CAL(クライアントアクセスライセンス)
0円で構築するActive Directory

～ Samba4で構築するMS AD環境 ～

オープンソース・ソリューション・テクノロジ株式会社
代表取締役 チーフアーキテクト 小田切 耕司

OSSTech

お問い合わせ info@osstech.co.jp

オープンソース・ソリューション・テクノロジ（株）
会社紹介

OSSTech

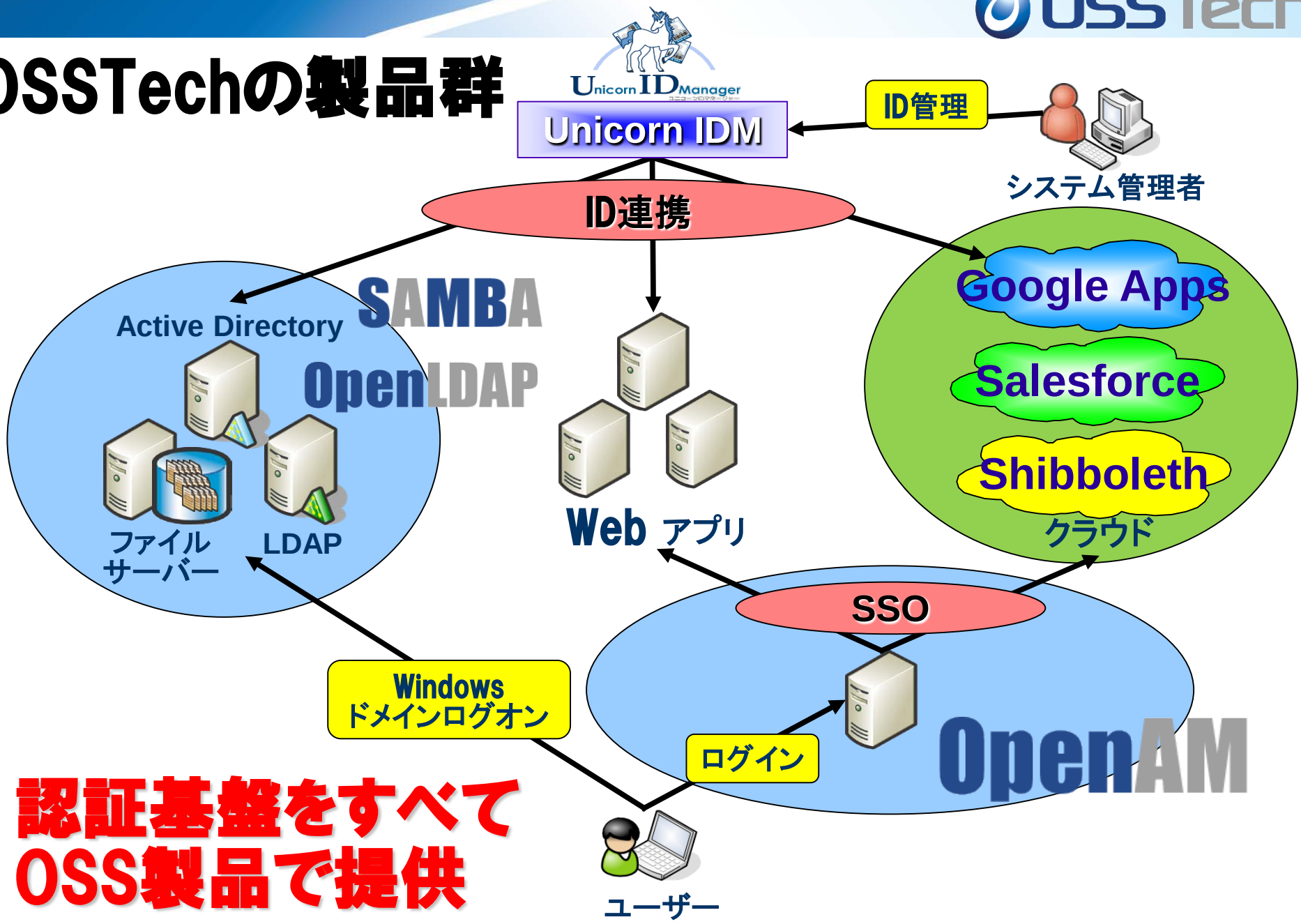
オープンソース・ソリューション・テクノロジ株式会社

「オープンソースソフトウェア」の新しい価値を創造し、高機能・高品質を追求する

統合認証　シングルサインオン　アイデンティティ管理ソリューション

- **OSに依存しないOSSのソリューションを中心に提供**
  Linuxだけでなく、AIX, Solaris, Windowsなども対応！
- **OpenAM, OpenLDAP, Sambaによる認証統合／シングル・サイン・オン、ID管理ソリューションを提供**
  - 製品パッケージ提供
    機能証明、定価証明が発行可能
  - 製品サポート提供
    3年～5年以上の長期サポート
    コミュニティでサポートが終わった製品のサポート
  - OSSの改良、機能追加、バグ修正などコンサルティング提供

OSSTechの製品群



認証基盤をすべて
OSS製品で提供

OSSTechの製品群（すべてOSSで提供）
原則Linux/Solaris/AIX共にRPMで提供

- OpenAM
  - Tomcat, OpenLDAP対応で高機能なシングルサインオン製品
- OpenLDAP
  - 認証統合、ディレクトリサービス、シングルサインオンのインフラ
- Samba
  - Active Directoryの代替、高性能NAS（CIFSサーバー）の代替
- Unicorn ID Manager
  - Google Apps, Active Directory, LDAP, Sambaに対応した統合ID管理製品
- ThothLink
  - WebブラウザからのWindowsファイルサーバアクセス機能を提供

Part 1.

Samba機能と特徴

Sambaとは？

機　能	Samba 3	Samba 4
ファイルサーバ機能	Samba3.6からSMB2対応	SMB2,SMB3（Windows8）対応
	NASとして使うには現時点では Samba4より安定	サーバーサイドコピーなどに対応
		CTDBによるクラスター機能対応
ドメインコントローラ機能	NTドメイン互換	Active Directory（Win2008R2）互換
	NTLMv2認証	Kerberos認証（Kerberosサーバー内蔵）
	システムポリシー	グループポリシー
	冗長化には外部のLDAPが必要	LDAPを内蔵しているためSambaのみで冗長化が可能
Windows GUIによる管理機能	Windows2000のUSRMGR Windows 7,8で動作しない	RSAT対応 Windows 7,8で動作可能
名前解決機能	NTドメイン互換なのでWINSサーバーが必要	ADドメイン互換なのでDNSによる名前解決が必要
	SambaがWINSサーバー機能を持つ	WINSサーバーは不要 SambaがDNSサーバー機能を内蔵
	DNSでSamba3 DCを見つけることはできない	DNSがないとSamba4 DCを見つけられない

WindowsサーバーをSambaで構築するメリット

コスト削減

- Windowsサーバでは、アクセスするユーザごとにCAL（Client Access License）が必要
- サーバーの低価格化によりOSライセンスコストの割合が増加

セキュリティ対策

- Samba4をADとして利用する場合はアンチウィルスソフト購入不要
- Windowsに比べ、ウィルスなどの被害が圧倒的に少ない。

高機能

- 設定ファイルにスクリプトを定義するだけで機能拡張が可能
  ユーザ管理、共有管理機能、ユーザホーム自動作成、パスワードチェック
- VFSモジュールを開発することで機能拡張が可能
  クラスタ機能、監査機能、ACL制御、容量制限、ウィルスチェック

高い信頼性

- 連続運転に強い
- オープンソースなので障害調査でき、不具合修正も可能

運用のしやすさ

- シェルスクリプトによる運用の効率化が可能
- 修正モジュールの適用に、OSリブートの必要がない

Part 2.

Windows移行 Q & A

Windowsドメイン移行に関するQ&A

Q. SambaでWindows ADドメインを移行できますか？

A. はい、できます。

- Samba4を既存のWindows ADドメインに参加させ、「FSMO:Flexible Single Master Operation」(操作マスター)をSamba4へ転送することで移行可能です。
- FSMO転送後は既存のWindows ADのDCは撤去可能です。
- Samba4はGC (Global Catalog) を持つことも可能です。

Q. 現在WindowsマシンをDNSサーバー、Kerberosサーバー、DHCPサーバー、Radiusサーバーとして利用しています。これをSambaに移行することはできますか？

A. はい、できます。

- Samba4はDNSサーバーとKerberosサーバーになることができ、Linux OSが標準搭載している製品コンポーネントでDHCPサーバーやRadiusサーバーを構築することができます。

Windowsドメイン移行に関するQ&A :サーバ管理

Q. 現在DC(ドメインコントローラ)として利用しているWindowsマシンを、SambaのDC移行後もそのままDCとして利用できますか？

A. はい、可能です。

SambaとWindowsのDCの混在利用が可能です。

FSMOはSambaとWindowsのどちらのDCでも構いません。

Q. Samba4をDCとなっているADドメインにWindowsサーバーをDCとして設置できますか？

A. はい、可能です。

Samba4で新規構築したADドメインにWindowsサーバーをDCとして参加させることが可能です。

Windowsドメイン移行に関するQ&A

Q. 現在のWindowsドメインは別なADドメインと信頼関係を結んでいます。これも移行することはできますか？

A. 現在開発中です。

Samba 4はADドメインとの信頼関係をサポートしています。

明示的な片方向の信頼関係はもちろん
ADの推移的な双方向の信頼関係もサポートします。
しかし、現在は開発中のため機能しません。

Windowsドメイン移行に関するQ&A

Q. ADドメイン移行後、Samba4マシンを旧Windows DCと同じ
マシン名、同じIPアドレスで運用しようと思いますが、
大丈夫ですか？

A. はい、可能です。しかし、そのためにはSamba4をDCに追加後、既存ADのDC
を撤去後に同じホスト名、IPアドレスでSamba4を構築します。
SIDは引き継がれるのでアクセス権やプロファイルもそのまま使えます。

Q. SambaでWindows ADドメインを移行した時、ユーザの
パスワードも移行できますか？
ADドメインの時のパスワードがそのまま使えますか？

A. はい、そのまま使えます。

Q. ADのグループポリシーは移行できますか？

A. はい、移行可能です。

Samba4をDCとして参加させて、SYSVOL共有を複製することでグループポリシーがSamba4へ移されます。（rsyncなどの複製サービスは別途必要）

Windowsドメイン移行に関するQ&A

Q.　移動プロファイルは移行できますか？

A.　はい、移行できます。

移動プロファイルをSambaのプロファイル共有にコピーすることで移行できます。

Q.ローカルプロファイルは継続して利用できますか？

A.はい、利用できます。

Sambaに移行した場合もユーザSIDはSamba DCに引き継がれますので、スタートメニューやデスクトップもそのまま継続利用できます。

Q. 移行作業中に既存ドメインは利用できますか？

A. はい、利用できます。

SambaをDCに追加する作業などで既存のADドメインを止める必要はありません。

しかし、FSMOを転送するときはユーザー追加などはできる限りしないようにしましょう。

Part 3.

LPIC レベル3にて Samba4も出題範囲！

300試験範囲：出題範囲詳細（Ver1.0）

主題390：OpenLDAP の設定
- 390.1 OpenLDAPのレプリケーション
- 390.2 ディレクトリの保護
- 390.3 OpenLDAPサーバのパフォーマンスチューニング

主題391：OpenLDAPの認証バックエンドとしての利用
- 391.1 PAMおよびNSSとLDAPの統合
- 391.2 アクティブディレクトリおよびKerberosとLDAPの統合

主題392：Sambaの基礎
- 392.1 Sambaの概念とアーキテクチャ
- 392.2 Sambaを設定する
- 392.3 Sambaの保守
- 392.4 Sambaのトラブルシューティング
- 392.5 国際化

主題393：Sambaの共有の設定
- 393.1 ファイルサービス
- 393.2 Linuxファイルシステムと共有/サービスのパーミッション
- 393.3 プリントサービス

主題394：Sambaのユーザとグループの管理
- 394.1 ユーザアカウントとグループアカウントの管理
- 394.2 認証と許可およびWindbind

主題395：Sambaのドメイン統合
- 395.1 SambaのPDCとBDC
- 395.2 Samba4のAD互換ドメインコントローラ
- 395.3 Sambaをドメインメンバーサーバとして設定する

主題396：Sambaのネームサービス
- 396.1 NetBIOSとWINS
- 396.2 アクティブディレクトリの名前解決

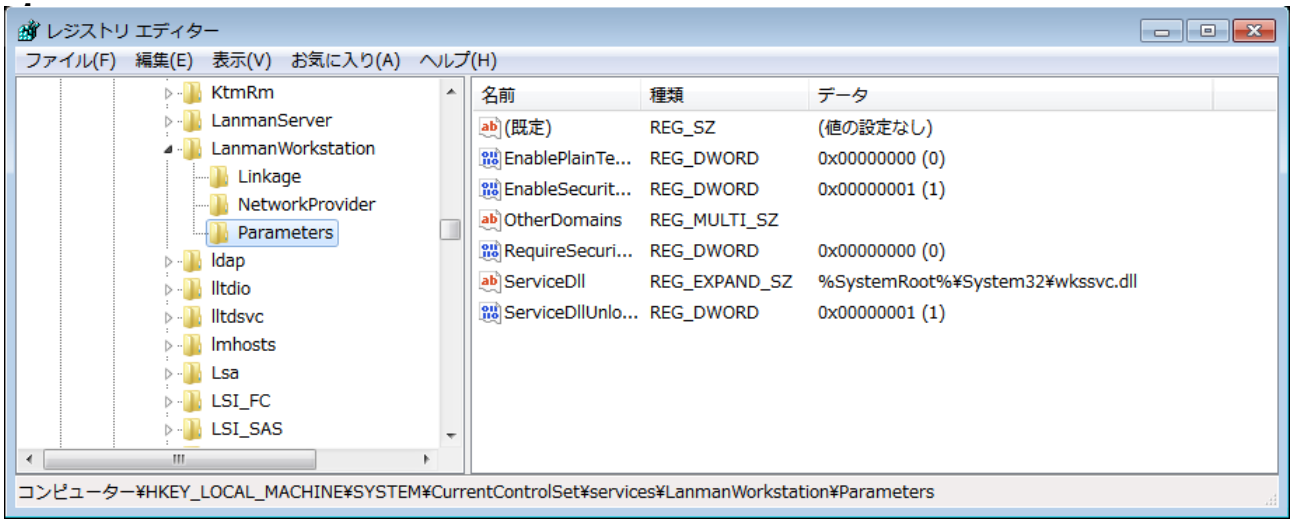
主題397：LinuxおよびWindowsクライアントの操作
- 397.1 CIFS連携
- 397.2 Windowsクライアントの操作

Samba 4による Active Directory構築

Samba 4 とドメインログオン

- 最新のWindows 8も含め、Windows Serverと同等のドメイン認証機能を利用可能

- Samba 3 で必要であったレジストリ変更操作は不要
  - HKLM¥SYSTEM¥CurrentControlSet¥Services¥Lanman¥Workstation¥Parameters¥DNSNameResolutionRequired = 0
  - HKLM¥SYSTEM¥CurrentControlSet¥Services¥Lanman¥Workstation¥Parameters¥DomainCompatibilityMode =



Samba 4と管理ツール

- Linux上は samba-toolコマンド
  - ドメイン管理系操作をサポート
    - ドメイン管理系
      - domain、drs、fsmo、gpo、sites
    - ユーザー・グループ管理系
      - user、group
    - DNS管理
      - dns
    - ouの追加については未サポート
- Windows端末からはMicrosoft標準ツール(RSAT)
  - Windows Vista、7、8用それぞれ提供

時刻同期

- DCとクライアント間の時刻は同期させる
  - クライアントをDCの時刻に合わせる

- Samba4

  # service ntpd start

  # chkconfig ntpd on

    - ntpの設定については今回は省略
- Windowsクライアント（Windows7）
  - ドメインに参加するとDCと自動的に時刻同期を行う
    - HKLM¥SYSTEM¥CurrentControlSet¥Services¥W32Time¥Parameters¥Type = NT5DS（ドメイン参加前はNTP）

    http://support.microsoft.com/kb/223184/ja

Samba 4 AD DC 設定情報

項目	設定内容
サーバー名	cent65k1
DNS名	samba4dom.com
NT ドメイン名	SAMBA4DOM
DNS フォワード先	192.168.2.2
サーバーの役割	DC
Administratorのパスワード	P@ssw0rd

- Administratorユーザーのパスワードは複雑性を満たす必要あり
  - 英大文字/英小文字/数字/記号のうち、3種類以上を含む
  - 文字列長は7文字以上

Samba 4 AD DC 構築 1

- 対話形式でドメイン設定
  - samba-tool コマンドでドメイン設定する際、「--interactive」を利用
    - 利用しない場合、オプションで個々に指定

```
# /opt/osstech/bin/samba-tool domain provision --interactive --
  use-rfc2307
  Realm [SAMBA4DOM.COM]:
  Domain [SAMBA4DOM]:
  Server Role (dc, member, standalone) [dc]:
  DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
  DNS forwarder IP address (write 'none' to disable forwarding) [XX.XX.XX.XX]:
 Administrator password:
 Retype password:
```

Samba 4 AD DC起動/確認1

- /etc/krb5.confと/etc/resolv.conf を修正
- Samba4プロセス起動

```
# service osstech-samba start
```

- smbclientによるアクセス確認

```
# /opt/osstech/bin/smbclient //localhost/netlogon -U
  Administrator
Enter Administrator's password:
Domain=[SAMBA4DOM] OS=[Unix] Server=[Samba 4.1.0-59.el6]
smb: ¥>
```

Samba 4.1 より、smbclientに「-m SMB2/SMB3」を指定することでSMB2/SMB3プロトコルでの通信も可能。

Samba 4 AD DC起動/確認2

- Kerberos 確認
  - チケット発行

```
# kinit administrator@SAMBA4DOM.COM
Password for administrator@SAMBA4DOM.COM:
Warning: Your password will expire in 41 days on Wed Dec 11 01:28:00 2013
```

  - チケット確認

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SAMBA4DOM.COM

Valid starting     Expires            Service principal
10/30/13 02:32:16  10/30/13 12:32:16
    krbtgt/SAMBA4DOM.COM@SAMBA4DOM.COM
renew until 11/06/13 02:32:13
```

Samba 4 AD DC起動/確認3

- SRV、Aレコード確認

```
# host -t SRV _ldap._tcp.samba4dom.com.
_ldap._tcp.samba4dom.com has SRV record 0 100 389  takeuchi104.samba4dom.com.

# host -t SRV _kerberos._udp.samba4dom.com.
_kerberos._udp.samba4dom.com has SRV record 0 100 88 takeuchi104.samba4dom.com.

# host -t A takeuchi104.samba4dom.com.
takeuchi104.samba4dom.com has address 10.0.104.104
```

samba-toolコマンドによるユーザー管理 1

- ユーザーの登録状況を確認

```
# /opt/osstech/bin/samba-tool user list
Administrator
krbtgt
Guest
```

- ユーザー登録
  - ユーザー名:cui-user1
  - パスワード:Secret123$

```
# /opt/osstech/bin/samba-tool user add cui-user1
New Password:
Retype Password:
User 'cui-user1' created successfully
```

samba-toolコマンドによるユーザー管理 2

- オプションを指定して登録
  - ユーザー名:cui-user2
  - パスワード:Secret123$
  - 姓:テスト
  - 名:ユーザー

```
# /opt/osstech/bin/samba-tool user add cui-user2
  Secret123$ ¥  --surname=テスト -given-name=ユーザー
    User 'cui-user2' created successfully
```

他にもオプションは存在するが、ADで登録する時の項目すべてを設定できるわけではない

samba-toolコマンドによるユーザー管理 3

- root権限によるパスワード強制変更
  - ユーザー名:cui-user1
  - 新パスワード:P@ssw0rd

```
# /opt/osstech/bin/samba-tool user setpassword ¥ --
  newpassword=P@ssw0rd cui-user1
    Changed password OK
```

samba-toolコマンドによるユーザー管理 4

- ユーザー自身によるパスワード変更
  - 該当ユーザーの認証やポリシー制限あり
    - ユーザー名:cui-user2
    - 元パスワード:Secret123$
    - 新パスワード:P@ssw0rd

```
$ /opt/osstech/bin/samba-tool user password ¥  --
  newpassword=P@ssword --password=Secret123$
Changed password OK
```

ただし、ユーザー作成直後は、デフォルトのパスワードポリシーによりエラーとなる。

```
ERROR: Failed to change password : samr_ChangePasswordUser3 for ¥
  'SAMBA4DOM¥cui-user2' failed: NT_STATUS_PASSWORD_RESTRICTION
```

samba-toolコマンドによるグループ管理 1

- グループの登録状況を確認

```
# /opt/osstech/bin/samba-tool group list
Domain Computers
Domain Admins
Domain Users
```

- グループ登録
  - グループ名:cui-group1

```
# /opt/osstech/bin/samba-tool group add cui-group1
Added group cui-group1
```

samba-toolコマンドによるグループ管理 2

- グループにメンバーを所属

```
# /opt/osstech/bin/samba-tool group addmembers cui-group1
  ¥
    cui-user1,cui-user2
Added members to group cui-group1
```

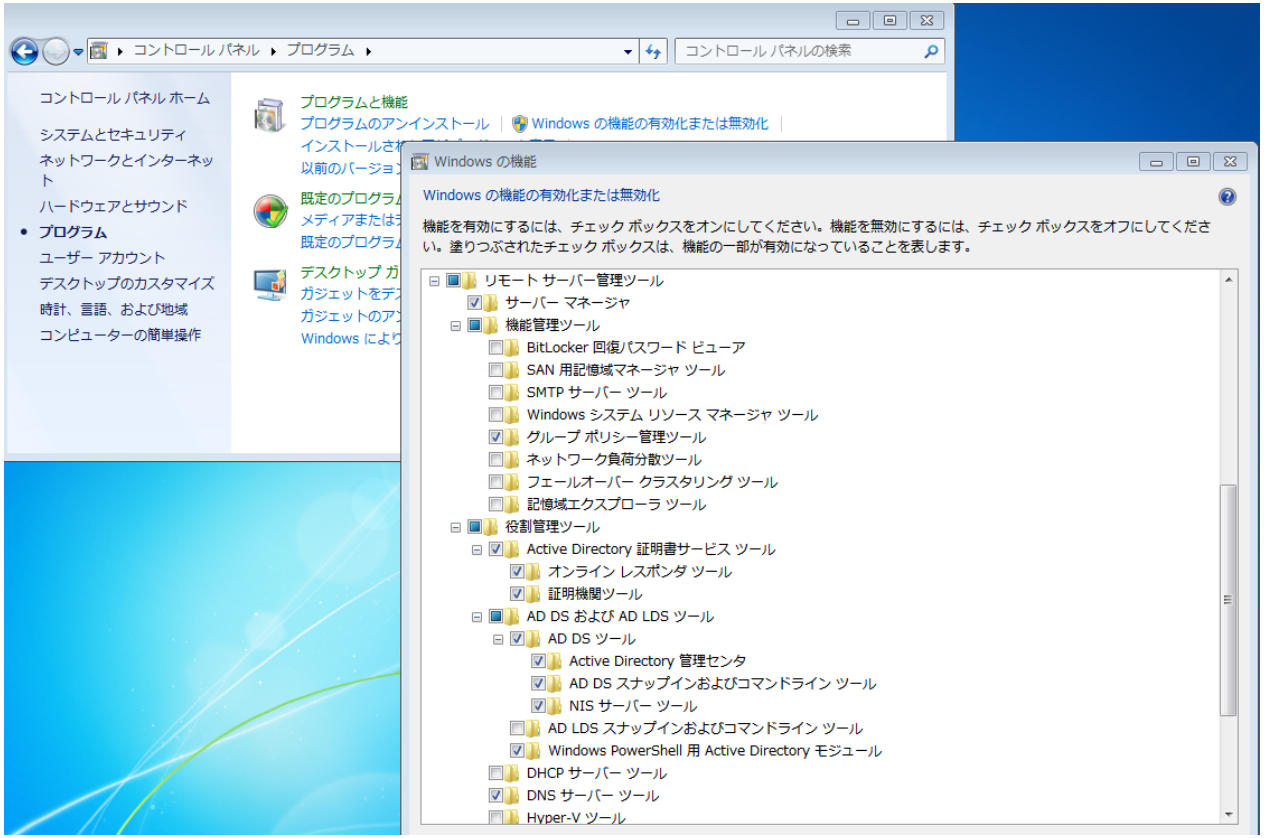
- グループのメンバーを確認

```
# /opt/osstech/bin/samba-tool group listmembers cui-group1
cui-user1
cui-user2
```

Windows7をドメイン参加させ、ADを管理

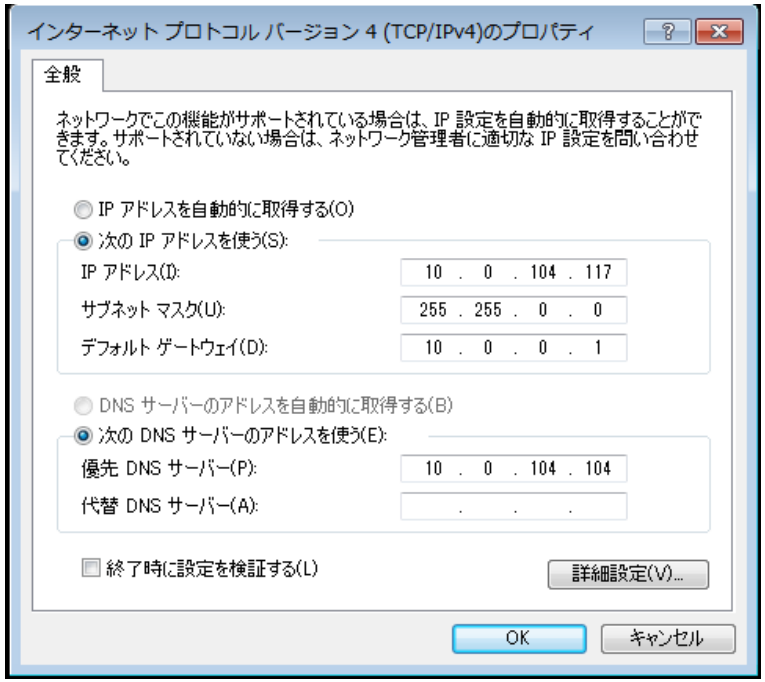
RSATを利用するための準備

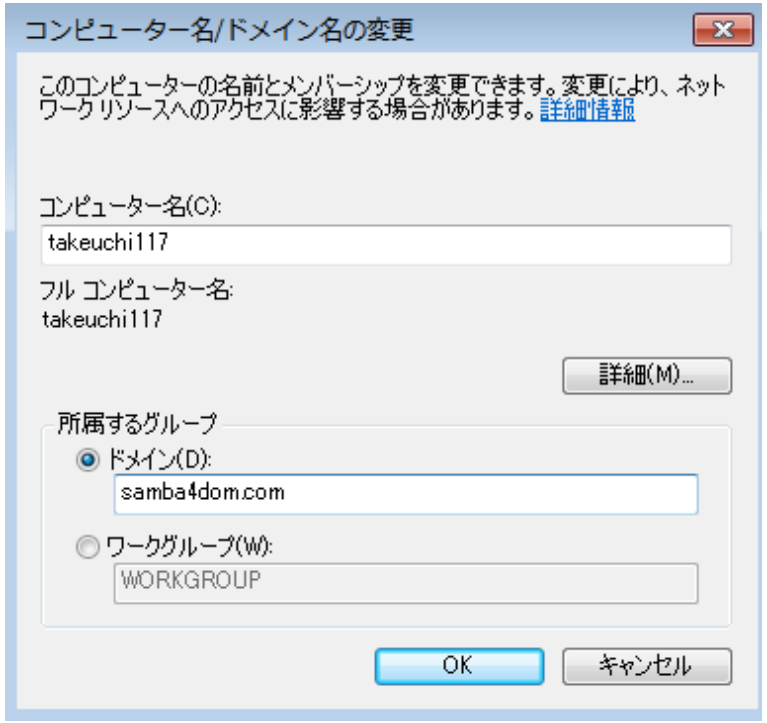
- RSATはインストールしただけでは利用不可
  - [コントロールパネル] – [プログラム] – [Windowsの機能の有効化または無効化] で [リモートサーバー管理ツール] を有効に



Windows7をドメイン参加

- Windows7をSamba4での AD DCにドメイン参加
  - DNSサーバーをSamba4サーバーに変更
  - ドメインをsamba4dom.comに変更





RSATによる情報確認

- RSATの起動は [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]
  - samba-toolコマンドで登録した情報の確認
  - Computersの確認
  - DNSマネージャー

RSATによる管理

- 組織単位(ou)の新規追加
- ユーザー登録
- グループ登録
  - グループにメンバー追加
- GPOを設定
  - Default Domain Policy を利用

パスワードポリシー 1

- GPOに設定項目が存在するが利用不可
- samba-toolコマンドで設定する必要がある
  - 現状のポリシー確認

```
# /opt/osstech/bin/samba-tool domain passwordsettings show
```

項目	ポリシー内容	設定内容
Password complexity	パスワードの複雑性	on
Store plaintext passwords	暗号化を元に戻せる状態でパスワードを保存	off
Password history length	パスワードの履歴保持	24
Minimum password length	パスワードの長さ	7
Minimum password age (days)	パスワードの変更禁止期間（日）	1
Maximum password age (days)	パスワードの有効期間（日）	42

パスワードポリシー 2

```
# /opt/osstech/bin/samba-tool domain passwordsettings set ¥
 --complexity=on/off
--store-plaintext=on/off
--history-length=回数
--min-pwd-length=長さ
--min-pwd-age=日数
--max-pwd-age=日数
```

Windows AD DCから Samba4 AD DCに切替

Windows AD DC 設定情報

項目	設定内容
サーバー名	takeuchi28
DNS名	testdom.com
NT ドメイン名	TESTDOM
realm	testdom.com
サーバーの役割	DC
Administratorのパスワード	P@ssw0rd

Samba4をWindows AD DCに参加

```
# /opt/osstech/bin/samba-tool domain join testdom.com DC ¥  --
    realm=testdom.com -U testdom¥¥Administrator
Finding a writeable DC for domain 'testdom.com'
Found DC takeuchi28.testdom.com
Password for [TESTDOM¥Administrator]:

workgroup is TESTDOM
realm is testdom.com
....
Joined domain TESTDOM (SID S-1-5-21-325366957-3734438017-426939442) as a
    DC
```

Samba4 AD DC起動/確認 1

- 起動

  # service osstech-samba start

- SRV、Aレコード確認

  # host -t SRV _ldap._tcp.testdom.com.

  _ldap._tcp.testdom.com has SRV record 0 100 389 takeuchi28.testdom.com.

  _ldap._tcp.testdom.com has SRV record 0 100 389 takeuchi114.testdom.com.

  # host -t SRV _kerberos._udp.testdom.com.

  _kerberos._udp.testdom.com has SRV record 0 100 88 takeuchi28.testdom.com.

  _kerberos._udp.testdom.com has SRV record 0 100 88 takeuchi114.testdom.com.

  # host -t A takeuchi114.testdom.com.

  takeuchi114.testdom.com has address 10.0.104.114

操作マスターをSamba4に移動 1

- 現状の操作マスターの確認

```
# /opt/osstech/bin/samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS  Settings, ¥
    CN=TAKEUCHI28,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
RidAllocationMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI28,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
PdcEmulationMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI28,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
DomainNamingMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI28,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
SchemaMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI28,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites,¥ CN=Configuration,DC=testdom,DC=com
```

操作マスターをSamba4に移動 2

- 操作マスターの移動

```
# /opt/osstech/bin/samba-tool fsmo transfer -role=all
```

- 移動後の操作マスターの確認

```
# /opt/osstech/bin/samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI114,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
RidAllocationMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI114,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
PdcEmulationMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI114,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
DomainNamingMasterRole owner: CN=NTDS Settings, ¥
    CN=TAKEUCHI114,CN=Servers,CN=Default-First-Site-Name,CN=Sites, ¥
    CN=Configuration,DC=testdom,DC=com
SchemaMasterRole owner: CN=NTDS Settings, ¥ CN=TAKEUCHI114,CN=Servers,CN=Default-
    First-Site-Name,CN=Sites, ¥ CN=Configuration,DC=testdom,DC=com
```

ユーザー登録/確認

- samba-toolコマンドでユーザー登録
  - ユーザー名:samba-add
  - パスワード:P@ssw0rd

```
# /opt/osstech/bin/samba-tool user add samba-add P@ssw0rd
```

- RSAT(Windows Server 2008 R2上)よりユーザー登録
  - ユーザー名:windows-add
  - パスワード:P@ssord
- Windows7 でドメインログオン
  - windows-add、samba-add両ユーザーでログオン

Windows AD DCをシャットダウン後

- samba-toolコマンドでユーザー登録
  - ユーザー名:samba-add1
  - パスワード:P@ssw0rd

```
# /opt/osstech/bin/samba-tool user add samba-add1
P@ssw0rd
```

- Windows7 でドメインログオン
  - samba-add1ユーザーでログオン

Windows AD DCにてdcpromoより本来、[Active Directoryドメインサービス]のアンインストールが可能だが、現状 DC=ForestZones の転送で失敗する為、今回はシャットダウンすることとする

付録.

Samba vs Windows比較表

参考資料：日経BP

Samba 4によるWindowsネットワーク構築

http://itpro.nikkeibp.co.jp/article/COLUMN/20131018/511929/

「オープンソースソフトウェア」の新しい価値を創造し、高機能・高品質を追求する

統合認証 シングルサインオン アイデンティティ管理ソリューション

OSSTech オープンソース・ソリューション・テクノロジ株式会社 Open Source Solution Technology Corporation
〒141-0031 東京都品川区西五反田1-29-1 コイズミビル 8F Tel:03-6417-0753 Fax:03-6417-0754 Mail:info@osstech.co.jp