

Change Auditor for VMware vCenter

VMware vCenter auditing tool tracks, reports on and alerts on critical changes

Proper auditing and log management for your VMware vCenter Server infrastructure components are critical for security and compliance, but they can prove nearly impossible in practice using native auditing tools. Because VMware vCenter was designed as a management application, not a security application, it lacks the granularity in policy enforcement required for secure deployments. And because there's no central console, you've got to repeat each 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. Moreover, because native trails can be deleted or overwritten, the integrity of the log data can be compromised — defeating the purpose of auditing in the first place. As a result, even the most skilled and diligent vCenter-based organizations are often left exposed to the security risks associated with inadequate auditing and log management.

Quest® Change Auditor for VMware vCenter helps you ensure the security, compliance and control of vCenter Server by managing, auditing, reporting and alerting on all changes in chronological order and related events in real time.

You'll be confident knowing that your data is safe and that you've met the compliance demands necessary to satisfy the scrutiny of any auditor.

BENEFITS:

- Installs in minutes with fast event collection for immediate analysis into vCenter environments
- Enables enterprise-wide auditing and compliance from a single client and stores all audit data in one secure, central database
- Ensures a secure and compliant vCenter environment by tracking all critical changes in real time to any device for immediate response
- Delivers faster time to resolution by enabling administrators to group, sort and filter search results
- Turns information into intelligent, in-depth forensics for auditors and management
- Streamlines compliance with internal security policies and external regulations, including SOX, PCI DSS and HIPAA



With Change Auditor for VMware vCenter, you can add comments on why a specific change was made in order to fulfill your audit requirements.

SYSTEM REQUIREMENTS

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

AUDIT ALL CRITICAL CHANGES

Change Auditor for VMware vCenter provides extensive, customizable auditing and reporting for all critical changes to vCenter configuration settings, VMware ESX hosts, folders, clusters, resource pools, virtual machines and users. 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 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.

TRACK USER ACTIVITY

Change Auditor for VMware vCenter helps tighten enterprise-wide auditing and compliance policies by tracking user and administrator activity such as additions and deletions on changes to resources. With in-depth analysis and reporting capabilities, your vCenter infrastructure is protected from exposure to suspicious behavior or unauthorized access, and is always in compliance with corporate and government standards.

INTEGRATED EVENT FORWARDING

Easily integrate with SIEM solutions to forward Change Auditor events to Splunk, Micro Focus ArcSight or IBM QRadar. Additionally, Change Auditor integrates with Quest® InTrust® for long-term 20:1 compressed event storage and aggregation of native or third-party logs to reduce storage costs on SIEM forwarding and create a highly compressed log repository.

TURN IRRELEVANT DATA INTO MEANINGFUL INFORMATION TO DRIVE SECURITY AND COMPLIANCE

Change Auditor for VMware vCenter 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 VMware vCenter 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

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.