Quest

Quest® Change Auditor for EMC® 7.0

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 EMC Event Reference Guide
Updated - September 2018
Software Version - 7.0

Contents

1

Introduction

Change Auditor for EMC 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. Change Auditor for EMC also allows you to 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 EMC events locally in a Windows event log. This event log can then be collected using InTrust to satisfy long-term storage requirements.

NOTE: EMC auditing and event logging are ONLY available if you have licensed Change Auditor for EMC and defined an EMC Auditing template for each EMC file server (CIFS) to be audited. Contact your Sales Representative for more information on obtaining Change Auditor for EMC.

This document lists the events that can be captured by Change Auditor for EMC. 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 EMC Events

Change Auditor for EMC queries EMC Celerra/VNX/Isilon file servers for modifications made to files and folders. This chapter lists the audited events captured by Change Auditor when Change Auditor for EMC is licensed and an EMC Auditing template is created for each EMC file server (CIFS) to be audited. These events are listed in alphabetical order by facility:

- Change Auditor Internal Auditing
- EMC

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 the Change Auditor for EMC 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 by Change Auditor for EMC. 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 Change Auditor for EMC license that is required to capture each event.

Change Auditor Internal Auditing

Table 1. Change Auditor Internal Auditing event

Event	Description	Severity
CEPP Configuration Changed	Created when the cepp.conf configuration file is changed by another user or third-party application. The change to this configuration file may prevent Change Auditor for EMC from capturing EMC events.	Medium

EMC

Table 2. EMC events

Event	Description	Severity
EMC File Access Rights Changed (no from-value)	Created when file access rights have changed on a file server. For more information see, Note 3, Note 5, and Note 6.	Medium
EMC File Contents Written	Created when the contents of a file was written on a file server.	Medium
EMC File Created	Created when a file is created on a file server.	Medium
EMC File Deleted	Created when a file is deleted on a file server.	Medium
EMC File Moved	Created when a file is moved on a file server.	Medium

Table 2. EMC events

Event	Description	Severity
EMC File Opened	Created when a file is opened on a file server.	Medium
EMC File Ownership Changed (no from-value)	Created when the ownership of a file is changed on a file server. For more information see, Note 3 and Note 6.	Medium
EMC File Renamed	Created when a file is renamed on a file server.	Medium
EMC Folder Access Rights Changed (no from-value)	Created when the access rights of a folder have changed on a file server. For more information see, Note 3, Note 5, and Note 6.	Medium
EMC Folder Created	Created when a folder is created on a file server. For more information see,Note 2	Medium
EMC Folder Deleted	Created when a folder is removed from a file server. For more information see,Note 2	Medium
EMC Folder Moved	Created when a folder is moved on a file server. For more information see,Note 2	Medium
EMC Folder Ownership Changed (no from-value)	Created when the ownership of a folder has changed on a file server. For more information see, Note 3 and Note 6.	Medium
EMC Folder Renamed	Created when a folder is renamed on a file server.	Medium

3

Log Events

When event logging for EMC is enabled on the Agent Configuration page of the Administration Tasks tab in Change Auditor, EMC audited events will also be written to a Windows event log, named ChangeAuditor for EMC event log. These log events can then be gathered by InTrust and Quest Knowledge Portal for further processing and reporting.

ChangeAuditor for EMC event log

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

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

Table 3. ChangeAuditor for EMC event log events

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

4

Notes and Performance Considerations

This section contains a numerical list of notes for Change Auditor for EMC events.

Note 1

Only EMC events initiated via a Common Internet File System (CIFS) are captured. EMC events initiated via FTP, NFS or other protocols are not captured.

Note 2

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 3

Security events do 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.

Note 4

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

Note 5

Change Auditor access control list (ACL) events (that is, discretionary access control list (DACL) and system access control list (SACL) changes) will not report inherited access control entry (ACE) changes.

Note 6

For performance and limitations in EMC APIs, the ‘from’ value is not available for the following events when auditing EMC file servers:

- EMC File Ownership Changed
- EMC File Access Rights Changed
- EMC Folder Ownership Changed
- EMC Folder Access Rights Changed

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.