Секреты работы с командной строкой в WINDOWS

Автор: Игорь Логинов
Источник: CHIP

Интерфейс командной строки

Итак, консоль командной строки присутствует во всех версиях операционных систем Windows. Ранние версии ОС поддерживали режим MS-DOS напрямую, что позволяло выполнять простые команды прямо из консоли. Представители же семейства NT, такие как Windows 2000 или Windows Server 2003, работают уже совсем по другим принципам, однако MS-DOS в них тоже поддерживается, но через виртуальную машину (NT Virtual DOS Machine, NTVDM), что позволяет контролировать и администрировать системные ресурсы прямо из консоли командного режима. В качестве интерпретатора командного режима выступает программа cmd.exe, запуск которой осуществляется через меню «Start -> Run». Кроме того, для запуска консоли можно воспользоваться элементом меню «Start -> All Programs -> Accessories -> Command Prompt».

Запустив консоль командного режима, пользователь может управлять ресурсами как локальной системы, так и ресурсами удаленной машины. Существуют команды, выполняющие мониторинг системы и выявляющие критические места в настройках сервера. Отличием работы из командной строки является полное отсутствие больших и громоздких графических утилит. Программы командной строки позволяют более тонкую настройку в виде параметров-ключей, указанных справа от самой команды.

С помощью специальных файлов-скриптов (наборов команд, выполняющихся последовательно или в запрограммированном порядке) администратор может свести к минимуму выполнение рутинных ежедневных операций. Существующие современные утилиты могут запускать такие скрипты с заданной периодичностью без присутствия администратора системы.

Сам администратор может выполнять как одиночные команды, так и список команд, используя специальные управляющие символы (&, |). Например:

```
Команда 1 & Команда 2 — сначала будет выполнена
Команда 1 и только затем Команда 2;

Команда 1 && Команда 2 — только после успешного
выполнения Команды 1 будет запущена Команда 2.
```

Существует возможность перенаправить выводимый программой поток напрямую в текстовый файл для дальнейшей обработки. Для этого необходимо использовать управляющий символ «>» и имя текстового файла. Пример вывода содержания текущего каталога в текстовый файл Report.txt при помощи команды dir приведен ниже:

```
dir> Report.txt
```

Администратор может запустить несколько копий консоли, вызвав в командной строке программу cmd.exe. Использование вложенной консоли позволяет работать с переменными окружения операционной системы без каких-либо последствий для всей системы в целом, так как после закрытия вложенной консоли изменения переменных окружения не сохраняются. Для контроля над этим процессом используются команды setlocal, endlocal и set.

В современных операционных системах существует множество команд и утилит. Запомнить такое количество различных программ, а тем более их параметров очень сложно, поэтому одним из самых важных параметров для каждой программы является сочетание символов /?. Выполнив команду с таким параметром, пользователь получит исчерпывающее сообщение о применении утилиты и синтаксисе ее параметров.

Обратите внимание, что на рисунке в левом верхнем углу следующей страницы использован сложный синтаксис. Так, сразу после команды shutdown /? после специального разделителя «|» идет команда more, что позволяет выводить информацию на экран не целиком, а определенными порциями, удобными для дальнейшего чтения.

Для того чтобы закрыть консоль командной строки, необходимо выполнить команду exit.

Кто здесь главный?

По своим возможностям консольные программы делятся на:

- команды управления операционной системой — это такие команды, как shutdown или taskkill;
- сетевые команды — net и ipconfig;
- команды для мониторинга системы — tasklist и systeminfo;
- команды для поддержки файловой системы — dir, mkdir, copy;
- команды для обслуживания жестких дисков — defrag и diskpart;
- команды для поддержки службы каталогов (Active Directories) — addrep и dsadd;
- вспомогательные команды, в этот раздел входят различные утилиты для создания сценариев, настройки принтеров, работы с переменными окружения и т. д.

Рассмотрим типичных представителей каждой группы и позволим себе дать некоторые рекомендациями по использованию включенных в них команд.

Команды мониторинга и диагностики

Для выявления неполадок в аппаратной части и проблем с программным обеспечением предназначены команды мониторинга, такие как systeminfo и tasklist. Эти утилиты впервые появились только в операционной среде Windows Server 2003, поэтому администраторы еще не в полной мере оценили функциональные возможности этих команд. Так, например, теперь не надо залезать в закладку «Свойства» иконки «Мой компьютер» — команда systeminfo напечатает на экране консоли основную информацию обо всех компонентах системы с полной расшифровкой. Параметр /s выведет информацию о любом удаленном компьютере. Например, для выяснения конфигурации компьютера TESTSERVER необходимо выполнить следующую команду:

```
systeminfo /s TESTSERVER
```

А утилита tasklist покажет процессы, запущенные на вашем компьютере.

Утилита tasklist позволяет опрашивать системы, соединенные в сеть. Параметр /v дает возможность получать подробные листинги с полезной информацией, в том числе и об именах пользователей, а параметр /т показывает процессы, загрузившие конкретный dll-файл. Другая полезная утилита — openfiles — позволяет получить информацию обо всех открытых файлах локальной и удаленной операционной системы. В прежних версиях операционных систем Windows приходилось использовать команду oh.exe, в современных

версиях достаточно выполнить в командной строке консоли команду, которая устанавливает режим мониторинга для всех открытых файлов системы:

```
openfiles /local on
```

Пользователь получит информацию обо всех открытых файлах системы, используя команду с простым синтаксисом:

```
openfiles
```

Команда openfiles с параметрами /query /v показывает, какие пользователи запустили процессы, открывшие файлы. С помощью других параметров-ключей можно задать различный режим вывода информации.

Команды управления операционной системой

Windows Server 2003 предоставляет администраторам новые команды, которые помогают не только диагностировать систему, но и управлять ею. К таким командам можно отнести утилиту shutdown. В качестве параметров-ключей этой утилиты можно использовать следующие:

- /s — полное штатное отключение системы;
- /r — перезагрузка;
- /p — выключение питания;
- /f — завершение работы активных приложений;
- /д — переход в режим пониженного энергопотребления;
- /I — завершение сеанса без отключения компьютера.

В виде средства, регистрирующего все штатные выключения компьютера, выступает обработчик событий штатных выключений (Shutdown Event Tracker), который собирает и диагностирует все отключения, выполненные администратором. Также предусмотрена возможность выключать систему с указанием причины, для этого необходимо использовать ключ /d.

Команда taskkill, аналог команды kill в операционных системах семейства *nix, позволяет «убить» зависшее приложение. Совместно с командой tasklist эти утилиты представляют собой мощное средство для оперативного вмешательства в ход выполнения приложений, представляющих потенциальную угрозу для производительности сервера. Из параметров этой команды необходимо отметить ключ/pid, который позволяет завершать процесс по его уникальному идентификатору, и ключ /im — для завершения приложения с указанным именем. Следующий пример позволяет завершить процессы с идентификаторами 1000 и 1240:

```
taskkill /pid 1000 /pid 1240
```

Команды для обслуживания жестких дисков

Оптимизацию жесткого диска позволяет выполнить команда defrag. Утилита умеет дефрагментировать диски с файловой системой FAT, FAT32 и NTFS. Defrag одинаково хорошо работает как с динамическим типом диска, так и с базовым. Синтаксис вызова этой команды следующий:

```
defrag диск [ -a j [ -f ] [ -v ] [ -? ]
```

Параметр -a предусматривает только анализ информации на диске, параметр -f — оптимизацию информации, в том числе и при отсутствии необходимого дискового пространства для создания временных файлов, а параметр -v — вывод отчета о ходе оптимизации. Не забудьте, что для успешной дефрагментации диск должен содержать как минимум 15% свободного места.

Команда fdisk уже не поддерживается ядром операционной системы Windows Server 2003. На смену ей пришла команда diskpart, также предназначенная для обслуживания жестких дисков. Разбить диск на разделы, создать логические диски, удалить их — вот лишь некоторые задачи, решаемые этой утилитой. В основном команда diskpart ориентирована на работу со специальными файлами-сценариями, в которых описаны процедуры обслуживания жестких дисков. Вот как выглядит вызов этой команды для файла-сценария Scriptl.txt:

```
diskpart /s Scriptl.txt
```

Каждая строка такого файла является инструкцией для какой-нибудь операции. Так, например, дает команду для создания нового раздела с определенным размером строка

```
create partition logical size=2048
```

Сетевые команды

Среди сетевых команд хотелось бы выделить две утилиты. Первая — это команда ipconfig, вторая — netstat. Системные администраторы используют эти команды не только для мониторинга сети, но и для защиты от опасных программ, пытающих установить контроль над системой.

При помощи утилиты ipconfig пользователь может узнать сетевой адрес своего компьютера, а вызвав эту команду с параметром /all, получить полную информацию о конфигурации сети на локальном компьютере. Параметр /renew позволяет изменить сетевые настройки без перезагрузки всей системы в целом.

Если вы заметили, что с вашим компьютером происходит что-то неладное, то в этом случае поможет команда netstat, которая не только укажет на открытые сетевые порты, по которым злоумышленники могли подсоединиться к вашей системе, но и идентифицирует процессы, запущенные на сервере без вашего ведома. Так, ключ /o выводит информацию об идентификаторе процесса (PID), использующего то или иное сетевое соединение. Существует возможность посмотреть, какие компьютеры в сети взаимодействуют с вашей локальной операционной системой.

Команды для поддержки службы каталогов

Вся сеть состоит из компонентов и представляет собой сложную иерархическую структуру, построенную в виде дерева. Объектами такой системы являются сайты, подсети, серверы, компьютеры, группы, пользователи, контакты, разделяемые сетевые устройства.

Для мониторинга такой сложной структуры в операционной системе предусмотрена команда dsquery, которая предназначена для расширенного поиска компонентов службы каталогов. Также этой командой можно пользоваться для вывода информации о свойствах выбранных компонентов (ключ -attr). Параметры -scope, -subtree, -onelevel, -base

определяют уровень вложенности поиска, а ключ -filter позволяет задействовать фильтр поиска.

Команда dsmod может помочь в случае необходимости модификации одной или нескольких учетных записей для выбранного компонента службы каталогов. Например, можно удалить пользователя из группы или назначить ему новый пароль. Пример изменения учетной записи для пользователя TestUser приведен ниже:

```
dsmod user

"CN=TestUser,CN=Users,DC=bigtex,DC=net
" -pwd Uf@tfmgerelt -mustchpwd yes
```

Команда dsmove перемещает объект в пределах текущего домена. При помощи ключей -newname и -newparent можно задавать новое имя объекта и менять его местоположение.

Команды для поддержки файловой системы

Описание некоторых часто употребляющихся команд для работы с файлами и директориями представлено в таблице. Команду deltree, которая выполняла каскадное удаление папок и файлов в них, заменяет теперь rmdir с ключом /s.

Команда	Описание
copy	копирует файлы
del	удаляет один или более файлов
dir	выводит список файлов и поддиректорий в выбранном каталоге
find	ищет заданную подстроку в файлах
move	перемещает файлы
mkdir	создает каталоги
rmdir	переименовывает и удаляет каталоги
tree	выводит иерархическое дерево всех файлов и поддиректорий в выбранном каталоге

Маленькие секреты большой системы

Изменение приглашения для командной строки

Найдите в реестре ключ: [HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\ Controf\Session\ Manager\Environment] Создайте в этом ключе строковый параметр «PROMPT» с типом (REG_EXPAND_SZ) и присвойте одно из следующих значений:

- $B — вертикальная черта «I»;
- $D — текущая дата;
- $G — знак больше «>»;
- $1_ — знак меньше «<»;
- $N — текущий диск;
  $P — текущий диск и путь;
- $Q — знак равно «=»;
- $T — текущее время;

- $V — версия Windows;
- $$ — знак доллара «$».

После перезагрузки вы увидите приглашение в определенном вами виде.

Автонабор команд

Для включения возможности автонабора команд по нажатию клавиши «Tab», найдите в реестре ключ: [HKEY_CURRENT_USER \Software \Microsoft \Command Processor]

Затем установите значение параметра CompletionChar равным 9, что соответствует идентификатору клавиши «Tab», закройте реестр и перезагрузите компьютер. В окне консоли, набирая часть имени команды, вы можете теперь нажать клавишу «Tab», и Windows автоматически подставит необходимую команду.

Изменение цвета консоли

Найдите в реестре ключ: [HKEY_CURRENT_USER\Software\Microsof t\Command Processor]

Измените параметр DefaultCoior. Значение -F0 определит вывод черного текста на белом фоне, а значение IE удивит вас желто-синей расцветкой консоли.

Быстрый запуск консоли командной строки из контекстного меню

Найдите в реестре ключ: [HKEY_CLASSES_ROOT \Directory \Shell]

Добавьте в него подразделы «CommandPrompt -> Command". Параметру Default ключа Command присвойте значение «cmd.exe /k cd "%1"».

Параметру Default ключа Command Prompt присвойте значение «Open Command Prompt".

Щелкнув правой кнопкой мыши на любой папке в Проводнике, можно выбрать команду Open Command Prompt, которая запустит консоль с командной строкой в нужной директории.

Заключение

Ну, вот и все. Мы рассказали об основах работы с консолью. Дальше предоставляем вам возможность самим исследовать функциональность и многообразие консольных команд. Только не забывайте заветный ключ /?, а остальное придет со временем и опытом.