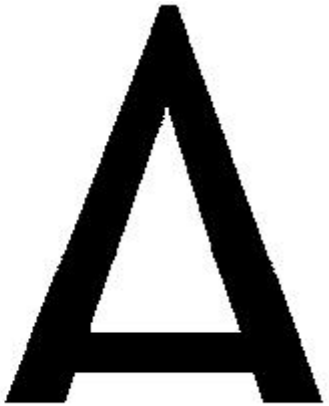
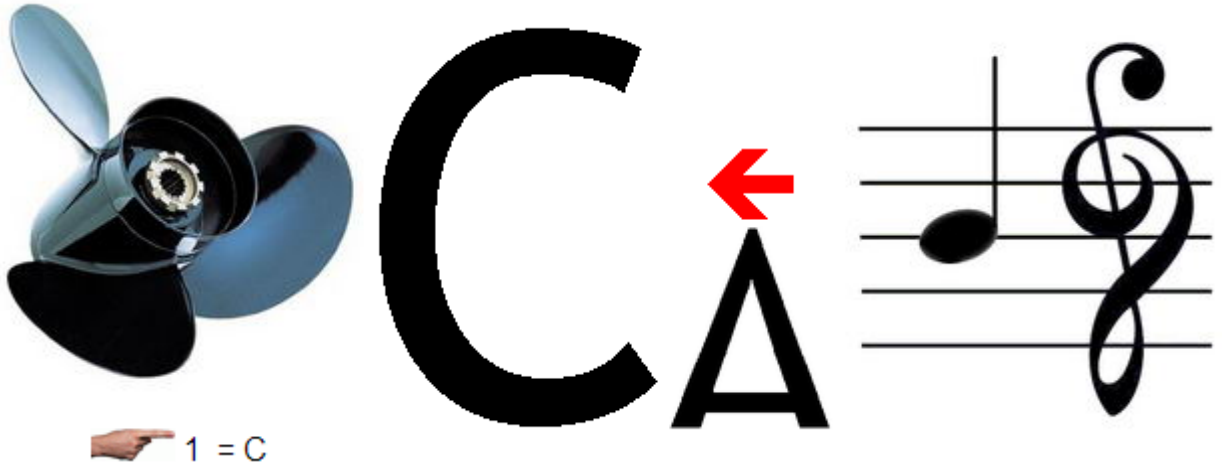
+ Н

1 = И

1 = В



SETI.UCOZ.RU



SETI.UCOZ.RU

Централизованное хранилище данных. Каталоги LDAP

SETI.UCOZ.RU

В ОС Linux существует несколько сервисов, позволяющих централизованно управлять учетными записями пользователей и другой сервисной информацией.

К таким сервисам относятся **NIS** и **LDAP**.

- Сервис **NIS** позволяет хранить следующую информацию по учетным записям пользователей:
  - имена пользователей;
  - пароли пользователей;
  - группы пользователей;
  - расположения домашних каталогов.

В настоящее время на смену сервису NIS пришел более защищенный и производительный сервис каталогов **LDAP**.

SETI.UCOZ.RU

- **Используя сервис LDAP**, пользователи могут работать как на ОС Unix/Linux, так и на ОС Windows.
- **Используя сервис NIS,** пользователи могут работать только на ОС Unix/Linux

- Более того, в ОС Linux существует возможность реализовать подобие домена Active Directory для аутентификации записями пользователей следует пользователей с использованием протокола **Kerberos.**

SETI.UCOZ.RU

Для реализации сервиса каталогов LDAP в ОС Linux используется ПО **openLDAP.** Данное ПО можно разделить на следующие компоненты:

- **серверы:** предоставляют службы LDAP;
- **клиенты:** оперируют данными LDAP;
- **утилиты:** поддерживают работоспособность сервера LDAP;
- **библиотеки:** предоставляют API для доступа к данным LDAP;

SETI.UCOZ.RU

- **Серверная часть сервиса LDAP** представлена демоном **slapd**, который предоставляет доступ к одному или нескольким каталогам данных.

- **Серверная часть LDAP** может хранить данные локально или предоставлять доступ к внешним источникам данных.

SETI.UCOZ.RU

- **Клиенты** получают доступ к сервису **LDAP через LDAP-протокол**. Их функция заключается в формировании и передаче запросов к демону **slapd**, который выполняет необходимые операции над данными в каталогах.
- Обычно сначала клиент подключается к демону slapd, аутентифицируется, а затем осуществляет необходимые операции, посылая LDAP запросы.
- После получения ответа на посланный запрос клиент завершает процесс биндинга и отключается

SETI.UCOZ.RU

- **Утилиты LDAP**, в отличие от клиентов, не используют протокол LDAP для доступа к каталогам - они подключаются к серверу на более низком уровне и выполняют служебные операции над данными, например, создают новые каталоги.

- Данные утилиты используются в основном для сопровождения демона **slapd.**

SETI.UCOZ.RU

Для **развертывания сервиса LDAP** в ОС Linux должны быть установлены пакеты **openLDAP** и **openLDAP-servers**. В общем случае процесс развертывания сервиса LDAP делится на следующие этапы:

- **установка бинарных пакетов openLDAP и openLDAP-servers;**
- **настройка сервера LDAP при помощи конфигурационного файла slapd.conf;**
- **проверка конфигурационного файла slapd.conf при помощи утилиты slaptest;**
- **создание каталога LDAP;**
- **настройка клиентов LDAP при помощи конфигурационного файла ldap.conf.**

SETI.UCOZ.RU

Настройка конфигурационных файлов LDAP

- Все модули LDAP условно разделяются **на**

1)хранилища данных LDAP (backends), в которых непосредственно хранятся записи каталога LDAP

2)расширения LDAP (overlay), которые используются для добавления новых функциональных возможностей сервиса LDAP.

SETI.UCOZ.RU

- Основным конфигурационным файлом, который использует демон **slapd,** является файл **/etc/slapd.conf**. Данный файл содержит множество директив, которые разделяются на три группы:
- **Basics**
- **Database Configuration**
- **ACLs.**

SETI.UCOZ.RU

- После того, как конфигурационный файл **slapd.conf** будет создан, необходимо проверить его синтаксис, запустив команду **slaptest -y -f /etc/openldap/slapd. conf.**

- Если файл содержит ошибки, то в выводе будет указана строка, содержащая ошибку и сама ошибка.

SETI.UCOZ.RU

Создание каталога LDAP

- Каждый объект в каталоге LDAP называется **записью,** а каждая запись обладает несколькими **атрибутами.**
- Среди атрибутов есть **обязательные** и **необязательные**.
- Каждая запись **идентифицируется** своим **отличительным именем Distinguish Name (DN).**
- Записи LDAP обычно составляются на основе использования атрибута **objectClass.**

SETI.UCOZ.RU

- Записи добавляются в каталог с использованием файла **формата LDIF**.
- Каждая запись в данном файле начинается с отличительного **имени (DN),** которое уникальным образом идентифицирует запись в каталоге.
- Запись состоит из нескольких атрибутов, записанных в отдельной строке.

SETI.UCOZ.RU

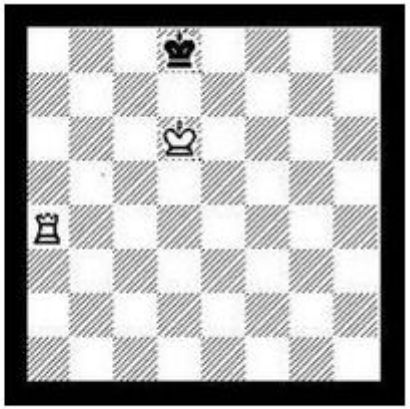
- После добавления всех записей из файла **LDIF** необходимо **установить соответствующие права** для пользователя **ldap,** от имени которого запускается демон **slapd,** на все файлы базы данных каталога **LDAP,** находящихся в каталоге **/var/lib/ldap.**

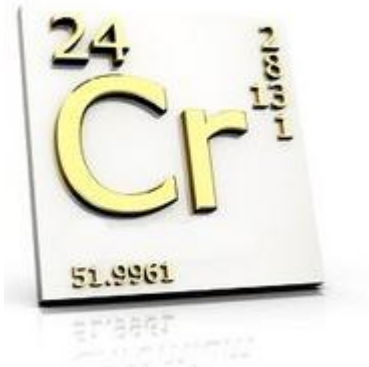
SETI.UCOZ.RU

Подключение к серверу LDAP

- Для того чтобы клиенты могли **подключаться к серверу LDAP,** в их системе должны быть установлены пакеты openldap-clients и nss_ldap.
- Данные пакеты могут использовать как утилиты работы с каталогами LD AP, такие как **ldapsearch** (поиск записей) или **ldapadd** (добавление записей), так и конечные приложения, например, почтовый клиент **Evolution.**

SETI.UCOZ.RU





”

SETI.UCOZ.RU

,  ” X „

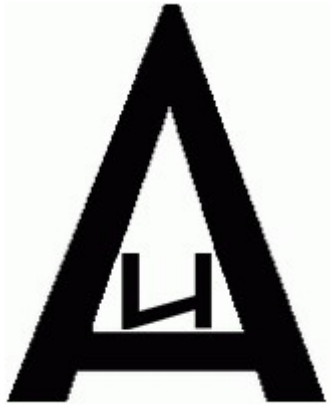
, 

 2 = B

SETI.UCOZ.RU

Б,  ’

Д,  ” 



SETI.UCOZ.RU