ADMC

Дмитрий Дегтярев
Software Engineer, BaseALT

Microsoft

Active Directory

Задачи

- Управление учетными записями, группами, компьютерами, групповыми политиками
- Добавление компьютеров в домен
- Редактирование прав пользователей
- И другие...

Существующие решения

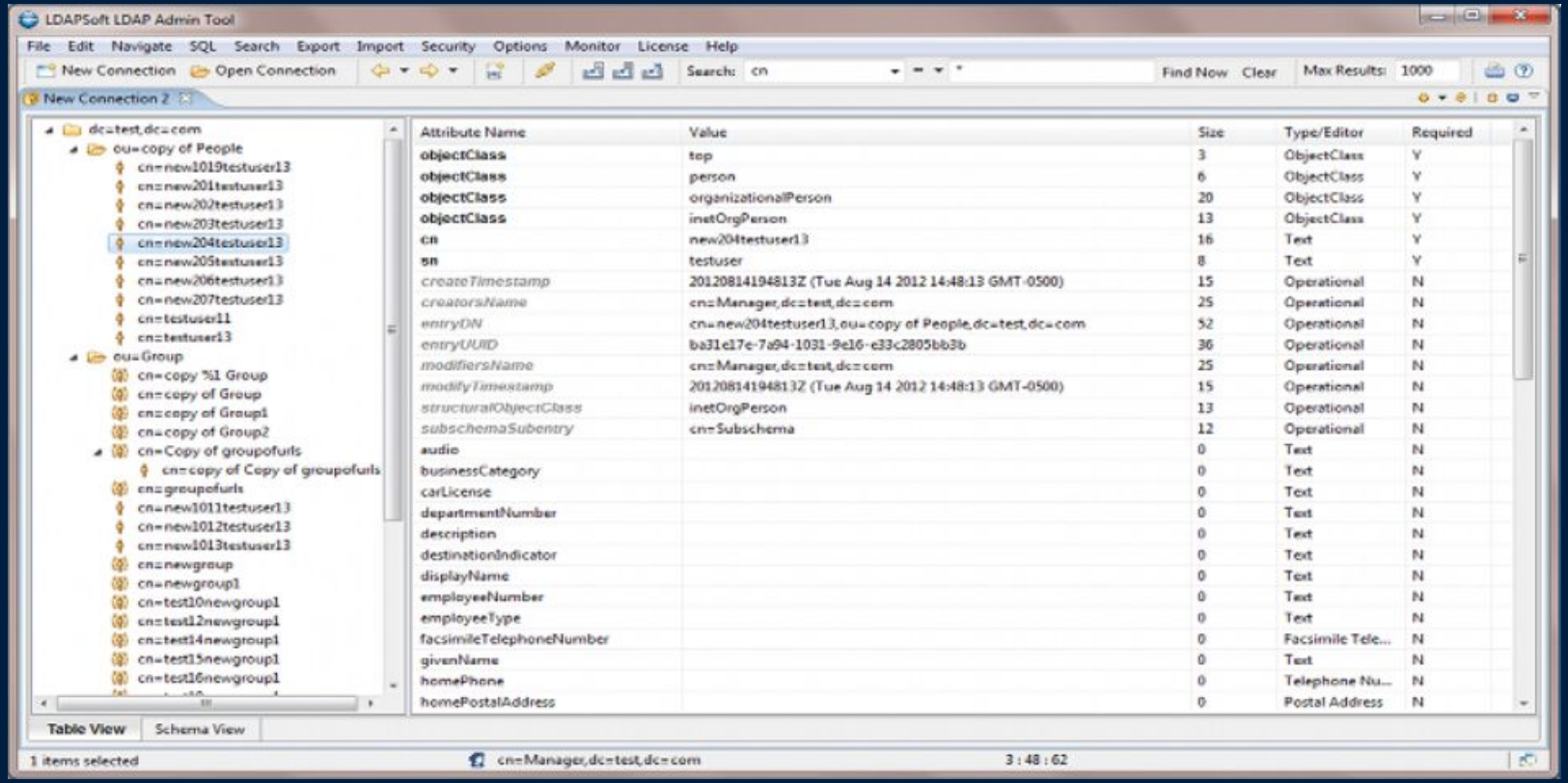
ldapsearch


LDAPSearch - www.SecurityXploded.com
LDAP Search
Simple LDAP Directory Search Tool
Show Help
About
Connection
Host Name or IP Address:
ldap.uconn.edu
LDAP Port:
636
Use SSL
Server Certificate File:
Use Certificate (DER format only)
Authentication
Login DN:
Password:
Search
LDAP Base DN:
Object Filter:
(objectClass=*)
Search for Attributes:
dn,cn,sn
Get all possible attributes
Scope of Search:
LDAP_SCOPE_BASE
Search Timeout (seconds):
10
Start Search
Result
LDAP Search is started ....
Host = ldap.uconn.edu
Port = 636
Connection Type = SSL
Timeout = 10 seconds
STEP 1 => Performing LDAP-SSL initialization
LDAP SSL initialization completed
STEP 2 => Connecting to LDAP server using the given credentials...
LDAP bind completed successfully.
STEP 3 => Searching on the server ...
Export

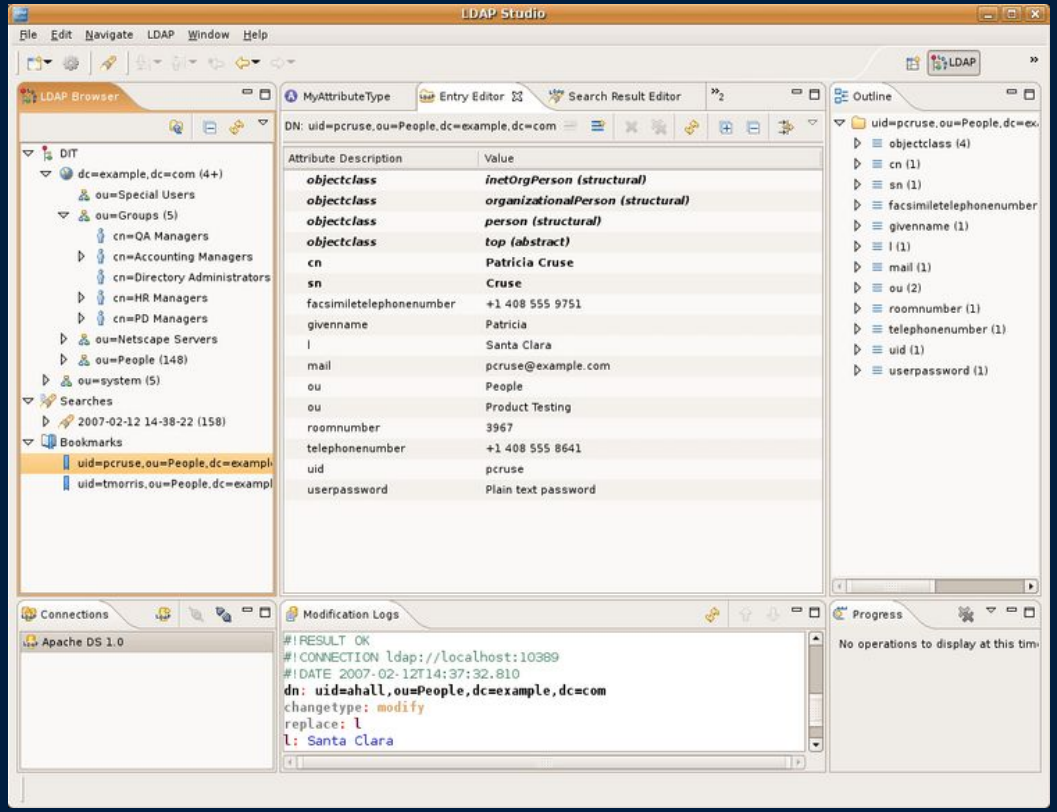
samba-tool

```
root@adc1:~# samba-tool -h
Usage: samba-tool <subcommand>

Main samba administration tool.


Options:
  -h, --help       show this help message and exit

  Version Options:
    -V, --version  Display version number


Available subcommands:
  dbcheck     - Check local AD database for errors.
  delegation  - Delegation management.
  dns         - Domain Name Service (DNS) management.
  domain      - Domain management.
  drs         - Directory Replication Services (DRS) management.
  dsacl       - DS ACLs manipulation.
  fsmo        - Flexible Single Master Operations (FSMO) roles management.
  gpo         - Group Policy Object (GPO) management.
  group       - Group management.
  ldapcmp     - Compare two ldap databases.
  ntacl       - NT ACLs manipulation.
  processes   - List processes (to aid debugging on systems without setproctitle).
  rodc        - Read-Only Domain Controller (RODC) management.
  sites       - Sites management.
  spn         - Service Principal Name (SPN) management.
  testparm    - Syntax check the configuration file.
  time        - Retrieve the time on a server.
  user        - User management.
  vampire     - Join and synchronise a remote AD domain to the local server.
For more help on a specific subcommand, please type: samba-tool <subcommand> (-h|--help)
```

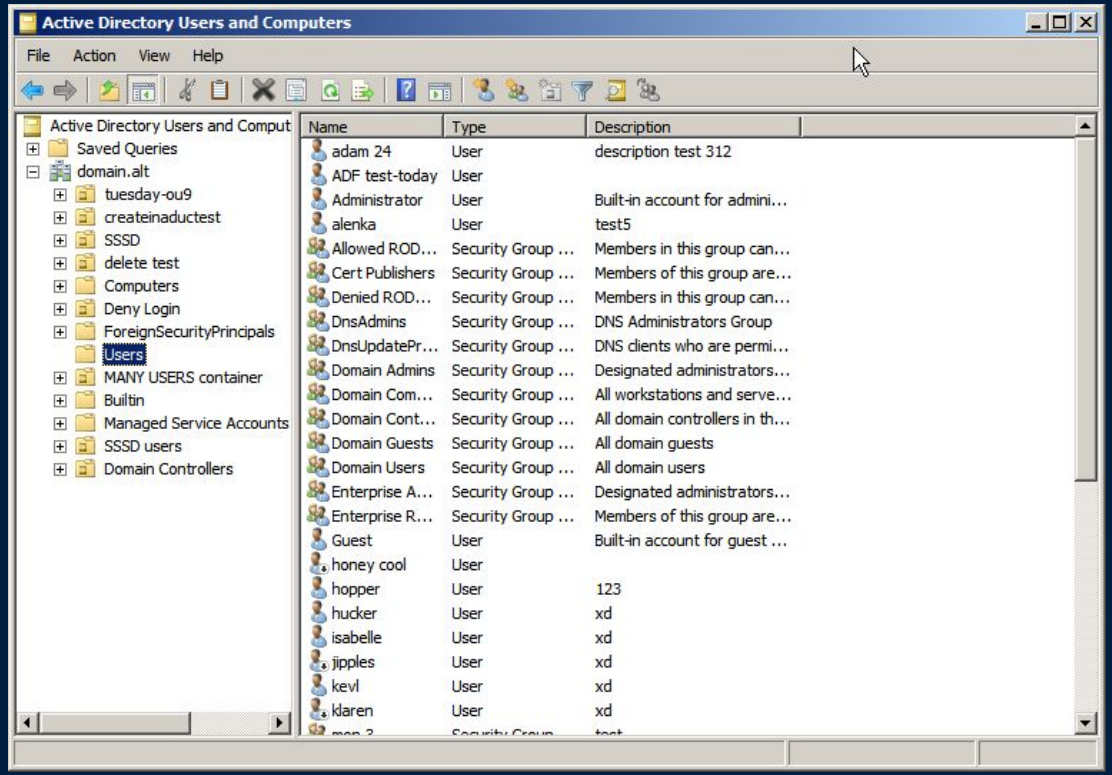
LDAP Browser



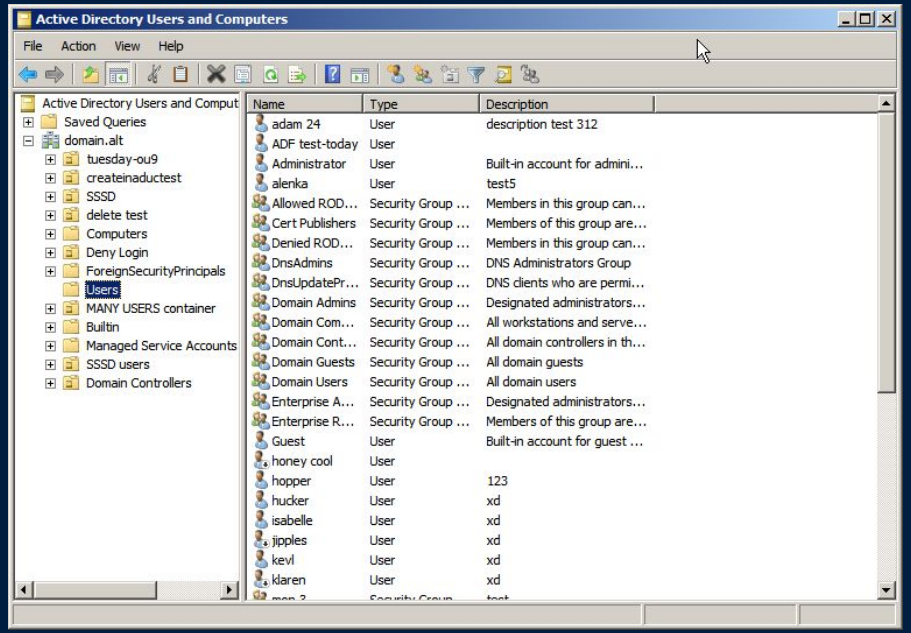
Apache Directory

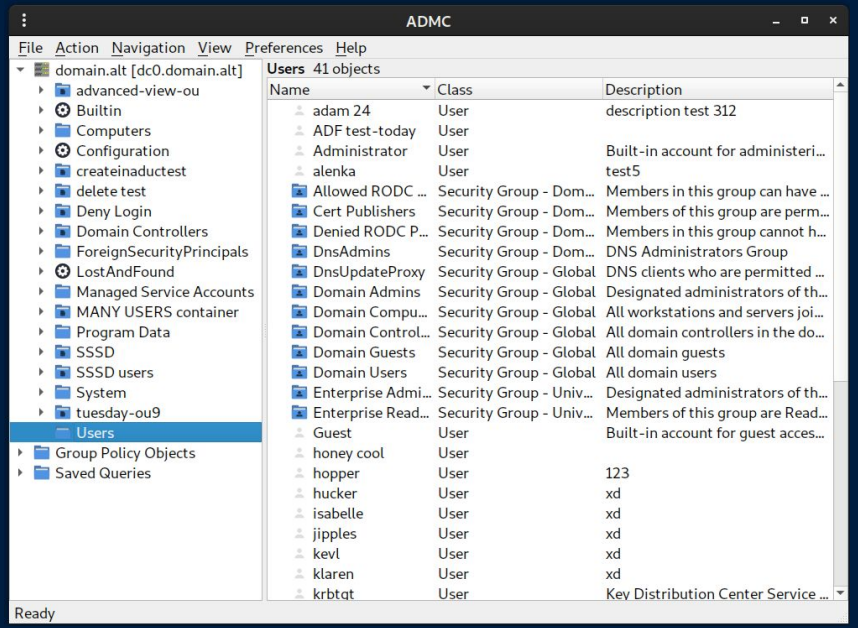


ADUC


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Comput
Saved Queries
domain.alt
tuesday-ou9
createinaductest
SSSD
delete test
Computers
Deny Login
ForeignSecurityPrincipals
Users
MANY USERS container
Builtin
Managed Service Accounts
SSSD users
Domain Controllers
Name
Type
Description
adam 24 User description test 312
ADF test-today User
Administrator User Built-in account for admini...
alenka User test5
Allowed ROD... Security Group ... Members in this group can...
Cert Publishers Security Group ... Members of this group are...
Denied ROD... Security Group ... Members in this group can...
DnsAdmins Security Group ... DNS Administrators Group
DnsUpdatePr... Security Group ... DNS clients who are permi...
Domain Admins Security Group ... Designated administrators...
Domain Com... Security Group ... All workstations and serve...
Domain Cont... Security Group ... All domain controllers in th...
Domain Guests Security Group ... All domain guests
Domain Users Security Group ... All domain users
Enterprise A... Security Group ... Designated administrators...
Enterprise R... Security Group ... Members of this group are...
Guest User Built-in account for guest ...
honey cool User
hopper User 123
hucker User xd
isabelle User xd
jipples User xd
kevl User xd
klaren User xd

ADUC and ADMC





ADUC использует

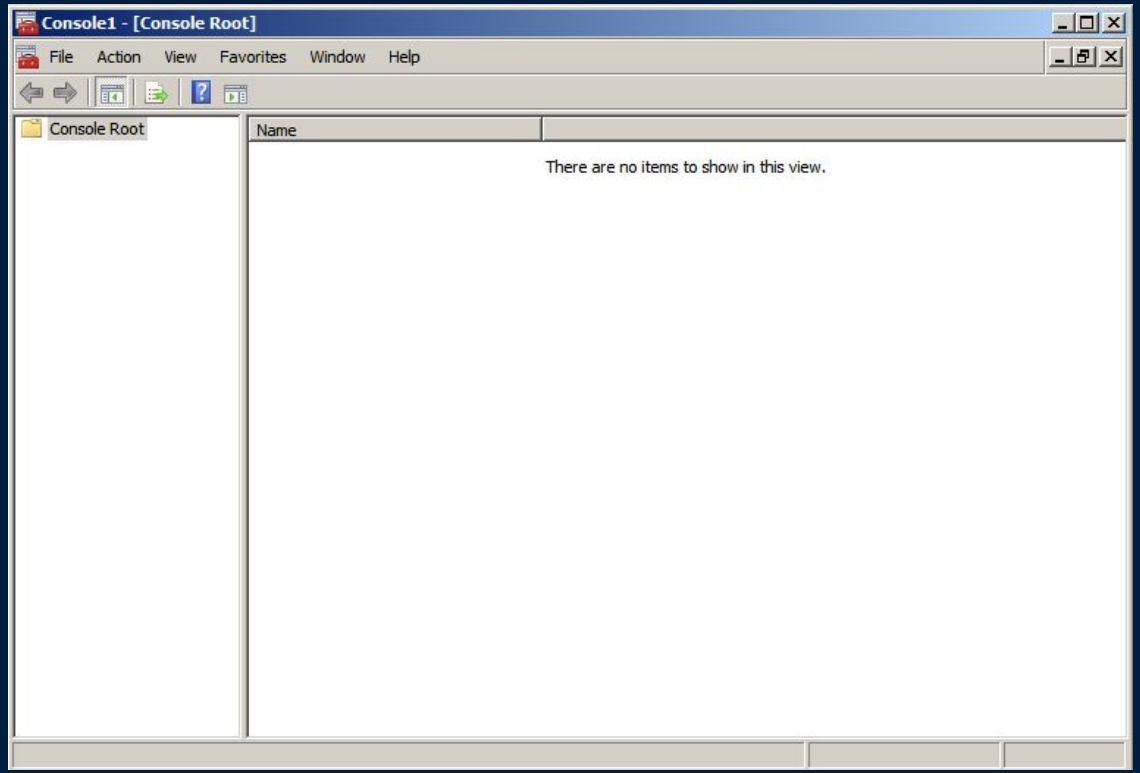
- MMC (Microsoft Management Console)
- ADSI (Active Directory Services Interface)
- Другие библиотеки Microsoft

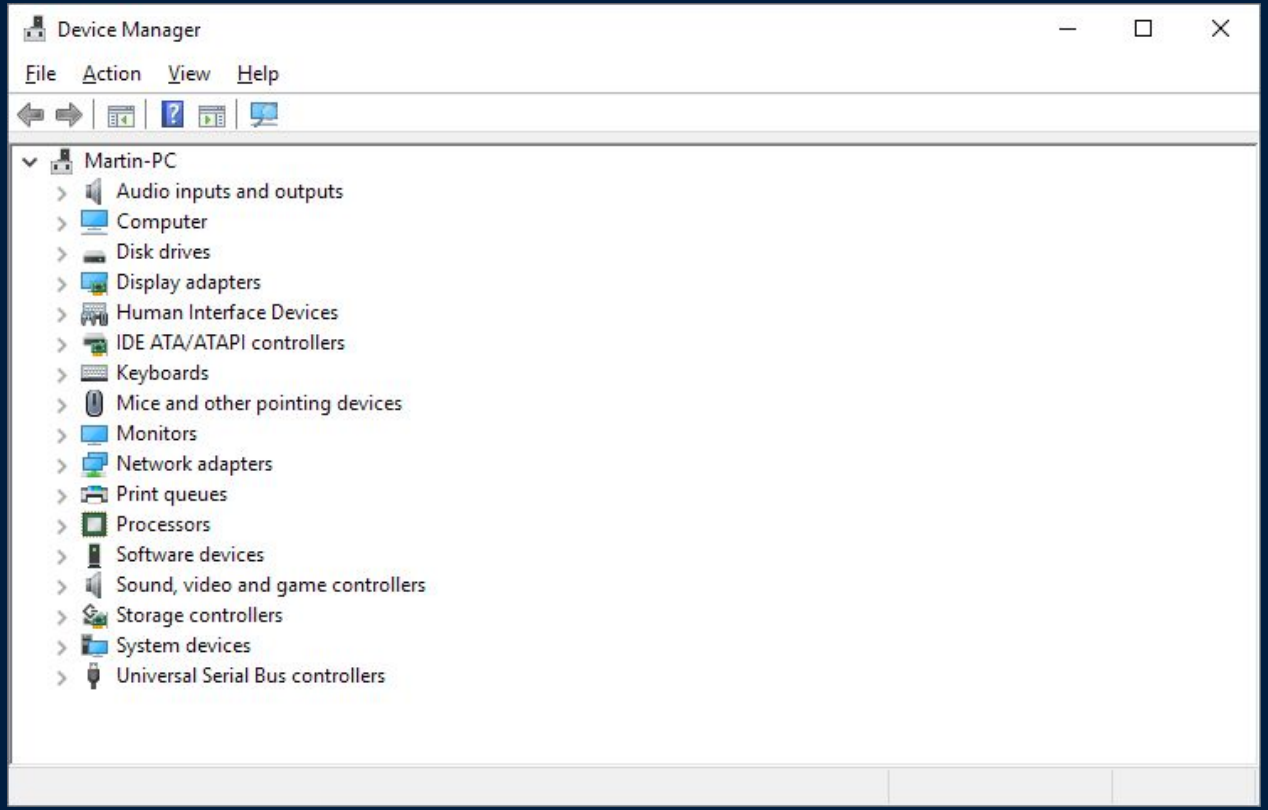
ADMC использует

- Qt
- OpenLDAP
- Samba
- Libkrb5
- И другие...

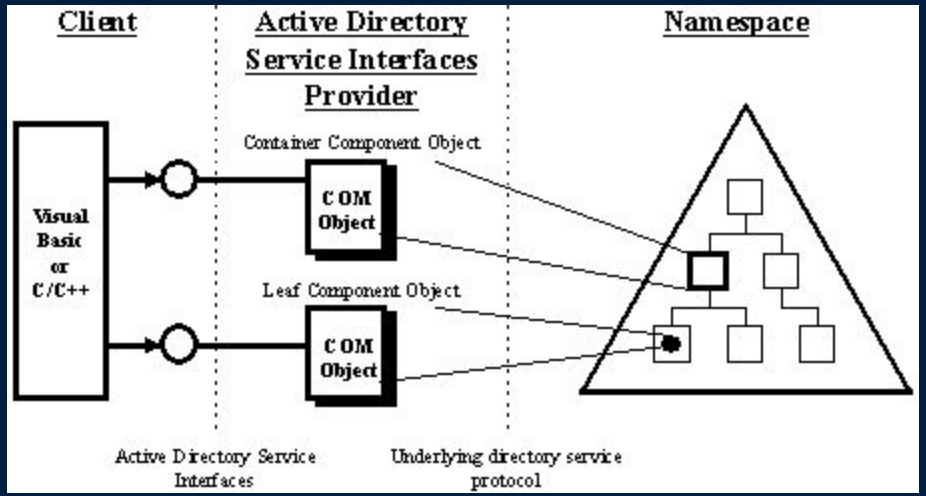
Переписываем MMC и ADSI

MMC - Microsoft Management Console

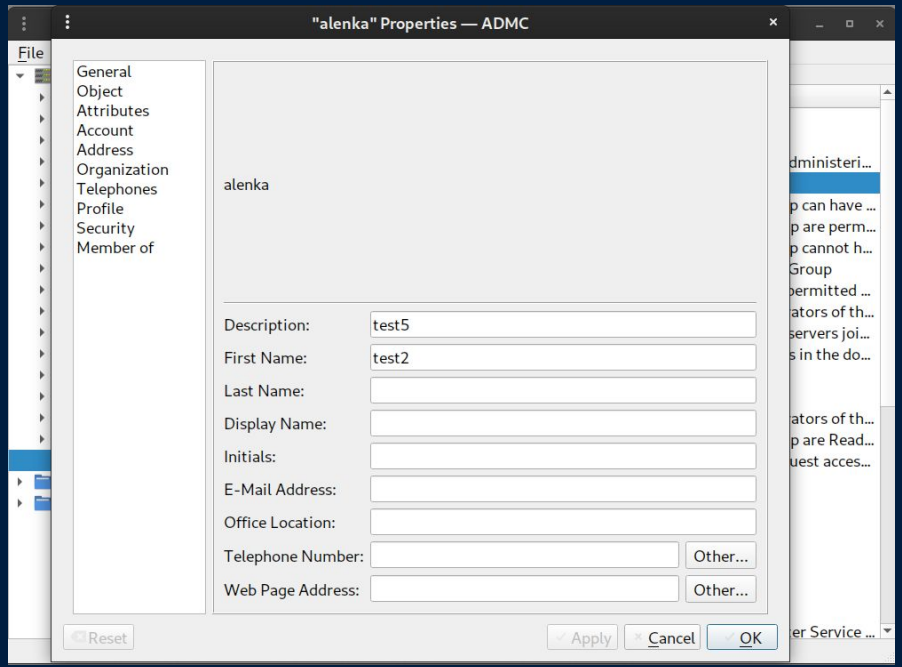


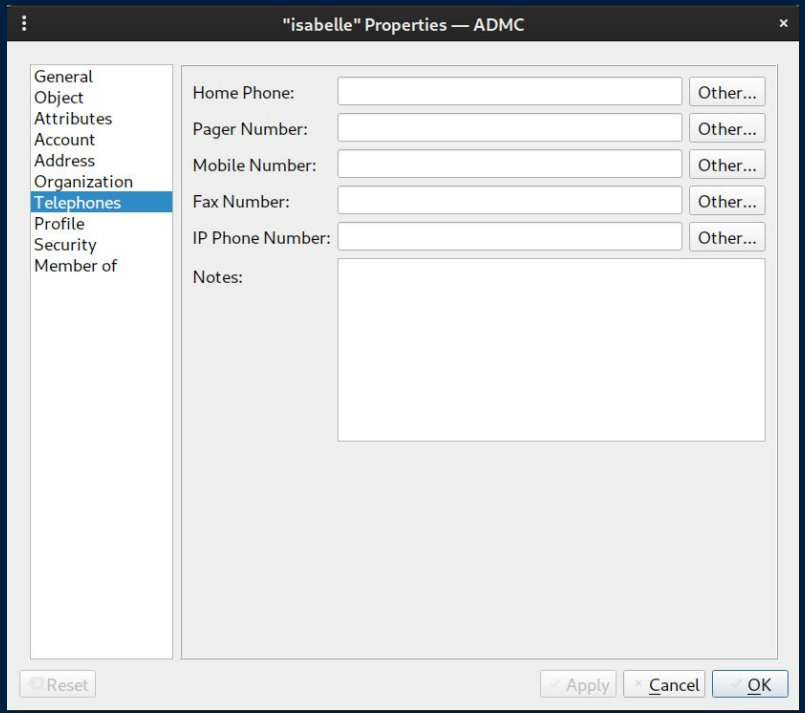

Device Manager
File
Action
View
Help
Martin-PC
Audio inputs and outputs
Computer
Disk drives
Display adapters
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Print queues
Processors
Software devices
Sound, video and game controllers
Storage controllers
System devices
Universal Serial Bus controllers

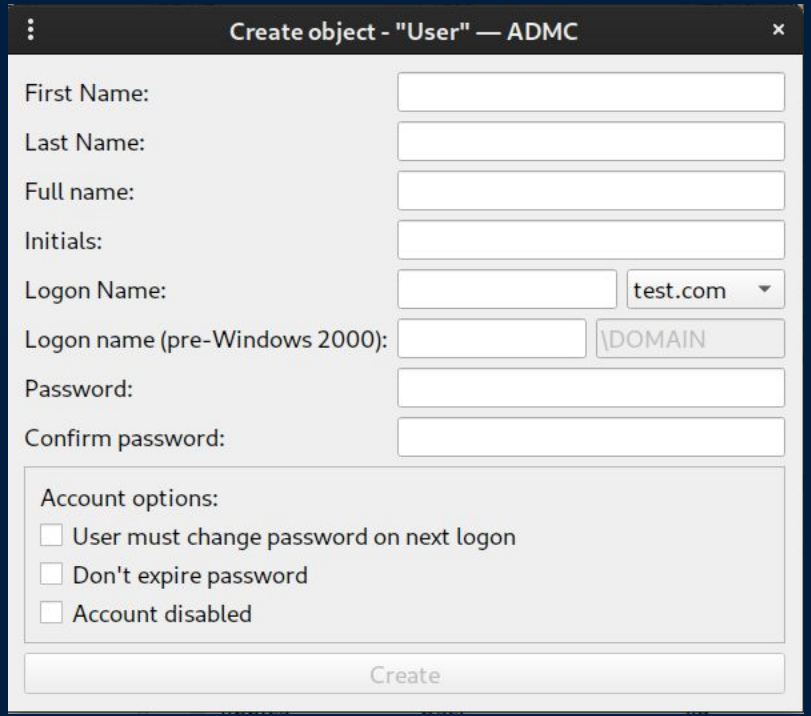
ADSI

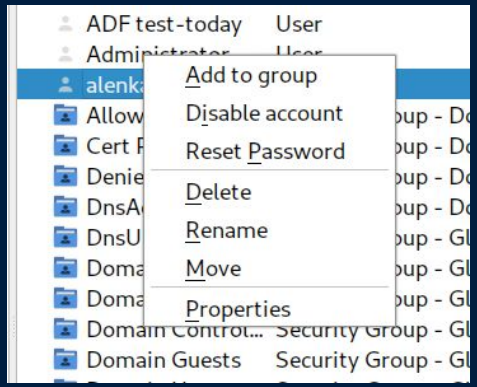

Client
Active Directory Service Interfaces Provider
Namespace
Container Component Object
COM Object
Visual Basic or C/C++
Leaf Component Object
COM Object
Active Directory Service Interfaces
Underlying directory service protocol

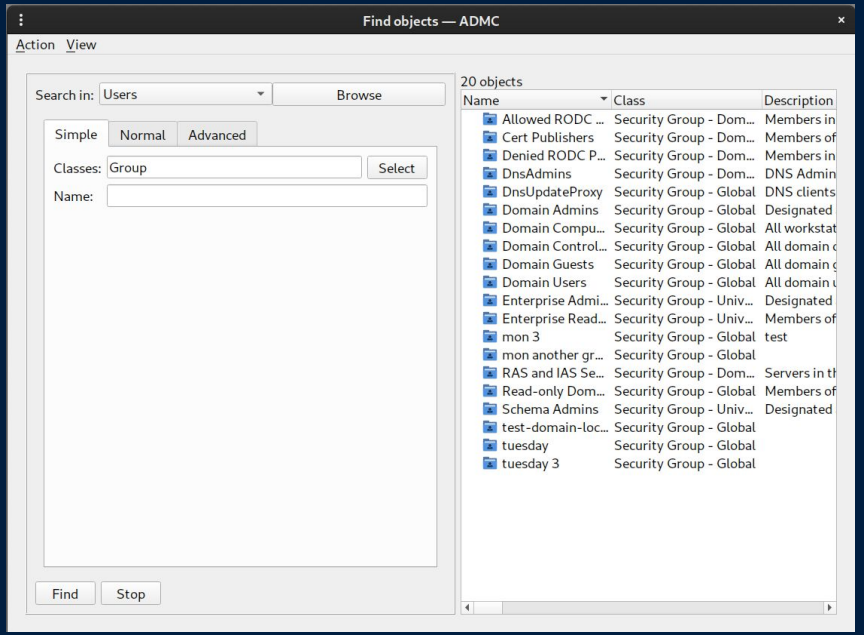
Немного скринов (WIP!)


"alenka" Properties — ADMC
File
General
Object
Attributes
Account
Address
Organization
Telephones
Profile
Security
Member of
alenka
Description: test5
First Name: test2
Last Name:
Display Name:
Initials:
E-Mail Address:
Office Location:
Telephone Number: Other...
Web Page Address: Other...
Reset
Apply
Cancel
OK


"isabelle" Properties — ADMC
General
Object
Attributes
Account
Address
Organization
Telephones
Profile
Security
Member of
Home Phone: Other...
Pager Number: Other...
Mobile Number: Other...
Fax Number: Other...
IP Phone Number: Other...
Notes:
Reset
Apply
Cancel
OK


Create object - "User" — ADMC
First Name:
Last Name:
Full name:
Initials:
Logon Name:
test.com
Logon name (pre-Windows 2000):
\DOMAIN
Password:
Confirm password:
Account options:
User must change password on next logon
Don't expire password
Account disabled
Create


ADF test-today User
Add to group
Disable account
Reset Password
Delete
Rename
Move
Properties
Domain Guests Security Group - Gl


Find objects — ADMC
Action View
Search in: Users
Browse
Simple
Normal
Advanced
Classes: Group
Select
Name:
Find
Stop
20 objects
Name
Class
Description
Allowed RODC ... Security Group - Dom... Members in
Cert Publishers Security Group - Dom... Members of
Denied RODC P... Security Group - Dom... Members in
DnsAdmins Security Group - Dom... DNS Admin
DnsUpdateProxy Security Group - Global DNS clients
Domain Admins Security Group - Global Designated
Domain Compu... Security Group - Global All workstat
Domain Control... Security Group - Global All domain
Domain Guests Security Group - Global All domain
Domain Users Security Group - Global All domain
Enterprise Admi... Security Group - Univ... Designated
Enterprise Read... Security Group - Univ... Members of
mon 3 Security Group - Global test
mon another gr... Security Group - Global
RAS and IAS Se... Security Group - Dom... Servers in th
Read-only Dom... Security Group - Global Members of
Schema Admins Security Group - Univ... Designated
test-domain-loc... Security Group - Global
tuesday Security Group - Global
tuesday 3 Security Group - Global

Будущее

- Дополнить функционал
- Тестирование
- Визуальный дизайн
- CLI альтернативное приложение
- ADMC на Windows (?)

Вопросы