Евгений Синельников

Управление деревом LDAP-объектов через интерфейс файловой системы — ADFS

План доклада

- Клиентские средства управления AD в Samba
  - samba-tool
  - ldapsearch/ldapmodify
  - ldbsearch/ldbmodify
- Задачи администрирования AD
  - Управление доменом с доверенных узлов
  - Применение групповых политик
- Unix way powershell для Active Directory

Клиентские средства Linux управления Active Directory (1)

- samba-tool
  - Работает локально от администратора
  - Не требует аутентификации в домене
  - Обращается к файлам базы ldb напрямую

```
[root@dc0 ~]# klist
klist: Credentials cache keyring 'persistent:0:0' not found
[root@dc0 ~]# samba-tool user list
ldb_wrap open of secrets.ldb
krbtgt
adgpotest
Guest
Administrator
[root@dc0 ~]#
```

Клиентские средства Linux управления Active Directory (2)

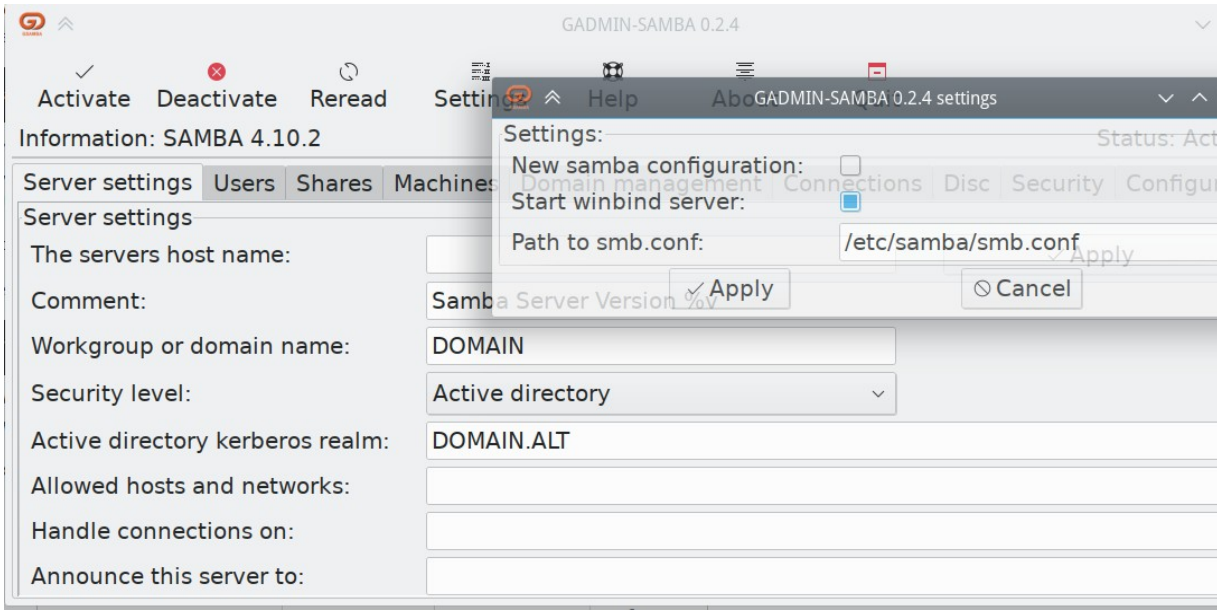
- Samba-tool из-под администратора
  - На рабочей станции работа не предусмотрена

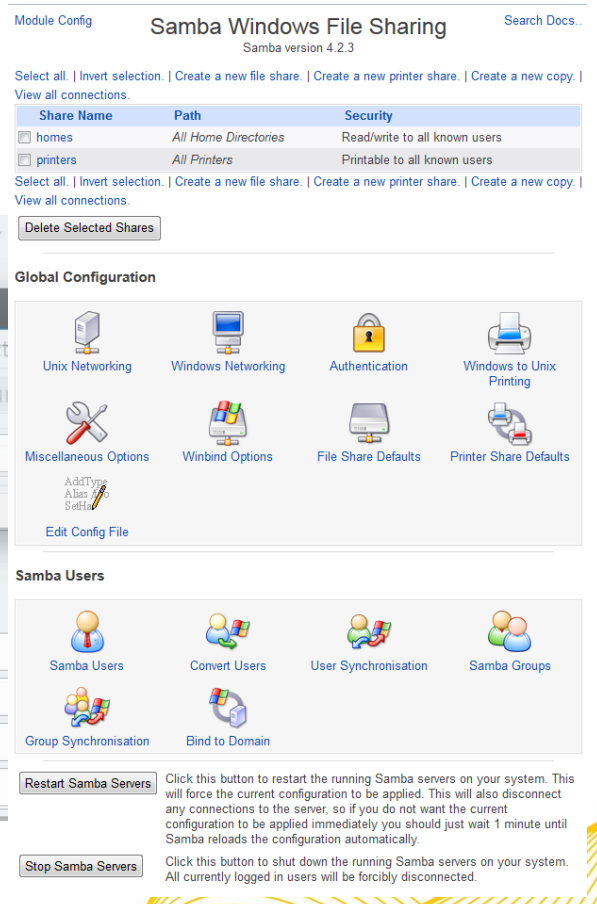
```
[root@clw0 ~]# samba-tool user list
ltdb: tdb(/var/lib/samba/private/sam.ldb): tdb_open_ex: could not open file /var/lib/samba/private/sam.ldb: No

Unable to open tdb '/var/lib/samba/private/sam.ldb': No such file or directory
Failed to connect to 'tdb:///var/lib/samba/private/sam.ldb' with backend 'tdb': Unable to open tdb '/var/lib/sa
ERROR(ldb): uncaught exception - Unable to open tdb '/var/lib/samba/private/sam.ldb': No such file or directory
  File "/usr/lib64/python3/site-packages/samba/netcmd/__init__.py", line 185, in _run
    return self.run(*args, **kwargs)
  File "/usr/lib64/python3/site-packages/samba/netcmd/user.py", line 535, in run
    credentials=creds, lp=lp)
  File "/usr/lib64/python3/site-packages/samba/samdb.py", line 67, in __init__
    options=options)
  File "/usr/lib64/python3/site-packages/samba/__init__.py", line 115, in __init__
    self.connect(url, flags, options)
  File "/usr/lib64/python3/site-packages/samba/samdb.py", line 82, in connect
    options=options)
[root@clw0 ~]#
```

Клиентские средства Linux управления Active Directory (3)

- Gadmin-samba / system-config-samba ?
- Webmin samba plugin ?

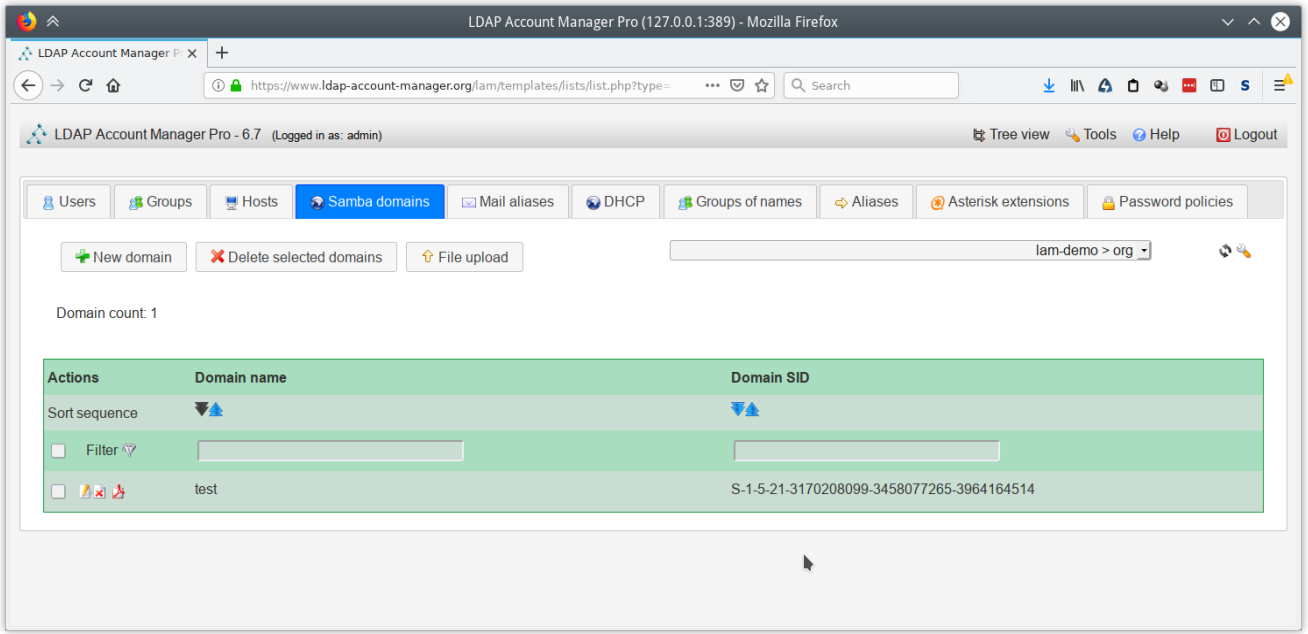




Клиентские средства управления Active Directory (4)

LDAP-браузеры?

- Web-клиенты (Lam, ...)
- Толстые клиенты (Apache Directory Studio, ...)



Родные инструменты администрирования (RSAT)

- Службы на уровне протоколов
  - LDAP (с аутентификацией через Kerberos)
  - DCE/RPC
  - …
  - WBEM + DCOM = WMI
  - WSMAN + SOAP = WinRM
- Службы на уровне приложений:
  - Оснастки под службы
    - Домен, Схема, Сайты, Групповые политики, …

Задачи администрирования Active Directory (минимум)

- Объекты управления доменом
  - Пользователи, Группы, Компьютеры, Контейнеры
  - Сайты, Зоны DNS, Сертификаты
  - Схема LDAP, FSMO-роли, …
- Инструменты управления конфигурациями
  - Групповые политики компьютеров
- Инструменты управления пользователями
  - Групповые политики пользователей

Архитектура инструментария управления AD под Linux

Инструменты управления для рабочей станции:

- fuse-приложение для LDAP:
  - **ADFS** (*Active Directory File System*) — backend
- Графическое приложение (на базе QT):
  - **ADMC** (*Active Directory Management Center*) — frontend
- fuse-приложение для GPO:
  - **GPOM** (*Group Policy Object Manager*) — backend
- Клиентские средства конфигурирования:
  - **oddjob_gpoapply** PAM-module — system backend
  - **Конфигуратор** на шине DBUS — system configurator

Unix way powershell для Active Directory (1)

Интерфейс ADFS:

$ kinit

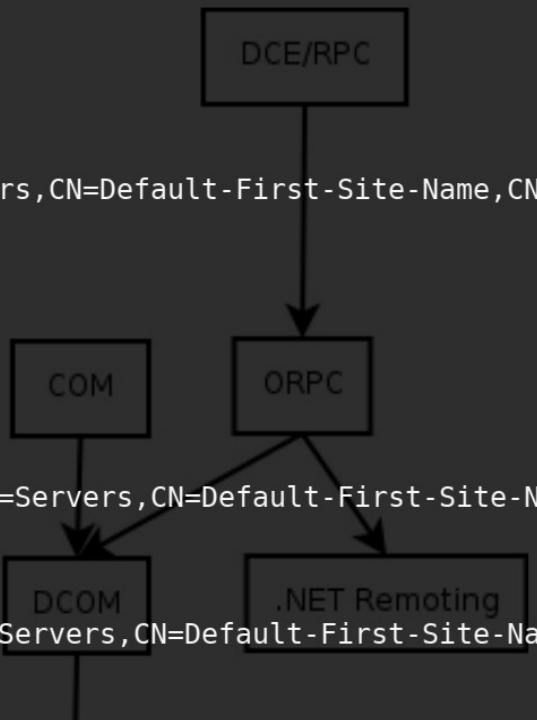
$ mount <mountpoint> <domain_controller>

```
[sin@xpi ~]$ ls /home/sin/work/samba/ui/hadfs/mnt
'CN=Builtin'                  'CN=Managed Service Accounts'  'OU=Allow'
'CN=Computers'                'CN=NTDS Quotas'               'OU=Allow Login'
'CN=Configuration'            'CN=Program Data'              'OU=Deny Login'
'CN=ForeignSecurityPrincipals' 'CN=Schema,CN=Configuration'  'OU=Domain Controllers'
'CN=Infrastructure'           'CN=System'
'CN=LostAndFound'             'CN=Users'
[sin@xpi ~]$ grep -i samba /home/sin/work/samba/ui/hadfs/mnt/.attributes
oEMInformation: Provisioned by SAMBA 4.9.4
```

Unix way powershell для Active Directory (2)

```
$ less mnt/.attributes
```

```
fSMORoleOwner: CN=NTDS Settings,CN=DC0,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=alt
forceLogoff: -9223372036854775808
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=domain,DC=alt;0]
instanceType: 5
isCriticalSystemObject: TRUE
lockOutObservationWindow: -18000000000
lockoutDuration: -18000000000
lockoutThreshold: 0
masteredBy: CN=NTDS Settings,CN=DC0,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=alt
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCount: 1
modifiedCountAtLastProm: 0
ms-DS-MachineAccountQuota: 10
msDS-AllUsersTrustQuota: 1000
msDS-Behavior-Version: 4
msDS-IsDomainFor: CN=NTDS Settings,CN=DC0,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=alt
msDS-NcType: 0
msDS-PerUserTrustQuota: 1
msDS-PerUserTrustTombstonesQuota: 10
msDs-masteredBy: CN=NTDS Settings,CN=DC0,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=alt
nTMixedDomain: 0
name: domain
nextRid: 1000
oEMInformation: Provisioned by SAMBA 4.9.4
```



- Windows Management Instrumentation
  - basically WBEM with DCOM as transport
  - Core Model, Common Model, Microsoft-specific model (CIMv2)

Unix way powershell для Active Directory (3)

```
$ echo -n 'Pa$$w0rd' >.chpwd
```

```
[sin@xpi hadfs]$ grep KnownObjects /home/sin/work/samba/ui/hadfs/mnt/.attributes | grep Users
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=domain,DC=alt
[sin@xpi hadfs]$ ls -a /home/sin/work/samba/ui/hadfs/mnt/CN\=Users/
 .attributes
 .attributes.json
'CN=Administrator'
'CN=Allowed RODC Password Replication Group'
'CN=Cert Publishers'
'CN=Denied RODC Password Replication Group'
'CN=DnsAdmins'
'CN=DnsUpdateProxy'
'CN=Domain Admins'
'CN=Domain Computers'
'CN=Domain Controllers'
'CN=Domain Guests'
'CN=Domain Users'
'CN=Enterprise Admins'
'CN=Enterprise Read-only Domain Controllers'
'CN=Group Policy Creator Owners'
'CN=Guest'
'CN=krbtgt'
'CN=RAS and IAS Servers'
'CN=Read-only Domain Controllers'
'CN=Schema Admins'
[sin@xpi hadfs]$ cd /home/sin/work/samba/ui/hadfs/mnt/CN\=Users/CN\=Administrator/
[sin@xpi CN=Administrator]$ ls -a
.attributes  .attributes.json  .chpwd
[sin@xpi CN=Administrator]$ echo -n 'Pa$$w0rd' >.chpwd
[sin@xpi CN=Administrator]$
```

Заключение

Active Directory File System (Haskell POC)

https://github.com/altlinuxteam/hadfs