

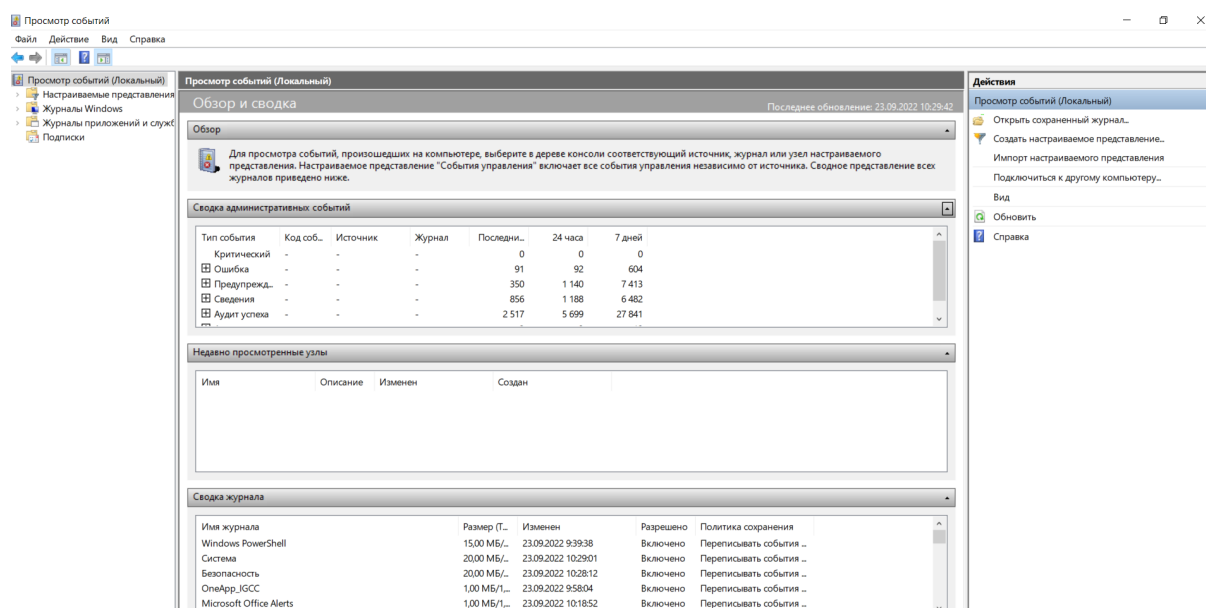
В процессе работы ОС Windows записывает часть данных в спец. документы (их еще называют логами или системными журналами). Как правило, под-запись попадают различные события, например, включение/выключение ПК, возникновение ошибок, обновления и т.д.

Разумеется, в некоторых случаях эти записи могут быть очень полезными. Например, при поиске причин возникновения ошибок, синих экранов, внезапных перезагрузок и т.д. Если установлена не официальная версия Windows — может так стать, что журналы будут отключены...

1. Щелкните **«Пуск»** и перейдите по надписи **«Панель управления»**.
2. Затем зайдите в раздел **«Система и безопасность»**.
3. Далее щелкайте по наименованию раздела **«Администрирование»**.
4. Попад в указанный раздел в перечне системных утилит ищите наименование **«Просмотр событий»**. Кликните по нему.
5. Целевой инструмент активирован. Чтобы конкретно попасть в журнал системы, кликните по пункту **«Журналы Windows»** в левой области интерфейса окошка.

Еще один способ: нажать сочетание **Win+X** — появится меню со ссылками на основные инструменты, среди которых будет и журнал событий.


«01.event»



«02.command_apr»

ARP - Отображает и изменяет вводимые данные в кэше протокола определения адреса ARP (Address Resolution Protocol).

arp -а команда отображает текущие таблицы ARP, опрашивая текущие данные протокола

 Командная строка

```
Microsoft Windows [Version 10.0.19044.2006]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\tnfla>arp -a

Интерфейс: 192.168.0.139 --- 0x9
    адрес в Интернете      Физический адрес      Тип
192.168.0.1                e8-65-d4-af-35-e0      динамический
192.168.0.100              00-15-00-d6-dc-97      динамический
192.168.0.169              9c-2e-a1-ce-ca-11      динамический
192.168.0.255              ff-ff-ff-ff-ff-ff      статический
224.0.0.22                 01-00-5e-00-00-16      статический
224.0.0.251                01-00-5e-00-00-fb      статический
224.0.0.252                01-00-5e-00-00-fc      статический
239.255.102.18             01-00-5e-7f-66-12      статический
239.255.255.250            01-00-5e-7f-ff-fa      статический
255.255.255.255            ff-ff-ff-ff-ff-ff      статический

C:\Users\tnfla>
```

«03.drivers»

Чтобы отобразить список установленных драйверов устройств на локальном компьютере, в командной строке ввести команду driverquery

Командная строка

Microsoft Windows [Version 10.0.19044.2006]

(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\tnfla>driverquery

Модуль	Название	Тип драйвера	Дата ссылки
1394ohci	1394 OHCI-совместимый	Kernel	
3ware	3ware	Kernel	19.05.2015 3:28:03
ACPI	Драйвер Microsoft ACPI	Kernel	
AcpiDev	Драйвер устройств с AC	Kernel	
acpiex	Microsoft ACPIEx Drive	Kernel	
acpiaggr	Драйвер агрегатора про	Kernel	
AcpiPmi	Драйвер устройства изм	Kernel	
acpitime	Драйвер ACPI Wake Alar	Kernel	
acsock	acsock	Kernel	11.03.2021 22:13:44
Asx01000	Asx01000	Kernel	
ADP80XX	ADP80XX	Kernel	10.04.2015 1:49:48
AFD	Драйвер дополнительных	Kernel	
afunix	afunix	Kernel	
ahcache	Application Compatibil	Kernel	
amdgpio2	Драйвер GPIO-клиента A	Kernel	07.02.2019 14:32:20
amdi2c	Служба контроллера I2C	Kernel	20.03.2019 9:57:33
AmdK8	AMD K8 драйвер процесс	Kernel	
AmdPPM	Драйвер процессора AMD	Kernel	
amdsata	amdsata	Kernel	14.05.2015 17:14:52
amdsbs	amdsbs	Kernel	12.12.2012 2:21:44
amdxata	amdxata	Kernel	01.05.2015 5:55:35
AppID	Драйвер AppID	Kernel	
applockerflt	Драйвер фильтра Smartl	Kernel	
AppvStrm	AppvStrm	File System	
AppvVemgr	AppvVemgr	File System	
AppvVfs	AppvVfs	File System	
arcsas	Adaptec SAS/SATA-II RA	Kernel	10.04.2015 0:12:07
aswArPot	aswArPot	Kernel	19.08.2022 0:22:46
aswbidsdriver	aswbidsdriver	File System	19.08.2022 0:24:40
aswbidsh	aswbidsh	File System	19.08.2022 0:24:32
aswbuniv	aswbuniv	File System	19.08.2022 0:24:33
aswElam	aswElam	Kernel	29.06.2022 17:24:37
aswKbd	aswKbd	Kernel	19.08.2022 0:22:49
aswMonFlt	aswMonFlt	File System	19.08.2022 0:22:56
aswNetHub	aswNetHub	Kernel	19.08.2022 0:23:24
aswRdr	aswRdr	Kernel	19.08.2022 0:22:49
aswRvrt	aswRvrt	Kernel	19.08.2022 0:22:57
aswSnx	aswSnx	File System	19.08.2022 0:23:04
aswSP	aswSP	File System	19.08.2022 0:23:20
aswStm	aswStm	Kernel	19.08.2022 0:23:17
aswVmm	aswVmm	Kernel	19.08.2022 0:23:08
AsyncMac	Драйвер асинхронного н	Kernel	
atapi	Канал IDE	Kernel	

Командная строка

VMSVSP	VmSwitch Extensibility	Kernel	
volmgr	Драйвер диспетчера том	Kernel	
volmgrx	Диспетчер динамических	Kernel	
volsnap	Драйвер теневого копир	Kernel	
volume	Драйвер тома	Kernel	
vpc	Виртуальная шина PCI M	Kernel	
vpcivsp	Сервер PCI Microsoft H	Kernel	
vpna	Cisco AnyConnect Secur	Kernel	01.05.2019 20:01:32
vsmraid	vsmraid	Kernel	23.04.2014 0:21:41
VSTXRAID	Драйвер RAID-контролле	Kernel	22.01.2013 0:00:28
vwifibus	Virtual Wireless Bus D	Kernel	
vwififlt	Virtual WiFi Filter Dr	Kernel	
vwifimp	Virtual WiFi Miniport	Kernel	
WacomPen	Wacom - драйвер пера п	Kernel	
wanarp	Драйвер IP ARP для уда	Kernel	
wanarpv6	Драйвер IPv6 ARP для у	Kernel	
wcifs	Windows Container Isol	File System	
wcnfs	Windows Container Name	File System	
WdBoot	Драйвер загрузки антив	Kernel	
Wdf01000	Служба платформ драйве	Kernel	
WdFilter	Драйвер с функцией мин	File System	
wdiwifi	WDI Driver Framework	Kernel	
WdmCompanion	WdmCompanionFilter	Kernel	
WdNisDrv	Системный драйвер пров	Kernel	
WFPLWFS	Платформа фильтрации M	Kernel	
WiManH	WiMan Service	Kernel	07.12.2021 18:19:27
WIMMount	WIMMount	File System	
WindowsTrust	Windows Trusted Execut	Kernel	
WindowsTrust	Служба безопасности до	Kernel	
WinMad	Служба WinMad	Kernel	19.06.2019 18:18:11
WinNat	Драйвер NAT Windows	Kernel	
WINUSB	Драйвер WinUsb	Kernel	
WinVerbs	Служба WinVerbs	Kernel	19.06.2019 18:18:12
WirelessButt	HP Wireless Button Dri	Kernel	12.11.2021 9:40:51
WmiAcpi	Microsoft Windows Mana	Kernel	
Wof	Windows Overlay File S	File System	
WpdUpFiltr	WPD Upper Class Filter	Kernel	
ws2ifsl	Драйвер WinSock IFS	Kernel	
WudfPf	User Mode Driver Frame	Kernel	
WUDFRd	Windows Driver Foundat	Kernel	
WUDFWpdFs	Драйвер файловой систе	Kernel	
WUDFWpdMtp	WUDFWpdMtp	Kernel	
xboxgip	Драйвер протокола игро	Kernel	
xinputhid	Драйвер-фильтр HID XIN	Kernel	

C:\Users\tnfla>_

04.command

Командлет `Get-EventLog` использует параметр `List` для отображения доступных журналов.

```
Администратор: Windows PowerShell
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\windows\system32> Get-EventLog -List

Max(K) Retain OverflowAction      Entries Log
-----
20 480    0 OverwriteAsNeeded      47 652 Application
3 906    0 OverwriteAsNeeded      5 690 Cisco AnyConnect Secure Mobility Client
20 480    0 OverwriteAsNeeded      0 HardwareEvents
512     7 OverwriteOlder        467 HP Analytics
4 096    7 OverwriteOlder        18 HP Sure Start
4 096    7 OverwriteOlder      0 HPNotifications Application
512     7 OverwriteOlder      0 IntelAudioServiceLog
512     7 OverwriteOlder      0 Internet Explorer
20 480    0 OverwriteAsNeeded      0 Key Management Service
128     0 OverwriteAsNeeded      1 545 OALerts
512     7 OverwriteOlder      3 474 OneApp_IGCC
20 480    0 OverwriteAsNeeded     30 965 Security
20 480    0 OverwriteAsNeeded     51 684 System
15 360    0 OverwriteAsNeeded     13 557 Windows PowerShell

PS C:\windows\system32>
```

05.command_current

Чтобы узнать, какая версия PowerShell установлена, необходимо запустите консоль PowerShell (или ISE), ввести `$PSVersionTable` и нажмите клавишу ВВОД. Найти значение `PSVersion`

```
Администратор: Windows PowerShell
PS C:\windows\system32> $PSVersionTable

Name Value
----
PSVersion 5.1.19041.1682
PSEdition Desktop
PSCompatibleVersions {1.0, 2.0, 3.0, 4.0...}
BuildVersion 10.0.19041.1682
CLRVersion 4.0.30319.42000
WSManStackVersion 3.0
PSRemotingProtocolVersion 2.3
SerializationVersion 1.1.0.1

PS C:\windows\system32>
```