Samba 3.0.20はこう変わった!

Samba 3.0.20の新機能を紹介！

日本Sambaユーザ会

たかはし もとのぶ (高橋基信)

おおた としや(太田俊哉)

http://www.samba.gr.jp/

Samba 3.0.20とは

- **Samba 3.0.14aの次期バージョン(2005/08/20)**
  - バージョン番号がスキップされているのは、「amount of changes」を意識付けるため
    - **http://marc.theaimsgroup.com/?l=samba&m=111721010206997&w=2**
- 「amount of changes」の正体……
  - **Winbind機構の非同期化、非同期I/Oの試験実装などの内部実装の変更**
  - 外面的な機能拡張自体は、それほど多くない
- **Samba 3.0.20a/bとは**
  - 基本的にバグフィックス版で、機能追加はなし

Samba 3.0.20の機能拡張（1）

- 主な機能拡張
  - ACLサポートの拡張
    - 幾つかのパラメータを追加
  - ゲストアクセス機能の拡張
    - Winbind機構が動作していないメンバサーバでの挙動を改善
  - Winbind機構の拡張
    - winbinddがADのSFU属性を参照可能に
    - idmap機構がADのSFU属性を参照可能に
  - 動的なユーザ名マッピング機能の実装

Samba 3.0.20の機能拡張（2）

- 主な機能拡張（2）
  - Windowsサービスのリモート管理機能の実装
  - SeTakeOwnershipPrivilegeユーザー権利の追加
  - 所有者を親ディレクトリから引きつぐ機能の実装
  - ファイル共有の移行をサポート
    - net share migrateコマンド
  - Print Migrator（プリンタ移行ツール）のサポート

Samba 3.0.20の機能拡張（3）

- その他の機能拡張、改善点
  - 幾つかのWin32 RPCパイプのサポートの追加
  - OS/2 クライアントのサポートの改良
  - 実験的な非同期ファイルI/Oサービスのサポート
    - `aio read size / aio write size` パラメータの新設
  - LinuxのCIFSファイルシステムクライアントを利用する際のPOSIXパス名サポートの実装見直し
  - 非同期`winbindd`の新登場
  - Windows NTのレジストリI/Oライブラリの新設

ACLサポートの拡張

- **Windows**ファイルサーバにおける**ACL**の実運用を考慮したパラメータが幾つか追加
  - **`acl group control / acl check permissions / acl map full control`**
- **ACL**とは
  - 各ファイル(ディレクトリ)に対して、**Windows**の**NTFS**と同様に複数のユーザ、グループに対するアクセス許可を設定する機能

ACLサポートの拡張(1)

- **Samba 3.0.14aまで**
  - ファイルのACLを変更できるのは、rootと所有者(特定ユーザ)のみ
    - UNIX(Linux)の仕様に準拠
- **Samba 3.0.20以降**
  - 「`acl group control = yes`」により、所有グループに所属するユーザもACLの変更が可能

ACLサポートの拡張(1) ― 概要

- acl group controlパラメータの目的
  - Windowsファイルサーバの運用をエミュレート
    - Windowsでは、自グループの共用ファイル領域について、フルコントロール権限を与える運用が多い
      ※上記はSamba Teamの見解
    - フルコントロールを与える目的は、ACLの編集を可能とするため
      - フルコントロールにすることで、ACLの編集も可能に
      - POSIXのACL機構では、「ACLの編集」という権限は存在しない
        ACLの編集はrootと所有者のみ(もしくはrootのみ)が可能

ACLサポートの拡張(1) ー 設定

- 「acl group control = yes」の設定を行う
  - testuser以外のユーザでもACLの編集が可能
  - 例えば、ユーザribbon（ribbonグループ所属）でも、ACLの編集が可能
    - 所有者自体の変更はできない

ACLサポートの拡張(2)

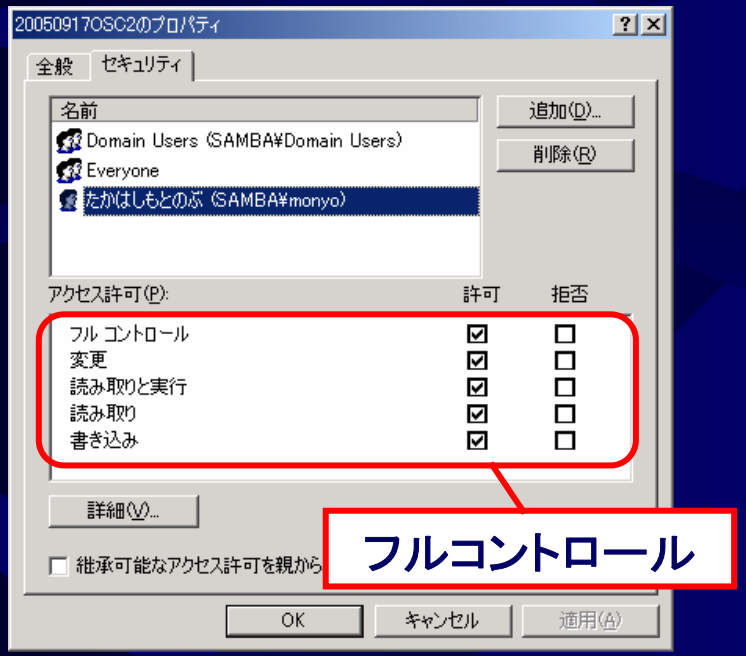
- **Samba 3.0.14a**まで
  - **UNIX**側のパーミッション「**rwx**」は、**Windows**側の「フルコントロール」にマッピング
- **Samba 3.0.20**以降
  - 「**acl map full control = no**」により、**UNIX**側のパーミッション「**rwx**」を**Windows**側の「読み取り＋書き込み＋実行」にマッピング

ACLサポートの拡張(2) ー 詳細

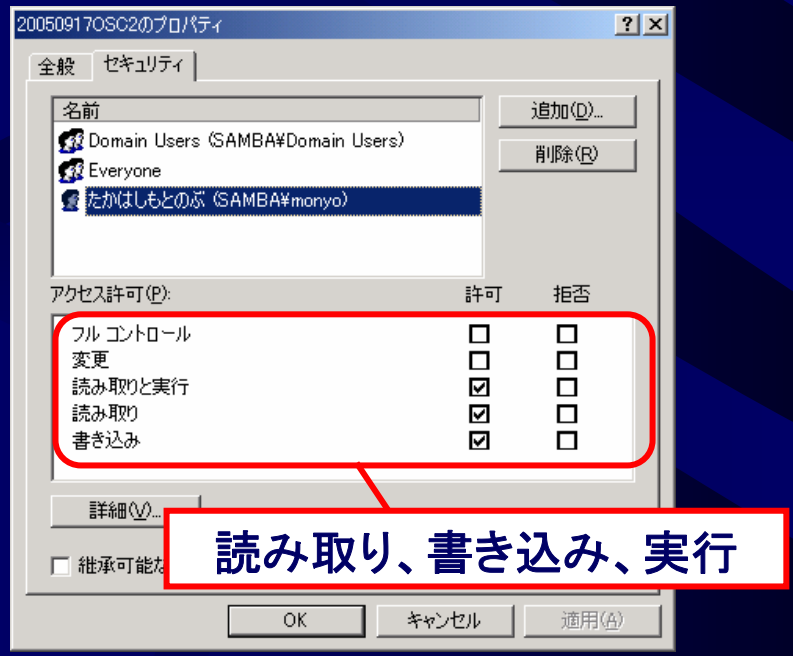
- このパラメータの目的
  - 「読み取り(r)」と「書き込み(w)」を設定したファイルのアクセス許可がWindowsから「フルコントロール」として見えてしまうことを防ぐ
    - **Windows**のファイルサーバの運用では、ユーザに読み取りや書き込みを許可しても、フルコントロールまでは許可しない運用が普通

ACLサポートの拡張(2) ー 設定

- 「acl map full control = no」の設定を行う
  - UNIX上で「rwx」となってるパーミッションをWindowsから参照した際の見え方が異なる



acl map full control = yes



acl map full control = no

ACLサポートの拡張(3)

- Samba 3.0.20以降
  - 「acl check permissions」パラメータが追加
  - このパラメータが「yes」の場合、ファイルの削除時にACLのチェックを行う
    - Samba 3.0.13以前と同様の実装になる
  - 現段階では具体的に用途などが不明
    - ソース(smbd/dosmode.c)を見ると、このパラメータが「yes」の時には、ファイル削除時にディレクトリに書き込み可能かどうか、ACLのチェックを行なう
      → 通常は、パーミッションにおけるチェックのみ

ゲストアクセス機能の拡張

- **SambaサーバがドメインのメンバサーバかつWinbind機構を使用していない環境において.....**
  - ドメインで認証済かつSambaサーバにアカウントのないユーザからアクセスがあった場合.....
- **Samba 2.2系列まで**
  - 「`map to guest = Bad User`」でゲスト認証
- **Samba 3.0.0～Samba 3.0.14aまで**
  - 認証拒否
- **Samba 3.0.20**
  - 「`map to guest = Bad Uid`」(新設)でゲスト認証

ゲストアクセス機能の拡張 ― 概要

- ゲストアクセス機能とは
  - 認証されないアクセスをゲストアクセスとして認証
    → 認証されないアクセスは接続できないため
    - 共有にアクセスする前に、Sambaサーバにアクセスする時点で、なんらかのユーザとしての認証が必要

ゲストアクセス機能の拡張 ー 設定

- map to guestパラメータの値が拡張
  - Bad Uid値が追加

パラメータの値	ユーザ:正当 認証:失敗	ユーザ:不正 (認証:失敗)	ユーザ:不正 認証:成功
Never	認証失敗	認証失敗	認証失敗
Bad User	認証失敗	ゲスト認証	認証失敗(注)
Bad Password	ゲスト認証	ゲスト認証	ゲスト認証
Bad Uid(新規)	**認証失敗**	**ゲスト認証**	**ゲスト認証**

注: Samba 2.2系列では、ゲスト認証

ゲストアクセス機能の拡張 － 補足

- **Winbind機構が有効な場合**
  - 認証に成功した段階でSambaユーザが自動的に生成されるので、「ドメインで認証済かつSambaユーザが存在しない」という状況が発生しない
    → `Bad Uid` が有用な条件が発生しない
- 従来からの対処策
  - `add user script`パラメータにより、Sambaユーザの自動生成を行う
    → Winbind機構使用時と同様に `Bad Uid` が有用な状態が発生しない

Winbind機構の拡張

- Samba 3.0.14aまで
  - Winbind機構で作成されたユーザのシェル、ホームディレクトリは、パラメータで一律に作成
    - `template homedir`
    - `template shell`
- Samba 3.0.20
  - 「`winbind nss info = sfu`」により、SFUで拡張されるUNIX属性から、値を取得可能
    - 「`security = ads`」が前提
    - シェル、ホームディレクトリの情報を取得可能

Winbind機構の拡張　－　設定

- 「security = ads」の設定で、ドメインに追加
- Winbind機構を動作させる
- Windows側のDCにSFUのNISモジュールをインストールして、スキーマを拡張する
- smb.confに以下の設定を行う

```
[global]
   ...
   winbind nss info = sfu
```

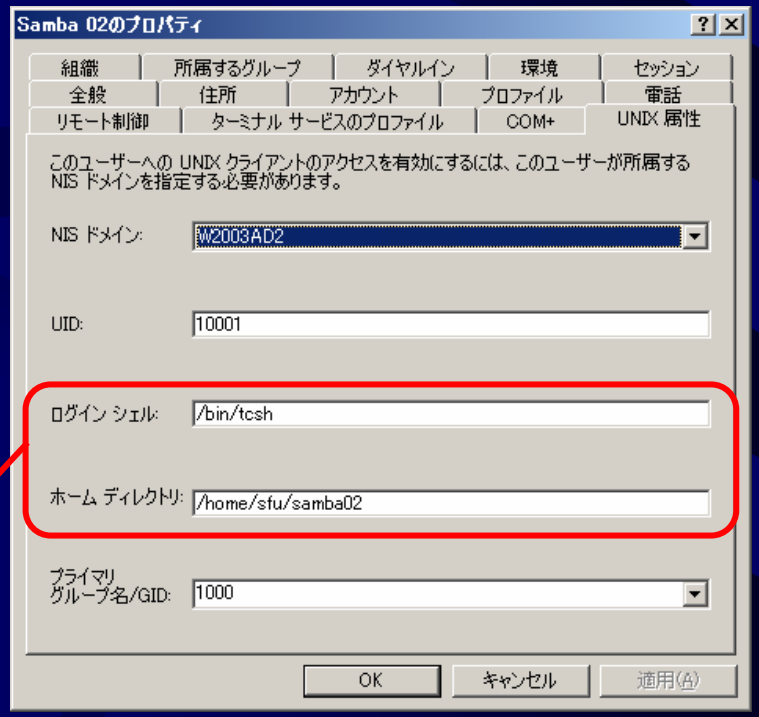
デフォルト値「winbind nss info = template」の場合、もしくは該当のユーザにUNIX属性が存在しない場合は、template homedir および template shell パラメータの値が用いられる

Winbind機構の拡張 ー 設定2

- 実行例

```
$ getent passwd W2003AD2¥¥samba02
W2003AD2¥samba02:x:20001:2000:Samba 02:/home/sfu/samba02:/bin/tcsh
```

  - template shell / template homedir パラメータの値に関わらず、UNIX属性の値が用いられる



反映されるのは、ログイン シェルとホーム ディレクトリのみ

Winbind機構の拡張(2)

- Samba 3.0.14aまで
  - Winbind機構で作成されたユーザのsidとuidのマッピング情報は、ファイルもしくはLDAPに格納
    - `idmap backend = (NULL)|ldap`
- Samba 3.0.20
  - 「`idmap backend = ad`」により、SFUで拡張されるUNIX属性から、マッピング情報を取得可能
    - 「`security = ads`」が前提
    - UNIX属性のuidの情報を取得可能

Winbind機構の拡張(2) ー 設定

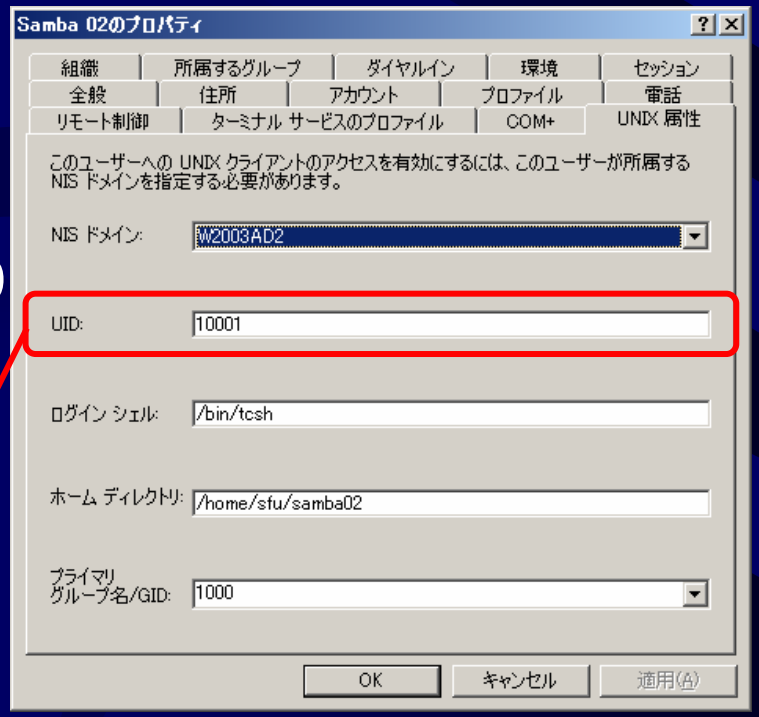
- 「`security = ads`」の設定で、ドメインに追加
- Winbind機構を動作させる
- Windows側のDCにSFUのNISモジュールをインストールして、スキーマを拡張する
- `idmap_ad.so`モジュールを作成する
  - Samba本体をビルドした後で「`make bin/idmap_ad.so`」と入力して個別に作成する必要がある
- `idmap_ad.so`モジュールをインストールする
  - デフォルトの場合「`/usr/local/samba/lib/idmap/ad.so`」というファイル名でインストール
- 「`idmap backend = ad`」の設定を追記

Winbind機構の拡張(2) ー 設定2

- 実行例

```
$ getent passwd W2003AD2¥¥samba02
W2003AD2¥samba02:x:10001:2000:Samba 02:/home/sfu/samba02:/bin/tcsh
```

  - uid値として、UNIX属性の値が用いられる
  - 「プライマリグループ名/GID」については、参照されないので注意



UIDの値が反映される

動的なユーザ名マッピング

- **Samba 3.0.14aまで**
  - **Username Mapファイル（username mapパラメータ）**による静的なマッピングのみ
  - サーバ毎に設定する必要がある
- **Samba 3.0.20**
  - **username map script**パラメータの設定による、動的かつ柔軟なマッピングのサポートが新設

```
[global]
  ...
  username map script = /usr/local/samba/lib/mapusers.sh
```

※スクリプト名は任意

動的なユーザ名マッピング　－　設定

- Windows側のユーザ名を引数に取り、対応するUNIXユーザ名を出力するスクリプトを作成
  - LDAPなどに格納したマッピング情報の利用も可能に

```
#!/bin/sh

if [ "$1" == "Administrator" ]; then
  echo root
elif [ "$1" == "TAKAHASHI Motonobu" ]; then
  echo monyo
fi
```

Windows側のユーザ名「Administrator」をUNIXユーザ「root」に、同じく「TAKAHASHI Motonobu」を「monyo」にマッピングするスクリプト
Windows側のユーザ名は大文字小文字を区別するので注意

Windowsサービスのリモート管理

- net rpc serviceコマンド

```
# net rpc service
net rpc service list                    View configured Win32 services
net rpc service start <service>         Start a service
net rpc service stop <service>          Stop a service
net rpc service pause <service>         Pause a service
net rpc service resume <service>        Resume a paused a service
net rpc service status <service>        View the current status of a
service
```

- 実行例(Windowsマシン上のサービス列挙)

```
$ net rpc service list -I 192.168.135.1 -U test1%test1
ACS                     "ACU Configuration Service"
Alerter                 "Alerter"
ALG                     “Application Layer Gateway Service”
...
```

ユーザー権利の追加

- **SeTakeOwnershipPrivilegeユーザー権利**
  - 「所有権の取得」権利に相当
- 実行例

```
# net rpc rights grant monyo SeTakeOwnershipPrivilege -U root%samba
Successfully granted rights.

# net rpc rights list accounts -U root%samba
...
Everyone
No privileges assigned

SAMBA¥monyo
SeTakeOwnershipPrivilege

# net rpc rights revoke monyo SeTakeOwnershipPrivilege -U root%samba
Successfully revoked rights.
```

ユーザー権利の追加 － 詳細

- ユーザー権利とは
  - 一般ユーザに特殊な権限を付与する機能
    - 管理作業をroot以外のユーザで実施することが可能に
      → 管理分散、セキュリティ向上が実現
    - Samba 3.0.11以降で実装
    - 「`enable privileges = yes`」で有効化
    - `SeMachineAccountPrivilege`
      - ドメインへのマシン追加、削除
    - `SeAddUsersPrivilege`
      - Sambaドメイン（マシン）のユーザ管理
    - `SePrintOperatorPrivilege`
      - `printer admin`パラメータを代替

所有者を親ディレクトリから引きつぐ

- **Samba 3.0.14aまで**
  - 所有者は、**UNIX**の実装に依存
    → 通常はファイル/ディレクトリ作成者
  - 「`force user`パラメータ」などである程度設定可能
- **Samba 3.0.20**
  - 新設された「`inherit owner = Yes`」により、新規作成ファイル/ディレクトリの所有者を、親ディレクトリから引きつぐことが可能に

ファイル共有の移行サポート

- 「net share migrate」コマンド
  - FILES ー 共有内のファイルを移行
  - SHARES ー 共有を移行
    - add share commandにより共有を作成する
  - SECURITY ー 共有のACLを移行

```
net [<method>] share MIGRATE FILES <sharename> [misc. options] [targets]
        Migrates files from remote to local server
net [<method>] share MIGRATE SHARES <sharename> [misc. options] [targets]
        Migrates shares from remote to local server
net [<method>] share MIGRATE SECURITY <sharename> [misc. options] [targets]
        Migrates share-ACLs from remote to local server
net [<method>] share MIGRATE ALL <sharename> [misc. options] [targets]
        Migrates shares (including directories, files) from remote
        to local server
```

ファイル共有の移行サポート

- 実行例

```
# net share migrate all tako -I 192.168.135.11 -S mayuko -U
SAMBA¥¥Administrator%samba --attrs
migrating: [TAKO], path: C:¥temp¥tako, comment: , without share-ACLs
           [TAKO] does already exist
syncing    [TAKO] files and directories without ACLs, including DOS
Attributes
migrating: [TAKO], path: C:¥temp¥tako, comment: , including share-ACLs
```

mayukoという192.168.135.11のマシン上にある「TAKO」という共有中の共有定義、共有中のファイル、ファイル属性を移行するコマンド例

「net share migrate shares(もしくはall)」を用いて、「C:¥temp¥tako」というパスを移行した場合、/temp/takoというパスに移行されるため、共有定義は手作業で移行することを推奨

Print Migratorのサポート

- **Print Migratorとは**
  - **Windowsサーバ間で、プリンタサーバの構成情報を移行するツール**
    `http://support.microsoft.com/kb/315983/ja`
- **Samba 3.0.20は、Print Migratorによる移行をサポート**

まとめ

- Samba 3.0.20の新機能について簡単に説明
  - 詳細については、ドキュメントや実験で確認
- 参考書籍
  - 「Sambaのすべて」
    - 出版社: 翔泳社 / ¥3,980
    - ISBN: 4-7981-0854-5