Samba 3.2による Solaris 10 の Active Directory ドメイン認証統合設定手順書

オープンソース・ソリューション・テクノロジ(株)

2009年6月21日

目次

1. はじめに

1.1 目的

本書では、Samba 3.02 の winbind 機能を利用し、Solaris 10 を Active Directory（以下、「AD」）ドメインに参加させ、AD のユーザーとグループ情報を Solaris 10 から利用するための設定手順について解説する。

これにより、Solaris 側のユーザー管理コストを最小限にすることを目的とする。

1.2 対象

本書は、以下の環境において検証した結果に基づき解説を行っている。

- Microsoft Windows Server 2008
- Sun Solaris 10（SPARC 版 / x64 版）
- Samba 3.2.8（OSSTech 製）

なお、Samba 3.2 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する。 Solaris 10 標準の Samba パッケージは本書では対象としない。

2. 構成パターン

AD のユーザーとグループを UNIX 上で表現するには、UNIX 特有の属性（UID, GID, GECOS, ホームディレクトリ、シェル）を別途決定してやらなければならない。Samba の winbind 環境では、次の 3 パターンの構成が可能である。

- 全ての UNIX 属性を自動割り当てする構成
- UID と GID のみを自動割り当てする構成
- すべて手動割り当てする構成

以下に各方式における割り当てられる UNIX 属性値の違いと利点・欠点について述べる。なお、GECOS の値だけは方式による差はない。

2.1 全ての UNIX 属性を自動割り当てする構成

すべての UNIX 属性を定義済みの ID 範囲とテンプレートに従い自動的に割り当てる方式。この構成では AD 側での追加の作業が不要となる。ただし、特定のユーザーやグループに例外を設けることはできず、すべてのユーザー/グループに同一のテンプレートが適用される。

- 割り当て値
  - UID, GID の値
    - 予め Samba で設定した ID の範囲から自動的に割り当てられる。
  - ホームディレクトリ、シェルの値
    - 予め Samba で設定したテンプレートに従って割り当てられる。（テンプレートのデフォルト値はホームディレクトリが「/home/*NT ドメイン名*/*ユーザー名*」、シェルが「/bin/false」）
  - GECOS の値
    - AD 内のユーザーエントリの name 属性の値が用いられる。（Windows Server の「Active Directory ユーザーとコンピュータ」画面の「Users」ツリー以下にあるユーザーエントリの「名前」の欄の文字列）
- 利点
  - AD ドメインコントローラに SFU スキーマあるいは NIS（RFC 2307）スキーマを追加する必要がない。
  - AD のユーザーとグループに UNIX 属性を設定する必要がない。
  - Samba 側の実装が一番簡単であるため、不具合が発生する可能性が低いと思われる。
- 欠点
  - すべてのユーザー/グループに同一のテンプレートが適用される。つまり、特定のユーザー/グループに別のテンプレートを適用することはできない。

2.2 UID と GID のみを自動割り当てする構成

UID と GID 値だけを定義済みの ID 範囲から自動的に割り当て、それ以外の属性を AD 内のユーザー/グループエントリの UNIX 属性により決定する方式。ただし、UNIX 属性を持たないユーザーエントリは、定義済みのテンプレートに従い自動的に割り当てられる。

- 割り当て値
  - UID, GID の値
    - 予め Samba で設定した ID の範囲から自動的に割り当てられる。
  - ホームディレクトリ、シェルの値
    - AD 内のユーザーエントリの UNIX 属性が用いられる。
    - UNIX 属性を持たないユーザーは、予め Samba で設定したテンプレートに従って割り当てられる。
  - GECOS の値
    - AD 内のユーザーエントリの name 属性の値が用いられる。(Windows Server の「Active Directory ユーザーとコンピュータ」画面の「Users」ツリー以下にあるユーザーエントリの「名前」の欄の文字列)
- 利点
  - UID/GID 値以外であれば、ユーザーごとに個別に任意の属性値を設定することが可能。
  - ユーザーごとの個別の属性値の設定が必要になるまでは、AD ドメインコントローラへの SFU スキーマあるいは NIS (RFC 2307) スキーマの追加、および AD ユーザーの UNIX 属性の設定は必要とならない。
- 欠点
  - 運用開始後にスキーマを追加した場合、 winbindd プロセスを再起動する必要がある。

2.3 すべて手動割り当てする構成

すべての UNIX 属性を AD 内のユーザー/グループエントリの UNIX 属性により決定する方式。

- 割り当て値
  - UID, GID, ホームディレクトリ、シェルの値
    - AD 内のユーザー/グループエントリの UNIX 属性が用いられる。
    - ただしユーザーの UNIX 属性のプライマリグループ名 (GID) は無視され、AD ユーザー属性のプライマリグループ名が用いられる (ほかの構成と同じプライマリグループとなる)。
    - UNIX 属性を持たないユーザーとグループは無効になる。ログインできないだけでなく、ユーザー/グループ一覧にも含まれない。

- GECOS の値
  - AD 内のユーザーエントリの name 属性の値が用いられる。(Windows Server の「Active Directory ユーザーとコンピュータ」画面の「Users」ツリー以下にあるユーザーエントリの「名前」の欄の文字列)

- 利点
  - すべての属性において、ユーザー/グループごとに個別に任意の属性値を設定することが可能。
  - すべてのユーザー/グループ情報を AD ドメインコントローラで集中管理可能。
  - 任意のユーザー/グループを無効にすることが可能。
- 欠点
  - AD ドメインコントローラに SFU スキーマあるいは NIS (RFC 2307) スキーマを追加する必要がある。
  - 必要なすべてのユーザーとグループに UNIX 属性を設定する必要がある。

3. 設定手順

3.1 前提条件

本書では、以下の構成における設定例を示す。

- AD ドメイン構成
  - AD ドメイン名: EXAMPLE.JP
  - NT ドメイン名: EXAMPLE
- AD ドメインコントローラ（兼 AD 用 DNS サーバー）マシン
  - OS: Microsoft Windows Server 2008
  - ホスト名: ads.example.jp
  - IP アドレス: 10.0.0.1
  - 備考: Subsystem for Unix based Applications を追加導入済み（全 UNIX 属性を自動割り当てする場合は不要）
- Solaris 10 マシン
  - OS: Sun Solaris 10 (SPARC)
  - ホスト名: sol.example.jp
  - IP アドレス: 10.0.0.16
- Samba パッケージ
  - バージョン: 3.2.8
  - 備考: OSSTech 製品パッケージ

3.2 既存設定ファイルのバックアップ

何かしらの理由で winbind 環境以前の状態に戻す必要がある場合、以下のファイルを適宜バックアップしておく。

- /etc/hosts（/etc/inet/hosts）
- /etc/resolv.conf
- /etc/nsswitch.conf
- /etc/pam.conf

3.3 Samba と関連パッケージのインストール

Samba パッケージと依存する関連パッケージを Solaris 10 にインストールする。 インストール手順については、「OSSTech Samba 3.2 インストールガイド」を参照のこと

3.4 DNS の設定

Samba ホストを AD ドメインに参加させるには、AD ドメインコントローラのサービス名とホスト名を解決できること、そして自ホストの完全なホスト名（FQDN）を解決できる必要がある。そのためには /etc/hosts ファイルか /etc/resolv.conf ファイルを適切に設定しなければならない。

3.4.1 /etc/hosts による設定

以下のいずれかに該当する場合、/etc/hosts による設定が推奨される。

- AD のドメイン名と DNS のドメイン名が異なる場合。
- AD と DNS でドメイン名は一致しているが、各々用に権威 DNS サーバーを分けている場合。
- 権威 DNS サーバーに AD ドメインコントローラのホスト名とサービス名と IP アドレス、Samba（winbind）ホストの名前と IP アドレス（逆引き含む）が**登録されていない場合。**

このようなときは、/etc/hosts に自ホストと AD ドメインコントローラの IP アドレスと FQDN を記述することで名前解決できるようにする。

/etc/hosts に Solaris 10 と AD ドメインコントローラのホスト名と IP アドレスを記述

```
127.0.0.1       localhost
10.0.0.16       sol.example.jp  sol     loghost
10.0.0.1        ads.example.jp  ads
```

AD ドメインコントローラが複数ある場合は、その数だけ「*IP アドレス ホスト名*」行を記述する。

3.4.2 /etc/resolve.conf による設定

前述の /etc/hosts による設定を推奨する場面に該当しない場合、特に AD ドメインコントローラが DNS サーバーを兼任しており、同名の DNS ドメインの権威サーバーにもなっている場合は、/etc/resolv.conf による設定が推奨される。次のように、AD ドメインコントローラ（兼 DNS サーバー）の IP アドレスを一番上の nameserver 行として記述する。

/etc/resolve.conf に AD の DNS サーバーを設定（抜粋）

```
nameserver 10.0.0.1
nameserver そのほかの DNS キャッシュサーバー
...
```

AD ドメインコントローラ（兼 DNS サーバー）が複数ある場合は、その数だけ「nameserve *IP アドレス*」行を記述する。

3.5 Kerberos クライアントの設定

AD ドメインは認証基盤として Kerberos を採用しているため、AD ドメインメンバーとする Samba ホストに Kerberos クライアントの設定が必要となる。

3.5.1 時刻の同期

Kerberos を利用するにはクライアントとサーバーの時刻が同期している必要がある。時刻のずれが大きいと Kerberos の認証は失敗してしまう。通常、AD ドメインコントローラは NTP サーバーとしても機能するため、これを利用するのが一番手軽である。以下の手順は、AD ドメインコントローラが NTP サーバーとして適切に設定されていることを前提とする。

最初に ntpdate コマンドを利用して時刻を同期する。NTP サーバーとの時刻のずれが 0.5 秒以上の場合、ntpdate は一瞬で時刻を進めるか戻すことで時刻調整を行なう。このため、以下のコマンドラインはシングルユーザーモードで実行することが望ましい。

ntpdate による時刻の同期

```
# ntpdate 10.0.0.1
 8 Mar 16:37:02 ntpdate[22366]: adjust time server 10.0.0.1 offset 0.000067 sec
```

/etc/inet/ntp.conf を作成し、server 行に AD ドメインコントローラの IP アドレスを記述する。

/etc/inet/ntp.conf に NTP サーバーを設定

```
server 10.0.0.1
```

ntpd を起動する。

ntpd の起動

```
# svcadm enable ntp
```

3.5.2 /opt/osstech/etc/krb5.conf の設定

Samba ホストの Kerberos レルム名と KDC（AD ドメインコントローラ）のホスト名を記述する。OSSTech 製 Samba 3.2 パッケージは Solaris 10 付属の Kerberos ではなく、同じく OSSTech 製の Kerberos パッケージを利用するため、/etc/krb5.conf や /etc/krb5/krb5.conf ではなく /opt/osstech/etc/krb5.conf を設定しなければならない。

/etc/osstech/etc/krb5.conf に Kerberos レルム名と KDC を設定

```
[libdefaults]
default_realm = EXAMPLE.JP
[realms]
EXAMPLE.JP = {
    kdc = ads.example.jp
}
[domain_realms]
example.jp = EXAMPLE.JP
.example.jp = EXAMPLE.JP
```

AD ドメインコントローラが複数ある場合は、[realm] セクションの EXAMPLE.COM = {...} 内にその数だけ「kdc = *ホスト名*」行を記述する。

3.5.3 Kerberos クライアントの動作確認

Kerberos クラアイアントの設定が正しいことを確認するため、kinit で Kerberos チケットの取得実験を行なう。次の例は AD 内のユーザー administrator で試行しているが、それ以外の有効な AD ユーザーで確認してもよい。

Kerberos クライアントの動作確認

```
# /opt/osstech/bin/kinit administrator@EXAMPLE.JP
Password for administrator@EXAMPLE.JP: Administrator のパスワードを入力
```

kinit に成功すると、表示はなにもなく終了し、Kerberos チケットが発行される。Kerberos チケットを確認するには klist コマンドを利用する。

Kerberos チケットの確認

```
# /opt/osstech/bin/klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EXAMPLE.JP
```

```
Valid starting     Expires            Service principal
02/20/09 10:55:56  02/20/09 20:56:33  krbtgt/EXAMPLE.JP@EXAMPLE.JP
        renew until 02/21/09 10:55:56


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

3.6 Samba の設定

Samba を設定し、AD ドメインメンバーとする。

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

smb.conf に Samba を AD ドメインメンバーとするための設定を記述する。

構成パターンにより、idmap backend パラメータと winbind nss info パラメータの値を次のように調整する。

- 全ての UNIX 属性を自動割り当てする構成

```
idmap domains = BUILTIN  EXAMPLE
idmap config BUILTIN:backend = rid
idmap config BUILTIN:range = 1000 - 1999
idmap config EXAMPLE:backend = rid
idmap config EXAMPLE:range= 2000 - 60000
```

- UID と GID のみを自動割り当てする構成

```
idmap domains = BUILTIN EXAMPLE
idmap config BUILTIN:backend=rid
idmap config BUILTIN:range = 1000 - 1999
idmap config EXAMPLE:backend=rid
idmap config EXAMPLE:range = 2000 - 60000
winbind nss info = sfu
```

- すべて手動割り当てする構成

```
idmap domains = EXAMPLE
idmap config EXAMPLE:backend=ad
idmap config EXAMPLE:range = 2000 - 60000
winbind nss info = sfu
```

UID と GID のみを自動割り当てする構成の場合、次のようになる。

/etc/samba/smb.conf の基本設定と AD ドメインメンバー設定

```
[global]
unix charset = UTF-8
```

```
display charset = UTF-8
dos charset = CP932
security = ADS
workgroup = EXAMPLE
realm = EXAMPLE.JP
password server = ads.example.jp

winbind use default domain = yes
winbind enum users = yes
winbind enum groups = yes
winbind separator = _
winbind nested groups = no
idmap uid = 1000-100000
idmap gid = 1000-100000
template homedir = /home/%D/%U
template shell = /bin/sh
allow trusted domains = no

## Conf1: Full auto
idmap domains = BUILTIN  EXAMPLE
idmap config BUILTIN:backend = rid
idmap config BUILTIN:range = 1000 - 1999
idmap config EXAMPLE:backend = rid
idmap config EXAMPLE:range= 2000 - 60000
winbind nss info = template

## Conf2: UID/GID only (SFU or SUA required on AD to use customized UNIX attrs)
# idmap domains = BUILTIN EXAMPLE
# idmap config BUILTIN:backend=rid
# idmap config BUILTIN:range = 1000 - 1999
# idmap config EXAMPLE:backend=rid
# idmap config EXAMPLE:range = 2000 - 60000
# winbind nss info = sfu

## Conf3: Full manual (SFU or SUA and UNIX attrs required on AD)
# idmap domains = EXAMPLE
# idmap config EXAMPLE:backend=ad
# idmap config EXAMPLE:range = 2000 - 60000
# winbind nss info = sfu
```

AD ドメインコントローラが複数ある場合は、[global] セクションの password server パラメータに空白文字で区切って列挙する。

3.6.2 /opt/osstech/etc/samba/smb.conf の設定内容のテスト

Samba の testparm コマンドを利用して smb.conf に無効な設定パラメーター名が記述されていないこと、Samba サーバーの役割りがドメインメンバー（ROLE_DOMAIN_MEMBER）となることを確認する。

smb.conf のテスト

```
# /opt/osstech/bin/testparm -s
Load smb config files from /opt/osstech/etc/samba/smb.conf
```

```
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
デフォルトと異なる値が設定されているパラメータが表示される
```

3.6.3 AD ドメインへの参加

Samba の net コマンドのサブコマンドを利用して AD ドメインへ参加する。

AD ドメインへの参加

```
# /opt/osstech/bin/net ads join -Uadministrator
administrator's password: Administrator のパスワードを入力

Using short domain name -- EXAMPLE
Joined 'SOL' to realm 'EXAMPLE.JP'
```

3.6.4 AD ドメインへの参加の確認

Samba の net コマンドのサブコマンドを利用して AD ドメインメンバーになれたことを確認する。

AD ドメインメンバーの動作確認

```
# /opt/osstech/bin/net ads testjoin
Join is OK
# /opt/osstech/bin/net ads info
LDAP server: 10.0.0.1
LDAP server name: ads.example.jp
Realm: EXAMPLE.JP
Bind Path: dc=EXAMPLE,dc=JP
LDAP port: 389
Server time: AD ドメインコントローラの時刻
KDC server: 10.0.0.1
Server time offset: AD ドメインコントローラと Samba サーバーの時刻の差
```

3.6.5 winbindd の起動

Samba の winbind 機能はデーモンプログラム winbindd により実装されている。winbindd を起動するには Samba パッケージ付属の init スクリプトを利用する。

winbindd の起動

```
# /opt/osstech/sbin/service osstech-winbind start
```

OS のブートとシャットダウンで winbindd を自動的に起動・停止させるために、/etc/rc?.d 以下に init スクリプトへのシンボリンクリンクを作成する。

winbindd を自動起動/停止させるための設定

```
# /opt/osstech/sbin/chkconfig osstech-winbind on      （自動起動を有効にする）
# /opt/osstech/sbin/chkconfig osstech-winbind off     （自動起動を無効にする）
```

3.6.6 winbindd の動作確認

Samba の wbinfo コマンドを利用して winbindd の動作確認を行なう。

AD ドメインメンバーのマシン信頼アカウントの確認

```
# /opt/osstech/bin/wbinfo -t
checking the trust secret via RPC calls succeeded
```

AD ドメインユーザーとグループの一覧表示の確認

（表示は AD に登録されている情報や smb.conf の設定により多少異なる）

```
# /opt/osstech/bin/wbinfo -u
administrator
guest
krbtgt
# /opt/osstech/bin/wbinfo -g
domain computers
domain controllers
schema admins
enterprise admins
domain admins
domain users
domain guests
group policy creator owners
```

AD ユーザーの UNIX 属性の確認

（表示は AD に登録されている情報や smb.conf の設定により多少異なる）

```
# /opt/osstech/bin/wbinfo -i administrator
administrator:*:2500:2513:Administrator:/home/EXAMPLE/administrator:/bin/false
```

AD ユーザーの認証の実験

```
# /opt/osstech/bin/wbinfo  -a  administrator%Administrator のパスワード
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

3.7 NSS の設定

NSS（Name Service Switch）を設定し、winbind が提供する AD ユーザー/グループ情報を利用できるようにする。NSS には Samba 3.2 付属の nss_winbind モジュールを利用する。

3.7.1 nscd の無効化

winbind 自身に AD ユーザー情報のキャッシュ機能があるため、nscd（name service cache daemon）の利用を推奨しない。逆に nscd を利用していると AD 側の更新内容が UNIX 側で参照できない問題が発生するので、nscd を無効化する。

nscd の無効化

```
# svcadm disable name-service-cache
```

3.7.2 /etc/nssswitch.conf の設定

ユーザー情報（passwd）とグループ情報（group）において nss_winbind_osstech を利用するように設定する。

/etc/nsswitch.conf（抜粋）

```
passwd: files winbind_osstech
group: files winbind_osstech
```

3.7.3 NSS の動作確認

getent コマンドや id コマンドを利用して、NSS が winbind 経由で AD のユーザー/グループ情報を参照できることを確認する。

ユーザーの一覧に AD のユーザー一覧が含まれていることを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# getent passwd
…AD 以外のユーザー一覧…
administrator:*:2500:2513:Administrator:/home/EXAMPLE/administrator:/bin/false
guest:*:2501:2514:Guest:/home/EXAMPLE/guest:/bin/false
krbtgt:*:2502:2513:krbtgt:/home/EXAMPLE/krbtgt:/bin/false
```

ユーザー名から AD のユーザー情報を得られることを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# getent passwd administrator
administrator:*:2500:2513:Administrator:/home/EXAMPLE/administrator:/bin/false
```

ユーザー ID から AD のユーザー情報を得られることを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# getent passwd 2500
administrator:*:2500:2513:Administrator:/home/EXAMPLE/administrator:/bin/false
```

グループの一覧に AD のグループ一覧が含まれていることを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# getent group
…AD 以外のグループ一覧…
domain computers:*:2515:
domain controllers:*:2516:
schema admins:*:2518:administrator
enterprise admins:*:2519:administrator
domain admins:*:2512:administrator
domain users:*:2513:
domain guests:*:2514:
group policy creator owners:*:2520:administrator
dnsupdateproxy:*:3102:
```

グループ名から AD のグループ情報が得られることを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# getent group "domain users"
domain users:*:2513:
```

グループ ID から AD のグループ情報が得られることを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# getent group 2513
domain users:*:2513:
```

AD ユーザーのプライマリグループ、セカンダリグループが正しいことを確認

(表示は AD に登録されている情報や smb.conf の設定により多少異なる)

```
# id -a administrator
```

```
uid=2500(administrator) gid=2513(domain users) groups=2518(schema admins),2519(enterprise
admins),2512(domain admins),2520(group policy creator owners)
```

3.8 PAM の設定

PAM (Pluggable Authentication Module) を設定し、winbind が提供する AD ユーザーの認証機能を利用できるようにする。PAM には pam_winbind モジュールを利用する。

3.8.1 /etc/pam.conf の設定

ユーザー認証で pam_winbind_osstech を利用するように設定する。以下のように、モジュールタイプが「auth」でモジュールが「pam_authtok_get.so.1」の行の直後に pam_winbind_osstech.so.1 の行を追加する。以下の例はサービス「login」で winbind 認証を利用するための設定例となるが、**ほかのサービスでも winbind 認証を利用する場合は、各サービスごとに pam_winbind_osstech の設定が必要**となる。

/etc/pam.conf による winbind 認証の設定（抜粋）

```
login   auth requisite          pam_authtok_get.so.1
login   auth sufficient         pam_winbind_osstech.so.1 use_first_pass
login   auth required           pam_dhkeys.so.1
login   auth required           pam_unix_cred.so.1
login   auth required           pam_unix_auth.so.1
login   auth required           pam_dial_auth.so.1
```

ユーザーアカウント確認で pam_winbind を利用するように設定する。以下のように、モジュールタイプが「account」でモジュールが「pam_unix_account.so.1」の行の直前に pam_winbind.so.1 の行を追加する。以下の例はサービス「other」（デフォルト用サービス名）で winbind アカウント確認を利用するための設定例となるが、ほかのサービスでも winbind アカウント確認を利用する場合は、各サービスごとに pam_winbind の設定が必要となる。

/etc/pam.conf による winbind アカウント確認の設定（抜粋）

```
other   account requisite       pam_roles.so.1
other   account sufficient      pam_winbind_osstech.so.1
other   account required        pam_unix_account.so.1
```

3.8.2 PAM の動作確認

login, rlogin, ssh コマンドなどを利用して、PAM が winbind 経由で AD のユーザーを認証できることを確認する。以下に telnet による確認例を示す。

telnet で PAM が winbind を利用していることを確認

```
# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
login: administrator
Password: Administrator のパスワード
No directory! Logging in with home=/
Last login: Tue Feb 20 22:39:36 from localhost
Sun Microsystems Inc.   SunOS 5.10      Generic January 2005
$
```

AD のユーザーが認証されログインできたら、与えられた権限が正しいか確認する。

AD ユーザーの権限の確認（表示は AD に登録されている情報や smb.conf の設定により多少異なる）

```
$ id -a
uid=2500(administrator) gid=2513(domain users) groups=2518(schema admins),2519(enterprise
admins),2512(domain admins),2520(group policy creator owners)
```