

Техническое описание информационно-коммуникационных технологий, используемых в МОУ «Лицей №1»

Оглавление

Введение.....	1
историческая справка.....	1
поддерживаемые парадигмы.....	1
исследовательский интерес.....	1
Планирование.....	2
Требования.....	2
наличие предыдущего опыта.....	2
выбор инструментов.....	2
Реализация.....	2
Технические характеристики оборудования.....	2
Постановка задачи.....	2
Порядок установки.....	2
Процесс работы.....	4
Оценка результата.....	4
Отзывы.....	4
Использованные справочные материалы.....	5
Послесловие.....	5
Приложение 1.....	6

Введение

историческая справка

Лицей начал свою работу 22 июня 1989 года. Первым его отделением стало физико-математическое. Углубленная физико-математическая подготовка способствовала развитию информационных технологий в учебном процессе.

поддерживаемые парадигмы

В то время, как лицей развивался, в более крупных масштабах развивались и новые идеи среди программистов мира. Среди них — идея open source (всё программное обеспечение (ПО) должно быть бесплатно, а так доступно для ознакомления и модификации). Но больше всего набирали популярность операционные системы на базе ядра Linux — как самого известного проекта в духе open source. Учась и работая на кафедре математического моделирования, я серьёзно увлёкся изучением всем, что связано с компьютерами и, в частности, Linux. Поэтому не удивительным был выбор курса использования открытого ПО, когда мне доверили развивать информационные технологии в Лицее.

Но не только бесплатность привлекает в такого рода ПО, но открытость таит в себе более серьёзные вещи. Очевидно, что программисты — люди, а им свойственно ошибаться. Благодаря открытости выявление и исправление ошибок происходит куда быстрее, чем в закрытых программах. Повышается надёжность и безопасность программ. А это одни из ключевых моментов.

исследовательский интерес

Нет ничего хуже для исследователя или интересующегося чем-либо, чем невозможность изучить не только «оболочку», но и «внутренности». Проприетарное ПО подобно закрытому чёрному ящику с торчащими рычагами. Нам разрешено дёргать за них, но нет возможности узнать, как именно тот или иной рычаг работает, нет возможности улучшить механизм. Меня, как и многих других людей, не устраивает такое положение вещей, желая быть свободным в действиях, я оставляю себе право изучать и изобретать.

Планирование

Перейдём ближе к теме. Сформирую теоретические основы, которыми буду руководствоваться далее. Это: требования, наличие опыта и используемые инструменты.

Требования

Понятно, что первыми требованиями будут функциональность, надёжность и безопасность. Что мы хотим видеть от данного проекта. Сначала сформируем понятия о структурах всего ИКТ. Во-первых, сюда входит обеспечение рабочих мест - клиентов. Во-вторых, сюда входят серверы — компьютеры, выбранные для обслуживания клиентов. И, наконец, сеть, которая объединяет и серверы, и клиентов.

Структурно разделения будут следующими: серверы, компьютерные классы, рабочие станции в кабинетах сотрудников. Серверы должны быть изолированными от доступа посторонних лиц. Компьютеры в классах должны быть изолированными от компьютеров сотрудников. У всех должен быть контролируемый администратором доступ к Интернету. У сотрудников должна быть электронная почта. Должна быть возможность сделать электронную почту ученикам.

наличие предыдущего опыта

По сколько опыт настройки разных сетевых сервисов имелся, то осталось всё объединить в одном проекте.

выбор инструментов

В качестве аппаратного обеспечения было выбрано серверное решение Intel, в качестве ПО были выбраны: Slackware Linux (позже — замена на Gentoo Linux), OpenSuSE Linux

Реализация

Технические характеристики оборудования

Сервер Intel на базе материнской платы SE7520BD23D

Процессор 2 x Intel(R) Xeon(TM) CPU 3.00GHz

Память: 4 GB

Дисковый контроллер: Intel(R) RAID Controller SRCS16

Дисковые накопители: 4 x 320GB

Уровень RAID: 5

Дополнительно: Сетевой контроллер Intel® PRO/1000 MT Dual Port Server Adapter PWLA8492MT, ИБП Smart-UPS 1500 RM

Постановка задачи

Аппаратно-программный комплекс должен отвечать требованиям и быть в некотором роде экспериментом по использованию новых технологий. Для этого был выбран метод запуска виртуальных сред на одной аппаратной платформе. В качестве виртуальной машины взят XEN. <http://ru.wikipedia.org/wiki/Xen>: «Xen — Монитор [виртуальных машин](#) (VMM), или [гипервизор](#). Работает в [паравиртуальном](#) режиме и в режиме аппаратной виртуализации (HVM), использует аппаратные возможности процессоров, поэтому не имеет привязки к конкретной операционной системе и может быть установлен «поверх» только лишь аппаратного обеспечения, в так называемом режиме [bare metal](#)[2]. Способен поддерживать одновременную работу большого числа виртуальных машин на одной физической, при этом не тратя значительных вычислительных ресурсов.»

На схеме ([приложение 1](#)) нарисована логика сети. Хост-система выполняет задачу по запуску и останову гостевых, управлением оборудованием, а так же служит брэндмауром. Почтовая и http служба на одном виртуальном сервере httpsrv вынесены в виртуальную подсеть так называемой «демилитаризованной зоны» (DMZ), как это делается во многих случаях и с реальными серверами. Виртуальный сервер учётных записей и личных данных пользователей profsrv доступен из 2-х подсетей так, как если бы он был напрямую подключен в коммутатор. Наконец, сервер базы данных со служебной информацией dbsrv доступен только из служебной подсети.

Порядок установки

Сначала был разбит диск. Общий объём массива (/dev/sda) получился 959.9 GB

/dev/sda1 размером 55MB был задействован под boot
/dev/sda2 размером 500MB был задействован под swar хост-системы
/dev/sda3 размером 10GB был отведён для / хост-системы

Остальная часть диска была отставлена для размещения гостевых систем, для чего была включена в LVM. В качестве хост-системы был поставлен Slackware Linux из-за более простой системы пакетов, в сравнении с большинством современных дистрибутивов, чтобы меньше места занимал. В группе LVM свободное пространство распределилось следующим образом:

httpsrv 80,00G
profsrv 350,00G
dbsrv 100,00G

Остальное — свободно для добавления в любой раздел.

Подобный способ деления на прямую исходит из задач, под которые выделяется пространство. На каждую гостевую систему был поставлен дистрибутив OpenSUSE.

- XEN

Был собран хеп из svn с официального сайта, а так же ядро, которое его поддерживает.

- Сеть

Сети были настроены согласно требованиям и постанровке.

- LDAP

Сервис LDAP установлен на сервере profsrv (основные пакеты: openldap2, nss_ldap, pam_ldap). Конфигурация сервиса перенесена в само хранилище LDAP, что позволяет гибко настраивать сервис без его перезапуска. Загружены схемы для достаточного функционирования системных авторизаций, а так же SAMBA и Почтовых аккаунтов (т.е. Описывающие классы объектов posixAccount, shadowAccount, sambaSamAccount, inetOrgPerson, CourierMailAccount).

- Учётные записи

Учётные записи (у.з.) хранятся в базе LDAP. Есть условность, с которой задаются имена у.з. Так, для сотрудников учреждения ФИО переводится в транслитерацию, берётся фамилия, после неё через точку следует первая буква имени, снова точка, потом первая буква отчества. у.з. студента образуется на основе года поступления, группы и порядкового номера, например, st09-01-01. Поля записи LDAP содержат следующее (только базовые):

uid — имя у.з.
sn — base64-кодированную фамилию
cn — base64-кодированные ФИО полностью
displayName — ФИО транслитерацией
mail — почтовый адрес

- Доступ в интернет

Доступ в сеть Интернет осуществляется через 2-х провайдеров. Для этого на брандмауэре есть два сетевых интерфейса wan1 и wan2. Пользователи подключаются к прокси-серверу squid, расположенному на httpsrv. В зависимости от правил прокси, клиент работает с Интернетом либо через одного провайдера, либо через другого (за эту функцию отвечает настройка tcp_outgoing_address в squid)

- Почта

ПО: dovecot, postfix, clamav, dspam (будет изменён на amavisd-new)

Пользователи виртуальные — база LDAP, находящаяся на profsrv. Схема для Courier Mail Server была использована как основа для схемы аккаунтов. Порты imap, pop3 и smtp открыты наружу, чтобы иметь доступ вне стен организации (так же у нас ещё 3 корпуса в разных частях города). Все протоколы защищены TLS.

Фильтр почтовых ящиков: (&(objectClass=CourierMailAccount)(uid=%u))

Фильтр алиасов: (&(objectClass=CourierMailAlias)(mail=%s))

- Samba

На серверах profsrv и dbsrv установлены сервисы SAMBA. База аккаунтов находится в LDAP — это те же самые записи, что и в почте и в прокси-сервере.

SAMBA на profsrv экспортирует пользовательские домашние каталоги, общие ресурсы, такие как обменная папка, учебные материалы и т.п. Так же сервис работает контроллером домена для локальной сети организации. SAMBA на dbsrv экспортирует внутренние файлы и документы, доступные только из служебной подсети.

- Базы данных

На dbsrv установлены базы данных (сейчас firebird)

Процесс работы

В компьютерных классах стоят машины с 2-й загрузкой: Windows из «Первой Помощи» и OpenSUSE — общим количеством 30 шт. В служебной сети больше 10 компьютеров, включая переносные устройства.

Все клиенты входят в один SAMBA/WIN домен, соответственно, пользователь сети может с помощью любого из них получить доступ к своему рабочему окружению, своим данным, получать почту, работать в Интернете. Все клиенты настроены одинаково, поэтому при ремонте одного клиента не теряется информация, не теряется работоспособность учебного процесса.

Замечание по Linux: за подключение домашнего каталога с сервера отвечает модуль `ram_mount`. Файловые системы в домашний каталог с сервера экспортируются посредством `cifs`, сохраняя права `unix`. Идентификаторы пользователей клиенты получают так же с сервера.

Оценка результата

В итоге, было реализовано целостное комплексное решение на базе открытого программного обеспечения, отвечающего требованиям безопасности хранения информации, масштабируемости (легко можно разделить функции на несколько аппаратных платформ, разнести на расстояние). Один сервер занимает меньшую площадь и тратит меньше энергии. Пользователи застрахованы от потери данных, могут выполнять свою деятельность, не смотря на сбои части клиентских машин. Каждый может иметь свой адрес электронной почты. Это позволяет проще обмениваться информацией учителям и ученикам. Успешно использована относительно новая технология паравиртуализации. Результат не исключает применение проприетарных продуктов, которые функционально дополняют возможности более полного использования потенциала СПО.

Отзывы

Мулюкова Наталия Анатольевна, главный инженер информационно-аналитического отдела:

Преимущества	Недостатки
<ol style="list-style-type: none">1. Стабильность2. Покупка сервера обошлась дешевле, чем под Windows3. Отсутствие вирусов4. Возможность полноценной работы старой техники (в учебном процессе)5. Защищенность важных данных от вторжения со стороны учащихся	<ol style="list-style-type: none">1. Иногда некорректно открывается документ Ms Office в OO (особенно презентации). Но это, скорее, не про сервер

Н.А.(выделенным — моё примечание): «старый сервер зависал раза два в неделю. С новыми такой проблемы нет. Сотрудники ИАО (Исследовательско-аналитический отдел) работают практически без замечаний в последнее время (проблемы с профилем возникают очень редко). В учебном процессе на Ветлужской проблем нет. А вот в 212 надо будет спросить у преподавателей. Сейчас Сергей Анферов (преподаватель) сказал, что иногда некоторые профили учеников на некоторых компьютерах не грузятся (в Windows). А через неделю, опять нормально работают. Обслуживание ведется одним администратором удаленно. Возникшие проблемы решаются оперативно. Каждый пользователь имеет личный профиль (в скорой перспективе использование Moodle), электронный ящик.»

Использованные справочные материалы

1. <http://wiki.xensource.com/xenwiki/>
2. www.xgu.ru/wiki/Xen
3. <http://ru.opensuse.org/Документация>
4. Много разных страниц man
5. Google
6. Интернет

Послесловие

Внедрение начато (боюсь ошибиться) в 2004-2005 заменой почтового сервера с ОС Windows на Linux, далее, по мере идей и задумок, шёл дальнейший процесс, а результат, близкий к сегодняшнему дню был достигнут до появления государственных программ. Этим обуславливается выбор дистрибутивов. Так же хочу подчеркнуть, что это не конечный пункт, и развитие лично мне видится в использовании внутренней ip-телефонии, kerberos, репликаций, ключей gpg и т. п.

В другом учебном корпусе был установлен сервер с «Школьным терминальным сервером 4.0». По сколько процесс установки был тривиален, большого интереса он не представляет. Стоит упомянуть, что терминальный сервер дал вторую жизнь 15-ти компьютерам, с весьма скромными характеристиками. Так же для оснащения второго класса были приобретены тонкие клиенты Depo Sky 220.

Приложение 1.

