EFS File Auditing – встроенный инструмент аудита для систем хранения EditShare

Максим Бабулин

В этом году модельный ряд систем хранения EditShare EFS пополнился новым компонентом, отвечающим за организацию аудита действий пользователей в файловой системе.

Максимальная ответственность за контент

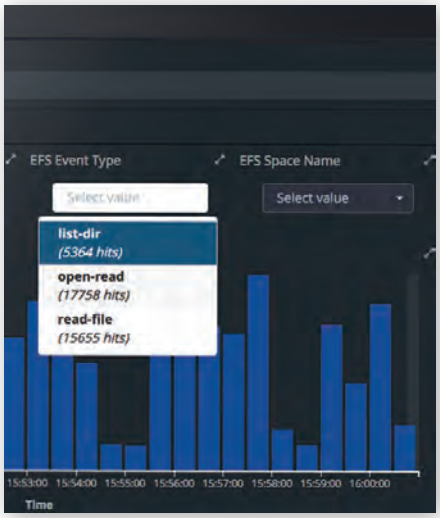
Глобальные киберугрозы и громкие инциденты, имевшие место в последнее время и затронувшие интересы крупных киностудий и иных обладателей прав на контент, потрясли средства массовой информации и киноиндустрию. Эти события стали дополнительным стимулом для развития новых технологий безопасности, которые должны защищать критически важные медиаресурсы и интеллектуальную собственность.

В данной статье рассматривается новая встроенная функция файловой системы EditShare – EFS File Auditing. Этот программный инструмент регистрирует все операции с файлами, включая чтение, запись, удаление и перемещение, открытие каталога и внесение в него изменений. Кроме того, ведется учет подключения пользователей к системе хранения и отключение пользователя от нее. Анализируя эту информацию, системный администратор может обнаруживать признаки, по которым можно с высокой долей вероятности судить о том, были ли те или иные некорректные действия обусловлены просто человеческой ошибкой либо за ними стоит злой умысел.

Эффективный интерфейс для анализа информации

Сервис EFS File Auditing — это значительно больше, чем просто механизм, регистрирующий события с записью в системный журнал. Основным рабочим инструментом системы является наглядный и интуитивно понятный web-интерфейс. Он позволяет оперативно – в режиме реального времени – отслеживать текущие операции, выполняемые в файловой системе EFS.

Набор фильтров позволяет администратору быстро сконцентрироваться на отдельных операциях или на действиях пользователей. Он может выделять для себя нужную информацию, указав IP-адрес, имя пользователя, каталог, время, тип события, связанного с файлом, или использовать в качестве критерия любую комбинацию этих параметров.



Выбор типа события для анализа

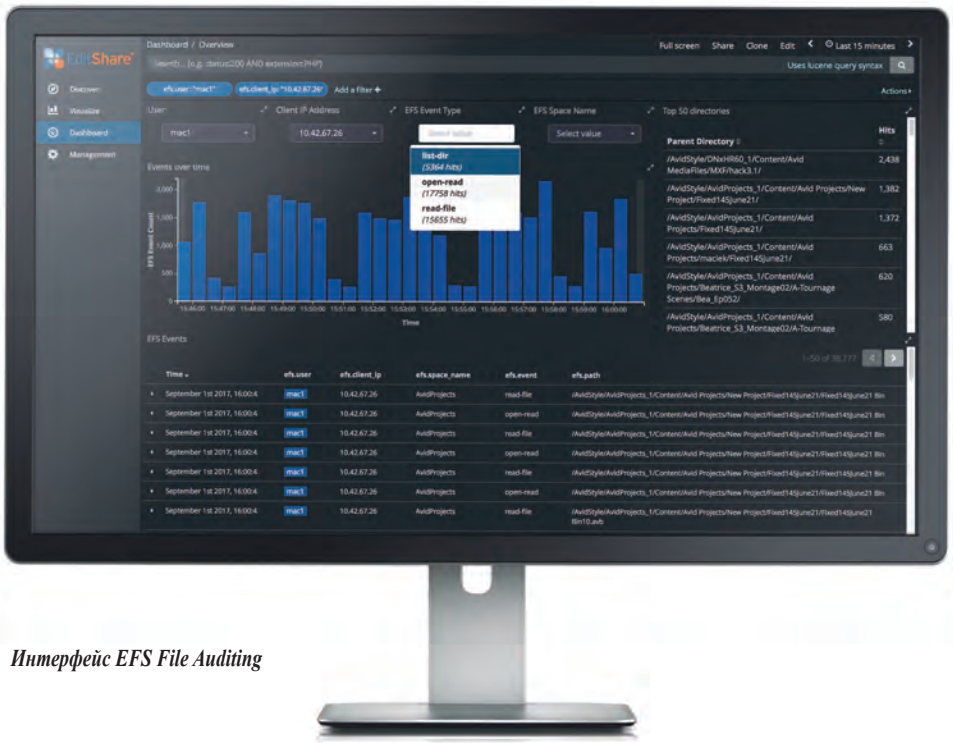
Результаты анализа сразу отображаются в графическом интерфейсе системы и динамично обновляются по ходу ее работы. Благодаря этому администратор получает возможность понять кто, когда, откуда и каким образом взаимодействует с файлами, хранящимися в системах EditShare EFS.

EFS File Auditing предоставляет важную информацию, которая помогает выявить проблемы с безопасностью и помочь предотвратить ошибки персонала за счет улучшения программы обучения сотрудников, которые регулярно «делают не то», либо противостоять злонамеренным действиям, связанным с утечкой данных. И в том и в другом случае обеспечивается повышенная защита от событий, способных повлечь существенные потери, как финансовые, так и, в определенных обстоятельствах, репутационные.

Кроме того, отчеты системы смогут служить документальной основой при решении спорных вопросов с заказчиками и владельцами контента.

Защита и эффективность

Одной из целей, которая ставилась при разработке систем хранения EditShare EFS, была минимизация задержек при обработке конкурирующих запросов. Именно поэтому системы обрабатывают все входящие запросы,



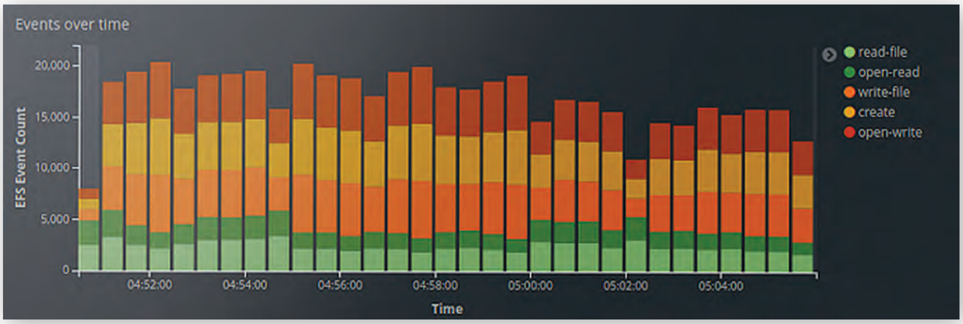
Интерфейс EFS File Auditing

Time	efs.user	efs.client_ip	efs.space_name	efs.event	efs.path
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	read-file	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	open-read	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	read-file	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	open-read	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	read-file	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	open-read	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin
September 1st 2017, 16:00:4	mac1	10.42.67.26	AvidProjects	read-file	/AvidStyle/AvidProjects_1/Content/Avid Projects/New Project/Fixed145June21/Fixed145June21 Bin10.avb

Журнал событий в EFS File Auditing

используя буфер метаданных файловой системы, всегда находящийся в оперативной памяти сервера. В результате скорость ответа сервера никогда не зависит от других действии, выполняемых файловой системой, и от задержек, связанных с имеющимся пределом скорости обращения к дискам.

Аналогичная философия применяется в работе EFS File Auditing. Все данные системы хранятся в оперативной памяти сервера, а на выделенном и защищенном от сбоев зеркальном SSD-хранилище непрерывно ведется журнал учета этих данных. Поэтому операции, связанные с сохранением и анализом информации EFS File Auditing, практически не влияют на скорость работы системы хранения в целом.



Графическое представление зарегистрированных в системе событий

Варианты конфигурации

Любая система хранения из модельного ряда EditShare EFS может быть дополнена сервисом EFS File Auditing. В зависимости от модели системы хранения, ее конфигурации и степени загрузки EFS File Auditing можно использовать либо как опцию, встраиваемую в систему хранения, либо интегрировать ее в выделенный сервер EFS Metadata Controller. В этом случае выделенный сервер принимает на себя и часть функций по обработке метаданных файловой системы. А значит, побочная нагрузка на систему хранения снижается, благодаря чему возрастает ее общая производительность.

Для систем хранения, приобретенных ранее, EFS File Auditing может поставляться как программный пакет для установки непосредственно на месте эксплуатации.

Лучшие практики безопасности

Организации MPAA (Motion Pictures Association of America – Американская ассоциация кинокомпаний) и CDSA (Content Delivery and Security Association – Ассоциация по доставке и защите контента), занимающиеся вопросами повышения эффекивности защиты контента, опубликовали документы, описывающие лучшие практики безопасности для сферы съемки, обработки и звукозаписи медиаданных. Эти ассоциации рекомендуют использовать многоуровневый подход к обеспечению безопасности контента. Одним из важнейших уровней назван аудит файловой системы. В этой связи можно быть уверенными, что системы хранения EFS отвечают самым современным тенденциям в сфере безопасности.