Quest

Quest® Change Auditor for NetApp® 6.9

Event Reference Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Change Auditor for NetApp Event Reference Guide
Updated - November 2017
Software Version - 6.9

Contents

1

Introduction

Change Auditor for NetApp tracks, audits and alerts on file and folder changes in real time, translating events into simple text and eliminating the time and complexity required by native auditing. The auditing scope can be set on an individual file or folder or an entire file system recursive or non-recursive. You can also include or exclude certain files or folders from the audit scope in order to ensure a faster and more efficient audit process.

In addition to real-time event auditing, you can also enable event logging to capture NetApp filer events locally in a Windows event log. This event log can then be collected using InTrust to satisfy long-term storage requirements.

NOTE: NetApp Filer auditing and event logging are only available if you have licensed Change Auditor for NetApp and have applied a NetApp Auditing template for each NetApp filer to be audited. Contact your Sales Representative for more information on obtaining Change Auditor for NetApp.

This guide lists the events that can be captured by Change Auditor for NetApp. Separate event reference guides are provided that list the core Change Auditor events (when any Change Auditor license is applied) and the events captured when the different auditing modules are licensed.

2

Change Auditor for NetApp Events

Change Auditor for NetApp queries NetApp filers for modifications made to files and folders. This auditing functionality is based on NetApp's Data ONTAP file screening policy (FPolicy), which allows third-party screening software to interact with the NetApp filer. This section lists the audited events captured by Change Auditor when Change Auditor for NetApp is licensed and a NetApp auditing template is created for each NetApp filer to be audited. These events are listed in alphabetical order by facility.

IMPORTANT: When expecting large numbers of events, it may be necessary to increase the Max Events per Connection setting in the client (Agent Configuration on the Administration Tasks tab) to avoid an ever-increasing backlog of events waiting to be sent from the agent to the coordinator database.

NOTE: To view a complete list of all events, open the Audit Events page on the Administration Tasks tab in the client. This page contains a list of all the events available for auditing. It also displays the facility to which the event belongs, the severity assigned to each event, if the event is enabled or disabled, and the type of license that is required to capture each event.

NetApp

See Notes and Performance Considerations on page 9 for strategies to help minimize performance issues.

Table 1. NetApp events

Event	Description	Severity
NetApp File Access Rights Changed (no from-value)	Created when file access rights have changed on a NetApp filer. **NOTE:** Change Auditor access control list (ACL) events, i.e., discretionary access control list (DACL) and system access control list (SACL) changes, will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. **NOTE:** This event is the same as the previous event, but does not return a from value. The security events that return a from value require synchronous event exchange and can have a negative impact on performance. Whereas, the 'no from-value' events allow Change Auditor to connect and use asynchronous interfaces. If it is essential to audit this type of change and you are experiencing performance degradation, it is recommended that you disable the previous event and enable this one instead.	Medium
NetApp File Contents Written	Created when the contents of a file was written on a NetApp filer.	Medium
NetApp File Created	Created when a file is created on a NetApp filer.	Medium
NetApp File Deleted	Created when a file is deleted on a NetApp filer.	Medium
NetApp File Moved	Created when a file is moved on a NetApp filer.	Medium
NetApp File Opened	Created when a file is opened on a NetApp filer.	Medium
NetApp File Ownership Changed (no from-value)	Created when the ownership of a file is changed on a NetApp filer. **NOTE:** This event is the same as the previous event, but does not return a from value. The security events that return a from value require synchronous event exchange and can have a negative impact on performance. Whereas, the 'no from-value' events allow Change Auditor to connect and use asynchronous interfaces. If it is essential to audit this type of change and you are experiencing performance degradation, it is recommended that you disable the previous event and enable this one instead.	Medium
NetApp File Renamed	Created when a file is renamed on a NetApp filer.	Medium
NetApp Folder Access Rights Changed (no from-value)	Created when the access rights of a folder have changed on a NetApp filer. **NOTE:** Change Auditor access control list (ACL) events, i.e., discretionary access control list (DACL) and system access control list (SACL) changes, will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. **NOTE:** This event is the same as the previous event, but does not return a from value. The security events that return a from value require synchronous event exchange and can have a negative impact on performance. Whereas, the 'no from-value' events allow Change Auditor to connect and use asynchronous interfaces. If it is essential to audit this type of change and you are experiencing performance degradation, it is recommended that you disable the previous event and enable this one instead.	Medium
NetApp Folder Created	Created when a folder is created on a NetApp filer.	Medium
NetApp Folder Deleted	Created when a folder is removed from a NetApp filer.	Medium

Table 1. NetApp events

Event	Description	Severity
NetApp Folder Moved	Created when a folder is moved on a NetApp filer.	Medium
NetApp Folder Ownership Changed (no from-value)	Created when the ownership of a folder has changed on a NetApp filer. **NOTE:** This event is the same as the previous event, but does not return a from value. The security events that return a from value require synchronous event exchange and can have a negative impact on performance. Whereas, the 'no from-value' events allow Change Auditor to connect and use asynchronous interfaces. If it is essential to audit this type of change and you are experiencing performance degradation, it is recommended that you disable the previous event and enable this one instead.	Medium
NetApp Folder Renamed	Created when a folder is renamed on a NetApp filer.	Medium

3

Log Events

When event logging for NetApp is enabled in Change Auditor, NetApp filer events will also be written to a Windows® event log, named ChangeAuditor for NetApp. This event log can then be gathered by InTrust and Quest Knowledge Portal for further processing and reporting.

NOTE: To enable event logging, select **Event Logging** on on the Agent Configuration page (Administration Tasks tab), and select the type of event logging to enable.

ChangeAuditor for NetApp event log

The following table lists the log events captured when NetApp event logging is enabled. They are listed in numeric order by event ID.

Table 2. ChangeAuditor for NetApp event log events

Event ID	Description
500	NetApp Folder Created
501	NetApp Folder Deleted
502	NetApp Folder Moved
503	NetApp Folder Renamed
504	NetApp Folder Ownership Changed NetApp Folder Ownership Changed (no from-value)
505	NetApp Folder Access Rights Changed NetApp Folder Access Rights Changed (no from-value)
506	NetApp File Created
507	NetApp File Deleted
508	NetApp File Moved
509	NetApp File Renamed
510	NetApp File Ownership Changed NetApp File Ownership Changed (no from-value)
511	NetApp File Access Rights Changed NetApp File Access Rights Changed (no from-value)
512	NetApp File Opened
513	NetApp File Contents Write

4

Notes and Performance Considerations

This section contains a numerical list of notes for Short Product Name events.

Note 1

File changes to a NetApp filer initiated from the server hosting the Change Auditor agent responsible for capturing NetApp events will NOT be reported by the filer. This is a limitation of the NetApp filer's FPolicy and not a limitation of Change Auditor.

Note 2

ONTAP™ 7.3 (or later) is required to monitor permission change events.

Note 3

Events are generated as described below when actions are taken on folders that have subordinate files and folders:

- **Moving a parent folder:** For a 'Move' operation, only **one** event will be generated for the parent folder because action is only on the parent folder's path, none of the child folders or files are physically moved.
- **Deleting a parent folder:** For a 'Delete' operation, an event will be generated for each folder or file because each object will be removed separately.
- **Copying a parent folder:** For a 'Copy' operation, an event will be generated for each folder and file because a new object will be created within the target folder.

If a parent folder is copied to a target folder that is not being monitored, no event will be generated. The target folder must be monitored in order for an event to be generated.

Note 4

For better performance:

- Only monitor 'File/Folder Ownership Changed' and 'File/Folder Access Rights Changed' events when necessary. (See Note 5)
- Specify only the volumes that need to be audited.
- If possible, exclude file extensions to exclude files that do not need to be audited.

Note 5

If it is essential to audit security changes and you are experiencing performance degradation, it is recommended that you disable the event that returns the from value and enable the one that does not return the from value. The security events that return a from value require synchronous event exchange and can have a negative impact on performance. Whereas, the 'no from-value' events allow Change Auditor to connect and use asynchronous interfaces.

Note 6

You may improve performance by assigning a NetApp Auditing template to more than one agent. When multiple agents are assigned to the same template, events are load-balanced between these agents. However, the downside is that the ‘where’ field for NetApp events may contain any one of the agents being monitored by this single auditing template. In addition, if NetApp event logging is enabled in Change Auditor, events will be written on multiple agent servers.

Note 7

If a NetApp filer is not available, the agent will retry the connection every 10 minutes.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.