

Использование СПО в ВУЗе

ДОКЛАД НАЧАЛЬНИКА УИ ПГУТИ ЛЕМЖИНА М.И.

7 ОКТЯБРЯ 2021 ГОДА

История вопроса



ПГУТИ

История вопроса

- 2015 год – Приказ Минкомсвязи «Об утверждении плана по импортозамещению программного обеспечения» от 01.02.2015 № 96.
- 2018 год – Приказ Минкомсвязи «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения» от 20.09.2018 № 486
- 2019 год – Приказ Минкомсвязи России «О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 20.09.2018 № 486 «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения» от 18.04.2019 № 156

История вопроса

- 12.2020 – Дистрибьютор продуктов Microsoft компания «Софтлайн», не сможет более поставлять софт МГТУ им. Н. Э. Баумана из-за новых санкций США.
- 08.2021 – В МГТУ им. Н.Э. Баумана тестируют отечественное программное обеспечение. К новому учебному году на его использование планируют перевести 5 тысяч рабочих мест. Импортозамещением занимается НИИ «Восход» и «Планируется, что после реализации проекта его распространят и в других вузах.»

Наш опыт 2011-2021



- Виртуализация
- Системы хранения данных (СХД)
- Централизованное управление пользователями и компьютерами
- Тонкие клиенты, LTSP
 - > Групповые политики в среде Linux
 - > СПО на рабочих местах сотрудников
- Учебный процесс

Виртуализация



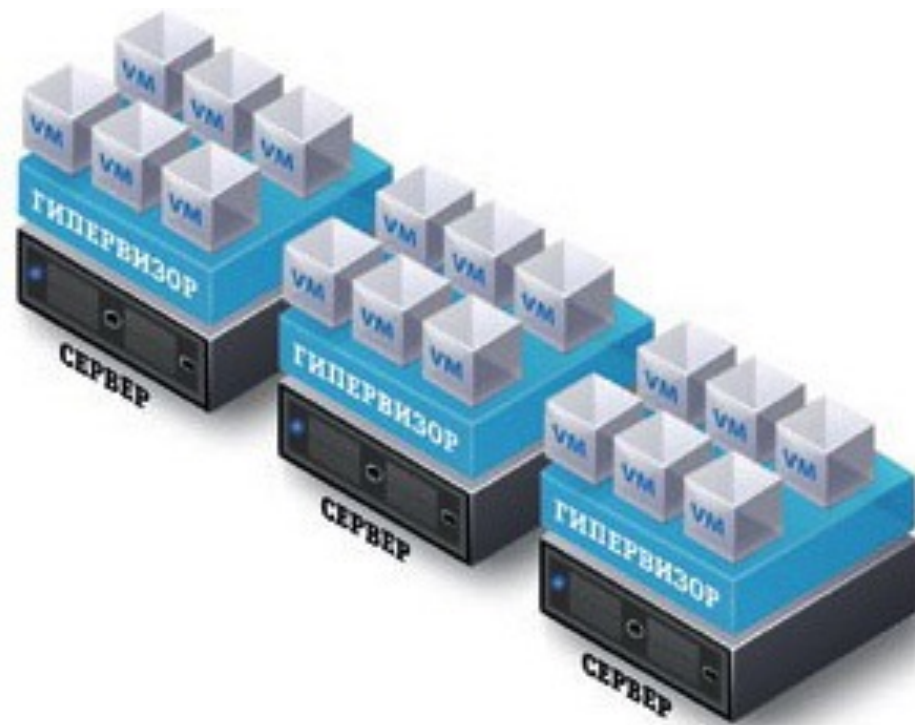
Proxmox Virtual Environment — система виртуализации с открытым исходным кодом, основанная на Debian GNU/Linux. В качестве гипервизоров использует KVM и LXC.

История:

Начинали в 2010м году с версии Proxmox 1.7-1.9, в настоящее время переходим с Proxmox 5.4 на Proxmox 6.3

Возможности:

- Живая миграция VM
- Проброс USB флешек/устройств напрямую в VM (ключи 1С)
- Работа с разными СХД: NFS, iSCSI, ZFS, поддержка Serp и т.д.
- Удобный графический web-интерфейс
- При использовании PBS быстрые инкрементальные бэкапы с дедупликацией и возможностью шифрования
- Снапшоты

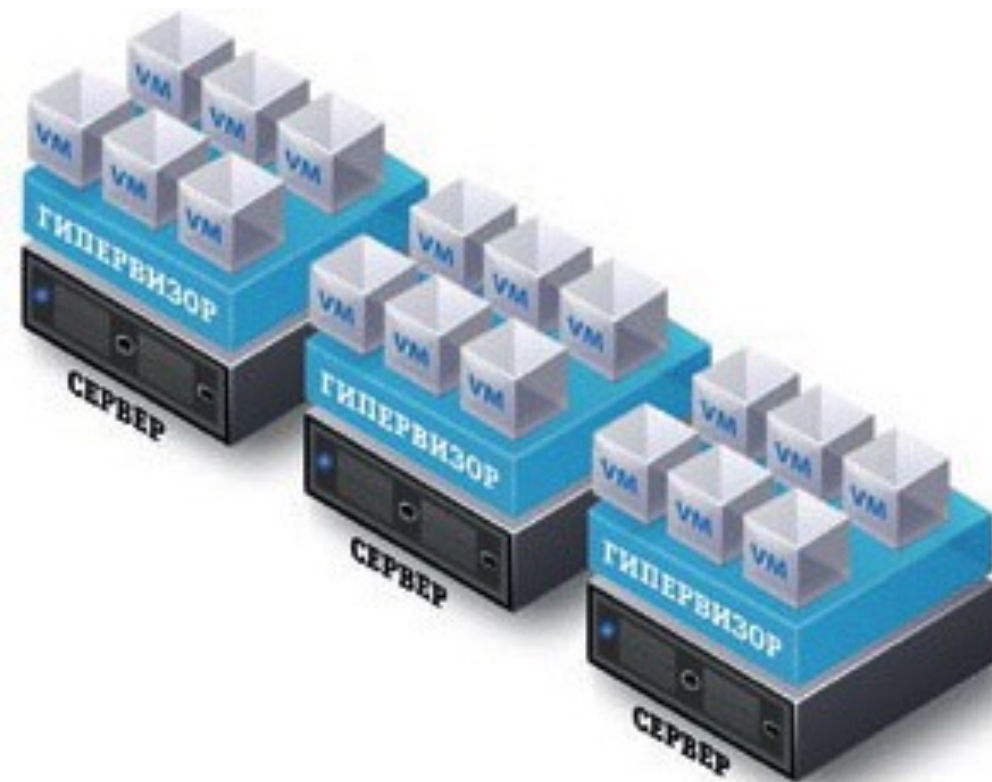


Виртуализация



Недостатки:

- Временами нестабильная работа служб синхронизации кластера
- При большой нагрузке на СХД иногда не хватает таймаутов интерфейса (удаление снапшотов)
- Баги/ошибки, напр. в версии 6+ при неполадках в сети иногда не восстанавливается работа точек монтирования NFS



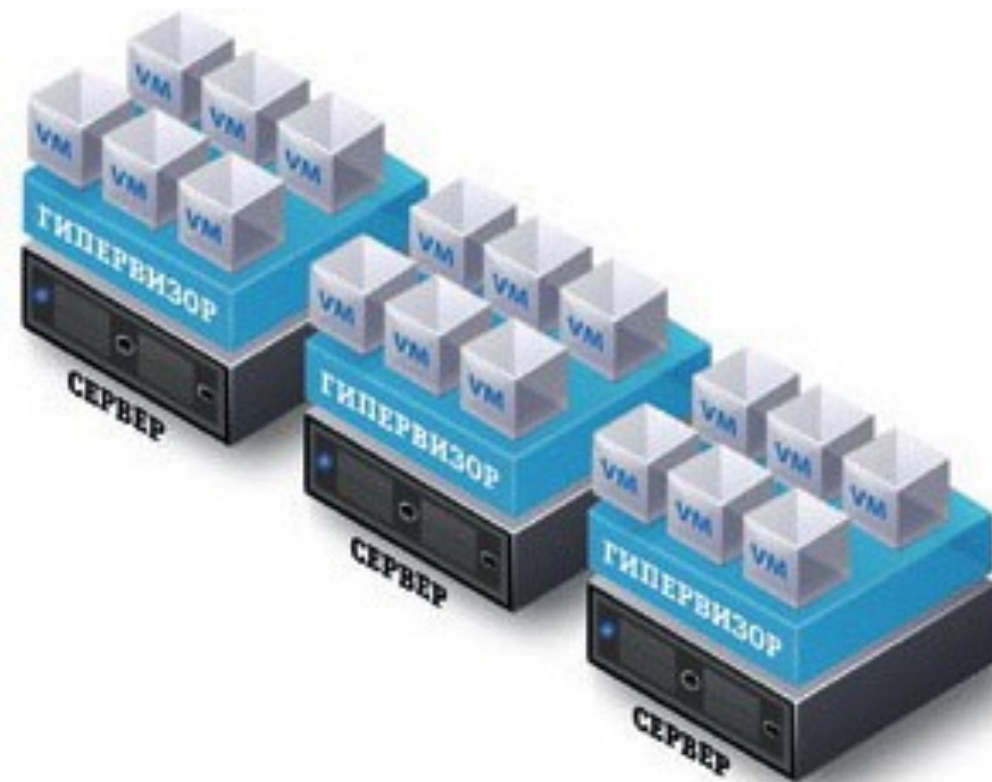
Виртуализация



Текущее состояние кластера:

- Работающих VM ~ 140
- Общее количество CPU ~ 376
- Общий объем памяти ~ 1.3 Тб

Ресурсы используются как для запуска служебных VM, так и для обеспечения учебного процесса («доставка приложений», виртуальные сервера и учебные комплексы кафедр)



Виртуализация. Импортозамещение

- Система серверной виртуализации «**P-Виртуализация**» (libvirt, KVM, QEMU)
- Программный комплекс "**Средства виртуализации «Брест»**" (libvirt, KVM, QEMU)
- Платформа управления и мониторинга среды виртуализации «**Sharx Stream**» (облачное решение, которое не подходит для госконтрактов в 95% случаев (секретность и т.д.)
- Программный комплекс виртуализации серверов, рабочих столов и приложений «**ХОСТ**» (KVM x86)
- Система безопасного управления средой виртуализации "**Z|virt**" (он же oVirt+KVM)
- Система управления средой виртуализации «**ROSA Virtualization**» (он же oVirt+KVM)
- Гипервизор **QP VMM** (слишком похож на Oracle Virtual Box, чтобы быть чем-то другим)

<https://habr.com/ru/post/447670/> (с)

Системы хранения данных

Используем обычные сервера Supermicro, сеть 10Гбит/с:

2010-2018 – ext4 поверх RAID 5

2018-2021 – ZFS on Linux (sdd + raidz)

Возможности:

- Контроль целостности данных (cow, checksums)
- Отказоустойчивость raidz выше чем RAID5 (нет write hole)
- Мгновенные «бесплатные» снапшоты всего пула
- Прозрачное сжатие (120%-170%)
- Adaptive Replacement Cache, hit rate в среднем 90%

Недостатки:

- Ниже производительность, нужен кэш = RAM
- Не рекомендуется включать дедупликацию = очень много RAM



Централизованное управление пользователями

История:

В 2014 году было принято решение ввести в тестовую эксплуатацию систему FreeIPA как потенциальную замену MS Active Directory

Возможности:

- Создание аналога «домена» MS AD (LDAP, Kerberos, CA, DNS)
- Централизованное управление компьютерами и пользователями (введение в домен компьютеров, создание пользователей, включение в группы)
- Назначение прав доступа пользователей “на компьютеры”
- Назначение прав и правил использования sudo
- Доверие FreeIPA -> MS AD
- Поддерживается Red Hat

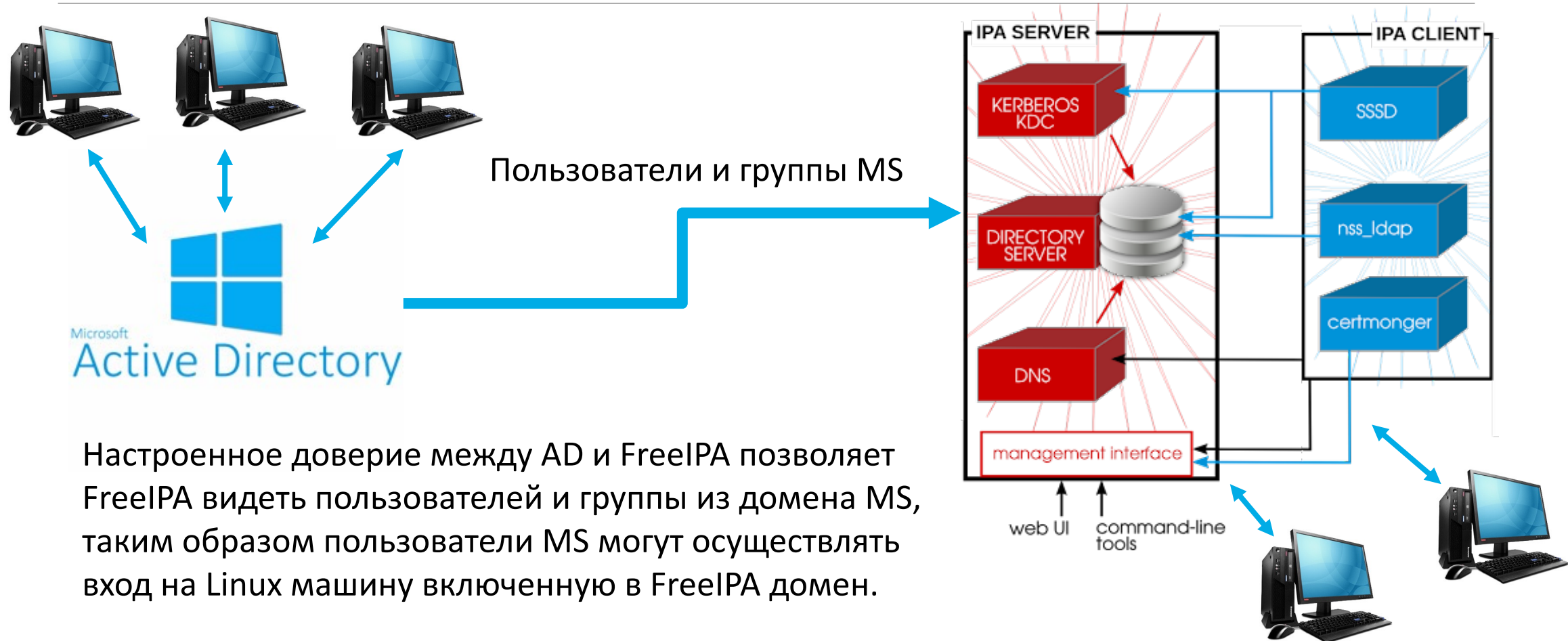
Недостатки:

- Нет групповых политик
- Нет обратного доверия MS AD → FreeIPA



freeIPA
identity | policy | audit

Централизованное управление пользователями и компьютерами



Настроенное доверие между AD и FreeIPA позволяет FreeIPA видеть пользователей и группы из домена MS, таким образом пользователи MS могут осуществлять вход на Linux машину включенную в FreeIPA домен.

Тонкие клиенты, LTSP

История:

С 2009 года университет закупал бездисковые тонкие клиенты (ТК) в учебные классы, ТК подключались к Windows Server

С 2013-2014 года в качестве эксперимента начался перевод тонких клиентов на использование терминальных серверов на базе Ubuntu (14->16->18), LTSP

Возможности:

- Загрузка по сети (PXE), можно использовать как ТК, так и старые компьютеры
- Web-управление настройками подключения ТК к терминальным серверам
- Балансировка клиентов между несколькими терминальными Linux серверами
- Проброс USB флешек и при желании проброс USB устройств на сервер
- Подключение клиентов по протоколу x2go (сжатие потока, можно смотреть youtube в небольшом окне), с пробросом USB флешек



Тонкие клиенты, LTSP

Возможности:

- Автоматическое монтирование сетевых папок Windows для пользователя MS AD (FreeIPA → MS AD)
- Linux приложения ставятся и запускаются нативно
- Windows приложения запускаются через сервис Remote App («доставка приложений»)



Тонкие клиенты, LTSP

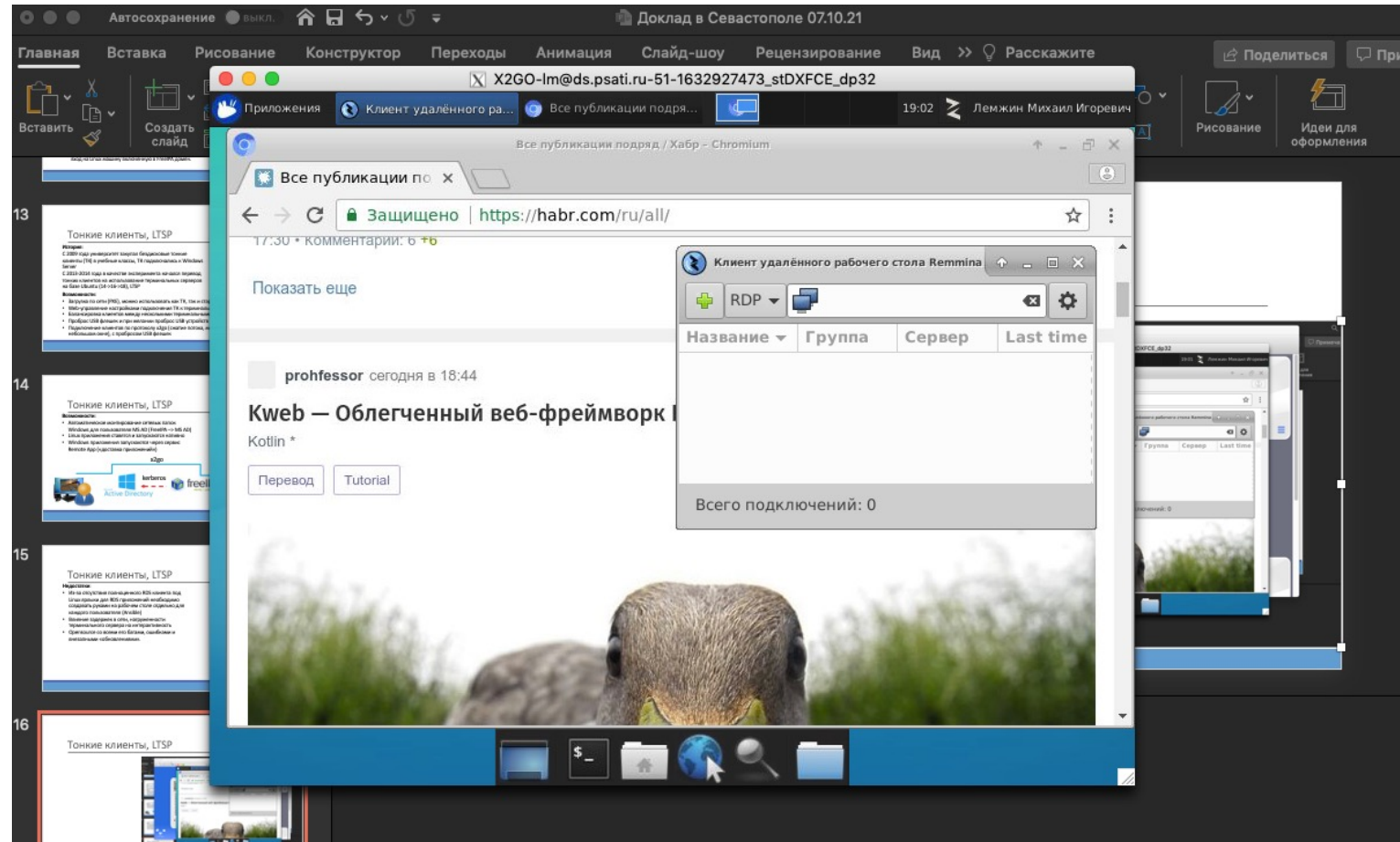
Недостатки:

- Из-за отсутствия полноценного RDS клиента под Linux ярлыки для RDS приложений необходимо создавать руками на рабочем столе отдельно для каждого пользователя (Ansible)
- Влияние задержек в сети, нагрузки терминального сервера на интерактивность
- Opensource со всеми его багами, ошибками и внезапными «обновлениями».



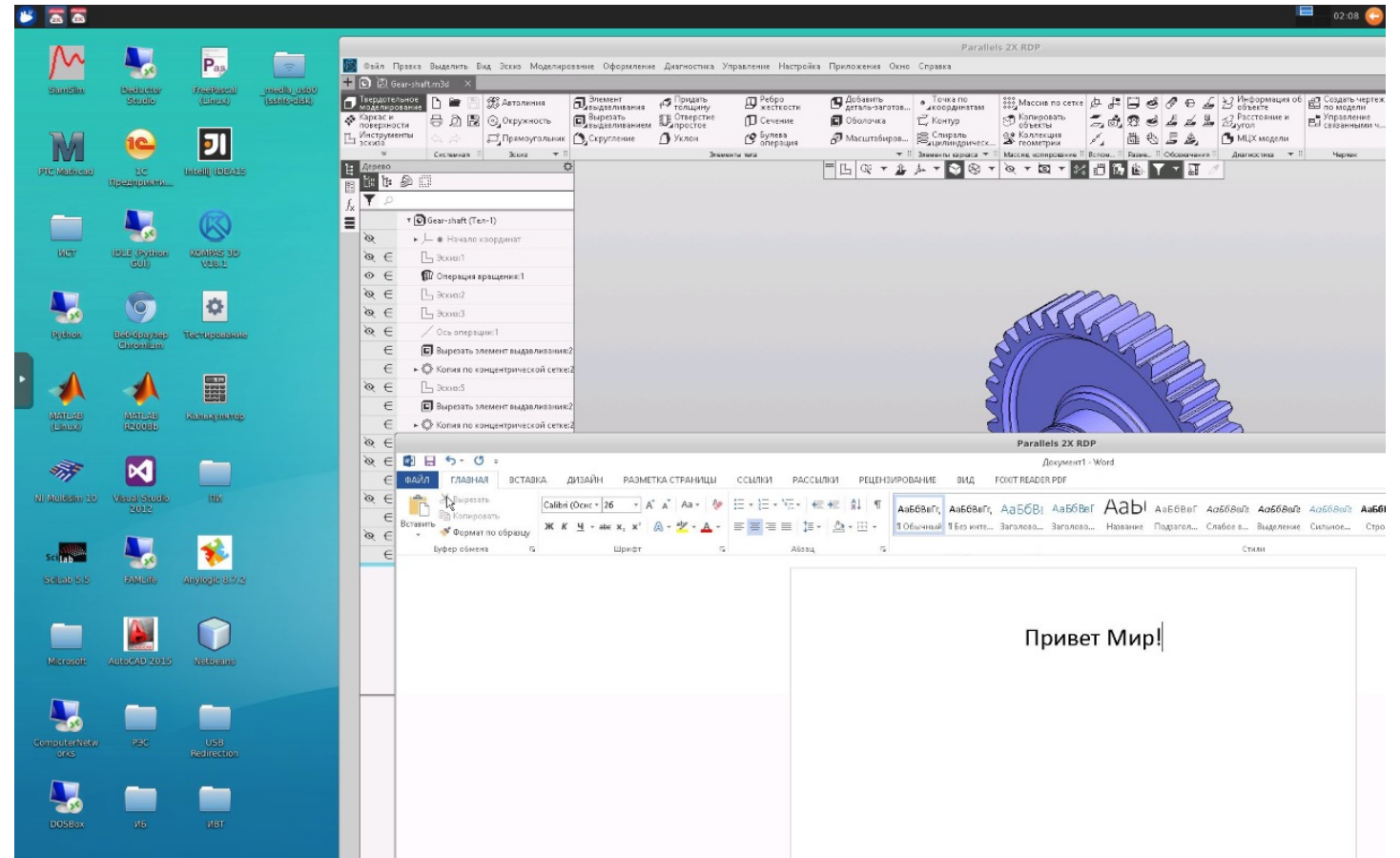
Тонкие клиенты, LTSP

Пример работы по протоколу
x2go



Тонкие клиенты, LTSP

Пример рабочего стола тонкого клиента



Групповые политики в среде Linux

История:

В 2018 году, рамках нависшей «угрозы» импортозамещения возникла идея реализации функционала групповых политик в доменном окружении Linux на базе FreeIPA + Ansible

В 2019 году были запущены тестовые рабочие места в читальном зале НТБ на базе ОС GosLinux на которые имеется возможность воздействовать групповыми политиками в виде сценариев Ansible



Групповые политики в среде Linux

Техническое задание:

- Компьютер должен сам периодически запрашивать политики с сервера
- Политики должны действовать на компьютеры в зависимости от того в какие доменные группы входит компьютер
- Состав групп управляется через контроллеры FreeIPA



freeIPA
identity | policy | audit

Реализация:

- Групповые политики в виде yaml сценариев размещаются в открытом на чтение git репозитории
- Компьютер в домене FreeIPA, включается в состав определенных групп
- Планировщик заданий (cron) каждый час в случайное время запускает на клиенте ansible в режиме pull в качестве параметров передавая адрес git репозитория с yaml сценариями и списком групп в которые входит компьютер
- Ansible применяет «на себя» необходимые изменения



ANSIBLE

Групповые политики в среде Linux

Достоинства:

- Работает уже сейчас опираясь на стабильные крупные проекты (git, freeipa, ansible)
- Политики-сценарии описываются на yaml разметке (проще чем писать скрипт)
- Политики действуют асинхронно на все компьютеры в домене (хоть 1000 штук) в независимости от того включен компьютер или нет

Недостатки:

- Сложность реализации, т.к. необходимо поддерживать актуальность базовых скриптов (включение в домен, запуск применения групповых политик)
- Нет защиты от «дурака», ошибка в сценарии окажет влияние на все компьютеры в домене



freeIPA
identity | policy | audit



ANSIBLE

Групповые политики в среде Linux

Примеры сценариев:

Установить все обновления

```
- name: upgrade all CentOS packages
  yum: name=* state=latest
```

Скопировать на компьютер (группу компьютеров) файл и назначить права

```
- name: Copy file with owner and permissions
  copy:
    src: /tmp/test.txt
    dest: /mnt/test.txt
    owner: root
    group: root
    mode: '0644'
```



freeIPA
identity | policy | audit



ANSIBLE

СПО на рабочих местах

История:

В 2019 году были запущены тестовые рабочие места в читальном зале НТБ на базе ОС GosLinux на которые имеется возможность воздействовать групповыми политиками в виде сценариев Ansible

В 2020-2021 годах все вновь вводимые сервера включаются в домен FreeIPA и попадают под действие групповых политик

Проблемы:

Сложно найти «жертву» для перехода на СПО, пока переход не стал вынужденным



СПО в рабочем/учебном процессе

- В 2009-2011 годах начато внедрение системы VoIP телефонии на базе Asterisk. В настоящее время университет практически отказался от старой «проводной» нумерации, используется пул VoIP номеров 339-11-xx



СПО в рабочем/учебном процессе

- 2011 году запущена система дистанционного обучения на базе LMS eFront



A screenshot of the eFront LMS interface displayed in a Mozilla Firefox browser window. The browser's address bar shows the URL 'do.psuti.ru/home/www/userpage.php'. The page title is 'Система ДО ПГУТИ | Lifetime Education - Mozilla Firefox'. The interface includes a navigation menu with 'Главная' (Home) and 'Мои дисциплины' (My Courses). A user profile for 'Осипов Олег Владимирович | Преподаватель | (6)' is visible. The main content area is titled 'Мои дисциплины' and features a search bar with the text 'Материал в процессе'. Below this, there are three course entries: 1. '031600 Реклама и связи с общественностью (полная)' with a sub-entry for 'Безопасность жизнедеятельности - PCO - 1 - 2 - 2011 Вороной А.А. (Преподаватель)'. 2. '031600 PCO (1 курс) (1 семестр)' with a sub-entry for 'Иностранный язык - PCO - 1 - 1 - Ерофеева Ю.В. Ермакова Е.А. (Преподаватель)'. 3. '031600 PCO (1 курс) (1 семестр)' with a sub-entry for 'История - PCO - 1 - 1 - 2011 Ипполитов Г.М. (Преподаватель)'. Each course entry lists various activity types like 'Лекционные', 'Практические', 'Контрольные', and 'Лабораторные'.

СПО в рабочем/учебном процессе

- В 2013 году запущена система электронных заявок ИТ на базе OTRS и в 2019-2021 годах распространена на другие подразделения университета



The screenshot displays the OTRS Community Edition web interface. At the top, there is a navigation menu with items like "Дайджест", "Клиенты", "Календарь", "Заявки", "FAQ", "Сервисы", "CMDB", "Изменения", "Учет затраченного времени", "Отчеты", and "Администрирование". The main content area is divided into several sections:

- Эскалированные заявки**: A table listing 10 tickets with columns for "ЗЯЯВКА", "ВОЗРАСТ", and "НАЗВАНИЕ".
- Новые Заявки**: A table listing 10 tickets with columns for "ЗЯЯВКА", "ВОЗРАСТ", and "НАЗВАНИЕ".
- Статистика за неделю (7 дней)**: A line chart showing the number of "Создан/а" (Created) and "Закрытые" (Closed) tickets per day from Sunday to Saturday.
- Предстоящие события**: A list of upcoming events with details like "1018902 Ремонт системного блока" and "1018943 СРТПЦ_провода".

СПО в рабочем/учебном процессе

- В 2014 году на движок Drupal переведен сайт ПГУТИ



A screenshot of the website for PGTU (Povolzhskiy gosudarstvennyy universitet telekommunikatsiy i informatsiy). The page has a dark blue header with the university's logo (1956-2021) and name. Below the header is a navigation menu with items like "ГЛАВНАЯ", "УНИВЕРСИТЕТ", "ОБРАЗОВАНИЕ", etc. The main content area features a large blue banner with the text "СУПЕРСЕРВИС ПОСТУПАЙ В ВУЗ ОНЛАЙН ЧЕРЕЗ ГОСУСЛУГИ". A yellow box on the left contains the text "ПОСТУПИ В ВУЗ ОНЛАЙН" and "Поступай в вуз онлайн через Госуслуги: ...". The footer includes contact information for the admissions commission and the university's logo.

СПО в рабочем/учебном процессе

- В 2014 году развернут внутренний GitLab сервер использующийся в том числе в образовательном процессе



Admin Area > Dashboard

Admin Overview

Projects: 134

New project

Users: 59

New user

Groups: 10

New group

Statistics

Forks	0
Issues	0
Merge Requests	7
Notes	35
Snippets	0
SSH Keys	10
Milestones	0
Active Users	58

Features

Sign up	⏻
LDAP	●
Gravatar	●
OmniAuth	●
Reply by email	⏻
Container Registry	⏻
GitLab Pages	⏻
Shared Runners	●

Components update asap

GitLab	11.10.1 (861fe405571)
GitLab Shell	9.0.0
GitLab Workhorse	v8.5.1
GitLab API	v4
Ruby	2.5.3p105
Rails	5.0.7.2
PostgreSQL	9.6.11
Gitaly Servers	

СПО в рабочем/учебном процессе

- В 2020 году запущен учебный сервер СУБД MySQL с аутентификацией студентов в домене
- В 2021 рассматриваем возможность полного переноса на Linux учебного сервера 1С



Так же мы используем свободное ПО:

JetBrains IDEs
FreePascal
NetBeans
R
MATLAB
Maxima
Scilab
QGIS

Qucs
KiCAD
FreeCAD
Gimp
Inkscape
Dia

Wireshark
Mozilla Firefox
Mozilla Thunderbird
и т.д.



Спасибо за внимание!

