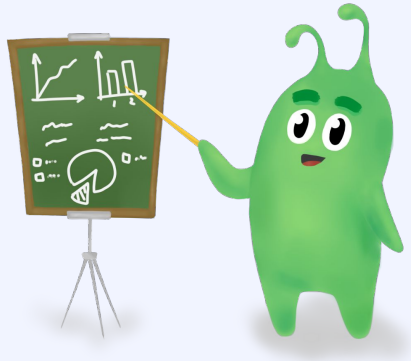
namespaces и cgroups

План занятия

- namespaces
- cgroups
- systemd-nspawn



namespaces

Механизм изоляции процессов

Типы namespaces

cgroups – изоляция cgroups

IPC – изоляция очередей сообщений

network – изоляция сетевого окружения

mount – изоляция точек монтирования файловых систем

PID – изоляция древа процессов

Time – изоляция системных часов

User – изоляция таблицы пользователей

UTS – изоляция настроек доменного имени

User namespace

Изолирует таблицу пользователей в процессах

Может владеть другими пространствами имён

Информация, связывающая UID из одного User namespace с другим называется маппингом UID

Маппинги UID

cat /proc/<ID>/uid_map

Первый столбец – стартовый UID диапазона для User namespace процесса

Второй столбец – зависит от того, находится ли в одном namespace процесс, который файл открыл, и процесс, которому файл принадлежит.

- Разные User неймспейсы – начало диапазона UID в неймспейсе процесса, который открыл файл
- Один User неймспейс – начало диапазона UID в родительском неймспейсе процесса, которому файл принадлежит

Третий столбец – длина диапазона

cgroups

control groups
ограничение ресурсов групп процессов

Подсистемы cgroups v1

blkio – лимиты на чтение/запись устройств

cpu – настройки шедулера процессора

cpuacct – отчёты об использовании ресурсов процессора

cpuset – ограничение на использование ядер процессора

memory – выделение памяти для процессов

net_prio – настройка приоритета трафика

pids – максимальное количество процессов в группе

perf_event – мониторинг ресурсов группы

Подсистемы cgroups v2

io – ограничение на чтение/запись

memory – выделение памяти для процессов

pids – максимальное количество процессов в группе

cpu – настройка шедулера и генерация отчётов CPU

cpuset – ограничение на использование ядер процессора

perf_event – мониторинг ресурсов группы

В следующей серии

Отладка