Windows_logs

Пуск- Панель управления-Система безопасности-Администрирование-Просмотр событий-Журналы Windows

В Журнале Windows 5 вкладок, из которых 3 основных: "Приложение", "Безопасность", "Система":

1. **Журнал событий Приложений** содержит события, сгенерированные приложениями, а не системой. Например, сервер базы данных может записывать ошибки, возникающие при его работе в журнал приложений. Разработчики программ сами решают какие события имеет смысл протоколировать в журнале событий Приложения. Например, Microsoft SQL Server протоколирует подробную информцию о важных аварийных ситуациях возникающих при работе SQL-сервера, таких как "недостаточно памяти", "сбой при резервном копировании базы данных" и т.д. При этом события, сгенерированные разными приложениями, попадают в единый журнал приложений. Приложения идентифицируются как разные "источники" в базовом свойстве событий. Поэтому несложно выделить события конкретного приложения. Также стоит учитывать что ID события (код события) тоже определяется приложением, сгенерировавшим событие и коды могут дублироваться для разных источников. Таким образом события определенного типа идентифицируются и источником и кодом, а не только кодом, как для других журналов, например для журнала Безопасность. Эти данные могут пригодиться как системным администраторам и разработчикам программного обеспечения, так и обычным пользователям, желающим установить причину отказа той или иной программы.
2. **Журнал событий Безопасность** содержит события, влияющие на безопасность системы. Это попытки (и удачные и неудачные) входа в аккаунты системы, использование ресурсов (файлов, реестра, устройств), управление учетными записями, изменения прав и привилегий аккаунтов, запуск и остановка процессов (программ) и т.д. Администратор может сконфигурировать какие категории событий необходимо регистрировать. Например, по умолчанию система сконфигурирована регистрировать события управления учетными записями, события входа в систему, а аудит доступа к объектам не включен. Стоит быть осторожным при настройке аудита доступа к файлам, то это может привести к появлению большого

количества событий, что в свою очередь может негативно отразиться на общей производительности системы и быстрому переполнению журнала безопасности. Запись в журнал безопасности производится только системными компонентам, коды событий однозначно идентифицируют события. Журнал событий Безопасность является важным источником информации при расследовании инцидентов нарушения безопасности и его анализ актуален для администраторов безопасности, специалистов по информационной безопасности и специалистов по цифровой криминалистической экспертизе.

3. **Журнал событий Установки** содержит события, связанные с установкой приложений.
4. **Журнал событий Система** содержит события, сгенерированные системными компонентами. Например, отказы драйверов или других системных компонентов при запуске системы записываются в системный журнал событий. Типы и коды событий системных компонентов предопределены разработчиками операционной системы Windows. Аналогично журналу приложений, системный журнал содержит события из разных источников (системных компонентов) и следует учитывать что конкретные события идентифицируются не только кодом, но источником. Журнал событий Система - важный источник информации при поиске причин отказов и проблем системными администраторами и техническими специалистами.
5. В **журнале Перенаправленные события** сохраняются события, произошедшие на удаленных компьютерах.