答は、やってみなくちゃわからない Sambaドメイン評価環境で

discover samba

日本Sambaユーザ会

太田俊哉

日本 samba ユーザ会

http://wiki.samba.gr.jp

講師紹介

太田俊哉

- 日本電気株式会社
  ITプラットフォームソリューション事業部
  OSS推進グループ　（組織名変わりました）
  主に、OSSミドルウェアサポートサービスのとりまとめをやってます
  http://www.nec.co.jp/oss
  http://www.nec.co.jp/oss/middle_support/
- 日本Sambaユーザー会スタッフ（発起人）

本日のお品書き

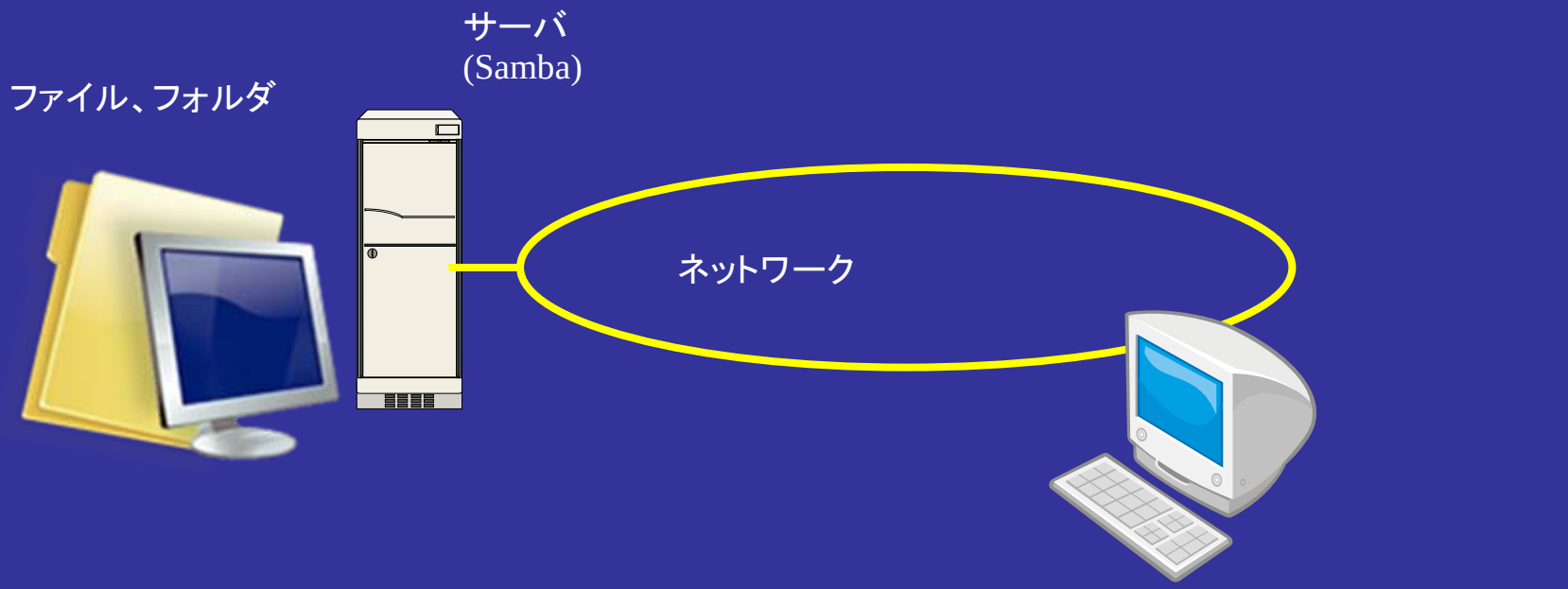
- Sambaドメイン評価環境とは
- 評価環境でできること
- Samba評価環境のインストール
- 動作の詳細
- まとめ

Sambaドメイン評価環境とは

- Sambaのドメイン環境を構築するのは少々手間
  - いろいろな設定ファイルを準備する必要がある
- あらかじめ設定した環境を準備
  - すぐに使える
  - 設定の例として使える
  - デバッグにも使える
  - ....その他
- 数年にわたりSambaユーザー会が提供

Samba評価環境の利用イメージ

- サーバ（OpenSUSE）にSambaをインストール
- クライアント（Windows）の設定はほとんど不要



今までのもの(V3まで)

- debianをベース
- あらかじめ設定ファイルをカスタマイズ
- 結構コンパクト
- Sambaドメイン構築済み
- ....でも
  - Sambaドメインがどのようなものかを確認する程度
  - debianに慣れていないとメンテしづらい

V4では

- 思い切ってベースOSを切り替える
- 選択時に必要なポイント
  - カスタマイズの容易性
  - 作成した環境の容量
  - 普及度
  - 操作性

V4では

- 思い切ってベースOSを切り替える
- ベースの選択
  - FreeBSD(*BSD)
  - OpenSolaris
  - Fedora
  - Vine
  - CentOS
  - OpenSUSE
    - SuSE Studio

評価環境でできること

- Sambaドメインの評価
  - あらかじめ一通りの設定済み
  - あとはWindowsクライアントをドメインに参加させるだけ
  - 初期化スクリプト用意済み。繰り返しテスト可能
  - VMwareイメージ
- Samba機能のテスト
  - VFSの例
  - smb.confの例
  - などなど

Sambaドメイン環境

- 「SAMBADOM」というドメイン
  - winbindやpamの設定済み
  - unixパスワードとの同期設定済み
  - 初期ユーザ設定済み
- OpenSUSEの流儀に
  - yastのコマンドラインインタフェースで設定
  - pam関係の設定ファイルをいじる必要はなし
  - Red Hat(CentOS)とはかなり異なる

ゴミ箱機能

- ご存じネットワークドライブ上のゴミ箱機能
- recycletest 共有に設定済み
- ファイルを消すと.recycleに移ります
- 一通りのことは出来ます
- 掃除するスクリプトは仕込んでいません

アクセス制御

- groupsという共有
  - smb.confパラメータによる制御
    - read only,write list,read list invalid users
  - UNIX本来のアクセス制御
    - owner,group,otherに対してrwx（と t）
  - ACL
- これらを組み合わせた例を設定しています
  たとえば……

パズル

/home/groups

```
# file: groups
# owner: root
# group: users
# flags: --t
user::rwx
user:ldap03:rwx
group::rwx
mask::rwx
other::r-x
```

smb.conf

```
read only      = Yes
write list     = @ldapg1
invalid users = ldap11
read list      = ldap12 ldap13
```

user	group
ldap01	domusers
ldap02	domusers,ldapg1
ldap03	domusers,ldapg1
ldap11	domusers,ldapg2
ldap12	domusers,ldapg2
ldap13	domusers,ldapg2

答え(1)

- ユーザldap01は、このディレクトリを読めますが書き込めません。

```
# file: groups
# owner: root
# group: users
# flags: --t
user::rwx
user:ldap03:rwx
group::rwx
mask::rwx
other::r-x
```

user	group
ldap01	**domusers**

```
read only       = Yes
write list      = @ldapg1
invalid users = ldap11
read list       = ldap12 ldap13
```

答え(2)

- ユーザldap02は、ディレクトリのアクセス権にwが無いので書き込めません。

```
# file: groups
# owner: root
# group: users
# flags: --t
user::rwx
user:ldap03:rwx
group::rwx
mask::rwx
other::r-x
```

user	group
ldap02	**domusers,ldapg1**

```
read only      = Yes
write list     = @ldapg1
invalid users = ldap11
read list      = ldap12 ldap13
```

答え(3)

- ユーザldap03は書き込み可能です。

```
# file: groups
# owner: root
# group: users
# flags: --t
user::rwx
user:ldap03:rwx
group::rwx
mask::rwx
other::r-x
```

user	group
ldap03	**domusers,ldapg1**

```
read only      = Yes
write list     = @ldapg1
invalid users = ldap11
read list      = ldap12 ldap13
```

答え(4)

- ユーザldap11はアクセスできません。

```
# file: groups
# owner: root
# group: users
# flags: --t
user::rwx
user:ldap03:rwx
group::rwx
mask::rwx
other::r-x
```

user	group
ldap11	**domusers,ldapg2**

```
read only      = Yes
write list     = @ldapg1
invalid users = ldap11
read list      = ldap12 ldap13
```

答え(5)

- ユーザldap12,ldap13は読み込み可能です。

```
# file: groups
# owner: root
# group: users
# flags: --t
user::rwx
user:ldap03:rwx
group::rwx
mask::rwx
other::r-x
```

user	group
ldap12	**domusers,ldapg2**
ldap13	**domusers,ldapg2**

```
read only       = Yes
write list      = @ldapg1
invalid users = ldap11
read list       = ldap12 ldap13
```

監査機能

- vfstestという共有
- vfsモジュール
  - audit
  - extd_audit　　今回はこれを使用
  - full_audit
- 粒度が違う
- syslogに出るので後でログインして確認

ログの例

```
[2010/09/05 22:17:30,  1, pid=30946, effective(50001, 50000), real(0, 0)]
 modules/vfs_extd_audit.c:174(audit_opendir)
  vfs_extd_audit: opendir ./
[2010/09/05 22:17:30,  2, pid=30946, effective(50001, 50000), real(0, 0)]
 modules/vfs_extd_audit.c:235(audit_open)
  vfs_extd_audit: open newtext.txt
[2010/09/05 22:17:30,  2, pid=30946, effective(50001, 50000), real(0, 0)]
 smbd/open.c:580(open_file)
  ldap01 opened file newtext.txt read=Yes write=No (numopen=2)
[2010/09/05 22:17:30,  1, pid=30946, effective(50001, 50000), real(0, 0)]
 modules/vfs_extd_audit.c:174(audit_opendir)
  vfs_extd_audit: opendir ./
[2010/09/05 22:17:30,  1, pid=30946, effective(50001, 50000), real(0, 0)]
 modules/vfs_extd_audit.c:174(audit_opendir)
  vfs_extd_audit: opendir ./
[2010/09/05 22:17:30,  1, pid=30946, effective(50001, 50000), real(0, 0)]
 modules/vfs_extd_audit.c:174(audit_opendir)
  vfs_extd_audit: opendir .
```

username map 機能

- 2つのマッピング方法
  - username map (static)
  - username map script (dynamic)
- 同時共存は可能です
- 「ldapuser」を「ldap01」と透過になるstaticな設定がなされています。

その他

- 日本語マニュアル
  - 3.4系列の最終版
  - 3.4.3とはほとんど差はない
  - (翻訳の)バグ修正程度
- OpenSUSEの場合、二つ以上選択可能なものについては、manコマンド実行時に1アクション増えるので注意

オプション

- ソースファイルの閲覧
  - samba 3.4.3 を globalで処理したもの
  - webアクセス経由
  - 量が大きいので別パッケージ
  - apache起動済み、ファイルをインストールするだけ
  - cgiは設定していません

Samba評価環境のインストール

- 用意するもの
  - VMware Workstation(たぶん5.5以降)
  - Vmware Player(たぶん3以降)
  - 2Gぐらいのディスク容量(MAX 8G)
  - VMイメージのZIPファイル(samba.gr.jpから)
- ZIPファイルを解凍するだけ
- Webページを読んで、rootのパスワードやその他の設定情報を確認

最初にやること

- ネットワーク設定ファイルの初期化
  - VMパラメータの調整
  - /etc/udev/rules.d/70-persistent-net.rules ファイルを削除。その後再起動。
  - rootでログイン。/root/sambasetup.sh を実行 。
  - これで、設定が初期化されます。

使用法

- すでにドメインの設定が終わっています。
- Windows クライアントから、ドメインに参加してください。
- Windows XP、Windows 7で確認済みです。
- そのほか、各機能はWindowsから、あるいはログインしてから使えます。

動作の詳細

- 初期化スクリプト
- 設定の要点
- 各共有毎の設定
- オプション

初期化スクリプト

- オリジナルは 堀田@net-newbieさんが作られたもの
- 大幅に手直し
  - OpenSUSE(SuSE Studio)対応
  - 全部スクリプトないで処理しない(一部は別ファイル)
  - メッセージの英文化(world wide対応?)
  - 機能追加、繰り返し初期化可能、エラーチェック等

スクリプト内のPAM設定

- 昔
  手で直す(/etc/pam.d/system-authなど)
- 堀田さんのスクリプト
  Red Hat(CentOS)の設定コマンド
- Samba評価環境(V3)
  あらかじめ設定済み
- Samba評価環境(V4)
  YASTによる設定

スクリプト内のLDAPの設定

- slapd.confはOpenSUSEのものを流用
  - Samba用にいくつか修正
- スキーマが大問題
  - Red Hat(CentOS)とOpenSUSEではスキーマが違う
  - RFC2307とRFC2307bis
    - posixGroupがstructual ではなくなった
    - そのままではSambaのスキーマ利用時にエラー
    - 結局Sambaにパッチ当て
  - 評価環境にはパッチ当てたものが入ってます

RFC2307bisについてもうちょっと

- 詳しくは日本LDAPユーザ会の技術情報を
  http://www.ldap.jp/_media/doc/rfc2307diff.xls
- 一番大きな違い
  - posixGroup STRUCTURALから AUXILIARY
  - ldapsam:editposix に影響
    - net sam provision コマンド内で既定値のエントリを作成出来ない
  - BugID #4597で報告あり
    - 結論は出ていない(未クローズ)

ソースの当該箇所

```
d_printf(_("Adding the Domain Users group.¥n"));
/* 略 */
uname = talloc_strdup(tc, "domusers");
wname = talloc_strdup(tc, "Domain Users");
dn = talloc_asprintf(tc, "cn=%s,%s", "domusers", lp_ldap_group_suffix());
gidstr = talloc_asprintf(tc, "%u", (unsigned int)domusers_gid);
gtype = talloc_asprintf(tc, "%d", SID_NAME_DOM_GRP);
/* 略 */
smbldap_set_mod(&mods, LDAP_MOD_ADD, "objectClass", LDAP_OBJ_POSIXGROUP);
smbldap_set_mod(&mods, LDAP_MOD_ADD, "objectClass", LDAP_OBJ_GROUPMAP);
smbldap_set_mod(&mods, LDAP_MOD_ADD, "cn", uname);
smbldap_set_mod(&mods, LDAP_MOD_ADD, "displayName", wname);
smbldap_set_mod(&mods, LDAP_MOD_ADD, "gidNumber", gidstr);
smbldap_set_mod(&mods, LDAP_MOD_ADD, "sambaSid",
            sid_string_talloc(tc, &gsid));
smbldap_set_mod(&mods, LDAP_MOD_ADD, "sambaGroupType", gtype);
talloc_autofree_ldapmod(tc, mods);
rc = smbldap_add(ls, dn, mods);
```

OpenSUSE固有の問題

- OpenLDAPのスキーマをどうするか
  - 世の中一般的なスキーマ
    - core.schemaとかnis.schemaとか
  - アプリケーション固有のスキーマ
    - samba.schema
  - RFCで定義
  - RFC2307とRFC2307bis
    - RFC2307bisの方が機能が多い
    - 先走り
    - 結局失効

V4での解決策

- スキーマを変えるか、ソースを変えるか
- smb.confに対するパラメータの追加
  - editposix_rfc2307bis
    - namedObject と groupOfNames が選べる
    - 両者ともSTRUCTUALなオブジェクトクラス
    - 副作用が(たぶん)ない(MUSTが少ない)
- 変更は意外と簡単
  - smb.conf中のパラメータを評価する関数
  - ソース中ほぼどこでも使える

smb.conf

- 機能に応じた共有を設定
  - [groups]
    - read only,write list,invalid users,read list等
  - [recycletest]
    - recycle:repository = .recycleなど
  - [vfstest]
    - vfs objects = extd_audit
  - そのほかに、profiles,homesも定義済み

まとめ

- とりあえず使うための環境
- テストしたり、デバッグしたり
- 繰り返し使える

- Sambaはいろいろな機能を持っています
  だから、

答は、やってみなくちゃわからない

Sambaドメイン評価環境で

リソース

- ドメイン評価環境のページ
  - http://wiki.samba.gr.jp から
    プロジェクト->Sambaドメイン評価環境プロジェクト
- メーリングリスト
  - samba-jp ML
    (http://cgi.samba.gr.jp/mailman/listinfo/samba-jp)
- SuSE Studio
  - http://susestudio.com/

ご静聴ありがとうございました

日本 samba ユーザ会

http://wiki.samba.gr.jp