Samba

Samba — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части. Является свободным программным обеспечением, выпущена под лицензией GPL.

https://www.samba.org/

Печать из Samba

Решение проблем

Примеры использования

- Миграция на LDAP
- Примеры структур Samba LDAP
- Выполнение программы входа в домен (Logon Script)

Сервер

Для доступа пользователей через winbind:

1. Установить

```
apt install\
    samba\
    smbldap-tools\
    winbind\
    libpam-winbind\
    libnss-winbind\
```

2. Выполнить настройку winbind
3. По необходимости выполнить настройку PAM

Решение проблемы increasing rlimit_max

Клиент

```
apt-get install samba smbclient winbind
```

Только работа с пользователями:

```
apt-get install winbind
```

Статус сервера

```
smbstatus
```

Статус сервера, включая список открытых файлов.

Перечитать настройки

```
smbcontrol all reload-config
```

Добавление в домен

```
net join -U ИМЯ_АДМИНИСТРАТОРА_ДОМЕНА
```

или

```
net rpc join -S КОНТРОЛЛЕР_ДОМЕНА -w ИМЯ_ДОМЕНА -U АДМИНИСТРАТОР_ДОМЕНА
```

Проверка:

```
net rpc testjoin
```

UNC

UNC path

```
smb://domain;user:password@server
smb://domain;user:password@server/share
```

Mac OS X Hints — Specify the domain in SMB login strings

winbind

Winbind – это демон, работающий на клиентах Samba и действующий как прокси для связи между PAM и NSS

Для работы через `winbind` нужно в NSS добавить: `winbind` в строки с `passwd:` и `group:` в файл `/etc/nsswitch.conf`

Пример:

```
passwd:     files winbind
group:      files winbind
```

---

winbindd (NSS daemon)

IDMAP

Fix Me!

idmap_ldap

Samba, GID, UID и AD — kurazhos blog

Exporting & Importing Winbind User Maps for Samba (for Backup & Restore of User maps) - infotinks

NTFS-ACLs

Подробнее о Списках доступа (POSIX ACL)

/etc/samba/smb.conf

```
vfs objects = acl_xattr
acl map full control = true
inherit acls = yes
map acl inherit = yes
nt acl support = yes
acl group control = true
```

Save NTFS-ACLs in Extended Attributes (EAs)

TDB

Chapter 41. Managing TDB Files

PAM

Debian: Работа с PAM



/etc/pam.d/common-account

```
account sufficient pam_winbind.so
account required pam_unix.so
```

/etc/pam.d/common-session

```
session sufficient pam_winbind.so
session required pam_unix.so
```

/etc/pam.d/common-password

```
password        [success=2 default=ignore]      pam_unix.so obscure sha512
password        [success=1 default=ignore]      pam_winbind.so use_authtok try_first_pass
password        requisite                       pam_deny.so
password        required                        pam_permit.so
```

Samba как NT4 PDC

Должен ли я перейти на Samba AD?

Одним из распространённых заблуждений является: «Samba 4» означает «только Active Directory»: Это неправильно!

Поддержка Active Directory (AD) Domain Controller (DC) является одним из усовершенствований, реализованных в

Samba 4.0. Однако все новые версии включают в себя функции предыдущих версий - в том числе поддержку NT4-style (classic). Это означает, что вы можете обновить Samba 3.x NT4-style PDC до последней версии, как вы обновили в прошлом - например, от 3.5.x до 3.6.x. Нет необходимости выполнять переход домена NT4-style на AD.

Кроме того, все последние версии продолжать поддерживать создание нового NT4-style PDC. Поддержка AD в Samba 4.0 и более поздних не является обязательным и не заменяет для функционал PDC. Команда Samba понимает трудности, представленные существующими структурами LDAP. По этой причине, у нас нет планов, чтобы удалить поддержку классического PDC. Кроме того, мы продолжаем тестировать поддержку PDC в новых версиях.

Перевод оригинала: Samba as NT4 Primary Domain Controller / Do I have to migrate to Samba AD?

Required Settings for Samba NT4 Domains - SambaWiki

Контроллер домена



Если в файле `smb.conf` указано `bind interfaces only = yes` то в параметре `interfaces` нужно указывать основной адрес сетевого интерфейса, а не его псевдоним (alias), подробнее о настройке сетевых интерфейсов здесь.

 Все ниже перечисленные примеры применимы только для ситуации когда данные контроллера домена хранятся на LDAP сервере OpenLDAP.
Для перехода на использование LDAP сервера в качестве хранилища данных читайте: **Миграция на Samba LDAP**

Папки:

```
/etc/samba
/etc/smbldap-tools
/var/cache/samba
/var/lib/samba
/var/log/samba
```

Установка

```
apt install\
    libpam-ldapd\
    libnss-ldapd\
    samba\
    samba-doc\
    smbclient\
    cifs-utils\
    smbldap-tools\
    slapd\
    mcrypt\
    ldap-utils\
    libgd-tools\
```

Решение проблемы increasing rlimit_max

Доступ к серверу LDAP

1. Пароль доступа к LDAP серверу, указывается для пользователя, который задан в переменной `ldap admin dn` файла `smb.conf`:

```
smbpasswd -w ПАРОЛЬ
```

Пароль пользователя, определённого в `ldap admin dn` сохраняется в файле `/var/lib/samba/private/secrets.tdb`

2. Также пароль нужно указать в файле `/etc/smbldap-tools/smbldap_bind.conf`

Для сохранения дампа файла и для контроля за его содержимым можно использовать команду:

```
tdbdump /var/lib/samba/private/secrets.tdb
```

Настройка Smbldap-tools

Подробное описание: Smbldap-tools

Файл `/etc/smbldap-tools/smbldap.conf`

LDAP

OpenLDAP

samba.ldif

Для того, чтобы работал поиск по содержимому атрибуту `sambaAcctFlags` нужно изменить схему `samba.schema` путем добавления строки `SUBSTR caseIgnoreIA5SubstringsMatch` в описание атрибута, вот что должно быть:

samba.schema

```
attributetype ( 1.3.6.1.4.1.7165.2.1.26 NAME 'sambaAcctFlags'
        DESC 'Account Flags'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{16} SINGLE-VALUE )
```

olcDbIndex_samba.ldif

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: sambaSID eq,sub
-
add: olcDbIndex
olcDbIndex: sambaPrimaryGroupSID eq
-
add: olcDbIndex
olcDbIndex: sambaDomainName eq
-
add: olcDbIndex
olcDbIndex: sambaSIDList eq
-
add: olcDbIndex
olcDbIndex: sambaGroupType eq
```

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/samba.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f olcDbIndex_samba.ldif
```

---

samba.schema

```
samba_4.5.16+dfsg-1_amd64.deb
deb://CONTENTS/usr/share/doc/samba/examples/LDAP/samba.schema.gz
```

sambaAcctFlags

Accounts

Within a Windows network (Domain) there are two types of accounts: machine and user accounts. The machine accounts are better kown as Computer accounts since they live in the ou=Computers. OpenLDAP uses objectClass=person and objectClass=device for this. Hence the choice for ou=Devices and ou=People in the DIT structure.

There are three ways that one can distinguish a machine account from a user account:

The object class A machine account ends with a $ e.g. computer01$ The account flags Accounts have passwords, so persons and devices can have a password associated with the account. SAMBA can work with LanManager passwords and NT passwords. LanManager should not be used anymore, so we will only provide LDIFs with the NT4 password field set.

In LDAP there is an sambaAcctFlags attribute which consists of a

```
[ 11 positions of information or spaces and a ]
```

A regular user account looks like this:

```
[U          ]
```

, while a machine account looks like this:

```
[W          ]
```

Next to an account type indicator one can also set account settings to for example disable an account. The available options are:

Account Flags (sambaAcctFlags)

Типы

U	Пользователь
W	Рабочая станция
S	Сервер (контроллер домена)
I	Domain Trust Account
M	Majority Node Set (MNS)

Параметры

H	Home directory required
N	Учетная запись не имеет пароля (поле паспорта LANMAN Password Hash или NT Password Hash игнорируется). Заметьте, пользователям будет позволен вход без пароля только если установлен параметр `null passwords = yes` в конфигурационном файле `smb.conf` в секции [global]
X	Пароль не имеет срока давности, т.е. не истечет
D	Учетная запись отключена
T	Temporary duplicate of other account
L	Учетная запись заблокирована автоматически

sambaPwdLastSet

Число секунд с начала 1970 (Unix time) когда били изменены значения атрибутов `sambaLMPassword` или `sambaNTPassword`

Преобразование в нормальную дату на bash:

```
date -d @1208428441 "+%Y-%m-%d %T"
```

sambaPwdCanChange

Пользователь не может изменить пароль (user cannot change password) если значение 2147483647 (The integer time in seconds since 1970)

sambaDomainName

gidNumber и uidNumber создаются автоматически

sambaNTPassword

Fix Me!

Пустой пароль	31D6CFE0D16AE931B73C59D7E0C089C0

sambaGroupType

Тип группы:

- 2 Domain group
- 4 Local group (alias)
- 5 Builtin

Дополнительные: Fix Me!

- 0 NONE
- 1 USER
- 2 DOM_GRP
- 3 DOMAIN
- 4 ALIAS
- 5 WKN_GRP
- 6 DELETED
- 7 INVALID
- 8 UNKNOWN
- 9 COMPUTER

Samba3/LDAP: Valid values for attribute sambaGroupType?

sambaUserWorkstations

Чтобы избежать ошибки NT_STATUS_INVALID_WORKSTATION при ограничении входа на машины с Samba нужно указывать их имена в списке с использованием префикса: «\\»
Пример:

```
\\server01,\\server02,win_server01,win_server02
```

Идентификаторы

Fix Me!

SID-ы, RID-ы, UID-ы и GID-ы

Where a Unix system only cares about uid numbers and gid numbers (the names are just to make it easier for humans), Windows systems only care about the SID or Security IDentifier. Since there is only one identifier it means there is a conflict with the uid and gid system. On unix systems root has uid 0 and gid 0, and the group is also called root. This is impossible in the Windows world. The SID has to be unique, meaning that the group and the user need to have a SID that is different from one another. Next to that no names can be used as duplicates. So there can not be a user root and a group root.

Before we add users and groups to LDAP, we first need to explain the SID and RID used in the Microsoft environment. SID stands for Security IDentifier. Within an Microsoft networking environment the SID is globally unique. In comparision with Unix-like systems, you could create a group with gid 99 and a user with uid 99, meaning that on a system level both have an ID of 99. This is not possible in a Microsoft world. It should also be noted that you can not have a group with name «test» and a user called «test». Also the naming has to be unique within your domain.

RID is a Relative IDentifier. Relative to the SID that is. The RID is the last part and should be unique for a certain object within a domain.

Структура SID

```
S-[Ревизия]-[IdentifierAuthority]-[SubAuthority0]-[SubAuthority1]-...-
[SubAuthority[SubAuthorityCount]](-RID)
```

Ревизия — для текущей версии Windows NT всегда 1.

Таблица Identifier Authorities и SubAuthorities:

SID	RID	Описание
S-1	0	NULL SID authority: used to hold the «null» account SID
S-1-0	0	The null account
S-1	1	World SID authority: used for the «Everyone» group, which is the only account in this authority.
S-1-1	0	The Everyone group (\EVERYONE)
S-1	2	Local SID authority: used for the «Local» group, which is the only account in this group.
S-1-2	0	The Local group
S-1	3	Creator SID authority: responsible for the CREATOR_OWNER, CREATOR_GROUP, CREATOR_OWNER_SERVER and CREATOR_GROUP_SERVER well known SIDs. These SIDs are used as placeholders in an access control list (ACL) and are replaced by the user, group, and machine SIDs of the security principal.
S-1-3	0	Creator Owner account (\CREATOR OWNER)
S-1-3	1	Creator Group account (\CREATOR GROUP)
S-1-3	2	Creator Owner Server account (\CREATOR SERVER OWNER)
S-1-3	3	Creator Group Server account (\CREATOR SERVER GROUP)
S-1	4	Non-unique authority: Not used by NT
S-1	5	NT authority: accounts that are managed by the NT security subsystem.
S-1-5	2	NT authority: Network (AUTHORITY\NETWORK)
S-1-5	4	NT authority: Interactive (AUTHORITY\INTERACTIVE)
S-1-5	11	NT authority: Authenicated users (AUTHORITY\AUTHENTICATED USERS)
S-1-5	18	NT authority: System (AUTHORITY\SYSTEM)
S-1-5	19	NT authority: Local service (AUTHORITY\LOCAL SERVICE)
S-1-5	20	NT authority: Network service (AUTHORITY\NETWORK SERVICE)
S-1-5	21	Non-unique SIDs, used for domain SIDs: The SID S-1-5-21 is followed by 3 RIDs (96 bytes) that defines the domain. Which could look like this S-1-5-21-0123456789-0123456789-0123456789. The 3 RIDs are created during initial domain installation. Since it is a random number duplicates can exist, there is no such thing as a central domain number authority. The domain SID is followed by a RID identifying the account within the domain. This RID is just a simple counter assigning a new RID to an account.
S-1-5	32	SID S-1-5-32 Builtin resources
S-1	9	Resource manager authority: is a catch-all that is used for 3rd party resource managers.

A unix system uses UIDs and GIDs for the identification of users and groups. Red Hat based systems use UIDs less then 500 for system users and groups. Debian based systems regard everything under 1000 to be system related. Exceptions to these rules are:

Имя	Тип	Debian	CentOS
nobody	пользователь	65534	99
nogroup	группа	65534	
nobody	группа		99
nfsnobody	пользователь		65534
nfsnobody	группа		65534

If you are in the lucky situation that you can start with a clean installation I would suggest the following:

- ID 000 - 499 : POSIX UID and GID numbers
- ID 500 - 999 : SAMBA and Windows RID numbers, with corresponding UID and GID numbers
- ID 1000 - up : free to use

an important note here is that Windows can not handle two identities with the same ID number. That means that every object in AD has a unique SID. While in the POSIX world we are used to uidNumber 0 for the root user and gidNumber 0 for the root group. This also brings forward another problem in the Windows world: two entries being called root, a user and a group. This is also not possible in the Windows world. Your name has to be unique too, even if the object is part of a different tree in the AD structure the name of the object (CN) has to be unique within your domain. If you would like to work with Personal User Groups on your POSIX systems, I would suggest using:

- User account: name - uidnumber
- Group naming: name_group - uidnumber+1

This means you need two numbers for every entry. But it gives you the benefit that you can use domainSID-uidNumber or domainSID-gidNumber as the SID for the object. But in the end this is only cosmetics.

UID, GID, SID and RID

SID S-1-5-21

Известные RID-ы:

RID	Название	Тип
500	DOMAINNAME\Administrator	User
501	DOMAINNAME\Guest	
512	DOMAINNAME\Domain Admins	Group
513	DOMAINNAME\Domain Users	
514	DOMAINNAME\Domain Guests	

SID S-1-5-32

Встроенные (Builtin resources):

RID	Название	Тип
544	BUILTIN\Administrators	Group
545	BUILTIN\Users	
546	BUILTIN\Groups	
548	BUILTIN\Account Operators	
549	BUILTIN\Server Operators	
550	BUILTIN\Print Operators	
551	BUILTIN\Backup Operators	
552	BUILTIN\Replicator	

Ссылки

- Samba
- Все о Samba
- Установка Samba PDC + LDAP на Debian Squeeze
- SAMBA LDAP Accounts (Or how to migrate to LDAP)
- Chapter 11. Account Information Databases, Part III. Advanced Configuration
- Домашняя страница Непорожнева Антона » Samba
- **Переводы официальной документации к samba, smbldap-tools, openldap**
- Русскоязычные статьи о Samba 4
- Debian Wiki: Samba Domain Controller
- How to create samba3 PDC with LDAP backend
- Samba 4 Active Directory domain controller (Русский)
- Установка Samba 3 PDC плюс LDAP на FreeBSD
- Логирование операций с файлами в Samba
- Сохранение удаленных файлов Samba в корзине
- Chapter 5. Backup Domain Control
- Setting up Samba4 as PDC and BDC
- Сбор и анализ логов samba в ELK Stack
- Логирование операций с файлами в Samba
- IBM: Официальное руководство и HOWTO по Samba 3.2.x: Основы настройки серверов
- **Chapter 41. Managing TDB Files**

Kerberos

- Samba, Active Directory & LDAP - SambaWiki
- Running a Samba AD DC with MIT Kerberos KDC - SambaWiki

http://sysadminmosaic.ru/samba/samba

2024-02-15 12:49

