# Управление схемой службы каталогов

Что такое Active Directory?

Что такое схема Active Directory?

Обзор способов перепрограммирования схемы

- методы (LDAP и ADSI)

- [Directory Services Data Exchange](https://msdn.microsoft.com/en-us/library/windows/desktop/aa813598(v=vs.85).aspx) and [DSML Services for Windows](https://msdn.microsoft.com/en-us/library/windows/desktop/aa813632(v=vs.85).aspx) – Надстройки

Обзор существующих решений по управлению схемой службы каталогов.

### **CSVDE**

Средство CSVDE позволяет импортировать новые объекты в Active Directory, используя исходный CSV-файл; оно также дает возможность экспортировать существующие объекты в файл CSV. CSVDE нельзя использовать для изменения существующих объектов; при использовании этого средства в режиме импорта можно лишь создавать новые объекты.

Экспорт списка существующих объектов с помощью CSVDE довольно прост. Ниже показано, как экспортировать объекты Active Directory в файл под названием ad.csv:

**csvde –f ad.csv**

Параметр –f указывает, что за ним следует имя выходного файла. Но следует понимать, что, в зависимости от среды, этот базовый синтаксис может привести к выводу огромного и неудобного файла. Чтобы ограничить средство экспортом лишь объектов внутри определенного структурного подразделения (OU), команду можно изменить следующим образом:

**csvde –f UsersOU.csv –d ou=Users,dc=contoso,dc=com**

Предположим далее, что мне необходимо экспортировать лишь объекты пользователя в мой файл CSV. В таком случае можно добавить параметр –r, позволяющий указать фильтр протокола LDAP для данного поиска, который ограничит число экспортируемых атрибутов (заметьте, что все нижеследующее является одной строкой):

**csvde –f UsersOnly.csv –d ou=Users,dc=contoso,dc=com –r  
“(&(objectcategory=person)(objectclass=user))” –l  
DN,objectClass,description**

Параметр –i позволяет импортировать объекты в Active Directory из исходного файла CSV. Однако создание объектов пользователя с помощью CSVDE имеет один важный недостаток: с помощью этого средства нельзя устанавливать пароли пользователей, поэтому я бы не стала использовать CSVDE для создания объектов пользователей.

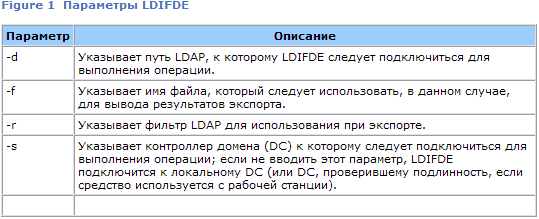
### **LDIFDE**

Active Directory предоставляет второе встроенное средство для пакетных операций пользователей, именуемое LDIFDE и обладающее более широкими и гибкими возможностями, чем CSVDE. Помимо создания новых объектов, LDIFDE позволяет модифицировать и удалять существующие объекты и даже расширять схему Active Directory. Платой за гибкость LDIFDE является то, что необходимый входной файл (файл LDIF) с расширением .ldf использует более сложный формат, чем простой файл CSV. (Немного поработав, можно также настраивать пароли пользователей, но об этом чуть позже.)

Начнем с простого примера — экспорта пользователей в структурном подразделении в файл LDF (отметьте, что все нижеследующее является одной строкой ):

**ldifde -f users.ldf -s DC1.contoso.com -d “ou=UsersOU,dc=contoso,dc=com”  
–r “(&(objectcategory=person)(objectclass=user))”**

Как и в случае большинства средств командной строки, полное описание параметров LDIFDE можно получить, запустив команду LDIFDE /? . На Рис. 1 показаны те, что я использовала здесь. (Заметьте, что параметры для команд CSVDE и LDIFDE одинаковы.)



По-настоящему возможности LDIFDE раскрываются при создании объектов и управлении ими. Однако перед этим необходимо создать входной файл. Нижеследующий код создает две новых учетных записи пользователя — afuller и rking; для создания входного файла введите текст в блокноте (или другом редакторе открытого текста) и сохраните его как NewUsers.ldf:

dn: CN=afuller, OU=UsersOU, DC=contoso, DC=com  
**changetype: add**  
**cn: afuller**  
**objectClass: user**  
**samAccountName: afuller**

**dn: CN=rking, OU=UsersOU, DC=contoso, DC=com**  
**changetype: add**  
**cn: rking**  
**objectClass: user**  
**samAccountName: rking**

После того как создание файла завершено, запустите следующую команду:

**ldifde –i –f NewUsers.ldf –s DC1.contoso.com**

Единственный новый параметр здесь — это -i, который, как несложно догадаться, указывает, что выполняется операция импорта, а не экспорта.

При модификации или удалении существующих объектов синтаксис команды LDIFDE не меняется; вместо этого изменяется содержимое файла LDF. Для изменения поля описания учетных записей пользователей создайте текстовый файл, именуемый ModifyUsers.ldf, такой как показано на Рис. 2.

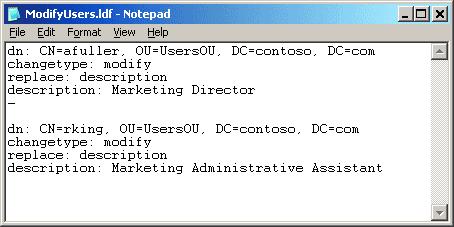


Рис. 2 Файл LDF ModifyUsers

Изменения импортируются путем запуска того же синтаксиса команды LDIFDE, что и раньше, с указанием нового файла LDF после параметры -f. Формат LDF для удаления объектов еще проще; для удаления пользователей, с которыми вы работали, создайте файл, именуемый DeleteUsers.ldf, и введите следующее:

**dn: CN=afuller OU=UsersOU, DC=contoso, DC=com**  
**changetype: delete**

**dn: CN=rking, OU=UsersOU, DC=contoso, DC=com**  
**changetype: delete**

Отметьте, что, в отличие от CSVDE, LDIFDE может настраивать пароли пользователей. Однако перед настройкой атрибута unicodePWD для учетной записи пользователя необходимо настроить шифрование SSL/TLS на контроллерах домена.

Вдобавок, LDIFDE может создавать и модифицировать любые объекты Active Directory, а не только учетные записи пользователей. Например, нижеследующий файл LDF создаст новое расширение схемы, именуемое EmployeeID-example, в схеме леса contoso.com:

**dn: cn=EmployeeID-example,cn=Schema,**  
**cn=Configuration,dc=contoso,dc=com  
changetype: add  
adminDisplayName: EmployeeID-Example  
attributeID: 1.2.3.4.5.6.6.6.7  
attributeSyntax: 2.5.5.6  
cn: Employee-ID  
instanceType: 4  
isSingleValued: True  
lDAPDisplayName: employeeID-example**

Поскольку в файлах LDIFDE используется стандартный отраслевой формат файла LDAP, приложения от сторонних производителей, которым необходимо модифицировать схему Active Directory, часто поставляют файлы LDF, с помощью которых можно изучить и одобрить изменения, прежде чем применять их к производственной среде.