Peter Gubarevich

WindowsNT.LV

Применение Аудита Windows для отслеживания деятельности пользователей

СРЕДА, 31 - АВГУСТ - 2011 КОММЕНТАРИИ (9) (HTTPS://BLOG.WINDOWSNT.LV/2011/08/31/TRACKING-USER-ACTIVITY-RUSSIAN/#COMMENTS)

Иногда случаются события, которые требуют от нас ответить на вопрос **«кто это сделал?»** Такое может происходить «редко, но метко», поэтому к ответу на вопрос следует готовиться заранее.

Практически повсеместно существуют проектные отделы, бухгалтерия, разработчики и другие категории сотрудников, совместно работающие над группами документов, хранящихся в общедоступной (Shared) папке на файловом сервере или на одной из рабочих станций. Может случиться так, что кто-то удалит важный документ или директорию из этой папки, в результате чего труд целого коллектива может быть потерян. В таком случае, перед системным администратором возникает несколько вопросов:

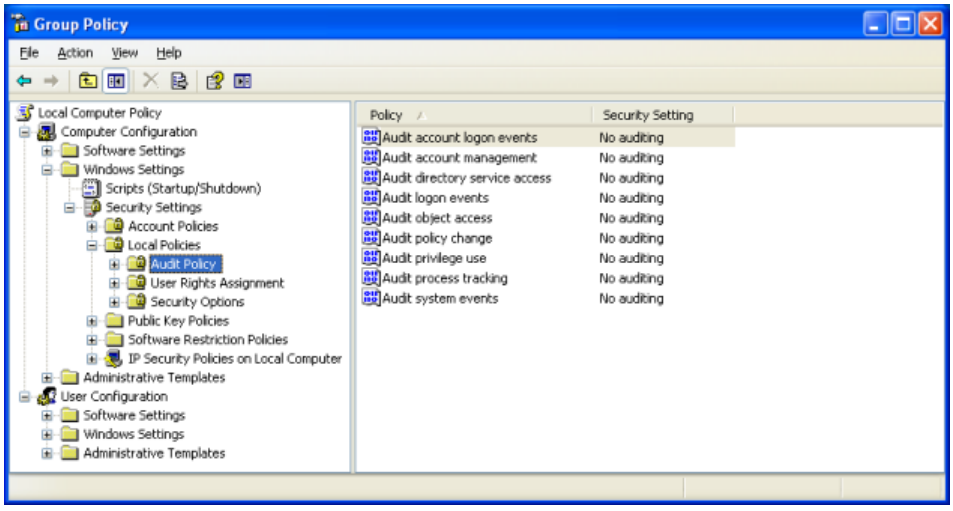
- Когда и во сколько произошла проблема?
- Из какой наиболее близкой к этому времени резервной копии следует восстановить данные?
- Это случилось непреднамеренно, или же кто-то действовал с умыслом?
- Может, имел место системный сбой, который может повториться ещё раз?

В Windows имеется система **Аудита,** позволяющая отслеживать и журналировать информацию о том, когда, кем и с помощью какой программы были удалены документы. По умолчанию, Аудит не задействован — слежение само по себе требует определённый процент мощности системы, а если записывать всё подряд, то нагрузка станет слишком большой. Тем более, далеко не все действия пользователей могут нас интересовать, поэтому политики Аудита позволяют включить отслеживание только тех событий, что для нас действительно важны.

Система Аудита встроена во все операционные системы **Microsoft Windows NT:** Windows XP/Vista/7, Windows Server 2000/2003/2008. К сожалению, в системах серии Windows Home аудит спрятан глубоко, и его настраивать слишком сложно.

Что нужно настроить?

Для включения аудита зайдите с правами администратора в компьютер, предоставляющий доступ к общим документам, и выполните команду **Start → Run → gpedit.msc.** В разделе Computer Configuration раскройте папку **Windows Settings → Security Settings → Local Policies → Audit Policies:**

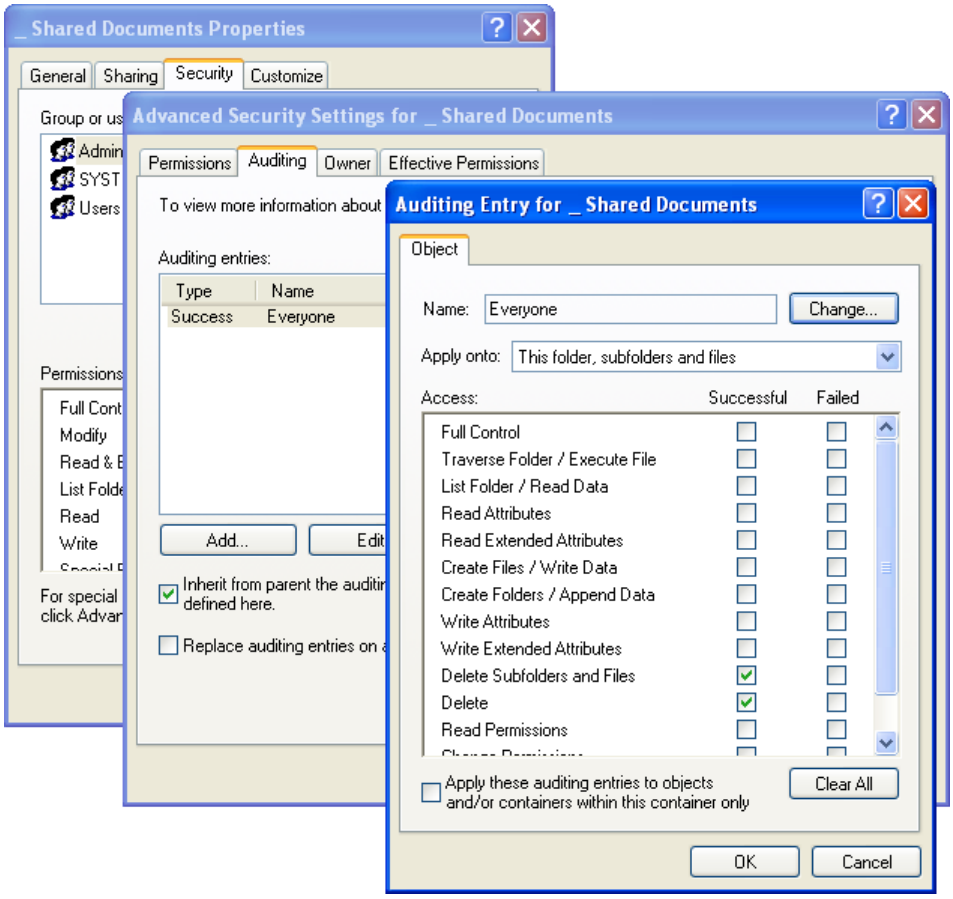


(https://windowsntlv.files.wordpress.com/2011/08/audit_policy.png)

Дважды щёлкните по политике **Audit object access (Аудит доступа к объектам)** и выберите галочку **Success.** Этот параметр включает механизм слежения за успешным доступом к файлам и реестру. Действительно, ведь нас интересуют только удавшиеся попытки удаления файлов или папок. Включите Аудит только на компьютерах, непосредственно на которых хранятся отслеживаемые объекты.

Простого включения политики Аудита недостаточно, мы также должны указать, доступ к каким именно папкам требуется отслеживать. Обычно такими объектами являются папки общих (разделяемых) документов и папки с производственными программами или базами данных (бухгалтерия, склад и т.п.) — то есть, ресурсы, с которыми работают несколько человек.

Заранее угадать, кто именно удалит файл, невозможно, поэтому слежение и указывается за Всеми (Everyone). Удавшиеся попытки удаления отслеживаемых объектов любым пользователем будут заноситься в журнал. Вызовите свойства требуемой папки (если таких папок несколько, то всех их по очереди) и на закладке **Security (Безопасность) → Advanced (Дополнительно) → Auditing (Аудит)** добавьте слежение за субъектом **Everyone (Все),** его успешными попытками доступа **Delete (Удаление)** и **Delete Subfolders and Files (Удаление подкаталогов и файлов):**



(https://windowsntlv.files.wordpress.com/2011/08/audit_files.png)

Событий может журналироваться довольно много, поэтому также следует отрегулировать размер журнала **Security (Безопасность)**, в который они будут записываться. Для
этого выполните команду **Start → Run → eventvwr.msc.** В появившемся окне вызовите свойства журнала Security и укажите следующие параметры:

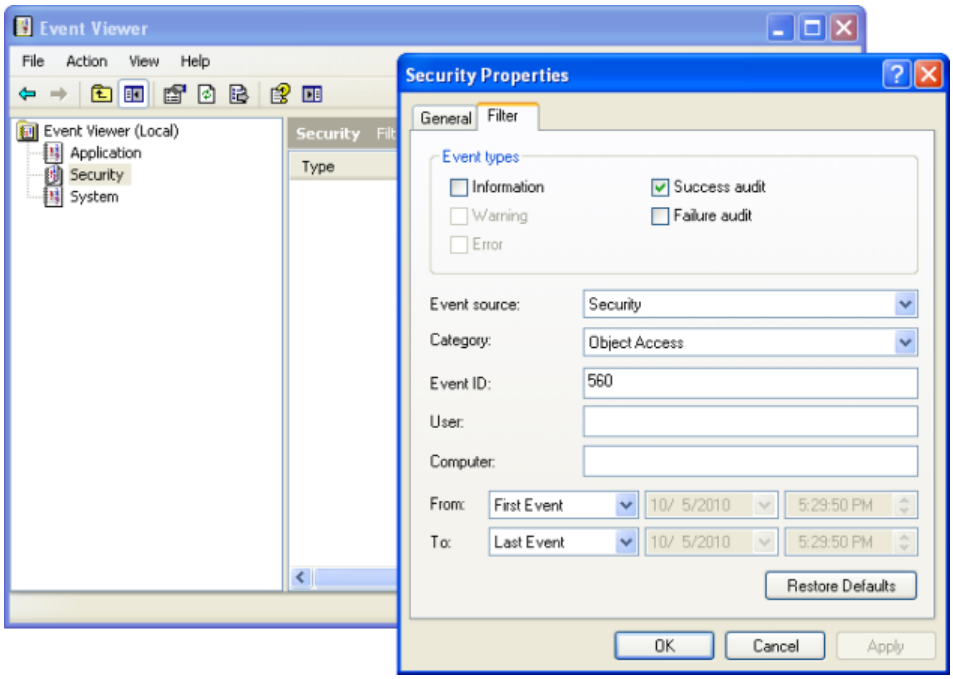
- Maximum Log Size = **65536 KB** (для рабочих станций) или **262144 KB** (для серверов)
- Overwrite events as needed.

На самом деле, указанные цифры не являются гарантированно точными, а подбираются опытным путём для каждого конкретного случая.

Итак, кто же удалил документы (Windows 2003/XP)?

Нажмите **Start → Run → eventvwr.msc** и откройте для просмотра журнал **Security (Безопасность).** Журнал может быть заполнен событиями, прямого отношения к проблеме не имеющими. Щёлкнув правой кнопкой по журналу Security, выберите команду **View → Filter** и отфильтруйте просмотр по следующим критериям:

- Event Source:Security;
- Category: Object Access;
- Event Types: Success Audit;
- Event ID: 560;

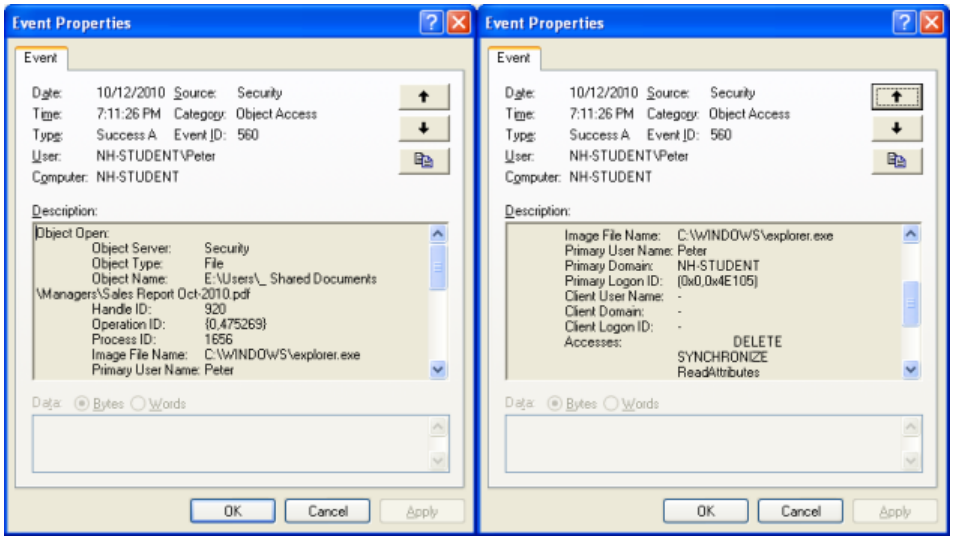


(https://windowsntlv.files.wordpress.com/2011/08/audit_events2003.png)

Просмотрите список отфильтрованных событий, обращая внимание на следующие поля внутри каждой записи:

- **Object Name.** Название искомой папки или файла;
- **Image File Name.** Имя программы, с помощью которой удалили файл;
- **Accesses.** Набор запрашиваемых прав.

Программа может запрашивать у системы сразу несколько типов доступа — например, **Delete+Synchronize** или **Delete+Read_Control.** Значимым для нас правом является **Delete.**

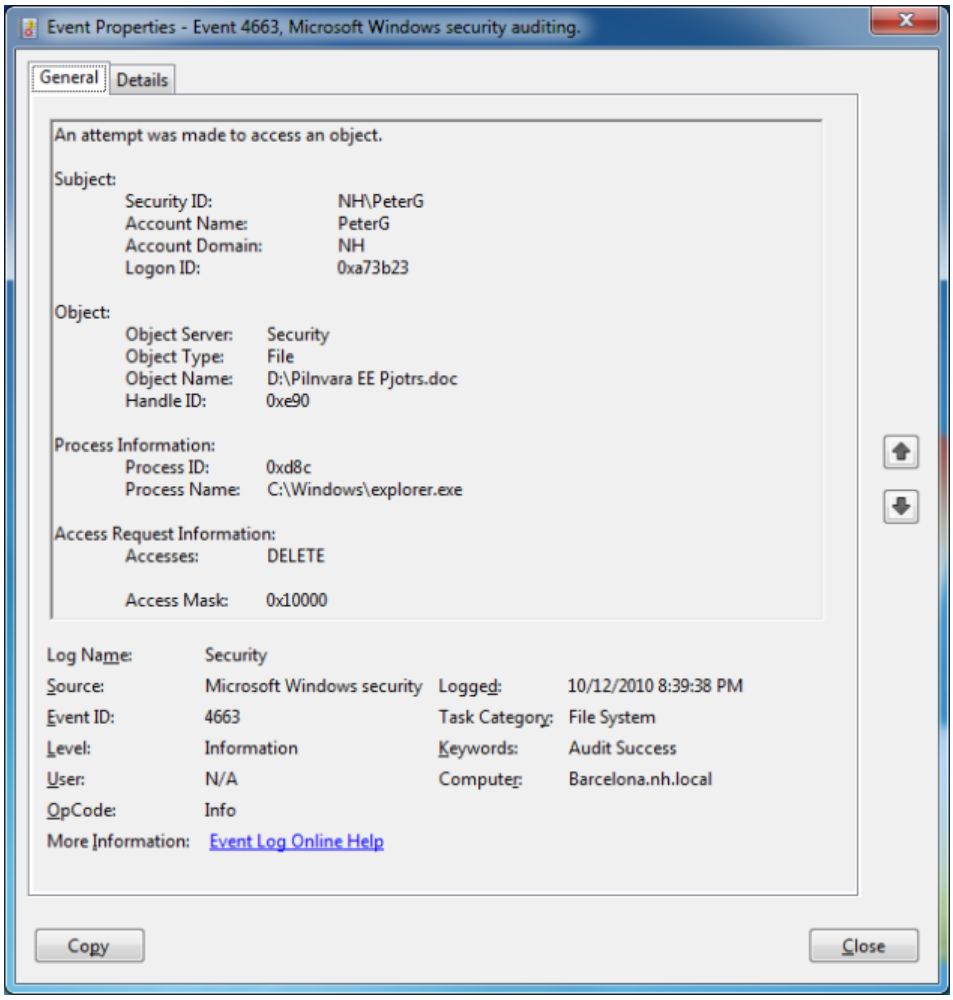


(https://windowsntlv.files.wordpress.com/2011/08/audit_details2003.png)

Итак, кто же удалил документы (Windows 2008/Vista)?

Нажмите **Start → Run → eventvwr.msc** и откройте для просмотра журнал **Security (Безопасность).** Журнал может быть заполнен событиями, прямого отношения к проблеме не имеющими. Щёлкнув правой кнопкой по журналу Security, выберите команду **View → Filter** и отфильтруйте просмотр по следующим критериям:

- Event Source: Security;
- Category: Object Access;
- Event Types: Success Audit;
- Event ID: 4663;



(https://windowsntlv.files.wordpress.com/2011/08/audit_events20081.png)

Не спешите интерпретировать все удаления как злонамеренные. Эта функция зачастую используется при обычной работе программ — например, исполненяя команду **Save (Сохранить),** программы пакета **Microsoft Office** сначала создают новый временный файл, сохраняют в него документ, после чего удаляют предыдущую версию файла. Аналогично, многие приложения баз данных при запуске сначала создают временный файл блокировок **(.lck),** затем удаляют его при выходе из программы.

Мне приходилось на практике сталкиваться и со злонамеренными действиями пользователей. Например, конфликтный сотрудник некоей компании при увольнении с места работы решил уничтожить все результаты своего труда, удалив файлы и папки, к которым он имел отношение. События такого рода хорошо заметны — они генерируют десятки, сотни записей в секунду в журнале безопасности. Конечно, восстановление документов из **Shadow Copies (Теневых Копий)** или ежесуточно автоматически создаваемого архива не составляет особого труда, но при этом я мог ответить на вопросы «Кто это сделал?» и «Когда это произошло?».

Last Content Update: 05-Oct-2010

FILED UNDER MICROSOFT WINDOWS: БЕЗОПАСНОСТЬ TAGGED WITH АНТИВИРУС, БЕЗОПАСНОСТЬ, СЛАВА ПРОТОКОЛУ, MICROSOFT, WINDOWS

9 Responses to *Применение Аудита Windows для отслеживания деятельности пользователей*

Андрей Маркин:
Понедельник, 12 - Март - 2012 в 19:22
Спасибо за интересную статью! Есть программа File Server Change Reporter http://www.netwrix.com/ru/file_server_auditing_change_reporting_freeware.html, которая позволяет осуществлять аудит изменений файлового сервера и устройств хранения, которую выпускает наша компания NetWrix.

Мы будем рады сотрудничеству с Вами!

Ответить

Алена:
Пятница, 27 - Декабрь - 2013 в 06:19
просто мега статья!!!Спасибо большущее!теперь слежу за всеми)

Ответить

Vova:
Среда, 22 - Январь - 2014 в 17:48
На Windows 7 это работает?

Ответить

Peter Gubarevich:
Четверг, 23 - Январь - 2014 в 20:25
Там скриншот с семёрки, неубедительно?

Ответить

Ал:
Суббота, 05 - Июль - 2014 в 09:16
Такое же окно и в Vista, так что не убедил

Ответить

Михаил:
Четверг, 26 - Март - 2015 в 10:26
Здравствуйте!
после настройки аудита согласно данной статье, журнал «Безопасность» начинают забивать события 5156 (Подключение платформы фильтрации) и 5145 (Сведения об общем файловом ресурсе), забивают очень быстро. Вопрос: как избавится от этих событий (чтобы они не писались в лог) ?

Ответить

Peter Gubarevich:
Четверг, 26 - Март - 2015 в 10:42
Для современных версий Windows делайте так:
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration

Оставьте там только действительно нужное.

Ответить

VN:
Четверг, 21 - Май - 2015 в 21:13
Приветствую,
у меня есть ситуация в домене W2K3 (в этом году таки мигрируем на W2K12) — нужно узнать кто удалил файл — погуглив я понял, что надо отфильтровать события 560 (инфа кто открывал и получал доступ, — по-моему Access: delete_open) и 564 (сам факт удаления файла, но не показывает кто удалял, почему и нужны эти 2 события) — а как это выгрузить Powershell'ом ?
Спасибо

Ответить

Peter Gubarevich:
Суббота, 23 - Май - 2015 в 21:22
Get-EventLog security | ?{$_.eventid -eq 560 -and $_.EntryType -eq «SuccessAudit» -and $_.message -like «*Accesses:`t%delete*»}

Ответить