EFS File Auditing

Bringing extreme accountability to content production workflows

Extreme Accountability for High Value Content

Global cyber threats and high-profile incidents impacting large studios have shaken the media and entertainment industry to its core. Emerging from the dust are new security practices and technologies that better protect critical media assets and intellectual property.

Introducing File Auditing for EditShare EFS scale-out storage, a native feature that generates an audit event each time a user accesses a media file. All file reads, writes, deletes and moves, all directory opens and modifications and all user logins and logouts are captured in a dedicated file audit log. By analysing the content of an EFS file audit log, a system administrator can detect behavior patterns that might point to human error or malicious intent.

Powerful Intuitive Dashboard

EFS File Auditing is far more than a syslog mechanism, however. Instead of saddling an administrator with the task of manually sifting through mountains of audit, it includes a powerful, easy-to-use File Auditing Analysis dashboard that provides a set of filters that make zeroing in on specific system events effortless. For example, users can analyse behavior by specifying an IP address, user name, directory, timeframe, file event type or any combination of these elements. Once gathered, the information is rendered into an easy-to-interpret graphical display of the activity of interest.

EFS File Auditing provides administrators with means to understand the Who, What, When, Where and How of user interaction with valuable media assets. Clearly, EFS File Auditing can provide important clues about security vulnerabilities and costly data breaches. But it can also enhance employee training programs by identifying human error and other innocent behavior. Furthermore, we at EditShare anticipate that being able to provide file audit records will be 'table stakes' for engaging with both major studios and minor content owners alike.

EditShare®

Protection and Efficiency

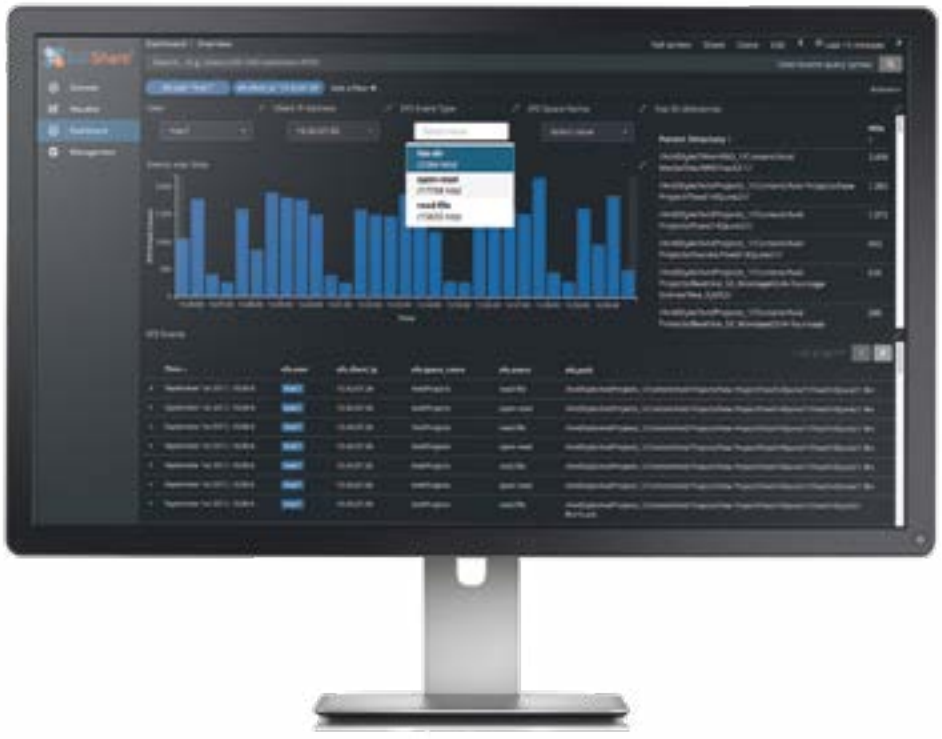
The design objective of the EditShare EFS Shared Storage is to minimize or manage the resource contention that is inevitable in a busy storage cluster. For example, by storing system metadata in dedicated, fast RAM, EFS response to file transactions is never delayed by other file system processes. Likewise, our approach to media file storage ensures that disk and node contention and latency are detected and managed long before they impact latency real-time operations. This same philosophy is applied to EFS File Auditing. Dedicated, redundant audit log storage means that collection and analysis of audit logs never impacts EFS storage performance or vice-versa and that audit log information is protected against hardware failures.

Configuration Options

File Auditing is an available option on EFS 450 and EFS 300 storage configurations and field upgrade kits are available to retrofit existing systems. And File Auditing can be extended to other EFS storage variants through the addition of a dedicated EFS Metadata Controller. EFS File Auditing is available for EditShare software versions 7.2.3 and newer. Future enhancements are planned that will enable users to integrate EFS Storage with 3rd party Security Information and Event Management solutions to support facility-wide file auditing and event correlation.

Best Security Practices

Advocates for improved content security in the Media & Entertainment segment, including the Motion Pictures Association of America and the Content Delivery and Security Association, have published ‘best security practices’ documents for production, post production and music recording studios. These recommend a multi-layer approach including a File Auditing layer. The EditShare EFS Shared Storage solution now provides a path towards full compliance with emerging content security practices.



EditShare®