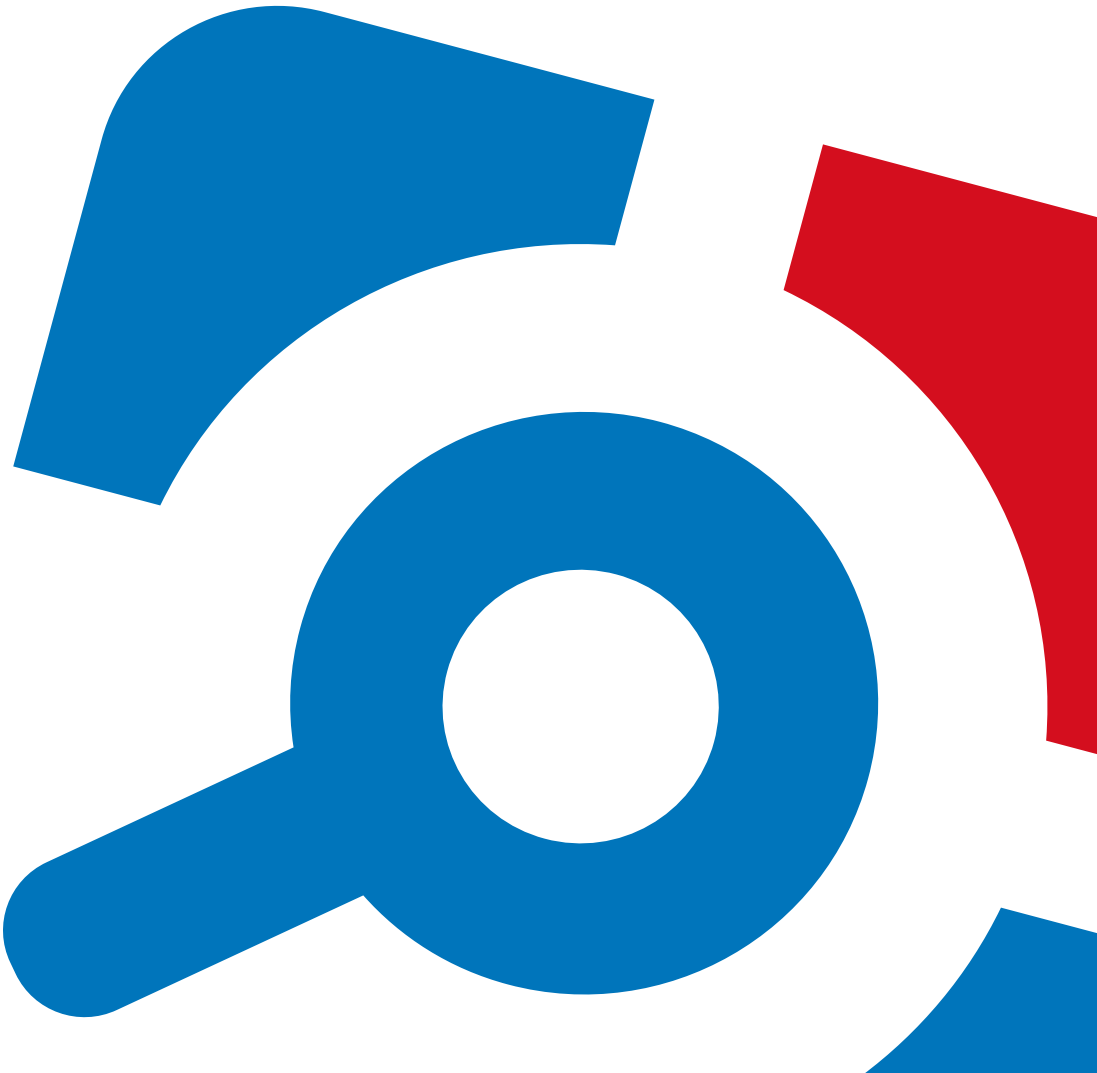
netwrix

Netwrix Auditor for NetApp

Quick-Start Guide

Version: 8.5
11/17/2016



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. 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 Managed Object 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 Auditor Installation and Configuration Guide
- Netwrix Auditor Administrator's Guide
- Netwrix Auditor User Guide

1.1. Netwrix Auditor Overview

Netwrix Auditor is a visibility and governance platform that enables control over changes, configurations and access in hybrid cloud IT environments to protect sensitive 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, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, and Windows Server. Empowered with a RESTful API and user activity video recording, 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

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. Netwrix Auditor 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.

2.1. Supported Audited Systems

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

Audited System	Supported Versions
NetApp	• NetApp Data ONTAP 7 (CIFS configuration only) • NetApp Data ONTAP 8 in 7-mode (CIFS configuration only) • NetApp Clustered Data ONTAP 8.2.1 - 8.2.3, 8.3, 8.3.1, 8.3.2 (CIFS configuration only) • NetApp ONTAP 9.0 (CIFS configuration only)

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

Before installing Netwrix Auditor, make sure that your hardware meets the following requirements:

Hardware Component	Minimum	Recommended
Processor	Intel or AMD 32 bit, 2 GHz	Intel Core 2 Duo 2x 64 bit, 3 GHz Preferably a virtual machine

Hardware Component	Minimum	Recommended
RAM	2 GB	8 GB Required size highly depends on the number of changes per day and may be up to 32 GB (approximately 3 million changes per day).
Disk space	• 500 MB physical disk space for the product installation • 30 GB for the file-based Long-Term Archive • 500 MB for the SQL Server-based Audit Database where audit data is going to be stored **NOTE:** These are rough estimations, calculated for evaluation of Netwrix Auditor for NetApp. Refer to Netwrix Auditor Installation and Configuration Guide for complete information on the Netwrix Auditor disk space requirements.	
Screen resolution	1280 x 1024	1920 x 1080 and higher

2.2.2. Software Requirements

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

Component	Requirements
Operating system	• Windows Desktop OS (64-bit): Windows 7 SP1, Windows 8.1 • Windows Server OS (64-bit): Windows Server 2008 R2 SP1, Windows Server 2012/2012 R2
Framework	• .Net Framework 3.5 SP1
Installer	• Windows Installer 3.1 and above

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.

Service or component	Recommendations
Network and audited system	Test connectivity to your audited system. Make sure you can access it by its NetBIOS and DNS names 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.
SQL Server 2014 with SSRS (optional step)	Although Netwrix Auditor provides a convenient interface for downloading SQL Server 2014 Express right from Netwrix Auditor Administrator Console, it is recommended to deploy SQL Server instance in advance. Test your SQL Server connectivity. **NOTE:** Netwrix Auditor provides an option to verify SSRS settings right in the Netwrix Auditor Administrator Console.

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 Processing Account Rights and Permissions 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 Processing Account Rights and Permissions

The Data Processing Account is used to collect audit data from the target systems. To ensure successful data collection, the Data Processing Account must comply with the following requirements depending on the audited system.

NOTE: The information in this section is outside the quick-start guide scope and is provided for reference only. See Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to configure your Data Processing Account.

Audited system	Rights and permissions

NetApp Filer	***On the target server:***
	• A member of **Builtin\Administrators** group
	• The **Read** permissions (resultant set) on the audited shared folders
	• The **Read** permissions (resultant set) on the audit logs folder and its contents and **Delete** permissions (resultant set) on the contents of this folder.
	• To connect to **NetApp Data ONTAP 7** or **Data ONTAP 8 in 7-mode**, an account must have the following capabilities:
	  • login-http-admin
	  • api-vfiler-list-info
	  • api-volume-get-root-name
	  • api-system-cli
	  • api-options-get
	  • cli-cifs
	• To connect to **NetApp Clustered Data ONTAP 8** or **ONTAP 9**, an account must be assigned a custom role (e.g., fsa_role) on SVM that has the following capabilities with access query levels:
	  • version readonly
	  • volume readonly
	  • vserver audit readonly
	  • vserver audit rotate-log all
	  • vserver cifs readonly
	NOTE: You can also assign the builtin **vsadmin** role.
	If you want to authenticate with AD user account, you must enable it to access SVM through ONTAPI. The credentials are case sensitive.

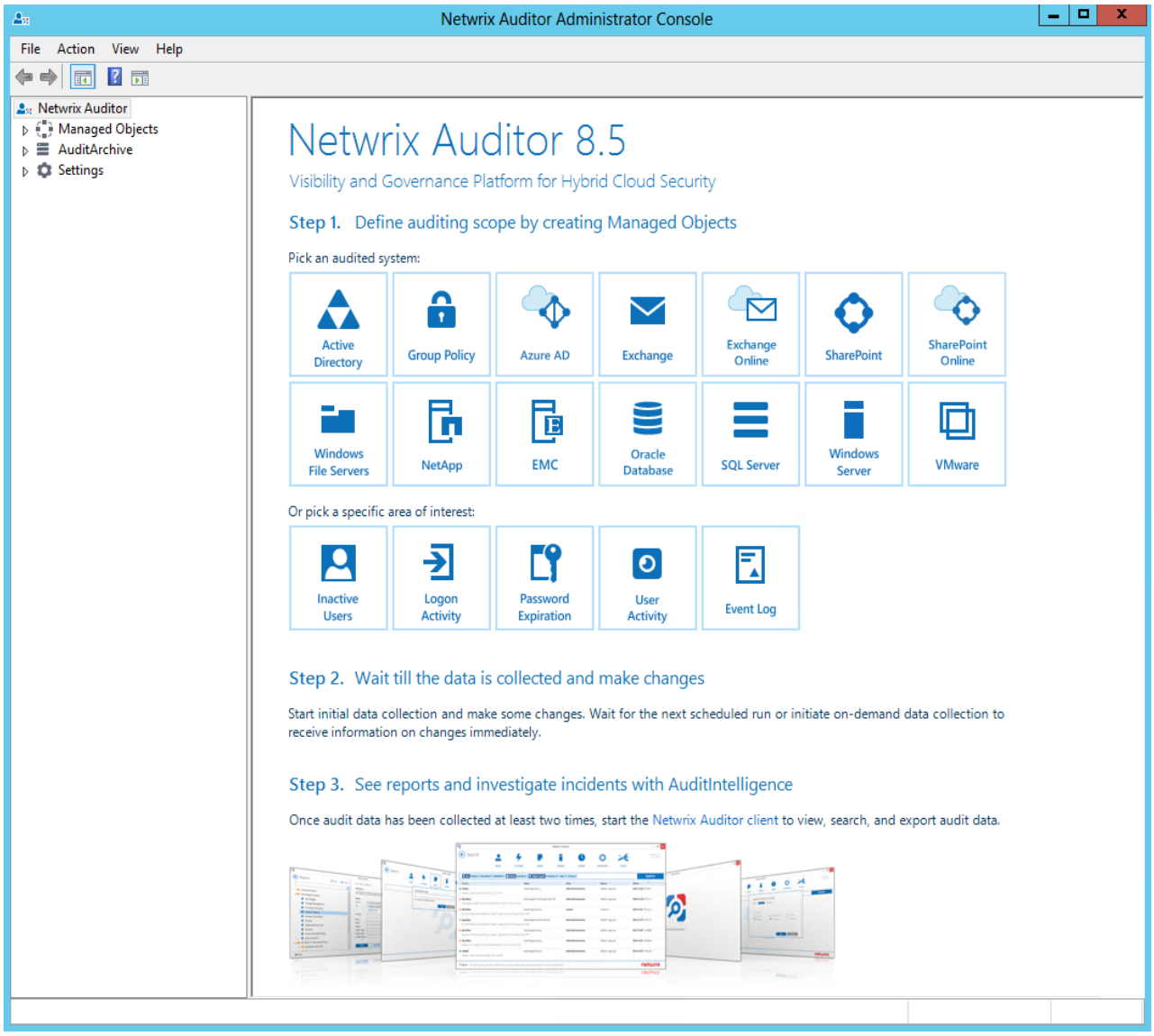
4. Install the Product

To install Netwrix Auditor

1. Download Netwrix Auditor 8.5 on 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. Click **Install**.

After a successful installation, Netwrix Auditor shortcuts will be added to the **Start** menu/screen and Netwrix Auditor Administrator Console will open.


Netwrix Auditor Administrator Console
File
Action
View
Help
Netwrix Auditor
Managed Objects
AuditArchive
Settings
Netwrix Auditor 8.5
Visibility and Governance Platform for Hybrid Cloud Security
Step 1. Define auditing scope by creating Managed Objects
Pick an audited system:
Active Directory
Group Policy
Azure AD
Exchange
Exchange Online
SharePoint
SharePoint Online
Windows File Servers
NetApp
EMC
Oracle Database
SQL Server
Windows Server
VMware
Or pick a specific area of interest:
Inactive Users
Logon Activity
Password Expiration
User Activity
Event Log
Step 2. Wait till the data is collected and make changes
Start initial data collection and make some changes. Wait for the next scheduled run or initiate on-demand data collection to receive information on changes immediately.
Step 3. See reports and investigate incidents with AuditIntelligence
Once audit data has been collected at least two times, start the Netwrix Auditor client to view, search, and export audit data.

5. Configure NetApp Filer for Auditing

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

- Automatically when creating a Managed Object

  NOTE: For NetApp Data ONTAP 7 and 8 in 7-mode, configure audit automatically. For NetApp Clustered Data ONTAP 8 or ONTAP 9 only file share audit settings can be configured automatically. See Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Auditing for more information.

- Manually. See Netwrix Auditor Installation and Configuration Guide for more information.

5.1. Configure NetApp Clustered Data ONTAP 8 and ONTAP 9 for Auditing

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

- Prerequisites
- Configure ONTAPI Web Access
- Configure Firewall Policy
- Configure Event Categories and Log

5.1.1. 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.

5.1.2. 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:

```
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
```

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.

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

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

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

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

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

6. Make sure that the builtin **vsadmin** role or a custom role (e.g., fsa_role) assigned to your Data Processing Account can access ONTAPI. For example:

```
cluster2::> vserver services web access show -vserver vs2
Vserver           Type      Service Name    Role
--------------    -------   ------------    ---------------
vs2               data      ontapi          fsa_role
vs2               data      ontapi          vsadmin
vs2               data      ontapi          vsadmin-protocol
vs2               data      ontapi          vsadmin-readonly
```

```
cluster2::> vserver services web access show -vserver vs2
vs2                data      ontapi          vsadmin-volume
5 entries were displayed.
```

5.1.3. Configure Firewall Policy

Configure firewall to make file shares and Clustered Data ONTAP HTTP/HTTPS ports accessible from the computer where Netwrix Auditor Administrator Console 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...
	NetApp Clustered Data ONTAP 8.2
Create a policy	`cluster1::> system services firewall policy create -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy create -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
Modify existing policy	`cluster1::> system services firewall policy modify -policy pol1 -service http -vserver vs1 -action allow -ip-list 192.168.1.0/24` `cluster1::> system services firewall policy modify -policy pol1 -service https -vserver vs1 -action allow -ip-list 192.168.1.0/24`
	NetApp Clustered Data ONTAP 8.3 and ONTAP 9
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`

To...	Execute...
	`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 Administrator Console resides.

5.1.4. 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

1. Configure audit settings in the context of Cluster or Storage Virtual Machine. Navigate to command prompt through the **SSH/Telnet** connection.
2. Log in as a cluster administrator. Create and enable audit. For more information on audit configuration, refer to NetApp documentation.

To...	Execute...
Create audit	`vs1::> vserver audit create -destination <path>` where `<path>` is a volume, e.g., `/audit`. **NOTE:** 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`).
Enable audit	`vs1::> vserver audit enable`

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

```
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: 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
```

4. Check the following options:

Option	Setting
`Auditing State`	`true`
`Categories of Events to Audit`	`file-ops` **NOTE:** Only required if you use ONTAP 8.3 or 9. You cannot select event categories if you use Clustered Data ONTAP 8.2.
`Log Format`	*"XML"* or *"EVTX"*

5. 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.

6. 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
```

To configure logs retention period

1. On the computer where Netwrix Auditor Administrator Console is installed, open **Registry Editor**: navigate to **Start** → **Run** and type *"regedit"*.
2. Navigate to **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **Wow6432Node** → **Netwrix Auditor** → **File Server Change Reporter**.
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.

6. Create Managed Object to Audit File Servers

To start auditing your IT Infrastructure with Netwrix Auditor, you must create a Managed Object. A Managed Object is a container within Netwrix Auditor that stores information on the auditing scope, the Data Processing Account used for data collection, Audit Database settings, etc.

To create a Managed Object to audit NetApp appliances

1. On the main Netwrix Auditor Administrator Console page, click the **NetApp** tile to launch the **New Managed Object** wizard.
2. On the **Select Managed Object Type** step, select **Computer Collection** as a Managed Object type.
3. On the **Specify Default Data Processing Account** step, click **Specify Account**.

   Enter the default Data Processing Account that will be used by Netwrix Auditor for data collection. For a full list of the rights and permissions required for the Data Processing Account, and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.
4. On the **Specify Email Settings** step, specify the email settings that will be used for Change Summaries, reports and real-time alerts delivery. Netwrix Auditor automatically detects SMTP settings or you can provide them manually. Complete the following fields:

Option	Description
SMTP server	Enter your SMTP server name. It can be your company's Exchange server or any public mail server (e.g., Gmail, Yahoo).
Port	Specify your SMTP server port number.
Sender address	Enter the address that will appear in the **From** field. **NOTE:** It is recommended to click **Verify**. The system will send a test message to the specified email address and inform you if any problems are detected.
SMTP Authentication	Select this checkbox if your mail server requires the SMTP authentication.
User name	Enter a user name for the SMTP authentication.

Option	Description
Password	Enter a password for the SMTP authentication.
Confirm password	Confirm the password.
Use Secure Sockets Layer encrypted connection (SSL)	Select this checkbox if your SMTP server requires SSL to be enabled.
Implicit SSL connection mode	Select this checkbox if the implicit SSL mode is used, which means that an SSL connection is established before any meaningful data is sent.

5. On the **Specify Computer Collection Name** step, enter the computer collection name.
6. On the **Audit Database Settings** step, make sure that the **Make audit data available via summary emails only** checkbox is cleared. By default, the Audit Database is created automatically and is used to store collected audit data.

   Select one of the following:

   - **Automatically install and configure a new instance of SQL Server Express Edition** to automatically install and configure SQL Server 2014 Express with Advanced Services.
   - **Use an existing SQL Server instance with SQL Server Reporting Services** to use an already installed SQL Server instance. Netwrix Auditor detects local SQL Server instance automatically and pre-populates the fields.

   Complete the following fields:

Option	Description
	SQL Server Settings
SQL Server instance	Specify the name of the SQL Server instance to store audit data.
Authentication	Select the authentication type you want to use to connect to the SQL Server instance: • Windows authentication • SQL Server authentication
User name	Specify the account to be used to connect to the SQL Server instance. **NOTE:** This account must be granted the **database owner (db_**

Option	Description
	owner) role and the **dbcreator** server role. See Netwrix Auditor Installation and Configuration Guide for more information.
Password	Enter a password.
	SQL Server Reporting Services Settings
Report Server URL	Specify the Report Server URL. Make sure that the resource is reachable.
Report Manager URL	Specify the Report Manager URL. Make sure that the resource is reachable.
User name	Specify the account to be used to connect to SSRS.
Password	Enter a password.

7. On the **State-in-Time Reports** step, you can enable or disable **State-in-Time Reports**. This feature allows generating reports on your system configuration state at a specific moment of time in addition to change reports. If enabled, snapshots will be created daily and written to the Audit Database. This option is unavailable if the **Audit Database** settings are not configured.
8. On the **Add Items to Computer Collection** step, click **Add** to select items that you want to audit. You can add several items to collection. In the **Computer Collection New Item** dialog that opens, select the item type:
   - **NetApp Filer**—Complete the following:
     1. On the **Specify Items** step, provide a server name by entering its FQDN, NETBIOS or IP address. You can click **Browse** to select a computer from the list of computers in your network. Select **Only these** and click **Add** to select shared folders. Otherwise, all file shares (except hidden) hosted on this server will be audited.
     2. On the **Configure NetApp Filer Auditing** step, complete the following fields:

Option	Description
Use protocol	Select one of the following: • **Automatically detected**—If selected, a connection protocol will be detected automatically. • **HTTP**

Option	Description
	• **HTTPS** **NOTE:** Refer to Netwrix Auditor Installation and Configuration Guide for detailed instructions on how to enable HTTP or HTTPS admin access.
Specify account	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 as the Data Processing Account), select **Custom** and enter credentials. The credentials are case sensitive. **NOTE:** See Netwrix Auditor Installation and Configuration Guide for more information on required rights and permissions. Take into consideration that even if a custom account is specified, the Data Processing Account selected on the **Specify Computer Collection Name** step must be a member of the **Builtin\Administrators** group and have sufficient permissions to access audit logs shared folder and audited shares.
Provide a File Share UNC path to audit logs	Select one of the following: • **Automatically detected**—If selected, a shared resource will be detected automatically. • **UNC path**—Path to the file share located on a NetApp Filer with event log files (e.g., *CORP**ETC$**log*\).

9. On the **Configure Audit in Target Environment** step, select **Automatically for the selected audited systems** if you want to audit file shares on NetApp Data ONTAP 7 and 8 in 7-mode. For NetApp Data ONTAP 8 in C-mode, only audit settings for file shares can be configured automatically, other settings must be applied manually. Your current audit settings will be periodically checked and adjusted if necessary.

   NOTE: For a full list of audit settings required for Netwrix Auditor to collect comprehensive audit data and instructions on how to configure them, refer to Netwrix Auditor Installation and Configuration Guide.

10. On the **Configure File Servers Change Summary Delivery Settings** step, enter your email.
11. On the **Configure File Servers Auditing Scope** step, select checkboxes next to successful and failed

changes.

Option		Description
Audit File Servers changes	Successful	Use this option to track changes to your data. Helps find out who made changes to your files, including their creation and deletion.
	Failed	Use this option to detect suspicious activity on your file server. Helps identify potential intruders who tried to modify or delete files, etc., but failed to do it.
Audit File Servers read access	Successful	Use this option to supervise access to files containing confidential data intended for privileged users. Helps identify who accessed important files besides your trusted users. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.
	Failed	Use this option to track suspicious activity. Helps find out who was trying to access your private data without proper justification. **NOTE:** Enabling this option on public shares will result in high number of events generated on your file server and the amount of data written to the AuditArchive.

NOTE: Actions reported by Netwrix Auditor vary depending on the file server type and the audited object (file, folder, or share).

12. On the last step, review your Managed Object settings and make sure **Run data collection now** is enabled. Click **Finish** to exit the wizard. The newly created Managed Object will appear under the **Managed Objects** node.

    When a new Managed Object is created, Netwrix Auditor starts collecting data from the audited IT infrastructure. The first data collection runs automatically and gathers information on the audited system's current configuration state. Netwrix Auditor uses this information as a benchmark to collect data on changes. After the first data collection has finished, an email notification is sent to your email stating that the analysis has completed.

7. Make Test Changes

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

For example, make the following test changes:

- Create a new file/folder in your file share
- Modify a file attribute in your file share

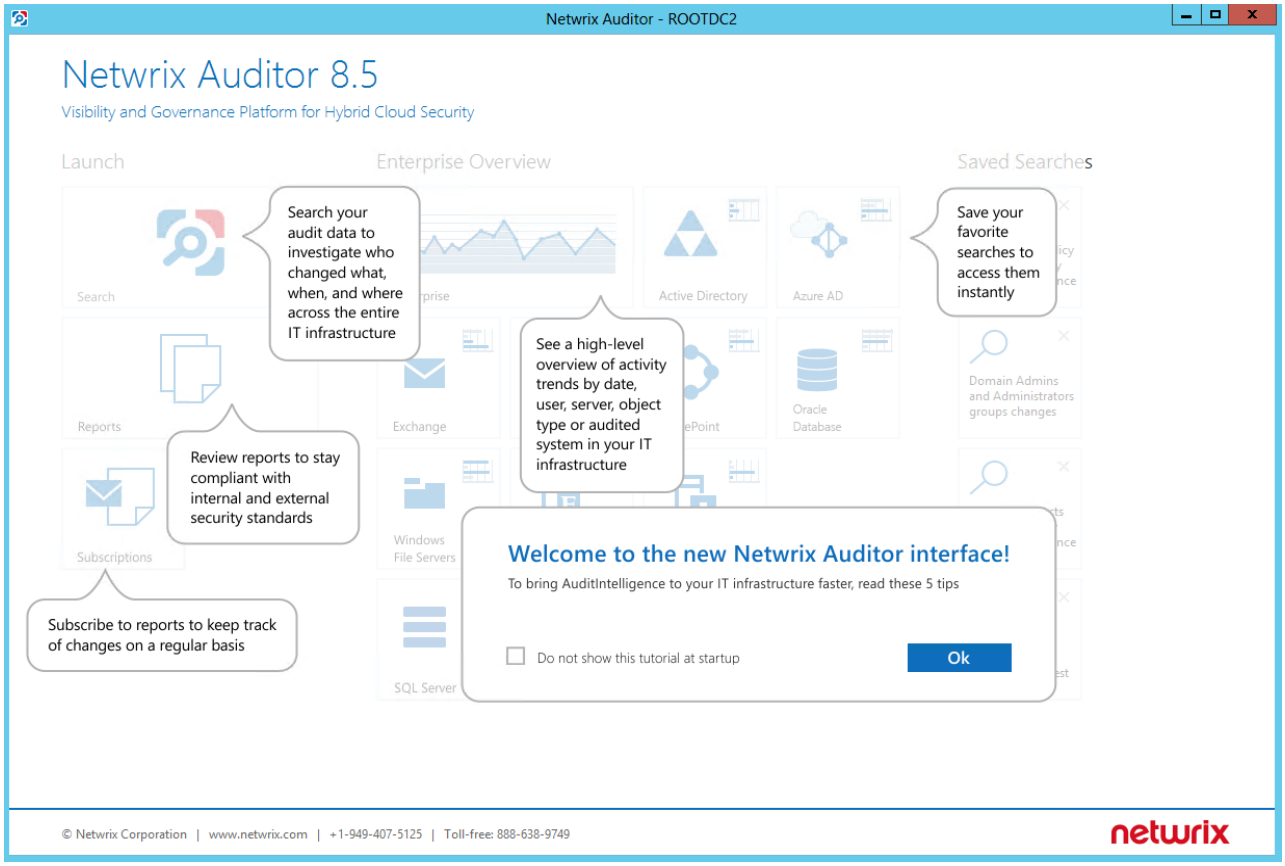
NOTE: Before making any test changes to your environment, ensure that you have the sufficient rights, and that the changes conform to your security policy.

8. See How Netwrix Auditor Enables Complete Visibility

After you have made test changes to the audited environment, you can see how Netwrix Auditor brings AuditIntelligence into your IT infrastructure and enables its complete visibility. This section explains how to review your test changes in the Netwrix Auditor client and Change Summary.

To launch the Netwrix Auditor client

- Navigate to **Start** → **Netwrix Auditor**.



Review the following for additional information:

- Review a Change Summary
- Browse Data with AuditIntelligence Search
- Review File Servers Overview
- Review the All File Servers Activity Report

In order not to wait for a scheduled data collection and a Change Summary generation, launch data collection manually.

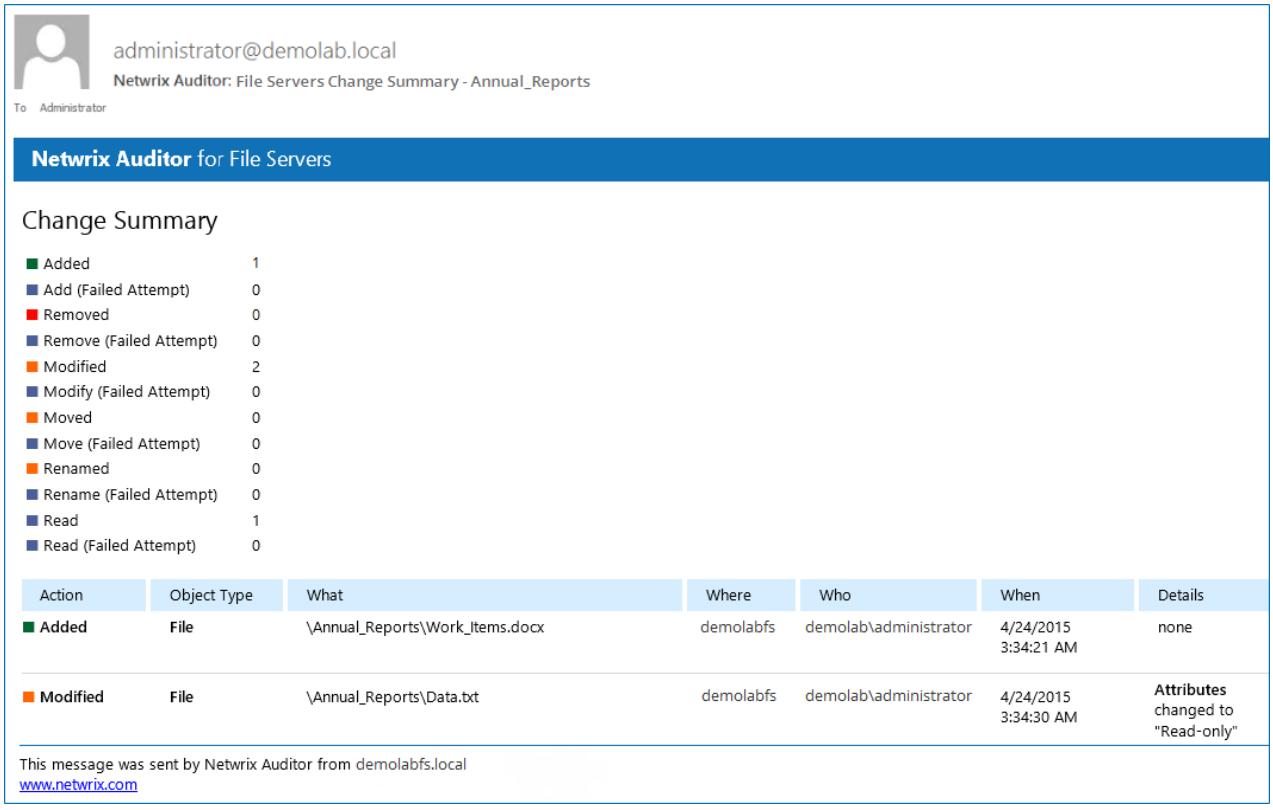
To launch data collection manually

1. In the Netwrix Auditor Administrator Console, navigate to **Managed Objects** → **your_Managed_Object_name**.
2. In the right pane, click **Run**.
3. Check your mailbox for an email notification and make sure that the data collection has completed successfully.

8.1. Review a Change Summary

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

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



administrator@demolab.local
Netwrix Auditor: File Servers Change Summary - Annual_Reports
To Administrator

Netwrix Auditor for File Servers

Change Summary

Added	1
Add (Failed Attempt)	0
Removed	0
Remove (Failed Attempt)	0
Modified	2
Modify (Failed Attempt)	0
Moved	0
Move (Failed Attempt)	0
Renamed	0
Rename (Failed Attempt)	0
Read	1
Read (Failed Attempt)	0

Action	Object Type	What	Where	Who	When	Details
Added	**File**	\Annual_Reports\Work_Items.docx	demolabfs	demolab\administrator	4/24/2015 3:34:21 AM	none
Modified	**File**	\Annual_Reports\Data.txt	demolabfs	demolab\administrator	4/24/2015 3:34:30 AM	**Attributes** changed to "Read-only"

This message was sent by Netwrix Auditor from demolabfs.local
www.netwrix.com

The example Change Summary provides the following information:

Column	Description
Action	Shows the type of action that was performed on the object.
Object Type	Shows the type of the object.
What	Shows the name of the changed object or its path.
Where	Shows the name of the server where the change occurred.
Who	Shows the name of the account under which the change was made.
When	Shows the exact time when the change occurred.
Details	Shows the before and after values of the modified object, object attributes, etc.

8.2. Browse Data with AuditIntelligence Search

Netwrix Auditor delivers complete visibility into your IT infrastructure. Its convenient AuditIntelligence search interface enables you to investigate incidents and browse audit data collected across the entire IT infrastructure. When running a search in Netwrix Auditor, you are not limited to a certain audited system, 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 AuditIntelligence search.

To browse your audit data and see you test changes

1. On the main Netwrix Auditor page, navigate to **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:

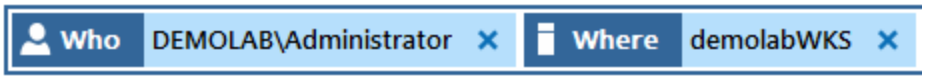
   - Add different filters to your search. Search results will be sorted by all selected filters since they work as a logical conjunction (e.g., **Who***: Administrator* AND **Action***: Added*).
   - Specify several values in the same filter to search for any of them (e.g., **Action***: Modified* OR **Action***: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

   For example, consider adding these filters:

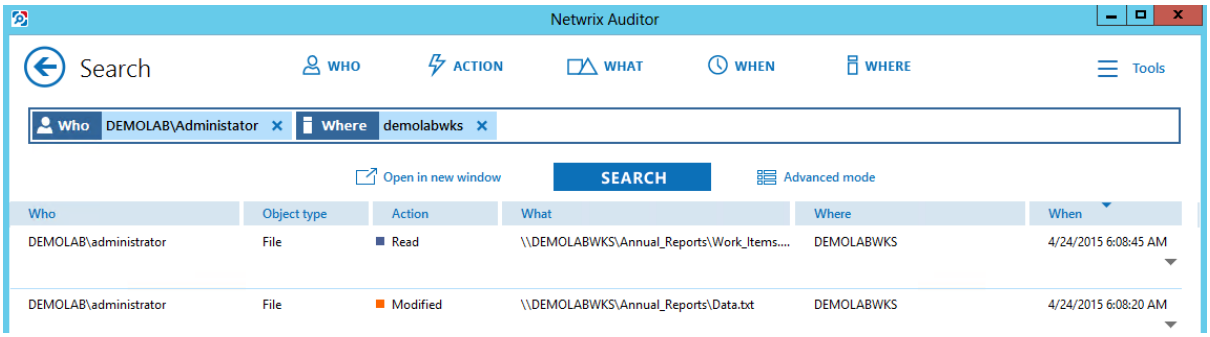
Filter	Value
WHO	Specify your account name, as you performed test changes.
WHERE	Specify your file server name.

NOTE: Refer to Netwrix Auditor User Guide for detailed instructions on how to apply filters and change match types.

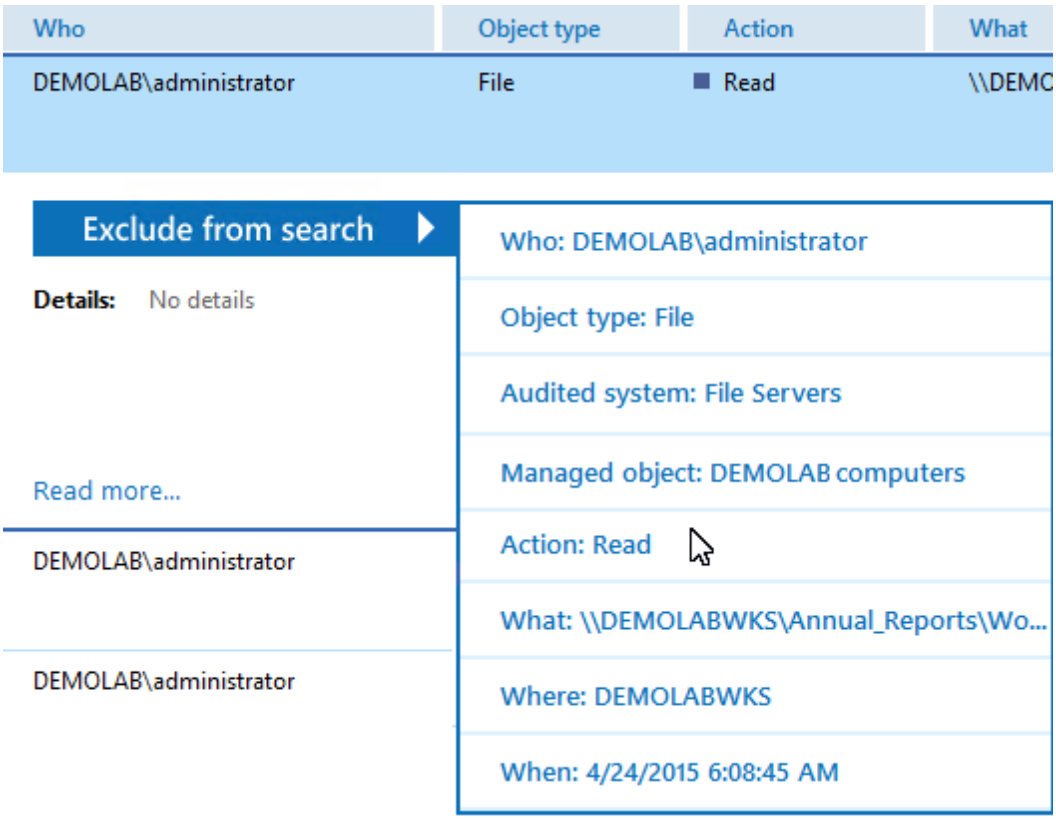
As a result, you will see the following filters in the **Search** field:



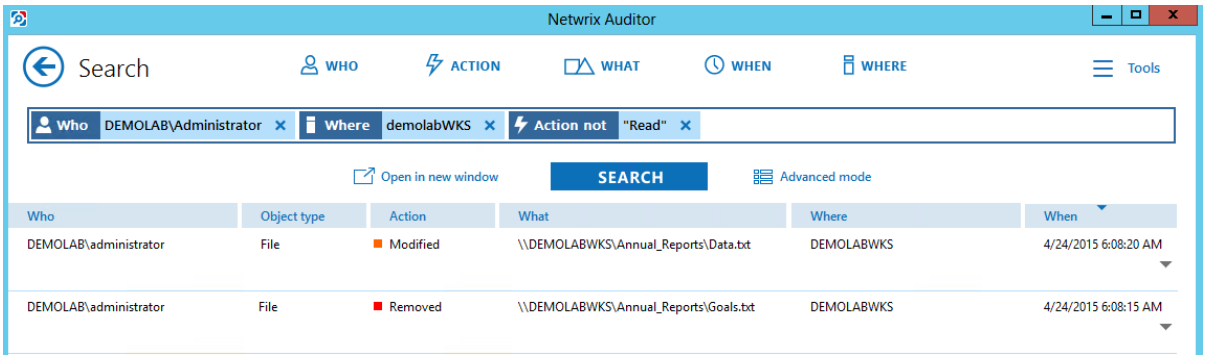
3. Click **Search**.



4. Now, you can narrow your search and modify it right from the search results pane. Double-click any entry that contains excess data, select **Exclude from search** and specify a filter, e.g., **Action**: *Read* to leave information on modifications and removals 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 **Export data** to save your search results as a *.pdf or *.csv file.
   - Click **Save search** to save the selected set of filters. This search will be added to the **Saved Searches** section on the main Netwrix Auditor page, so that you will be able to access it instantly. Refer to Netwrix Auditor User Guide for detailed instructions on how to create saved searches.

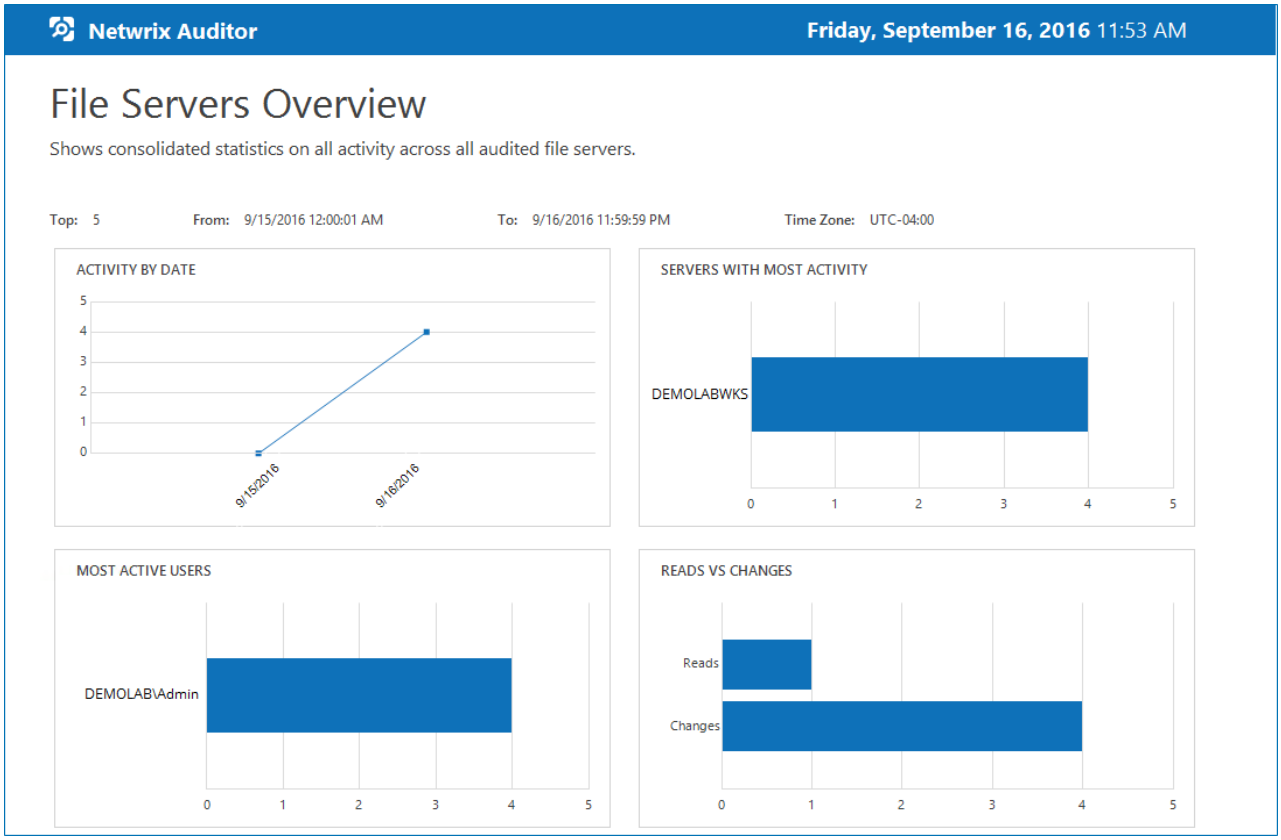
8.3. Review File Servers Overview

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

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 **Enterprise Overview** section.
2. Click the **NetApp** tile to open it.
3. Review your changes.
4. Click on any chart to jump to a table report with the corresponding grouping and filtering of data.



8.4. Review the All File Servers Activity Report

Netwrix Auditor allows generating audit reports based on Microsoft SQL Server Reporting Services (SSRS). The Netwrix Auditor client provides a variety of predefined reports that aggregate data from the entire

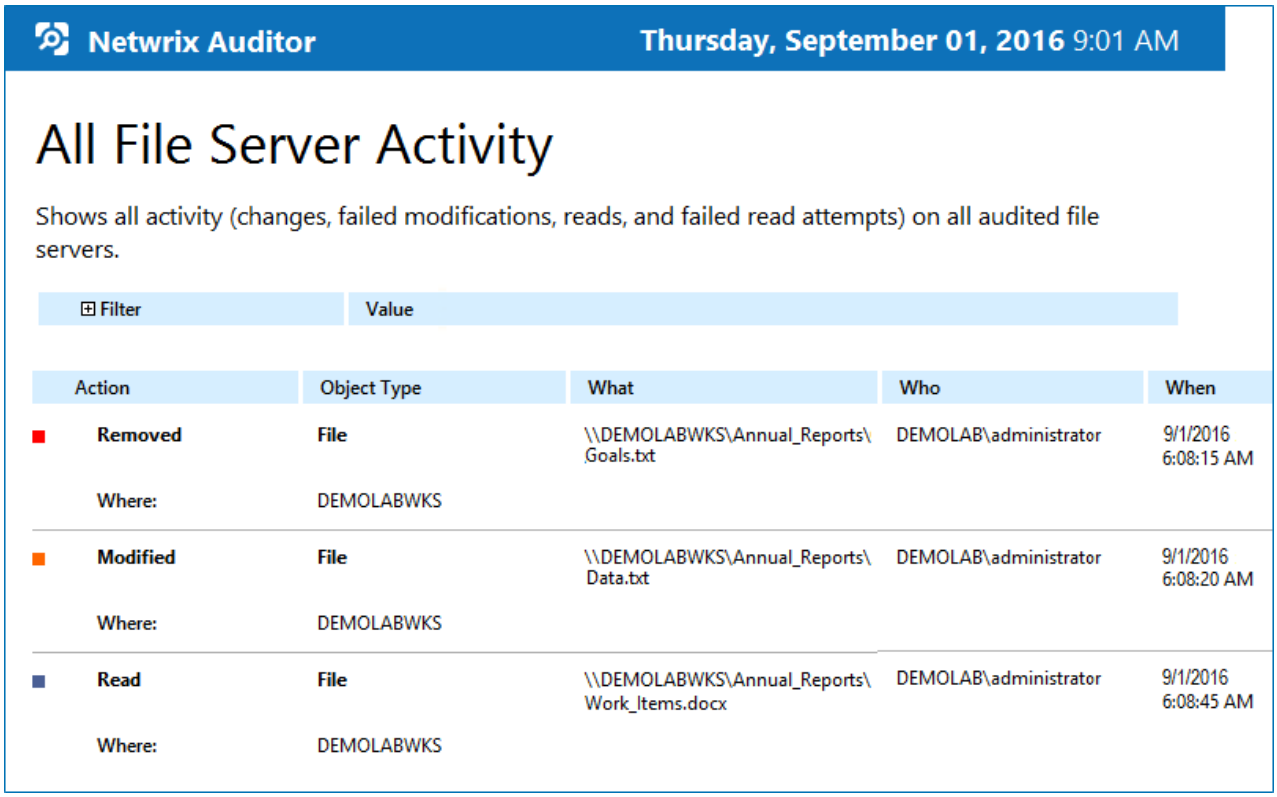
audited IT infrastructure, an individual system, or a Managed Object.

Change reports can be found under the **Reports** → **File Servers** → **File Servers Activity** 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. In the Netwrix Auditor client, navigate to **Reports** → **File Servers** → **File Servers Activity**.
2. Select the **All File Servers Activity** report.
3. Click **View** to open the report.



Netwrix Auditor — Thursday, September 01, 2016 9:01 AM

All File Server Activity

Shows all activity (changes, failed modifications, reads, and failed read attempts) on all audited file servers.

Filter	Value

Action	Object Type	What	Who	When
Removed	**File**	\\DEMOLABWKS\Annual_Reports\Goals.txt	DEMOLAB\administrator	9/1/2016 6:08:15 AM
Where:	DEMOLABWKS			
Modified	**File**	\\DEMOLABWKS\Annual_Reports\Data.txt	DEMOLAB\administrator	9/1/2016 6:08:20 AM
Where:	DEMOLABWKS			
Read	**File**	\\DEMOLABWKS\Annual_Reports\Work_Items.docx	DEMOLAB\administrator	9/1/2016 6:08:45 AM
Where:	DEMOLABWKS			

9. Related Documentation

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

Document	Description
Netwrix Auditor Installation and Configuration Guide	Provides detailed instructions on how to install Netwrix Auditor, and explains how to configure your environment for auditing.
Netwrix Auditor Administrator's Guide	Provides step-by-step instructions on how to configure and use the product.
Netwrix Auditor User Guide	Provides detailed instructions on how to enable complete visibility with AuditIntelligence.
Netwrix Auditor Integration API Guide	Provides step-by-step instructions on how to leverage Netwrix Auditor audit data with on-premises and cloud auditing solutions using RESTful API.
Netwrix Auditor Release Notes	Lists the known issues that customers may experience with Netwrix Auditor 8.5, and suggests workarounds for these issues.