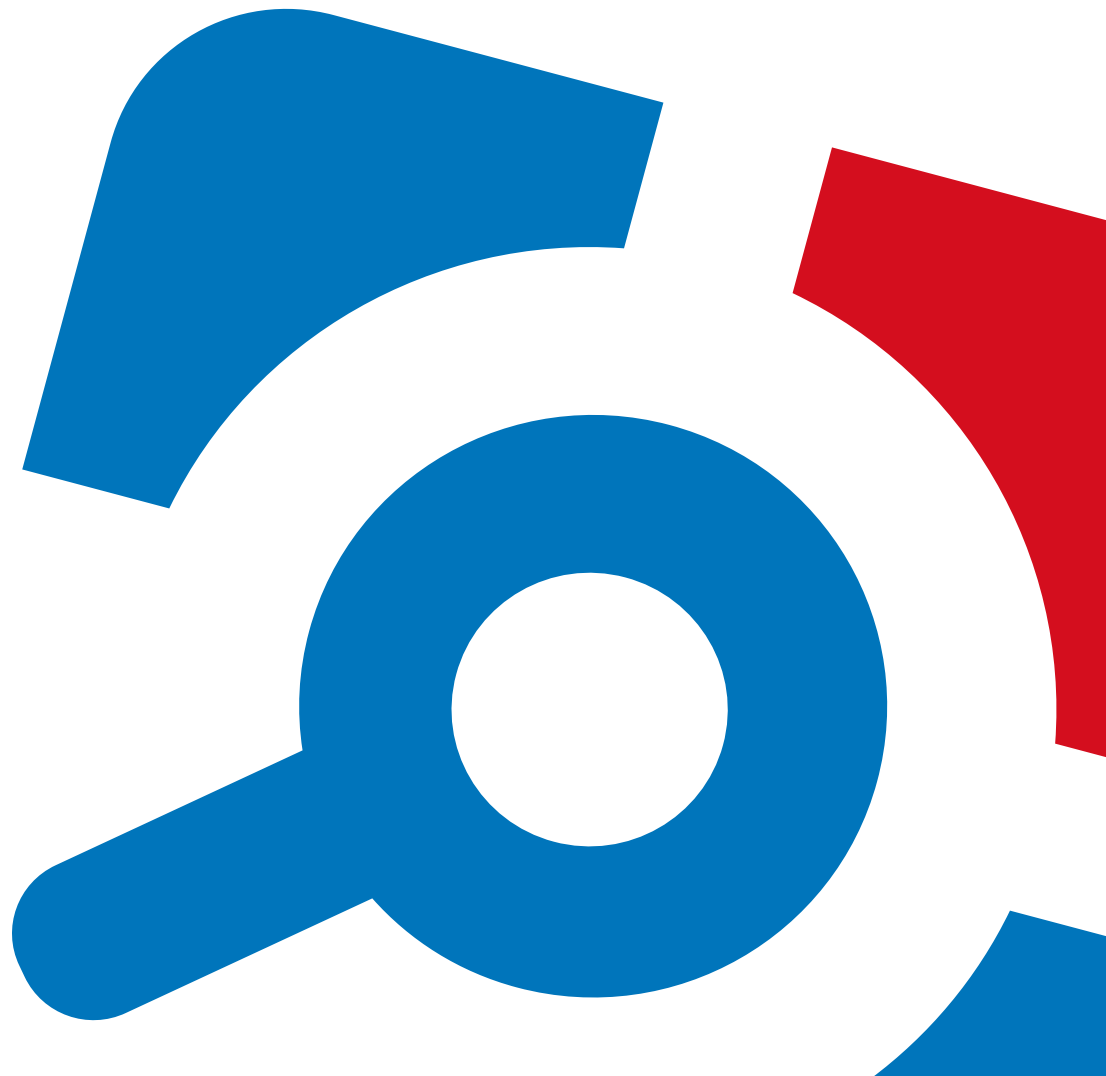


Netwrix Auditor

Release Notes

Version: 9.96
5/16/2021



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.

© 2020 Netwrix Corporation.

All rights reserved.

Table of Contents

1. What's New in 9.96	4
2. Known Issues	6
2.1. General	6
2.2. Netwrix Auditor for Active Directory	7
2.3. Netwrix Auditor for Exchange	8
2.4. Netwrix Auditor for File Servers (Windows File Server, EMC, NetApp, Nutanix Files)	9
2.5. Netwrix Auditor for Oracle Database	11
2.6. Netwrix Auditor for SharePoint	11
2.7. Netwrix Auditor for SQL Server	13
2.8. Netwrix Auditor for VMware	14
2.9. Netwrix Auditor for Windows Server	14
3. What Has Been Fixed	16

1. What's New in 9.96

Level up your database and virtual security

New features and improvements you'll get excited about

New: State-in-Time reports for SQL Server

Close permission gaps in your SQL Server to ensure your database security — Untangle complex database- and server-level permissions, and get a clear picture of who has access to what, so you can close your security gaps before threat actors get their chance. Simplify the entitlement review process, and keep user permissions in line with internal policies and further reduce the number of audit findings.

Maintain good database hygiene — Reduce the time and frustration associated with gathering and analyzing critical database configurations settings by getting a single-pane-of-glass view into your database setup, so you can ensure that everything is in line with your internal policies and finally take a well-deserved break at work.

New: State-in-Time reports for VMware

Remediate your weak spots to improve the security of your virtual environment — Understand the permissions in your virtual environment and clearly see who has access to what, so you can remediate excessive rights that increase the risk of attackers getting their hands on your sensitive data, disrupting business processes or causing you additional audit findings.

New: Netrix Auditor for Network Devices

Simplify IT auditing of Cisco Meraki, HPE Aruba and Pulse Connect Secure — Gain a single-pane-of-glass-view into Cisco Meraki, HPE Aruba and Pulse Connect Secure configuration changes and both successful and failed logon attempts, so you can have the entire audit trail available from one place.

Respond to events that might cause downtime before anyone notices — Quickly detect when your switches, routers or other network devices suddenly stop responding, so you can troubleshoot the issue before it causes downtime and affects your users or customers.

New: The Account locked out alert — Whenever an AD account gets locked out, get an alert with all the critical details required for troubleshooting, so you can restore access before user even picks up the phone.

New: The Azure AD sign-in from suspicious location alert — Promptly detect successful and failed logons to your Azure AD and cloud applications that come from outside your trusted location, such as a specific IP address, IP range or even country. Then immediately investigate this suspicious activity and take proper measures to prevent damage.

Other major improvements

Transition to MFA while keeping your IT auditing centralized — Netrix Auditor now supports MFA-only tenants, so it's the right time to comply with this Microsoft security requirement while keeping your top-notch, centralized IT auditing across SharePoint Online, Exchange Online and Azure AD.

Easily secure your Netwrix service account — Netwrix Auditor now supports group Managed Service Accounts (gMSA) for Netwrix services and data collection, so you can keep your service accounts secure while automating common management tasks, like resetting their passwords.

+ Other enhancements that improve Netwrix Auditor usability and performance.

2. Known Issues

This section provides a list of all currently known issues that customers may experience with Netwrix Auditor 9.96. For each issue, there is a brief description and a workaround or a comment if available.

2.1. General

ID	Issue Description	Comment
160222	After upgrading to Netwrix Auditor 9.95 you may need to wait for 24 hrs (until data collection daily cycle is completed) for the User Accounts - Attributes report to display all data as designed.	<p>The report may be empty until <i>parentCanonicalName</i> property is collected and stored to the audit database.</p> <p>The following information based on related properties may be not reported properly:</p> <ul style="list-style-type: none"> ○ Account locked (<i>accountLockedOut</i>) ○ Password expired (<i>pwdExpiringTime</i>) ○ User cannot change password (<i>cannotChangePassword</i>) <p>The following information will not be reported:</p> <ul style="list-style-type: none"> ○ Parent OU/container (<i>parentCanonicalName</i>) ○ Manager (<i>managerDisplayName</i>) ○ Manager email address (<i>managerEmail</i>) ○ Street address (<i>streetPoBox</i>) ○ Last modified (<i>whenChanged</i>)

158106 Netwrix Auditor Event Log Manager: the setup fails to

ID	Issue Description	Comment
	copy remote distributed modules. Error details: <i>The process cannot access the file because it is being used by another process.</i>	
88793	If a Monitoring Plan includes multiple AD domains containing groups with the same name, then Search using <i>Who—In Group</i> filter without specified domain name will return the results for one domain only.	To search within certain domain using this filter, specify filter value in the <i>domain\group</i> format.

ID	Issue Description	Comment
132274	Nutanix does not send SMB notification in case the file was changed using some text editors, like Notepad, WordPad, etc. Some other editors work fine (e.g. MS Word). As a result, NDC does not detect file changes, and re-index for changed file does not start automatically. So, it will be re-indexed during the next scheduled re-index task (1 week by default).	

2.2. Netwrix Auditor for Active Directory

ID	Issue Description	Comment
10831	Since the AD Configuration partition is common for all domains in a forest, any change to this partition will be reported by the product for each of the audited domains. The name of the user who made the change will only be displayed for the domain where the change was made. Product reports for other audited domains will show the "System" value in the "Who" column.	Ignore entries with the "System" value in the "Who" column for other domains.
11090	If changes to group membership are made through Exchange Control Panel, the product will report on addition and deletion of all group members in addition to these changes.	
13619	If a change is made to the audited domain through Microsoft Exchange installed in another domain, the originating workstation for such changes will be reported as "Unknown".	
14291	If changes to Active Directory objects are made through	

ID	Issue Description	Comment
	Exchange Management Console or Exchange Control Panel, the "Workstation" field in reports showing the computer from which a change was made may contain several workstations.	
31008 31046	Netwrix Auditor reports the scheduled task or service start as an interactive logon.	
63500	The Administrative Group Members report does not show administrative group members beyond the monitored domain (e.g., child domain users).	

2.3. Netwrix Auditor for Exchange

ID	Issue Description	Comment
178976	When monitoring Exchange Online, <i>Add/Remove mailbox</i> actions will not be reported if mailboxes are created by the cloud services as a result of the user's license assignment. (The assignment of the license is reported by Netwrix Auditor for Azure AD.)	For <i>Add/Remove mailbox</i> actions to be reported, they must be created / removed via the PowerShell, using the <code>New-mailbox</code> or <code>Remove-mailbox</code> cmdlet.
11537	If a user is added through Active Directory Users and Computers, and then a mailbox is created for this user through the Exchange Management Console within a short period of time (less than 10 minutes), the product will show duplicate entries for the mailbox creation event in the "Who" column. One change will show the Exchange name of the account under which a user was created, and the other—the name of the user who created a mailbox.	Ignore the duplicate entry with the Exchange account in the "Who" field.
11110	For Microsoft Exchange, changes to text strings that have line breaks will contain the before and after values only for the text fragment before the line break. The fact of the change itself will be reported for the whole text string.	Check the resulting value through Active Directory Users and Computers or other tools.
10897	The product does not report on changes made on an Exchange with the Edge Transport role.	
10590	For Microsoft Exchange, changes to the <code>inetOrgPerson</code> object type will be reported in the Exchange audit reports with the "user" value in the "Object Type" column.	

ID	Issue Description	Comment
10431	<p>If a previously disconnected mailbox is reconnected to a user, the Exchange reports will display the mailbox GUID instead of a canonical user name in the "What" column.</p> <p>If, as a result of this operation, the email address of this user is modified, this change will be reported in the Active Directory reports with the Exchange name in the "Who" column.</p>	<p>To get a canonical user name in an Exchange report, look for the "User" attribute in the "Details" field of the reconnected mailbox change entry.</p> <p>To get the "Who" value for the email address change entry, open Exchange report for the same time period and look for the entry reflecting the mailbox reconnection event. The user who reconnected the mailbox is the same user who initiated the email address change event. You can match the email notification entry with the mailbox reconnection entry by comparing the Object Path field in the Active Directory report with the User attribute in the "Details" field of the Exchange report.</p>

2.4. Netwrix Auditor for File Servers (Windows File Server, EMC, NetApp, Nutanix Files)

ID	Issue Description	Comment
128593	For Nutanix file server: effective permissions (as a combination of NTFS and Shared permissions) are not calculated properly for the local Administrators group members.	
126202	For Windows file server: if a mount point is a shared folder, then the objects in its root will be initially collected by Netwrix Auditor and appear as processed by <i>System</i> account.	During the next data collections, all actions for these objects will be monitored in a normal way.

ID	Issue Description	Comment
126198	Netwrix Auditor for Windows File Server does not audit the mount points targeted at the subfolder of a file share.	To process such mount points, in the monitored item settings provide network path to the target subfolder.
2871 762 42760	For NetApp 8.3.1 (or earlier) and EMC Isilon systems Netwrix Auditor may skip empty files creation and newly created folders in reports and activity summaries.	
30698 30847	<p>If you switch native log format (EVTX and XML) on a NetApp 8.3.1 (or earlier) file server, you will receive errors on data collections until the first change event is captured and log is created. These errors can be ignored.</p> <p>If you performed a switch when the data collection was in progress you will receive an error stating that the log cannot be read. After a switch, Netwrix Auditor will not be able to get data from the previously used log.</p>	
9450 9208 8887	When monitoring NetApp8.3.1 (or earlier), viewing an object's security properties may be reported as a change to these properties.	
34787	<p>When monitoring NetApp 8.3.1 (or earlier), if an audit configuration error occurred within previous 11 hours, further data collection statuses may be Working and Ready even if this error persists.</p> <p>Netwrix Auditor automatically checks audit settings every 11 hours irrespective of scheduled or on-demand data collections, and writes a single notification into the Netwrix Auditor System Health log. Scroll down the log to see the error/warning.</p>	<p>To keep data collection status up-to-date, it is recommended to run data collections less frequently (e.g., twice a day—every 12 hours).</p> <p>To resolve configuration error:</p> <ul style="list-style-type: none"> • Enable automatic audit configuration. • Fix the error manually if this error is related to insufficient object permissions.

ID	Issue Description	Comment
		<ul style="list-style-type: none"> Add a problem object to omitcollect.txt to exclude it from monitoring.

2.5. Netwrix Auditor for Oracle Database

ID	Issue Description	Comment
158579	When adding Oracle Database instance or Wallet item to monitoring plan, Netwrix Auditor shows the following error: "Failed to install one or more required components."	Restart the Netwrix Auditor for Oracle Database Audit Service.

2.6. Netwrix Auditor for SharePoint

ID	Issue Description	Comment
1549	SharePoint Central Administration URL specified on monitoring plan creation cannot exceed 80 characters.	If your SharePoint Central Administration URL exceeds 80 characters, create a short name and specify it in the Alternate Access Mappings , and create a Site Binding in IIS for SharePoint Central Administration v4.
12683	When a lot of SharePoint changes are made within a short period of time (15-20 changes per second), some events may be lost and not reflected in audit reports and Activity Summaries because of the default IIS recycle settings (the IIS Worker Process that accumulates data on changes is restarted before all data is written to the Audit Database).	Modify the default IIS recycle settings to keep data when the process is restarted. For details on how to configure recycling, refer to the following Microsoft article: Recycling Settings for an Application Pool .
12883	The timestamp for SharePoint farm configuration changes in audit reports and Activity Summary emails is the time when Netwrix Auditor generates the daily Activity Summary, not the actual event time.	

ID	Issue Description	Comment
13445	<p>The following changes are reported by the product with the "Unknown" value in the "Who" column:</p> <ul style="list-style-type: none">• Automatic creation of SharePoint groups on site creation if it uses unique permissions instead of inheriting them• All changes made under the "Anonymous" user if the security policy permits such changes	
13918	<p>The following changes are reported with the "SHAREPOINT\system" value in the "Who" column:</p> <ul style="list-style-type: none">• Changes made under an account that belongs to Farm Admins• Changes made under an account that is a Managed account for the Web Application Pool• Changes made under an account that is specified in the User Policy of the modified Web Application with the "Operates as a system" option enabled• Changes resulting from SharePoint Workflows	
13977	<p>The "Workstation" field is not reported for content changes if they were made in one of the following ways:</p> <ul style="list-style-type: none">• Through powershell cmdlets• Through the Site settings → Content and Structure menu• Through Microsoft servers and Office applications integrated with SharePoint• Through SharePoint workflows• Through the Upload Multiple Files menu option• Through the Open With Explorer menu option• Through a shared folder• Deletion of items through the context menu	
33670	<p>Netwrix Auditor does not report on changes to lists, list items, and web sites that had occurred before these objects were removed.</p>	

2.7. Netwrix Auditor for SQL Server

ID	Issue Description	Comment
7769	Removal of a SQL Job together with unused schedules is reported with the "System" value in the "Who" column.	
6789	<p>With the Audit data changes option enabled, when you try to perform the UPDATE/INSERT/DELETE operations in an audited database, an error is returned stating that the statements cannot be executed because the database owner SID cannot be resolved or SIDs do not match.</p> <p>NOTE: Database backup and restore may lead to unresolved or not matching SIDs.</p>	<p>For detailed information about the issue and for a solution, refer to the following Netwrix Knowledge base article:</p> <p>An error is returned stating that you have problems accessing an audited database.</p>
25667	Netwrix Auditor shows the same workstation name in reports and search results for all changes made to an object within the data collection period (24 hours for default data collection schedule or between two manual launches) even if changes were made by different users and from different workstations.	
155774	The 'Object Permissions in SQL Server' and 'Account Permissions in SQL Server' reports will not show the ALTER (SERVER_ROLE) capability for the privileged users in SQL Server 2008 R2 due to that SQL Server version implementation.	
139588	The 'Object Permissions in SQL Server' and 'Account Permissions in SQL Server' reports will not show the RESTORE capability for the database owner.	
139554	Permissions for INFORMATION_SCHEMA granted via <i>master db</i> will not be reported in the 'Account Permissions in SQL Server' report.	
155179	State-in-time data for some system tables may not be collected properly.	
145577	Windows principals and windows_membership data will not be included in the state-in-time snapshot when collecting data on the group having members who belong to the outgoing trust domain.	

2.8. Netwrix Auditor for VMware

ID	Issue Description	Comment
160233	Netwrix Auditor for VMware will not collect data on Failed Logon event in case of incorrect logon attempt through VMware vCenter Single Sign-On.	
168911	When creating a state-in-time snapshot, Netwrix Auditor for VMware will not collect data on AD users if these users' permissions were granted via membership in their Primary Group.	

2.9. Netwrix Auditor for Windows Server

ID	Issue Description	Comment
134683	<p>When calculating "Servers with unauthorized antivirus software" risk metric value, Windows 2016/2019 machines where pre-installed Windows Defender is running are considered a risk factor.</p> <p>They will be also considered a risk factor when the "Antivirus Baseline" filter in the "Windows Server Inventory" report is applied.</p>	<p>If you install a third-party antivirus product, you should uninstall Windows Defender as recommended by Microsoft.</p> <p>Otherwise, there will be two antiviruses running: Windows Defender and third-party solution. In this case, Netwrix Auditor will treat Windows Defender as a main antivirus, and related calculations will be performed accordingly.</p>
102460	When calculating "Servers with unauthorized antivirus software" risk metric value, Windows 7 machines where pre-installed Windows Defender is running are considered a risk factor.	Microsoft Action Center does not classify Windows Defender on Windows 7 machines as antivirus software (see this article for more information). Use fully-featured antivirus software, e.g. Kaspersky Internet Security, ESET File security, Microsoft Security

ID	Issue Description	Comment
		Essentials, etc.
12743	Some registry changes may be reported as <i>who=system</i> or <i>who=computer account</i> .	
12745	Software upgrade is reported by the product as two consecutive changes: software removal and software installation. The entry for software removal will have the "System" value in the "Who" column.	Look for the user name in the entry for software installation to determine who performed the upgrade.
User Activity		
12763	Links to video recordings will not open from reports saved in the doc/xls format, or reports received by subscription and attached to emails in one of these formats.	Save reports in the PDF format and select this format when configuring a subscription to a report.
12807	On Windows 8.1/Windows Server 2012, the information on the launch of Windows Store (Metro-style) applications is not written to the detailed activity log (reports metadata), as applications in a tile-based interface do not have application descriptions or window titles. Therefore, data search or positioning inside video files will be unavailable for such applications. A video recording session will not start before the user accesses their desktop for the first time.	
12451	Video capture of an RDP session will be terminated if this session is taken over by another user.	

3. What Has Been Fixed

This section lists issues that were known in the earlier versions and have been fixed in Netwrix Auditor 9.96.

Issue	Description
Update 6	
Ticket 178978	Netwrix Auditor for Active Directory fails to process a large amount of data for the domain containing duplicate AD objects.
Bugs 180184, 180185	The product shows unwanted changes configured to be excluded using the "omiteventuserlist".
Update 5	
Tickets 174861, 179625	The following error occurs during the State-in-Time data collection for a SQL Server monitoring plan: "Destination array is not long enough to copy all the required data. Check array length and offset".
Ticket 177844	The following error occurs during the State-in-Time data collection for a SQL Server monitoring plan: "Snapshot inconsistency was detected for the latest snapshot. Reports on <database name> database may contain incomplete audit data".
Ticket 178232	Netwrix Auditor for Windows Server. Read-only domain controllers are not included in the monitoring scope.
Bug 179401	Unexpected high CPU usage when uploading a SQL Server daily snapshot to a database.
Update 4	
Ticket 175246	Error when generating the "File and folder names containing sensitive data" report.
Ticket 175625	The product fails to collect state-in-time data for a SharePoint Online site collection.
Ticket 178090	The following error occurs when auditing an SQL Server instance: "None of the databases was processed successfully".

Issue	Description
Ticket 178435	The Netwrix Auditor for File Servers service crashes when auditing EMC storages.
Update 3	
Ticket 297102: Item 175340	Current state-in-time SQL snapshot is sometimes updated less frequently than once a day in Netwrix Auditor for Active Directory.
Ticket 299387: Item 176978	Netwrix Auditor for SharePoint Online fails to collect state-in-time date due to the following error: <i>"System.Net.WebException: The remote server returned an error: (503) Server Unavailable."</i>
Ticket 298768: Item 176949	Netwrix Auditor for SharePoint Online fails to collect state-in-time data or import historical snapshot due to the following error: <i>"Cannot resolve the collation conflict between 'Latin1_General_CI_AS' and 'French_CI_AS' in the equal to operation."</i>
Ticket 296529: Item 176948	Netwrix Auditor for SharePoint Online fails to collect state-in-time data due to the following errors: <i>"Too many requests (429)" / "Keyset does not exist"</i> .
Ticket 298582: Item 176390	Netwrix Auditor for SharePoint Online fails to collect state-in-time data due to the following error: <i>"System.Security.Cryptography.CryptographicException: Keyset does not exist"</i> .
Ticket 294566: Item 173896	Netwrix Auditor for SharePoint Online fails to collect state-in-time data due to the following error: <i>"The request uses too many resources"</i> .
Ticket 292176, 296905: Item 172729	Netwrix Auditor for SharePoint Online fails to collect state-in-time data.
Ticket 295816: Item 176089	Monitoring Plans and monitored items added in Netwrix Auditor for File Servers are not shown in the Data Classification reports.
Ticket 297020: Item 174733	Reports on categorized files and folders display <i>'Item: No item found'</i> message.
Ticket 299426: Item 176590	Password not cleared when data collecting account is changed.

Issue	Description
Ticket 299514: Item 176808	Alerts that were triggered prior to daylight savings time switch now appear as removed in the Behavior Anomalies dashboard.
Update 2	
Ticket 296776, 297206: Item 173805	Netwrix Auditor for Azure AD cannot collect Azure AD snapshot due to the following error: <i>'ValueType 'System.Int32' cannot be null'.</i>
Ticket 294404: Item 170229	Netwrix Auditor for Office 365 is unable to collect mailbox permissions due to the following error: <i>'The underlying connection was closed: A connection that was expected to be kept alive was closed by the server.'</i>
Ticket 294246: Item 170762	Netwrix Auditor for Office 365 is unable to collect mailbox permissions state-in-time data due to the following error: <i>'The operation timed out.'</i>
Ticket 292883: Item 172094	Degraded performance of Netwrix Auditor for Active Directory when trying to analyze a large amount of logon events.
Ticket 295626: Item 172620	Password Expiration Notifier cannot open the " Filter by Group " dialog box because it cannot determine whether the computer named "<DC_Name>" is joined to a domain.
Ticket 295384: Item 173576	Netwrix Auditor for Office 365 cannot save mailbox audit data to AuditArchive storage (Long-Term Archive and auxiliary folders) due to the following error: <i>'Object reference not set to an instance of an object.'</i>
Ticket 296851: Item 173912	' Activity Outside Business Hours ' detailed sub-report does not show data of the ' User Activity ' data source.
Bug 173259: Item 173718	' Behavior Anomalies ' report displays the data incorrectly: some alerts on daily chart are missing or displayed within another day.
Bug 174485: Ticket 297171: Item 174175	Duplicates of license counters appear after Netwrix Auditor Server migration to a new machine, and the following configuration issue occurs: <i>'A child item with this name already exists'.</i>

Issue	Description
Ticket 297768: Item 174801	Netwrix Auditor for Windows Server periodically creates multiple instances of <i>plsrv.exe</i> process on the target server, increasing memory usage.
Ticket 296654, 296513: Item 173971	Working folder size of Netwrix Auditor for File Server increases due to retention settings not applied properly to the old data.
Ticket 295764: Item 173786	Netwrix Auditor for NetApp crashes during state-in-time data collection.