「Samba 4 で構築する Active Directory 環境」

～インストールから UID/GID の話まで ～

OSSTech

オープンソース・ソリューション・テクノロジ
株式会社
2014/09/05
亀井 裕

自己紹介

- 亀井 裕 (かめい ゆたか)
- オープンソース・ソリューション・テクノロジ株式会社所属
- Samba と OpenLDAP の製品開発を行っています
- Samba 4 の書籍も執筆しました

内容

- Samba 4 の紹介
- Samba 4 で Active Directory ドメインを構築
- Samba 4 の UID/GID について - 運用後の話

Samba 4 の紹介（1）

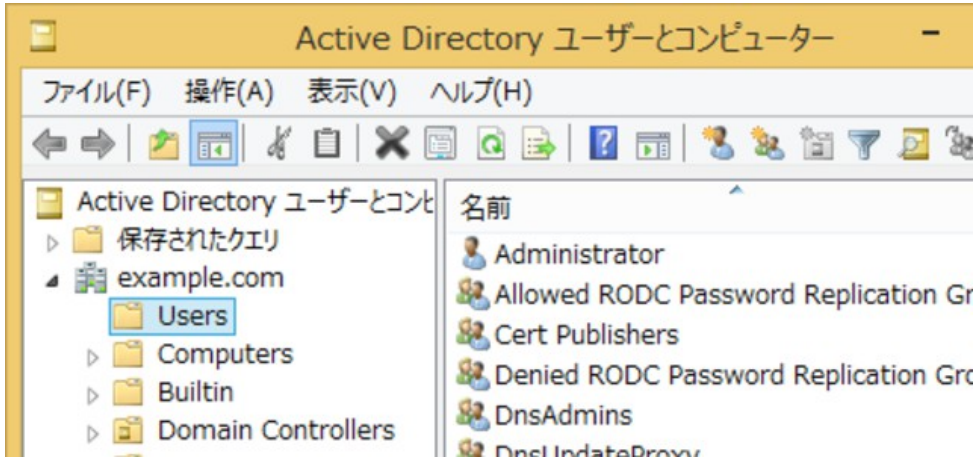
- Samba はWindows サーバー互換の機能を提供するオープンソース・ソフトウェアです
- 主な機能は次のとおりです
  - ファイルサーバー
  - ドメインコントローラー
  - ドメインメンバー
- 他にも、 WINS サーバー、プリントサーバー、 DNS サーバー、 KDC サーバーなどがあります

Samba 4 の紹介 (2)

- そもそも、なぜ Samba ？
  - コストを抑えたい
    - オープンソースなのでクライアント・アクセス・ライセンス(CAL)が不要
  - サーバーはUNIXやLinuxにしたい
  - ベンダーロックインを避けたい

Samba 4 の紹介 (3)

- 2012 年 12 月にメジャーバージョンが 4 の Samba がリリース
- Active Directory (AD) ドメインにてドメインコントローラーとしての機能をサポート
- リモートサーバー管理ツール (RSAT) で操作できる
- SMB3やサーバーサイドコピーもサポート



Samba 4 で Active Directory ドメインを構築 (1)

- デモ環境について
  - ホスト名: sv1
  - DNS名: sv1.example.com
  - NT ドメイン名: EXAMPLE
  - Administrator パスワード: Password-123

Samba 4 で Active Directory ドメインを構築 (2)

- Samba 4 のインストール
  - 事前に必要なライブラリ等をインストールしたうえでソースからビルドしてインストールします
  - ビルドに必要なパッケージは https://wiki.samba.org/index.php/OS_Requirements を参照

```
# curl -O ftp://ftp.samba.org/pub/samba/stable/samba-4.1.11.tar.gz
# tar xzf samba-4.1.11.tar.gz
# cd samba-4.1.11
<ビルドに必要なパッケージをインストール>
# ./configure
# make
# make install
```

Samba 4 で Active Directory ドメインを構築 (3)

- 次のコマンドで AD 環境の構築は完了です

```
# samba-tool domain provision --realm=example.com \
                              --domain=example \
                              --host-name=sv1 \
                              --adminpass=Password-123 \
                              --use-rfc2307 \
                              --server-role dc
```

Samba 4 で Active Directory ドメインを構築 (4)

- 環境構築後次のような出力が得られます

```
Server Role:           active directory domain controller
Hostname:              sv1
NetBIOS Domain:        EXAMPLE
DNS Domain:            example.com
DOMAIN SID:            S-1-5-21-871698246-2010901038-889881753
```

Samba 4 で Active Directory ドメインを構築 (5)

- あとはプログラムを実行するだけで AD ドメインコントローラーが起動します
- OS の再起動は不要です
- Windows Serverとは違い、関連するファイルを消せば何度でもやり直しができます

```
# samba

(関連ファイルを消すコマンド)
# rm -f /ur/local/samba/etc/smb.conf
# find /usr/local/samba/{var,private} -not -type d | xargs rm
```

Samba 4 で Active Directory ドメインを構築 (6)

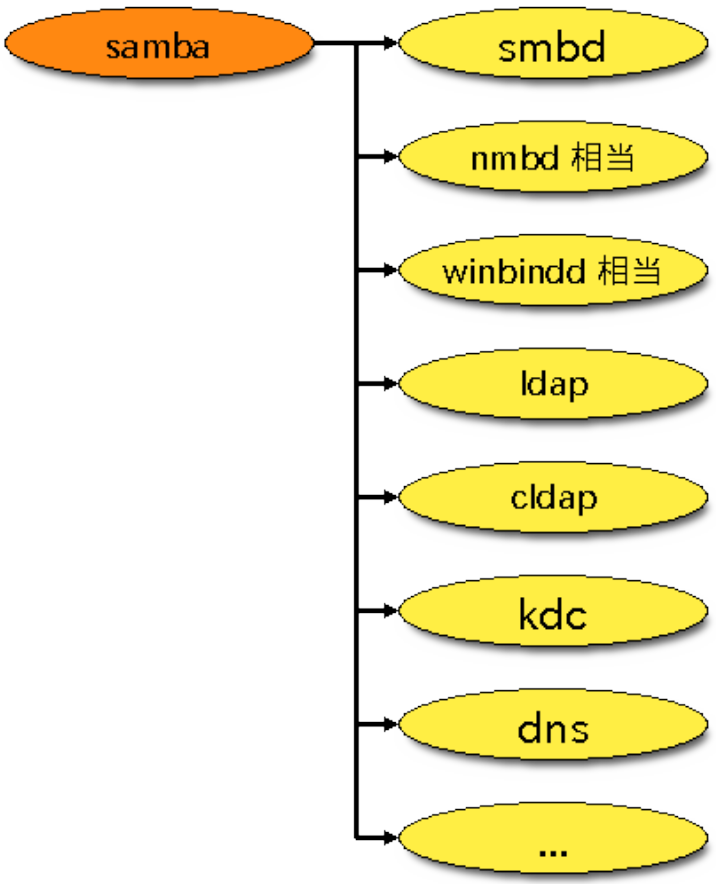
- ここまでの作業のデモ

余談 - Samba 4 のデーモンプログラムについて (1)

- Samba 4 には「samba」というプログラムが追加され、デーモンプログラムが 4 つになりました
  - samba: AD DC として使用
  - smbd: ファイルサーバーや NT DC として使用
  - nmbd: ブラウジングや WINS サーバーとして使用
  - winbindd: AD ドメインのメンバーサーバーとして使用

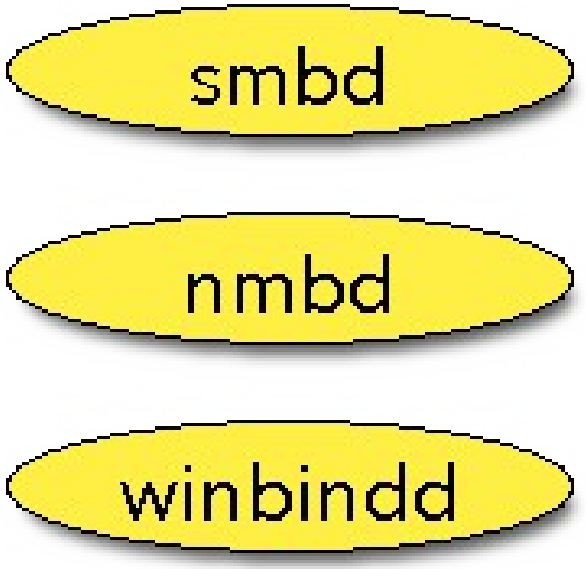
余談 - Samba 4 のデーモンプログラムについて (2)

- 「samba」プログラムは機能ごとにプロセスをフォークします
- フォークしたプロセスはAD DC として動作させるために必要な仕事をします
- 「samba」プログラムはSamba 4 で登場しました



余談 - Samba 4 のデーモンプログラムについて (3)

- その他のプログラムはそれぞれ独立したプログラムです
- たとえば、単にファイルサーバーとして利用したければ smbd だけを起動します
- 「samba」プログラムとの併用はできません

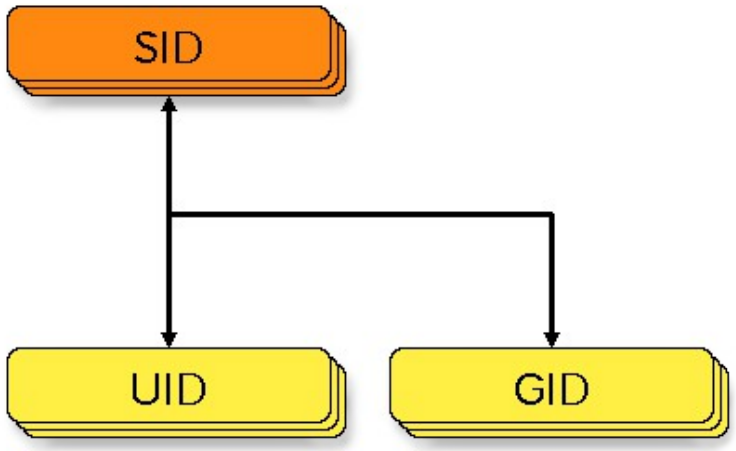


Samba 4 の UID/GID について (1)

- 運用の中で特に UID/GID について話す理由
  - まだあまり情報がない
  - あってもそれが本当に正しいのか確信が持てない
  - これまで Samba 3 を利用してきた方が特にハマりやすい罠がある

Samba 4 の UID/GID について (2)

- どのようにしてユーザーやグループ等を識別するのか
  - Windows の場合: SID で識別
  - UNIX/Linux の場合: UID/GID で識別
- Samba はこの異なる識別方式をカバーしなければならない



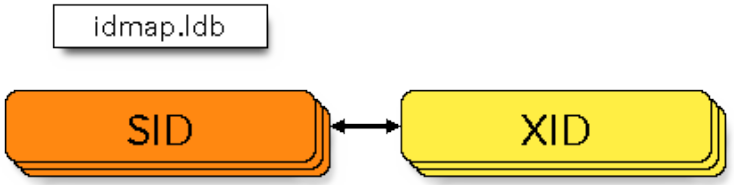
Samba 4 の UID/GID について (3)

- 方法1: xidNumber 属性を利用 (デフォルト)
  - Samba内部でxidNumberという属性とSIDを紐付けてマッピング
- 方法2: uidNumber/gidNumber 属性を利用
  - アカウントのエントリにuidNumber/gidNumberを追加することでマッピング

	xidNumber	uidNumber/gidNumber
関連ファイル	idmap.ldb	sam.ldb
複製	されない	される

Samba 4 の UID/GID について (4)

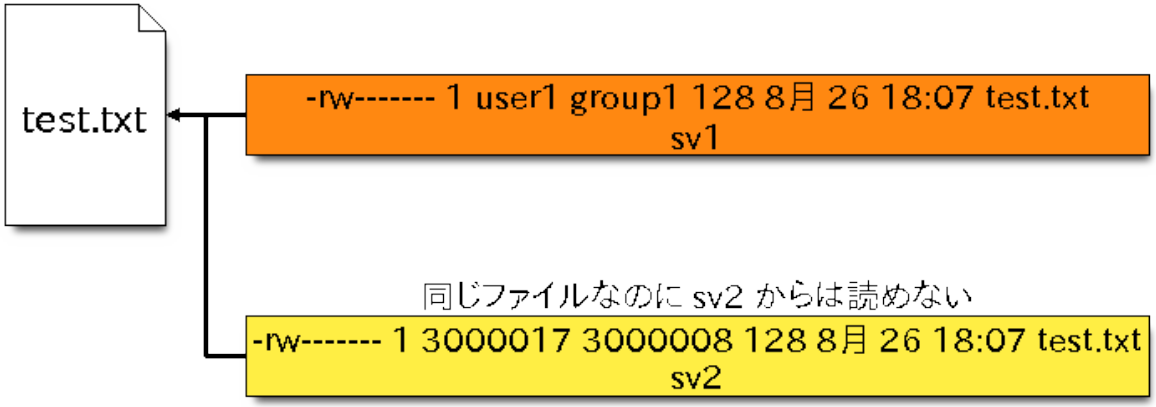
- xidNumberによる UID/GID割り当て
  - idmap.ldbでSIDと xidNumberを紐付け




```
dn: CN=S-1-5-21-871698246-2010901038-889881753-1103
cn: S-1-5-21-871698246-2010901038-889881753-1103
objectClass: sidMap
objectSid: S-1-5-21-871698246-2010901038-889881753-1103
type: ID_TYPE_BOTH
xidNumber: 3000017
distinguishedName: CN=S-1-5-21-871698246-2010901038-889881753-1103
```

Samba 4 の UID/GID について (5)

- xidNumberによるUID/GID割り当ての問題
  - xidNumber は idmap.ldb に生成されますが、 idmap.ldb 自体が複製されません
  - そのため、ドメインコントローラーごとにUID/GID値が異なります

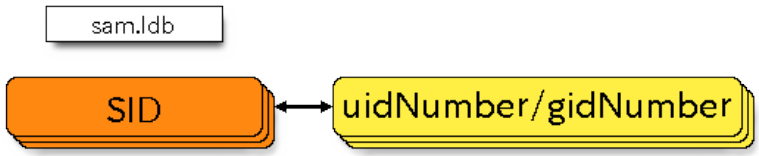


Samba 4 の UID/GID について (6)

- xidNumber による UID/GID 割り当てデモ

Samba 4 の UID/GID について (7)

- uidNumber/gidNumber による UID/GID割り当て
  - sam.ldbでSIDとuidNumber/gidNumberを紐付け




```
dn: CN=user1,CN=Users,DC=example,DC=com
uidNumber: 1234

dn: CN=Domain Users,CN=Users,DC=example,DC=com
gidNumber: 513
```

Samba 4 の UID/GID について (8)

- uidNumber/gidNumber を利用するために
  - smb.confに「idmap_ldb:use rfc2307 = yes」が設定されている必要があります
  - ユーザー属性にuidNumber/gidNumberが存在しなければいけません
    - 現在の実装では、Samba自身がuidNumber/gidNumberを付与することはありません
  - 「idmap_ldb:use rfc2307 = yes」は「samba-tool domain provision」に―use-rfc2307を指定すれば自動で設定されます

Samba 4 の UID/GID について (9)

- uidNumber/gidNumber による UID/GID割り当てデモ

Samba 4 の UID/GID について (10)

- UID/GIDに関するまとめ
  - UID/GIDのマッピングはxidNumberかuidNumber/gidNumberを利用している
  - xidNumberはレプリケーションされないのでDCごとにUID/GIDが異なる
  - uidNumber/gidNumberを使えば各DCで同一のUID/GIDを使える
    - Samba 3 winbindd のidmap_adバックエンドのような動き

余談 - idmap_ridを使えば統一管理できるのでは?

- Samba 4 でも idmap_rid は使用できますが、あくまでもメンバーサーバーのときしか使用できません
  - 以下の idmap config 設定は AD DC では無効

```
[global]
        workgroup = EXAMPLE
        realm = example.com
        netbios name = SV1
        server role = active directory domain controller
        dns forwarder = 192.168.12.254
        idmap_ldb:use rfc2307 = yes

        idmap config *: backend = rid
        idmap config *: range = 10000-50000
```

Samba 4 の今後

- AD DCでwinbinddをデフォルトで動かす (Samba 4.2)
  - Samba4.1まではwinbinddではなくwinbind
  - winbinddはSamba 3の実装を引き継いだもの
  - winbinddのidmap_ridがあればxidNumberに悩まされなくてすむ
    - と思っていましたが、winbinddは自分で管理するドメインに関してはpassdbという特殊なバックエンドを利用するため設定をしてもidmap_ridは機能しません
      - もちろん、メンバーサーバーとしてはしっかり機能します

ご清聴ありがとうございました

- ご質問があればどうぞ

OSSTech