Active Directoryはもういらない!!
Samba4最新情報

OSSTech

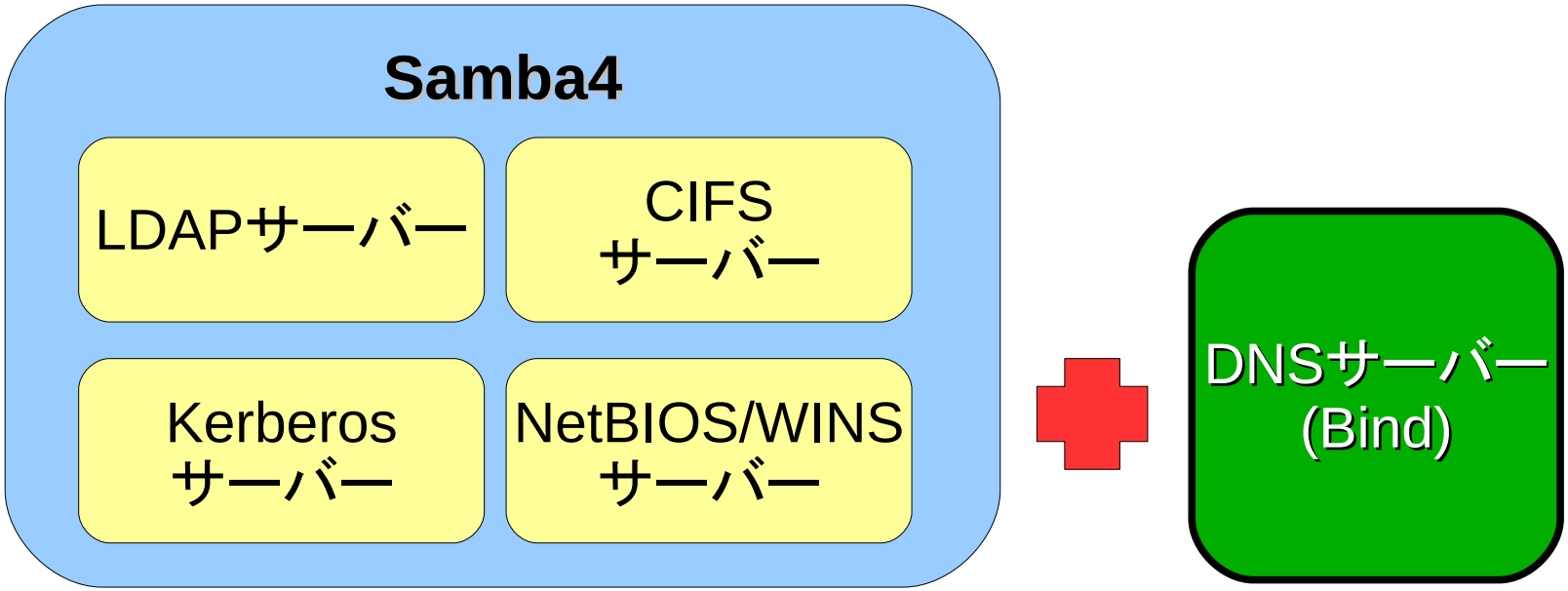
オープンソース・ソリューション・テクノロジ株式会社
2009/11/20
技術取締役 武田 保真

目次

- Samba4 サーバー設定方法
- Samba4 Active Directory機能確認結果

Samba4 概要

- Active Directoryドメインコントローラー機能サポート
  - 機能レベル: Windows2003～2008R2選択可能
- Samba4にDNS以外の機能を組み込み
  - LDAPのみ外部サーバーと連携可能



namedのアップデート

- Active Directoryで必要なDNSのGSS-TSIG更新に対応するbind-9.5.0以降が必要

```
# rpm -Uhv bind-9.6.1*rpm --nodeps
```

- caching-nameserverをインストール

```
# yum install caching-nameserver
```

Samba4 インストール手順(CentOS5)

- gitのインストール

```
$ wget http://download.fedora.redhat.com/pub/epel/5/i386/epel-release-5-3.noarch.rpm
# rpm -ihv epel-release-5-3.noarch.rpm
# vi /etc/yum.repos.d/epel.repo
  「enabled = 1」を「enabled = 0」に変更
# yum --enablerepo=epel install git
```

- samba4の最新ソースの取得

```
$ git clone git://git.samba.org/samba.git samba-master
$ cd samba-master
```

Samba4 コンパイル手順(CentOS5)

- develパッケージのインストール

```
# yum install libaio-devel
```

- samba4のコンパイル

```
# cd samba-master/source4
# ./autogen.sh
# ./configure
# make
# make install
```

provisioningコマンドによるセットアップ

- セットアップ前に/etc/hostsの設定

```
127.0.0.1       localhost.localdomain localhost
10.0.102.15     samba4-cent5.samba4.lan.osstech.co.jp samba4-cent
```

これを忘れると、作成されるnamed用のzoneファイルの
Aレコードが127.0.0.1で作成されてしまう

provisioningコマンドによるセットアップ

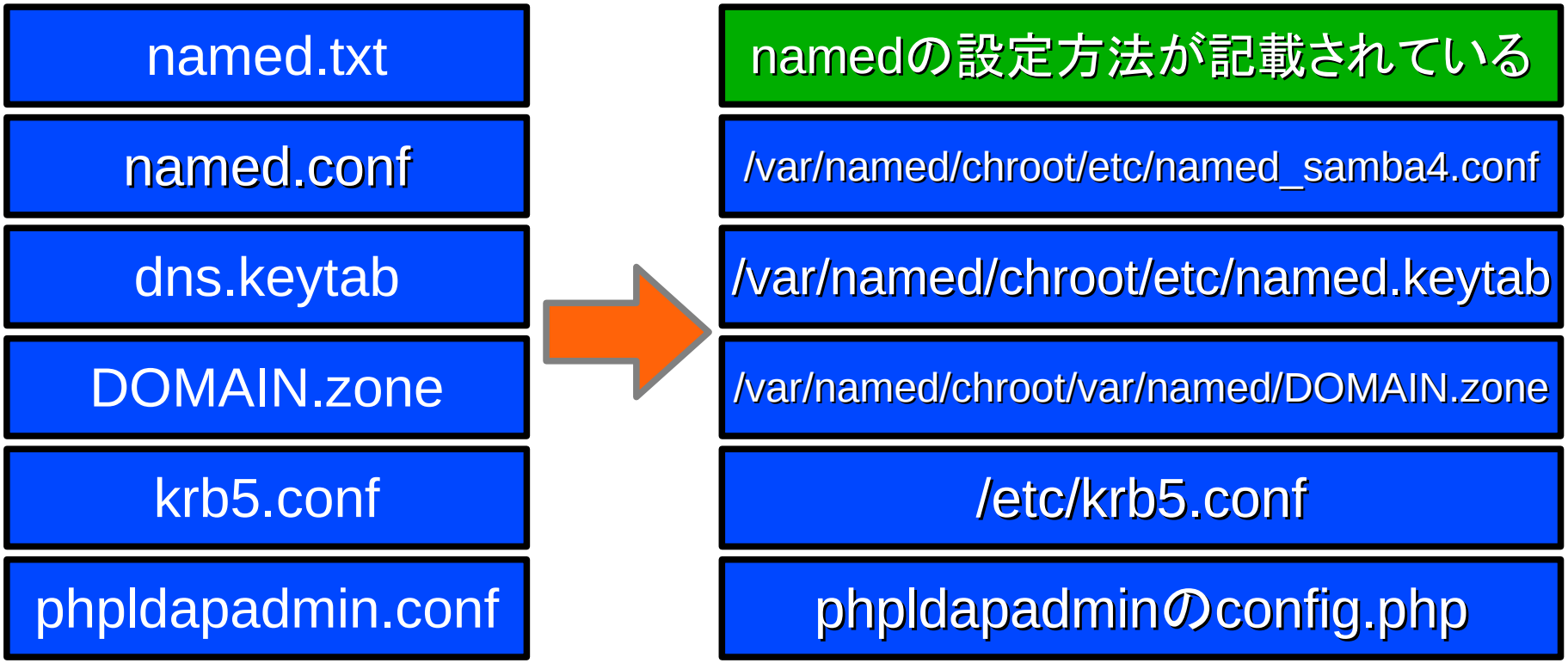
- --interactiveオプションで簡単セットアップ

```
# /usr/share/samba/setup/provision --interactive
Realm [SAMBA4.LAN.OSSTECH.CO.JP]:
 Domain [SAMBA4]:
 Server Role (dc, member, standalone) [dc]:
Administrator password: ********
... 省略 ...

Server Role:            domain controller
Hostname:               samba4-cent5
NetBIOS Domain:         SAMBA4-CENT5
DNS Domain:             samba4.lan.osstech.co.jp
DOMAIN SID:             S-1-5-21-1612879468-2748088164-743427320
Admin password:         secret123
```

各種設定ファイルの配置

- /var/lib/samba4/privateに以下の設定ファイルが自動作成されるので、適切な場所にコピー



namedの設定

- named_samba4.conf
  - zoneファイルのパスをchroot環境に合わせて修正
  - 逆引きのIPアドレスを設定

```
zone “samba4.lan.osstech.co.jp.” IN {
        type master;
        file “/var/named/samba4.lan.osstech.co.jp.zone”;
... 省略 ...

zone "102.0.10.in-addr.arpa" in {
        type master;
        file "102.0.10.in-addr.arpa.zone";
        update-policy {
                grant *.LAN.OSSTECH.CO.JP wildcard *.102.0.10.in-addr.arpa. PTR;
        };
};
```

namedの設定

- named.conf
  - ファイルの所有グループをnamedグループに設定
  - include /etc/named_samba4.conf を追加
  - named.confに、named.txtに記録されているtkeyの設定を追加

```
options {
        directory   “/var/named”;
        dump-file  “/var/named/data/cache_dump.db”;
        statistics-file          “/var/named/data/named_stats.txt”;
        memstatistics-file     “/var/named/data/named_mem_stats.txt”;
        tkey-gssapi-credential "DNS/samba4.lan.osstech.co.jp";
        tkey-domain "SAMBA4.LAN.OSSTECH.CO.JP";
};
view “internal” {
        match-clients { any; };
        include “/etc/named_samba4.conf”;
};
```

keytabファイルの設定

- namedでGSS-TSIG用のkeytabを利用可能に設定
  - 権限の変更

```
# chgrp named /var/named/chroot/etc/named.keytab
# chmod g+r /var/named/chroot/etc/named.keytab
```

- named起動

```
# /sbin/service named start
```

namedの動作確認

- Samba4サーバーのホスト名解決

```
# dig @localhost  samba4
```

- SRVレコードの確認

```
# dig @localhost _ldap._tcp.dc._msdcs.ドメイン名  SRV
... 省略 ...
;; ANSER SECTION
_ldap._tcp.dc._msdcs.samba4.lan.osstec.co.jp. 604800
IN SRV 0 100 389 samba4-cent5.samba4.lan.osstech.co.jp
```

- /etc/resolv.confの設定

```
search samba4.lan.osstech.co.jp
nameserver 127.0.0.1
```

ADサーバーの初期設定

- /etc/samba4/samba/smb.conf

```
[globals]
netbios name = SAMBA4-CENT5
workgroup = SAMBA4
realm = SAMBA4.LAN.OSSTECH.CO.JP
server role = domain controller
[netlogon]
        path = /var/lib/samba4/sysvol/samba4.lan....
        read only = no
[sysvol]
        path = /var/lib/samba4/sysvol
        read only = no
```

Sambaサーバーの起動

- Sambaサーバーの起動

```
# /etc/init.d/samba4 start
```

/usr/sbin/sambaデーモンが起動

- Sambaサーバーの動作確認

```
# wbinfo -u
Administrator
Guest
...
# smbclient //localhost/share -U Administrator
```

Samba 4のsmbdで起動されるサービス(1)

サービス名	役割	ポート番号
kdc	Kerberos認証サーバー(DCの時のみ)	TCP 88,464
ldap	LDAPサービス(DCの時のみ)	TCP 389
cldapd	CLDAPサービス(DCの時のみ)	UDP 389
winbindd	winbindサービス	unixソケット
smb	CIFS/SMBサービス	TCP 445,139
samba3	CIFS/SMBサービス(Samba3)	TCP 445,139
nbtd	NetBIOSサービス、WINSサービス	UDP 137,138
wrepl	WINSの複製機能	TCP 42

Samba 4のsmbdで起動されるサービス(2)

サービス名	役割	ポート番号
web	SWAT専用Webサービス	TCP 901
auth	内部認証バックエンド用サービス	無し
drepl	ディレクトリ複製サービス(DCの時のみ)	無し
kcc	KCCサービス(DCの時のみ)	無し
rpc	RPCサービス	動的変更
ntp_signd	内部時刻サービス	unixソケット

ユーザー登録 & パスワード変更

- ユーザー登録

```
# /usr/share/samba/setup/newuser tatsuya
New Password: ********
```

- パスワード設定

```
# /usr/share/samba/setup/setpassword tatsuya
New Password: ********
```

パスワードの有効期限変更

- パスワードの有効期限変更

```
# /usr/share/samba/setup/setexpiry tatsuya --days=30
```

- パスワードを無期限に変更

```
# /usr/share/samba/setup/setexpiry tatsuya --noexpiry
```

ドメインのパスワードポリシーの確認・設定

- パスワードポリシーの確認

```
# /usr/share/samba/setup/pwsettings show
Password complexity: on
Password history length: 24
Minimum password length: 7
Minimum password age (days): 0
Maximum password age (days): 42
```

- パスワードポリシーの設定

```
# /usr/share/samba/setup/pwsettings set --history-length=12
Password history lengt changed!
```

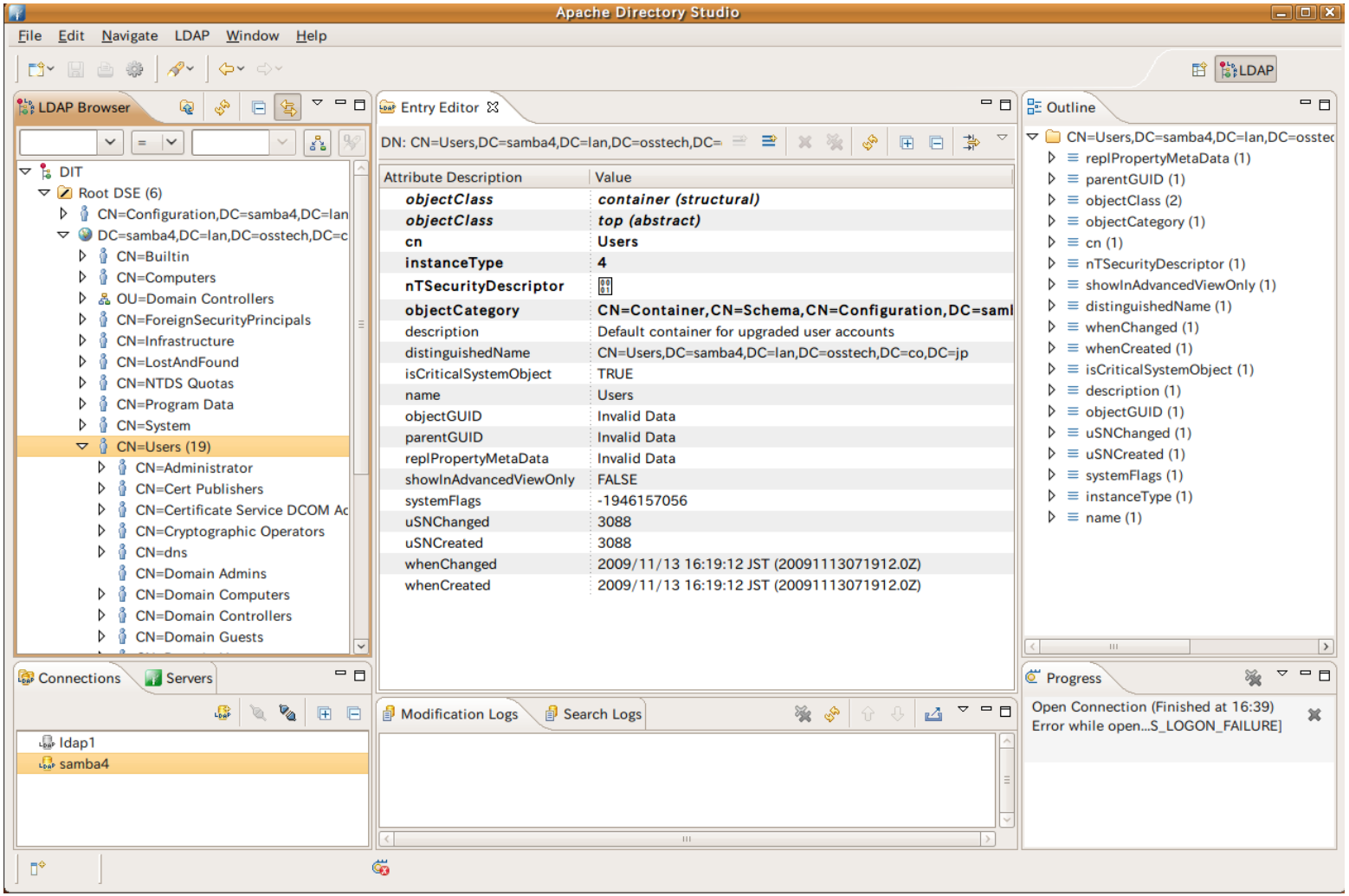
Samba4のデーター操作

- ldbコマンド
  - ldbsearchによる検索

```
# ldbsearch -H 'ldapi://%2Fvar%2Flib%2Fsamba4%2Fprivate%2Fldapi'
```

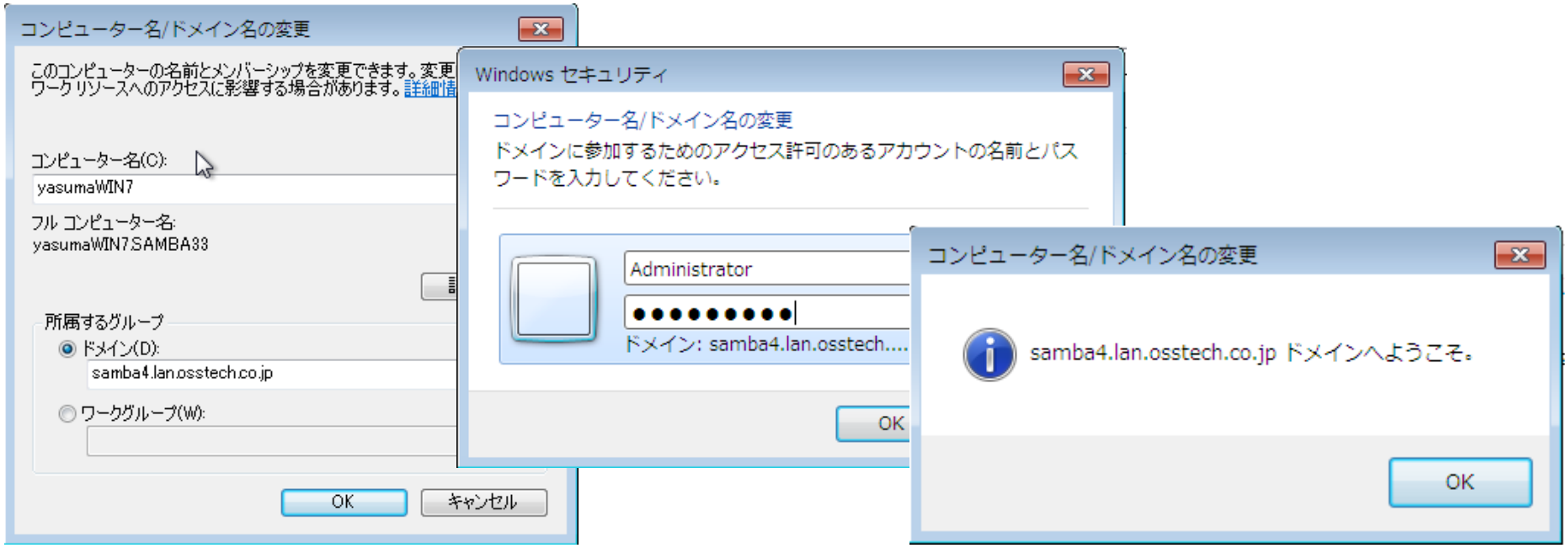
- LDAPクライアント
  - 管理者ユーザー名(次のどちらでも)
    - Administrator@ドメイン名 (Windows方式)
    - CN=Administrator,CN=Users,DC=samba4,DC=lan,DC=osstech,DC=co,DC=jp
  - 管理者パスワード　provisiningスクリプト実行時に設定

Samba4をApache Directory Studioで参照



Windows7をSamba4 ADドメインに参加

- 参照DNSサーバーをSamba4サーバーに設定
- Windows7端末の時刻をSamba4サーバーと同期
- Windows7をドメイン参加

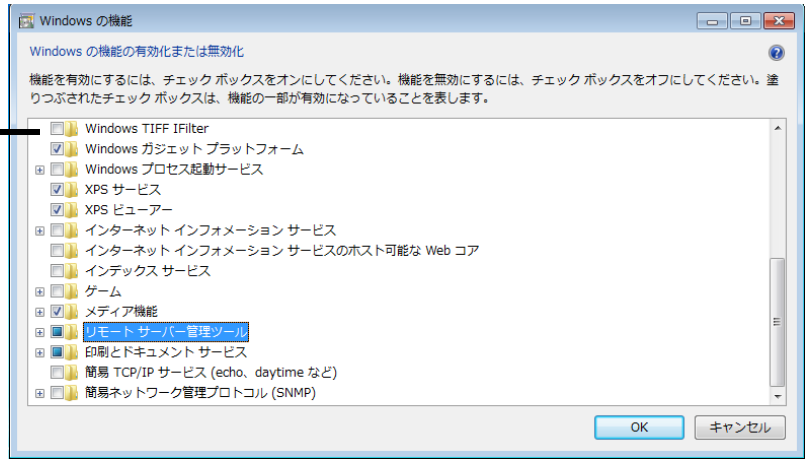


Windowsの管理ツール

- Windows Vista以降 RSATツールを利用
- Windows XP ... adminpakを利用

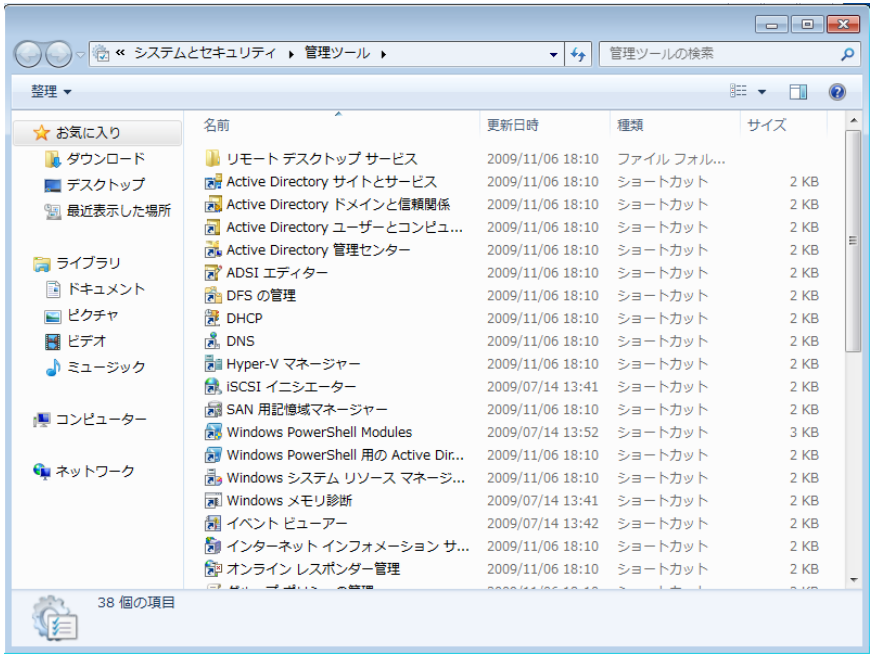
RSAT管理ツール URL
Windows Vista 32bit用
http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=9ff6e897-23ce-4a36-b7fc-d52065de9960
Windows 7 32bit用
http://www.microsoft.com/downloads/details.aspx?FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d&DisplayLang=ja

- RSAT管理ツールの有効化
  - 「コントロールパネル」-「プログラム」-「プログラムと機能」の「リモートサーバー管理ツール」を有効



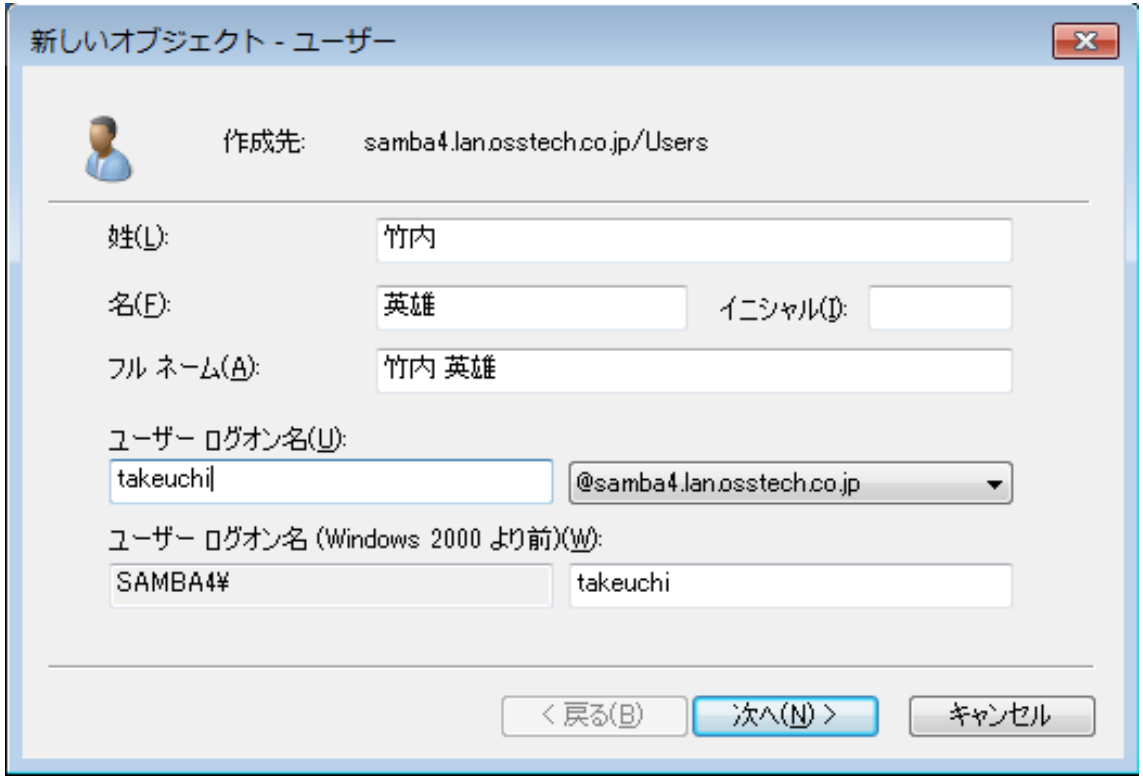
RSATによるSamba4サーバーの管理

- Windows7にドメインログオン
  - Domain\Administrator / パスワード
- 「コントロールパネル」-「システムとセキュリティ」-「管理ツール」



Active Direcotry ユーザーとコンピューター

- ユーザー管理
  - ユーザー作成、グループ作成、OU作成など問題なし

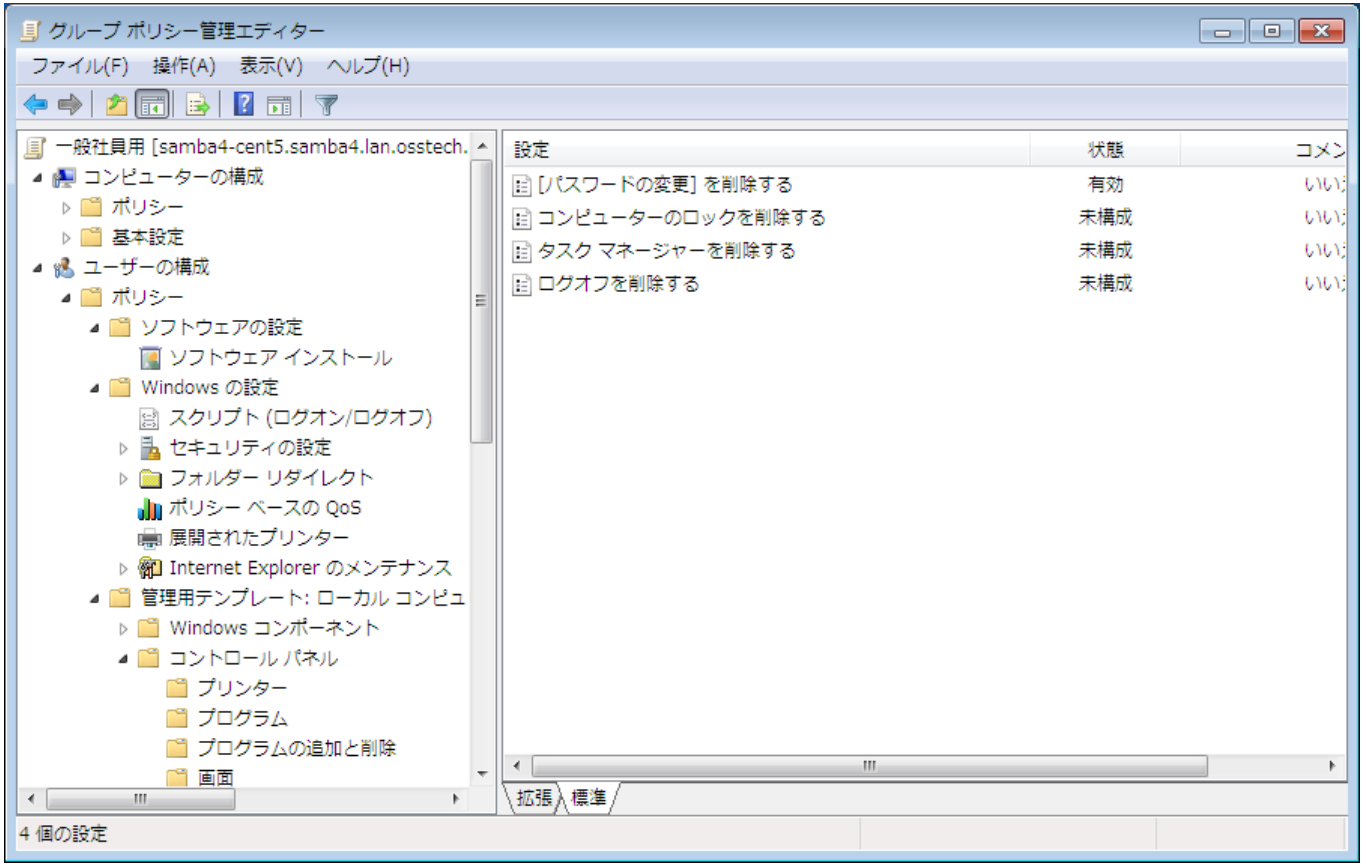


グループポリシーの管理

- グループポリシーの作成成功
- グループポリシーのモデル作成不可
- グループポリシーの結果ウィザード成功
- グループポリシーの適用成功
  - 「CTRL」+「ALT」+「Delete」のパスワード変更メニューを表示しない
  - リムーバブルデバイスの読み取りアクセスを拒否する

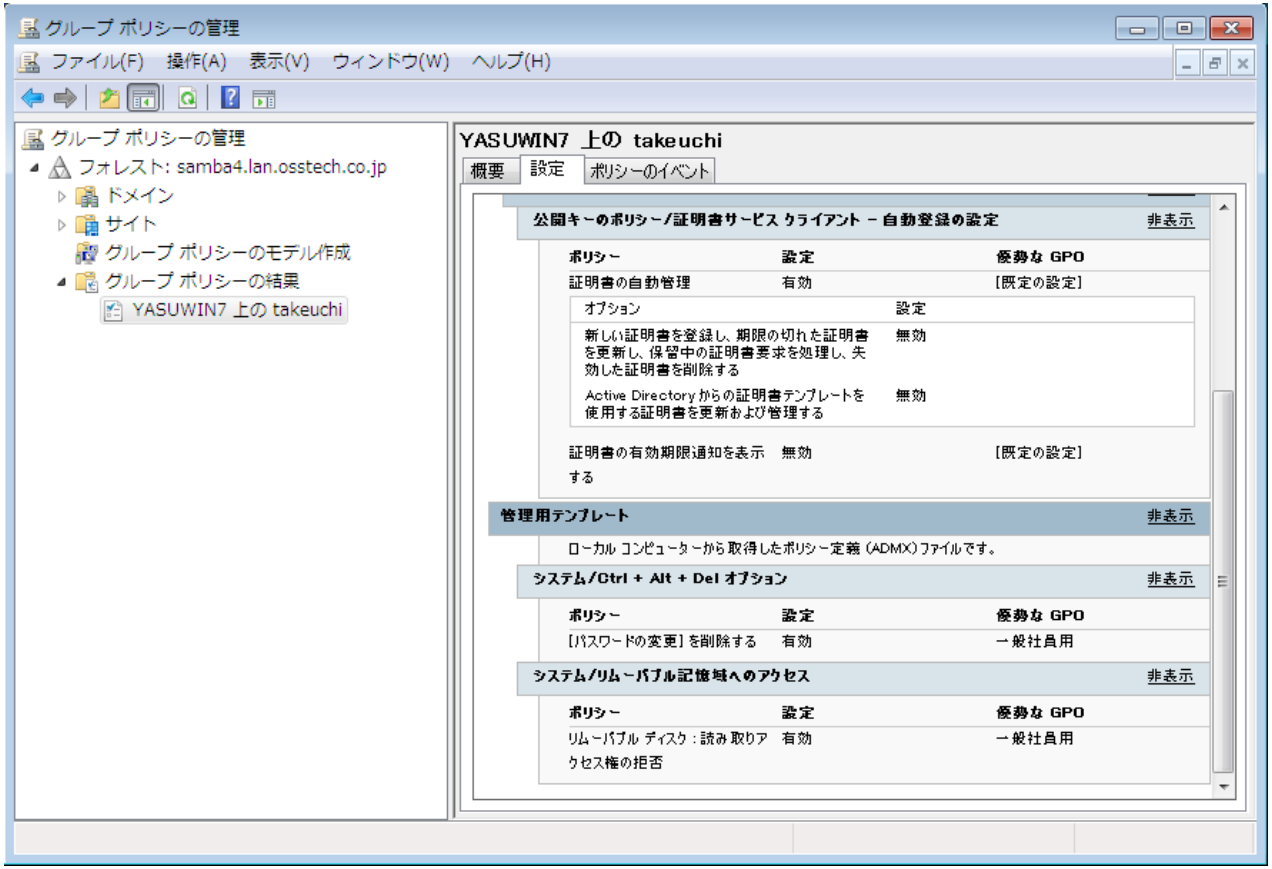
グループポリシーの管理

- グループポリシーの作成



グループポリシーの管理

- グループポリシーの結果ウィザード

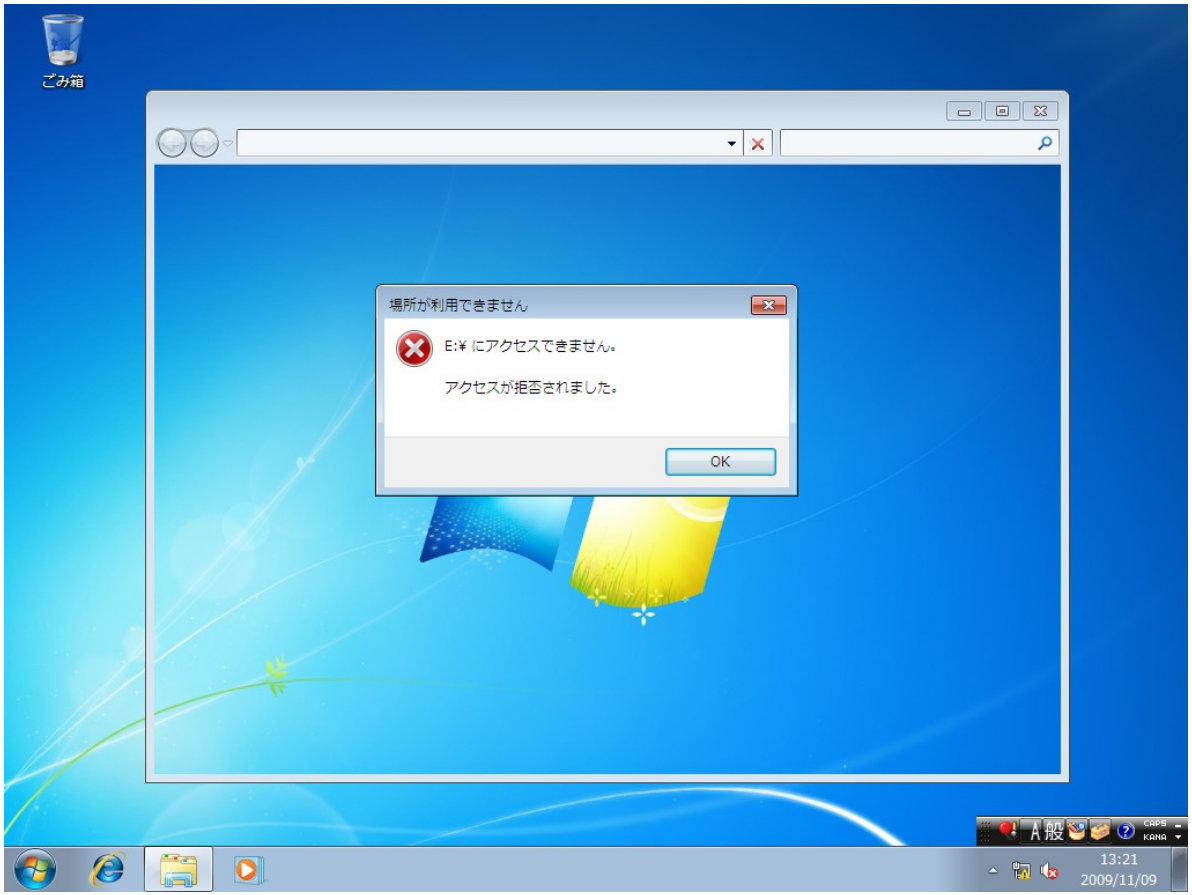


グループポリシーの適用確認

- パスワード変更メニューの非表示

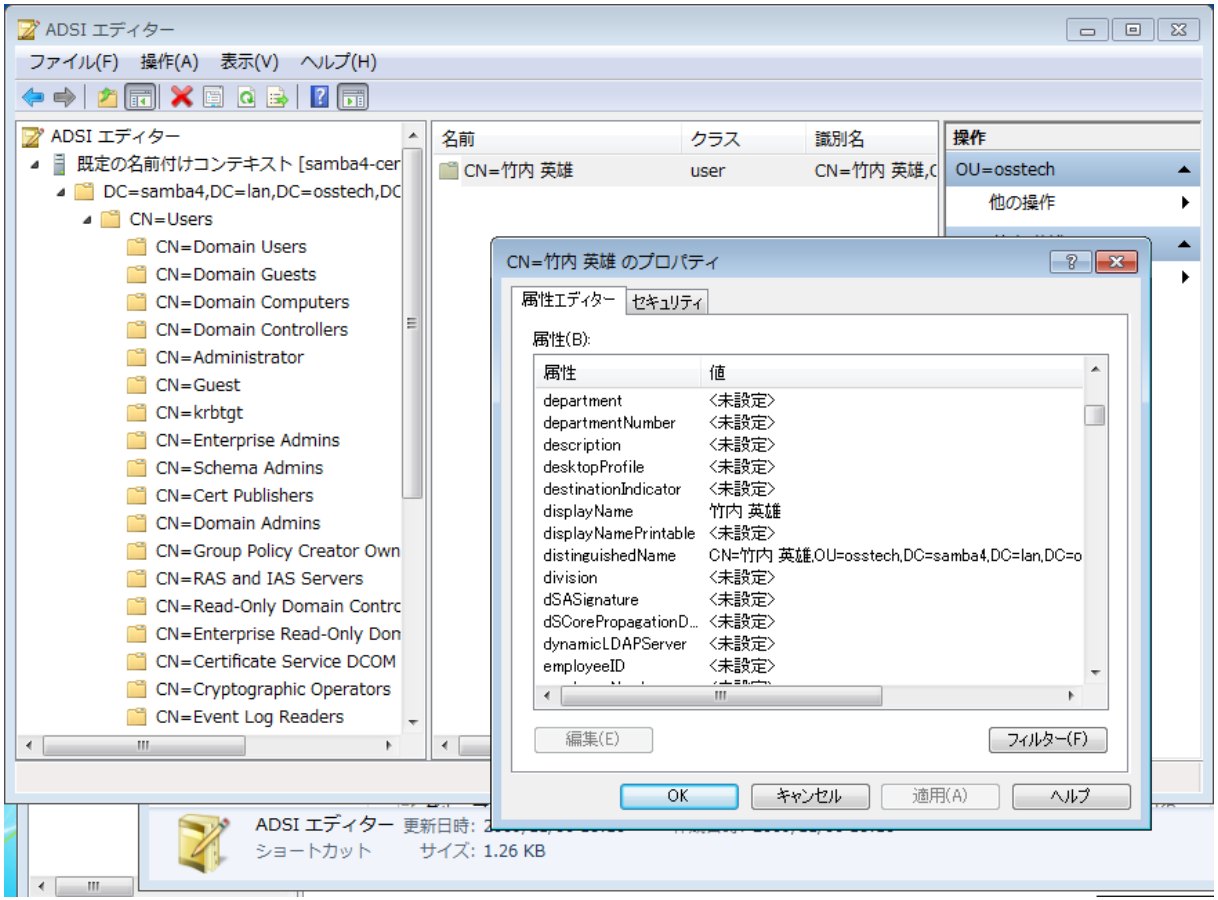
グループポリシーの適用確認

- リムーバブルデバイスの読み取りアクセス拒否



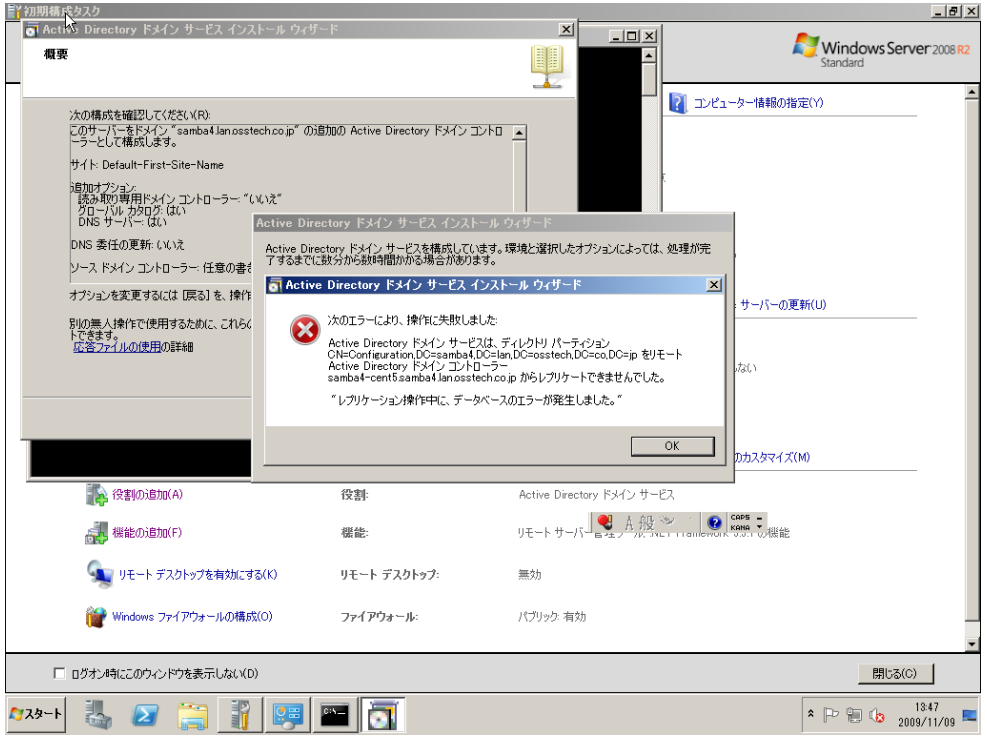
ADSIエディタ

- 値の変更も可能



Samba4 AD DC + Windows 2008 R2 DC

- Windows 2008 R2をSamba4のADドメインにdcpromo.exeで追加
  - ディレクトリのレプリケーションに失敗



Samba4 AD DC + Samba3 Winbind連携

- 特に問題無し

動作しなかったもの

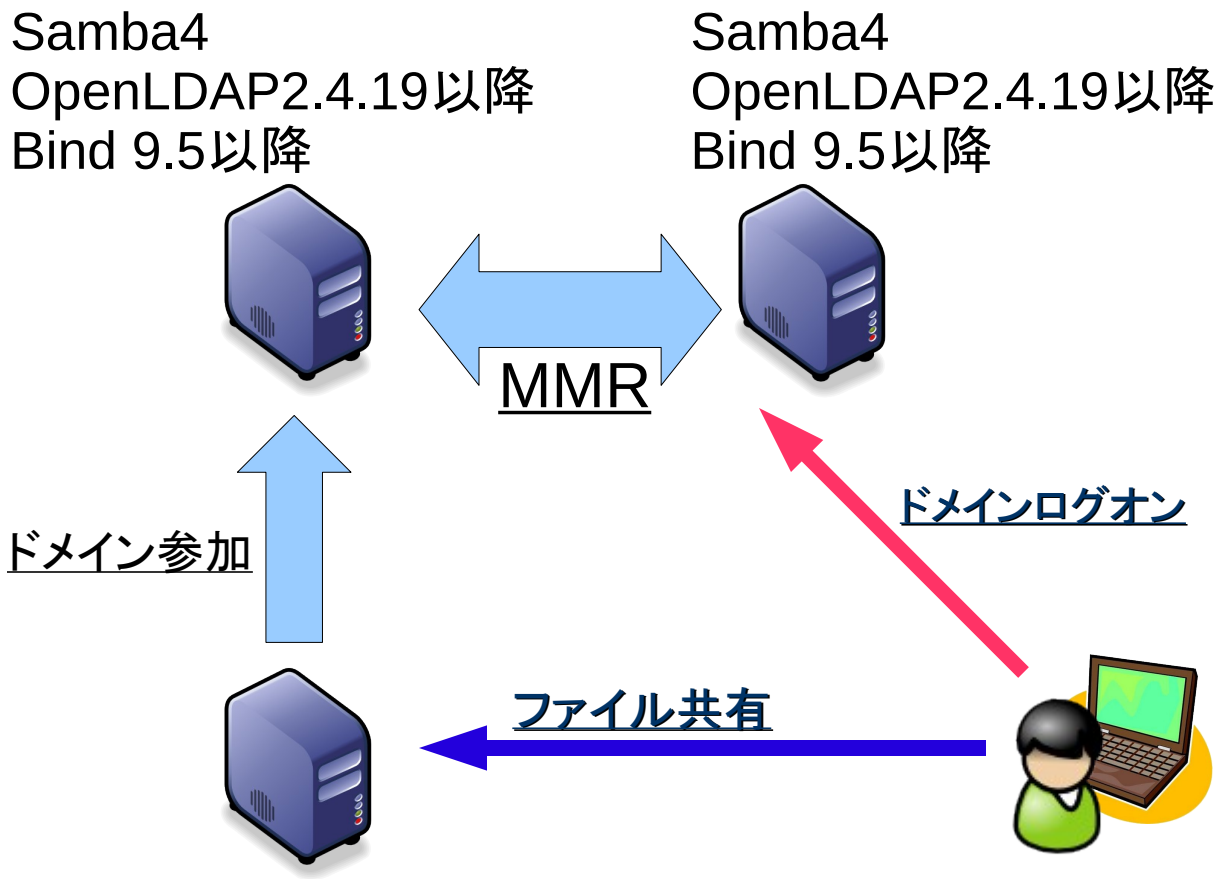
- 共有管理
  - 残念ながら動作せず
- イベントビューア

OpenLDAPバックエンドの利用

- OpenLDAP 2.4.17以降必須(2.4.19を推奨)
  - Samba4でderefオーバーレイが必要
- MMR(Multi Master Replication)対応
- 試してみたが、provisioningが正常終了せず
  - alpha9リリース時に再挑戦?

```
# /usr/share/samba/setup/provision --realm=samba4.lan.osstech.co.jp
 --domain=samba4 --ldapadminpass=secret123
 --ldap-backend-type=openldap --server-role='domain controller'
 --slapd-path=/opt/osstech/sbin/slapd
```

想定されるSamba4の利用形態



お試し用Samba4パッケージ

- CentOS5 (x86) 用
  - Samba4
    - OS標準のSambaパッケージのファイルを一部強制上書きインストールが必要なので、お試し専用
  - Bind 9.6.1

問題があっても自分で調査できる人向け
問い合わせをいただいても回答できません

http://www.osstech.co.jp/download/samba4/samba4-4.0.0.alpha9_bbe4a9c.tar.bz2