Инструкция для открытия журнала событий Windows.

Основным предназначением Журнала событий в Windows 7/10 является сбор данных, которые могут пригодиться при устранении неисправностей в работе системы, программного обеспечения и оборудования. Впрочем, заносятся в него не только ошибки, но также и предупреждения, и вполне удачные операции, например, установка новой программы или подключение к сети.

Где находится журнал событий Windows

Физически Журнал событий представляет собой набор файлов в формате **EVTX**, хранящихся в системной папке *%SystemRoot%/System32/Winevt/Logs*.

Как открыть журнал

Запустить утилиту можно из классической Панели управления, перейдя по цепочке *Администрирование – Просмотр событий* или выполнив в окошке Run (Win+R) команду **eventvwr.msc**.

В левой колонке окна утилиты можно видеть отсортированные по разделам журналы, в средней отображается список событий выбранной категории, в правой – список доступных действий с выбранным журналом, внизу располагается панель подробных сведений о конкретной записи. Всего разделов четыре: настраиваемые события, журналы Windows, журналы приложений и служб, а также подписки. Наибольший интерес представляет раздел «Журналы Windows», именно с ним чаще всего приходится работать, выясняя причины неполадок в работе системы и программ. Журнал системных событий включает три основных и две дополнительных категории. Основные это **«Система», «Приложения» и «Безопасность»,** дополнительные – «Установка» и «Перенаправленные события».

Категория **«Система»** содержит события, сгенерированные системными компонентами – драйверами и модулями Windows.

Ветка **«Приложения»** включает записи, созданные различными программами. Эти данные могут пригодиться как системным администраторам и разработчикам программного обеспечения, так и обычным пользователям, желающим установить причину отказа той или иной программы.

Третья категория событий **«Безопасность»** содержит сведения, связанные с безопасностью системы. К ним относятся входы пользователей в аккаунты, управление учётными записями, изменение разрешений и прав доступа к файлам и папкам, запуск и остановка процессов и так далее.

Так как число событий может исчисляться тысячами и даже десятками тысяч, в eventvwr предусмотрена возможность поиска и фильтрации событий по свойствам – важности, времени, источнику, имени компьютера и пользователя, коду и так далее. Допустим, вы хотите получить список системных ошибок. Выберите слева *Журналы Windows – Система*, справа нажмите «Фильтр текущего журнала» и отметьте в открывшемся окне галочкой уровень события – пункты «Ошибка» и «Критическое». Нажмите «ОК» и утилита тут же отфильтрует записи.

Чтобы просмотреть конкретную запись, кликните по ней дважды – сведения откроются в окошке «Свойства событий».

Включение записи событий

По умолчанию запись событий на Windows 10 включена. Однако нелишним будет проверить работоспособность соответствующей службы — вдруг она не запускается в автоматическом режиме.

1. Щёлкаем правой кнопкой по «Пуску» и в контекстном меню выбираем пункт «Диспетчер задач». Можно также использовать сочетание клавиш Ctrl+Shift+Esc.
2. Переходим на вкладку «Службы».
3. Кликаем по ссылке «Открыть службы».

4. Перейти в список служб можно и другим способом, но это один из самых удобных.
5. Находим в списке «Журнал событий Windows».
6. Открываем свойства службы двойным кликом.
7. Устанавливаем тип запуска «Автоматически».
8. В поле «Состояние» нажимаем «Запустить».
9. Сохраняем конфигурацию, нажимая на кнопку «ОК».

ARP

Область применения: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012.

Отображает и изменяет записи в кэше протокола ARP. Кэш ARP содержит одну или несколько таблиц, которые используются для хранения IP-адресов и разрешенных физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного на компьютере, существует отдельная таблица. При использовании без параметров в **ARP** отображаются справочные сведения.

Синтаксис

```
arp [/a [<inetaddr>] [/n <ifaceaddr>]] [/g [<inetaddr>] [-n <ifaceaddr>]] [/d
<inetaddr> [<ifaceaddr>]] [/s <inetaddr> <etheraddr> [<ifaceaddr>]]
```

Параметры

Параметр	Описание
[/a [<inetaddr>] [/n <ifaceaddr>]	Отображает текущие таблицы кэша ARP для всех интерфейсов. Параметр **/n** учитывает регистр. Чтобы отобразить запись кэша ARP для определенного IP-адреса, используйте **ARP/a** с параметром **inetaddr** , где **inetaddr** — это IP-адрес. Если **inetaddr** не указан, используется первый подходящий интерфейс. Чтобы отобразить таблицу кэша ARP для определенного интерфейса, используйте параметр **/nifaceadd** в сочетании с параметром **/a** , где **inetaddr** — это IP-адрес, назначенный интерфейсу.
[/g [<inetaddr>] [/n <ifaceaddr>]	Идентично **/a**.

[/d <inetaddr> [<ifaceaddr>]	Удаляет запись с указанным IP-адресом, где **inetaddr** — это IP-адрес. Чтобы удалить запись в таблице для определенного интерфейса, используйте параметрifaceadd , гдеifaceadd — это IP-адрес, назначенный интерфейсу. Чтобы удалить все записи, используйте подстановочный знак звездочки (*) вместо **inetaddr**.
[/s <inetaddr> <etheraddr> [<ifaceaddr>]	Добавляет статическую запись в кэш ARP, которая разрешает IP-адрес **inetaddr** с физическим адресом **etheraddr**. Чтобы добавить статическую запись кэша ARP в таблицу для определенного интерфейса, используйте параметрifaceadd , где ifaceadd — это IP-адрес, назначенный интерфейсу.
/?	Отображение справки в командной строке.

Примеры

Чтобы отобразить таблицы кэша ARP для всех интерфейсов, введите:

Копировать
```
arp /a
```

Чтобы отобразить таблицу кэша ARP для интерфейса, которому назначен IP-адрес *10.0.0.99*, введите:

Копировать
```
arp /a /n 10.0.0.99
```

Чтобы добавить статическую запись кэша ARP, которая разрешает IP-адрес *10.0.0.80* к физическому адресу *00-AA-00-4F-2A-9C*, введите:

Копировать
```
arp /s 10.0.0.80 00-AA-00-4F-2A-9C
```

DriverQuery - **отобразить список установленных драйверов**. Команда DriverQuery позволяет администратору просмотреть список установленных драйверов устройств. Отображаемые данные могут быть представлены в виде списка, таблицы, или. CSV (Comma-Separated Values - значения, разделённые запятыми).