ЦИФРОВАЯ АКАДЕМИЯ

Вебинар №5.
Модули ядра, устройства, архивация, журналирование и запуск по расписанию

Что будет сегодня

ЦИФРОВАЯ АКАДЕМИЯ

Узнаете об управлении устройствами и модулями ядра

Познакомитесь с файловыми хранилищами в ОС Astra Linux

Узнаете об архивации и сжатии данных

Узнаете о системе журналирования и научитесь запускать задания по расписанию

ЦИФРОВАЯ АКАДЕМИЯ

Управление устройствами и модулями ядра

Псевдофайловая система sysfs

Система файлов sysfs является псевдофайловой системой в Linux, которая предоставляет информацию о различных компонентах системы в виде файлов и каталогов.
Sysfs представляет собой интерфейс для ядра и пользовательских программ для взаимодействия с аппаратными средствами системы и управления ими.
В Astra Linux sysfs также используется для доступа к информации об аппаратном обеспечении и устройствах.

Менеджер устройств systemd-udevd

Systemd-udevd — это демон*, который управляет устройствами в системе.
Он отвечает за обнаружение, создание и удаление устройств во время загрузки системы и во время её работы.
Systemd-udevd используется в различных дистрибутивах Linux, в том числе и в Astra Linux.

ЦИФРОВАЯ АКАДЕМИЯ

Правила udev

Правила udev — это инструкции, которые определяют, как система Linux должна обрабатывать устройства, включая их создание, изменение и удаление. В Astra Linux правила udev создаются в каталоге /etc/udev/rules.d/.
udevadm — это утилита командной строки для управления демоном systemd-udevd. Она предоставляет множество команд для отладки, тестирования и настройки работы systemd-udevd. Некоторые частые примеры использования udevadm включают:

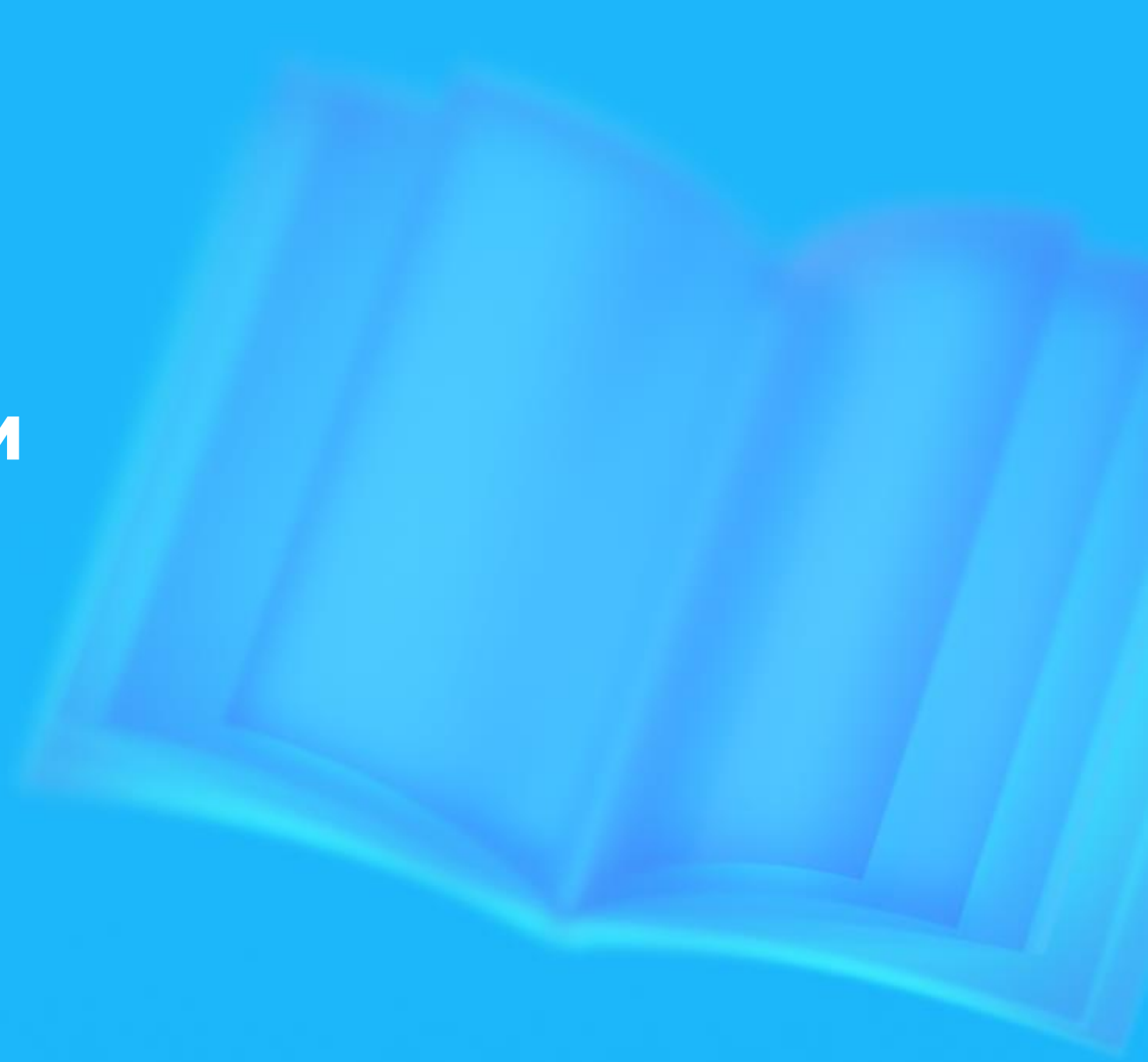
- Информацию об устройстве: udevadm info позволяет выводить подробную информацию о заданном устройстве, такую как идентификатор, атрибуты и дополнительную информацию о драйверах и подсистемах.
- Мониторинг событий: udevadm monitor позволяет отслеживать события, связанные с устройствами, такие как подключение и отключение устройств. Эта команда может быть особенно полезна при отладке и тестировании устройств.

В Astra Linux информация об устройствах может быть получена с помощью команд и утилит, таких как lsusb, lspci, lsblk, udevadm и других.

Управление модулями ядра в Astra Linux можно осуществлять с помощью различных команд и утилит, таких как lsmod, modinfo, modprobe, rmmod и других.

ЦИФРОВАЯ АКАДЕМИЯ

Сетевые каталоги



КОНФИГУРАЦИОННЫЙ ФАЙЛ SMB.CONF

Конфигурационный файл (smb.conf), который мы создали, состоит из трёх секций:
1. global — отвечает за общие настройки Samba-сервера;
2. public — секция описания настроек директорий общего доступа;
3. private — секция описания настроек директорий общего доступа.

Защищённой сетевой файловой системой для работы с информацией ограниченного доступа в Astra Linux Special Edition является Samba SMB/CIFS.

NFS – ТЕКСТ

NFS (сетевая файловая система) позволяет хосту монтировать разделы, находящиеся на удалённом хосте, и использовать их аналогично локальным файловым системам. Это позволяет централизованно хранить файлы и получать к ним полноценный доступ с разных хостов.
Для настройки NFS-сервера требуется утилита nfs-kernel-server.

При работе в Astra Linux Special Edition с включённой политикой мандатного управления доступом (МРД) и обработкой информации ограниченного доступа применять сетевую файловую систему NFS для хранения данных в общем случае не рекомендуется.

FTP-СЕРВЕР

ЦИФРОВАЯ АКАДЕМИЯ

VSFTP (от англ. Very Secure FTP) — это сервер FTP (File Transfer Protocol), который предоставляет возможность обмена файлами между компьютерами по сети. VSFTP является одним из самых быстрых и безопасных FTP-серверов для Linux-систем.

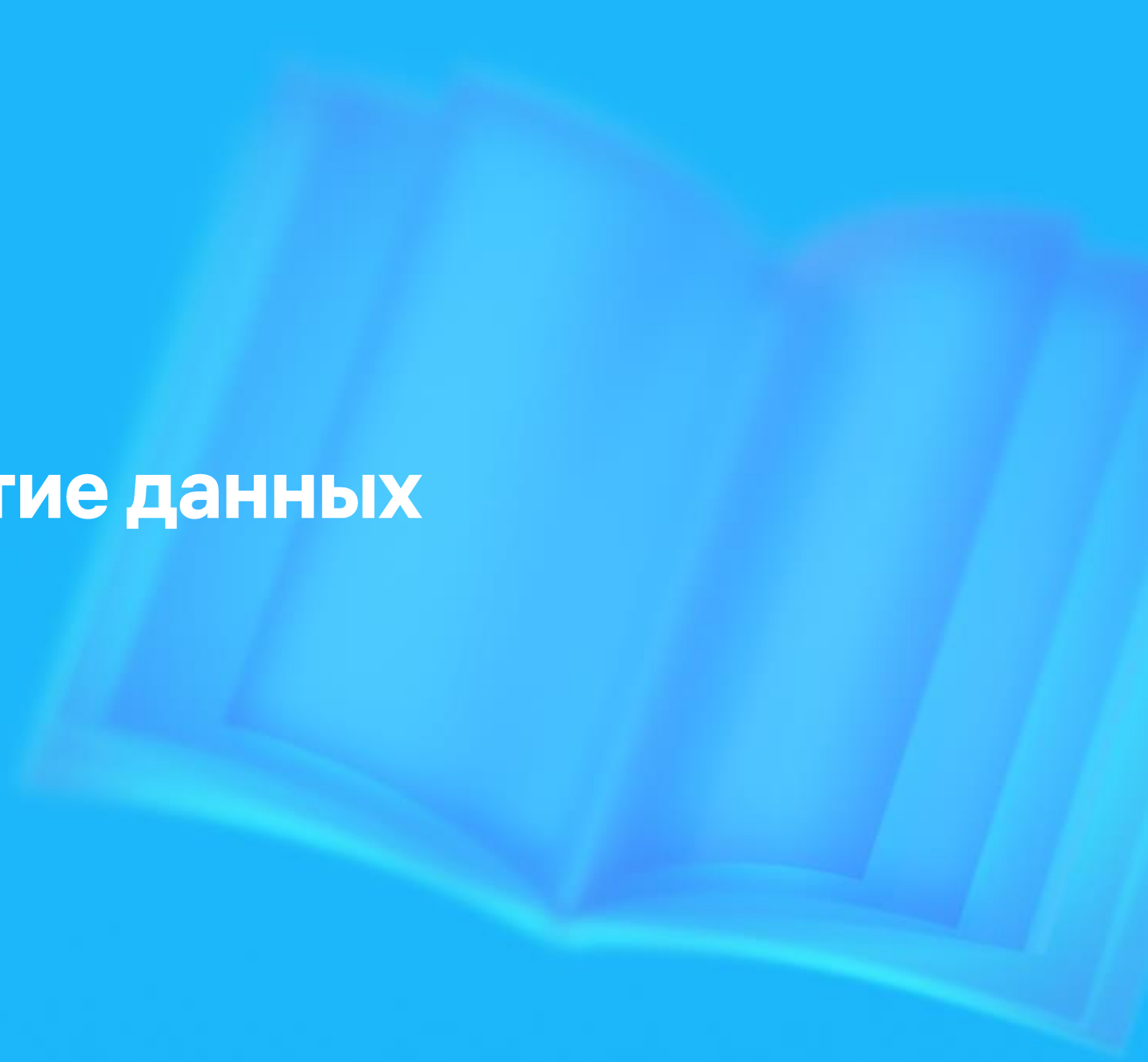
Особенности VSFTP-сервера:

- VSFTP использует шифрование SSL/TLS для обеспечения безопасности при передаче данных.
- VSFTP поддерживает многопользовательский режим с контролем доступа на основе IP и пользователей.
- Сервер обслуживает FTP, FTPS и SFTP- протоколы.
- VSFTP предоставляет функцию ограничения скорости передачи, чтобы избежать перегрузки сервера.
- В сборке VSFTP присутствует несколько функций для защиты от DDoS-атак.

Сервер поддерживает обычный режимы работы, то есть только авторизации, и анонимный. В анонимном режиме пользователи могут подключаться к серверу, не предоставляя учётных данных для аутентификации, что может быть полезно для обмена общедоступными файлами в интернете.

ЦИФРОВАЯ АКАДЕМИЯ

Архивация и сжатие данных



Архивирование/разархивирование

tar -cvf archive.tar(tar.gz) file1 file2 directory1

Некоторые опции команды tar:

- **c** — создание архива;
- **v** — вывод списка обрабатываемых файлов на экран;
- **f** — указание имени архива;
- **r** — добавление файлов в уже существующий архив;
- **x** — извлечение файлов.

Клонирование дисков

ЦИФРОВАЯ АКАДЕМИЯ

Для выполнения клонирования диска в Linux с помощью **dd** выполните следующую команду:
sudo dd if=/dev/sda of=/dev/sdb bs=1M

В данной строке:
- **/dev/sda** — это исходный диск;
- **/dev/sdb** — это целевой диск, на который вы хотите скопировать данные;
- флаг **bs** указывает размер блока данных.

В приведённом примере размер блока равен 1 МБ. Команда должна выполняться с правами суперпользователя.

Вот как выглядит вызов команды **dd** для записи ISO-файла на USB-диск:
sudo dd if="./filename.iso" of="/dev/sdb" status="progress" conv="fsync"

Создать образ CD/DVD, используя большой размер блока и игнорируя ошибки:
sudo dd if=/dev/cdrom of=backup.iso bs=2048 conv=noerror.

Clonezilla/Gparted

Clonezilla — это бесплатный инструмент для резервного копирования и клонирования дисков, который основан на Linux. Он обеспечивает поддержку множества файловых систем и может клонировать как отдельные разделы, так и целые диски.
Для использования Clonezilla вам нужно загрузиться с CD или USB-накопителя, содержащего Clonezilla, и выполнить несколько простых шагов, чтобы начать клонирование диска.

Gparted — это бесплатный инструмент для управления дисками в Linux, который также может использоваться для клонирования дисков.

rsync

rsync -avz --exclude='*.txt' user1@hostname1:/path/to/source/ user2@hostname2:/path/to/destination/

- user — имя пользователя;
- hostname — имя удалённого хоста;
- /path/to/source — это исходный каталог на удалённом сервере;
- -a означает режим архива, который сохраняет все метаданные оригинальных файлов;
- -v — режим вывода, который выводит подробную информацию о процессе копирования;
- -z — опция означает использование сжатия gzip для данных, что полезно при копировании больших файлов.

ЦИФРОВАЯ АКАДЕМИЯ

Система журналирования в Astra Linux

Основные системные журнальные файлы

Основные системные журнальные файлы в Astra Linux включают в себя:

1. /var/log/messages — содержит информацию о работе ядра операционной системы, запуске сервисов и других важных событиях. Этот файл содержит общие сообщения, полезные для диагностики и устранения проблем;
2. /var/log/syslog — предназначен для журналирования системных сообщений от демонов (фоновые процессы, работающие без прямого взаимодействия с пользователем) и сервисов. Содержит информацию об общих системных задачах, таких как работа сети, монтирование файловых систем, процесс входа в систему и т.д.;
3. /var/log/auth.log — регистрирует все попытки аутентификации. Полезен для определения необычной активности и анализа, кто и когда входил в систему;
4. /var/log/kern.log — содержит сообщения о ядре системы, отображает взаимодействие системы с аппаратным обеспечением.

Использование утилиты journalctl для получения сообщений из journald

ЦИФРОВАЯ АКАДЕМИЯ

1. Просмотр журнала событий:
   sudo journalctl
2. Фильтрация событий по определённым параметрам (текстовый поиск, уровень критичности, период времени и т. д.):
   sudo journalctl -p err -t sshd
3. Сохранение журналов в файле:
   sudo journalctl > /var/log/journal.txt
4. Очистка журналов:
   sudo journalctl --vacuum-size=1G

Ротация журналов при помощи logrotate

/var/log/<нужная_служба>.log {
  rotate 12 # максимальное количество файлов хранения;
  monthly # годовой, месячный, недельный, дневной;
  compress # архивирование и сжатие;
  delaycompress # последний и предпоследний файл не будут заархивированы;
  missingok # если файла лога нет, то не будет и нотификации об ошибке;
  size 100M # размер лога, после которого он будет ротирован;
  dateext # добавляет дату ротации перед заголовком старого лога;
  create # создает пустой файл после того, как старый будет ротирован;
  postrotate/endscript # выполняет после ротации какой-либо скрипт
    <путь к скрипту или команда>
}

- Запуск ротации всех журналов, указанных в конфигурационном файле:

sudo logrotate /etc/logrotate.conf

- Для проверки корректной работы logrotate можно выполнить команду:

sudo tail -f /var/log/syslog

Эта команда позволяет просмотреть последние записи в системном журнале, где выводятся сообщения о ротации журналов.

ЦИФРОВАЯ АКАДЕМИЯ

Запуск заданий по расписанию

Выполнение заданий по расписанию с помощью службы cron

ЦИФРОВАЯ АКАДЕМИЯ

Для настройки расписания заданий используется команда:

crontab -e

Структура записи в crontab следующая:

минута час день месяц день_недели путь_к_скрипту_или_непосредственно_команда

Если время запуска неважно, используется символ *.

Пример: для запуска shell-скрипта каждый день в 3:10 утра запись будет выглядеть следующим образом:

10 3 * * * /home/admuser/my.sh

Также можно отредактировать глобальный файл crontab:

/etc/crontab.

Планирование выполнение заданий через systemd

ЦИФРОВАЯ АКАДЕМИЯ

Таймер Daily backup	Сервис Daily backup	Таймер Every 5 minutes
/etc/systemd/system/name.timer	**/etc/systemd/system/name.service**	**/etc/systemd/system/name.timer**
[Unit]	**[Unit]**	**[Unit]**
Description=Daily backup timer	Description=Daily backup service	Description=Every 5 minutes timer
Requires=name.service		Requires=name.service
[Timer]	**[Service]**	**[Timer]**
OnCalendar=*-*-* 10:00:00	Type=oneshot	OnUnitActiveSec=5min
Persistent=true	ExecStart=/usr/bin/backup.sh	Unit=every-5-minutes.service
[Install]	**[Install]**	**[Install]**
WantedBy=timers.target	WantedBy=multi-user.target	WantedBy=timers.target

Описание параметров таймеров:

- OnBootSec= Таймер сработает через указанное время после старта системы.
- OnStartupSec= Для системных таймеров действие аналогично предыдущему, для пользовательских таймеров – это время после первого входа пользователя в систему.
- OnActiveSec= Через какое время, после активации таймера системным менеджером, запускать юнит.

ЦИФРОВАЯ АКАДЕМИЯ

Спасибо за внимание!