

ЛАБОРАТОРНАЯ РАБОТА №5

СЦЕНАРИЙ «Практическое использование протокола LDAP»

Работа нацелена на получение практических навыков по работе с протоколом LDAP, получению доступа к данным пользователя корпоративного домена по сети, в т.ч. в полностью автоматическом виде.

Используемые приложения доступны по ссылке ниже или на официальных сайтах компаний-разработчиков:

https://drive.google.com/drive/folders/1p-S3ZnYWMKX_fytjITX3Gllu-wGphCPi?usp=sharing

В работе используются:

1. Программа (оконное приложение) LDAP-клиент **LDAP Admin**: <http://www.ldapadmin.org/>
2. Комплект программ (консольное приложение) **LDAP-клиент OpenLDAP**:
<http://www.openldap.org/>
3. **Контроллер домена универсального сетевого каталога Active Directory**, развернутый в облаке по адресу _194.226.199.73:38938

Работа состоит из 3-х частей:

1. **Часть 1:** практическое знакомство с протоколом LDAP, работа в оконном приложении (LDAP Admin) – **6 баллов**
Необходимо подключиться к удаленному контроллеру домена по протоколу LDAP с использованием LDAP Admin, изучить структуру сетевого каталога, посмотреть данные по пользователям домена и компьютерам.
2. **Часть 2:** практическое знакомство с протоколом LDAP, работа в консольном приложении (OpenLDAP) – **6 баллов**
Необходимо подключиться к удаленному контроллеру домена по протоколу LDAP с использованием OpenLDAP, с помощью команд скачать данные по пользователям или компьютерам.
3. **Дополнительная (необязательная) часть повышенной сложности:** реализовать корпоративный мини-PKI — реализовать скрипты, автоматически скачивающие данные по пользователям домена и создающий для них цифровые сертификаты согласно лабораторной работе №2 (только пользовательские!) - **6 баллов**

Часть 1. Практическая работа с протоколом LDAP в оконном приложении (LDAP Admin)

Вес части при выполнении всех условий: 6 баллов

С помощью LDAP-клиента LDAP Admin изучите возможности по использованию протокола LDAP для доступа к Active Directory OC Windows Server. Найдите и ознакомьтесь с основными ресурсными объектами каталога: пользователями, компьютерами, правилами, системными объектами и т.д.

- Установите соединение с LDAP-сервером Windows Server. Установите соединение с сервером 194.226.199.73:38938
- Настройки соединения приведены ниже:
 - Логин пользователя: admin, пароль: xxXX1234
Обращаем внимание, что в **реальной ситуации использование пароля администратора для подключения по LDAP недопустимо!**
 - Тип аутентификации: GSS-API, имя домена: dc=demo,dc=lab

Если всё выполнено корректно, при нажатии Test Connection появится окно об успешном соединении. Нажмите кнопку OK.

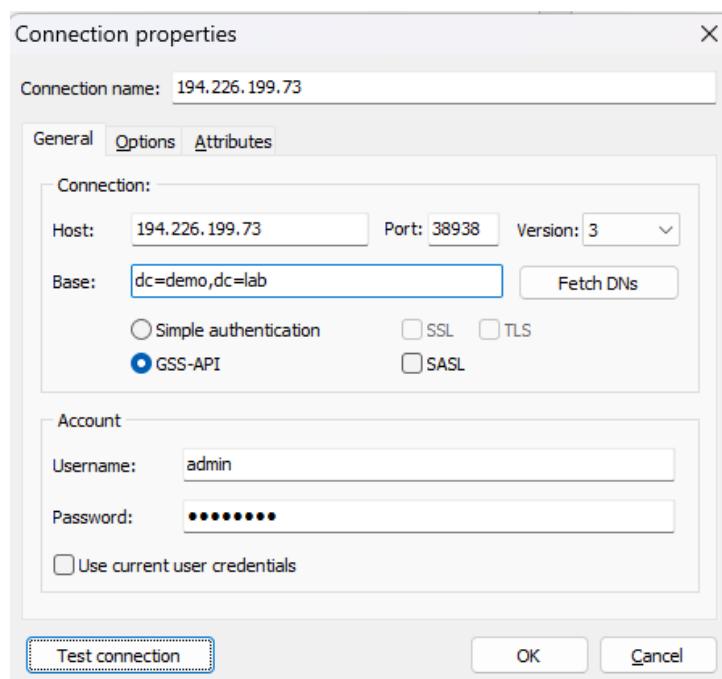


Рис. 1 Настройки соединения LDAP Admin

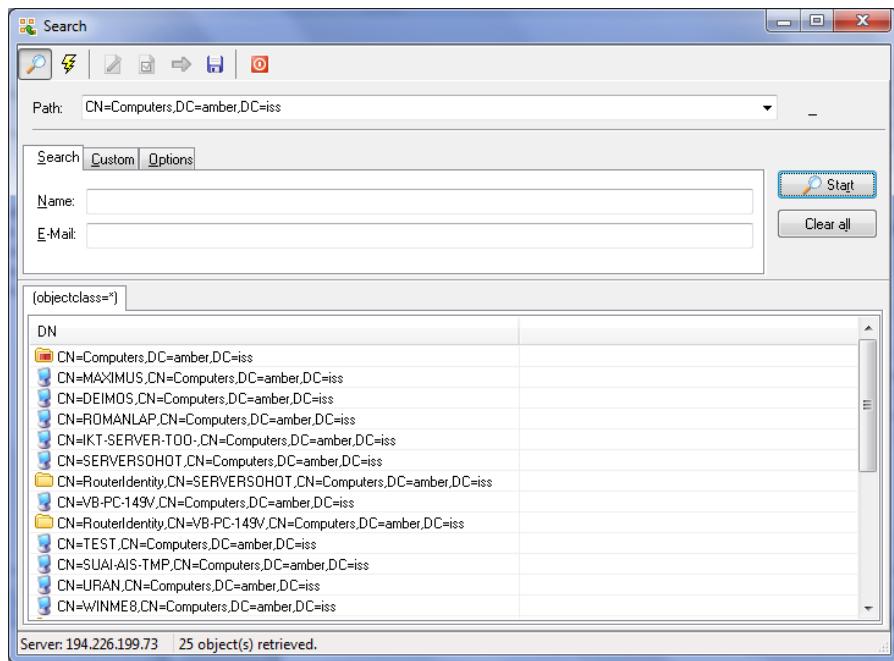


Рис. 2 Окно поиска LDAP Admin

- Последовательно найдите 2х любых пользователей, у которых первая буква имени или фамилии совпадает с первой буквой Вашего имени или фамилии. Откройте окно атрибутов и сделайте снимок экрана для загрузки в LMS.

По итогу части 1 Л/Р загрузите в LMS скриншоты (2 шт.) окна LDAPAdmin с найденными атрибутами пользователей, согласно условия выше.

Часть 2. Практическая работа с протоколом LDAP в консольном приложении (OpenLDAP)

Вес части при выполнении всех условий: 6 баллов

Выполните необходимые операции поиска, по шаблону, предоставленному преподавателем.

- С помощью LDAP-клиента OpenLDAP реализуйте консольные запросы к LDAP-серверу, согласно примера (.bat скрипта), выданного преподавателем. Настройки подключения идентичны настройкам подключения с помощью LDAP Admin.
Обратите внимание, что IP-адрес и номер порта в .bat файле необходимо изменить.
- Получите данные тех же пользователей, что в части 1 с использованием команды LDAP ldapsearch.

По итогу части 2 Л/Р загрузите в LMS:

- Скриншот (1 файл) измененного bat-файла с запросами на данные одного (или нескольких) пользователей домена согласно условиям выше.
- Скриншот (1 файл) консоли cmd после выполнения bat-файла, демонстрирующий, что данные пользователей (согласно условия выше) получены из домена.

Если, кроме целевых 2-х пользователей получены другие (т.е. запрос неточен): минус 3 балла.

Часть 3. Мини-РКІ с использованием протокола LDAP

Часть повышенной сложности для получения дополнительных баллов.

Вес части при выполнении всех условий: 6 баллов.

Реализуйте программу (на любом языке программирования или с помощью скриптов), выполняющую функции корпоративного Центра регистрации, а именно:

- Автоматическая загрузка данных по пользователям (или компьютерам) из домена demo.lab (см. выше) по протоколу LDAP согласно условию (ниже). Используйте для подключения утилиту openldap или аналог в консольном режиме. Домен для подключения используется тот же, что в частях 1 и 2. Пример использования openldap представлен в LMS в теме по LDAP.
- Автоматическая интерпретация данных (парсинг) для передачи в созданный в рамках лабораторных работ 1 и 2 Центр сертификации (набор скриптов по созданию сертификатов).
- Автоматическое создание сертификатов пользователей согласно условию выше.

Итог работы: для заданных в параметре bat-файла пользователей должна подгружаться автоматически информация из AD и автоматически создаваться пользовательские ключи/сертификаты только для этих пользователей.

По итогу части 3 Л/Р загрузите в LMS архив со всеми исполняемыми файлами, необходимыми для выполнения работы (.bat файлы, программа парсинга полученных по LDAP данных и т.п.). При проверке будет оценена работоспособность решения.

Проверка заключается в запуске головного скрипта/исполняемого файла, после чего автоматически в каталоге должны появиться цифровые сертификаты для выбранных в соответствие с заданием пользователей.