

新ユーザー管理システム

HSL 鈴木 平成 15 年 8 月 6 日(水)

新ユーザー管理システムは、WindowsNT や、Windows2000Server 及び Linux (RedHat9.0) の統合環境を実現するものです。但し、グループポリシーなど一部機能については Windows2000Server のみで行うものとなっています。

1. Windows 系と Linux 系の認証方法概要

Windows 系と Linux 系 (以降 Win 系と Linux と呼びます) が混在する認証統合環境は大変複雑です。現在、よく専門雑誌などに幾つかの認証統合の方法が特集されますが、それぞれ長所短所があり、物理的な各サーバーの環境によって一概にどれが一番良い方法かは決められません。初期の検討をする上で、まず分ける方法を考えるとしたら、各サーバー構成で以下の方法があると思います。

① Win 系のサーバーは無く、NT ドメインと同等の認証をする場合

ドメインコントローラー (以降 DC) の代わりに Samba を DC として使う方法があります。Samba 2.2.4 以降では Win 系からドメインログオン、ログオンスクリプト、移動プロファイル等で、ファイルサーバーやプリンタサーバーを作れます (2003 年 7 月末時点の最新は Samba 2.2.8a)。ただし、Samba サーバー以外に Linux クライアントがある場合は、別途 Linux 用のアカウント管理が必要です。

② Win 系のサーバーがあり、Win 系と Linux がある場合

Win 系で DC があるときは、Linux で Winbind 機能を使うことで、Linux クライアントから DC を通して動的のアカウント認証が行えます。但し、動的のアカウントであるが故に、各 Linux での同名アカウントであっても UID、GID が一致せず、そのアカウント名で NFS を使うことが出来ないため、サーバーに各アカウントのホームディレクトリを共通に持つ方法が難しくなります。

③ Win 系サーバーと Linux サーバーが混在する場合 1

Win 系から DC 機能を付けず、Linux に LDAP サーバーを作ることで、Win 系クライアントと Linux クライアントの両方から同一アカウント認証が行えます。Windows2000Server の ActiveDirectory にも内部に LDAP 機能がありますが、Linux に LDAP クライアント設定を行っても認証が出来ませんでした。既存の Win 系で既に DC を運用している場合では Linux LDAP との混在が、まだ不透明な部分が多くので難しいです。

④ Win 系サーバーと Linux サーバーが混在する場合 2

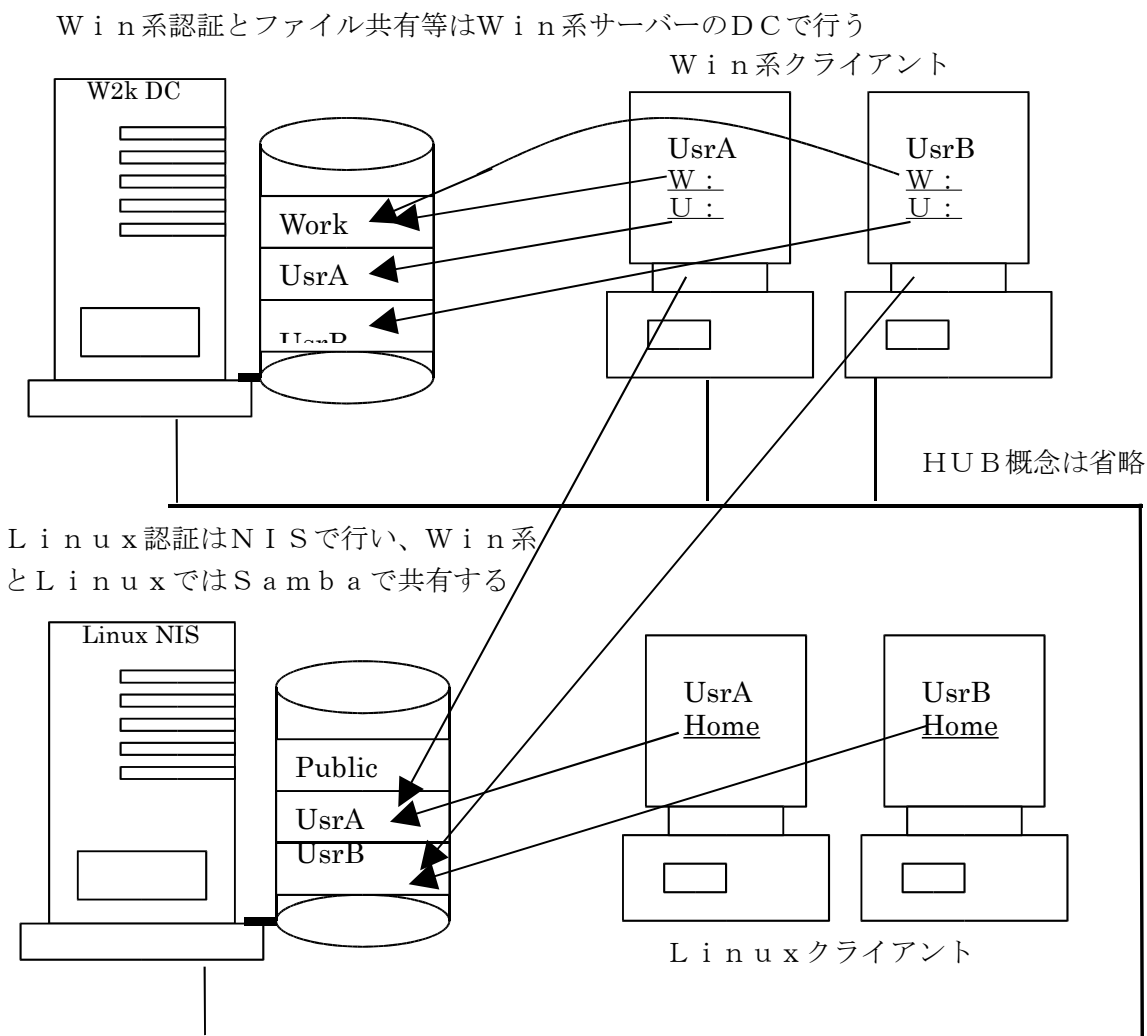
既存の Win 系で既に DC を運用している場合では、Linux サーバーに NIS サーバーと Samba サーバーを作り、Win 系クライアントは DC 認証により、Win 系サーバーと Samba によるファイルサーバーを使えるようにします。

Linux クライアントでは NIS 認証により、NFS で Linux サーバーにあるホームディレクトリを共有化します。

LinuxでNFSとしてエクスポートしている部分をSambaでも同アカウント名のホームディレクトリとすることでWin系クライアントとLinuxクライアントの同アカウントデータを共有します。

2. 今回行う認証統合方法

今回は上記④の認証統合を行います。以下にシステム概要図を記載します。



※Win系からLinuxファイルの読書きと、そのファイルをLinuxからの読書きは、Sambaの機能により日本語ファイル名を正常に読書きできますがLinuxからWin系ファイルサーバーの日本語ファイル名は文字が正常に読み取れません。

これはWin系がシフトJISコード、Linux (UNIX) 等がEUCコードを使っている為で、SambaはWin系で作られたシフトJISコードをLinuxで表示するときEUCに変えているからSambaからのみ表示出来るのです。

3. 設定方法

具体的な設定方法ですが、W i n系DCとW i n系クライアント設定については割愛します。

尚、以降のディレクトリ位置はR e d H a t 9でツールやアプリケーションを標準に組み込んだ場合のディレクトリ名で説明します。

3.1 L i n u xサーバーのS a m b a認証設定

これはW i n系クライアントがL i n u xサーバーのファイルやプリンタ共有をするために行うものです。これによってL i n u xサーバーに作られる同名アカウントを同じアカウントとして自動認証します。

①ファイル/etc/hostsにDCのホスト名とIPアドレスを記載する。

```
192.168.2.121    sa1 sa1.jh.loc
```

②ファイル/etc/samba/lmhostsにDCのホスト名とIPアドレスを記載する。

```
192.168.2.121    sa1
```

※hosts, lmhostsはDNSやWINSが動いており、それらサーバーにDCが登録されている場合にはsmb.confに以下を設定することでこの作業が不要となります。

smb.confに wins server = 192.168.2.121 等とWINSサーバーを指定できる。

③ファイル/etc/samba/smb.confの[global]セッション設定

これらの設定は、このファイルでマスクされている場合があるので一度検索して、無ければ追加するようにしましょう。

- ・セキュリティーモードとパスワードサーバー指定

```
security = DOMAIN
```

```
password server = SA1
```

(サーバ名の代わりに*をすると探します。また複数指定も出来ます。)

- ・暗号化パスワード指定とS a m b a側のパスワード保存場所指定

```
encrypt passwords = yes
```

```
smb passwd file = /etc/samba/smbpasswd
```

- ・ドメイン名かワークグループ名指定

```
workgroup = JH
```

- ・S a m b a側のディレクトリやファイル名に日本語を使うための設定

```
coding system = EUC
```

```
client code page = 932
```

※この他の[global]セッション設定についてはデフォルトのままで良い。

④W i n系に共有させるディレクトリの指定

- ・各アカウント名のホームディレクトリ指定

```
[homes]
comment = Home Directories
browseable = no
writable = yes
valid users = %S
create mode = 0664
directory mode = 0775
```

自分以外のアカウントからは見せない設定です。

- ・全員が使えるワーク用のディレクトリを作る場合

共有ディレクトリ名： s a 3 - p u b

```
[sa3-pub]
comment = Public Stuff
path = /home/sa3-pub
public = yes
writable = yes
printable = no
guest ok = yes
force create mode = 0666
force directory mode = 0777
```

共有するディレクトリは予め作成してき、読書き全てOKとする場合は、ディレクトリの属性もそれに合わせる。
これをW i n系で例えると左記の指定は共有での読書き指定であり、このディレクトリ属性はW i n系セキュリティと同等です。

- ・共有プリンタ[printers]設定（デフォルトで共有可能）

```
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
# Set public = yes to allow user 'guest account' to print
guest ok = no
writable = no
printable = yes
```

⑤ S a m b a サーバーをW i n 系D C にファイルサーバーとして登録

例としてD C のドメイン名をJ H、ホスト名をS A 1として記載します。

D C の管理者アカウントに administrator を使いますが、ドメイン管理者権限があれば別のアカウントでもOKです。

S a m b a 側のスーパーユーザーで以下のコマンドを実行

```
# smbpasswd -U administrator -j JH -r SA1 「リターン」
Password: (パスワードを入れる)
Joined domain JH. (これが出ればOK)
```

⑥アカウントの自動作成と削除

実はS a m b a では、L i n u x 側にも同アカウント名を登録しておかないとW i n 系側からのアクセスは出来ません。方法としてL i n u x にアカウントの自動作成と削除用スクリプトを作り、ファイル/etc/samba/smb.confの[global]セッションに以下の2行を加えます。

```
add user script = /etc/samba/smb-uadd %u
delete user script = /etc/samba/smb-udel %u
```

・アカウント作成スクリプト

```
#!/bin/sh
#
useradd -s /bin/bash -d /home/smb-pub/$1 $1
passwd -fu $1
mkdir -p /home/smb-pub/$1
chown $1 /home/smb-pub/$1
#
# 以下はN I S アカウント変換のため
cd /var/yp
make
```

・アカウント削除スクリプト

(但し、これは必須ではありません。)

```
#!/bin/sh
userdel $1
rm -rf /home/smb-pub/$1
```

3.2 LinuxのNISサーバー設定

NISはUNIXがNISドメイン内で複数のワークステーションでのユーザー管理を統一する上で古くから使われているものです。以下にNIS設定を記載します。

尚、NISとは別ですが、今回シャドウパスワードを使わないようにするので以下のコマンドでシャドウパスワードを使わない変更をしています。

```
# pwunconv (逆に使う場合の変更は pwconv を使う)
```

①NISドメインの設定

ファイル `/etc/sysconfig/network` に以下を追加する (ドメイン例: `sa3nis`)

```
NISDOMAIN = sa3nis
```

また、コマンドラインから以下を実行すると直ぐに反映される。

```
#domainname sa3nis
```

②NISの起動

NISは本体サービスの `ypserv`、`ypxfrd`、パスワード変更用に `ypasswdd` を起動する。GUIのサービスマネージャを使っても良いが、コマンドで行う場合は以下である。

```
# /sbin/chkconfig --level 35 ypserv on
```

```
# /sbin/chkconfig --level 35 ypasswdd on
```

```
# /sbin/chkconfig --level 35 ypxfrd on
```

③アカウントファイルの初期化

- ・ファイル `/var/yp/securenets` で使用ネットワークを指定 (例: `192.168.2.0`)

```
255.0.0.0 127.0.0.0
```

```
255.255.255.0 192.168.2.0
```

- ・ファイル `/var/yp/Makefile` の修正 (例: シャドウパスワードを使用しない)

```
shadow = false
```

```
gshadow = false
```

- ・これらで初期化する

初期化は以下のコマンドを実行すると内部で `make` も実行される。

```
# /usr/lib/yp/ypinit -m
```

※`make` は `passwd` ファイルにユーザーを追加する度にNISに反映させるために必要となります。手動コマンドで行う場合は以下を実行しますが、今回は `Samba` でスクリプトとして自動で実行しています。(3.1の⑥を参照)

```
# cd /var/yp
```

```
# make
```

④ホームディレクトリ用のエリアをエクスポート

N I Sサーバー設定とは別ですが、クライアントのホームディレクトリをサーバー側に作れば、あるユーザーが別のL i n u xマシンからログインしても自分のデータや使用環境を同じに使えます。

- ・ファイル /etc/exports を編集する。

ここでは smb-pub をネットワーク 192.168.2.0 からアクセス可能で読書きOKと sa3-pub をホスト sa4 だけからアクセス可能で読書きOKとしています。

/home/smb-pub/	192.168.2.0/255.255.255.0(rw,sync)
/home/sa3-pub/	sa4(rw,sync,no_subtree_check)

- ・反映させるためのコマンドを実行

```
# exportfs -a
```

尚、G U IにあるN F Sサーバーツールでは設定すると内部的に exportfs -a まで行っているのG U Iの方が簡単です。

コラム

L i n u x (U N I X) の歴史がコンピュータとしては長いため殆どがコマンドレベルで設定が出来ます。X W i n d o w系の発達により、G U Iでも設定が出来るが、細かな調整にはコマンドの方が便利か、コマンドでしか出来ないものがあります。

G U IにS a m b aサーバーのツールもありますが、今回の様に日本語設定やスクリプト追加など様々なことはテキスト設定ファイルを編集して行うしか出来ません。また、注意点としては、テキスト設定ファイルを編集した後で、G U Iツールを起動して保存すると、手動で編集した部分が消される場合があります。

全てではないですがS a m b aサーバーのツールはこのタイプなので、G U Iは使わないで下さい。

N F Sサーバーは単純なのでどちらで行っても問題はありません。

N I Sとは無関係ですが、その他としてプリンターなどを設定追加出来るG U Iが良く成っています。

R e d H a t 9ではかなり最近のプリンタドライバまで用意されているので、ウィザードを使ってメーカーとプリンタ種類すれば設定できます。

3.3 LinuxのNISクライアント設定

NISクライアントはOSのインストール時であればNISドメイン名とNISサーバー名を記載するだけで簡単に設定が出来ます。今回はインストールが済んでいるものにNISクライアント設定をするもので説明します。

- ①ファイル/etc/hosts にホスト名とIPアドレスを記載する。

```
127.0.0.1    cc01 localhost          (例 : cc01)
192.168.2.121 sa1 sa1.jh.loc
192.168.2.123 sa3 sa3.jh.loc          (NISサーバー)
```

- ②ファイル/etc/fstab でNFSサーバーにあるホームディレクトリをマウント設定

```
sa3:/home/smb-pub /home/smb-pub nfs auto,rw 0 0
```

マウントするには、ローカルに/home/smb-pubディレクトリを作っておく

```
# mkdir /home/smb-pub
```

これでコマンドで `mount -a` を行えばマウント可能ですが、`fstab` に記載しておけば、次回起動時にはマウントされています。もしマウントされないときはNFSサーバーの `exports` 設定を再度確認する必要があります。(3.2の④を参照)

- ③ファイル/etc/nsswitch.confでNIS指定

```
passwd:    files nis
group:     files nis
```

- ④ファイル/etc/yp.confのNISドメイン設定

```
domain sa3nis server sa3
```

- ⑤ファイル/etc/sysconfig/networkにNISドメイン設定

```
NISDOMAIN = sa3nis
```

- ⑥NISサービスの起動設定

```
# /sbin/chkconfig --level 35 ybind on
```

ご注意

この資料は、有限会社ヒューマンシステムラボが作成しているもので、著作権を有します。