МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «Воронежский государственный
технический университет»

Е.Н. Королев

СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

ВВЕДЕНИЕ

Операционная система представляет собой комплекс программ, обеспечивающий управление аппаратными средствами компьютера, организующий работу с файлами и выполнение прикладных программ, осуществляющий ввод и вывод данных.

Сегодня наиболее известными операционными системами являются операционные системы семейства Microsoft Windows и UNIX-подобные системы.

К основным функция операционных систем следует отнести следующие:

– исполнение запросов программ (ввод и вывод данных, запуск и остановка других программ, выделение и освобождение дополнительной памяти и др.);

– загрузка программ в оперативную память и их выполнение;

– стандартизованный доступ к периферийным устройствам;

– управление оперативной памятью, распределение памяти между выполняющимися процессами, организация виртуальной памяти;

– управление доступом к данным на энергонезависимых носителях таких как жесткий диск, оптические диски и прочие, организованным в той или иной файловой системе;

– обеспечение пользовательского интерфейса;

– сохранение информации об ошибках системы;

– параллельное или псевдопараллельное выполнение задач (многозадачность);

– эффективное распределение ресурсов вычислительной системы между процессами;

– разграничение доступа различных процессов к ресурсам;

– организация надежных вычислений (невозможности одного вычислительного процесса намеренно или по ошибке

повлиять на вычисления в другом процессе), основана на разграничении доступа к ресурсам;

– взаимодействие между процессами: обмен данными, взаимная синхронизация;

– защита самой системы, а также пользовательских данных и программ от действий пользователей (злонамеренных или по незнанию) или приложений;

– многопользовательский режим работы и разграничение прав доступа.

Цель администрирования ОС заключается в обеспечении ее надежного функционирования. К основным задачам администрирования ОС относятся следующие:

– добавление/удаление пользователей в систему;

– выбор настроек пользовательского окружения по умолчанию (политики групп);

– управление правами пользователей;

– разграничение прав доступа к различным ресурсам;

– установка и конфигурация драйверов устройств;

– разбиение винчестера на разделы;

– выбор размера виртуальной памяти, используемой системой;

– управление списком сервисов, запускаемых автоматически при загрузке ОС;

– конфигурация сетевых настроек;

– настройка брандмауэра (firewall);

– выбор стандартных переменных среды.

1. ОСНОВНЫЕ ЗАДАЧИ И ПРИНЦИПЫ АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ

Организация эффективной и надежной защиты операционной системы невозможна с помощью только программно-аппаратных средств. Эти средства обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита не будет эффективна.

К основным административным мерам защиты относятся следующие:

1. Постоянный контроль корректности функционирования операционной системы, особенно ее подсистемы защиты. Такой контроль наиболее удобно организовать, если операционная система поддерживает регистрацию событий (event logging). В этом случае операционная система автоматически регистрирует в специальном журнале (или нескольких журналах) наиболее важные события, произошедшие в процессе функционирования системы.

2. Организация и поддержание адекватной политики безопасности.

Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.

3. Инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой и контроль за соблюдением этих мер.

4. Регулярное создание и обновление резервных копий программ и данных операционной системы.

5. Постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы.

Основные принципы администрирования операционных систем:

– непрерывность;
– комплексность;
– актуальность;
– адекватность;
– непротиворечивость. (разграничение доступа, настроек процессов);
– формальный подход. Применение методик (инструкций, положений, приказов, РД и прочих рекомендательных документов) и четких концептуальных принципов при постановке задач администрирования и их реализации;
– подконтрольность.

Система информационной безопасности операционных систем обычно должна решать следующие задачи:

– ввод в систему списка имен пользователей и терминалов, допущенных к информации ОС;
– подготовку и запись паролей пользователей на носители;
– ввод в систему назначенных полномочий пользователей и терминалов;
– раздачу пользователям носителей с паролями и значений паролей, запоминаемых и вводимых пользователями вручную с клавиатуры;
– сбор сигналов несовпадения паролей и нарушения полномочий пользователей;
– установление времени, места и причины несанкционированного доступа;
– анализ ситуации, принятие адекватных мер и восстановление нормального функционирования ОС;
– контроль конфигурации системы;
– сбор сигналов вскрытия аппаратуры и контроль ввода (вывода) аппаратуры в ремонт и на профилактику;
– контроль функционирования системы защиты;

– подготовку ключей, контроль и обеспечение функционирования средств шифрования информации;

– регистрацию, учет и разграничение доступа к носителям информации и ПО;

– ведение статистики и прогнозирование не санкционированного доступа.

К системе безопасности ОС предъявляются также определенные требования:

– четкость определения полномочий и прав пользователей на доступ к определенным видам информации;

– предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;

– сведение к минимуму числа общих для нескольких пользователей средств защиты;

– учет случаев и попыток несанкционированного доступа к конфиденциальной информации;

– обеспечение оценки степени конфиденциальной информации;

– обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

2. АДМИНИСТРИРОВАНИЕ ОС WINDOWS

2.1 Использование командной строки

Командная среда – это программный продукт Microsoft, который обеспечивает связь между пользователем компьютера и операционной системой. Оболочка Windows использует интерпретатор cmd.exe и присутствует во всех версиях операционных систем Windows. Многие возможности и функции управления операционной системой недоступны из графического интерфейса и поэтому cmd является единственным средством доступа к этим инструментам.

Отличием работы из cmd является полное отсутствие больших и громоздких графических утилит. Пользовательский интерфейс текстовой строки предоставляет среду, в которой выполняются приложения и служебные программы.

Существует целый ряд команд, которые можно ввести для выполнения в командной строке. Для получения подробного списка команд, необходимо ввести в командной строке help, а затем нажать Enter. Чтобы унять больше о команде необходимо ввести имя_команды /?. К примеру, ping /?.

Таким образом, можно сделать вывод о том, что в руках профессионала командная строка может оказаться очень полезным и удобным инструментом, благодаря которому работа в системе Windows облегчается многократно, а для таких профессий, как системный администратор – станет незаменимым помощником в управлении сетью. Далее рассмотрим самые популярные команды администрирования операционных систем.

2.2 Команды для изучения системной информации

Команда WHOAMI сообщает имя пользователя, зарегистрированного в системе на данный момент, например, kor\Евгений;

Команда SYSTEMINFO выдает подробную информацию о конфигурации системы, в том числе сведения о версии, типе и изготовителе операционной системы, процессоре, версии BIOS, объеме памяти, региональных стандартах, часовом поясе и конфигурации сетевого адаптера.

Формат командной строки:

SYSTEMINFO [/S <система> [/U <пользователь> [/P [<пароль >]]]] [/FO формат] [/NH]

Список параметров:

/S <система>

Подключаемый удаленный компьютер.

/U [<домен>\]<пользователь>

Пользовательский контекст, в котором должна выполняться эта команда.
/P [<пароль>]
Пароль для этого пользовательского контекста. Запрашивает ввод пароля, если он не задан.
/FO <формат>
Описание формата выходного файла. Допустимые значения: "TABLE", "LIST", "CSV".
/NH
Отключение отображения заголовка "Column Header" в выходных данных. Допустимо для форматов "TABLE" и "CSV".
/? Вывод справки по использованию.

Команда Ipconfig представляет собой утилиту командной строки для вывода деталей текущего соединения и управления клиентскими сервисами DHCP и DNS. Используется для отображения текущих настроек протокола TCP/IP.

Примеры использования:

ipconfig – отобразить базовые сетевые настройки для всех сетевых адаптеров, присутствующих в системе.

ipconfig /all – отобразить подробную информацию о настройках всех сетевых адаптеров, присутствующих в системе.

По умолчанию (без обозначения параметров) выводится только IP-адрес, маска подсети и основной шлюз для каждого адаптера, связанного с TCP/IP. При вводе /all Ipconfig выводит все текущие значения конфигурации TCP/IP, в том числе IP-адрес, маску подсети, основной шлюз и конфигурацию служб WINS (Windows Internet Naming Service, служба имен Интернета Windows) и DNS.

Команда NETSTAT предназначена для получения сведений о состоянии сетевых соединений и слушаемых на данном компьютере портах TCP и UDP, а также, для отображения статистических данных по сетевым интерфейсам и протоколам.

Пример отображаемой информации:

Активные подключения

Имя	Локальный адрес	Внешний адрес	Состояние
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	192.168.0.3:5401	17.11.13.23:551	ESTABLISHED
TCP	127.0.0.1:56635	127.0.0.1:443	ESTABLISHED

Имя – название протокола. Локальный адрес – локальный IP-адрес участвующий в соединении или связанный со службой, ожидающей входящие соединения (слушающей порт). Если в качестве адреса отображается 0.0.0.0, то это означает – "любой адрес", то есть в соединении могут использоваться все IP-адреса существующие на данном компьютере. Адрес 127.0.0.1 – это петлевой интерфейс, используемый в качестве средства IP протокола для взаимодействия между процессами без реальной передачи данных.

Внешний адрес — это внешний IP-адрес, участвующий в создании соединения. Состояние — состояние соединения. Состояние Listening говорит о том, что строка состояния отображает информацию о сетевой службе, ожидающей входящие соединения по соответствующему протоколу на адрес и порт, отображаемые в колонке "Локальный адрес ". Состояние ESTABLISHED указывает на активное соединение. В колонке "Состояние" для соединений по протоколу TCP может отображаться текущий этап TCP-сессии определяемый по обработке значений флагов в заголовке TCP - пакета (Syn, Ask, Fin). Возможные состояния:

- CLOSE_WAIT – ожидание закрытия соединения.
- CLOSED – соединение закрыто.
- ESTABLISHED – соединение установлено.
- LISTENING – ожидается соединение (слушается порт).
- TIME_WAIT – превышение времени ответа.

Утилита BOOTSECT.EXE позволяет изменить программный код загрузчика Windows для переключения между двумя вариантами диспетчера загрузки – BOOTMGR или NTLDR. Загрузчик ntldr использовался до появления операци-

онной системы Windows Vista. В процессе начальной загрузки, программный код загрузочного сектора раздела (PBR – Partition Boot Record) обеспечивал поиск, считывание в память и передачу управления файлу ntldr, который размещался в корневом разделе загрузочного диска. Конфигурирование загрузчика ntldr выполнялось с помощью простого текстового файла boot.ini, содержимое которого задавало список загружаемых операционных систем, их параметры загрузки, размещение системных файлов и т.п.

В операционных системах Windows Vista /Server 2008 и более поздних, загрузчик ntldr не используется, и заменен диспетчером загрузки bootmgr. Соответственно, изменился и программный код загрузочного сектора раздела, обеспечивающий передачу управления файлу bootmgr. Новый диспетчер загрузки использует собственные данные конфигурации загрузки (Boot Configuration Data – BCD) и может выполнять, при определенных настройках, загрузку любых операционных систем семейства Windows. Загрузчик ntldr не поддерживает возможность загрузки Windows Vista и старше. Для его конфигурирования используется команда BCDEDIT.

Команда BOOTSECT позволяет записывать заданный программный код загрузочных секторов, обеспечивающих загрузку либо ntldr, либо bootmgr.

Формат командной строки:

bootsect {/help|/nt60|/nt52} {SYS|ALL|:} [/force] [/mbr]

Параметры командной строки Bootsect:

/help – отображение справочной информации;

/nt52 – запись программного кода загрузочного сектора, обеспечивающего использование загрузчика ntldr для операционных систем, предшествующих Windows Vista.

/nt60 – запись программного кода в загрузочные сектора для обеспечения загрузки файла bootmgr – диспетчера загрузки Windows Vista/Server 2008 и более поздних ОС семейства Windows.

SYS – запись будет выполнена в секторы системного раздела, который использовался для загрузки Windows, в среде которой выполняется данная команда.

ALL – запись программного кода будет выполнена для всех существующих разделов, которые могут быть использованы для загрузки Windows.

DriveLetter – буква диска, для которого будет выполнена перезапись программного кода загрузочных секторов.

/force – принудительное отключение используемых другими программами томов дисков для обеспечения монопольного доступа утилиты bootsect.exe

/mbr – изменение программного кода главной загрузочной записи (MBR - Master Boot Record) без изменения таблицы разделов диска. При использовании с параметром /nt52, MBR будет совместима с предшествующими Windows Vista версиями. При использовании с параметром /nt60 - MBR будет совместима с операционными системами Windows Vista и более поздними.

Примеры:

bootsect /nt52 E: – создать для диска E: загрузочные записи для операционных систем Windows XP/2000/NT, т.е для загрузки на базе ntldr.

bootsect /nt60 /mbr C: – изменить загрузочные сектора диска C: для обеспечения загрузки диспетчера bootmgr.

bootsect /nt60 SYS – изменение загрузочных секторов для раздела, с которого выполнена загрузка текущей ОС Windows.

2.3 Конфигурирование загрузчика операционной системы

Команда BCDEDIT применяется в операционных системах Windows Vista и старше для редактирования данных конфигурации загрузки операционной системы (BCD – Boot Configuration Data).

При загрузке операционной системы, сначала считывается первый сектор с устройства загрузки, представляющий собой главную загрузочную запись (Master Boot Record – MBR). Стандартно, в качестве MBR выступает первый сектор загрузочного диска. MBR содержит список разделов, признак активного раздела (раздела, с которого будет выполняться загрузка ОС), некоторые служебные данные, а также программный код для считывания в память загрузочного сектора активного раздела (Partition Boot Record – PBR) и передачи ему управления. Программный код PBR, в случае загрузки операционных систем Windows Vista и старше, должен обеспечить поиск, считывание и передачу управления диспетчеру загрузки bootmgr, который и будет продолжать процесс загрузки системы. В соответствии с конфигурацией загрузки, диспетчер BOOTMGR может выполнить загрузку ядра Windows или, например, Linux, загрузить диагностические программы, выполнить загрузку ядра с измененными параметрами.

Обычно файл bootmgr имеет атрибуты "скрытый" и "системный". Код диспетчера загрузки, получив управление, выполняет поиск и обработку данных конфигурации загрузки (файл BCD в папке \BOOT\ активного раздела), в соответствии с которыми выполняется дальнейшие этапы загрузки (отображение меню, выбор загружаемой ОС или средств диагностики, загрузка ядра и т. п.). По типу структуры, файл \\boot\BCD является кустом реестра и отображается в редакторе реестра Windows как раздел HKEY_LOCAL_MACHINE\BCD00000000.

Данный раздел реестра обрабатывается диспетчером загрузки bootmgr и в редакторе реестра имеет разрешение только на чтение. Разрешение на запись можно установить через контекстное меню редактора.

Средство командной строки bcdedit.exe позволяет редактировать данные конфигурации загрузки и входит в состав стандартных программ, а также может использоваться при загрузке с установочного диска системы или диска аварийного восстановления. Естественно, для изменения конфигурации

загрузки Windows, программа должны быть запущена с правами администратора.

Данные конфигурации загрузки можно условно разделить на 3 основных элемента:

– хранилище BCD (Store);

– записи в хранилище (Entries);

– параметры записей (Entry Options).

Иерархически, хранилище можно представить в виде совокупности объектов (Objects), состоящих из элементов (Elements). Например, объектом конфигурации является группа элементов, обеспечивающих загрузку отдельной ОС. BCDEDIT позволяет удалять, создавать, копировать и изменять объекты и элементы конфигурации загрузки BCD. Если в командной строке bcdedit не задан ключ /store – то ее действие выполняется по отношению к системному хранилищу (активной конфигурации, используемой для данной загрузки).

Хранилище данных конфигурации загрузки (BCD) заменяет собой простой текстовый файл Boot.ini, использовавшийся в операционных системах Windows NT/2000/XP для загрузчика ntldr. Данные конфигурации в более поздних версиях Windows хранятся в виде специальных программных объектов, не являющихся текстовыми элементами. Каждый объект данных конфигурации BCD имеет глобальный уникальный идентификатор. Обозначается GUID в виде наборов шестнадцатеричных цифр, разделяемых дефисами для удобства записи, и заключенными в фигурные скобки:

{166769E1-88E8-11CF-A6BB-0080C7B2D6A2}

Некоторые из объектов хранилища кроме идентификаторов GUID, могут также иметь псевдонимы для удобства использования, например, {bootmgr} (соответствует диспетчеру загрузки) и {default} (соответствует используемому по умолчанию загрузчику Windows). Для отключения использования псевдонимов в командной строке bcdedit предусмотрен ключ /v:

bcdedit /v позволяет отобразить данные текущей системной конфигурации загрузки без использования псевдонимов (только с идентификаторами GUID).

Для определения конфигурации приложения загрузки системы (OSLOADER) используется несколько десятков типов данных, которые можно разделить на группы – Загрузка, Отображение, Память и т.д. В стандартной конфигурации, большинство из дополнительных параметров приложения OSLOADER не нужны, и принимают значения, необходимые для обычной загрузки Windows. В некоторых случаях, может потребоваться изменение параметров распределения памяти, адресного пространства, уровня детализации журнала и т.п. Так, например, для 32-битных операционных систем семейства Windows, по умолчанию каждому пользовательскому процессу отводится виртуальное адресное пространство размером 2Гб, независимо от объема реальной памяти. В большинстве случаев, этого вполне достаточно для работы приложений, но при необходимости, его можно увеличить, указав параметр INCREASEUSERVA (целое число):

bcdedit /set increaseuserva 3072 – установить размер виртуального адресного пространства для приложений равным 3 Гб.

bcdedit /set increaseuserva 2048 – установить размер виртуального адресного пространства для приложений равным 2 Гб.

bcdedit /deletevalue increaseuserva – удалить параметр INCREASEUSERVA из конфигурации загрузки.

Действие данной команды, аналогично предыдущей, поскольку отсутствие элемента INCREASEUSERVA предполагает, что будет задано адресное пространство размером 2Гб. Естественно, это верно только для 32-разрядных ОС, поскольку для 64-разрядных, размер адресного пространства – 4Гб.

Просмотреть текущие параметры для приложения загрузки Windows можно с помощью команды: bcdedit /enum osloader.

Примеры использования bcdedit для сохранения и восстановления конфигурации:

bcdedit /export C:\Backup\BCD2012 – сохранение текущей системной конфигурации в файл bcd2012 каталога C:\Backup\. Каталог, куда выполняется сохранение, должен существовать. При наличии пробелов в пути, используются двойные кавычки:

bcdedit /export "C:\My Backup\BCD2012"

Для восстановления конфигурации из ранее сохраненной копии используется команда: bcdedit /import C:\backup\bdc2012.

Команда BCDEDIT без параметров выводит текущую конфигурацию загрузки на экран. Для использования команды в командных файлах или применения последующих команд, полезно иметь текстовый файл с результатами выполнения команды, для чего можно воспользоваться стандартным приемом - перенаправлением вывода в текстовый файл:

BCDEDIT > C:\bcdconf.txt – сохранить результаты отображения текущей конфигурации загрузки в текстовом файле C:\bcdconf.txt

BCDEDIT /v > C:\bcdconf.txt – сохранить результаты отображения текущей конфигурации загрузки в текстовом файле C:\bcdconf.txt с выводом полных GUID вместо псевдонимов.

bcdedit /timeout 40 - установить время ожидания выбора системы для загрузки равным 40 секунд.

bcdedit /displayorder {ntldr} {current} – установить порядок отображения загружаемых ОС – сначала Windows XP (идентификатор - {ntldr}), затем – Windows 7 (идентификатор – {current})

bcdedit /default {ntldr} – установить в качестве загружаемой по умолчанию системы Windows XP.

bcdedit /default {current} – установить в качестве загружаемой по умолчанию системы текущую ОС, в среде которой выполняется команда bcdedit, т. е. – в данном примере конфигурации BCD – Windows 7. При необходимости выбора дру-

гой ОС, не являющейся текущей, нужно указывать ее GUID – bcdedit /default {d1f837a3-7e0f-11df-bc8b-f6edb78d41b5}

Для просмотра отдельных категорий или полного перечня параметров конфигурации загрузки используется команда BCDEDIT /enum . Эта команда перечисляет все записи в хранилище. Команда /enum используется по умолчанию, поэтому использование "bcdedit" без параметров эквивалентно "bcdedit /enum ACTIVE".

Примеры:

bcdedit /enum OSLOADER – отобразить все записи для загрузчика операционной системы:

bcdedit /enum BOOTMGR – отобразить все записи диспетчера загрузки.

Для добавления новых записей в хранилище BCD используется команда bcdedit /create. Эта команда создает новую запись в хранилище данных конфигурации загрузки. Если указан известный идентификатор, то указание параметров /application, /inherit и /device не требуется.

Самый простой способ добавления новых записей - для стандартных загрузчиков и с использованием псевдонимов.

bcdedit /create {ntldr} /d "Загрузчик ОС прежних версий"– для создания новой записи в текущей конфигурации загрузки для операционных систем Windows NT/2000/XP

bcdedit /create /d "Windows Vista" /application osloader – для создания новой записи конфигурации загрузки для Windows Vista и старше.

Нужно учитывать, что команда /create всего лишь создает новую запись в хранилище данных конфигурации и сообщает пользователю ее идентификатор GUID. Для создания работоспособной конфигурации загрузки этого недостаточно - необходимо еще задать необходимые параметры для записи, соответствующей данному GUID. Значения параметров определяются в зависимости от типа загружаемой системы, особенностей ее загрузчика места нахождения файлов и каталогов.

Создать необходимые параметры данной записи для передачи управления загрузчику Windows XP:

bcdedit /set device=partition=z. где Z: – буква диска, где находится диспетчер загрузки.

Пример создания конфигурации загрузки Windows XP с помощью команды bcdedit:

bcdedit /create {ntldr} /d "Microsoft Windows XP" - создать объект для загрузки Windows XP

bcdedit /set {ntldr} device partition=C: – указать устройство загрузки (активный раздел)

bcdedit /set {ntldr} path \ntldr – указать путь к загрузчику ntldr

bcdedit /displayorder {ntldr} /addlast – добавить в конец меню выбора вариантов загрузки новый пункт.

При создании новой записи можно сохранить созданный GUID: bcdedit /create /device > ramdevice.txt – GUID нового устройства будет записан в текстовый файл ramdevice.txt для удобства использования его в последующих командах

Диспетчер загрузки bootmgr позволяет выполнить загрузку операционных систем с использованием приложения загрузочного сектора (/application BOOTSECTOR). Обычно такой метод загрузки используется для операционных систем Linux/Unix. Конфигурация загрузки BCD создается таким образом, чтобы диспетчер bootmgr мог выполнить загрузку и передачу управления программе загрузочного сектора раздела PBR загружаемой ОС. Таким образом, кроме записи конфигурации BCD, для успешного выполнения загрузки, требуется специальный файл с копией загрузочной записи PBR. Утилита bcdedit.exe не предназначена для создания приложений загрузки (как bootsector, так и прочих) и используется только для конфигурирования данных хранилища загрузки. Для создания копии загрузочной записи раздела PBR потребуются другие программные средства, набор которых довольно обширен и определяется типом операционной системы (DD в

Linux, Grub4DOS в Windows, дисковые утилиты с функцией посекторного копирования загрузочных записей в файл и т. п.). Пример создания конфигурации загрузки для операционной системы Linux:

bcdedit /create /d "Linux OS" /application BOOTSECTOR – создать запись в системном хранилище конфигурации для объекта приложения загрузочного сектора. Полученный при выполнении данной команды идентификатор {GUID} используется в последующих командах, определяющих значение элементов объекта.

bcdedit /set {GUID} device partition=C: - буква или диск для активного раздела.

bcdedit /set {GUID} path \grub.pbr путь к файлу, содержащему загрузочную запись PBR.

bcdedit /displayorder {GUID} /addlast - добавит новый пункт в конец меню выбора операционных систем.

2.4 Работа с сетевыми ресурсами

Утилита NET.EXE существует во всех версиях Windows и является одной из самых используемых в практической работе с сетевыми ресурсами. Позволяет подключать и отключать сетевые диски, запускать и останавливать системные службы, добавлять и удалять пользователей, управлять совместно используемыми ресурсами, отображать статистические данные об использовании ресурсов и многое другое.

Выполнение команды net без параметров вызывает краткую справку со списком возможных уровней использования, запуск с параметром help позволяет получить более подробную информацию об использовании net.exe.

Net.exe может использоваться для работы с системными службами. Данный режим использования NET.EXE, в некоторой степени, является не характерным для основного предназначения утилиты, и начиная с Windows XP, для управления системными службами используется специальная утилита командной строки SC.EXE. Тем не менее, NET.EXE в

среде любой версии операционных систем Windows может быть использована для запуска и остановки системных служб (сервисов). Согласно справочной информации, список служб, которыми можно управлять с помощью net.exe можно получить используя следующую команду:

net help services

Но это не совсем верно, и на самом деле, с помощью net.exe можно запустить или остановить практически любую системную службу, и в том числе, не представленную в списке, отображаемом при выполнении данной команды. Для остановки используется параметр stop, а для запуска - параметр start:

net stop dnscache – остановить службу dnscache

net start dnscache – запустить службу dnscache

Возможно использование как короткого, так и полного имени ("Dnscache" – короткое, "DNS-клиент" - полное имя службы). Имя службы, содержащее символы русского алфавита и пробелы заключается в двойные кавычки.

net stop "DNS-клиент" – остановить службу DNS-клиент.

Полное имя службы можно скопировать из "Панель управления" – "Администрирование" – "Службы" – Имя службы – "Свойства" – "Выводимое имя".

Для приостановки некоторых системных служб или продолжения работы ранее приостановленной службы используются команды NET PAUSE и NET CONTINUE:

net pause "Планировщик заданий" – приостановить службу "Планировщик заданий"

net continue schedule – продолжить работу службы "Планировщик заданий". Имя службы задано в коротком формате.

Net.exe может использоваться для работы с сетевыми дисками.

Примеры выполнения команды NET USE для подключения сетевых дисков:

net use X: \\server\shares – подключить сетевой диск X: которому соответствует разделяемый сетевой каталог с именем shares на компьютере с именем server.

Примонтируем сетевой диск под буквой X, расположенный на сервере \\VasyaServer\Share, имя пользователя VASYA, домен VASYADOMAIN, пароль 12345. Для этого нужно выполнить следующую команду:

net use x: \\VasyaServer\Share /user:VASYADOMAIN\VASYA 12345

Пример размонтирования диска:

net use x: /delete

Для изменения режима запоминания подключенных сетевых дисков используется ключ /PERSISTENT

net use /PERSISTENT:NO – не запоминать сетевые подключения.

net use /PERSISTENT:YES – запоминать сетевые подключения.

Необходимо учитывать, что режим, определяемый значением ключа /PERSISTENT, относится к вновь создаваемым подключениям. Если, например, сетевой диск X: был создан при установленном режиме запоминания (PERSISTENT:YES), а затем вы выполнили смену режима командой net use /PERSISTENT:NO и подключили сетевой диск Y: , то после перезагрузки системы, не будет восстановлено подключение диска Y: , но будет восстановлено подключение диска X:

NET SHARE – эта команда позволяет выделить ресурсы системы для сетевого доступа. При запуске без других параметров, выводит информацию обо всех ресурсах данного компьютера, которые могут быть совместно использованы. Для каждого ресурса выводится имя устройства или путь и соответствующий комментарий.

net share – получить список разделяемых в локальной сети ресурсов данного компьютера.

Для добавления нового разделяемого по сети ресурса используется:

net share TEMP="C:\Documents And Settings\LocalSettings\games" – добавить новый разделяемый каталог под именем TEMP

net share TEMP="C:\Documents And Settings\LocalSettings\games" /users:5 – добавить новый разделяемый каталог под именем TEMP с максимальным числом одновременно подключающихся пользователей равным 5.

Для удаления существующего разделяемого ресурса используется параметр /DELETE:

net share TEMP /DELETE - удалить разделяемый ресурс под именем TEMP

Удаление выполняется только для имени разделяемого ресурса и не затрагивает каталог локального диска, связанный с данным именем. Для получения списка компьютеров домена с разделяемыми ресурсами используется команда

net view - отобразить список компьютеров в сетевом окружении.

net view | more – отобразить список компьютеров в постраничном режиме вывода на экран.

net view > C:\computers.txt – отобразить список компьютеров с записью результатов в текстовый файл.

Утилита NET.EXE позволяет отобразить данные об учетных записях пользователей и групп, добавлять новые записи, удалять существующие, отображать параметры безопасности, связанные с авторизацией пользователей и некоторые другие операции по администрированию на локальном компьютере или контроллере домена.

NET ACCOUNTS – эта команда используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON). При использовании этой команды без указания параметров, выводятся текущие значения параметров, определяющих требования к паролям и входу в сеть, – время принудительного завершения сессии, минимальную длину пароля, максимальное и минимальное время действия пароля и его уникальность.

Синтаксис команды NET USER:

net user [имя_пользователя [пароль | *] [параметры]] [/domain]
net user имя_пользователя {пароль | *} /add [параметры] [/domain]
net user имя_пользователя [/delete] [/domain], где

– имя_пользователя – указывает имя учётной записи пользователя, которую можно добавить, удалить, отредактировать или просмотреть. Имя может иметь длину до 20 символов.

– пароль – присваивает или изменяет пароль пользователя. Введите звездочку (*) для вывода приглашения на ввод пароля. При вводе с клавиатуры символы пароля не выводятся на экран.

– /domain – выполняет операцию на контроллере основного для данного компьютера домена.

– параметры – задает параметр командной строки для команды.

– net help команда – отображение справки для указанной команды net.

– /delete – удаление учетной записи пользователя.

Дополнительные параметры команды NET USER:

– /active:{yes | no} - активирует или деактивирует учетную запись. Если учетная запись не активирована, пользователь не может получить доступ к серверу. По умолчанию учетная запись активирована.

– /comment:"текст" – позволяет добавить описание учетной записи пользователя (максимум 48 символов). Текст описания заключается в кавычки.

– /countrycode:*nnn* – использует код страны, указанный для операционной системы, для реализации соответствующих языковых файлов при отображении пользовательской справки и сообщений об ошибках. Значение 0 соответствует коду страны, используемому по умолчанию.

– /expires:{дата | never} – дата истечения срока действия учетной записи. Значение never соответствует неогра-

ниченному сроку действия. Дата указывается в формате мм/дд/гг или дд/мм/гг в зависимости от кода страны. Месяц может указываться цифрами, полностью или в сокращенном виде (тремя буквами). Год может указываться двумя ли четырьмя цифрами. Элементы даты разделяются слэшем (/) без пробелов.

– /fullname:"*имя*" – полное имя пользователя (в отличии от имени учетной записи пользователя). Имя указывается в кавычках.

– /homedir:*путь* – указывает путь к домашнему каталогу пользователя. Указанное место должно существовать.

– /passwordchg:{yes | no} –указывает, может ли пользователь изменять свой пароль (по умолчанию может).

– /passwordreq:{yes | no} – указывает, должна ли учетная запись пользователя иметь пароль (по умолчанию должна).

– /profilepath[:путь] – указывает путь к профилю входа в систему пользователя.

– /scriptpath:*путь* – путь к сценарию, используемому пользователем для входа в систему.

– /times:{время | all} – время для входа в систему. Параметр время указывается в формате день[-день][,день[-день]],час [-час][,час [-час]], причем приращение равняется 1 часу. Название дней недели могут указываться полностью или в сокращенном виде. Часы могут указываться в 12- или 24-часовом представлении. Для 12-часового представления используются обозначения am, pm, a.m. или p.m. Значение all соответствует отсутствию ограничений на время входа в систему, а пустое значение обозначает полный запрет на вход в систему. Значения дней недели и времени разделяются запятой; несколько записей для значений дней недели и времени разделяются точкой с запятой.

– /usercomment:"текст" – позволяет администратору добавить или изменить комментарий к учетной записи.

– /workstations:{имя_компьютера[,...] | *} – позволяет указать до 8 компьютеров, с которых пользователь может войти в сеть. Если для параметра /workstations не указан список компьютеров или указано значение *, пользователь может войти в сеть с любого компьютера.

Примеры использования:

– net user – отобразить список пользователей;

– net user /DOMAIN – отобразить список пользователей текущего домена;

– net user VASYA /USERCOMMENT:"Тестовый пользователь " /add – добавить пользователя с именем VASYA;

– net user VASYA /delete – удалить созданного пользователя;

– net user VASYA * –изменить пароль существующего пользователя VASYA. Новый пароль будет запрошен при выполнении команды.

Пример последовательности команд для создания нового пользователя с правами локального администратора:

net user VASYA Boss /ADD – создание учетной записи пользователя VASYA с паролем Boss;

net localgroup Администраторы VASYA /ADD – добавление пользователя в группу "Администраторы".

Для добавления учетной записи пользователя Petr с полным именем пользователя и правом на подключение с 8 до 17 часов с понедельника по пятницу используется следующая команда:

net user petr /add /times:Пн-Пт,08:00-17:00/fullname:"Petr".

2.5 Работа с точками подключения

Команда MOUNTVOL позволяет создавать, удалять и просматривать точки подключения томов (точки монтирования) в командной строке Windows. Точки монтирования доступны при использовании файловой системы NTFS. В среде операционных систем семейства Windows, существует два ви-

да точек монтирования: точка монтирования каталога (англ. junction point) и точка монтирования тома (англ. volume mount point). Создание точек монтирования первого типа осуществляется через консольную команду mklink /J, создание точек монтирования второго типа — через команду mountvol. На практике утилита mountvol используется для изменения конфигурации томов, автоматически смонтированных операционной системой, подключения томов без назначения букв дискам, увеличения свободного места на томе или замены жесткого диска, с использованием подключения к какому-либо его пути другого тома. Mountvol позволяет использовать один и тот же том с несколькими путями монтирования.

Формат командной строки:

MOUNTVOL [<диск>:]<путь> <имя тома>
MOUNTVOL [<диск>:]<путь> /D
MOUNTVOL [<диск>:]<путь> /L
MOUNTVOL [<диск>:]<путь> /P
MOUNTVOL /R
MOUNTVOL /N
MOUNTVOL /E

Параметры командной строки:

< путь > – Существующая папка NTFS, в которой будет располагаться точка подключения.

< имя тома > – Имя подключаемого тома.

/D –Удаление точки подключения тома из заданной папки.

/L – Вывод списка имен подключенных томов для заданной папки.

/P – Удаление точки подключения тома из заданной папки, отключение тома и перевод тома в неподключаемое состояние. Том можно сделать подключаемым, заново создав точку подключения тома.

/R – Удаление папок и параметров реестра точек подключения тома для томов, которые больше не существуют в системе.

/N Отключение автоматического подключения новых томов.

/E Включение автоматического подключения новых томов.

При выполнении команды mountvol без параметров, кроме справки по использованию, отображаются возможные значения имен томов вместе с текущими точками подключения.

Имя тома содержит префикс \\?\Volume и уникальный глобальный идентификатор - GUID :

\\?\Volume{152aae2e-3dfa-11e1-98a7-806e6f6e6963}\

Алгоритм формирования GUID построен таким образом, что каждый новый генерируемый идентификатор никогда не совпадает с другим, существующим в данной системе. Обозначается GUID в виде наборов шестнадцатеричных цифр, разделяемых дефисами для удобства записи, и заключенными в фигурные скобки:

{166769E1-88E8-11CF-A6BB-0080C7B2D6A2}

Соответственно, в каждой конкретной системе Windows, каждый конкретный том имеет свое уникальное имя.

Примеры использования:

mountvol – отобразить краткую справку и перечень томов с точками монтирования, допустимых в данной системе. Запись в форме:

\\?\Volume{e15660b7-46a7-11e3-b499-806e6f6e6963}\

*** НЕТ ТОЧЕК ПОДКЛЮЧЕНИЯ ***

означает, что в системе имеется том без точки монтирования. Обычно такая запись имеется в системах содержащих скрытые разделы восстановления или созданные при стандартной установке Windows 7/8 разделы для менеджера загрузки bootmgr.

При наличии точки монтирования в качестве пустой папки NTFS, информация отображается в следующем виде:

\\?\Volume{ade35767-bef1-11e3-a72c-d02788d7ed26}\
D:\
C:\MountPointD\
\\?\Volume{ade35767-bef1-11e3-a72c-d02788d7ed26}\ - идентификатор (имя) тома.

Том с данным именем смонтирован как логический диск D: и в качестве содержимого папки MountPointD на логическом диске C:

mountvol C:\mountpointD \\?\Volume{ade35767-bef1-11e3-a72c-d02788d7ed26}\ – подключить том с именем \\?\Volume{ade35767-bef1-11e3-a72c-d02788d7ed26}\ в качестве папки C:\mountpointD. Например, если данный том был подключен в качестве логического диска D: то содержимое папки C:\mountpointD будет полностью дублировать содержимое диска D:

mountvol C:\mountpointd /l – отобразить список подключенных томов для папки C:\mountpointD

mountvol C:\mountpointd /d – удалить точку монтирования тома в виде папки C:\mountpointD. Если вместо параметра /d используется /P то кроме отключения тома из заданной папки, он переводится в неподключаемое состояние. Чтобы сделать том подключаемым, нужно заново создать точку подключения.

mountvol /R – удалить папки и параметры реестра точек подключения для томов, которые больше не существуют в системе. Точки монтирования для съемных дисков данной командой не затрагиваются, даже если они не подключены на момент ее выполнения.

Команда MKLINK предназначена для создания символьной ссылки на файл или каталог.

Символьная (символическая) ссылка — специальный файл в файловой системе, для которого не формируются никакие данные, кроме одной текстовой строки с указателем. Ссылка может указывать на файл, каталог или даже несуществующий файл. Основное назначение символьных ссылок – создание удобной структуры файлов и каталогов в файловой

системе. Ссылки позволяют для одного файла или каталога иметь несколько имён, абсолютно никак не связанных с именами файлов или каталогов, на которые они ссылаются. На практике, символьные ссылки используются для подключения в нужное место файловой системы файлов или папок, расположенных в произвольных местах, а также для связывания содержимого с конкретным именем файла или каталога. Например, для подключения к каталогу, обслуживаемому FTP-сервером, съемного диска (флэшки) для временной раздачи по FTP. Вместо копирования содержимого флэшки, можно в домашнем каталоге сервера создать символьную ссылку, ссылающуюся на ее содержимое.

Формат командной строки MKLINK:

MKLINK [[/D] | [/H] | [/J]] Ссылка Назначение

Параметры командной строки:

/D — Создание символической ссылки на каталог. По умолчанию (без ключа /D) создается символическая ссылка на файл.

/H — Создание жесткой связи (hard link) вместо символической ссылки.

/J — Создание соединения для каталога.

Ссылка — Имя новой символической ссылки.

Назначение — Путь (относительный или абсолютный), на который ссылается создаваемая ссылка.

Примеры использования:

mklink /? — отобразить подсказку по использованию команды.

mklink /D slnk1 D:\1 — создать в текущем каталоге символьную ссылку с именем slnk1, ссылающуюся на каталог D:\1

mklink slnk2 D:\1\1.txt — создать символическую ссылку slnk2 на файл D:\1\1.txt

Для удаления созданных символических ссылок можно воспользоваться стандартными командами командной строки Windows:

erase lnkfile1 — удалить символьную ссылку на файл. Сам файл, на который ссылается ссылка, не удаляется.

rmdir C:\mountpoint\ShC — удаление символической ссылки на каталог. Сам каталог не удаляется. Обратите внимание, что использование команды del для файлов внутри каталога, на который ссылается ссылка, приводит к их удалению.

erase C:\mountpoint\ShC\lile1.txt — удалить файл из каталога, определенного символической ссылкой.

mklink /H hm histmacros.cmd — создать жесткую ссылку с именем hm, ссылающуюся на файл histmacros.cmd. Жесткие ссылки могут создаваться только в пределах одного раздела. Нельзя создать жесткую ссылку, например, командой:

mklink /H C:\mountpoints\hm D:\SCRIPTS\histmacros.cmd

И жесткая ссылка, и файл, на который она ссылается, должны быть на одном и том же логическом диске.

Команда SUBST позволяет создать виртуальный диск, содержимым которого, будет заданный в команде каталог файловой системы.

Формат командной строки:

SUBST [диск1: [диск2:]путь]

SUBST диск1: /D

диск1: Виртуальный диск, который сопоставляется указанному пути.

[диск:]путь Физические диск и путь, которым сопоставляется виртуальный диск.

/D Удаление ранее созданного виртуального диска.

SUBST без параметров используется для вывода текущего списка виртуальных дисков.

Примеры использования:

SUBST X: C:\ — создать виртуальный диск X: на основе содержимого диска C:

SUBST X: C:\USERS — создать виртуальный диск X:, на основе содержимого каталога C:\USERS

SUBST X: "C:\Documents and Settings\All Users\" — как и в предыдущем примере, но путь для физического каталога содержит пробелы и поэтому, заключается в двойные кавычки.

SUBST X: /D — удалить ранее созданный виртуальный диск X:

SUBST — отобразить список созданных командой SUBST виртуальных дисков.

2.6 Работа с процессами, создание, просмотр, удаление

Команда TASKLIST используется для получения списка процессов, выполняющихся на локальном или удаленном компьютере в данный момент времени.

Список параметров:

/S <система> Подключаемый удаленный компьютер.

/U [<домен>\]<пользователь> Пользовательский контекст, в котором должна выполняться эта команда.

/P [<пароль>] Пароль для этого пользовательского контекста. Запрашивает ввод пароля, если он не задан.

/M [<модуль>] Отображение всех задач, которые используют данное имя exe/dll. Если имя модуля не указано, то отображаются все загруженные модули.

/SVC Отображение служб для каждого процесса.

/V Ведение подробного протоколирования.

/FI <фильтр> Отображение списка задач, которые отвечают указанному в фильтре критерию.

/FO <формат> Описание формата выходного файла. Допустимые значения: "TABLE", "LIST", "CSV".

/NH Отключение отображения заголовка "Column Header" в выходных данных. Допустимо для форматов "TABLE" и "CSV".

/? Вывод справки по использованию.

Примеры использования:

tasklist /? — выдать краткую справку по использованию команды.

tasklist — отобразить на экране консоли список процессов, выполняющихся на локальном компьютере в данный момент времени. При этом отображается следующая информация:

Имя образа — имя исполняемого файла данного процесса. System Idle Process — это индикация режима простоя, когда ни один из процессов не выполняется.

PID - уникальный идентификатор процесса. Присваивается процессу при его создании.

Имя сессии - имя сессии отображает признак Services — процесс запущен в качестве системной службы,Console — интерактивный пользовательский процесс, RDP-Tcp#n — процесс, созданный удаленным подключением по RDP (клиентами служб терминалов) - .

№ сеанса — номер сеанса пользователя.

Память — объем используемой процессом памяти.

tasklist — S SERVER - отобразить список процессов, выполняющихся на удаленном компьютере SERVER в данный момент времени.

tasklist /m wsock32.dll — отобразить список процессов, которые подгружают библиотеку wsock32.dll. Пример отображаемых результатов выполнения команды:

Имя образа	PID	Модули
AvastSvc.exe	1456	WSOCK32.dll
AvastUI.exe	2252	WSOCK32.dll
firefox.exe	3268	WSOCK32.dll

tasklist /SVC — отобразить информацию о системных службах. Пример:

Имя образа	PID	Службы
System Idle Process	0	Н/Д
System	4	Н/Д
smss.exe	316	Н/Д
csrss.exe	432	Н/Д

wininit.exe	468	Н/Д
csrss.exe	488	Н/Д
services.exe	536	Н/Д
lsass.exe	556	KeyIso, SamSs

tasklist -s 192.168.0.1 -U mydomain\admin -P mypass /FI "memusage gt 10000" — отобразить список процессов, использующих более 10000кб (10 Мб) памяти на компьютере с IP-адресом 192.168.0.1 . При подключении к удаленному компьютеру используется имя пользователя admin в домене mydomain и пароль mypass.

Команда TASKKILL используется для завершения процессов по идентификаторам или именам исполняемых файлов на локальной или удаленной системе. Используется в операционных системах Windows XP и старше.

Описание параметров:

/S <система> Подключаемый удаленный компьютер.

/U [<домен>\]<пользователь> Пользовательский контекст, в котором должна выполняться эта команда.

/P <пароль> Пароль для этого пользовательского контекста. Запрашивает пароль, если он не задан.

/FI <фильтр> Применение фильтра для выбора набора задач. Разрешение использовать "*". Пример, imagename eq acme*.

/PID <процесс> Идентификатор процесса, который требуется завершить. Используйте TaskList, чтобы получить PID.

/IM <образ> Имя образа процесса, который требуется завершить. Знак подстановки "*" может быть использован для указания всех заданий или имен образов.

/T Завершение указанного процесса и всех его дочерних процессов.

/F Принудительное завершение процесса.

/? Вывод справки по использованию.

TASKKILL /IM notepad.exe — завершить процесс, исполняемым образом которого является notepad.exe . Если таких процессов более одного - то будут завершены все.

taskkill /PID 1234 /T —завершить процесс с идентификатором 1234 и все его дочерние процессы (/T) . Одной командой можно завершить несколько процессов, задавая их PID - taskkill /PID 1234 /PID 2345 /PID 800.

TASKKILL /S SERVER /U Mydomain\User /P UserPass /FI "IMAGENAME eq note*" — завершить все процессы, имя исполняемого файла которых начинается со строки note на удаленном компьютере с именем SERVER.

2.7 Управление реестром

Реестр — иерархическая централизованная база данных, используемая в ОС Microsoft Windows для хранения сведений, необходимых для настройки операционной системы для работы с пользователями, программными продуктами и устройствами.

В реестре хранятся данные, которые необходимы для правильного функционирования Windows. К ним относятся профили всех пользователей, сведения об установленном программном обеспечении и типах документов, которые могут быть созданы каждой программой, информация о свойствах папок и значках приложений, а также установленном оборудовании и используемых портах.

Файлы реестра создаются в процессе установки операционной системы и хранятся в папке %SystemRoot%\system32\config. Для операционных систем Windows это файлы с именами:

- default;
- sam;
- security;
- software;
- system.

Существует пять основных ветвей реестра, которые соответствуют определенному типу информации, хранящейся в реестре. Эти корневые разделы нельзя удалить, переименовать или переместить, потому что они — основа реестра:

1. HKEY_CLASSES_ROOT

Эта ветвь содержит информацию о соответствии типов файлов зарегистрированным компонентам программного обеспечения (классам), используемым операционной системой и приложениями.

Вся эта ветвь — это «зеркальное отображение» ветви HKEY_L0KAL_MACHINE\ SOFTWARE\Classes

2. HKEY_CURRENT_USER

В каждой ветви пользователя существуют настройки для текущего пользователя, такие как, например, настройки Панели управления. Большинство приложений сохраняют здесь также и определенную информацию пользователя, например, такую, как панели инструментов, рекорды в играх и другие личные настройки.

Настройки текущего пользователя разделены на несколько категорий: AppEvents, Control Panel, Identities, Software и System. Самая полезная из ветвей -Software, которая содержит данные для приложений, установленных на компьютере. В этом разделе и в разделе HKEY_LOCAL_MACHINE\SOFTWARE (мы поговорим о нем позже) можно найти все настройки ваших приложений. Большинство пользовательских настроек операционной системы находятся в HKEY_CURRENT_USER\ Software\Microsoft\Windows.

3. HKEY_LOCAL_MACHINE

Эта ветвь содержит информацию о «железе» и программном обеспечении, установленном на компьютере, которая не связана с конкретным пользователем, то есть настройки, которые являются общими для всех пользователей системы.

Так же, как и HKEY_CURRENT_USER, наибольший интерес представляет ветвь SOFTWARE. Она содержит всю

информацию, необходимую для приложений, установленных на компьютере. В ветви HKEY_CURRENT_USER хранятся все пользовательские настройки (даже если у компьютера только один пользователь), например, конфигурация Панели инструментов. Настройки, которые не зависят от пользователя, — папки, в которые установлены программы и списки установленных компонентов, — находятся в ветви HKEY_LOCAL_MACHINE. Чтобы найти настройки конкретного приложения, понадобится заглянуть в обе ветви, поскольку большинство производителей (даже Microsoft) не очень внимательно относятся к тому, какая именно ветвь используется для настроек.

4. HKEY_USERS

В этой ветви содержится подветвь текущего пользователя

Хотя вы и можете редактировать содержание этой ветви, но лучше все-таки использовать ветвь HKEY_CURRENT_USER:

HKEY_USERS\S-1-5-21-1727987266-1036259444-725315541-500

Неважно, какой пользователь подключен, HKEY_CURRENT_USER всегда связана с соответствующей частью HKEY_USERS.

5. HKEY_CURRENT_CONFIG

Эта ветвь содержит мало информации, большая часть которой является копией (зеркальным отображением) других разделов реестра. Обычно нет причин вмешиваться в работу этой ветви.

Все, что вы хотите изменить в реестре, можно сделать в разделе HKEY_CURRENT_USER или HKEY_LOCAL_MACHINE.

Параметры или ключи реестра имеют имена, представленные в обычном текстовом виде и значения, которые хранятся в виде стандартизированных записей определенного типа. Допустимые типы данных реестра:

REG_BINARY — двоичный параметр. Большинство сведений об аппаратных компонентах хранится в виде двоичных данных и выводится в редакторе реестра в шестнадцатеричном формате.

REG_DWORD —двойное слово. Данные представлены в виде значения, длина которого составляет 4 байта (32-разрядное целое). Этот тип данных используется для хранения параметров драйверов устройств и служб. Значение отображается в окне редактора реестра в двоичном, шестнадцатеричном или десятичном формате. Эквивалентами типа DWORD являются DWORD_LITTLE_ENDIAN (самый младший байт хранится в памяти в первом числе) и REG_DWORD_BIG_ENDIAN (самый младший байт хранится в памяти в последнем числе).

REG_QWORD — данные, представленные в виде 64-разрядного целого. Начиная с Windows 2000, такие данные отображаются в окне редактора реестра в виде двоичного параметра.

REG_SZ — строковый параметр.

REG_EXPAND_SZ — расширяемая строка данных. Многострочный параметр. Многострочный текст. Этот тип, как правило, имеют списки и другие записи в формате, удобном для чтения. Записи разделяются пробелами, запятыми или другими символами.

REG_RESOURCE_LIST — двоичный параметр. Последовательность вложенных массивов. Служит для хранения списка ресурсов, которые используются драйвером устройства или управляемым им физическим устройством. Обнаруженные данные система сохраняет в разделе \ResourceMap. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцатеричном формате.

REG_RESOURCE_REQUIREMENTS_LIST — двоичный параметр. Последовательность вложенных массивов. Служит для хранения списка драйверов аппаратных ресурсов, которые могут быть использованы определенным драйвером устройства или управляемым им физическим устройством.

Часть этого списка система записывает в раздел \ResourceMap. Данные определяются системой. В окне редактора реестра они отображаются в виде двоичного параметра в шестнадцатеричном формате.

REG_FULL_RESOURCE_DESCRIPTOR — двоичный параметр. Последовательность вложенных массивов. Служит для хранения списка ресурсов, которые используются физическим устройством. Обнаруженные данные система сохраняет в разделе \HardwareDescription. В окне редактора реестра эти данные отображаются в виде двоичного параметра в шестнадцатеричном формате.

REG_NONE — данные, не имеющие определенного типа. Такие данные записываются в реестр системой или приложением. В окне редактора реестра отображаются в виде двоичного параметра в шестнадцатеричном формате.

REG_LINK — символическая ссылка в формате Юникод.

При добавлении новых параметров в реестр, необходимо задавать не только имя и значение, а также правильный тип данных.

Главным отличием реестра операционных систем Windows Vista / Windows 7 / Windows Server 2008 и более поздних выпусков - появление нового раздела с данными конфигурации загрузки системы HKEY_LOCAL_MACHINE\BCD00000000.

Этот раздел содержит объекты и элементы конфигурации, используемые новым диспетчером загрузки BOOTMGR пришедшим на смену традиционному загрузчику NTLDR.

Раздел HKEY_LOCAL_MACHINE\BCD00000000 является системным хранилищем данных конфигурации загрузки (BCD — Boot Configuration Data) и физически, представляет собой файл реестра с именем bcd, находящийся в каталоге \BOOT активного раздела (раздела диска с загрузочной записью и файлом диспетчера BOOTMGR).

2.8 Использование точек восстановления

В операционных системах Windows, начиная с Windows XP, существует механизм, с помощью которого, при возникновении проблем, можно восстановить предыдущее состояние компьютера без потери личных файлов (документов Microsoft Word, рисунков, Избранного, Рабочего стола) с использованием точек восстановления (Restore Points), которые при стандартных настройках, создаются системой автоматически во время простоя компьютера или во время существенных системных событий, таких, как установка нового приложения или драйвера. Кроме того, имеется возможность в любое время создать точку восстановления принудительно, с помощью "Панель управления" – "Система" – "Дополнительные параметры" – "Защита системы" – "Создать".

Точки восстановления представляют собой набор файлов операционной системы и реестра, скомпонованный по определенным правилам и сохраняемый в виде подкаталога в скрытой системной папке System Volume Information. Сохраненные в точке восстановления данные позволяют, практически гарантировано, вернуть операционную систему к состоянию на момент их создания. При изучении реестра (и отсутствии практического опыта работы с ним) принудительное создание точки восстановления перед началом работы позволит восстановить работоспособность Windows даже в случае краха системы. Стандартное средство восстановления системы работает только в среде самой Windows, однако существуют способы, которые позволяют вернуть систему к жизни даже при возникновении "синего экрана смерти" по причине неудачного редактирования реестра. Об этом чуть позже.

Для восстановления системы используется точками восстановления используется приложение "Восстановление системы" — \windows\system32\restore\rstrui.exe для Windows XP и \windows\system32\rstrui.exe для Windows старше.

Данные точек восстановления хранятся в каталоге System Volume Information системного диска. Это скрытый

системный каталог, доступ к которому разрешен только локальной системной учетной записи (Local System), или, другими словами, не пользователям, а "Службе восстановления системы". Поэтому, если вы хотите получить доступ к его содержимому, вам придется добавить права вашей учетной записи с использованием вкладки "Безопасность" в свойствах каталога "System Volume Information".

При выполнении операции восстановления системы восстанавливаются основные системные файлы и файлы реестра.

Структура данных точек восстановления для Windows 7 отличается от той, что используется в Windows XP. Начиная с ОС Windows Vista, используется не только копирование файлов реестра и важнейших системных файлов, но и создаются снимки файловой системы (snapshot) службой теневого копирования томов. Снимки файловой системы также хранятся в каталоге System Volume Information и представляют собой сжатые файлы, в имени которых содержится глобальный идентификатор: {3808876b-c176-4e48-b7ae-04046e6cc752}

Количество снимков зависит от настроек системы и наличия свободного места на диске. Откат системы на точку восстановления является простым и эффективным способом восстановления работоспособности без потери пользовательских данных не только в случаях неудачного редактирования реестра, установки некорректно работающего системного программного обеспечения, но и, например, при вирусном заражении компьютера, когда имеется точка восстановления на момент времени, когда вируса еще не было в системе. Именно поэтому многие вредоносные программы пытаются уничтожить данные точек восстановления и отключить средства восстановления системы.

Для резервного копирования реестра используется REG.EXE SAVE, для восстановления - REG.EXE RESTORE

Для сохранения куста SYSTEM:
REG SAVE HKLM\SYSTEM system.hiv

Для сохранения куста SOFTWARE:
REG SAVE HKLM\SOFTWARE software.hiv

Сохраненные файлы можно использовать для восстановления реестра с использованием ручного копированием в папку %SystemRoot%\system32\config.

2.9 Системные службы Windows

Службы ОС Windows — приложения, автоматически запускаемые системой при запуске Windows и выполняющиеся вне зависимости от статуса пользователя.

Системные службы необходимы для обеспечения функциональности аппаратного и программного обеспечения.

Существует несколько режимов для служб:

– запрещен к запуску;
– ручной запуск (по запросу);
– автоматический запуск при загрузке компьютера;
– автоматический (отложенный) запуск (введен в Windows Vista и Windows Server 2008).
– обязательная служба/драйвер (автоматический запуск и невозможность (для пользователя) остановить службу).

Автоматический (отложенный) запуск применяется для служб, которым не нужно быть активными сразу после загрузки системы. Система запускает такие службы только после того, как запущены все службы, настроенные на автоматический запуск. Запуск отложенных служб осуществляется с самым низким приоритетом, что позволяет сэкономить ресурсы компьютера при загрузке этих служб.

Благодаря отложенному автоматическому запуску и низкому приоритету, существенно снижается нагрузка на систему, что позволяет ускорить вход пользователя в систему.

Список служб находится в ветке Windows «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services».

Значения параметра «Start» имеют тип «REG_DWORD» и могут принимать значения:

0 — Низкоуровневые драйверы, например, драйверы дисков, которые загружаются на самом раннем этапе загрузки — загрузки ядра;

1 — Драйверы, которые загружаются после инициализации ядра ОС;

2 — Службы, которые должны быть загружены диспетчером управления службами (равен параметру — «Авто»);

3 — Службы, запускаемые диспетчером управления службами только в случае получения явной инструкции на загрузку (равен параметру — «Вручную»);

4 — Службы, которые не загружаются (равен параметру — «Отключено»).

Прежде чем экспериментировать со службами лучше сделать резервную копию раздела реестра, который отвечает за запуск системных служб. Для этого необходимо экспортировать ветвь реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services

Рассмотрим некоторые службы.

DHCP-клиент — управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен. Если нет сети (Интернет или локальной сети), то можно отключить.

DNS-клиент — кэширует имена DNS (Domain Name System) и регистрирует полное имя данного компьютера. Если служба остановлена, то не разрешаются DNS-имена и нельзя разместить службу каталогов Active Directory контроллеров домена. Если Active Directory не используется и нет сети, службу можно отключить.

MS Software Shadow Copy Provider — управляет теневыми копиями, полученными при помощи теневого копирования тома. Можно отключить. NetMeeting Remote Desktop Sharing — разрешает проверенным пользователям получать доступ к рабочему столу Windows, используя NetMeeting. Можно отключить.

Plug and Play — позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо, не требуя вмешательства пользователя, либо сводя его к минимуму. Остановка или отключение этой службы может привести к нестабильной работе системы.

QoS RSVP — обеспечивает рассылку оповещений в сети и управление локальным трафиком для управляющих программ. Рекомендуется отключить.

Telnet — позволяет удаленному пользователю входить в систему и запускать программы. Рекомендуется отключить.

Автоматическое обновление — включает загрузку и установку обновлений Windows. Учитывая, что обновлять систему можно и вручную рекомендую отключить. Следует только не забыть отменить автоматическое обновление в окне "Свойства системы" (Мой компьютер правой кнопкой мыши - пункт "Свойства"- вкладка "Автоматическое обновление").

Беспроводная настройка — предоставляет автоматическую настройку 802.11 адаптеров - набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6 и 5 ГГц. Пользователям более известен по названию Wi-Fi. Если таковых нет, то эту службу можно отключить.

Брандмауэр Windows /Общий доступ к Интернету (ICS) — служба управляет стандартным брандмауэром Windows, а также возможностью общего доступа к Интернету (ICS). Стандартный брандмауэр Windows предоставляет минимальные функции обеспечения безопасности подключения к Интернету (он следит за всеми открытыми портами и извещает пользователя о попытке какой-либо программы передать данные из Интернета или в Интернет по одному из портов). Служба Брандмауэр Windows/Общий доступ к Интернету (ICS) занимает около 4360 Кбайт оперативной памяти и запускается с правами локальной системы (Local System) автоматически при каждом входе пользователя в систему (при этом она запускается как часть процесса svchost.exe). Если вы

используете брандмауэр сторонней фирмы и при этом не применяете функцию ICS, то данную службу можно отключить.

Служба восстановления системы — выполняет функции восстановления системы. Рекомендуется оставить эту службу, т.к. она может выручить Вас, если вы не знаете, как восстанавливать систему другими средствами.

Служба времени Windows — управляет синхронизацией даты и времени на всех клиентах и серверах в сети. Можно отключить.

Удаленный реестр — позволяет удаленным пользователям изменять параметры реестра на локальном компьютере. Желательно отключить.

Один из способов повышения производительности Windows Настройка служб, а точнее отключение ненужных служб. Вот краткий список служб, которые можно отключить:

Windows Search — весьма «прожорливая» служба, которая индексирует все данные на компьютере. Если вы не планируете использовать поиск, то отключите ее. При необходимости, вы можете запустить ее, найти то что искали, и снова отключить.

Браузер компьютеров (Browser) — обслуживает все компьютеры в локальной сети, индексирует их и создает списки, которые выдаются определенным программам по требованию.

Диспетчер печати можно смело отключать, если у вас нет принтера.

Вспомогательная служба IP необходима для использования дополнительных функций. Если остановить эту службу, то вы не сможете раздавать Wi-Fi с ноутбука (компьютера), а также использовать другие дополнительные возможности, такие, как туннельное подключение (виртуальное подключение) для IPv6 и так далее.

Вторичный вход в систему позволяет запускать программы от имени разных учетных записей (пользователей). Если вы единственный пользователь и являетесь администратором системы, то смело отключайте эту функцию.

Клиент изменившихся связей — позволяет поддерживать связи NTFS файлов (данных на жестком диске), которые перемещаются между компьютерами в одной локальной сети. Если вы не соединяете несколько компьютеров для передачи файлов между ними, то можете смело отключать данную функцию.

Сервер – обеспечивает возможность общего доступа к определенным файлам, принтерам, а также именованным каналам через локальную сеть.

Служба загрузки изображений Windows (WIA) — позволяет получать картинки со сканеров и фотоаппаратов (камер).

Служба регистрации ошибок Windows — позволяет отправлять отчеты в случае возникновения каких-либо ошибок в работе той или иной программы. Как правило, никто не использует подобные возможности, поскольку они работают исключительно на лицензионных изданиях, которые были официально куплены.

Удаленный реестр — необходим для того, чтобы удаленные пользователи могли вносить изменения в реестр ОС через сетевое соединение. Эту функцию можно смело отключать. В таком случае изменения в реестр смогут вносить только локальные пользователи, которые работают непосредственно за данным компьютером.

3. АДМИНИСТРИРОВАНИЕ ОС LINUX

3.1. Учетные записи в Linux

ОС Linux является многозадачной и многопользовательской системой, т. е. эта операционная система позволяет одновременно нескольким пользователям работать с ней. Для этих целей в Linux существует два понятия — учетные записи и аутентификация.

Учетная запись пользователя – это необходимая для системы информация о пользователе, хранящаяся в специальных файлах. Информация используется Linux для аутентификации пользователя и назначения ему прав доступа.

Аутентификация – системная процедура, позволяющая Linux определить, какой именно пользователь осуществляет вход.

Вся информация о пользователе обычно хранится в файлах /etc/passwd и /etc/group.

/etc/passwd – этот файл содержит информацию о пользователях. Запись для каждого пользователя занимает одну строку:

Каждая строка файла /etc/passwd описывает одного пользователя и содержит семь полей, разделённых двоеточиями:

1. регистрационное имя или логин;
2. хеш пароля (см. ниже);
3. идентификатор пользователя;
4. идентификатор группы по умолчанию;
5. информационное поле GECOS;
6. начальный (он же домашний) каталог;
7. регистрационная оболочка, или shell.

Имя пользователя – имя, используемое пользователем на все приглашения типа login при аутентификации в системе. Регистрационные имена должны быть уникальными и представлять собой строки не длиннее 32 символов (любые, кроме двоеточия и символа новой строки).

Зашифрованный пароль – обычно хешированный по необратимому алгоритму MD5 пароль пользователя или символ '!', в случаях, когда интерактивный вход пользователя в систему запрещен.

UID – числовой идентификатор пользователя. Система использует его для распределения прав файлам и процессам. Идентификатор пользователя — это число от 0 до 2 в степени 32. Пользователь с идентификатором 0 (обычно root) называ-

ется суперпользователем и имеет право на выполнение любых операций в системе.

GID – числовой идентификатор группы. Имена групп расположены в файле /etc/group. Система использует его для распределения прав файлам и процессам. В UNIX пользователь может принадлежать к одной или нескольким группам, которые используются для задания прав более чем одного пользователя на тот или иной файл.

Настоящее имя пользователя (GECOS) – используется в административных целях, а также командами типа fingerd (сетевой протокол, предназначенный для предоставления информации о пользователях удалённого компьютера). Поле GECOS хранит вспомогательную информацию о пользователе (номер телефона, адрес, полное имя и так далее). Оно не имеет четко определенного синтаксиса. Тем не менее, демон fingerd предполагает, что в нем содержатся следующие элементы, разделенные запятыми:

- полное имя;
- адрес офиса или домашний адрес;
- рабочий телефон;
- домашний телефон.

Домашний каталог – полный путь к домашнему каталогу пользователя. После входа в систему пользователь оказывается в своём домашнем каталоге. Исторически сложилось так, что домашний каталог пользователя root называется /root, а остальные имеют вид /home/имя_пользователя.

Оболочка – командная оболочка, которую использует пользователь при сеансе. Для нормальной работы она должна быть указана в файле регистрации оболочек /etc/shells.

/etc/group – этот файл содержит информацию о группах, к которым принадлежат пользователи.

Имя группы – имя, применяемое для удобства использования таких программ, как newgrp.

Шифрованный пароль – используется при смене группы командой newgrp. Пароль для групп может отсутствовать.

GID – числовой идентификатор группы. Система использует его для распределения прав файлам и процессам.

Пользователи, включенные в несколько групп. В этом поле через запятую отображаются те пользователи, у которых по умолчанию (в файле /etc/passwd) назначена другая группа.

В Linux, кроме обычных пользователей, существует один пользователь с неограниченными правами. Идентификаторы UID и GID такого пользователя всегда 0. Его имя, как правило, root, однако оно может быть легко изменено (или создано несколько символьных имен с одинаковым GID и UID), так как значение для применения неограниченных прав доступа имеет только GID 0. Для пользователя root права доступа к файлам и процессам не проверяются системой.

Команда login запускает сеанс интерактивной работы в системе. Она проверяет правильность ввода имени и пароля пользователя, меняет каталог на домашний, выстраивает окружение и запускает командный интерпретатор.

Команда su (switch user) позволяет сменить идентификатор пользователя уже в процессе сеанса. Синтаксис ее прост: su username, где username – имя пользователя, которое будет использоваться. После этого программа запросит пароль. При правильно введенном пароле, su запустит новый командный интерпретатор с правами пользователя, указанного su и присвоит сеансу его идентификаторы. Если имя пользователя опущено, то команда su использует имя root.

Команда passwd является инструментом для смены пароля в Linux. Для смены своего пароля достаточно набрать в командной строке passwd:

[student@ns student]$ passwd

Или ввести команду passwd и имя пользователя, для которого будет меняться пароль: $passwd student

3.2. Права доступа в Linux

Для каждого объекта в файловой системе Linux существует набор прав доступа, определяющий взаимодействие пользователя с этим объектом. Такими объектами могут быть файлы, каталоги, а также специальные файлы (например, устройства) — то есть по сути любой *объект* файловой системы. Так как у каждого объекта в Linux имеется владелец, то *права* доступа применяются относительно владельца файла. Они состоят из набора 3 групп по три атрибута:

– чтение(r), запись(w), выполнение(x) для владельца;

– чтение, запись, выполнение для группы владельца;

– чтение, запись, выполнение для всех остальных.

Такие права можно представить краткой записью:

rwxrwxrwx – разрешено чтение, запись и выполнение для всех

rwxr-xr-x – запись разрешена только для владельца файла, а чтение и выполнение для всех.

rw-rw-r-- – запись разрешена для владельца файла и группы владельца файла, а чтение – для всех.

Такое распределение прав позволяет гибко управлять ресурсами, доступными пользователям.

Права доступа распространяются и на каталоги. Они означают:

r – если установлено право на чтение из каталога, то можно увидеть его содержимое командой ls .

w – если установлено право записи в каталог, то пользователь может создавать и удалять файлы из текущего каталога. Причем удалить файл из каталога пользователь может даже если у него нет прав на запись в файл.

x – если установлено право исполнения на каталог, то пользователь имеет право перейти в такой каталог командами наподобие cd.

Команда chmod (Change MODe – сменить режим) – изменяет права доступа к файлу. Для использования этой команды также необходимо иметь права владельца файла или права root. Синтаксис команды таков:

chmod mode filename , где

filename – имя файла, у которого изменяются права доступа;

mode – права доступа, устанавливаемые на файл. Права доступа можно записать в 2 вариантах – символьном и абсолютном.

В символьном виде использование команды chmod будет выглядеть следующим образом:

$ chmod [references][operator][modes] file ...

```
                |r|
        |u|     |w|
        |g|  |+| |x|
chmod   |o|  |-| |X| filename,
        |a|  |=| |u|
                |g|
                |o|
```

References — определяют пользователей, которым будут меняться права. References определяются одной или несколькими буквами: u – владелец файла; g - пользователи, входящие в группу владельца файла; o - остальные пользователи; a - все пользователи, то есть для всех трех групп.

Operator —определяет операцию, которую будет выполнять chmod.

Modes — определяет какие именно права будут установлены, добавлены или удалены: r — чтение файла или содержимого каталога; w — запись в файл или в каталог; x - выполнение файла или чтение содержимого каталога.

Просмотр разрешений, установленных на файл осуществляется командой ls с ключом -l:

```
[student@ns student]$ ls -l lesson5.txt
-rw------- 1  student student  39 Nov 19 15:17  lesson5.txt
```

```
[student@ns student]$ chmod g+rw lesson5.txt

[student@ns student]$ ls -l lesson5.txt
-rw-rw----  1  student student  39 Nov 19 15:18  lesson5.txt
```

Возможно использование команды в числовом виде. Права записываются одной строкой сразу для трёх типов пользователей:

– владельца файла (u);

– других пользователей, входящих в группу владельца (g);

– всех прочих пользователей (o);

Например, chmod 444 {имя файла}: 400+40+4=444 — все имеют право только на чтение (идентично «r--r--r--»).

3.3 Процессы в Linux

Каждому процессу в системе назначаются числовые идентификаторы (личные номера) в диапазоне от 1 до 65535 (PID – Process Identifier) и идентификаторы родительского процесса (PPID – Parent Process Identifier). PID является именем процесса, по которому мы можем адресовать процесс в операционной системе при использовании различных средств просмотра и управления процессами. PPID определяет родственные отношения между процессами, которые в значительной степени определяют его свойства и возможности. Другие параметры, которые необходимы для работы программы, называют "окружение процесса". Один из таких параметров – управляющий терминал – имеют далеко не все процессы. Процессы, не привязанные к какому-то конкретному терминалу называются "демонами" (daemons). Такие процессы, будучи запущенными пользователем, не завершают свою работу по окончании сеанса, а продолжают работать, т.к. они не связаны никак с текущим сеансом и не могут быть автоматически завершены. Как правило, с помощью демонов реализуются серверные службы, так, например, сервер печати

реализован процессом-демоном cupsd, а сервер журналирования – syslogd.

Для просмотра списка процессов в Linux существует команда ps.

ps options [PID] – просмотр списка процессов. Без параметров ps показывает все процессы, которые были запущены в течение текущей сессии, за исключением демонов.

ps –aux (подробный вывод)

Пример1:

```
[gserg@WEBMEDIA gserg]$ ps
  PID TTY          TIME CMD
 3126 pts/2    00:00:00 bash
 3158 pts/2    00:00:00 ps
```

Родителем всех процессов в системе является процесс init. Его PID всегда 1, а PPID – 0.

Немаловажную роль в жизни процессов играет также планировщик – это часть ядра, ответственная за многозадачность системы. Ведь в единицу времени на одном процессоре может выполняться только одна задача. Именно планировщик определяет, какой из запущенных процессов первым будет выполняться, какой вторым. Для этого у каждого процесса существует еще один параметр, называемый приоритетом. Для того, чтобы посмотреть приоритет процессов, нам необходимо использовать уже знакомую команду ps с параметром l (long – расширенный вывод).

Во время своей работы, планировщик в первую очередь ставит на выполнение задачи с меньшим приоритетом. Так, приоритетом 0, обладают только критические системные задачи, а отрицательным приоритетом – процессы ядра. Задачам с большим приоритетом достается меньше процессорного времени и потому, работают они как правило, медленнее, и потребляют намного меньше системных ресурсов.

nice -n command — позволяет изменять приоритет, с которым будет выполняться процесс после запуска. Без указания команды command выдает текущий приоритет рабо-

ты. n по умолчанию равен 10. Диапазон приоритетов расположен от -20 (наивысший приоритет) до 19 (наименьший).

Другая команда, renice, служит для изменения значения nice для уже выполняющихся процессов. Ее формат таков:

renice priority [[-p] PID] [[-g] grp] [[-u] user]

Например, команда [root]# renice -1 987 увеличивает на 1 приоритет процесса с PID 987.

3.4 Команды для администрирования Linux

Команда Wget — (GNU Wget) свободная неинтерактивная консольная программа для загрузки файлов по сети. Поддерживает протоколы HTTP, FTP и HTTPS, а также поддерживает работу через HTTP прокси-сервер. Программа включена почти во все дистрибутивы GNU/Linux.

Wget позволяет загружать любые файлы во всемирной паутине (в том числе и (X)HTML-страницы) по протоколам http и https, а также файлы и списки директорий по протоколу ftp.

Wget поддерживает докачку файла в случае обрыва соединения. После загрузки, файл будет находиться в домашней директории

Скачивание файла file.zip в текущую директорию:

wget http://example.com/file.zip

Скачивание файлов в указанный каталог (-P):

wget -P /path/to/save http://example.com/file.zip

Докачивание файла file.zip в случаи обрыва:

wget -c http://example.com/file.zip

Скачивание всех файлов по шаблону

wget ftp://example.com/dir/*.zip

Использование имени пользователя и пароля на FTP/HTTP:

wget --user=login --password=password
ftp://ftp.example.org/some_file.iso

Команда ping — проверка доступности хоста.

В отличие от Windows, где команда "ping адрес_хоста" отправит только четыре пакета, в Linux такая команда будет непрерывно слать пакеты, пока вы не прервете ее работу. Для того, чтоб ограничить количество пакетов, следует указать параметр командной строки "-c количество"

ping –c 4 ya.ru

Команды tracepath и traceroute — трассировка маршрута до хоста

В отличие от утилиты ping, утилита tracepath и traceroute позволяет не только определить есть проблемы, или нет, но и проследить маршрут, по которому проходят пакеты к конкретному хосту и выявить из-за какого хоста возникают проблемы с подключением. Tracepath похожа на traceroute, но в отличие от последней не требует рутовых прав.

Стандартные утилиты tracert в Windows и traceroute в Линукс реализованы по-разному и могут давать разные результаты. Windows посылает ICMP, а Linux — UDP.

ICMP *(*Internet Control Message Protocol*)* — протокол межсетевых управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или хост, или маршрутизатор не отвечают.

Команда host — выполнение dns запросов. Команда host выполняет DNS запросы для прямого и обратного разрешения доменных имен. Запустите команду с IP адресом в качестве параметра**,** и она вернет доменное имя, ассоциированное с ним. Также можно по доменному имени определить IP адрес. Для этого в качестве параметра укажите доменное имя.

Команда ifconfig — настройка сетевого интерфейса. Команда ifconfig — одна из основных программ для настройки сети в Linux. Она имеет огромное количество параметров, которые позволят настроить, оптимизировать, а в случае необходимости — отладить работу сетевого интерфейса. Так-

же эта программа позволяет быстро определить IP адрес компьютера, а также другую информацию о сетевых интерфейсах, включая их имена, скорость и режим подключения и так далее.

Команда ifconfig — аналог IPconfig Windows, с другими ключевыми параметрами и более широким функционалом.

В современных дистрибутивах Linux утилита ifconfig считается устаревшей и заменена утилитой iproute2

В Ubuntu (как и в других linux-системах) имена сетевых устройств принимают вид *ethN*, где *N* — число, означающее номер устройства связи в системе. Нумерация устройств начинается с нуля. Если в компьютере две сетевых карты, то они получат имена *eth0* и *eth1*. Если в сетевую карту eth*N* вставлен сетевой провод, идущий в модем, роутер или свитч, будет написано *RUNNING*

Команда ifconfig *–a* удобна в тех случаях, когда надо быстро выяснить состояние интерфейсов, в частности, если необходимо узнать их IP-адреса. Помимо сведений о конфигурации сетевых интерфейсов, команда выдает еще много полезной информации, например, количество отправленных и полученных пакетов.

Интерфейс eth0 — это карта Ethernet, к которой можно подключить сетевой кабель. В текущий момент сетевой кабель не подключен, поэтому интерфейс не активен и для него не отображается ip-адрес, широковещательный адрес и маска подсети:

Интерфейс eth1 —вторая карта Ethernet. Сетевой кабель подключен, интерфейс активен, присвоен ip(10.7.9.6) и маска подсети (255.0.0.0).

Интерфейс lo — интерфейс обратной петли и позволяет компьютеру обращаться к самому себе. Интерфейс имеет ip-адрес 127.0.0.1 и необходим для нормальной работы системы:

Команда ifconfig позволит сконфигурировать сетевой интерфейс.

Остановить интерфейс (выключить):

~$ sudo ifconfig eth0 down

Поднять интерфейс (включить):

~$ sudo ifconfig eth0 up

Для изменения только ip-адреса используется следующий формат команды:

~$ sudo ifconfig eth1 10.7.9.6

Маска подсети:

~$ sudo ifconfig eth1 netmask 255.0.0.0

Меняем сразу адрес и маску:

~$ sudo ifconfig eth0 10.7.9.6 netmask 255.255.0.0

КОМАНДЫ ifdown и ifup — активация/деактивация сетевого интерфейса

Команда ifdown и ifup — это команды, выполняющие тоже самое, что и команды ifconfig up и ifconfig down. Указав в качестве параметра командной строки имя интерфейса, вы отключите, или включите конкретный интерфейс. Выполнение данной команды требует наличия прав суперпользователя:

$sudo ifdown eth0

$sudo ifup eth0

КОМАНДА netstat — отображение сетевой информации

Команда netstat отображает различную информацию о сетевом интерфейсе, например, список открытых сокетов и таблицу маршрутизации. Команда, запущенная без параметров командной строки, выведет информацию по открытым сетевым сокетам и сокетам файловой системы.

Основное назначение утилиты — поиск сетевых проблем и определение производительности сети.

Перечислить все порты: netstat –a

Перечислить все TCP порты: netstat –at

Перечислить все UDP порты: netstat –au

Показать статистику всех портов: netstat -s

netstat -s

Ip:

11150 total packets received

1 with invalid addresses

0 forwarded

0 incoming packets discarded
11149 incoming packets delivered
11635 requests sent out
Icmp:
13791 ICMP messages received
12 input ICMP message failed.
Tcp:
15020 active connections openings
97955 passive connection openings
135 failed connection attempts
Udp:
2841 packets received
180 packets to unknown port received.

Показать статистику только TCP портов: netstat -st

netstat -st

Показать статистику только UDP портов: netstat -su

netstat -su

Опция netstat -p добавит «PID/Program Name» в вывод netstat, и может быть совмещена с любым другим набором опций. Это очень полезно при отладке, для определения того, какая программа работает на определённом порту.

Выяснить, каким процессом используется определённый порт:

netstat -an | grep ':80'

Команда lsof умеет отображать процессы, которые работают с определенным файлом или сокетом.

Список всех сетевых соединений

lsof -i

Список процессов, работающих с портом 80

lsof -i :80

Linux – многозадачная среда. Даже консоль тоже является многозадачной.

Можно открыть несколько консолей, открыв в каждой из них по программе. Переключение между консолями будет производиться с помощью клавиш Ctrl+ <Alt+Fx>, где x – номер консоли.

Часто используемые пользователем переменные окружения это:

PATH — переменная содержит пути, в которых системе следует искать исполняемые файлы, если в командной строке не набирается полный или относительный путь к ним.

PWD — переменная содержит полное имя текущей директории.

HOME — переменная содержит полный путь домашнего каталога пользователя.

HOSTNAME — переменная содержит имя компьютера.

SHELL — содержит имя командной оболочки, запущенной в текущем сеансе.

USER — содержит имя пользователя, сеанс которого открыт сейчас.

Список переменных, установленных в системе можно увидеть с помощью команды export, введенной без параметров.

В современных Linux-системах механизм планирования заданий реализован с помощью демонов планирования заданий – at и cron.

С помощью этих программ появляется возможность установить выполнение программы на заранее известное время. Команда at используется в тех случаях, когда выполнение задания — разовая процедура.

Семейство команд at (at, atq, atrm) представляет собой инструменты для выполнения задания в определенное время по таймеру. Для правильного функционирования данной команды в системе должен быть запущен демон atd. Демон atd поддерживает очередь заданий, которые должны быть выполнены в то или иное время.

Для постановки задания (или нескольких заданий в очередь на одно и то же время) вам необходимо выполнить команду at:

Пример 1.

```
[student@Klass801 student]$ at 19:00
at> ls –l > /home/student/ls.txt
```

>Control-D>
job 1 at 2004-12-01 13:01
[student@Klass801 student]$_

Просмотреть очередь заданий можно используя команду atq:

Пример 2.

[student@Klass801 student]$ atq
1 2004-12-01 13:01 a student
[student@Klass801 student]$

Команда at позволяет поставить в очередь несколько заданий, которые будут последовательно выполнены друг за другом. Сделать это можно как в интерактивном режиме (набрав команду at в командной строке), так и указав команде at параметр -f:

[student@Klass801 student]$ at -f commands 14:50
job 8 at 2004-12-05 14:50
[student@Klass801 student]$_

Команда atrm удаляет из очереди задание:

[root@ns root]# atq
7 2004-12-05 14:48 a root
8 2004-12-05 14:50 a root
[root@ns root]# atrm 7
[root@ns root]# atq
8 2004-12-05 14:50 a root
[root@ns root]#

Если же задание предполагается выполнять с какой-либо периодичностью, то лучше всего использовать демон cron и команду crontab.

Демон cron, и команда управления планированием crontab позволят точно планировать задания. Задания запускает программа-демон crond. Команда crontab служит лишь для управления заданиями. Перед использованием команды необходимо создать файл, описывающий таблицу заданий (Файл crontab находится в /etc.).

Формат файла таков:

минуты часы дни_месяца месяц дни_недели команда

минуты – числа от 0 до 59, или *

часы – числа от 0 до 23, или *

дни_месяца – числа от 1 до 31, или *

месяц – числа от 1 до 12, или *

дни_недели – числа от 0 до 7, причем 0 или 7 – воскресенье, или *; например:

0 10 * * * /home/student/bin/script #запуск в 10:00 ежедневно

15 * * * 1 /home/student/bin/script2 #в 15 минут каждого часа в понедельник

Команда crontab позволяет также и редактировать список заданий с помощью параметра -e. В качестве редактора будет использоваться редактор, указанный (в порядке очередности) в переменной окружения $VISUAL, $EDITOR или /bin/vi. После сохранения файла, crontab автоматически переинициализирует таблицу заданий.

3.5 Конфигурационные файлы ОС Linux

Каталог **/etc** является одним из основных каталогов систем UNIX. Он содержит все базовые конфигурационные файлы системы.

Некоторые важные файлы каталога /etc:

- /etc/passwd это текстовый файл, который содержит всех пользователей системы и их зашифрованные пароли.
- /etc/inittab: конфигурационный файл для команды init, который играет основную роль в загрузке системы.

Непосредственно после того, как система Linux загружается и ее ядро монтирует корневую файловую систему, она выполняет первую программу -- init. После запуска программа init уходит в фоновый режим, следя за режимом работы системы и по необходимости изменяя его. Программа init должна следить за множеством вещей; все ее функции определены в файле /etc/inittab.

Например, при начале работы данный файл /etc/inittab запускает шесть виртуальных консолей. Для этого в фале /etc/inittab прописаны следующие строки:

```
c1:1235:respawn:/sbin/agetty 38400 tty1 linux
c2:1235:respawn:/sbin/agetty 38400 tty2 linux
c3:1235:respawn:/sbin/agetty 38400 tty3 linux
c4:1235:respawn:/sbin/agetty 38400 tty4 linux
c5:1235:respawn:/sbin/agetty 38400 tty5 linux
c6:12345:respawn:/sbin/agetty 38400 tty6 linux
```

- /etc/services: файл содержит список существующих сервисов сети.

Каждая строка в этом файле имеет такой формат:

service port/protocol [aliases]

Здесь service задает имя сервиса, port определяет номер порта, используемого этим сервисом, а protocol определяет, каким транспортным протоколом пользуется сервис. Имеется возможность различия протоколов udp или tcp. Сервис может работать с разными протоколами, а может быть два сервиса работают на одном порте, но с разными протоколами. Поле *aliases* (необязательное) позволяет задавать несколько имен (псевдонимов) для одного сервиса.

Пример части файла /etc/services:

```
ftp         21/tcp          # File Transfer Protocol (Control)
telnet      23/tcp          # Virtual Terminal Protocol
smtp        25/tcp          # Simple Mail Transfer Protocol
```

- /etc/profile: это конфигурационный файл shell, управляет системными переменными окружения.
- /etc/crontab: конфигурационный файл команды cron, программы, ответственной за периодическое выполнение программ.
- /etc/fstab: Список файловых систем, автоматически монтируемых при загрузке системы командой mount –a.

Каждая запись имеет следующие поля (которые разделяются пробелом или табуляцией):

<file system> <dir> <type> <options> <dump> <pass>

- Поле, <file system> *(файловая система)* сообщает демону монтирования файловых систем mount, что монтировать, имя монтируемого устройства.
- Второе поле, <dir> *(директория)*, определяет путь, по которому будет смонтирована <file system>.
- Поле <type> *(тип)* содержит тип файловой системы монтируемого устройства.
- dump> — используется утилитой dump для того чтобы определить, когда делать резервную копию. После установки, dump проверяет эту запись и использует значение, чтобы решить, подключать ли файловую систему. Возможные значения 0 или 1. Если 0, dump игнорирует файловую систему, если 1, dump сделает резервную копию. У большинства пользователей dump не установлен, поэтому в поле <dump> следует задать 0.
- <pass> *(номер прохода)*. Утилита для восстановления файловой системы fsck проверяет число, подставленное в поле <pass> и решает, в каком порядке проверять файловую систему. Возможные значения 0, 1 и 2. Файловые системы со значением <pass>, равным 0, не будут проверены утилитой fsck. У корневой системы должен быть наибольший приоритет, 1, остальные файловые системы должны иметь приоритет 2. Если равен единице, значит проверка будет производиться. Файловые системы проверяются в том порядке, в котором они описаны в этом файле. Если Вы хотите изменить порядок проверки, вместо единицы используйте двойку. Тогда сначала проверяются все файловые системы с единицей, а затем с двойкой.

Пример обычного файла fstab:

```
# <file system>  <dir>  <type>  <options>          <dump> <pass>
/dev/cdrom       /mnt/cd  iso9660  ro,user,noauto,unhide   0      0
/dev/dvd         /mnt/dvd  udf        ro,user,noauto,unhide   0      0
/dev/fd0         /mnt/fl    auto      user,noauto                0      0
/dev/hda1          swap       swap     defaults                   0      0
/dev/hda4            /          ext3     defaults                   0      1
/dev/hda3    /home      xfs    rw,suid,exec,auto,nouser,async 0      2
```

- /etc/group: Файл, описывающий группы пользователей (по аналогии /etc/passwd).
- /etc/hosts: Список хостов для преобразования имен в IP-адреса (обычно нужно для хостов локальной сети, о которых не знает система DNS).

Каждая строка в */etc/hosts* представляет один хост. Первая запись в каждой строке — это IP-адрес, а вторая — псевдоним этого хоста, а третья запись задает полностью определенное доменное имя (fully qualified domain name) хоста, например mail.absolutefreebsd.com.

```
# IP          local      fully qualified domain name
#
127.0.0.1     localhost
#
191.72.1.1    vlager     vlager.vbrew.com
191.72.1.2    vstout     vstout.vbrew.com
191.72.1.3    vale       vale.vbrew.com
```

- /etc/lilo.conf: Конфигурационный файл для LILO (LInux LOader, начальный загрузчик операционных систем).

Файл /etc/lilo.conf по умолчанию считывается системным менеджером загрузки lilo. Пример такого файла:

```
boot = /dev/hda2
delay = 50
# message = /boot/bootmesg.txt
root = current
image = /boot/vmlinuz-2.2.11-4bc
label = linux
read-only
```

other = /dev/hda1

table = /dev/hda

label = win

Строка boot указывает загрузочное устройство. Delay – определяет задержку для выбора системы.

С помощью команды message можно заставить загрузчик выдавать при загрузке произвольное сообщение.

Начиная со строки image, идут секции конфигурационного файла, соответствующие разным операционным системам, которые должны загружаться по выбору пользователя. В каждой такой секции имеется строка label. В этой строке записывается имя, которое вводится в ответ на приглашение LILO или является командой меню и служит для выбора пользователем загружаемой ОС. Если имя не выбрано по истечении времени, заданного строкой delay (задается в десятых долях секунды), то будет загружена ОС, выбираемая по умолчанию. В данном случае по умолчанию будет загружаться Linux, поскольку соответствующая ей секция стоит первой в файле. Можно указать загружаемую по умолчанию систему с помощью строки вида default=win (т. е., используя метку из соответствующей строки label).

Если вы задали строку (лучше сказать, секцию) other = /dev/hda1 в файле /etc/lilo.conf, то в корневом каталоге диска /dev/hda1 (диска C: в терминологии Microsoft) должен находиться вторичный загрузчик.

- /etc/mtab: Список смонтированных файловых систем в настоящий момент времени. Настраивается скриптом загрузки и обновляется командой mount.

Когда программа mount подключает файловую систему, она дописывает соответствующую строку в /etc/mtab. Ко-

гда umount отключает файловую систему, из этого файла соответствующая строка удаляется.

```
# cat /etc/mtab
/dev/hda3 / ext3 rw 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
/dev/hda5 /usr ext3 rw 0 0
/dev/hda6 /home ext3 rw 0 0
```

Более удобный для пользователя способ получения списка смонтированных файловых систем заключается в использовании утилиты df. Утилита df(название расшифровывается как diskfree - свободное пространство диска) имеет полезную дополнительную возможность, заключающуюся в выводе данных об объеме свободного пространства в каждой из смонтированных файловых систем, расположенных в разделах жестких дисков.

df показывает список всех файловых систем по именам устройств, сообщает их размер, занятое и свободное пространство и точки монтирования.

```
$ df -k
Filesystem          1K-blocks      Used Available Use% Mounted on
/dev/sda1            4166504   2449824   1505028  62% /
/dev/sda2           30056044  14173604  14351852  50% /usr
/dev/sda3           63988404   2690328  58047656   5% /var
tmpfs                524288        60    524228   1% /tmp
```

Ключ -k используется для отображения размеров блоками по 1 килобайту, вместо установленных по умолчанию блоков в 512 байт

- /proc/modules: Информация о том, какие модули ядра загружены в память в настоящий момент
- /var/run/utmp: Содержит информацию о пользователях, залогиненных в системе в настоящий момент. Команда who использует этот файл.

4. ПЛАН ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

1. Лабораторная работа №1. Администрирование пользователей ОС Windows.
2. Лабораторная работа №2. Работа с системными службами ОС Windows.
3. Лабораторная работа №3. Работа с реестром ОС Windows.
4. Лабораторная работа №4. Администрирование пользователей ОС Unix.
5. Лабораторная работа №5. Администрирование ОС UBUNTU SERVER 10.04 LTS.
6. Лабораторная работа №6. Работа с основными конфигурационными файлами ОС Unix.

4.1 Лабораторная работа № 1

Администрирование пользователей ОС Windows. Восстановление работоспособности ОС семейства Windows NT

Цель работы

Целью лабораторной работы является изучение возможных основных принципов работы с операционной системой семейства Windows NT, а также получение навыков восстановления работоспособности ОС Windows.

Задание на работу

1. Установить операционную систему Windows NT и изучить основные принципы работы с ней.
2. Настроить запуск в Безопасном режиме.
3. Удалить файл NTLDR, что приведет к неработоспособности операционной системы. Восстановить ОС с помощью консоли восстановления или загрузочного диска, скопировав файл NTLDR в корневой каталог логического диска, с которого производится загрузка («C:\»).

4. Настроить запуск виртуальной машины со съемных дисков. Загрузить систему с образа загрузочного диска. Изучить основные принципы работы с системой посредством загрузочного диска. Восстановить потерянные данные. Запустить проверку зараженного компьютера на вирусы.

5. Изучить работу по резервированию операционной системы с помощью профессиональных программ.

6. Подготовить отчет по выполненной лабораторной работе.

4.2 Лабораторная работа № 2

Работа с системными службами ОС Windows.

Цель работы

Изучить процессы, происходящие в оперативной памяти и процессоре, во время исполнения прикладной программы.

Задание на работу

1. Изучить рекомендации к выполнению работ.

2. Пользуясь рекомендациями, запустить, изучить и настроить для выполнения работы «Системный монитор».

3. Изучить порядок выполнения работ.

4. Выполнить лабораторную работу

5. Подготовить отчёт о проделанной работе в формате MS Word.

6. Ответить на контрольные вопросы

Рекомендации к выполнению работ:

1. В состав операционной системы Windows XP входит программа «Системный монитор», с помощью которой можно наблюдать за изменением различных показателей во время

работы компьютера, а также измерять производительность компьютера.

Запустите эту программу из меню программ: Пуск/Панель управления/Производительность и обслуживание/Администрирование и дважды щелкните по значку Производительность. Данный инструмент включает системный монитор (реализованный в виде элемента управления Active X) и Журналы и оповещения производительности (автономная оснастка для конфигурирования журналов производительности).

2. Система Windows XP получает информацию о производительности от компонентов операционной системы. Различные системные компоненты в ходе своей работы генерируют данные о производительности. Такие компоненты называются объектами производительности. В операционной системе имеется ряд объектов производительности, обычно соответствующих главным аппаратным компонентам, таким как память, процессоры и т. д. Приложения могут также инсталлировать свои объекты производительности. Каждый объект производительности предоставляет счетчики, которые собирают данные производительности. Например, счетчик Обмен страниц в сек(Pages/sec) объекта Память (Memory) отслеживает степень кэширования страниц.

Для просмотра данных, которые предоставляет конкретный счетчик, нажмите кнопку объяснения (Explain) в диалоговом окне добавления счетчиков добавить счетчики.

Если в системе установлено несколько процессоров, то объект процессор (Processor) будет иметь множество экземпляров. Более того, если объект поддерживает множество экземпляров, то при объединении экземпляров в группу появятся родительский экземпляр и дочерние экземпляры, которые будут принадлежать данному родительскому экземпляру.

Настроим программу так, чтобы видеть нужные нам характеристики.

Настройка счетчиков.

В окне «Системный монитор» на панели результатов в виде диаграмм отображаются показания счетчиков. В системе Windows XP это окно изначально содержит три счетчика: Обмен страниц в сек (Pages/sec)(объект Память), Средняя длина очереди диска (Avg. DiskQueueLength) (объект Физический диск) и % загруженности процессора (ProcessorTime) (объект Процессор). Для добавления других счетчиков выполните следующие действия:

a) На панели результатов щелкните правой кнопкой мыши и в контекстном меню выберите команду «Добавить счетчики», другой подход — нажать кнопку «Добавить» на панели инструментов или сочетание клавиш <Ctrl>+<!>.

b) В открывшемся окне выберите переключатель Использовать локальные счетчики для мониторинга компьютера, на котором запущена консоль мониторинга. Если вы собираетесь проводить мониторинг определенного компьютера, независимо оттого, где запущена консоль мониторинга, установите переключатель «Выбрать счетчики» с компьютера и укажите имя компьютера (по умолчанию установлено имя локального компьютера).

c) В списке Объект выберите объект для мониторинга.

d) В списке Выбрать счетчики из списка укажите счетчики, которые вы собираетесь использовать.

e) Для мониторинга всех выбранных экземпляров нажмите переключатель «Все вхождения». Для мониторинга только определенных экземпляров установите переключатель «Выбрать вхождения» из списка и выберите экземпляры, которые вы собираетесь отслеживать.

f) Нажмите кнопку «Добавить» и затем кнопку «Закрыть».

Нам нужны две диаграммы, показывающие, как загружен работой процессор и насколько занята оперативная память. Добавьте счетчики % загруженности процессора и «Диспетчер памяти».

Настройка способов представления информации.

Компонент «Системный монитор» предоставляет три средства просмотра информации о производительности системы: два графических (График и Гистограмма) и одно текстовое (Отчет). Для настройки внешнего вида окна мониторинга щелкните правой кнопкой мыши в окне диаграмм и выберите пункт «Свойства». В открывшемся окне для диаграммы и гистограммы можно задать ряд дополнительных параметров отображения:

— название диаграммы или гистограммы и дать название осям координат;

— диапазон вывода значений;

— характеристики кривой на диаграмме или колонок на гистограмме, такие как цвет, толщина, стиль и др. Для выбора способа просмотра информации производительности на вкладке «Общие» установите флажок для одной из опций «График», «Гистограмма» или «Отчет».

Вы увидите две диаграммы. Диаграммы "двигаются" влево, самая правая часть диаграммы - это то, что происходит в текущий момент. Первая диаграмма показывает, на сколько процентов загружен работой процессор, вторая - сколько памяти занято для работы всех программ.

Примечание. Объем используемой памяти может оказаться больше, чем реальный размер оперативной памяти. Тут нет никаких чудес — часть информации временно хранится на диске в специальном файле. Когда эти данные понадобятся, то будут загружены в оперативную память, а другие, давно не использовавшиеся, «сброшены» на диск.

Запустите процесс построения диаграмм заново.

3. Операционная система Windows многозадачная, т.е. мы можем запускать несколько программ, переходить из окна одной программы в окно другой. Не закрывая «Системный монитор», откройте графический редактор Paint, подождите немного, затем закройте.

4. На нижней диаграмме вы увидите (по колебаниям графика), как операционная система загрузила Paint в оперативную память, а затем выгрузила. На верхней диаграмме

видна работа процессора по запуску редактора и затем - по закрытию.

Возможно, вам придется отрегулировать скорость построения диаграмм (Диаграмма) и масштаб диаграммы загрузки памяти (Изменить представление).

Ваша задача: с помощью Системного монитора выяснить, как изменяется загрузка процессора и объем занятой оперативной памяти в ходе обычной работы с прикладной программой. Результаты лабораторной работы нужно будет оформить в виде отчета. Получившаяся в окне Системного монитора диаграмма должна быть «сфотографирована» и помещена в отчет с помощью, например, клавиши PrintScreen.

Порядок выполнения работы

1. Загрузите MS Word, откройте новый лист для отчета. Наберите заголовок, сохраните файл.

2. Запустите Системный монитор.

3. Раскройте на весь экран окно программы Системный Монитор и запустите графики заново.

4. После каждого из следующих действий переходите к окну с диаграммами, замечайте, что изменилось (между действиями выдерживайте небольшую паузу, чтобы отделить на диаграмме одно действие от другого):

• завершите работу программы MS Word;

• запустите Paint;

• перейдите к окну Системного монитора и нажмите клавишу PrintScreen, чтобы поместить картинку с экрана в буфер обмена;

• вставьте картинку из буфера обмена в документ программы Paint;

• сохраните файл с картинкой;

• завершите работу программы Paint.

5. Сделайте еще один "снимок" диаграмм и поместите именно его в ваш отчет.

6. Подпишите на диаграммах (на тех участках, где происходят изменения), какие действия вы выполняли.

7. Отметьте на картинке, какой объем памяти занимают операционная система, MS Word, Paint.

8. Создайте на листе вашего отчета таблицу и заполните ее: поставьте плюс, если устройство участвует в операции.

9. Поместите в отчет ответ на следующий вопрос: почему изменения на диаграмме памяти выглядят менее значительными в отличии от изменений на диаграмме процессора?

4.3 Лабораторная работа № 3

Работа с реестром ОС Windows. Организация пакетных файлов и сценариев в ОС Windows

Цель работы

Приобретение практических написания пакетных файлов ОС Windows, практическое знакомство с управлением вводом/выводом в операционных системах Windows и кэширования операций ввода/вывода, изучение основных команд для управления дисками и файлами.

Задание на работу

1. Ознакомиться с краткими теоретическими сведениями.

2. Ознакомиться с назначением и основными принципами написания командных файлов.

3. Изучить основные команды командных файлов и работу с параметрами.

4. Подготовить отчет для преподавателя о выполнении лабораторной работы и представить его в соответствии с графиком.

Задание1. Изучение команды SET.

1. Отобразите переменные среды двумя способами: из командной оболочки и окна свойств системы (Пуск| Панель управления| Система).

2. Задайте переменную среды, содержащую определенный путь к месту назначения, выбранный самостоятельно.

3. Проверьте наличие в системе переменной среды, заданной в предыдущем пункте задания.

4. Выведите значение выражения, определенного в соответствии с вариантом задания, в качестве переменной среды Result.

5. Задайте переменную среды с различными вариантами динамически формируемых значений. Варианты динамических значений выберете самостоятельно.

При выполнении задания используйте следующие инструкции:

• по каждому из пунктов задания в окне командной оболочки наберите соответствующую команду с необходимыми ключами;

• нажмите Enter для ввода;

• изучите полученный результат и сделайте вывод о проделанной работе;

• запишите полученную информацию в отчет.

Задание2. Изучение команд REM и ECHO.

Создайте пакетный файл, воспользовавшись любым текстовым редактором. Имя пакетного файла выберете самостоятельно.

1. Введите в созданный пакетный файл текст, приведенного выше примера.

2. Сохраните текст пакетного файла.

При выполнении задания используйте следующие инструкции:

– воспользовавшись командой Start и указав путь к пакетному файлу,

– запустите его на выполнение, нажав Enter для ввода,

– изучите пример и полученный с его помощью результат, обратив внимание

– на о, что команда Echo с точкой в конце выводит на экран пустую строку, а символ «коммерческое И» (@) перед командой Echo отключает режим отображения команд.

– сделайте соответствующий вывод и запишите его в отчет.

Задание3. Изучение утилиты FOR.

1. Скопируйте файлы каталога, путь к которому задайте самостоятельно, в точку назначения, заданную путем d:\Temp\. При копировании воспользуйтесь любым методом, изученным ранее.

2. К каждому из файлов, местоположение которых определено путем d:\Temp\, добавьте символ«!» в начале имени, воспользовавшись командой циклической обработки данных.

3. Подсчитать количество каталогов на локальном диске, воспользовавшись командой циклической обработки данных, в процессе выполнения выводя результат в переменную среды, выбранную самостоятельно. Проверьте полученный результат в файловом диспетчере Total Commander (Файл | Подсчитать занимаемое место), предварительно выделив содержимое локального диска.

4. Модифицируйте пакетный файл, полученный в предыдущем задании, воспользовавшись командой циклической обработки данных таким образом, чтобы в процессе его выполнения отображалось определенное количество раз выражение «********* the For command **********».

При выполнении задания используйте следующие инструкции: по каждому из пунктов задания в окне командной оболочки наберите соответствующую команду с необходимыми ключами, нажмите Enter для ввода, изучите полученный результат и сделайте вывод о проделанной работе, запишите полученную информацию в отчет.

Задание 4. Изучение команды IF.

Модифицируйте пакетный файл, полученный в предыдущем задании таким образом, чтобы выполнялись следующие условия:

1. Если не существует каталог d:\Temp\MyFont\, создайте его любым способом, изученным ранее. В противном случае выведите сообщение «Folder exists» (Каталог существует).

2. Если в каталоге d:\Temp\MyFont\ не существует файлов-шрифтов, скопируйте любые одним из методов, изученных ранее, из системного каталога c:\Windows\Fonts\. В противном случае выведите сообщение «Fonts exist» (Шрифты присутствуют).

3. Если в каталоге d:\Temp\MyFont\ существует файлы, удалите каталог вместе с его содержимым, изученным ранее способом и выведите сообщение «Folder deleted». В противном случае выведите сообщение «Folder is empty. Deleting is senseless» (Каталог пуст. Удаление бессмысленно).

Задание 5. Изучение принципов работы команды CALL.

1. Создайте новый (дочерний) пакетный файл, воспользовавшись любым текстовым редактором. Имя пакетного файла выберите самостоятельно.

2. Введите в дочерний пакетный файл процедуру форматирования гибкого диска, учитывающую переход в начало процедуры в случае ошибки, из приведенного выше примера.

3. Модифицируйте родительский пакетный файл, удалив из него лишние команды и добавив ссылку на дочерний пакетный файл для его вызова.

4. Сохраните тексты обоих пакетных файлов.

4.4 Лабораторная работа № 4

Администрирование пользователей ОС Unix. Основы администрирования ОС Windows Server

Цель работы

Изучение ОС Windows Server 2003. Получение навыков работы с учетными записями, локальными и глобальными группами.

Задание на работу

Для выполнения лабораторной работы нужно подключится к Windows 2003 Server. Для подключения к виртуальной машине выберете пункт Remote Desktop Connection в меню Пуск.

Требования к результатам выполнения лабораторного практикума:

– выполнить лабораторную работу в соответствии с заданием;

– составить отчет о проделанной работе;

– в отчете должны содержаться скриншоты, показывающие процесс выполнения заданий;

– отчет должен содержать выводы по результатам каждого выполненного задания;

– особое внимание обратить на планирование групп и их местоположение, включение в состав групп учетных записей пользователей.

Планирование групп

Предположим, пользователям Стамбульского и Квебекского доменов компании «Разноимпорт» необходим доступ к ресурсам обоих доменов. Вам — администратору сети компании — придется принять решение по следующим вопросам:

– глобальные группы и членство в них для каждого из доменов;

– локальные группы для каждого ресурса, включая местонахождение каждой группы;

– включение глобальных групп в состав локальных для предоставления пользователям доступа к ресурсам.

Занесите в шаблон планирования групп приведенные ниже сведения.

– имя группы — в графу «Название группы»;

– тип группы — локальная или глобальная — в графу «Локальная или глобальная»;

– учетные записи пользователей для каждой глобальной группы — в графу «Члены» (учетные записи пользователей Стамбульского и Квебекского доменов перечислены в приведенной ниже таблице; состав доменов одинаков);

– названия всех глобальных групп, которые будут включены в состав локальных групп, — в графу «Члены»;

– местонахождение сервера: главный контроллер домена, резервный контроллер или сервер — в графу «Местонахождение».

Принимая решения, имейте в виду следующее:

– всем сотрудникам необходим доступ к приложениям своего домена;

– всем сотрудникам необходим доступ к принтеру Стамбульского отделения;

– руководству и менеджерам обоих доменов необходим доступ к информации отдела кадров Квебекского домена;

– руководству, менеджерам, торговым представителям и персоналу по обслуживанию клиентов необходим доступ к данным о клиентах, которые находятся в Квебекском домене;

– сотрудникам бухгалтерий обоих доменов необходим доступ к данным о счетах бухгалтерии Квебекского домена;

– менеджерам обоих доменов необходим доступ к данным о сотрудниках, которые хранятся в Стамбульском домене.

Заполняя шаблон, руководствуйтесь изображенной схемой доменов (рис.1) и следующим списком пользователей:

– Vice President – Вице-президент;

– Director – Руководитель отдела кадров;

– SalesMgr – Торговый менеджер;

– SalesRep – Торговый представитель;

– CustomerServiceA – Представитель службы работы с клиентами (ночная смена);

– CustomerServiceB – Представитель службы работы с клиентами (дневная смена);

– AccountMgr – Главный бухгалтер;

– Accountant – Бухгалтер;

– Temp – Временный сотрудник.

Средствами консоли Active Directory создайте глобальные группы, запланированные в предыдущем задании.

Глобальная группа создается так.

1. Запустите консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Щелкните правой кнопкой контейнер, в который хотите поместить учетную запись пользователя. Выберите Создать (New), а затем Группа (Group). Откроется диалоговое окно Новый объект — группа (New Object — Group).

2. Введите имя группы. Имена глобальных учетных записей групп следуют тем же правилам, что и отображаемые имена для учетных записей пользователей. Они нечувствительны к регистру и могут содержать до 64 символов.

3. Первые 20 символов имени группы будут соответствовать имени группы в Windows NT версии 4.0 и более ранних версий. Это имя группы должно быть уникальным в домене. Если нужно, измените его.

4. Укажите область видимости группы — Локальная в домене (Domain Local), Глобальная (Global) или Универсальная (Universal).

5. Выберите тип группы: Группа безопасности (Security) или Группа распространения (Distribution).

6. Щелкните ОК.

Локальные группы создаются в консоли Локальные пользователи и группы (Local Users and Groups).

1. Откройте консоль Управление компьютером (Computer Management) с помощью одноименной команды меню Администрирование (Administrative Tools).

2. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дерене консоли и выберите «Подключиться к другому компьютеру» (Connect to Another Computer). Выберите систему, локальными учетными записями которой будете управлять. На контроллерах домена нет локальных пользователей и групп.

3. Разверните узел Служебные программы (System Tools) и выделите Локальные пользователи и группы (Local Users and Groups). Щелкнув правой кнопкой Группы (Groups), выберите «Создать группу» (New Group).

4. Введите имя и описание группы и щелкните кнопку «Добавить» (Add), чтобы добавить пользователей и группу.

5. В диалоговом окне Выбор: Пользователи (Select Users) введите имя нужного пользователя и щелкните «Проверить имена» (Check Names). Если совпадения найдены, укажите нужную учетную запись и щелкните ОК. Если совпадения не найдены, исправьте введенное имя и выполните поиск снова. При необходимости повторите этот шаг и по окончании щелкните ОК.

6. Если вы допустили ошибку, выберите имя пользователя и удалите его, щелкнув кнопку «Удалить» (Remove).

7. Завершив добавлять или удалять членов группы, щелкните «Создать» (Create).

Создайте все остальные локальные группы Квебекского домена, перечисленные в шаблоне планирования групп, и включите в их состав соответствующие учетные записи пользователей.

4.5 Лабораторная работа № 5

Мониторинг, оптимизация и аудит ОС Windows

Цель работы

Изучение программных модулей Msinfo32, Taskmgr.exe, Dxdiag.exe, Msconfig.exe

Задание на работу

Запустите на выполнение модули Msinfo32, Taskmgr.exe, Dxdiag.exe. Сверните появившиеся окна «Сведения о системе», «Средство диагностики DirectX» и «Диспетчер задач» на панель задач.

1. Разверните окно модуля «Сведения о системе» и последовательно просмотрите все категории сведений. При этом обратите внимание на то, что глобально все категории делятся на четыре класса «Ресурсы аппаратуры», «Компоненты», «Программная среда» и «Параметры обозревателя». Наиболее полезными с точки зрения сетевого администрирования являются категории «Конфликты/Совместное использование» и «Прерывания» в классе «Ресурсы аппаратуры», категория «Сеть» в классе «Компоненты», а также категории «Переменные среды», «Сетевые подключения» и «Службы» в классе «Программная среда». Необходимо отметить, что указанные классы ресурсов являются ценным источником системной информации, поскольку позволяют отслеживать аппаратные и программные изменения как локально, так и удаленно. Последнее может быть осуществлено посредством выбора «Удаленный компьютер…» в меню «Вид». Кроме того, отдельный интерес может представлять информация, собранная в классе «Параметры обозревателя».

2. Выберите «Журнал сведений о системе» в меню «Вид» и изучите его на предмет какие ресурсы аппаратуры и программные компоненты задействованы в текущий момент в системе.

3. Разверните окно следующего системного модуля «Диагностика DirectX», предназначенного для диагностирования аппаратных и программных компонентов компьютера, применяющихся для поддержки средств мультимедиа в играх и фильмах, и последовательно изучите все его вкладки. На вкладках «Дисплей», «Звук» и «Музыка» осуществите проверку соответствующих программных составляющих DirectX, а именно, интерфейсов DirectDraw, DirectSound и DirectMusic.

Сохраните все сведения в текстовый файл для отчета. Обратите внимание на то, что системный модуль «Диагностика DirectX» также может быть вызван из меню «Сервис» программного модуля «Сведения о системе».

4. Универсальный системный модуль «Диспетчер задач» как правило является наиболее часто используемым компонентом ОС, предназначенным для диагностики и мониторинга основных аппаратно-программных ресурсов системы, таких как центрального процессора, оперативной памяти, системных процессов. В частности, этот модуль позволяет управлять приложениями и процессами в оперативной памяти, снимать их с выполнения и назначать новое значение класса приоритета. Разверните окно системного модуля «Диспетчер задач» и последовательно ознакомьтесь со всеми его вкладками и меню. Выполните следующие действия:

– на вкладках «Приложения» и «Процессы» обратите внимание на количество работающих приложений и активных процессов,

– рядом с системным модулем «Диспетчер задач» разверните модуль «Сведения о системе» и откройте категорию «Выполняемые задачи» в классе «Программная среда»,

– в меню «Вид» в модуле «Диспетчер задач» добавьте следующие столбцы счетчиков: «память – максимум», «объем виртуальной памяти», «базовый приоритет», «счетчик потоков»,

– в модуле «Диспетчер задач» измените базовый приоритет процесса Dxdiag.exe на приоритет реального времени, перейдите в окно модуля «Сведения о системе», в меню «Вид» обновите системную информацию и обратите внимание на то, как изменилось значение в столбце «Приоритет» в категории «Выполняемые задачи»,

– на вкладке «Приложения» снимите с выполнения задачи «Сведения о системе» и «Средства диагностики DirectX», а на вкладке «Процессы» завершите процесс Taskmgr.exe.

– При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий по каждому из пунктов 1-5 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– результаты ознакомления с возможностями системного модуля «Диспетчер задач» занесите в отчет.

– сделайте вывод о проделанной работе.

4.6 Лабораторная работа № 6

Организация консоли администрирования в ОС Windows

Цель работы

Изучение консоли управления Microsoft Management Console (MMC)

Задание на работу

В лабораторной работе предполагается ознакомление с основными принципами организации и построения консоли администрирования MMC, а также с базовыми возможностями основных инструментов системного администратора — оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).

Перед началом выполнения заданий в среде ОС Windows XP необходимо выполнить следующее:

1. Запустить виртуальную машину с ОС Windows XP и активировать справочное меню (Пуск | Справка и поддержка);

2. Ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3. Ознакомиться возможностью получения сведений пункта 2 из альтернативного источника информации, доступного непосредственно в справке консоли администрирования MMC (Справка | Вызов справки);

4. Ознакомиться с описанием и возможностями оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).

Задание 1. Изменение параметров и способов настройки консоли администрирования ММС.

Задание 2. Добавление различных элементов и компонентов к дереву консоли администрирования ММС.

Задание3. Создание нового вида панели задач консоли администрирования ММС.

Задание 4. Добавление элементов и компонентов дерева консоли в виде списка ярлыков в меню «Избранное».

Задание 5. Ознакомление с оснасткой «Локальные пользователи и группы».

Задание 6. Взаимосвязь утилиты «Учетные записи пользователей» с оснасткой «Локальные пользователи и группы» при смене типа учетной записи.

Задание 7. Возможности оснастки «Локальные пользователи и группы» при работе с профилями пользователей.

Задание 8. Основные возможности оснастки «Редактор объекта групповой политики».

Задание 9. Возможности оснастки «Групповая политика» при настройке локального узла.

Задание 10. Возможности оснасток, предназначенных для диагностики, мониторинга, настройки и оптимизации.

Задание 11. Возможности оснастки «Просмотр событий».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Королев, Е.Н. Особенности работы с файловой системой ОС Linux [Текст]: учеб. пособие / Е.Н. Королев. − Воронеж: ВГТУ, 2007. - 134 с.

2. Татенбаум Э. Современные операционные системы [Текст] / Э. Татенбаум. – 2-е изд. – СПб.: Питер, 2002. – 1040 с.

3. Олифер, В.Г. Сетевые операционные системы [Текст] / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2002. – 544 с.

4. Робачевский, А.М. Операционная система Unix [Текст] / А.М. Робачевский. – СПб.: BHV – Санкт - Петербург, 1997. – 528 с.

5. Керниган, Б. Unix - универсальная среда программирования [Текст] : пер. с англ. / Б. Керниган, Р. Пайк – М.: Финансы и статистика, 1992. – 304 с.

6. Unixhelp for Users (http://www.winterweb.com/UNIX/)

ОГЛАВЛЕНИЕ