Samba

(ちょっと大きめの）

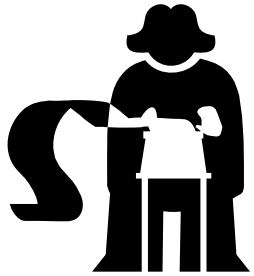
TIPS

日本Sambaユーザー会
(NEC OSS推進センター)
太田俊哉

本日のお題

- Sambaを使う上での小技をいくつか紹介します
- 日経Linuxで2006年3月から連載していた中からいくつか紹介します
  - 小技でないかもしれませんが...
- ごく単純なファイルサーバとしてSambaを使うときには、それほど技は必要ありませんが、少し便利な事をやりたい場合には、いろいろ技が必要です。

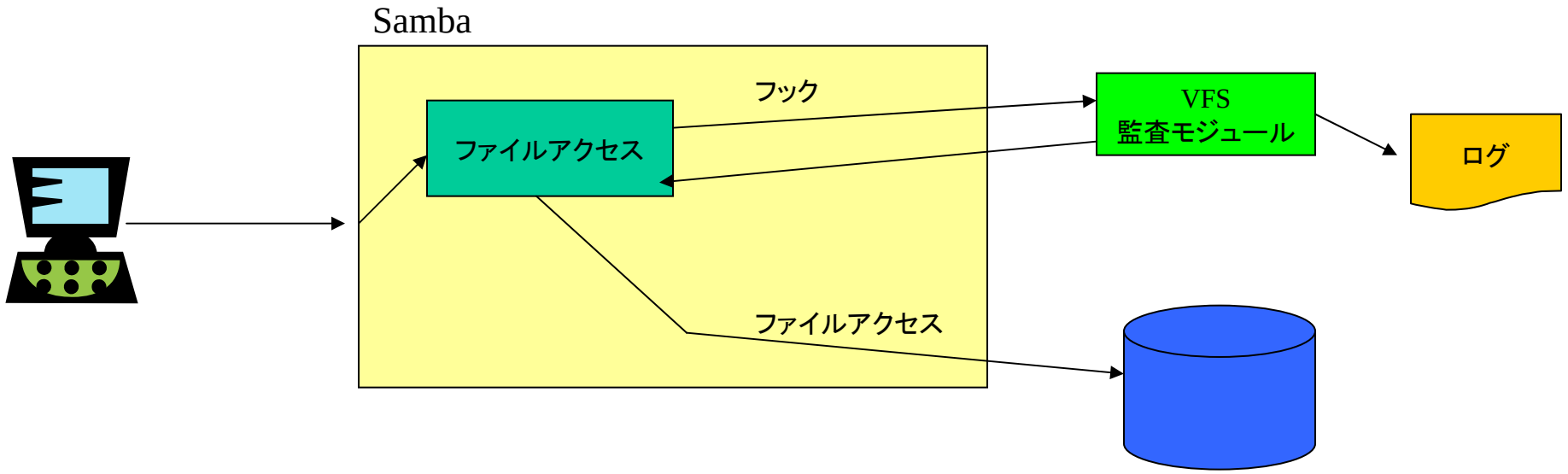
アクセスログを取る



- アクセスログとは
  - Sambaの動作のログ⇒通常のログ
    - 余計なものがたくさん（もともとデバッグ用）
  - アクセスログは、ファイル操作のログ
    - 何をやったかを知りたい
  - いわゆる監査機能
    - そういえばJ-SOX法とか、内部統制とか、いろいろありますね
    - ファイルサーバとしても、誰が何時どのようにデータを変更したかを記録することが要求される場合があります
- Sambaが持つ監査機能と言えます

VFS機能

- VFS:Virtual File System
  - Samba2.2から実装
  - ファイルシステムへのアクセスを仮想化する
  - ファイル操作に対しフックを用意、処理の拡張や代替操作が可能



提供されているvfsモジュール

- 以下の12種類が提供されている(CentOS5)

audit	システムログにファイル操作を出力
cap	ファイルのCAPエンコード
default_quota	既定値のquotaレコードをWindowsに提供
expand_msdfs	DFSクライアントを最寄りのhostにリダイレクトする? ※
extd_audit	syslogにファイル操作を出力
fake_perms	移動プロファイルをread only にする
full_audit	詳細な監査記録を取る
netatalk	AppleDoubleファイルを見せなくする
readahead	kernel buffer キャッシュをプリロードする
readonly	所定の時間共有をreadonlyにする
recycle	ゴミ箱機能を実現する
shadow_copy	shadow copy機能を実現する

※web上のマニュアルにはなし

sambaのweb上には

- もうちょっと別のものがあります
  - vfs_cacheprime
  - vfs_catia
  - vfs_commit
  - vfs_gpfs
  - vfs_notify_fam
  - vfs_prealloc
- ソース上には開発中のものもちらほら
  - acl関係が多いようです
  - ここではこれ以上説明しません

ドキュメントは3.0.25から

- それ以前はマニュアルがない
  - ソースを読む
    - それほど複雑ではない
  - 見よう見まね
- manpage が出来た
  - http://www.samba.org/samba/docs/man/manpages-3/
- manpageにないものも
  - CentOSに提供されていないものも
  - まだ整備が不完全
  - 日本語訳はなし(**皆さん協力しましょう**)

3つのモジュール

- audit
  - 基本的な機能を提供
  - Samba用のログに出力
- extd_audit
  - 機能はauditと同じ
  - ログ出力先がsyslogに
    - syslog watcher で監視が出来るようになる
- full_audit
  - 全部の操作を監視

設定してみよう(audit)

- 基本的な設定は smb.confにvfs関連の記述を追加することで行なう
  - auditの例

```
vfs object = audit
audit:facility = LOCAL1
audit:priority = NOTICE
```

  - syslogも変更

```
local1.*      /var/log/samba/audit.log
```

結果は(auditモジュール)

```
[2007/06/22 21:49:22, 2] smbd/open.c:open_file(352)
  ribbon opened file 新規テキスト ドキュメント.txt read=Yes write=Yes (numopen=2)
[2007/06/22 21:49:22, 2] smbd/close.c:close_normal_file(344)
  ribbon closed file 新規テキスト ドキュメント.txt (numopen=1)
[2007/06/22 21:49:26, 2] smbd/open.c:open_file(352)
  ribbon opened file 新規テキスト ドキュメント.txt read=No write=No (numopen=2)
[2007/06/22 21:49:26, 2] smbd/close.c:close_normal_file(344)
  ribbon closed file 新規テキスト ドキュメント.txt (numopen=1)
[2007/06/22 21:49:26, 2] smbd/open.c:open_file(352)
  ribbon opened file ./新規テキスト ドキュメント.txt read=No write=No (numopen=2)
[2007/06/22 21:49:26, 2] smbd/close.c:close_normal_file(344)
  ribbon closed file ./新規テキスト ドキュメント.txt (numopen=1)
[2007/06/22 21:49:27, 2] smbd/open.c:open_file(352)
  ribbon opened file test.txt.txt read=Yes write=No (numopen=2)
[2007/06/22 21:49:27, 2] smbd/close.c:close_normal_file(344)
  ribbon closed file test.txt.txt (numopen=1)
[2007/06/22 21:49:27, 2] smbd/open.c:open_file(352)
  ribbon opened file test.txt.txt read=No write=No (numopen=2)
[2007/06/22 21:49:27, 2] smbd/close.c:close_normal_file(344)
  ribbon closed file test.txt.txt (numopen=1)
```

結果は（syslog)

```
Jun 22 21:57:05 cent5 smbd_audit[11627]: connect to service ribbon by user ribbon
Jun 22 21:57:05 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:05 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:06 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:06 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:06 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:06 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:09 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:09 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:09 cent5 smbd_audit[11627]: open 新規テキスト ドキュメント.txt (fd 27) for writing
Jun 22 21:57:09 cent5 smbd_audit[11627]: fchmod_acl 新規テキスト ドキュメント.txt mode 0x1e4
failed: 利用可能なデータがありません
Jun 22 21:57:09 cent5 smbd_audit[11627]: close fd 27
Jun 22 21:57:09 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:12 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:12 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:12 cent5 smbd_audit[11627]: opendir .
Jun 22 21:57:12 cent5 smbd_audit[11627]: rename ./新規テキスト ドキュメント.txt -
> ./test.txt.txt
Jun 22 21:57:12 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:13 cent5 smbd_audit[11627]: open test.txt.txt (fd 27)
Jun 22 21:57:13 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:16 cent5 smbd_audit[11627]: close fd 27
Jun 22 21:57:16 cent5 smbd_audit[11627]: open test.txt.txt (fd 27) for writing
Jun 22 21:57:16 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:16 cent5 smbd_audit[11627]: close fd 27
Jun 22 21:57:18 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:18 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:18 cent5 smbd_audit[11627]: opendir ./
Jun 22 21:57:19 cent5 smbd_audit[11627]: unlink test.txt.txt
```

auditとextd_auditの違い

- auditが吐き出すsambaのログはおおざっぱ
- syslogへの出力の方が詳しい
- auditとextd_audit共にsyslogへのメッセージは同じ
- extd_auditにすると、sambaのログにもsyslogと同等のログが記録される
- 用途に応じて使い分ければよいでしょう
  - /var/log/messages をログ監視ツールで監視
  - /var/log/samba/*を別のツールで監視....etc

full_auditモジュール

- より詳細なaudit
- aclの設定変更なども監査可能
- 成功した処理、失敗した処理を記録できる
- 出力はsyslogに

syslogの結果

```
Jun 22 22:46:39 cent5 smbd_audit: ribbon|192.168.1.53|stat|fail (そのようなファイルやディレクトリはありません)|新規テキスト ドキュメント.txt
Jun 22 22:46:39 cent5 smbd_audit: ribbon|192.168.1.53|stat|fail (そのようなファイルやディレクトリはありません)|新規テキスト ドキュメント.txt
Jun 22 22:46:39 cent5 smbd_audit: ribbon|192.168.1.53|lstat|fail (そのようなファイルやディレクトリはありません)|新規テキスト ドキュメント.txt
Jun 22 22:46:39 cent5 smbd_audit: ribbon|192.168.1.53|stat|fail (そのようなファイルやディレクトリはありません)|新規テキスト ドキュメント.txt
Jun 22 22:46:39 cent5 smbd_audit: ribbon|192.168.1.53|stat|fail (そのようなファイルやディレクトリはありません)|新規テキスト ドキュメント.txt
Jun 22 22:46:39 cent5 smbd_audit: ribbon|192.168.1.53|fchmod_acl|fail (利用可能なデータがありません)|新規テキスト ドキュメント.txt|744
Jun 22 22:46:53 cent5 smbd_audit: ribbon|192.168.1.53|get_shadow_copy_data|fail (関数は実装されていません)|
Jun 22 22:46:53 cent5 smbd_audit: [2007/06/22 22:46:53, 0] modules/vfs_full_audit.c:log_success(682)
Jun 22 22:46:53 cent5 smbd_audit:   log_success() failed to get vfs_handle->data!
Jun 22 22:46:53 cent5 smbd_audit: ribbon|192.168.1.53|chdir|ok|chdir|/home/ribbon
Jun 22 22:46:53 cent5 smbd_audit: [2007/06/22 22:46:53, 0] modules/vfs_full_audit.c:log_success(682)
Jun 22 22:46:53 cent5 smbd_audit:   log_success() failed to get vfs_handle->data!
Jun 22 22:46:53 cent5 smbd_audit: ribbon|192.168.1.53|stat|ok|新規テキスト ドキュメント.txt
Jun 22 22:46:53 cent5 smbd_audit: [2007/06/22 22:46:53, 0] modules/vfs_full_audit.c:log_success(682)
Jun 22 22:46:53 cent5 smbd_audit:   log_success() failed to get vfs_handle->data!
Jun 22 22:46:53 cent5 smbd_audit: ribbon|192.168.1.53|lstat|ok|新規テキスト ドキュメント.txt
```

メッセージの整理が必要

- full_auditは大量にメッセージが出る
- メッセージの整理が必要
  - read,write,unlinkとか
- syslogに出る
  - sambaのlogには対して出ない
  - messagesの選別が必要
  - 文字コード
    - メッセージはstrerrerを使用

日本語のユーザ名を使いたい

- Windows XPでの初期設定
  - ユーザ名入力時にはかな漢字変換が**ON**
  - 自動的に日本語で入力される..日本語のユーザ名
  - そういえばLDAPもUTF-8対応

- UNIX系OSでのユーザ名は
  - 英数字のみ(はるか昔、英語以外の言語を扱う考え方そのものがなし)
  - 32文字まで(Linux)、16文字まで(BSD)、8文字まで(オリジナルUNIX)

何とかならないか

何とかしましょう

- ユーザー名を作り直す
  - 人数が多いほど大変な手間
  - ただ、社員IDとかで管理している体系があるならば可能か
  - システム刷新の時などに体系を切り替えることは可能かも
- 英語名と日本語名のマップを作る
  - ログインは日本語、内部は英数字
  - 二重管理になるのが難点
  - 若干見栄えは悪いけれどまあまあ使える

2つのマップ方式

- 静的マップと動的マップ
  - samba 3.0.20より前は静的マップのみ
    - username map パラメータ
    - このパラメータで指定したファイルでユーザ名を変換
    - unixuser = windowsuser (ここに日本語で書く)
    - 空白付きの名前も、" でくくればOK
    - 大文字/小文字を区別しない
  - samba 3.0.20以降は +動的マップ
    - username map script
    - たとえばldapから情報を得る
    - 大文字/小文字を区別する

やってみましょう（静的マップ）

- 設定ファイルを準備 (/etc/samba/username.map)
  - ribbon=シトロン
  - ribbon="Aqua Clear"
- ログインしてみる

```
[2007/06/23 14:41:39, 2] auth/auth.c:check_ntlm_password(309)
  check_ntlm_password:  authentication for user [シトロン] -> [ribbon] -> [ribbon] succeeded
[2007/06/23 14:41:39, 2] lib/module.c:do_smb_load_module(64)

[2007/06/23 14:57:38, 2] auth/auth.c:check_ntlm_password(309)
  check_ntlm_password:  authentication for user [Aqua Clear] -> [ribbon] -> [ribbon] succeede
d
```

- 無事出来ました

やってみましょう（動的マップ）

- 毎回データベースを検索
- たとえばldapの検索はこんな感じ

```
# more /etc/samba/mapscript.sh

#!/bin/sh
ldapsearch -x -b "ou=userinfo,dc=w2003,dc=local" sn=$1
 | grep cn: | cut -b 5-
```

- 動的に変更しても追随できます
  - それほどリアルタイム性を必要とする理由は?
  - 負荷も増えます

WINSサーバの複製

- PDC/BDC方式ではユーザ情報は複製可
- WINSサーバは複製できない
  - Sambaの場合、WINSサーバは1つ
  - PDCが倒れると……
- いくつかの解決方法
  - WINSサーバの静的な設定
  - samba4win
  - winssend.pl **始めて紹介！**

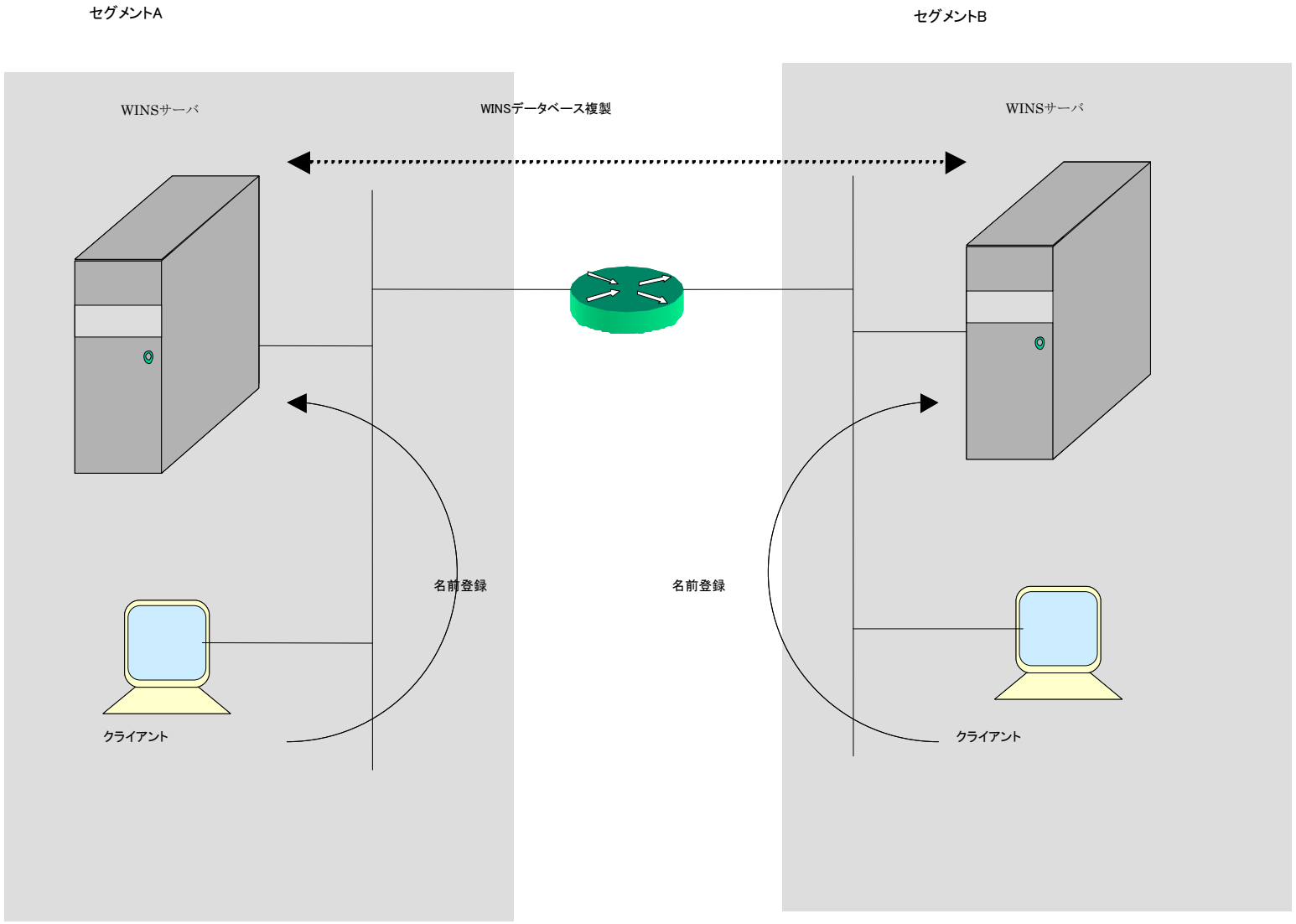
samba4winsとの比較

- samba4wins
  - samba4のソースコードをバックポートしたようなもの
  - 専用プログラム（サービス）
  - 基本的に同一サーバ内でSambaと共存不可能
- winssend.pl
  - 2006年のソフトウェアシンポジウムで発表
  - Sambaから起動されるスクリプト
  - Sambaと共存可能
  - 既存のSambaに対しほとんど設定変更なし
  - ほぼすべてのバージョンで利用可能

やっていること

- 物凄く単純
  - コンピュータ登録時にwins hook が呼ばれるので、そのインタフェースで他のwins server (samba)に名前登録を行なう
  - これだけ
    - 白山羊さん-黒山羊さん対処
    - 結果としてマルチマスタ機能

おおよそこんな感じ


セグメントA
セグメントB
WINSサーバ
WINSデータベース複製
WINSサーバ
名前登録
名前登録
クライアント
クライアント

プログラムは

- perl5で記述
  - コメント込みで346行
    - 抜けば200行くらい?
  - GPL V2
    - V3にするかは未定
  - いくつかのモジュールを使用
    - IO::Socket,File::Log,Net::Interface
    - Data::Hexdumper(デバッグ用)
    - 多くのモジュールがあるperlは便利

wiki.samba.gr.jpに置いてあります

- ソースプログラムはwiki.samba.gr.jpにあります
- 発表した論文は、ソフトウェアシンポジウムの論文誌に掲載されています
- 大規模環境での評価はしていません
  - 個人じゃ出来ません
  - デバッグに協力して頂けると助かります
  - 英訳手伝って頂ける方も募集中です
- 論文も公開しています
  - http://www.nec.co.jp/linux/topics070627.html

happy hakking!