clustered Data ONTAP 8 and ONTAP 9 for monitoring, perform the following procedures:

- [Prerequisites](#)
- [Configure ONTAPI Web Access](#)
- [Configure Firewall Policy](#)
- [Configure Event Categories and Log](#)

4.1.1. Prerequisites

Perform the steps below before proceeding with audit configuration:

1. Configure CIFS server and make sure it functions properly.

   **NOTE:** NFS file shares are not supported.

2. Configure System Access Control List (SACL) on your file share.

3. Set the **Security Style** for **Volume** or **Qtree** where the audited file shares are located to the "$ntfs" or "$mixed$".

4. Configure audit manually. For 8.3, review the [Auditing NAS events on SVMs with FlexVol volumes](#)
section in *Clustered Data ONTAP® 8.3 File Access Management Guide for CIFS*.

**NOTE:** The current version of Netwrix Auditor does not support auditing of Infinite Volumes.

### 4.1.2. Configure ONTAPI Web Access

Netwrix Auditor uses ONTAPI to obtain the current CIFS audit configuration and force the audit data flush from the internal filer format to an MS Event Viewer compatible format. Netwrix Auditor supports both the SSL and non-SSL HTTP access, trying HTTPS first, and falling back to HTTP if it is unavailable.

1. Navigate to your cluster command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator and review your current web access settings. Make sure that External Web Services are allowed. For example:

   ```bash
   cluster1::> system services web show
   
   External Web Services: true
   Status: online
   HTTP Protocol Port: 80
   HTTPs Protocol Port: 443
   TLSv1 Enabled: true
   SSLv3 Enabled: true
   SSLv2 Enabled: false
   
   cluster1::>
   ```

3. Enable ONTAPI access on the SVM where CIFS server is set up and configured. The example command output shows correct web access settings where `vs1` is your SVM name.

   ```bash
   cluster1::> vserver services web show -vserver vs1
   
   Vserver  Type  Service Name  Description                  Enabled
   --------  ----  -----------  --------------------------    ----- 
   vs1      data  ontapi     Remote Administrative API         true
            Support  
   ```

4. Enable **HTTP/HTTPS** access. For example:

   ```bash
   cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled true
   ```

5. Enable only **SSL** access (HTTPS in Netwrix Auditor). For example:

   ```bash
   cluster1::> vserver services web modify -vserver vs1 -name ontapi -enabled true -ssl-only true
   ```

6. Make sure that the built-in `vsadmin` role or a custom role (e.g., `fsa_role`) assigned to your account specified for data collection can access ONTAPI. For example:

   ```bash
   cluster2::> vserver services web access show -vserver vs2
   
   Vserver  Type  Service Name  Role
   --------  ----  -----------  ---- 
   ```
4. Configure NetApp Filer for Monitoring

4.1.3. Configure Firewall Policy

Configure firewall to make file shares and Clustered Data ONTAP HTTP/HTTPS ports accessible from the computer where Netwrix Auditor Server is installed. Your firewall configuration depends on network settings and security policies in your organization. Below is an example of configuration:

1. Navigate to your cluster command prompt through the SSH/Telnet connection.

2. Log in as a cluster administrator and review your current firewall configuration. For example:

   ```
   cluster1::> system services firewall show
   Node     Enabled   Logging
   --------  ---------  -------
   cluster1-01  true     false
   ```

3. Create firewall policy or edit existing policy to allow HTTP/HTTPS (note that modifying a policy you may overwrite some settings). For example:

   **To...** | **Execute...**
   --- | ---
   Create a policy | `-policy poll -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24`
   | `cluster1::> system services firewall policy create -policy poll -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24`
   | `cluster1::> system services firewall policy create -policy poll -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`

   Modify existing policy | `-policy poll -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24`
   | `cluster1::> system services firewall policy modify -policy poll -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24`
   | `cluster1::> system services firewall policy modify -policy poll -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
### 4. Configure NetApp Filer for Monitoring

#### 4.1.4. Configure Event Categories and Log

Perform the following procedures to configure audit:

- To configure auditing state, event categories and log
- To configure logs retention period

**To configure auditing state, event categories and log**

Configure audit settings in the context of Cluster or Storage Virtual Machine. All examples in the procedure below apply to SVM, to execute commands in the context of Cluster, add `--vserver name`, where `name` is your server name.

1. Navigate to command prompt through the SSH/Telnet connection.

2. Log in as a cluster administrator and switch to the context of SVM from the cluster. For example to switch to the SVM called `vsl`:

```bash
cluster1::> vserver context --vserver vsl
```

After a switch, you will be in the context of SVM:

```
vsl::>
```

<table>
<thead>
<tr>
<th>To...</th>
<th>Execute...</th>
</tr>
</thead>
</table>
| Create a policy | `cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24`
| | `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`
| Modify existing policy | `cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -allow-list 192.168.1.0/24`
| | `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -allow-list 192.168.1.0/24`

where `pol1` is your Firewall policy name and `192.168.1.0/24` is your subnet where Netwrix Auditor Server resides.

4. Apply the firewall policy to a LIF.

```bash
cluster1::> network interface modify -vserver vs1 -lif vs1-cifs-lif1 -firewall-policy pol1
```

To verify the policy was applied correctly, execute the following:

```bash
cluster1::> network interface show -fields -firewall-policy
```
3. Create and enable audit. For more information on audit configuration, refer to NetApp documentation. For example:

<table>
<thead>
<tr>
<th>To...</th>
<th>Execute...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create audit</td>
<td>vsl::&gt; vserver audit create -destination &lt;path to the volume&gt;</td>
</tr>
<tr>
<td></td>
<td>In the example above, the vserver audit create -destination /audit command executed on the vsl SVM creates and enables audit on the volume /audit.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Netwrix Auditor accesses audit logs via file shares. Make sure the volume you specified is mounted on SVM and shared (e.g., audit$ is a share name and its path is /audit).</td>
</tr>
</tbody>
</table>

| Enable audit| vsl::> vserver audit enable                                                |

4. Review your audit settings. For example, on ONTAPI 8.3 the default audit is configured as follows:

vsl::> vserver audit show -instance

**Auditing State:** true

Log Destination Path: /audit

Categories of Events to Audit: **file-ops, cifs-logon-logoff**

Log Format: **evtx**

Log File Size Limit: 100MB

Log Rotation Schedule: Month:—

Log Rotation Schedule: Day of Week:—

Log Rotation Schedule: Day:—

Log Rotation Schedule: Hour:—

Log Rotation Schedule: Minute:—

Rotation Schedules:—

Log Files Rotation Limit: 0

For ONTAPI 9.0 or later the default audit is configured as follows:

vsl::> vserver audit show -instance

**Auditing State:** true

Log Destination Path: /audit

Categories of Events to Audit: **file-ops, file-share, audit-policy-change, cifs-logon-logoff**

Log Format: **evtx**

Log File Size Limit: 100MB

Log Rotation Schedule: Month:—

Log Rotation Schedule: Day of Week:—

Log Rotation Schedule: Day:—

Log Rotation Schedule: Hour:—
4. Configure NetApp Filer for Monitoring

Log Rotation Schedule: Minute: —  
Rotation Schedules: —  
Log Files Rotation Limit: 0

5. Check the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing State</td>
<td>true</td>
</tr>
<tr>
<td>Categories of Events to Audit</td>
<td>file-ops</td>
</tr>
</tbody>
</table>

**NOTE:** Only required if you use Clustered Data ONTAP 8.3, ONTAP 9.0, ONTAP 9.1 or later. You cannot select event categories if you use Clustered Data ONTAP 8.2.

For ONTAP 9.0 and later, also check the following options: file-ops, file-share, audit-policychange.

For ONTAP 8.3, just check file-ops.

Log Format: "XML" or "EVTX"

6. Modify the log file size limit—set to 300 MB. Execute:

```
vs1::> vserver audit modify -rotate-size 300MB
```

300MB is the recommended maximum log size proceeding from performance evaluations.

7. After configuration, double-check your settings.

```
vs1::> vserver audit show -instance
```

**Auditing State**: true  
**Log Destination Path**: /audit  
**Categories of Events to Audit**: file-ops, cifs-logon-logoff  
**Log Format**: evtx  
**Log File Size Limit**: 300MB  
**Log Rotation Schedule**: Month: —  
**Log Rotation Schedule**: Day of Week: —  
**Log Rotation Schedule**: Day: —  
**Log Rotation Schedule**: Hour: —  
**Log Rotation Schedule**: Minute: —  
**Rotation Schedules**: —  
**Log Files Rotation Limit**: 0

**NOTE:** For ONTAP 9.0 and later, also check the following settings: file-ops, file-share, audit-policychange.

For ONTAP 8.3, just check file-ops.

*To configure logs retention period*
1. On the computer where Netwrix Auditor Server resides, open Registry Editor: navigate to Start → Run and type "regedit".


3. In the right-pane, right-click and select New → DWORD (32-bit Value).

   **NOTE:** For the backup logs retention functionality to work properly, you need to specify the CleanAutoBackupLogs name for the newly created registry value.

4. Double-click CleanAutoBackupLogs. The Edit DWORD Value dialog will open.

5. This value defines the time period (in hours) after which security event logs archives will be automatically deleted. By default, it is set to "0" (decimal). Modify this value, if necessary, and click OK to save the changes.

6. **NOTE:** If the CleanAutoBackupLogs registry value is set to "0", you will have to remove the old logs manually, or you may run out of space on your hard drive.
5. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 9.9 from Netwrix website.

2. Unpack the installation package. The following window will be displayed on successful operation completion:

3. Follow the instructions of the setup wizard. When prompted, accept the license agreement.

4. On the Select Installation Type step, select Full installation.

5. On the Destination Folder step, specify the installation folder.

6. On the Netwrix Customer Experience Program step, you are invited to take part in the Netwrix Customer Experience Program. It is optional on your part to help Netwrix improve the quality, reliability, and performance of Netwrix products and services. If you accept, Netwrix collects statistical information on how the Licensee uses the product in accordance with applicable law. Select Skip if you do not want to participate in the program.

   **NOTE:** You can always opt-out of the Netwrix Customer Experience Program later. See Netwrix Online Helpcenter for instructions on how to cancel participation in the program.

7. Click Install.
After a successful installation, Netwrix Auditor shortcut will be added to the **Start** menu/screen and the product will start.
6. Monitoring Plans

To start auditing your environment and analyzing user behavior with Netwrix Auditor, create a monitoring plan. All your monitoring plans are listed in the Monitoring Plans section.

A monitoring plan defines your data sources and general data collection, notification, and storage settings. To start collecting data, choose a data source, such as NetApp, and add items to its scope. Item is a specific object you want to audit. All data sources and items in your plan share common settings so that you can supervise and manage several data collections as one.

On a high level, you should perform the following steps to start monitoring your environment:

1. Specify a data source and create a monitoring plan with a wizard. See Create a New Plan for more information.
2. Add items for monitoring. Netwrix Auditor does not collect data until you specify an item. See Add Items for Monitoring for more information.

6.1. Create a New Plan

On the main Netwrix Auditor page, click the All data sources tile in the Quick Start section.

Then follow the steps of the Monitoring Plan Wizard:

- Choose a data source for monitoring
- Specify an account for collecting data
- Specify default SQL Server instance and configure the Audit Database to store your data
- Configure notification settings
- Specify the recipients who will receive daily activity summaries
- Specify a plan name

6.1.1. Settings for Data Collection

At this step of the wizard, specify the account that Netwrix Auditor will use to access the data source, and general settings for data collection.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the account for collecting data</td>
<td>Provide a user name and a password for the account that Netwrix Auditor will use to collect data. By default, the user name is prepopulated with your account name. Make sure the account has sufficient permissions to collect data. For a full list</td>
</tr>
</tbody>
</table>
## 6.1.2. Default SQL Server Instance

To provide searching, alerting and reporting capabilities, Netwrix Auditor needs an SQL Server where audit data will be stored in the databases. To store data from the data sources included in the monitoring plan, the wizard creates an Audit Database for each plan. At this step, you should specify the default SQL Server instance that will host Netwrix Auditor databases. To read more, refer to [SQL Server and Audit Database](#).

**NOTE:** Alternatively, you can instruct Netwrix Auditor not to store data to the databases but only to the repository (Long-Term Archive) - in this scenario, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided.
NOTE: Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared.

Select one of the following options:

- **Install a new instance of Microsoft SQL Server Express automatically** — this option is available at the first run of the wizard. It allows you to deploy SQL Server 2016 SP2 Express with Advanced Services on the local machine. This SQL Server will be used as default host for Netwrix Auditor databases.

- **Use an existing SQL Server instance** — select this option to use an existing SQL Server instance.

  **NOTE:** Local SQL Server instance is detected automatically, and input fields are pre-populated with its settings.

Complete the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server instance</td>
<td>Specify the name of the SQL Server instance to store audit data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Select the authentication type you want to use to connect to the SQL Server instance:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Windows authentication</td>
</tr>
<tr>
<td></td>
<td>- SQL Server authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User name</th>
<th>Specify the account to be used to connect to the SQL Server instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>NOTE:</strong> This account must be granted the database owner (db_owner) role and the dbcreator server role.</td>
</tr>
</tbody>
</table>

| Password   | Enter a password. |

### 6.1.3. Database Settings

At this step, you need to specify a database where Netwrix Auditor will store data collected from the data sources included in this monitoring plan.

**NOTE:** It is strongly recommended to target each monitoring plan at a separate database.

Make sure the **Disable security intelligence and make data available only in activity summaries** checkbox is cleared and **Use default SQL Server settings** is checked.
### Audit Database

Specify the database to store your data and configure settings.

- **Disable security intelligence and make data available only in activity summaries**
- **Database:** `Netwrix_Auditor_Monitoring_Exchange`

**Use default SQL Server settings**

- **Specify custom connection parameters**
  - **Authentication:** `Windows authentication`
  - **User name:** `corp\administrator`
  - **Password:** `***************`

---

Configure the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disable security intelligence ...</strong></td>
<td>Only select this option if you do not want your data to be stored in the database. In this case, you will only be able to receive activity summaries. Reporting and alerting capabilities will not be provided. To store data to the database, leave this check box cleared.</td>
</tr>
</tbody>
</table>

| Database | Default database name is `Netwrix_Auditor_<monitoring_plan_name>`. It is recommended that you enter a meaningful name for the database here. It may include the data source type (e.g., `Exchange_Audit_Data` or `OracleSrv02_Audit_Data`), or so. If you decided to use the existing SQL Server instance instead of dedicated, you may want to use `Netwrix_Auditor` prefix to distinguish Netwrix Auditor databases |
6. Monitoring Plans

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use default SQL Server settings</td>
<td>Select this option if you want Netwrix Auditor to connect to the SQL Server instance using the default settings you specified <strong>Default SQL Server Instance</strong>.</td>
</tr>
<tr>
<td>Specify custom connection parameters</td>
<td>Select this option to use custom credentials when connecting to SQL Server. Specify authentication method and the account that Netwrix Auditor will use. Make sure this account has sufficient rights to connect to SQL Server and work with the databases. See <strong>Configure Audit Database Account</strong> for details.</td>
</tr>
</tbody>
</table>

Netwrix Auditor will connect to the default SQL Server instance and create a database with the specified name on it.

**NOTE:** Global settings that apply to all databases with audit data (including retention period and SSRS server used for reporting) are available on the **Audit Database** page of Netwrix Auditor settings. See **Audit Database** for details.

### 6.1.4. SMTP Server Settings

When you create the first monitoring plan, you are prompted to specify the email settings that will be used for activity and health summaries, reports and alerts delivery. For the monitoring plans that follow, Netwrix Auditor will automatically detect SMTP settings; however, for your first plan you should provide them manually. See **this section** for details.

### 6.1.5. Email Notification Recipients

Specify who will receive daily emails: **Activity Summary Email** on changes in the monitored infrastructure, and **Health Summary Email** on Netwrix Auditor operations and health.

Click **Add Recipient** and enter your email.

**NOTE:** It is recommended to click **Send Test Email**. The system will send a test message to the specified email address and inform you if any problems are detected.

### 6.1.6. Monitoring Plan Summary

At this step of the wizard, to provide a meaningful name and optional description for your monitoring plan.
To start collecting data, you should specify the objects (items) that belong to the target data source and should be processed according to the settings of this monitoring plan. For example, for Exchange data source the item will be your Exchange server, for Windows Server data source - computer, IP range or AD container, and so on. To add items right after finishing the monitoring plan wizard, select the **Add item now** checkbox. See [Add Items for Monitoring](#) for details.

### 6.2. Add Items for Monitoring

Once you completed monitoring plan wizard and specified data sources, add items for monitoring.

Each data source has a dedicated item type. Netwrix Auditor automatically suggests item types associated with your data source. Select the **NetApp** item.

#### 6.2.1. NetApp

Complete the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Specify NetApp file server</td>
<td>Provide a server name by entering its FQDN, NETBIOS or IPv4 address. You can click <strong>Browse</strong> to select a computer from the list of computers in your network.</td>
</tr>
<tr>
<td>File share UNC path to audit logs</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Detect automatically</strong>—If selected, a shared resource will be detected automatically.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use this path</strong>—UNC path to the file share located on a NetApp Filer with event log files (e.g., <code>\CORP\ETC\$\log\</code>).</td>
</tr>
<tr>
<td>Specify the account for collecting data</td>
<td>Select the account that will be used to collect data for this item.</td>
</tr>
<tr>
<td><strong>ONTAPI</strong></td>
<td></td>
</tr>
<tr>
<td>Specify protocol for accessing ONTAPI</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Detect automatically</strong>—If selected, a connection protocol will be detected automatically.</td>
</tr>
<tr>
<td></td>
<td>• <strong>HTTP</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>HTTPS</strong></td>
</tr>
</tbody>
</table>

Specify management interface | Select management interface to connect to ONTAPI. If you want to
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify account for connecting to ONTAPI</td>
<td>Select an account to connect to NetApp and collect data through ONTAPI. If you want to use a specific account (other than the one you specified on the General tab), select Custom and enter credentials. The credentials are case sensitive. Take into consideration that even if a custom account is specified, the account selected on the General tab must be a member of the Builtin\Administrators group and have sufficient permissions to access audit logs shared folder and audited shares.</td>
</tr>
<tr>
<td>Monitor the following shares</td>
<td>If you want to limit your auditing scope by several shares, click Add under the Specific file shares and select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.</td>
</tr>
</tbody>
</table>
7. Make Test Changes

Now that the product has collected a snapshot of the data source's current configuration state, you can make test changes to see how they will be reported by Netwrix Auditor.

**NOTE:** Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

For example, make the following test changes:

- Create a new file/folder in your file share
- Modify a file attribute in your file share
8. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to your environment, you can see how Netwrix Auditor brings security intelligence into your IT infrastructure and enables complete visibility. Take a closer look at the Intelligence section. It contains everything you need to enable complete visibility in your environment.

This chapter explains how to review your test changes with some of the Intelligence options and Activity Summary. Review the following for additional information:

- Review an Activity Summary
- Review Overview Dashboard
- Review the All Changes Report
- Browse Data with Intelligence Search

In order not to wait for a scheduled Activity Summary generation, force data collection and email delivery.

To launch data collection manually

1. Navigate to Monitoring Plans and select your plan in the list.
2. Click Edit.
3. In the your monitoring plan settings, click Update in the right pane.
4. Check your mailbox for an email notification and make sure that the data collection has completed successfully.
8.1. Review an Activity Summary

Activity Summary email is generated automatically by Netwrix Auditor and lists all changes that occurred since the last Activity Summary delivery. By default, an Activity Summary is generated daily at 3:00 AM and delivered to the specified recipients. You can also launch data collection and Activity Summary generation manually.

After the data collection has completed, check your mailbox for an Activity Summary and see how your test changes are reported:

The example Activity Summary provides the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Shows the type of action that was performed on the object.</td>
</tr>
<tr>
<td>Object Type</td>
<td>Shows the type of the object.</td>
</tr>
<tr>
<td>What</td>
<td>Shows the name of the changed object or its path.</td>
</tr>
<tr>
<td>Item</td>
<td>Shows the item associated with the selected monitoring plan.</td>
</tr>
<tr>
<td>Where</td>
<td>Shows the name of the server where the change occurred.</td>
</tr>
<tr>
<td>Who</td>
<td>Shows the name of the account under which the change was made.</td>
</tr>
<tr>
<td>When</td>
<td>Shows the exact time when the change occurred.</td>
</tr>
<tr>
<td>Workstation</td>
<td>Shows the of the computer where the user was logged on when the change was</td>
</tr>
</tbody>
</table>
8. See How Netwrix Auditor Enables Complete Visibility

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>made.</td>
<td></td>
</tr>
</tbody>
</table>

Details Shows the before and after values of the modified object, object attributes, etc.

8.2. Review Overview Dashboard

Overview diagram provides a high-level overview of activity trends by date, user, server, object type or data source in your IT infrastructure. The Overview diagram aggregates data on all monitoring plans and all data sources, while system-specific diagrams provide quick access to important statistics within one data source.

After collecting initial data, making test changes to your environment and running data collection again, you can get at-a-glance statistics for changes with the File Servers Overview.

To see how your changes are reported with File Servers Overview

1. On the main Netwrix Auditor page, navigate to the Intelligence section and click the Reports tile.
2. Expand the Predefined → File Servers → File Servers Activity reports.
3. Select the File Servers Overview report and click View.
4. Review your changes.
5. Click on any chart to jump to a table report with the corresponding grouping and filtering of data.
8.3. Review the All Changes Report

The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire audited IT infrastructure or individual data sources.

Change and activity reports can be found under the Reports → Predefined → your data source type and provide a narrower insight into what is going on in the audited infrastructure and help you stay compliant with various standards and regulations (FISMA, HIPAA, PCI, SOX, etc.).

After collecting initial data, making test changes to your environment and running data collection again, you can take advantage of the reports functionality.

To see how your changes are listed in the report

1. On the main Netwrix Auditor page, navigate to Reports → Predefined → your data source.
2. Select the All File Server Activity report.
3. Click View to open the report.

8.4. Browse Data with Intelligence Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient interactive search interface enables you to investigate incidents and browse data collected across the entire IT infrastructure. When running a search, you are not limited to a certain data source, change type, or object name. You can create flexible searches that provide you with precise results on who changed what, and when and where each change was made.

After collecting initial data, making test changes to your environment and running data collection again, you can review changes in details with Intelligence search.
To browse your audit data and see your test changes

1. On the main Netwrix Auditor page, navigate to **Intelligence → Search**.

2. Add search filters to your search by clicking on a corresponding icon and providing a value. By default, all entries that contain this filter value are shown. For an exact match, use quotation marks.

   Filters are used to narrow your search results. To create a unique set of filters, you can:
   
   - Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., **Who: Administrator AND Action: Added**).
   - Specify several values in the same filter to search for any of them (e.g., **Action: Modified OR Action: Removed**). To do this, select a filter again and specify a new value.

   **NOTE:** Refer to [Netwrix Online Helpcenter](#) for detailed instructions on how to apply filters and change match types

3. Click **Search**.

4. Now, you can narrow your search and modify it right from the search results pane. Click any entry that contains excess data, select **Exclude from search** in the Details section and specify a filter, e.g., **Action: Added** to leave information on modifications only.

   Your **Search** field will be updated, the filter will be added. Make sure to click **Search** again to update your search results.

5. Having reviewed your search results, navigate to **Tools**.
   
   - Click **Save as report** to save the selected set of filters. This search will be added to the **Custom** section inside **Reports**, so that you will be able to access it instantly. Refer to [Custom Search-Based Reports](#) for detailed instructions on how to create saved searches.
   
   - Click **Create alert** to get instant email or SMS notifications on suspicious activity that matches your current search criteria. You only need to specify a name for a new alert, add recipient and assign a risk score. The selected set of search criteria will be associated with the new alert automatically. Refer to [Alerts](#) for detailed instructions on how to create and configure alerts.

Try making more similar test changes to provoke an alert. For example:
Once you have received the alert, click the **Behavior Anomalies** tile on the main Netwrix Auditor page to see how the product identifies potentially harmful users and displays their risk scores. Drill-down to user profile to review anomalies and mitigate risks. Refer to [Netwrix Online Helpcenter](#) for more information on behavior anomalies and risk scores.
8. See How Netwrix Auditor Enables Complete Visibility
# 9. Related Documentation

The table below lists all documents available to support Netwrix Auditor for NetApp:

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netwrix Auditor Online Help Center</td>
<td>Gathers information about Netwrix Auditor from multiple sources and stores it in one place, so you can easily search and access any data you need for your business. Read on for details about the product configuration and administration, its security intelligence features, such as interactive search and alerts, and Integration API capabilities.</td>
</tr>
<tr>
<td>Netwrix Auditor Installation and Configuration Guide</td>
<td>Provides detailed instructions on how to install Netwrix Auditor, and explains how to configure your environment for auditing.</td>
</tr>
<tr>
<td>Netwrix Auditor Administration Guide</td>
<td>Provides step-by-step instructions on how to configure and use the product.</td>
</tr>
<tr>
<td>Netwrix Auditor Intelligence Guide</td>
<td>Provides detailed instructions on how to enable complete visibility with Netwrix Auditor interactive search, report, and alert functionality.</td>
</tr>
<tr>
<td>Netwrix Auditor Integration API Guide</td>
<td>Provides step-by-step instructions on how to leverage Netwrix Auditor audit data with on-premises and cloud auditing solutions using RESTful API.</td>
</tr>
<tr>
<td>Netwrix Auditor Release Notes</td>
<td>Lists the known issues that customers may experience with Netwrix Auditor 9.9, and suggests workarounds for these issues.</td>
</tr>
</tbody>
</table>