Change Auditor for NetApp

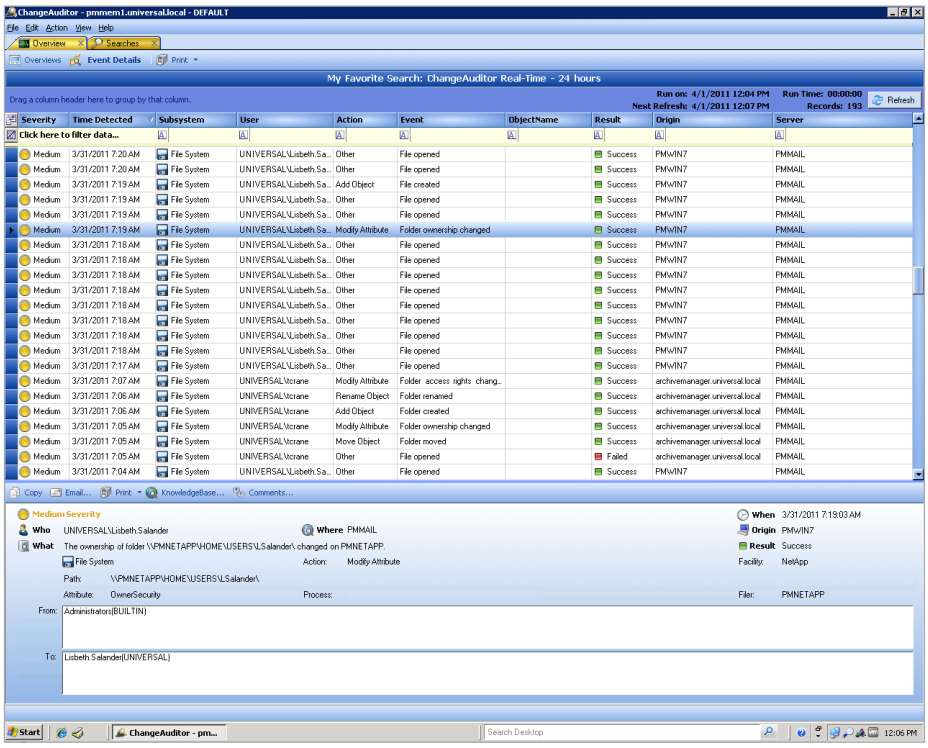
NetApp® filer change monitoring and auditing tool

Event logging and change reporting for NetApp filers is cumbersome and time consuming using native auditing tools. Because there's no central console, you've got 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 logs can be deleted or overwritten, the integrity of the log data can be compromised — defeating the purpose of auditing in the first place.

Lucky for you, there's Change Auditor for NetApp. 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 which 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 for NetApp, you can view the color-coded severity of live events from NetApp filers to see the who, what, when, where, why and workstation of events.

BENEFITS:

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

SYSTEM REQUIREMENTS

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

AUDIT ALL CRITICAL CHANGES

Change Auditor for NetApp provides extensive, customizable auditing and reporting for all critical changes to NetApp, 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 NetApp helps tighten enterprise-wide auditing and compliance policies by tracking user and administrator activity for NetApp 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 NetApp infrastructure is protected from exposure to suspicious behavior or unauthorized access, and is always in compliance with corporate and government standards.

TURN IRRELEVANT DATA INTO MEANINGFUL INFORMATION TO DRIVE SECURITY AND COMPLIANCE

Change Auditor for NetApp eliminates guesswork analysis reporting by translating isolated cryptic data into a series of meaningful events. You 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.

AUTOMATE REPORTING FOR CORPORATE AND GOVERNMENT REGULATIONS

Utilizing Microsoft's SQL Server Reporting Services, Change Auditor for NetApp 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 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 helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

DataSheet-ChangeAuditor4NetApp-US-KS-24830

Quest