Операционная система «ОСь» 2.1
Руководство администратора
Листов 16

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством администратора операционной системы «ОСь» (далее — «ОСь» или ОС).

Руководство описывает основные действия системного администратора после установки: загрузку системы; вход в систему; решение проблем. Полное руководство администратора оформлено в виде интерактивной справочной системы и поставляется на диске с ОС.

СОДЕРЖАНИЕ

1. ЗАГРУЗОЧНОЕ МЕНЮ

Старт операционной системы начинается с загрузочного меню. При помощи загрузочного меню, можно выбрать загрузку необходимой ОС (если установлено несколько ОС или несколько ядер ОС), можно передать ядру различные параметры до начала загрузки операционной системы.

Где:

– «Операционная система ОСь *версия ядра*» — обычная загрузка операционной системы;

– «e» (лат.) — изменение параметров ядра;

– «c» (лат.) — переход в командную строку.

Из меню загрузчика можно продолжить загрузку операционной системы, нажав клавишу [Enter]. Если на машине установлено несколько операционных систем, загрузчик предлагает выбрать одну из них, используя стрелки клавиатуры.

1.1. Вход в меню загрузчика

Включите компьютер, дождитесь окончания тестов базовой системы ввода-вывода и появления окна загрузчика. По умолчанию загрузчик ждёт несколько секунд, после чего начинает загрузку операционной системы. Если во время приветствия загрузчика нажать клавишу [e], откроется меню редактирования параметров загрузки.

Меню загрузчика может быть заблокировано, если установлен пароль загрузчика. Для того чтобы продолжить работу, нажмите клавишу [p] и введите пароль загрузчика.

1.2. Изменение параметров ядра

Для того чтобы изменить параметры ядра, нажмите клавишу [e] в меню загрузчика. Откроется редактор параметров загрузки, использующийся для настройки параметров до загрузки ОС. Параметры ядра находятся в строке, начинающейся со слова `linux`.

Параметры ядра — это командная строка, в которой нужно задавать аргументы вида:

```
<параметр>=<значение>
```

Аргументы необходимо разделять пробелом. В строке загрузки ядра уже установлены некоторые аргументы, изменять их или удалять не рекомендуется.

1.3. Командная строка

Нажмите [c], чтобы перейти в командную строку загрузчика. Командная строка загрузчика напоминает обычную командную строку Linux, но поддерживает ограниченное количество команд. По клавише [Tab] выводится список команд дополняющих набранную в строке команду. Для выхода из режима командной строки нажмите клавишу [ESC].

2. ПОЛУЧЕНИЕ ПРАВ СИСТЕМНОГО АДМИНИСТРАТОРА

2.1. Вход в систему системного администратора

После завершения загрузки выбранного варианта ОС отобразится окно приглашения входа в систему.

Вверху окна отображается дата и время.

В середине окна отображаются поля ввода имени и пароля. В качестве имени пользователя введите `root`, в поле «Пароль» — пароль пользователя `root`, заданного при установке ОС и нажмите клавишу [Enter].

При неверном вводе пароля администратора отобразится сообщение об ошибке, введите правильный пароль и нажмите клавишу [Enter].

П р и м е ч а н и е. Если система установлена без графического интерфейса, появится приглашение входа в режиме командной строки (`login:`). Введите `root`, [Enter], пароль `root`, [Enter].

2.1.1. Администрирование операционной системы

Администрирование операционной системы должно производиться от имени системного администратора. Системный администратор в ОС всегда имеет специальное имя пользователя: `root`, однако права администратора может получить обычный пользователь, зная пароль `root`. Пароль системного администратора запрашивается при установке операционной системы.

При загрузке операционной системы появляется приглашение входа в систему. Чтобы войти в систему как системный администратор, введите в качестве имени пользователя `root`, а в качестве пароля — тот пароль, что был указан при установке системы.

Во время работы под учётной записью обычного пользователя можно также осуществить вход от системного администратора при помощи команды `su`. Использовать команду `su` можно только на этапе первоначальной настройки операционной системы.

2.1.2. Администрирование при помощи sudo

Чтобы не работать постоянно от имени `root`, рекомендуется создать обычного пользователя с правами администратора. Данный пользователь сможет выполнять те же задачи, что и `root`, используя команду `sudo`.

1 способ.

При установке системы, при создании первого пользователя, выбрать пункт «Сделать пользователя администратором».

2 способ.

Если пользователь уже существует, его нужно добавить в группу `wheel`:

```
usermod -aG 'wheel' user
```

Теперь для выполнения команд от имени системного администратора достаточно будет выполнить от имени пользователя `user1`:

```
$ sudo <команда с аргументами>
```

`sudo` требует ввод пользовательского пароля (а не пароля системного администратора).

Чтобы организовать администрирование без необходимости ввода пароля, нужно добавить строку в файл `/etc/sudoers`:

```
user ALL=(ALL) NOPASSWD: ALL
```

Для изменения файла `/etc/sudoers` используйте команду `visudo`.

2.2. Получение подробной справочной информации

Данное руководство содержит минимальный набор сведений для начала администрирования ОС. Для получения подробного руководства об администрировании ОС, выберите в главном меню программу «Документация → Руководство администратора».

3. РЕШЕНИЕ ПРОБЛЕМ

В данном разделе перечислены основные проблемы, которые могут возникнуть в процессе настройки и/или эксплуатации ОС.

3.1. Вход в терминал

Если графическая система «зависла» и не отвечает на действия пользователя, можно выполнить вход в командной строке, чтобы корректно перезагрузить ОС. Нажмите сочетание клавиш [Ctrl+Alt+F2] и введите пользователя и пароль. Далее завершите «зависший» процесс, выполните диагностические процедуры, описанные ниже, или перезагрузите компьютер командой `reboot`.

3.2. Диагностика потребления ресурсов

В случае, когда ОС начинает реагировать на команды пользователя непривычно долго, выполните от имени системного администратора следующий сценарий диагностики:

1) выполните команду `free` для просмотра статистики использования памяти и файла подкачки:

```
# free -m
```

В случае, когда поле `used` значительно превышает поле `free`, низкая производительность может оказаться следствием чрезмерного потребления памяти каким-либо из процессов;

2) выполните команду `df` для просмотра статистики использования дисков. Если какой-либо из дисков заполнен более чем на 95% — это может приводить к значительному снижению производительности операций ввода-вывода. Наиболее частая причина внезапного исчезновения свободного места на жёстком диске — переполнение каталогов `/var/log` и `/tmp`;

3) выполните команду `top` для просмотра списка процессов, которые наиболее интенсивно используют центральный процессор. Данная строка показывает, что центральный процессор нагружен только наполовину:

```
Cpu(s): 52.6%us
```

Стоит учитывать, что на многоядерных процессорах степень загруженности зависит от числа процессоров. Например, на четырёхъядерной машине в списке процессов потребление процессорного времени будет обозначаться как 200%,

что означает полную загрузку только двух ядер из четырёх, при этом поле `Cpu(s)` будет отображать загрузку примерно 50%. Для того чтобы найти процесс, который потребляет больше всего оперативной памяти, нажмите сочетание клавиш [Shift+M]. Имеет смысл ориентироваться на объём занимаемой резидентной памяти (столбец `RES`);

4) для того чтобы уничтожить проблемный процесс, выполните команду:

```
# kill <PID>
```

или

```
# killall <имя>
```

Выполняя команду `killall` стоит иметь в виду, что будут уничтожены все процессы с таким же именем. Если после выполнения команды `killall` процесс продолжает работу («завис»), можно принудительно уничтожить процесс:

```
# kill -9 <PID>
```

или

```
# killall -9 <PID>
```

ВНИМАНИЕ! ВСЕ НЕСОХРАНЁННЫЕ ДАННЫЕ ПРОЦЕССА БУДУТ ПОТЕРЯНЫ. ИСПОЛЬЗУЙТЕ ДАННЫЙ МЕТОД ТОЛЬКО В КРАЙНЕМ СЛУЧАЕ.

3.3. Диагностика ошибок

Если при работе ОС возникает ошибка, характер которой не удаётся определить, наиболее результативным способом диагностики является чтение журналов. Выполните команду `journalctl -e`. В конце журнала находятся последние сообщения, которые имеют отношение к поломке. Для диагностики проблем на уровне ядра, запустите команду `dmesg`.

3.4. Восстановление пароля root

В случае, когда пароль root утерян или неизвестен, при наличии физического доступа к компьютеру его можно сбросить.

При загрузке системы нажмите `e` (редактировать параметры загрузки).

Найти строчку, которая начинается со слова «linux», в конец параметров ядра дописать:

```
rw init=bin/sh
```

Нажать [Ctrl+X] для загрузки. Система войдёт в режим обслуживания (см. ниже).

Выполнить команду `chroot /sysroot`.

Выполнить команду `passwd` и ввести новый пароль root.

Создать файл `.autorelabel` командой `touch .autorelabel`.

Выполнить команду `exit`.

Выполнить команду `reboot`.

Система дважды перезагрузится, что может занять время.

3.5. Восстановление системы из режима обслуживания

В случае нарушения работы, программного или аппаратного сбоя или ошибке администратора при настройке системы, после перезагрузки операционная система переходит в режим обслуживания (maintenance mode) или не может загрузиться. В этот режим система переходит автоматически при обнаружении проблем, на экран выводится краткое описание ошибки и предложение о вводе пароля системного администратора. Посмотреть подробную информацию о возникшей проблеме можно командой `journalctl -e`.

Для того, чтобы приступить к разрешению проблемы, введите пароль системного администратора. После ввода пароля появится приглашение командной строки и можно приступать к исправлению проблемы.

Наиболее частые причины аварийного перехода системы в режим обслуживания:

– нарушена целостность файловой системы;

– неправильная конфигурация жестких дисков (например, ошибка в файле `/etc/fstab`).

3.5.1. Восстановление файловой системы

Если проблема заключается в ошибке на жестком диске, необходимо выполнить команду `fsck`, указав проблемный раздел. Раздел, на котором произошла ошибка, обычно всегда выводится в терминал при входе в режим обслуживания. Выполните команду:

```
# fsck <путь до раздела>
```

Здесь, `<путь до раздела>` — полный путь до устройства жёсткого диска, на котором произошла ошибка.

Пример для раздела диска, размеченного с помощью логических томов:

```
# fsck /dev/mapper/VolGroup-lv_var_log
```

Пример для диска, размеченного классическим образом (по разделам):

```
# fsck /dev/sda1
```

3.5.2. Восстановление пароля root

Просто выполните `passwd` внутри `chroot /sysroot` и создайте файл `.autorelabel` (см. выше).

3.5.3. Восстановление повреждённых файлов и другое

В режиме обслуживания система загружается с примонтированной корневой файловой системой в режиме «только чтение», причём корневая файловая система ОС находится в каталоге `/sysroot`. Для того чтобы получить возможность изменения конфигурационных файлов на жёстком диске, необходимо выполнить перед этим следующую команду:

```
# mount -o remount,rw /sysroot
```

После этого корневая файловая система будет примонтирована в режиме «чтение/запись» и станет возможной правка файлов.

Смонтируйте `/dev`, `/proc` и `/sys` внутрь `sysroot`:

```
# mount -o bind /dev /sysroot/dev
# mount -o bind /proc /sysroot/proc
# mount -o bind /sys /sysroot/sys
```

Выполните вход в `sysroot` командой `chroot /sysroot`. Если система повреждена настолько, что `chroot` выполнить невозможно, необходимо восстановить систему используя ограниченный набор утилит аварийного режима. Вход в окружение `chroot` необходим, так как ОС загружается в режиме ограниченной функциональности и многие команды в таком режиме отсутствуют.

После этого вы можете:

– восстановить fstab;

– переустановить загрузчик;

– прочитать системный журнал и отключить службу, которая не даёт загрузиться ОС.

По окончании работы нужно выполнить команду `exit`, затем команду `reboot`.

3.6. Проверка и восстановление поврежденных файлов

В процессе неправильной настройки или эксплуатации операционной системы может возникнуть необходимость диагностики и/или восстановления как бинарных модулей системы, так и конфигурационных файлов.

Диагностика повреждённых файлов осуществляется командой `rpm`, а восстановление — командой `yum reinstall`. Обе команды могут быть запущены только от имени системного администратора. Данный инструмент является одним из наиболее эффективных средств диагностики, так как позволяет обнаружить:

– изменения в системных конфигурационных файлах, которые привели к неработоспособности системы/службы/приложения;

– удалённые или повреждённые системные файлы: библиотеки, приложения, ресурсы;

– изменения дискреционных прав доступа по умолчанию на файлы и каталоги, которые могут приводить к неработоспособности некоторых приложений и служб.

3.6.1. Локализация повреждённых файлов

Локализовать поврежденные файлы и характер повреждения позволяет встроенный механизм верификации (проверки). Для запуска механизма проверки необходимо запустить команду `rpm`.

Общая форма команды проверки `rpm` приведена ниже:

```
rpm -V|--verify [<параметры выбора>] [<параметры проверки>]
```

Операция проверки пакета сравнивает информацию о файлах установленных из пакета с информацией о них из метаданных пакета, хранимых в базе данных `rpm`. Среди прочего при проверке сравниваются размер, контрольная сумма, права доступа, тип, владелец и группа каждого файла. Любые расхождения будут отображены.

Файлы, которые не были установлены вместе с пакетом, например, файлы документации, исключенные при помощи параметра `--excludedocs`, будут проигнорированы без предупреждения.

Параметры выбора пакетов являются аналогичными запросу пакетов.

Параметры, уникальные для режима проверки, приведены ниже.

`--nodeps` не выполнять проверку зависимостей пакетов.

`--nodigest` не проверять при чтении дайджест пакета или заголовка.

`--nofiles` не проверять атрибуты файлов пакетов.

`--noscripts` не выполнять скриптлет `%verifyscript` (если существует).

`--nosignature` не проверять при чтении подпись пакета или заголовка при чтении.

`--nolinkto` не проверять изменение символьных ссылок (атрибут L).

`--nomd5` не проверять изменение контрольной суммы (атрибут 5).

`--nosize` не проверять изменение размера файла (атрибут S).

`--nouser` не проверять изменение владельца файла (атрибут U).

`--nogroup` не проверять изменение группы владельца файла (атрибут G).

`--nomtime` не проверять изменение времени изменения файла (атрибут T).

`--nomode` не проверять изменение прав доступа файла (атрибут M).

`--nordev` не проверять изменение номера устройства (атрибут D).

Формат вывода представляет собой строку из 8 символов и маркера из заголовка пакета, за которыми следует имя файла. Возможные маркеры атрибутов:

– `c %config` конфигурационный файл;

– `d %doc` файл документации;

– `g %ghost` «файл-призрак» (т. е. содержимое файла не включено в состав пакета);

– `l %license` файл с лицензией;

– `r %readme` файл readme.

Каждый из восьми символов отражает результат проверки атрибута(ов) файлов с значением того же атрибута, записанного в базе данных. Символ «.» (точка) означает, что проверка прошла, а символ «?» (вопросительный знак) означает, что проверка не может быть выполнена (например, права доступа к файлу не позволяют провести чтение). В противном случае будут отображены символы (для привлечения внимания выделены жирным), показывающие сбой проверки соответствующего `--verify` теста:

`S` — размер файла отличается;

`M` — режим доступа отличается (включая права доступа и тип файла);

`5` — отличается контрольная (MD5) сумма (как правило, это означает отличие в содержимом файла);

`D` — отличается старший/младший номер файла устройства;

`L` — отличается путь ссылки;

`U` — отличается владелец;

G — отличается группа владельца;

T — отличается время изменения.

Если проблемный пакет известен, лучше производить проверку только для одного конкретного пакета, так как объем выводимой информации сильно уменьшится. Например, проверка пакета kernel (ядро операционной системы):

```
# rpm -V kernel
```

Если команда ничего не выводит на экран, это означает, что все файлы в данном пакете не изменились с момента установки операционной системы.

В случае обнаружения файлов, отличающихся от предустановленных, rpm выведет их на экран:

```
# rpm -V httpd
S.5....T.  c /etc/httpd/conf/httpd.conf
```

В данном примере видно, что конфигурационный файл /etc/httpd/conf/httpd.conf (о чём свидетельствует символ c) имеет другой размер (S), отличается по содержимому (5) и времени изменения (T). Это стандартный набор изменений для конфигурационного файла: системные администраторы их часто меняют, чтобы изменить поведение веб-сервера и настроить программу под свои нужды, при этом меняется содержимое, размер и временная метка файла.

Можно также выполнять фильтрацию командой grep, если изменений очень много:

```
# rpm -V apache | grep ^??5
```

В данном примере будут выведены только те файлы, у которых изменилось содержимое. Контрольная сумма наиболее точно определяет изменения в файле, так как изменения в размере при изменения файла может и не происходить.

3.6.2. Восстановление файлов

В случае возникновения подобных проблем с целостностью системных файлов, можно прибегнуть к процедуре восстановления файлов с диска или репозитория. Для этого потребуется вставить DVD с ОС в устройство чтения дисков или подключить внешний репозиторий с пакетами ОС.

Рассмотрим ситуацию: администратор редактировал файл /etc/httpd/conf/httpd.conf для настройки веб-сервера и в определённый момент изменил его таким образом, что веб-сервер больше не работает.

В первую очередь, нужно установить, к какому пакету принадлежит файл:

```
# rpm -qf --qf '%{N}\n' /etc/httpd/conf/httpd.conf
httpd
```

Вывод команды сообщает, что файл относится к пакету `httpd` (версию и прочую информацию можно опустить).

Следующий этап — проверка данного пакета:

```
# rpm -V httpd
S.5....T.  c /etc/httpd/conf/httpd.conf
```

Вывод данной команды подтверждает наличие изменений в конфигурационном файле и только в нём. Перед восстановлением нужно удалить исходный файл. Так как удаление файла приведёт к невозможности его восстановить, рекомендуется вместо удаления всегда переименовывать файл:

```
# mv /etc/httpd/conf/httpd.conf{,.bak}
```

Таким образом, будет сохранена резервная копия, а впоследствии можно будет сравнить два файла конфигурации, чтобы точнее диагностировать проблему.

Восстановить удалённый (переименованный) файл можно следующей командой:

```
# yum reinstall -y httpd
```

Дождитесь окончания работы команды `yum`, после чего убедитесь, что файл восстановлен:

```
# rpm -V httpd
```

Вывод команды должен быть пуст.

После того как файл был восстановлен, следует приступить к анализу изменений конфигурационного файла, которые привели к ошибке:

```
# diff /etc/httpd/conf/httpd.conf{,.bak}
```

По завершении анализа можно будет перенести настройки из резервной копии в основной конфигурационный файл с учётом исправления ошибок.

Аналогичным образом можно восстановить любой повреждённый файл в системе, включая программы, библиотеки и т. п.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

КСЗ — комплекс средств защиты
НСД — несанкционированный доступ
ОС — операционная система
ПО — программное обеспечение
ПРД — правила разграничения доступа
ФС — файловая система