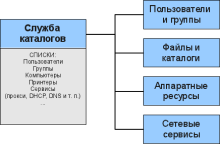
# Управление схемой службы каталогов

## Служба каталогов

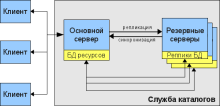
### Описание службы каталогов

**Служба каталогов** — это сетевой сервис, представляющий централизованные средства управления ресурсами автоматизированной системы. Под ресурсами подразумеваются все компоненты сетевой инфраструктуры, которые используются для выполнения функций АСУ: пользователи, файлы и каталоги, устройства, сетевые сервисы и т.д. ([рис.1](http://www.4stud.info/networking/directory-service.html#ds)).

*[](http://www.4stud.info/networking/img/directory-service.png)*

*Рис. 1. Служба каталогов*

Как правило, служба каталогов состоит из базы данных, в которой размещены сведения о сетевых ресурсах и серверного ПО, представляющего механизмы доступа к этой базе. Как база данных сервиса каталогов, так и ее управляющая программа могут быть распределены на несколько серверов ([рис. 2](http://www.4stud.info/networking/directory-service.html)).

*[](http://www.4stud.info/networking/img/distributed-ds.png)*

*Рис. 2. Распределенная служба каталогов*

Основными функциями службы каталогов являются следующие:

* Управление пользователями и группами (создание/удаление, настройка прав доступа).
* Управление ресурсами (представление в общий доступ, установка ограничений, удаленное администрирование и т.п.).
* Разграничение прав доступа (как правило, на уровне пользователей, групп и отдельных ресурсов).

Среди дополнительных функций сервиса каталогов можно указать, например, такие:

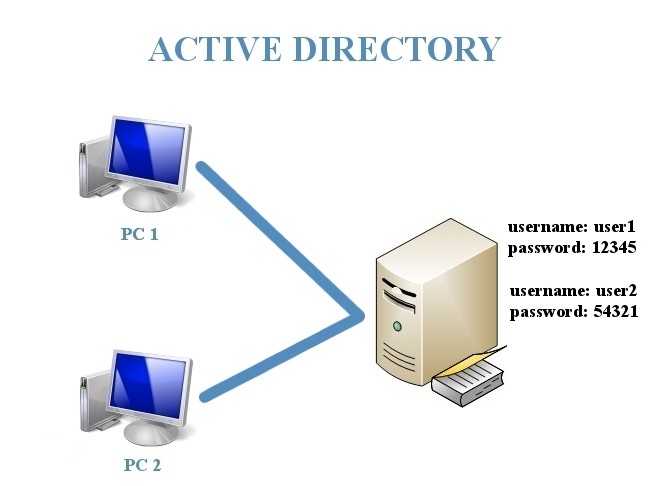
* поиск ресурсов;
* распространение сетевых политик;
* интеграция с другими сервисами.

**Сетевая политика** — совокупность правил, определяющих методы и средства взаимодействия с общими ресурсами в корпоративной сети.

Сетевые ресурсы в службе каталогов обычно представлены в виде иерархической структуры. Такой способ наиболее близок к реальной организационной модели подавляющего большинства предприятий и организаций. Корень иерархии описывает предприятие в целом, нижележащие уровни — подразделения и отдельные элементы. Для единообразного обращения к любому элементу иерархии протокол взаимодействия представляет унифицированную схему адресации — либо собственную, либо совместимую со стандартными схемами.

Active Directory — служба каталогов корпорации [Microsoft](http://geek-nose.com/kak-sozdat-uchetnuyu-zapis-microsoft-majkrosoft-detalnaya-instrukciya/) для ОС семейства Windows NT. Данная служба позволяет администраторам использование групповых политик для обеспечения единообразия настроек пользовательской рабочей среды, установки [ПО](http://geek-nose.com/programmy/), обновлений, пр

При наличии в сети более 10 рабочих станций, рационально оправданным стает подход, при котором одному узлу сети делегируют права выполнения аутентификации и авторизации. Этим узлом и выступает контролер домена — Active Directory. Контролер домена хранит базу данных учетных записей т.е. он хранит учетку и для РС1 и для РС2. Теперь все учетные записи прописываются один раз на контролере домена, а необходимость в локальных учетных записях теряет смысл.

[](http://geek-nose.com/wp-content/uploads/2015/03/active-directory-dlya-chaynikov-03.jpg)

Теперь, когда пользователь заходит на ПК, вводя свой [логин и пароль](http://geek-nose.com/kak-postavit-parol-na-noutbuk-poshagovaya-instrukciya/), эти данные передаются в закрытом виде на контролер домена, который выполняет процедуры аутентификации и авторизации, после чего контролер домена выдает пользователю, осуществившему вход, что-то вроде паспорта, с которым он в дальнейшем работает в сети и который он предъявляет по запросу других компьютеров сети, серверов к чьим ресурсам он хочет подключиться.

Контролер домена — это компьютер с поднятой службой Active Directory, который управляет доступом пользователей к ресурсам сети. Он хранит ресурсы (например, [принтеры](http://geek-nose.com/kakoj-printer-skaner-kopir-luchshe-dlya-doma/), папки с общим доступом), службы (например, [электронная почта](http://geek-nose.com/ustanovka-i-nastrojka-outlook/)), людей (учетные записи пользователей и групп пользователей), компьютеры (учетные записи компьютеров). Число таких сохраненных ресурсов может достигать миллионов объектов. В качестве контролера домена могут выступать следующие версии MS [Windows](http://geek-nose.com/operacionnye-sistemy/windows-10/): Windows Server 2000/2003/2008/2012 кроме редакций Web-Edition.

Контролер домена помимо того что является центром аутентификации сети, также является центром управления всеми компьютерами. Сразу после включения компьютер начинает обращаться к контролеру домена, задолго до появления окна аутентификации, таким образом выполняется аутентификация не только пользователя вводящего логин и пароль но и аутентификация клиентского компьютера.

### Настройка Active Directory

## Схема службы каталогов

### 2.2.1.. Описание схемы службы каталогов

Схема службы каталогов Active Directory

реализована как набор экземпляров

классов объектов, которые хранятся в каталоге

.

Этим она весьма отличается

от многих каталогов, в

которых схема существует, но хранится в виде

текстового файла, который должен читаться при запуске

.

Хранение схемы в

каталоге дает много преимуществ.

Например, пользовательские приложения

могут, читая схему, определить, какие объекты и свойства им доступны

.

В службе каталогов Active Directory

схема может обновляться динамически.

Это значит, что приложение может расширять схему, добавляя к ней новые

атрибуты и классы, и тут же воспользоваться этим расширением

.

Обновления

схемы выполняются путем создания или

изменения объектов схемы, которые

хранятся в каталоге. Как и все объекты в службе каталогов Active Directory,

объекты схемы защищены списками управления доступом

(ACL–Access Control Lists),

поэтому изменять схему могут только пользователи,

обладающими соответствующими полномочиями

.

### 2.2.2. Классы

### 2.2.3. Атрибуты

## Обзор методов управления схемой Active Directory

* + 1. LDAP
    2. ADSI
    3. Определение способа управления схемой службы каталогов

## Обзор существующих решений для управления 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.

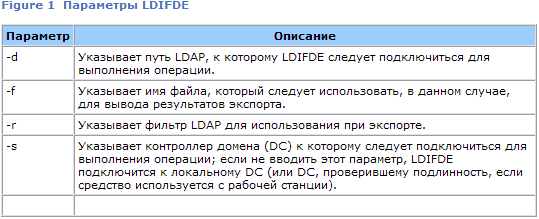
### **LDIFDE**

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.

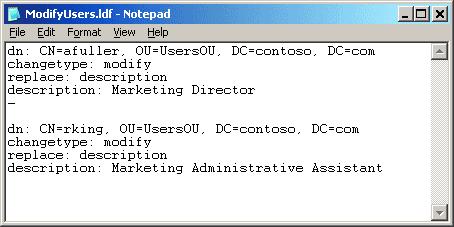


Рис. 2 Файл LDF ModifyUsers

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.