Федеральное агентство по образованию

Государственное общеобразовательное учреждение

высшего профессионального образования

Уфимский Государственный Авиационный Технический Университет

Кафедра вычислительной математики и кибернетики

# Отчет по курсовой роботе

# «Инсталляция, настройка и сопровождение LDAP-сервера.Linux/FreeBSD»

## По дисциплине «Администрирование информационных систем»

Выполнил: студент гр.

МО-516 Еникеев К.Р.

Проверил: профессор кафедры ВМиК

Верхотуров М.А.

**Уфа 2009**

# Содержательная и формальная постановка задачи.

1. Установка и настройка операционной системы Linux или FreeBSD.
2. Установка и настройка LDAP сервера.

# Структура решения.

Поставленную задачу можно разделить на четыре основных этапов:

1. Установка операционной системы
2. Установка LDAP сервера
3. Настройка LDAP сервера

# Обзор и анализ методов решения.

## Обзор операционных систем.

### Linux.

Linux — общее название UNIX-подобных операционных систем на основе одноимённого ядра и собранных для него библиотек и системных программ, разработанных в рамках проекта GNU.

GNU/Linux работает на PC-совместимых системах семейства Intel x86, а также на IA-64, AMD64, PowerPC, ARM и многих других.

К операционной системе GNU/Linux также часто относят программы, дополняющие эту операционную систему, и прикладные программы, делающие её полноценной многофункциональной операционной средой.

В отличие от большинства других операционных систем, GNU/Linux не имеет единой «официальной» комплектации. Вместо этого GNU/Linux поставляется в большом количестве так называемых дистрибутивов, в которых программы GNU соединяются с ядром Linux и другими программами. Наиболее известными дистрибутивами GNU/Linux являются Ubuntu, Debian GNU/Linux, Red Hat, Fedora, Mandriva, SuSE, Gentoo, Slackware, Archlinux. Российские дистрибутивы — ALT Linux и ASPLinux.

Большинство пользователей для установки GNU/Linux используют дистрибутивы. Дистрибутив — это не просто набор программ, а ряд решений для разных задач пользователей, объединённых едиными системами установки, управления и обновления пакетов, настройки и поддержки.

Самые распространённые в мире дистрибутивы:

* *Ubuntu* — быстро завоевавший популярность дистрибутив, ориентированный на лёгкость в освоении и использовании.
* *OpenSUSE* — бесплатно распространяемая версия дистрибутива SuSE, принадлежащая компании Novell. Отличается удобством в настройке и обслуживании благодаря использованию утилиты YaST.
* *Fedora* — поддерживается сообществом и корпорацией RedHat, предшествует выпускам коммерческой версии RHEL.
* *Debian GNU/Linux* — международный дистрибутив, разрабатываемый обширным сообществом разработчиков в некоммерческих целях. Послужил основой для создания множества других дистрибутивов. Отличается строгим подходом к включению несвободного ПО.
* *Mandriva* — французско-бразильский дистрибутив, объединение бывших Mandrake и Conectiva (англ.).
* *Slackware* — один из старейших дистрибутивов, отличается консервативным подходом в разработке и использовании.
* *Gentoo* — дистрибутив, собираемый из исходных кодов. Позволяет очень гибко настраивать конечную систему и оптимизировать производительность, поэтому часто называет себя мета-дистрибутивом. Ориентирован на экспертов и опытных пользователей.
* *Archlinux* — ориентированный на применение самых последних версий программ и постоянно обновляемый, поддерживающий одинаково как бинарную, так и установку из исходных кодов и построенный на философии простоты KISS, этот дистрибутив ориентирован на компетентных пользователей, которые хотят иметь всю силу и модифицируемость Linux, но не в жертву времени обслуживания.

Помимо перечисленных, существует множество других дистрибутивов, как базирующихся на перечисленных, так и созданных с нуля и зачастую предназначенных для выполнения ограниченного количества задач.

### Linux Ubuntu

Ubuntu (произносится: «убу́нту») — дистрибутив операционной системы Linux, основанный на Debian GNU/Linux. Генеральный спонсор Ubuntu — компания Canonical Ltd., основанная Марком Шаттлвортом. Проект активно развивается и поддерживается свободным сообществом.

Ubuntu сосредотачивается на удобстве и простоте использования, включает широко распространённое использование утилиты sudo, которая позволяет пользователям выполнять администраторские задачи, не запуская потенциально опасную сессию суперпользователя.

Ubuntu, кроме того, имеет развитую интернационализацию, обеспечивающую максимальную доступность для представителей разных языковых групп. С версии 5.04 кодировкой по умолчанию является UTF-8.

Ubuntu для работы нуждается в 256 мегабайт RAM и, при установке на жёсткий диск, в трёх гигабайтах свободного пространства.

### BSD.

BSD (англ. Berkeley Software Distribution) — система распространения программного обеспечения в исходных кодах, созданная для обмена опытом между учебными заведениями. Особенностью пакетов ПО BSD была специальная лицензия BSD, которую кратко можно охарактеризовать так: весь исходный код — собственность BSD, все правки — собственность их авторов.

В данный момент термин BSD чаще всего употребляется как синоним BSD-UNIX общего названия вариантов UNIX, восходящих к дистрибутивам университета Беркли.

К семейству BSD относятся: NetBSD, FreeBSD, OpenBSD, MirBSD, DragonFly BSD, PC-BSD, DesktopBSD, TrueBSD, Frenzy, Ultrix и частично Darwin (ядро Mac OS X).

Отличия от «классической» системы UNIX состоят в отсутствии переключения уровней выполнения, системе печати, файловой системе и командного процессора. Пользовательские команды практически идентичны.

* *NetBSD* - происходит из систем 4.3BSD и 386BSD. В конце 1995 года от NetBSD ответвился проект OpenBSD. Текущая версия — NetBSD 5.0 — выпущена 29 апреля 2009 года.
* *OpenBSD* — свободная многоплатформенная операционная система, основанная на 4.4BSD — BSD-реализации UNIX-системы. Основным отличием OpenBSD от других свободных операционных систем, базирующихся на 4.4BSD (таких, как NetBSD, FreeBSD), является изначальная ориентированность проекта на создание наиболее безопасной, свободной и лицензионно чистой из существующих операционных систем.
* *FreeBSD* — свободная UNIX-подобная операционная система, потомок AT&T Unix по линии BSD, созданной в университете Беркли. FreeBSD работает на PC-совместимых системах семейства x86, включая Microsoft Xbox, а также на DEC Alpha, Sun UltraSPARC, IA-64, AMD64, PowerPC, NEC PC-98, ARM. FreeBSD хорошо зарекомендовала себя как система для построения интранет- и интернет-серверов. Она предоставляет достаточно надёжные сетевые службы и эффективное управление памятью. FreeBSD широко представлена в списке веб-серверов с наибольшим временем непрерывной работы (согласно исследованию компании Netcraft)

## Сравнение наиболее популярных UNIX-подобных ОС

## BSD

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Название** | **Тип ядра** | **Поддерживаемые файловые системы** | **Поддерживаемые архитектуры** | **GUI** | **Управление пакетами** | **Родной API** |
| **FreeBSD** | Монолитное | UFS2, ext2, ext3, FAT, ISO 9660, UDF, NTFS, ReiserFS , XFS,ZFS | x86, x86-64, PC98, SPARC | нет | ports tree, packages | BSD, POSIX |
| **NetBSD** | UFS, UFS2, ext2, FAT, ISO 9660, NTFS, LFS | x86, x86-64, ARM, MIPS, PPC, SPARC64 | pkgsrc |
| **OpenBSD** | ffs, ext2, FAT, ISO 9660, NTFS | x86, x86-64, SPARC, 68k, Alpha, VAX | ports tree, packages |

## Linux

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Название** | Ядро Linux **по умолчанию** | **Поддерживаемые другие основные файловые системы** | **Поддерживаемые архитектуры** | **GUI** | **Управление пакетами по умолчанию/ Инструмент для установки ПО** | **Главный API и язык для текстовых /**CLI**приложений** |
| **AL**T Linux | 2.6.25 | ext2, FAT, ISO9660, JFS,XFS, ReiserFS, NFS, NTFS,UDF | x86 (i586), AMD64 | KDE | RPM, APT | LSB  with C,  POSIX |
| Arch Linux | 2.6.30 | ext2, ext3, ext4, FAT,ISO9660, JFS, NFS, NTFS, ReiserFS, UDF, XFS | x86 (i686), AMD64 | по выбору | pacman, ABS (Arch Build System) | LSB with C,  POSIX |
| ASPLinux | 2.6.17 | ext2, FAT, ISO9660, JFS,NFS, NTFS, ReiserFS, UDF,XFS | x86 (i586), AMD64, PPC | GNOME | RPM, pirut | LSB with C,  POSIX |
| Debian | 2.6.26 | ext2, FAT, ISO9660, JFS,NFS, NTFS, ReiserFS, UDF,XFS | x86, 68k, Alpha, AMD64, ARM, IA-64, Mac/VME, MIPS, PA-RISC, PPC,SPARC, SPARC64, S/390 | по выбору | dpkg, Synaptic, aptitude и APT | pre-LSB with C,  POSIX |
| Fedora | 2.6.29 | ext2, FAT, ISO9660, NFS, ReiserFS, UDF | x86 (i386), AMD64, PPC | GNOME | RPM, yum | LSB with C,  POSIX |
| Gentoo | 2.6.29 | ext2, ext3, FAT, ISO9660,JFS, NFS, NTFS, ReiserFS,Reiser4, UDF, XFS | x86, Alpha, AMD64, ARM, IA-64,MIPS, PA-RISC, PPC, PPC64,SPARC, SPARC64, SuperH, S/390 | по выбору | Portage | pre-LSB with C, Python,  POSIX |
| Knoppix | 2.6.19.1 | н.д. | x86 | KDE | dpkg and APT | н.д. |
| Mandriva | 2.6.22 | ext2, FAT, ISO9660, JFS,NFS, NTFS, ReiserFS, UDF,XFS | x86 (i586), AMD64, PPC | KDE | RpmDrake, urpmi | LSB with C,  POSIX |
| MEPIS | 2.6.10 | ext2, FAT, ISO9660, JFS,NFS, NTFS, UDF, XFS | x86 (i586) | KDE | dpkg and APT | LSB with C, POSIX |
| Slackware | 2.6.29.6 | FAT, ISO9660, JFS, NFS,NTFS, UDF, XFS | x86, IA-64, S/390 | по выбору | pkgtool, installpkg, upgradepkg | LSB with C,  POSIX |
| openSUSE | 2.6.28 | ext2, ext3, FAT, ISO9660,JFS (RO), NFS, NTFS,Reiser4, ReiserFS, UDF,XFS | x86, AMD64, IA-64, PPC | GNOME | RPM, YaST | LSB with C, POSIX |
| Ubuntu | 2.6.31 | ext2, ext3, JFS,FAT, NTFS, ReiserFS, XFS | x86, AMD64, PPC | GNOME/KDE | Synaptic Package Manager, dpkg,APT, PackageKit (KPackageKit),Adept package manager для Kubuntu | LSB with C,  POSIX |
| Xandros Desktop OS | 2.6.15 | ext2, ext3, FAT, ISO 9660,JFS, NFS, NTFS, UDF, XFS, | x86 | KDE | Xandros Networks (APT) | pre-LSB with C,  POSIX |

## LDAP сервер.

**LDAP** (англ. *Lightweight Directory Access Protocol* — «облегчённый протокол доступа к каталогам») — это сетевой протокол для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протоколаDAP. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (*bind*), поиска (*search*) и сравнения (*compare*), а также операции добавления, изменения или удаления записей. Обычно LDAP-сервер принимает входящие соединения на порт 389 по протоколам TCP или UDP. Для LDAP-сеансов, инкапсулированных в SSL, обычно используется порт 636.

Всякая запись в каталоге LDAP состоит из одного или нескольких *атрибутов* и обладает *уникальным именем* (DN — англ. *Distinguished Name*). Уникальное имя может выглядеть, например, следующим образом: «cn=Иван Петров, ou=Сотрудники, dc=example, dc=com». Уникальное имя состоит из одного или нескольких *относительных уникальных имен* (RDN — англ. *Relative Distinguished Name*), разделённых запятой. Относительное уникальное имя имеет вид ИмяАтрибута=значение. На одном уровне каталога не может существовать двух записей с одинаковыми относительными уникальными именами. В силу такой структуры уникального имени записи в каталоге LDAP можно легко представить в виде дерева.

Запись может состоять только из тех атрибутов, которые определены в описании класса записи (*object class*), которые, в свою очередь, объединены в схемы (*schema*). В схеме определено, одни атрибуты являются для данного класса обязательными, а другие — необязательными. Также схема определяет тип и правила сравнения атрибутов. Каждый атрибут записи может хранить несколько значений.

Из свободно распространяемых открытых реализаций наиболее известен сервер OpenLDAP, из проприетарных — поддержка протокола имеется в Active Directory — службе каталогов от компании Microsoft, предназначенной для централизации управления сетями Windows.

**Active Directory** — LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT.

**OpenLDAP Software** — открытая реализация LDAP, разработанная проектом **OpenLDAP Project**.

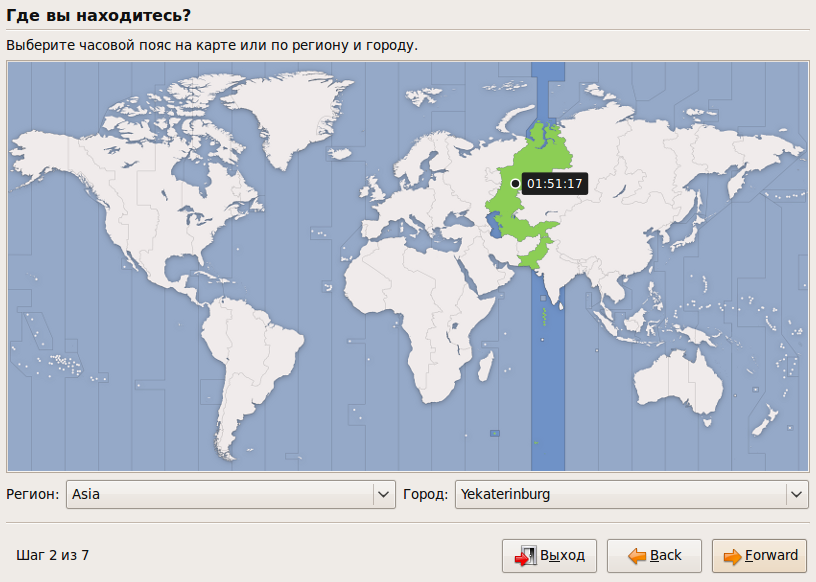
В данной работе использовался сервер **OpenLDAP.**

# Описание реализации применяемых методов.

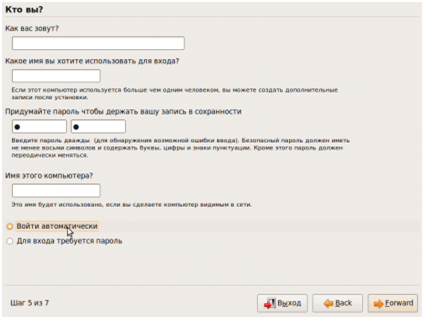
## Установка операционной системы

Установка операционной системы Ubuntu не представляет сложностей и напоминает установку Windows.

Выбор часового пояса:



Ввод личных данных.



Нажимаем «Далее» и видим все текущие настройки установки. Нажимаем «Установить».

После установки перезагружаем компьютер.

## Установка LDAP сеовера.

Чтобы LDAP сервер заработал, мы должны установить несколько пакетов

# apt-get install slapd ldap-utils migrationtools

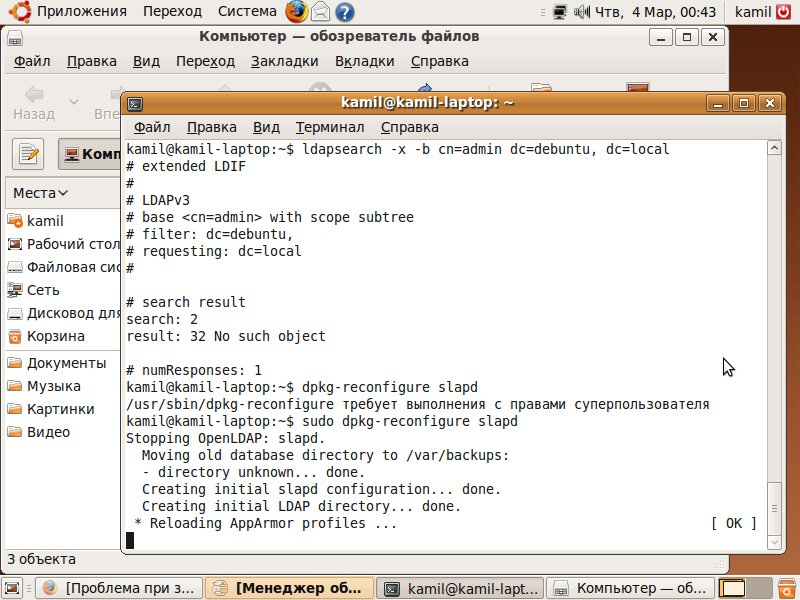
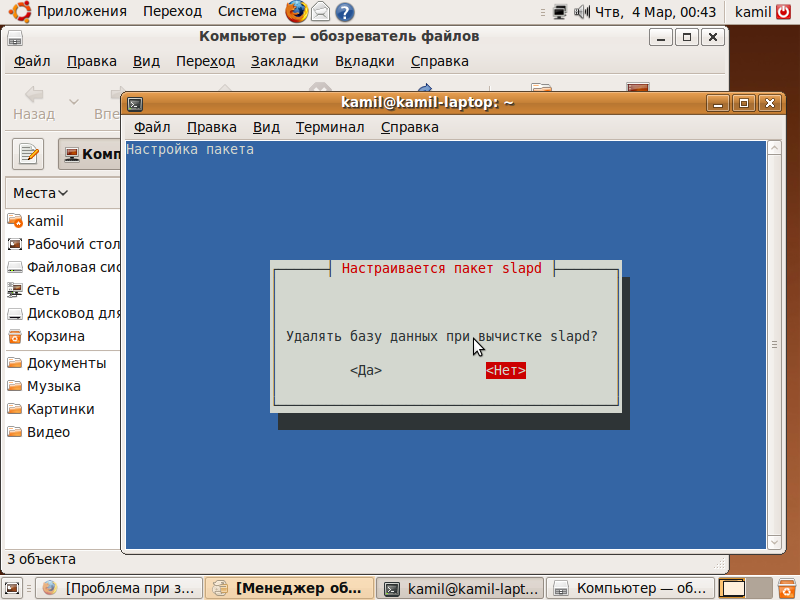
Необходимо ввести пароль администратора.

И затем переконфигурировать сервер

#dpkg-reconfigure slapd

задав следующие параметры:

#пропустить настройку сервера LDAP? ... Нет  
#Доменное имя DNS: ... debuntu.local  
#Название организации: ... Всечтоугодно & Со  
#Пароль для admin: 123  
#Подтвердите пароль: 123  
#Выбор формата базы ldap BDB  
#Удалять базу данных при вычистке slapd? ... Нет  
#Переместить старую базу данных? ... Да  
#Включить протокол LDAPv2? ... Нет



Теперь вы можете проверить, есть ли доступ к ldap-серверу:

$ ldapsearch -x -b dc=debuntu,dc=local

Если выдается ошибка скорее всего сервер не был запущен. Чтобы запустить нужно ввести команду:

# /etc/init.d/slapd start

## Настройка LDAP сервера.

**Заполнение базы:**

Используя migrationtools мы получаем возможность быстро импортировать  
всех существующих пользователей и групп с локальной системы в LDAP.

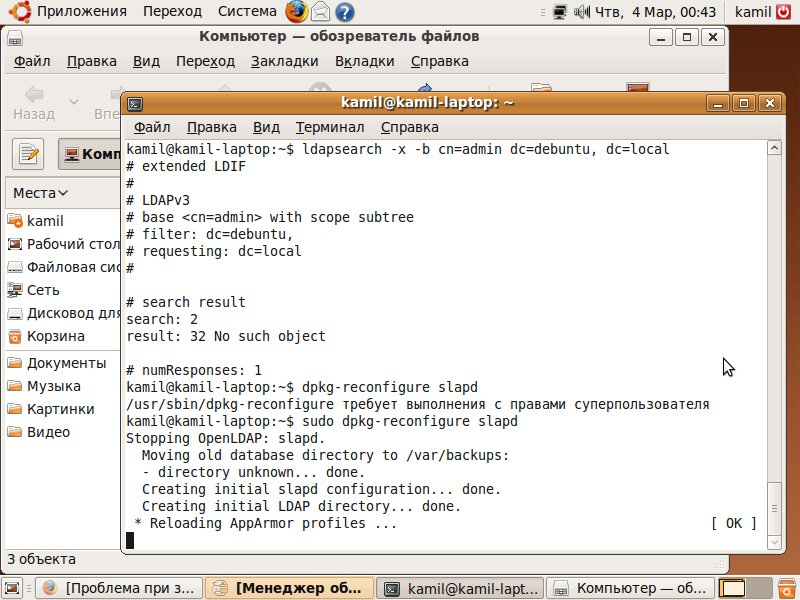
#cd /usr/share/migrationtools/

Нам необходимо отредактировать конфигурационный файл  
migrationtools, имеющий имя migrate\_common.ph и заменить следующие  
параметры:

$DEFAULT\_MAIL\_DOMAIN = "debuntu.local";  
$DEFAULT\_BASE = "dc=debuntu,dc=local";

Затем экспортируем данные:

# ./migrate\_group.pl /etc/group ~/group.ldif  
# ./migrate\_passwd.pl /etc/passwd ~/passwd.ldif



Cкрипт не создает ldap-узлы Group и People, так что нам  
нужно самим создать их. Чтобы сделать это, создаем фай в домашнем  
каталоге с именем ~/people\_group.ldif и заполняем его следующими  
данными:

dn: ou=People, dc=debuntu, dc=local  
ou: People  
objectclass: organizationalUnit

dn: ou=Group, dc=debuntu, dc=local  
ou: Group  
objectclass: organizationalUnit

Теперь у нас есть списки наших пользователей и групп, сконвертированные  
в LDAP формат ldif. Импортируем их в нашу LDAP базу.  
  
# cd  
# ldapadd -x -W -D "cn=admin,dc=debuntu,dc=local" -f ~/people\_group.ldif  
# ldapadd -x -W -D "cn=admin,dc=debuntu,dc=local" -f ~/group.ldif  
# ldapadd -x -W -D "cn=admin,dc=debuntu,dc=local" -f ~/passwd.ldif

где:  
**-x** означает, что мы не используем sasl  
**-W** будет запрошен пароль администратора LDAP  
**-D** используется для идентификации администратора  
**-f** указывает файл, где ldapadd будет брать данные для добавления

Теперь сервер готов для идентификации пользователей. Идем дальше и настроим наших клиентов.

### Настройка клиентов

Каждый клиент нуждается в установке нескольких пакетов. Установим следующие пакеты:

#apt-get install libnss-ldap libpam-ldap nscd

#Универсальный Идентификатор Ресурса сервера LDAP:  
ldapi:///debuntu.local

#Универсальное имя базы поиска  
dc=debuntu,dc=local  
#Использовать версию LDAP 3  
#Учетная запись LDAP для root  
cn=admin,dc=debuntu,dc=local  
#Пароль учетной записи LDAP для root: 123  
#Создать учетную запись администратора для локальной базы: Да  
#База данных требует учетное имя: Нет  
#Учетная запись LDAP для root  
#Пароль учетной записи LDAP для root: 123

libnss-ldap позволит нам использовать ldap как сервер имен, lippam-ldap  
позволит pam аутентифицировать пользователей через LDAP и, наконец, nscd  
- это lookup-демон паролей, групп и хостов, который кеширует результаты,  
чтобы не запрашивать повторно LDAP каждый раз, когда аутентификация  
будет пройдена.

Теперь отредактируем конфигурационные файлы и убедимся, что у нас  
установлены следующие настройки:  
  
#vi /etc/libnss-ldap.conf  
host ldap  
base dc=debuntu,dc=local  
rootbinddn cn=admin,dc=debuntu,dc=local  
  
#vi /etc/libnss-ldap.secret  
XXXXX  
  
#vi /etc/pam\_ldap.conf  
host ldap  
base dc=debuntu,dc=local  
rootbinddn cn=admin,dc=debuntu,dc=local  
  
#vi /etc/pam\_ldap.secret  
XXXXX

Файлы конфигурации pam должны быть отредактированы как указано ниже:

#vi /etc/pam.d/common-account  
account sufficient pam\_ldap.so  
account required pam\_unix.so  
#если вы хотите, чтобы домашний каталог пользователя создавался  
# при первом логине  
#if you want user homedir to be created on first login  
#session required pam\_mkhomedir.so umask=0022 skel=/etc/skel/ silent  
#vi /etc/pam.d/common-auth  
auth sufficient pam\_ldap.so  
auth required pam\_unix.so nullok\_secure use\_first\_pass  
#vi /etc/pam.d/common-password  
password sufficient pam\_ldap.so  
password required pam\_unix.so nullok obscure min=4 max=8 md5  
  
#vi /etc/pam.d/common-session  
session sufficient pam\_ldap.so  
session required pam\_unix.so  
session optional pam\_foreground.so

Наконец, отредактируем nsswitch, так чтобы система имела возможность  
переключаться с локальной аутентификации на аутентификацию ldap.

# vim /etc/nsswitch.conf  
passwd: files ldap  
group: files ldap  
shadow: files ldap

С этими настройками при логине пользователь сначала пытается залогиниться как  
локальный пользователь. Если совпадений имен не найдено, тогда  
запускается аутентификация с ldap сервера.

# Список литературы.

1. http://ubuntu.ru
2. http://ru.wikipedia.org
3. http://sudouser.com