Change Auditor for EMC

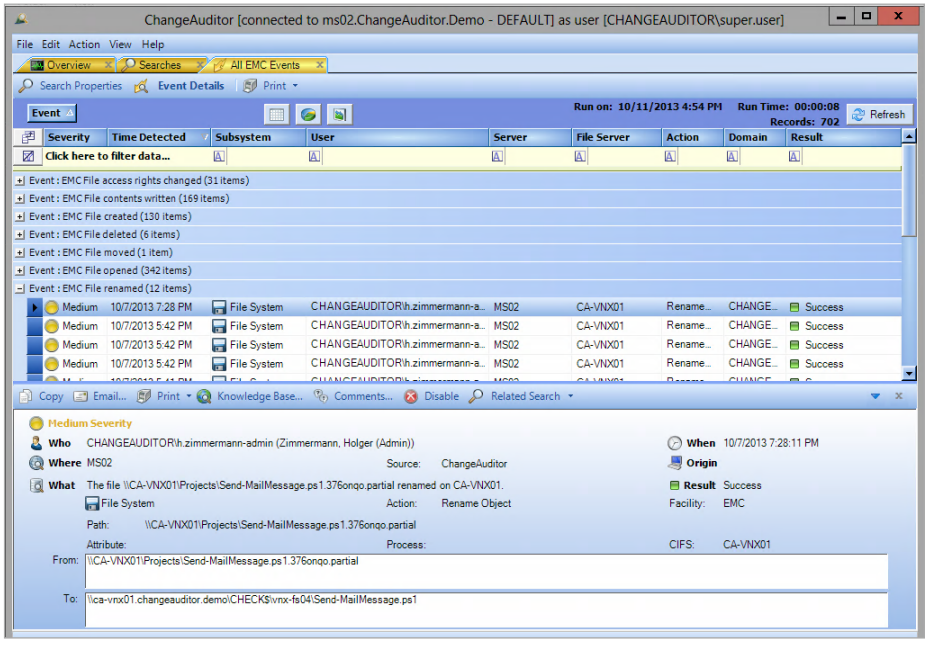
EMC server tool to track, audit, report on and alert on critical changes

Event logging and change reporting for EMC Celerra and VNX file servers is cumbersome and time consuming using native auditing tools. Because there's no central console, you have to repeat the process for each server, and you end up with a huge volume of data and a myriad of reports. That means proving compliance or reacting quickly to events is a constant challenge.

Your data security is also at risk because native event details are sparse and difficult to interpret. As a result, you may not find out about problems until it is too late. And because native tools can't prevent or even track deletions, you could lose log data — defeating the purpose of auditing in the first place.

Lucky for you, there's Quest® Change Auditor for EMC. This unparalleled tool helps ensure the security, compliance and control of files and folders by monitoring, auditing, reporting and alerting on all changes in real time. With Change Auditor, administrators can monitor, report on and analyze events and changes without complexity and fear of unknown security concerns. You will instantly know who made what change when, where, from what workstation and all related events to that change.

You can then automatically generate intelligent, in-depth forensics and reduce the risk associated with day-to-day modifications.



With Change Auditor, you can gather events from all your EMC storage servers in one place and in one format, so you can quickly see the most relevant and potentially dangerous changes.

BENEFITS:

- Proactively detects threats based on user behavior patterns
- Eliminates unknown security concerns, ensuring continuous access to EMC files, folders and users by tracking all events and those changes related to specific incidents
- Reduces security risks with real-time alerts to any device for immediate response
- Enables you to pinpoint problems quickly with robust search and filtering capabilities
- Facilitates auditing and management review by converting data into intelligently organized, in-depth forensics
- Streamlines internal security policies and external compliance regulations, including GDPR, SOX, PCI DSS, HIPAA, FISMA and SAS 70

SYSTEM REQUIREMENTS

For complete system requirements, please visit quest.com/products/change-auditor-for-emc.

AUDIT ALL CRITICAL CHANGES

Change Auditor for EMC provides extensive, customizable auditing and reporting for all critical changes to EMC filers, including files, folders, servers, permissions and configuration settings. You'll get complete visibility into all changes over the course of time and in chronological order with in-depth forensics on who, what, when, where, why and workstation, including any related events with before and after values. And, with real-time alerts to any device, you'll maintain constant awareness and the ability to respond to vital changes as they occur, reducing the risks associated with day-to-day modifications.

TRACK USER ACTIVITY

Change Auditor for EMC helps tighten enterprise-wide auditing and compliance policies by tracking user and administrator activity for EMC file changes. Change Auditor also provides information on administrators and users who have gained or changed file access rights. You'll see exactly who accessed, deleted, moved, created or renamed files and folders. And with 24x7 real-time alerts, in-depth analysis and reporting capabilities, your EMC infrastructure is protected from exposure to suspicious behavior or unauthorized access, and is always in compliance with corporate and government standards.

PROACTIVE THREAT DETECTION WITH CHANGE AUDITOR THREAT DETECTION

Simplify user threat detection by analyzing anomalous activity to rank the highest risk users in your organization, identify potential threats and reduce the noise from false positive alerts.

TURN IRRELEVANT DATA INTO MEANINGFUL INFORMATION TO DRIVE SECURITY AND COMPLIANCE

Change Auditor for EMC eliminates guesswork analysis reporting by translating isolated cryptic data into a series of meaningful events. You'll instantly get all information on the change you're viewing and all related events, such as what other changes came from specific users. You will also gain a better understanding of event trends with the ability to view, highlight and filter related events over the course of days, months and even years.

INTEGRATED EVENT FORWARDING

Easily integrate with SIEM solutions to forward Change Auditor events to Splunk, ArcSight or QRadar. Additionally, Change Auditor integrates with Quest® InTrust® for 20:1 compressed event storage and centralized native or third-party log collection, parsing and analysis with alerting and automated response actions to suspicious events.

AUTOMATE REPORTING FOR CORPORATE AND GOVERNMENT REGULATIONS

Utilizing Microsoft's SQL Server Reporting Services, Change Auditor for EMC provides clean, meaningful security and compliance reports on the fly. With a built-in compliance library and the ability to build your own custom reports, proving compliance for standards such as the General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA) and Statement on Auditing Standards No. 70 (SAS 70) is a breeze.

ABOUT QUEST

Quest provides software solutions for the rapidly changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid data centers, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-ChangeAuditor4EMC-US-KS-40684