



**Управление деревом LDAP-объектов
через интерфейс файловой системы —
ADFS**



- 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 ~]#
```

```
core team Samba
Failed to join domain: failed to join domain "DOMAIN.ALT" over rpc: None of the information to be transferred
Ждем задачу и утром сразу отправляем на тестирование:
#230473 BUILDING #6 [locked] [test-only] sisyphus samba_git=4.10.3-alt2
Еще один момент - почему join не работает через -k ?
[root@dc0 ~]# klist
Ticket cache: KEYSRING/persistent:0:0:000
Default principal: administrator@DOMAIN.ALT
Valid starting: Expires: Service principal
04.06.2019 09:28:42 04.06.2019 10:28:42 krbtgt@DOMAIN.ALT
```



Клиентские средства Linux управления Active Directory (2)

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

```
[root@clw0 ~]# samba-tool user list
ldb: 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 ?

GADMIN-SAMBA 0.2.4

Activate Deactivate Reread Settings Help AboGADMIN-SAMBA 0.2.4 settings

Information: SAMBA 4.10.2

Server settings Users Shares Machines

Server settings

The servers host name:

Comment:

Workgroup or domain name:

Security level:

Active directory kerberos realm:

Allowed hosts and networks:

Handle connections on:

Announce this server to:

Settings:

New samba configuration:

Start winbind server:

Path to smb.conf:

Apply Cancel

Module Config Samba Windows File Sharing Search Docs..

Samba version 4.2.3

Select all | Invert selection | Create a new file share. | Create a new printer share. | Create a new copy. | View all connections.

Share Name	Path	Security
<input type="checkbox"/> homes	All Home Directories	Read/write to all known users
<input type="checkbox"/> printers	All Printers	Printable to all known users

Select all | Invert selection | Create a new file share. | Create a new printer share. | Create a new copy. | View all connections.

Delete Selected Shares

Global Configuration

Unix Networking Windows Networking Authentication Windows to Unix Printing

Miscellaneous Options Winbind Options File Share Defaults Printer Share Defaults

Add New Alias Set Has Edit Config File

Samba Users

Samba Users Convert Users User Synchronisation Samba Groups

Group Synchronisation Bind to Domain

Restart Samba Servers Click this button to restart the running Samba servers on your system. This will force the current configuration to be applied. This will also disconnect any connections to the server, so if you do not want the current configuration to be applied immediately you should just wait 1 minute until Samba reloads the configuration automatically.

Stop Samba Servers Click this button to shut down the running Samba servers on your system. All currently logged in users will be forcibly disconnected.



Клиентские средства управления Active Directory (4)

LDAP-браузеры?

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

The screenshot shows the LDAP Account Manager Pro web interface in Mozilla Firefox. The browser address bar displays the URL: `https://www.ldap-account-manager.org/lam/templates/lists/list.php?type=`. The page title is "LDAP Account Manager Pro (127.0.0.1:389) - Mozilla Firefox". The interface includes a navigation menu with tabs for Users, Groups, Hosts, Samba domains (selected), Mail aliases, DHCP, Groups of names, Aliases, Asterisk extensions, and Password policies. Below the navigation menu, there are buttons for "New domain", "Delete selected domains", and "File upload". A search bar contains the text "lam-demo > org". The main content area shows "Domain count: 1" and a table with the following data:

Actions	Domain name	Domain SID
Sort sequence		
<input type="checkbox"/> Filter		
<input type="checkbox"/>	test	S-1-5-21-3170208099-3458077265-3964164514



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_groapply** 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=Computers'
'CN=Configuration'
'CN=ForeignSecurityPrincipals'
'CN=Infrastructure'
'CN=LostAndFound'
'CN=Managed Service Accounts'
'CN=NTDS Quotas'
'CN=Program Data'
'CN=Schema, CN=Configuration'
'CN=System'
'CN=Users'
'OU=Allow'
'OU=Allow Login'
'OU=Deny Login'
'OU=Domain Controllers'
```

```
[sin@xpi ~]$ grep -i samba /home/sin/work/samba/ui/hadfs/mnt/.attributes
oEMInformation: Provisioned by SAMBA 4.9.4
```

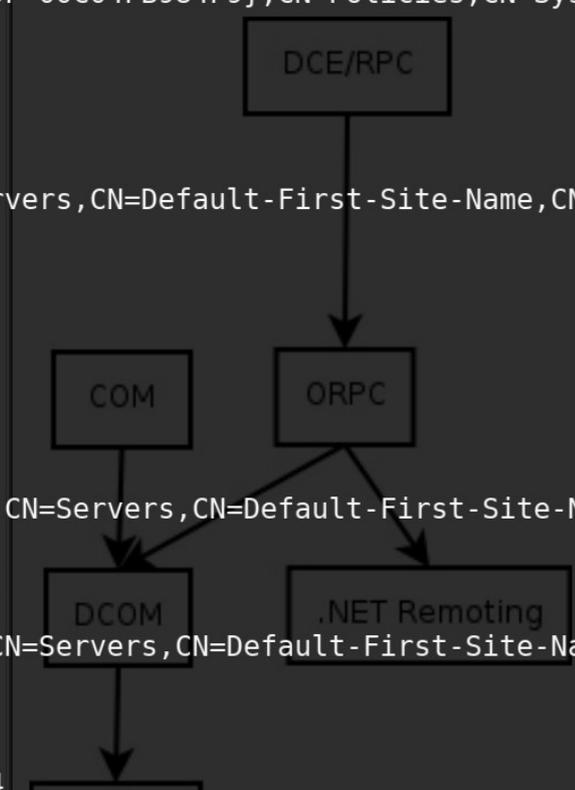


Unix way powershell для Active Directory (2)

```
$ 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]$ grep KnownObjects /home/sin/work/samba/ui/hadfs/mnt/.attributes
otherWellKnownObjects: B:32:1EB93889E404A4A4E0A0A0A0A0A0A0A0:CN=Managed Service Accounts,DC=domain,DC=alt
wellKnownObjects: B:32:09460C08AE1E4A4EA0A0A0A0A0A0A0A0:CN=Program Data,DC=domain,DC=alt
wellKnownObjects: B:32:18E2EA80684F11D2191A4B5C04D702BA:CN=Printers,DC=domain,DC=alt
wellKnownObjects: B:32:22B70C67D56E4EFB91A0A0A0A0A0A0A0:CN=Security Principals,DC=domain,DC=alt
wellKnownObjects: B:32:2FBAC1870ADE11D2191A4B5C04D702BA:CN=Infrastructure,DC=domain,DC=alt
wellKnownObjects: B:32:6227F0AF1FC2410D8E500A0A0A0A0A0A0:CN=Protected Administration,DC=domain,DC=alt
wellKnownObjects: B:32:A361B2FFFFD211D1A4B5C04D702BA:CN=System,DC=domain,DC=alt
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=domain,DC=alt
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=domain,DC=alt
wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=domain,DC=alt
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=ForestAndFound,DC=domain,DC=alt
[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]$
```



Заклучение

Active Directory File System (Haskell POC)

<https://github.com/altlinuxteam/hadfs>