Samba 3.2 による Solaris 10 の
ドメインコントローラー設定手順書

オープンソース・ソリューション・テクノロジ(株)

2008年11月7日

目次

1. はじめに

1.1 目的

本書は、Samba 3.2の ドメインコントローラー 機能を利用し、Solaris 10 を Windowsドメインコントローラーとして設定するための手順について説明します。

1.2 対象

本書は、以下の環境での構築を前提としています。

- Sun Solaris 10（SPARC、x86版）
- Samba 3.2.4(OSSTech製)

なお、Samba はオープンソース・ソリューション・テクノロジ(株)（以下、「OSSTech」）提供の製品パッケージを利用します。Solaris 10 には標準で Samba パッケージが含まれていますが、本書では対象としていません。

パッケージのインストール方法については、「OSSTech製 Samba 3.2インストールガイド」をご参照ください。

2. 構成パターン

本書では、プライマリ・ドメイン・コントローラー、バックアップ・ドメイン・コントローラーの2台のSambaサーバーの構築手順について説明します。

なおユーザー管理は、LDAPサーバー（OpenLDAP、SunJDS等）によって行われているものとし、LDAPサーバーの設定手順については省略します。

また、LDAPサーバーは、マスター、スレーブ構成とします。

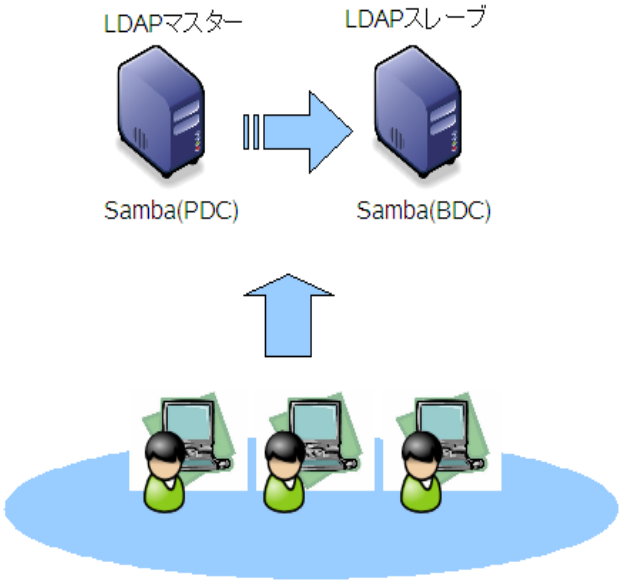

図 2.1.: Samba(PDC) + Samba(BDC)構成例

3. PDC の設定

3.1 /opt/osstech/etc/samba/smb.conf

まず最初に/opt/osstech/etc/samba/smb.conf を作成します。

雛形ファイルを本書の最終章に載せていますので、参照してください。

ユーザー環境に合わせて、次のパラメーターを変更してください。

パラメーター名	設定内容	設定例
workgroup	ドメイン名	workgroup = DOMAIN
passdb backend	ユーザー情報格納先	passdb backend = ldapsam:”ldap://127.0.0.1 ldap://192.168.1.2”
ldap admin dn	LDAP 管理者 DN	cn=Manager,dc=example,dc=jp
ldap suffix	LDAP suffix	dc=example,dc=jp
ldap user suffix	LDAP のユーザーアカウント格納先	ou=Users
ldap group suffix	LDAP のグループアカウント格納先	ou=Groups
ldap machine suffix	LDAP のマシンアカウント格納先	ou=Computers

更に Samba3.2 では必ず以下の設定を行ってください。

- global セクション

```
mangled names = no
vfs objects = notify_fam
```

(vfs objects = notify_fam は Solaris 10, CentOS 4, RHEL 4 のバージョン以前の OS を利用する場合に必要となります)

- 各セクション

各セクション（個々の共有）については、ファイルシステムが ZFS の領域、NFSv4 でマウントしている領域を共有する場合には以下の設定を行ってください。

```
vfs objects = notify_fam zfsacl
nfs4: mode = special
nfs4: chown = yes
nfs4: acedup = merge
```

3.2 /opt/osstech/etc/smbldap-tools/smbldap.conf

次に/opt/osstech/etc/smbldap-tools/smbldap.conf を設定します。

パラメーター名	設定内容	設定例
masterLDAP	LDAP マスター接続先	127.0.0.1
masterPort	LDAP マスター接続先ポート番号	389
slaveLDAP	LDAP スレーブ接続先	127.0.0.1
slavePort	LDAP スレーブ接続先ポート番号	389
SID	ドメイン SID	後述します
sambaDomain	Windows ドメイン名	DOMAIN
suffix	LDAP サフィックス	“dc=example,dc=jp”
usersdn	LDAP のユーザーアカウント格納先	“ou=Users,${suffix}”
groupsdn	LDAP のグループアカウント格納先	“ou=Groups,${suffix}”
computersdn	LDAP のマシンアカウント格納先	“ou=Computers,${suffix}”
sambaUnixIdPooldn	UID の割り当ての管理情報	“sambaDomainName=${sambaDomain},${suffix}”
userLoginShell	ユーザーのログインシェルのデフォルト値	“/bin/bash”
userHome	ユーザーのホームディレクトリ	“/home/%U”
userSmbHome	ユーザーに割り当てる WINDOWS の%USERSHARE%(必要な場合のみ)	“\\PDC\%U” など
userHomeDrive	ドメインログオン時、userSmbHome を、このドライブに割り当てます	“Z:”
userProfile	移動プロファイル利用時に、プロファイルを格納するパス名	“\\PDC\profiles\%U”
userScript	ログオンスクリプト名	logon.bat
mailDomain	ユーザーのメールアドレスのドメイン名	“example.jp”
OracleSES	OracleSES の利用の有無	“0” OracleSES 利用時は 1

smb.conf のドメイン名などの設定が完了していることを確認したのち、Windows ドメインに割り当てる SID 情報を取得するため、次のコマンドを実行します。

```
# /opt/osstech/bin/net getlocalsid
SID for domain PDC is : S-1-5-21-xxxxxx
```

表示されたSから始まる値が、このドメインに新しく割り当てられたSIDの値です。

このSIDの値を、smbldap.confのSIDパラメーターに設定します。

3.3 /opt/osstech/etc/smbldap-tools/smbldap_bind.conf

smbldap-toolsを利用する際に、LDAPにアクセスする識別名を設定します。

```
slaveDN=" cn=Manager,dc=example,dc=jp"
slavePw=" password"
masterDN=" cn=Manager,dc=example,dc=jp"
slavePw=" password"
```

LDAPマスター、LDAPスレーブにアクセスする際のLDAP管理者のDNとパスワードを設定します。

パスワードは平文で設定してください。

3.4 LDAP管理者をSambaに登録

SambaからLDAPにアクセスする際のLDAP管理者のパスワードを登録するために、次のコマンドを実行します。

```
# /opt/osstech/bin/smbpasswd -W
```

パスワード入力を求められますので、smb.confに指定した「ldap admin dn」のパスワードを入力します。

なおここで指定したLDAP管理者DNのパスワードを変更した場合、再度smbpasswdコマンドでパスワードを再設定する必要があります。

以上で、PDCの基本設定は完了です。

共有などは適時追加してください。

4. BDC の設定

4.1 /opt/osstech/etc/samba/smb.conf の設定

smb.conf のほとんどの設定は、PDC と共通です。

PDC と異なる設定が必要なのは、次のパラメーターです。

- passdb backend
  - 参照先をスレーブ LDAP、マスター LDAP の順番で設定します。
- os level
  - 32 に設定します。
- domain master
  - no に設定します。

以上の設定で smb.conf の設定は完了です。

4.2 /opt/osstech/etc/smbldap-tools/smbldap.conf の設定

smbldap.conf のほとんどの設定は PDC と共通です。

PDC と異なる設定が必要なのは、次のパラメーターです。

- masterLDAP
  - LDAP マスターの IP アドレスを設定します。このパラメーターには、データー更新可能な LDAP サーバーを指定しなければなりません。

4.3 /opt/osstech/etc/smbldap-tools/smbldap_bind.conf の設定

PDC と同じように、LDAP マスター、LDAP スレーブへアクセスする際の DN とパスワードを設定します。

4.4 LDAP 管理者パスワードの登録

PDC と同様に Samba から LDAP にアクセスする際の LDAP 管理者のパスワードを登録するために、次のコマンドを実行します。

```
# /opt/osstech/bin/smbpasswd -W
```

パスワード入力を求められますので、smb.conf に指定した「ldap admin dn」のパスワードを入力します。

4.5 ドメイン SID の登録

BDC 側では、PDC の「net getlocalsid」で取得したドメイン SID の値を、「net setlocalsid」コマンドで登録します。

```
# /opt/osstech/bin/net setlocalsid  S-1-5-21-254226858-1742755018-xxxxxxxxxx
```

5. 初期ユーザー登録

smbldap-tools を利用して、Windows ドメインで利用可能なユーザー、グループ情報の初期登録をすることができます。

```
# /opt/osstech/sbin/smbldap-populate -a Administrator -b Guest -k 998 -l 999 -m 512
```

各オプションは次の意味を表します。

- -a
  - Windows ドメイン管理者ユーザー名
- -b
  - Windows ドメインゲストユーザー名
- -k
  - Windows ドメイン管理者ユーザーの UID
- -l
  - Windows ドメインゲストユーザーの UID
- -m
  - マシンアカウントの GID

なお、本設定では、smb.conf に「admin users」として「Administrator」、「guest account」に「Guest」を設定しています。

smbldap-populate のオプションでユーザー名を変更する場合は、smb.conf の各パラメーターに設定するユーザー名も合わせて変更してください。

smbldap-populate が正常に完了したら、ユーザー情報、グループ情報が参照できるか getent passwd、getent group などで確認を行ってください。

6. 設定例

弊社が推奨する smb.conf ファイルの雛形を載せていますので、必要なパラメーターを追加して利用してください。

なおこの雛形は PDC 用のものですので、BDC では前述の変更点に従って変更を行ってください。

6.1 smb.conf

```
[global]
## Encoding
## ------------------------------------------------------------------------
dos charset = CP932
unix charset = UTF-8
display charset = UTF-8

## Identity
## ------------------------------------------------------------------------
workgroup = DOMAIN
netbios name = SAMBAPDC
server string = %L

## Network
## ------------------------------------------------------------------------
interfaces = 127.0.0.1 eth0
bind interfaces only = yes

deadtime = 10
keepalive = 300

## Logging
## ------------------------------------------------------------------------

log level = 1
log file = /var/log/samba/%m.log
max log size = 1000
debug hires timestamp = no
debug pid = yes
debug uid = yes

syslog = 0
utmp = yes

## Security
## ------------------------------------------------------------------------
security = user
domain logons = yes

guest account = Guest
```

```
map to guest = bad user

logon path =
logon home =
logon drive =
logon script =

## Password backend
## ------------------------------------------------------------------------

passdb backend = ldapsam:"ldap://127.0.0.1/ ldap://192.168.1.2"

ldap ssl = no
ldap admin dn = cn=Manager,dc=example,dc=jp
ldap passwd sync = yes
ldap delete dn = no
ldap suffix = dc=example,dc=jp
ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers

add user script = /opt/osstech/sbin/smbldap-useradd -m '%u'
rename user script = /opt/osstech/sbin/smbldap-usermod -r '%unew' '%uold'
delete user script = /opt/osstech/sbin/smbldap-userdel '%u'
set primary group script = /opt/osstech/sbin/smbldap-usermod -g '%g' '%u'
add group script = /opt/osstech/sbin/smbldap-groupadd -p '%g'
delete group script = /opt/osstech/sbin/smbldap-groupdel '%g'
add user to group script = /opt/osstech/sbin/smbldap-groupmod -m '%u' '%g'
delete user from group script = /opt/osstech/sbin/smbldap-groupmod -x '%u' '%g'
add machine script = /opt/osstech/sbin/smbldap-useradd -w '%u'

## Browser
## ------------------------------------------------------------------------

os level = 64
preferred master = auto
domain master = yes
local master = yes

## Misc global configuration
## ------------------------------------------------------------------------

wins support = yes
time server = yes
host msdfs = no
msdfs root = no
load printers = no

## Default configuration for each file/printer shares
## ========================================================================
```

```
admin users = Administrator
inherit permissions = yes
inherit acls = yes
map acl inherit = yes
store dos attributes = yes
ea support = yes

dos filemode = yes
dos filetimes = yes
dos filetime resolution = yes
fake directory create times = yes

vfs objects = notify_fam
mangled names = no
[NETLOGON]
## ============================================================================
## Logon script

available = no
path = /var/lib/samba/netlogon
comment = ログオンスクリプト
browseable = no
share modes = no
guest ok = yes
write list = Administrator

[PROFILES]
## ============================================================================
## Roaming profile

available = no

path = /var/lib/samba/profiles
comment = ユーザープロファイル
browseable = no
writeable = yes
create mask = 0611
directory mask = 0700
profile acls = yes
csc policy = disable
map system = yes
map hidden = yes

[C$]
## ============================================================================
## Shared storage

available = no
```

```
path = /share
comment = 共有領域ルートフォルダ
valid users = Administrator
writeable = yes
veto files = /lost+found/

[homes]
## ============================================================================
## User's home folders

available = no
browseable = no
#valid users = %S
invalid users = Administrator
guest ok = no
writeable = yes

[zfs-share]
path = /zfsshare
writeable = yes
vfs objects = notify_fam zfsacl
nfs4: mode = special
nfs4: chown = yes
nfs4: acedup = merge
```