
LPICレベル3技術解説無料セミナー
Samba + LDAPで
ドメインコントローラーを構築してみよう

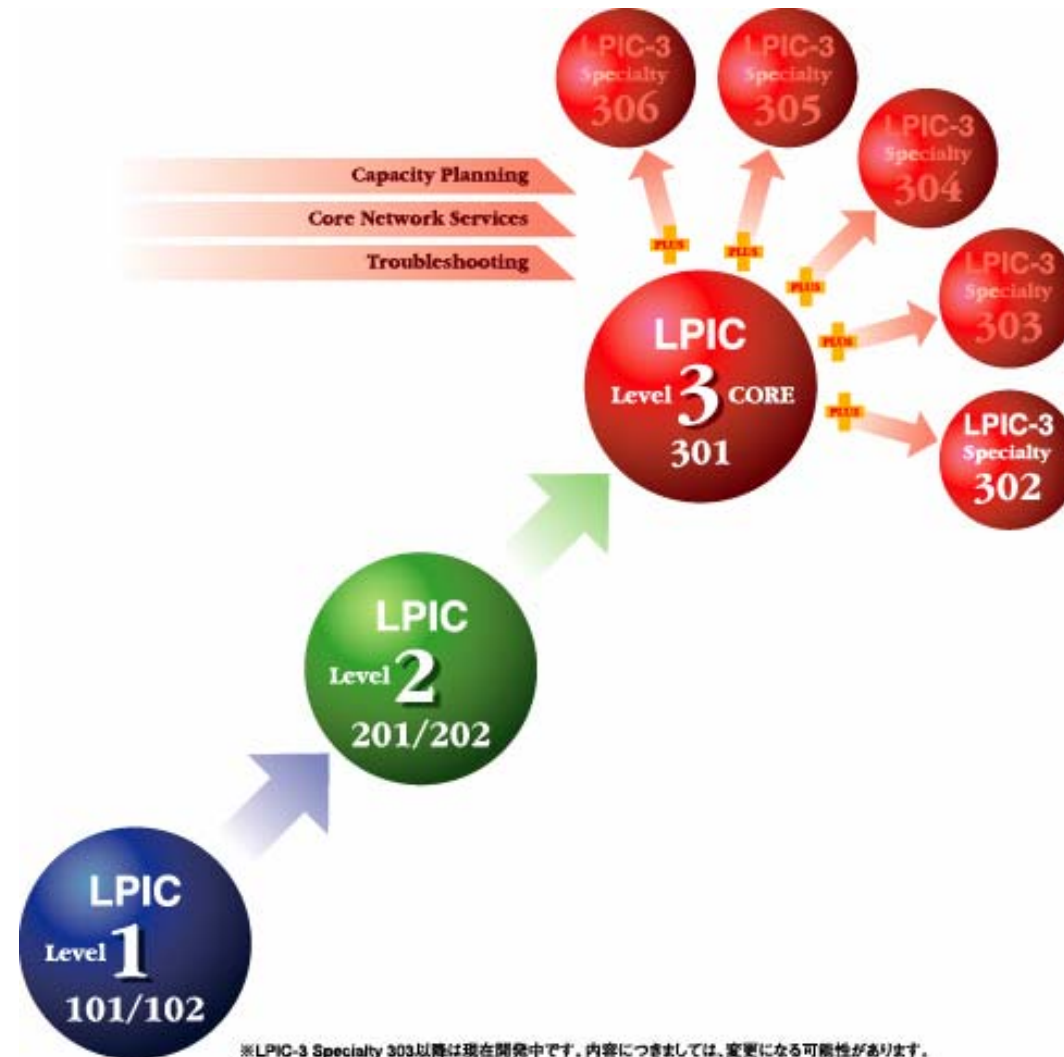
主催：特定非営利活動法人エルピーアイジャパン
講師：宮原 徹 (株式会社びぎねっと)



本日のアジェンダ

- LPIC レベル3の位置付け
- Windowsドメインについて
 - PDCとBDC
 - Samba + OpenLDAPとWindowsドメイン
- Sambaによるドメインコントローラーの構築
 - SambaとOpenLDAPを使ったPDCの構築
 - BDCの構築

LPICスキルアップ構成



技術者が求められるスキルの目安

認定レベル	試験	求められる技術レベル			
LPIC レベル 3 Specialty	選択科目 No.306 Mail & Messaging No.305 Web & Intranet No.304 High Availability & Virtualization No.303 Security No.302 Mixed Environment	開発中 LPIC レベル 3 全体を通して ●Capacity Planning ●Core Network Services ●Troubleshooting が横断的に含まれる LinuxとSambaなどによる混合環境の構築が行える			
			LPIC レベル 3 Core	No.301 Core	Linuxとディレクトリによる認証システムの構築、システムのキャパシティプランニングが行える
			LPIC レベル 2	No.202 Linuxネットワーク管理	Linuxによるシステム構築、ネットワーク構築が行える
				No.201 Linux応用管理	
			LPIC レベル 1	No.102 Linux一般2	Linuxの基本的な操作とシステム管理が行える
No.101 Linux一般1					

※LPIC-3 Specialty 303以降は現在開発中です。内容につきましては、変更になる可能性があります。

Windowsドメインとは

- Windows Networkのユーザー情報をドメインコントローラーが一元管理する仕組み
 - ユーザー名とパスワード
 - その他ユーザー個別の設定
- 各クライアントにユーザー情報の登録不要
- ログオン認証はドメインコントローラーが行う
- ファイル共有に対するアクセスもドメインに登録された情報で管理される
 - ドメインコントローラーとファイルサーバが別々のマシンでも、情報はネットワーク経由でやり取りされる

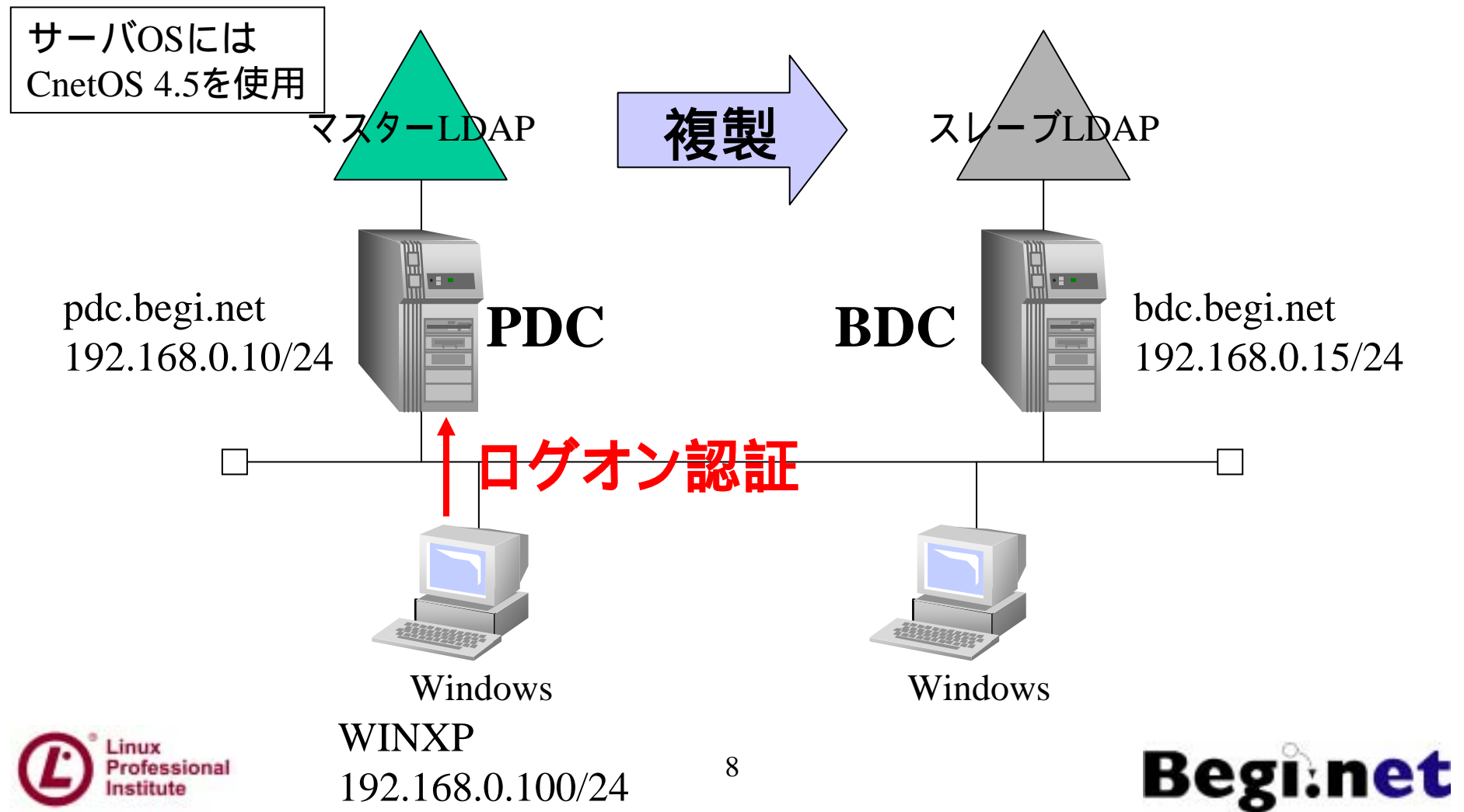
PDCとBDC

- PDC(Primary Domain Controller)
 - ドメインに登録されている情報のマスターを管理するドメインコントローラー
 - ユーザーのログオン認証を行う
 - 1つのドメインに1つ必要
- BDC(Backup Domain Controller)
 - PDCから情報を受け取り保持するドメインコントローラー
 - PDCに代わってログオン認証を行うこともある
 - 負荷が高い場合
 - PDCに障害が発生した場合
 - 1つのドメインに複数存在可能

SambaとOpenLDAP

- Samba単体では、単独のドメインコントローラー (PDCのみ) を実現可能
- ドメイン情報の複製が必要となるPDC・BDCの構成では、情報管理にOpenLDAPが必要
 - LDAPv3をサポートするLDAPサーバ
 - ユーザー名やグループ名、パスワード情報を管理
 - Sambaに対してドメインの情報を提供
 - LDAPサーバ間で情報の複製が可能

SambaとOpenLDAPによる構成



作業

Sambaのインストール

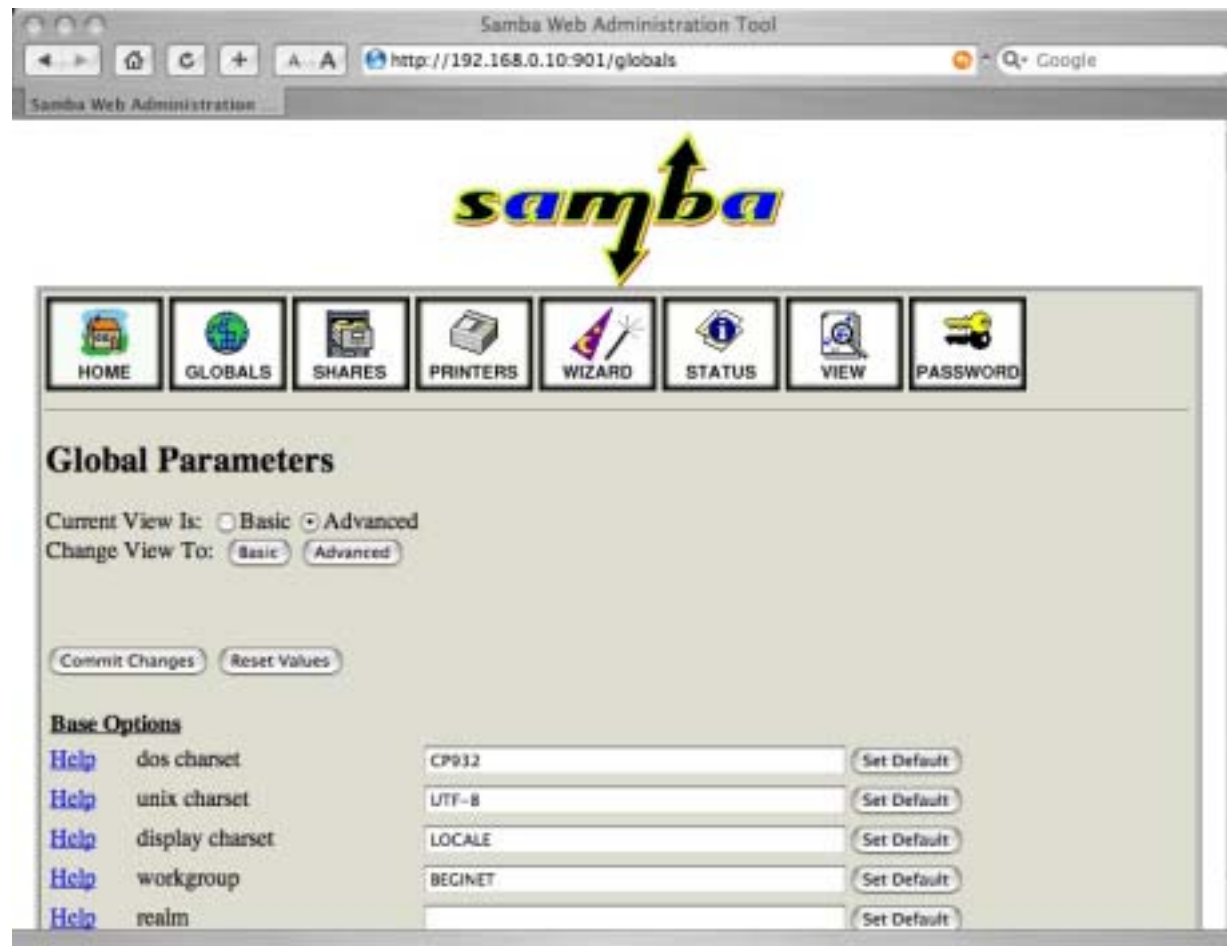
- RPMパッケージをインストールする
 - samba-common : Sambaに共通のファイル
 - samba : Sambaサーバ
 - samba-client : Samba付属のクライアント
 - samba-swath : Samba設定用SWAT
- 1. yumコマンドでインストール
 - # yum install samba-common samba samba-client
samba-swath

作業

SWATの使用

- SWAT (Samba Web Admin Tool) を使用することでWebブラウザからSambaの設定が行える
 1. `/etc/xinetd.d./swat`を修正
 - `disable = no`に設定 (# `chkconfig swat on`でも可)
 - `only_from`行をコメントアウト
 2. `xinetd`を起動(再起動)
 - # `service xinetd start(restart)`
 3. WebブラウザでSWATに接続
 - `http://server_address:901/`
 - `http://`を省略しないこと
 - 管理者`root`で認証
 - 文字コードの設定を行っておく (`dos charset = CP932`)

SWAT 文字コード設定



Windowsドメインの設定

- Samba+OpenLDAPによるPDCの構築
 1. OpenLDAPのインストール
 2. Sambaの設定
 3. smbldap-toolsのインストール
 4. ユーザーの登録とWindowsログオン
- BDCの構築
 1. OpenLDAPによる情報複製の設定
 2. Sambaの設定

OpenLDAPの設定手順

- **ドメイン情報を格納するためのLDAPサーバを設定する**
 1. LDAP認証の設定と確認
 2. LDAPパッケージのインストール
 3. LDAPサーバの設定
 4. LDAPサーバの起動

LDAP用語の基礎知識

- DN:Distinguished Name **識別名**
 - ディレクトリ内でオブジェクトを一意に識別できる名前
- DC:Domain Component
 - ドメインを表すために使用
- OU:Organizational Unit **組織単位**
 - ドメイン内部を組織単位に分割するために使用
 - ユーザーやグループなどのオブジェクトをまとめるためにも使用
- CN:Common Name **共通名**
- クラス (objectClass)
 - データのテンプレート
 - オブジェクトの属性を定義
 - ユーザ、グループなどLDAPで管理するデータの種類によって用意されている

作業

LDAP認証の設定

1. authconfigコマンドを実行
2. 認証の設定
 - ユーザー情報:「LDAPを使用」にチェック
 - 認証:「LDAP認証を使用」にチェック
 - LDAP設定
 - サーバ:127.0.0.1 **自分自身のIPアドレスを指定**
 - ベースDN:dc=begin,dc=net
 - X Windowの「システム設定」 - 「認証」でも同様に設定可能

作業

LDAP認証設定の確認

1. **ユーザー情報** : /etc/nsswitch.conf
passwd: files ldap
shadow: files ldap
group: files ldap
2. **認証** : /etc/pam.d/system-auth
auth sufficient pam_ldap.so use_first_pass
account [default=bad success=ok user_unknown=ignore] pam_ldap.so
password sufficient pam_ldap.so use_authtok
session optional pam_ldap.so
3. **LDAP設定** : /etc/ldap.conf
host 127.0.0.1
base dc=beginet,dc=net

作業

LDAPパッケージのインストール

- **必要なパッケージ**
 - openldap-servers
 - openldap-clients
- 1. yumでインストール
 - # yum install openldap-servers openldap-clients
- **同様に「アプリケーションの追加/削除」からインストールも可能**
 - 「ネットワークサーバ」 「openldap-servers」
 - 「システムツール」 「openldap-clients」

LDAPの設定

1. スキーマ設定ファイルのコピー
 - スキーマ設定は/etc/openldap/schemaに入れる
 - `# cp /usr/share/doc/samba-x.y.z/LDAP/samba.schema /etc/openldap/schema/`
2. LDAP管理者パスワードの生成
 - パスワードをMD5を使ってダイジェスト化
 - `# slappasswd -h {MD5} -s ldapadmin`
 - “ldapadmin”がパスワード(シークレット)

作業

/etc/openldap/slapd.confの設定

slapd.confに以下の追加と修正を行う

1. 追加

```
include /etc/openldap/schema/samba.schema
```

2. 修正

```
suffix "dc=begi,dc=net"
```

```
rootdn "cn=Manager,dc=begi,dc=net"
```

```
rootpw {MD5}TmZgZ01/Z0/29bOPByMr4A==
```

- slappasswdの結果をコピー & ペースト

作業

LDAPサーバの起動

1. OpenLDAPサーバの起動
 - # service ldap start
2. LDAPポートの確認
 - # netstat -tl
3. システム起動時に自動起動するように設定
 - # chkconfig ldap on

Sambaの設定手順

SambaをLDAPサーバと連携したPDCとして設定

1. Sambaの設定
2. 管理者パスワードの設定
3. smbldap-toolsのインストールと設定
 - Perlのモジュールをインストール

作業

smb.confの設定

1. /etc/samba/smb.confに設定

workgroup = **BEGINET**

passdb backend = **ldapsam:ldap://localhost**

admin users = **Administrator**

domain logons = **yes**

domain master = **yes**

ldap admin dn = **cn=Manager,dc=begi,dc=net**

ldap group suffix = **ou=Groups**

ldap machine suffix = **ou=Computers**

ldap passwd sync = **yes**

ldap suffix = **dc=begi,dc=net**

ldap user suffix = **ou=Users**



SWATで設定する場合、「²²詳細表示」(Advanced)で行う

Begi.net

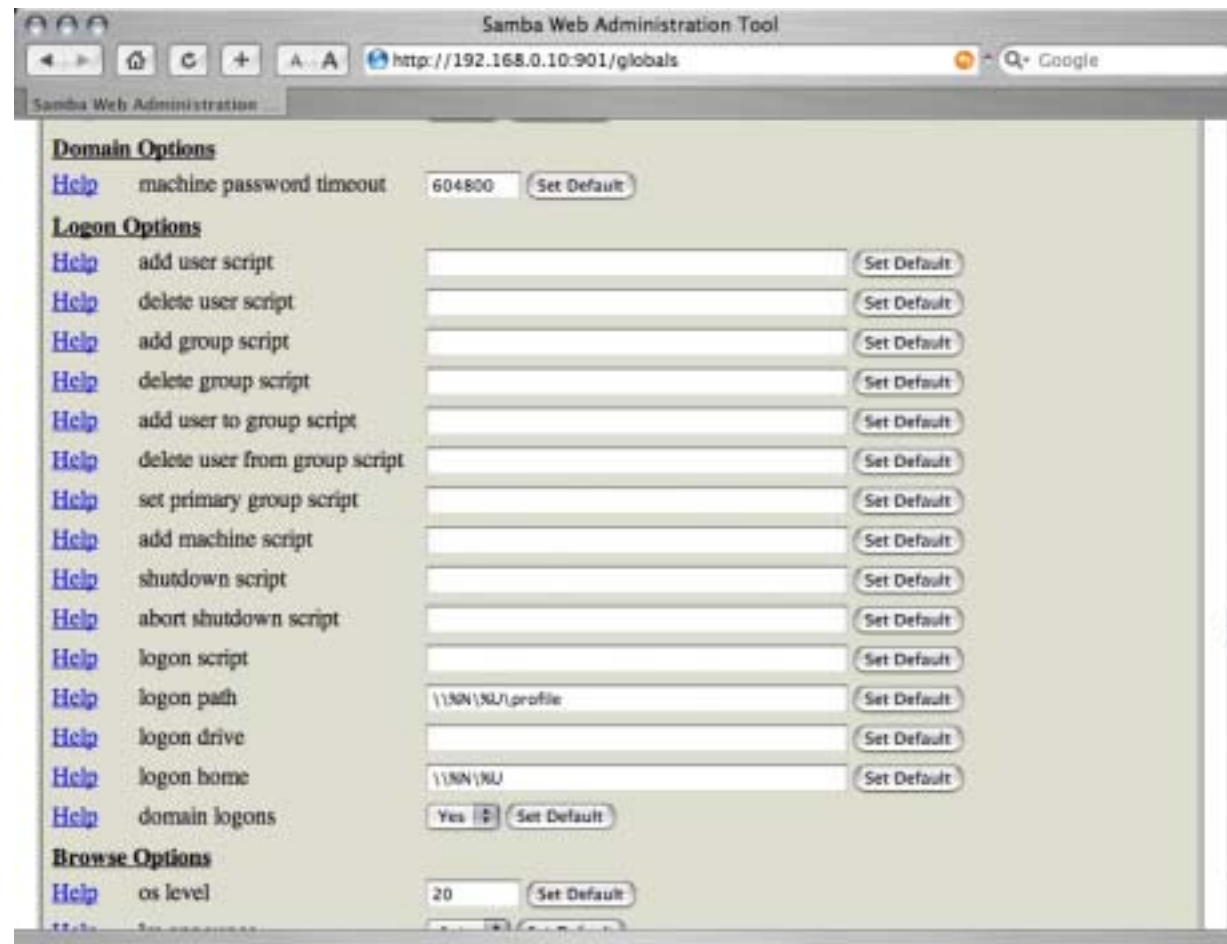
設定項目について(1)

- workgroup
 - ドメイン名を指定
- passdb backend
 - Sambaのユーザー情報の格納先を指定
 - smbpasswd tdbsam ldapsamの3種類から選択可能
- admin users
 - Samba管理者のユーザー名を指定
 - コンピュータがドメインに参加する際に必要
- domain logons
 - ドメインログオンをサポートするドメインコントローラになる
- domain master
 - ドメインマスタブラウザになる

設定項目について(2)

- ldap admin dn
 - LDAPサーバの管理者ユーザーをDNで指定する
- ldap suffix
 - LDAPの検索ベースを指定する
- ldap machine suffix/ldap user suffix/ldap group suffix
 - ドメイン情報の各格納先(OU)を指定する
- ldap passwd sync
 - SambaとUNIXのパスワード情報を同期させる

SWAT ドメイン設定



SWAT LDAP設定

The screenshot displays the Samba Web Administration Tool (SWAT) interface in a web browser. The browser's address bar shows the URL `http://192.168.0.10:901/globals`. The page title is "Samba Web Administration Tool". The interface is divided into several sections for configuring LDAP options:

- Global Options:**
 - posix locking: Yes (Set Default)
 - strict locking: Yes (Set Default)
 - share modes: Yes (Set Default)
- Ldap Options:**
 - ldap admin dn: `cn=Manager,dc=beginet,dc=net` (Set Default)
 - ldap delete dn: No (Set Default)
 - ldap filter: `(uid=%u)` (Set Default)
 - ldap group suffix: `ou=Groups` (Set Default)
 - ldap idmap suffix: (Set Default)
 - ldap machine suffix: `ou=Computers` (Set Default)
 - ldap passwd sync: Yes (Set Default)
 - ldap replication sleep: 1000 (Set Default)
 - ldap suffix: `dc=beginet,dc=net` (Set Default)
 - ldap ssl: no (Set Default)
 - ldap timeout: 15 (Set Default)
 - ldap user suffix: `ou=People` (Set Default)
- Miscellaneous Options:**
 - add share command: (Set Default)
 - change share command: (Set Default)
 - delete share command: (Set Default)
 - embed: (Set Default)

作業

LDAP管理者パスワードの設定

- SambaがOpenLDAPに接続する際に使用するパスワード
 - slapd.confのrootpwで設定した値と対応させる
 - rootpw :ldapadmin **実際にはハッシュ値**
 - ユーザー名はsmb.confに設定したldap admin dnの値が使用される
 - ldap admin dn :cn=Manager,dc=beginet,dc=net
1. smbpasswdコマンドに-wオプションで実行
 - # smbpasswd -w [ldapadmin](#)
 - /etc/samba/secrets.tdbに保存される

管理者パスワードの関係

OpenLDAP



slapd.conf

ユーザー名: rootdn "cn=Manager,dc=begi,dc=net"

パスワード: rootpw [{MD5}TmZgZ01/Z0/29bOPByMr4A==](#)
slappasswd -h {MD5} -s [ldapadmin](#)の結果を記述

それぞれのユーザー名 / パスワードを
一致させること



Samba

smb.conf

ユーザー名: ldap admin dn = cn=Manager,dc=begi,dc=net

パスワード: smbpasswd -w [ldapadmin](#)

/etc/samba/secrets.tdbに格納される

smbldap-toolsのインストール

- Perlで書かれたSamba+LDAP用管理ツール群
 - Samba+LDAPでドメインを構築するための初期化
 - ユーザー情報の管理
- Perlのモジュールをインストールする必要がある
- 接続先LDAPサーバの設定を行う
- バグがあるので、一部パッチを当てる必要がある

Perlモジュールのインストール

- smbldap-toolsが必要とするPerlのモジュール
 - Net::SSLeay
 - XML::NamespaceSupport
 - XML::SAX
 - IO::Socket::SSL
 - Authen::SASL
 - Convert::ASN1
 - Net::LDAP(perl-ldap)
- tar.gzからソースコードでインストール
- CPANの利用

作業

CPANでインストール

1. # cpan
 - 接続設定が必要だが、エンターキー連打
 - 接続先は[Asia]-[Japan]から選択
2. cpan> install Bundle::CPAN **かなり時間がかかるので注意**
3. cpan> exit
4. # cpan
5. cpan> install Net::SSLeay
6. cpan> install XML::NamespaceSupport
7. cpan> install XML::SAX
8. cpan> install XML::SAX::Writer
9. cpan> install Net::LibIDN **IO::Socket::SSLのために必要**
10. cpan> install IO::Socket::SSL **エラーが出てうまくインストールできない**
11. cpan> install Authen::SASL
12. cpan> install Convert::ASN1
13. cpan> install Net::LDAP

作業

CPANのエラー対処法

- CPANによるモジュールインストール時にエラーが発生した場合、コマンドラインでもインストール作業を行う
 1. 別のターミナルを起動する
 2. `# cd /root/.cpan/build/IO-Socket-SSL-??`
エラーが発生したモジュール名
 3. `# perl Makefile.PL`
 4. `# make test`
 5. `# make`
 6. `# make install`

作業

smbldap-toolsのインストール

- 以下の手順でインストールする
 1. `# cd /usr/share/doc/samba-x.y.z/LDAP/smbldap-tools/`
 2. `# cp *.p? /usr/local/sbin/`
 3. `# chmod 755 /usr/local/sbin/smbldap-*.pl`
 4. `# chmod 600 /usr/local/sbin/smbldap_*.pm`
 5. `# cd mkntpwd`
 6. `# make`
 7. `# cp mkntpwd /usr/local/sbin/`

参考

smbldap-toolsにパッチ当て

- 移動プロファイルを無効にしたい場合、パッチ当てを行う必要がある

1. smbldap-useradd.plを修正

```
- if (defined $valprofilepath) {  
+ if (defined $valprofilepath && defined $valprofilepath ne "") {
```

2. smbldap-usermod.plを修正

```
- push(@mods, 'sambaProfilePath' => $tmp);  
+ if ($tmp eq "") {  
+   push(@mods, 'sambaProfilePath' => []);  
+ } else {  
+   push(@mods, 'sambaProfilePath' => $tmp);  
+ }
```

SIDについて

- SID(Security Identifier・セキュリティ識別子)
- Windows内部のオブジェクトを識別するための一意の値
 - 「S-?-?-?」といった形式になっている
 - ドメイン毎に異なるSID値を持っている
- /etc/samba/secrets.tdbに保管されている
- ローカルドメインのSID値の確認
 - # net getlocalsid
- ローカルドメインのSID値の設定
 - # net setlocalsid *SID*
- その他のドメインのSID値の確認
 - # net rpc getsid [*domain*]

ドメインの初期化とユーザー登録

- SambaがPDCとして動作するために必要な初期情報をLDAPサーバに登録
- ユーザーおよびクライアントコンピュータを登録
 1. 初期ドメインデータの作成
 2. ユーザーの登録
 3. コンピュータの登録
 4. ドメイン参加とWindowsドメインログオン

初期ドメインデータの作成

1. 初期ドメインデータの作成
 - ドメインの動作に必要な初期データを作成する
 - # smbldap-populate.pl
 - /var/lib/ldap/にファイルが作成される
2. ドメイン管理者のパスワード設定
 - # smbldap-passwd.pl administrator
 - パスワード: domainadmin
 - 引数のユーザー名はsmb.confでadmin usersに設定したユーザーを指定する
 - このユーザー名とパスワードはWindowsコンピュータをドメインに参加させる時に必要

ドメインユーザー設定

- ユーザー登録
 - # smbldap-useradd.pl -a -m *username*
- ユーザーパスワード設定
 - # smbldap-passwd.pl *username*
- コンピュータ登録
 - # smbldap-usreadd.pl -w *computer_name*
- ユーザー情報修正
 - # smbldap-usermod.pl *options* *username*
- ユーザー削除
 - # smbldap-userdel.pl *username*

作業

ユーザーとコンピュータの登録

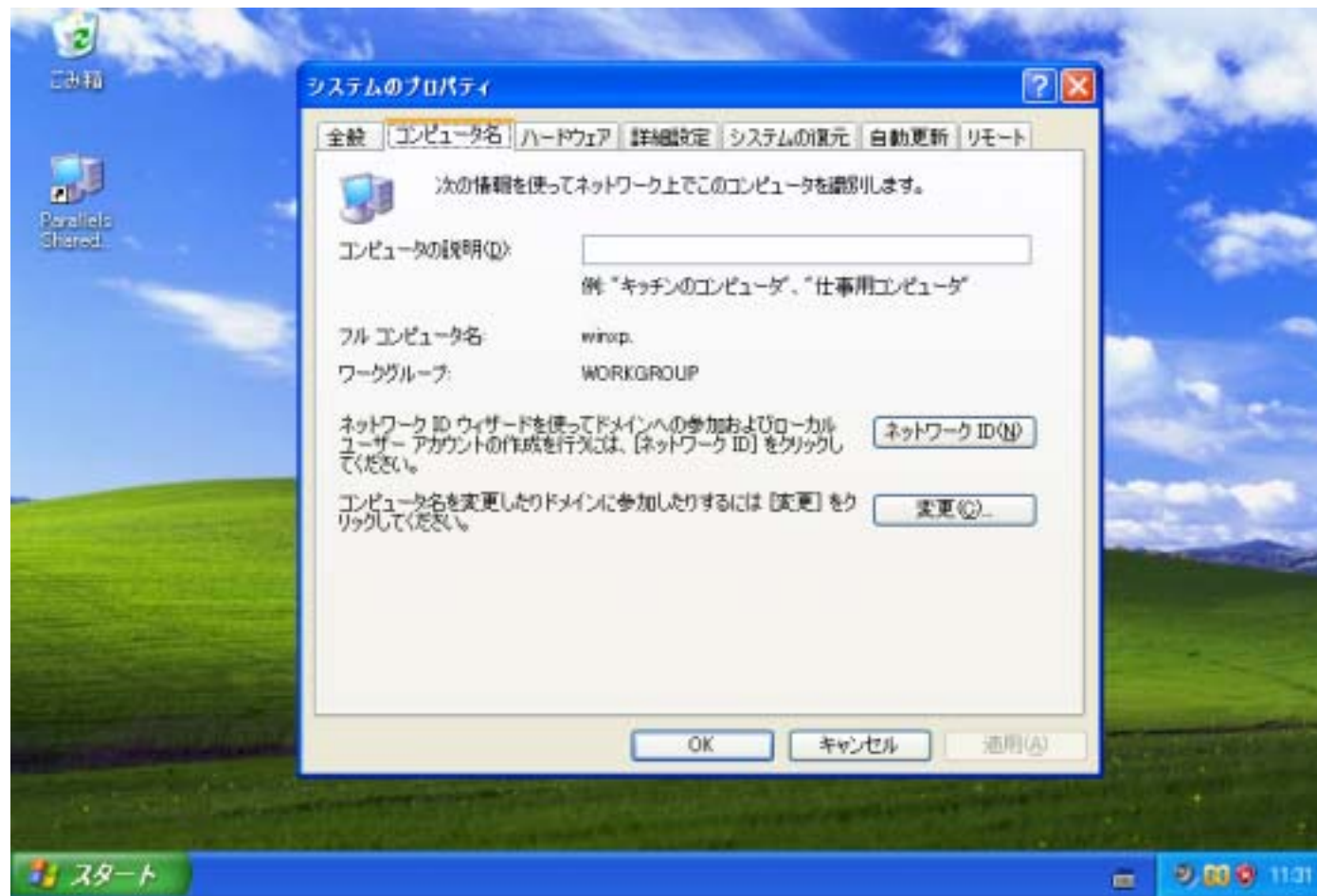
1. ユーザーbeginetを登録
 - # smbldap-useradd.pl -a -m beginet
 - # smbldap-passwd.pl beginet
 - パスワード:beginet
2. クライアントコンピュータwinxpを登録
 - # smbldap-useradd.pl -w winxp
3. 確認
 - # getent passwd
 - # smbldap-usershow.pl beginet
 - # smbldap-usershow.pl winxp\$ 末尾に\$が付く
4. Sambaを起動
 - # service smb start

作業

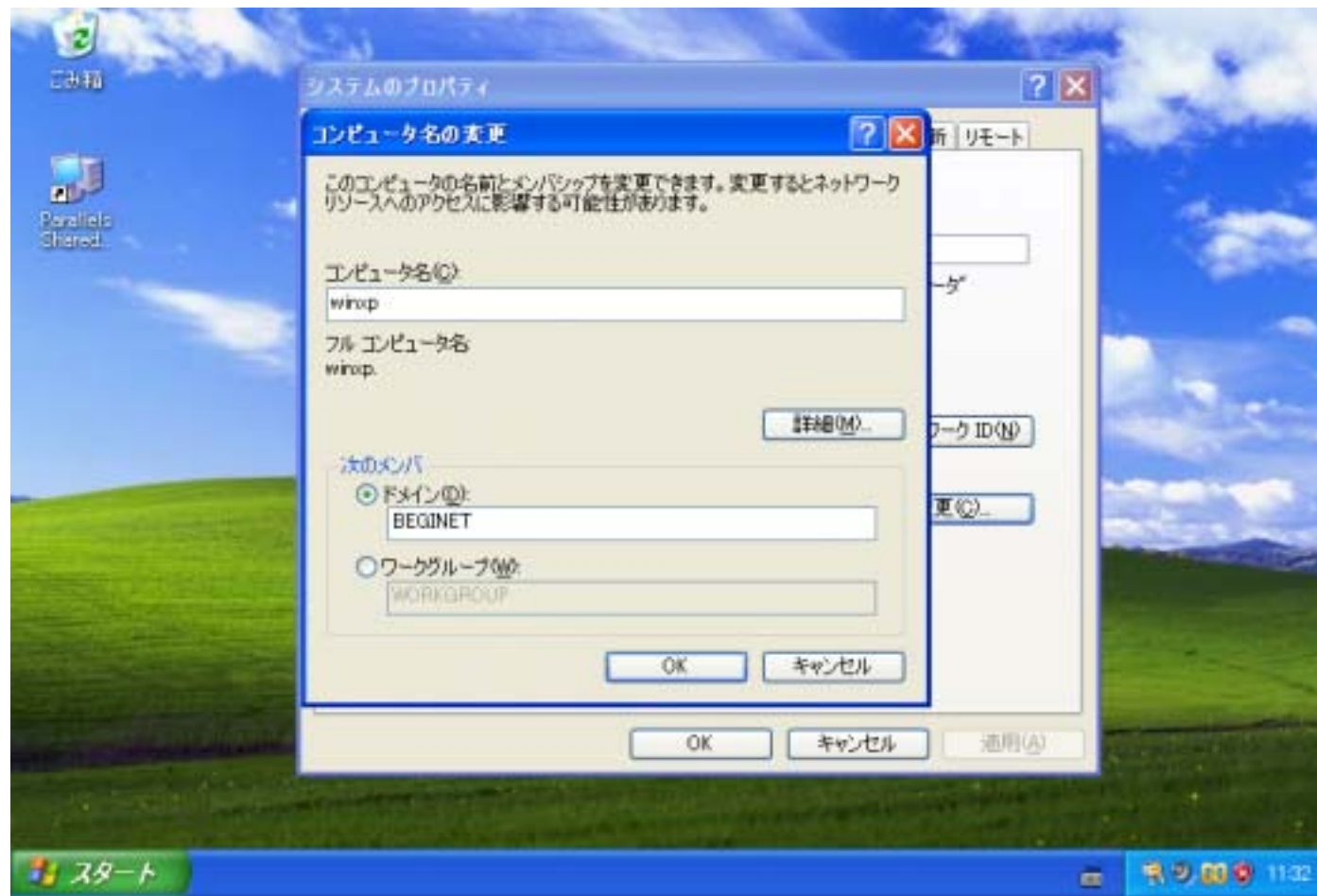
ドメイン参加とドメイン認証

1. Windowsクライアントのドメイン参加設定
 1. 管理者権限でログオン
 2. 「システムのプロパティ」 「コンピュータ名」 「変更」ボタンをクリック
 3. コンピュータ名をドメインに登録したコンピュータ名に設定(ここではwinxp)
 4. ドメイン名:beginet
 5. 管理者ユーザー名 / パスワードが必要
 6. 「Administrator/domainadmin」を入力
 7. ドメイン参加後、Windowsクライアントを再起動
2. ドメイン認証
 - ログオンダイアログでログオン先をドメインに変更
 - 移動プロファイルの問題が発生(後述)

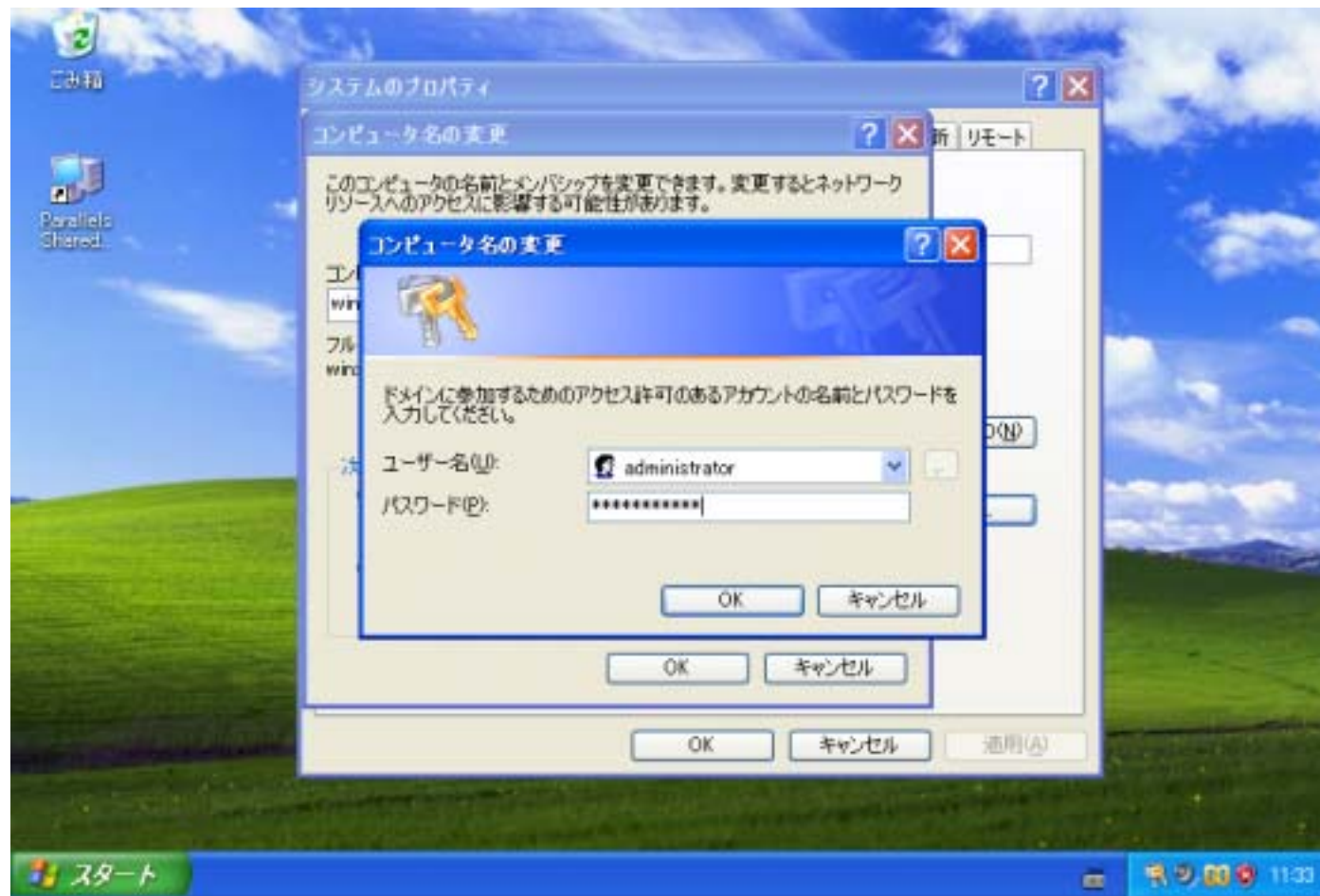
ドメイン参加(1)



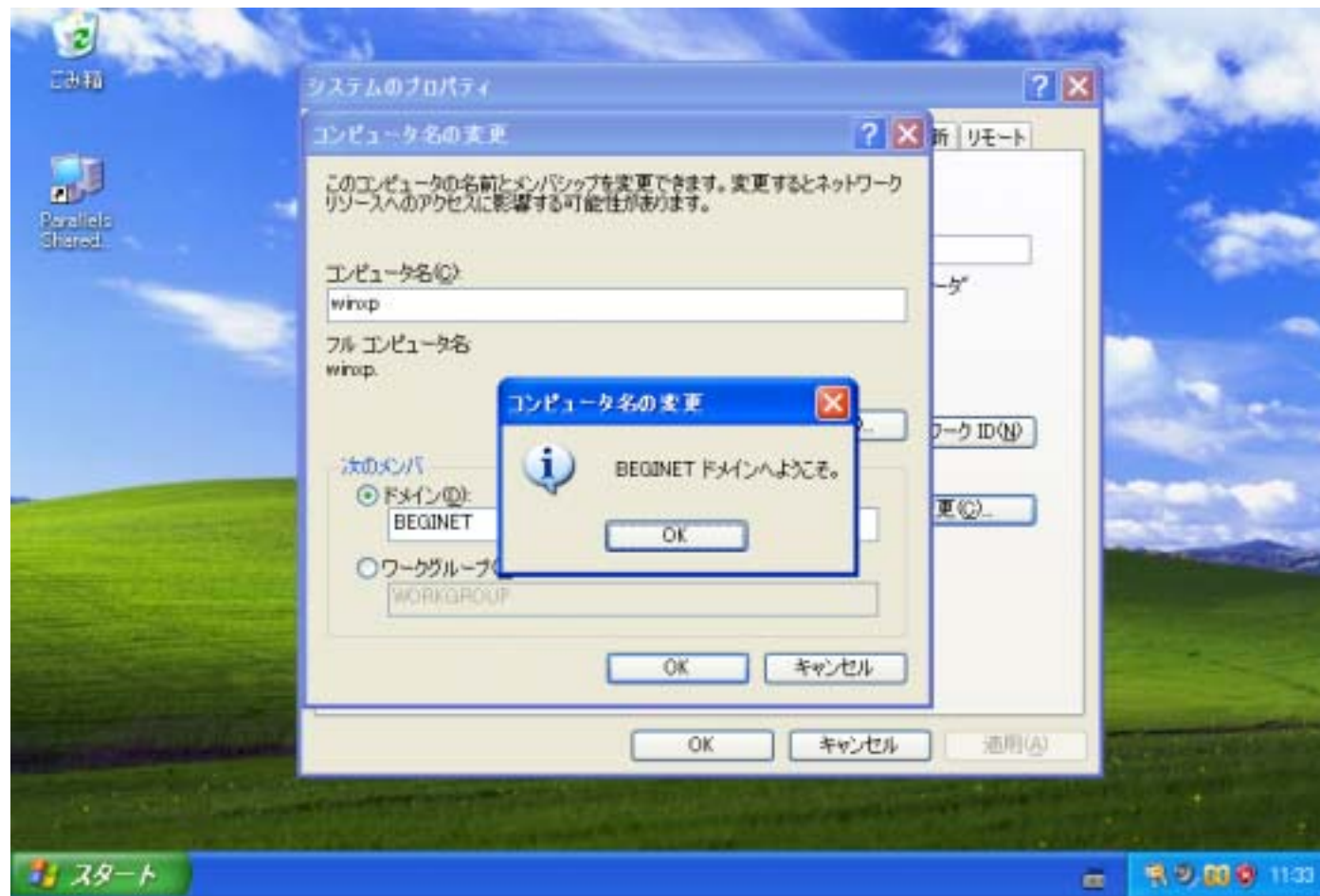
ドメイン参加(2)



ドメイン参加(3)



ドメイン参加(4)



実用上考慮すべきポイント

- 移動プロファイルの利用
 - smbldap-useradd.plの設定ではユーザー名が入る
 - `¥¥SERVER¥profiles¥username`と設定される
 - profilesというファイル共有を作っておく必要がある
 1. `# mkdir /home/profiles`
 2. `# chmod 777 /home/profiles`
 3. SWAT等で/home/profilesをprofiles共有として設定
 - 読み書き可能(read only = no)に設定すること

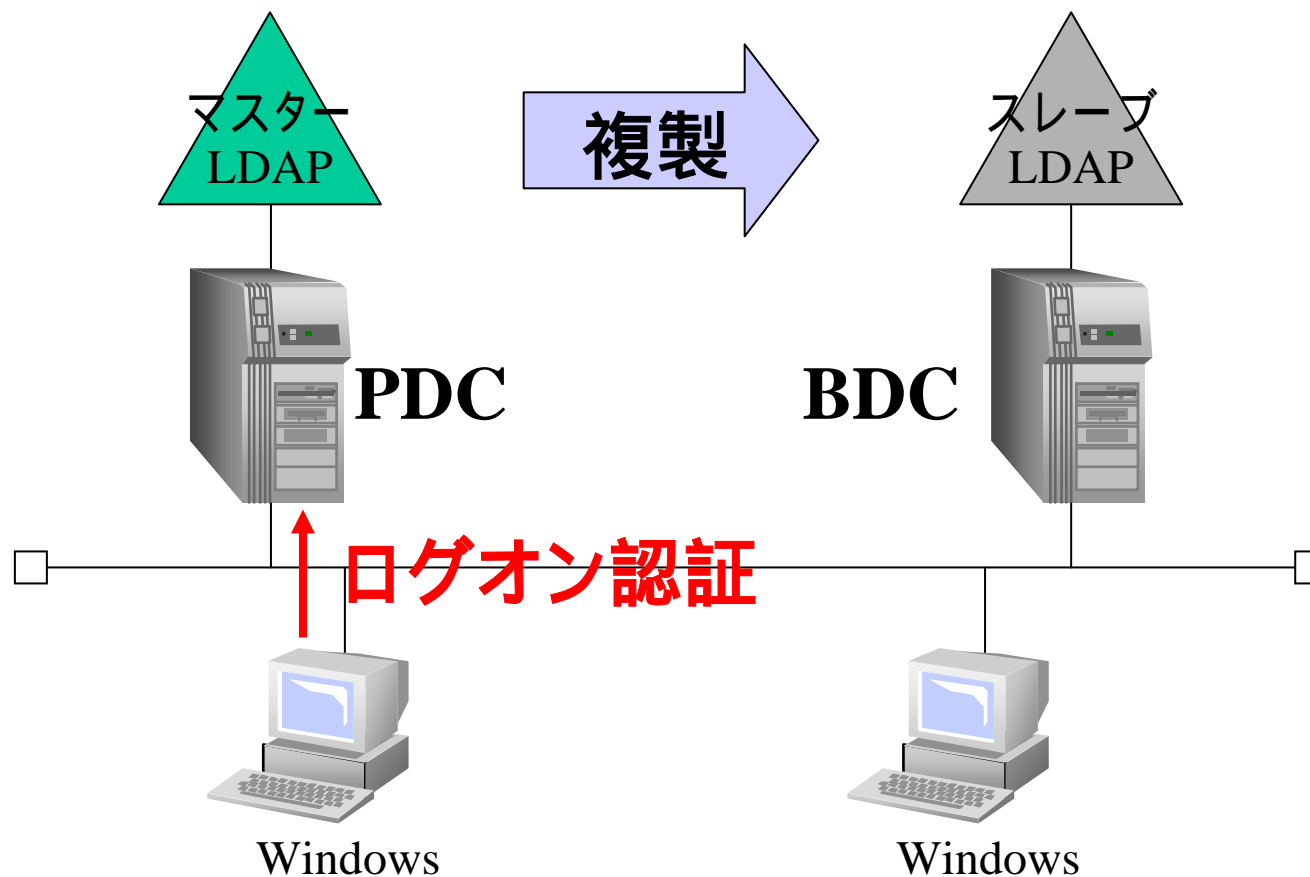
SambaによるPDC - BDCの構築

BDCの構築

PDCの保持情報の複製を作り、BDCを構築する

1. BDCで認証にLDAP使用を設定 (authconfig)
2. BDCにPDCと同様OpenLDAPとSambaをインストール
3. BDCでスキーマ設定ファイルのコピー
4. OpenLDAPの複製を設定
 - PDCからLDAPの情報ファイルをBにコピー
 - マスター / スレーブ間で複製を設定
5. SambaをBDCとして設定
 - ドメインマスターにならないサーバとして設定
 - ユーザー情報はOpenLDAPサーバから取得

SambaとOpenLDAPによる構成



作業

BDCへのLDAP情報のコピー

1. PDCのSambaとOpenLDAPサーバを停止する
 - PDC # `service smb stop`
 - PDC # `service ldap stop`
2. PDCのLDAP情報をアーカイブ
 - PDC # `cd /var/lib`
 - PDC # `tar cvf /root/ldap_data.tar ldap`
3. `ldap_data.tar`をPDCからBDCへコピー
 - BDC # `scp root@192.168.0.10:/root/ldap_data.tar /root`
4. LDAP情報をコピー
 - BDC # `tar xvf ldap_data.tar`
 - BDC # `rm -rf /var/lib/ldap/*`
 - BDC # `cp -p /root/ldap/* /var/lib/ldap/`

作業

LDAP情報複製の設定 (PDC側)

- /etc/openldap/slapd.confに以下の設定を追加

```
repllogfile /var/lib/ldap/openldap-master-replog
replica host=192.168.0.15
        binddn="cn=Manager,dc=begi,dc=net"
        bindmethod=simple credentials=ldapadmin
```
- hostには更新情報を伝播させたいスレーブのIPアドレス (ここでは192.168.0.15)を指定
- マスターに対する変更は差分ログとして記録される
- スレーブに対してbinddnで接続認証する
 - スレーブに管理者ユーザーのDNが存在しないといけない
 - 簡易認証・パスワードはldapadminで接続

作業

LDAP情報複製の設定 (BDC側)

- /etc/openldap/slapd.confを以下のように設定
include /etc/openldap/schema/samba.schema
suffix "dc=begin,dc=net"
rootdn "cn=Manager,dc=begin,dc=net"
rootpw {MD5}TmZgZ01/Z0/29bOPByMr4A==
updatedn "cn=Manager,dc=begin,dc=net"
updateref ldap://192.168.0.10
- updatednはローカルのrootdn、マスター側のbinddnと同じ設定にする
- updaterefは更新要求を受けた時にマスターの所在を知らせる

作業

LDAP情報複製の確認

1. PDC・BDCでOpenLDAPを起動
 - # service ldap start
2. PDCでユーザーを追加
 - PDC # smbldap-useradd.pl -a -m reptest
 - PDC # smbldap-passwd.pl reptest
 - PDC # id reptest
3. BDCでユーザーを確認
 - BDC # id reptest

作業

BDCのsmb.confの設定

- ドメインマスターにならない以外はPDCと同じ設定

workgroup = **BEGINET**

passdb backend = **ldapsam:ldap://localhost**

admin users = **Administrator**

domain logons = **yes**

domain master = **no** **ドメインマスターにはならない**

ldap suffix = **dc=begi,dc=net**

ldap machine suffix = **ou=Computers**

ldap user suffix = **ou=Users**

ldap group suffix = **ou=Groups**

ldap admin dn = **cn=Manager,dc=begi,dc=net**

作業

SIDの設定

- BDCにはPDCと同じSIDを設定する必要がある
- 作業はBDCで行う
- 1. PDCのSambaは動作させておく
 - PDC # service smb start
- 2. BDCでPDCのSIDを取得
 - BDC # net rpc getsid
- 3. BDCの/etc/samba/secrets.tdbを削除
 - BDC # rm /etc/samba/secrets.tdb
- 4. BDCのローカルSIDを設定
 - BDC # net setlocalsid *SID* netコマンドで取得したSID
- 5. BDCのSambaがスレーブLDAPサーバに接続する際のパスワードを設定

作業

BDCの動作の確認

1. あらかじめWindowsコンピュータのドメイン認証キャッシュに関する設定を変更しておく
 - 「コントロールパネル」 「管理ツール」 「ローカルセキュリティポリシー」 「ローカルポリシー」 「セキュリティオプション」 「対話型ログオン：ドメインコントローラが利用できない場合に使用する、前回ログオンのキャッシュ数」を0に設定
2. PDC・BDC両方を動作させる
3. Windowsクライアントからログオン・ログアウトする
 - PDCで認証される
4. PDCのネットワークケーブルを抜く
5. Windowsクライアントから再度ログオンする
 - BDCで認証される
 - PDC停止のため、移動プロファイルが使えないエラーが発生

ログオンキャッシュを無効にする(1)

