

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 ～



OSSTech

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

お問い合わせ info@osstech.co.jp

オープンソース・ソリューション・テクノロジー (株) 会社紹介



OSSTech

オープンソース・ソリューション・テクノロジー株式会社

「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



Unicorn IDM

ID管理

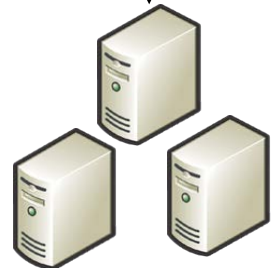


システム管理者

ID連携

Active Directory **SAMBA**
OpenLDAP

ファイルサーバー LDAP



Web アプリ

Google Apps
Salesforce
Shibboleth
クラウド

SSO

OpenAM

Windows
ドメインログオン

ログイン



ユーザー

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

OpenLDAP

SAMBA



●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

- 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. はい、できます。

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。

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！**

LPIC-3 300 出題範圍

395.2 Samba4 as an AD compatible Domain Controller (weight: 3)

http://wiki.lpi.org/wiki/LPIC-3_300_Objectives

395.2 Samba4 as an AD compatible Domain Controller (weight: 3)

Candidates should be able to configure Samba 4 as an AD Domain Controller.

Key Knowledge Areas:

Configure and test Samba 4 as an AD DC.

Using smbclient to confirm AD operation.

Understand how Samba integrates with AD services: DNS, Kerberos, NTP, LDAP.

The following is a partial list of the used files, terms and utilities:

smb.conf.

server role.

samba-tool domain (with subcommands).

samba.

396.2 Active Directory Name Resolution (weight: 2)

Candidates should be familiar with the internal DNS server with Samba4.

Key Knowledge Areas:

Understand and manage DNS for Samba4 as an AD Domain Controller.

DNS forwarding with the internal DNS server of Samba4.

The following is a partial list of the used files, terms and utilities:

samba-tool dns (with subcommands).

smb.conf.

dns forwarder.

/etc/resolv.conf

表 1. SambaとWindowsサーバーとの比較

機能	Samba 3.6	Samba 4.1	Windows Server 2008/2012
リソース管理			
ユーザー情報の格納場所	LDAP、簡易DB、テキストなどが利用可能	内蔵LDAP 外部のLDAPも利用できるが制限有り	Active Directory または 内部の独自DB
ユーザー情報の複製機能	△LDAPの複製機能を利用 Windows互換の複製機能は持たない	○	○
日本語ユーザー名	△利用は推奨しないが username map機能を使えば可能	○	○
日本語グループ名	△利用は推奨しないが username map機能を使えば可能	○	○
グローバルユーザー/ローカルユーザー	○	○	○
グローバルグループ/ローカルグループ	○	○	○
ネストグループ (グループの中にグループを 入れ子にするような階層化)	△AD互換のグループの入れ子はできない、 一部NT互換のネストグループ (ローカル グループの中にグローバルグループを入 れ子にするような階層化) は可能だが互換 性も低く、GUIで管理するのは難しい	○	○
日本語コンピュータ名	△利用は推奨しないが username map機能を使えば可能	○	○
通信プロトコル/認証方式			
LANMAN認証	○	○	○
NLM認証	○	○	○
NLMv2認証	○	○	○
Kerberos5認証	△メンバサーバの時のみ可能	○	○
SMB2	○	○	○
SMB3	×	○	○
セキュアチャネル	○	○	○
SMB署名	○	○	○
SPNEGO (RFC2478で規定されたSimple and Protected NEGOCIATION)	○	○	○
ドメイン管理			
ドメインレベル	NTドメイン	Windows 2008 ADドメイン互換	Windows 2008/2012 ADドメイン
ドメインログオン	○	○	○
PDC (プライマリドメインコントローラ)	○	○FSMO	○FSMO
BDC (バックアップドメインコントローラ)	○	○GC	○GC
ログオンスクリプト	◎ログオンスクリプトの動的生成/変更可 能	◎ログオンスクリプトの動的生成/ 変更可能	○固定スクリプトを実行可能
移動プロファイル	◎読み込み専用プロファイルもサポート	○	○
NT 4.0相当のユーザーポリシー (NT 4.0/2000/XP)	○	×	×
Windows 98相当のグループポリシー (95/98/Me)	○	×	×
Windows 2008相当のグループポリシー	×	○	○
複雑なパスワードの強制	◎外部スクリプトを使って カスタマイズ可能	○	○
パスワード履歴	○	○	○
明示的な片方向の信頼関係	○	○	○
推移的な双方向の信頼関係	×	○	○
ファイル/プリントサーバ機能			
ユーザー/グループによる容量制限	◎ディレクトリ単位にも対処可能	○	○
論理ボリュームマネージャ	○Sambaが動作するOSに依存	○Sambaが動作するOSに依存	○
ボリュームシャドウコピー (スナップショット) 機能	○Sambaが動作するOSに依存	○Sambaが動作するOSに依存	○NTFS必須
ゴミ箱機能	○	○	×
マッキントッシュ連携	○Netatalkをインストールすることで可能	○Netatalkをインストールすること で可能	○マッキントッシュサービスをイ ンストールすることで可能
UNIX NFS連携	○カーネルレベルによる OPLOCK連携可能	○カーネルレベルによる OPLOCK連携可能	○Service for UNIX (SFU, SUA) をイ ンストールすることで可能
ユーザーホーム機能	○	○	○
MS-DFS (ルートおよびサブディレクトリ)	○	○	○
MS-DFS Proxy	○	○	○
ACL機能 (ユーザー/グループによるアクセス制御)	○Sambaが動作するOSに依存 またはVFSモジュールでSamba上でのNTFS互 換ACLサポート	○Sambaが動作するOSに依存 またはVFSモジュールでSamba上での NTFS互換ACLサポート	○NTFS必須
ホスト名によるアクセス制御	○	○	×
日本語ディレクトリ/ファイル名	○	○	○
READ権のないファイルを見えなくする	○	○	○
WRITE権のないファイルを見えなくする	○	○	×
ユーザーモジュールによる共有機能の拡張・カス タマイズ	○標準で監査機能、ウィルスチェックなど を搭載。1つの共有に複数のモジュールを ロード可能	○標準で監査機能、ウィルスチェッ クなどを搭載。1つの共有に複数のモ ジュールをロード可能	○WINAPIでユーザーが作成可能
同一サーバーに複数のNetBIOS名を付ける	○smb.confで容易に指定可能	○smb.confで容易に指定可能	△レジストリ変更が必要でサポ ート対象外
スプールしながらの印刷	×	×	○
PDFライター機能	○GhostScriptとの連携	○GhostScriptとの連携	×
プリンタドライバ配布機能	○	○	○
名前解決機能			
DNSサーバー	×	○内蔵と外部の両方が利用可能	○
WINSサーバー	○	△	○
WINSクライアント	○	△	○
WINS複製	△外部スクリプトによりPushは可能	△	○
WINS静的マッピング	○ wins.datの直接編集	△	○
WINSとDDNSとの連携	○ wins hook機能	△	×
ブラウジング			
ドメインマスタブラウザ	◎ワークグループ構成でも可能	◎ワークグループ構成でも可能	○
リモートアナウンス	◎任意のワークグループ、ドメインにも可 能	◎任意のワークグループ、ドメイ ンにも可	○信頼するドメインのみ
ポテンシャルブラウザ	○	○	○

「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～



OSSTech

オープンソース・ソリューション・テクノロジー株式会社

2013/11/06

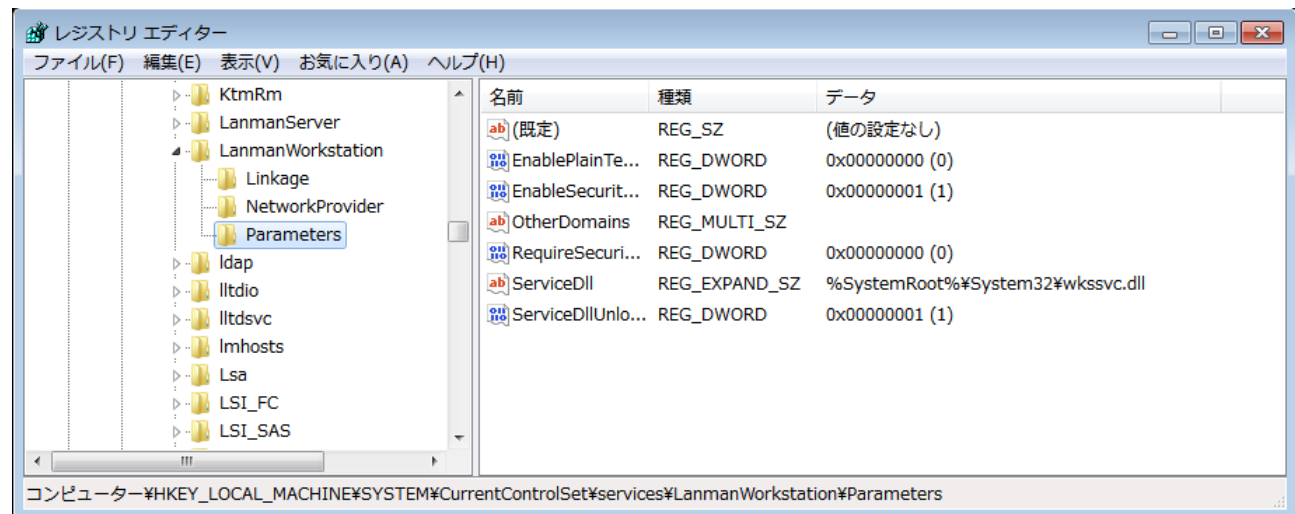
竹内 英雄

目次

- Samba 4 AD DC構築デモ
 - osstech版 rpmパッケージインストール
 - samba-toolコマンドによるAD構築
 - Windows7をドメイン参加
 - ユーザー管理 (samba-tool、RSAT、CSVDE)
 - RSAT:リモートサーバー管理ツール
 - グループ管理(samba-tool、RSAT)
 - ou追加(RSAT)
 - GPO追加(RSAT)
 - GPO:グループポリシー
- Windows AD DCからSamba4 AD DCに切り替えデモ

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 = 1



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

デモ環境

- Samba4
 - CentOS 6.4 64bit ([Minimal]インストール)
 - hostname:takeuchi104.samba4dom.com
 - IPアドレス:10.0.104.104
 - インストール後、iptables停止、selinuxをdisabled
 - 作業用にopenssh-clients、krb5-workstation、bind、bind-utils、ntpパッケージをyumコマンドでインストール済
 - DNSはSamba4内蔵DNSを利用
- Windowsクライアント
 - Windows7
 - hostname:takeuchi117.samba4dom.com
 - IPアドレス:10.0.104.117
 - RSAT:<http://www.microsoft.com/ja-jp/download/details.aspx?id=7887>

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>

Samba4 サーバーによるAD DC (Active Directory ドメインコントローラ) 構築をしよう

Samba 4 動作環境要件

- 各種ライブラリ (osstech版 rpmインストール時)

```
# yum install ksh perl pkgconfig avahi-libs gnutls cups-libs \  
perl-Parse-Yapp
```

Samba 4 動作環境要件

- 各種ライブラリ(ソースからBuild時)
 - http://wiki.samba.org/index.php/Samba_4/OS_Requirements
 - Red Hat Enterprise Linux or CentOS
- ```
yum install gcc libacl-devel libblkid-devel gnutls-devel \
readline-devel python-devel gdb pkgconfig \
krb5-workstation zlib-devel setroubleshoot-server \
libaio-devel setroubleshoot-plugins policycoreutils-python \
libsemanage-python setools-libs-python setools-libs \
popt-devel libpcap-devel sqlite-devel libidn-devel \
libxml2-devel libacl-devel libsepol-devel libattr-devel \
keyutils-libs-devel cyrus-sasl-devel cups-devel bind-utils
```

# Samba 4 インストール

```
rpm -ivh osstech-base-3.0-86.el6.noarch.rpm \
osstech-daemontools-1.03-40.el6.x86_64.rpm \
osstech-gamin-0.1.10-14.el6.x86_64.rpm \
osstech-libiconv-1.10-14.el6.x86_64.rpm \
osstech-samba-4.1.0-59.el6.x86_64.rpm \
osstech-samba-client-4.1.0-59.el6.x86_64.rpm \
osstech-samba-common-4.1.0-59.el6.x86_64.rpm \
osstech-samba-libs-4.1.0-59.el6.x86_64.rpm \
osstech-samba-libs-devel-4.1.0-59.el6.x86_64.rpm \
osstech-samba-pidl-4.1.0-59.el6.x86_64.rpm \
osstech-samba-python-4.1.0-59.el6.x86_64.rpm \
osstech-samba-test-4.1.0-59.el6.x86_64.rpm \
osstech-samba-winbind-4.1.0-59.el6.x86_64.rpm
```

# Samba 4 AD DC 設定情報

| 項目                  | 設定内容          |
|---------------------|---------------|
| サーバー名               | takeuchi104   |
| DNS名                | samba4dom.com |
| NT ドメイン名            | SAMBA4DOM     |
| DNS フォワード先          | 10.0.0.4      |
| 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

- 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
```

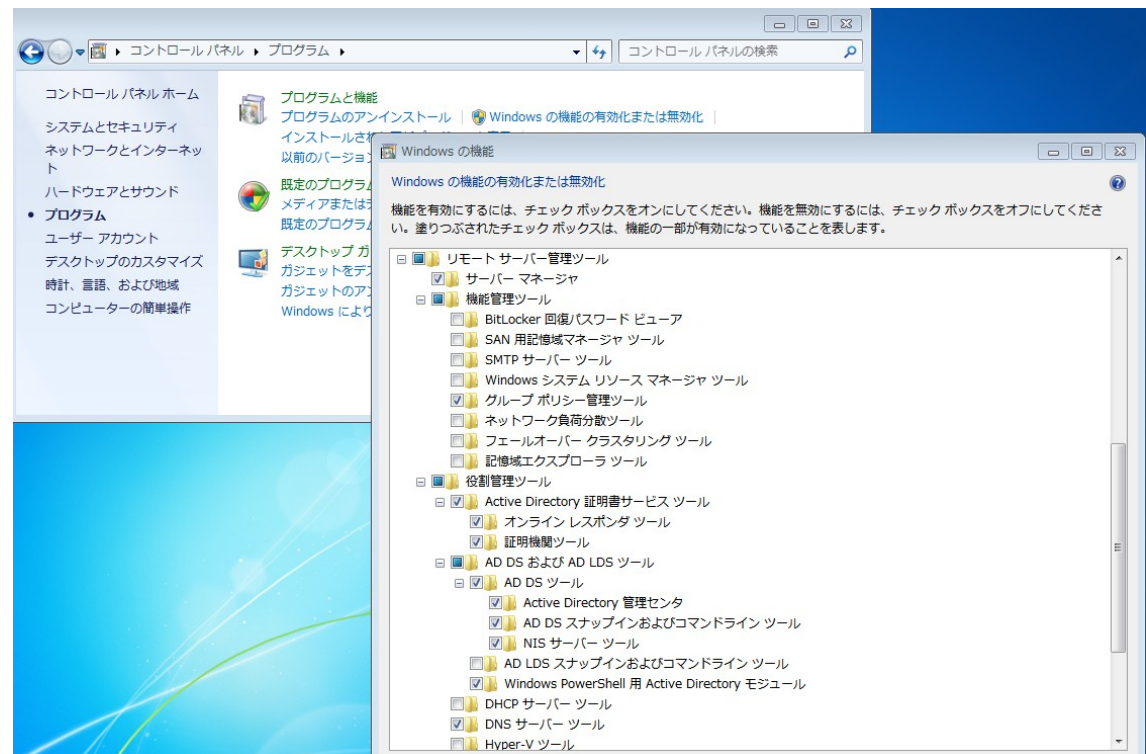
```
cui-user1
```

```
cui-user2
```

**Windows7をドメイン参加させ、ADを管理してみよう**

# RSATを利用するための準備

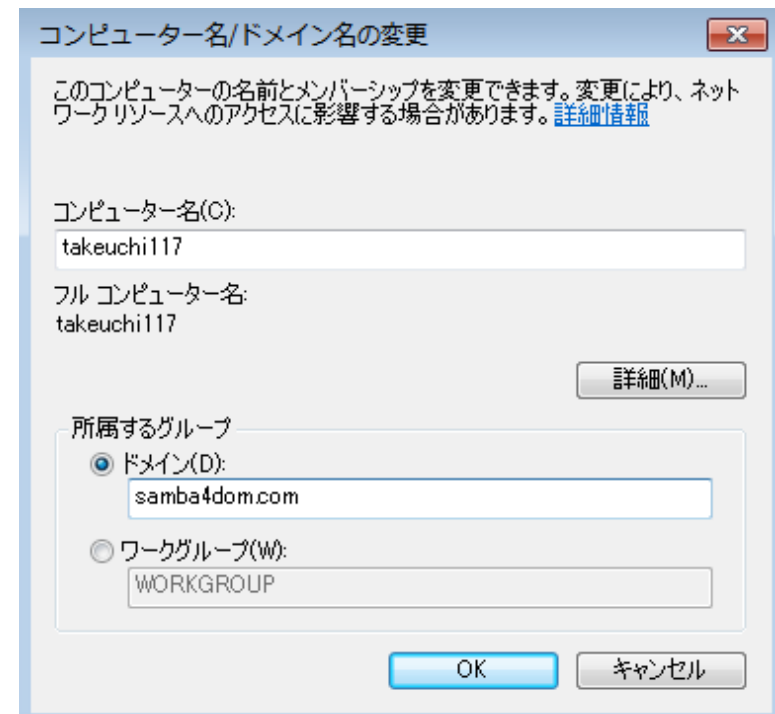
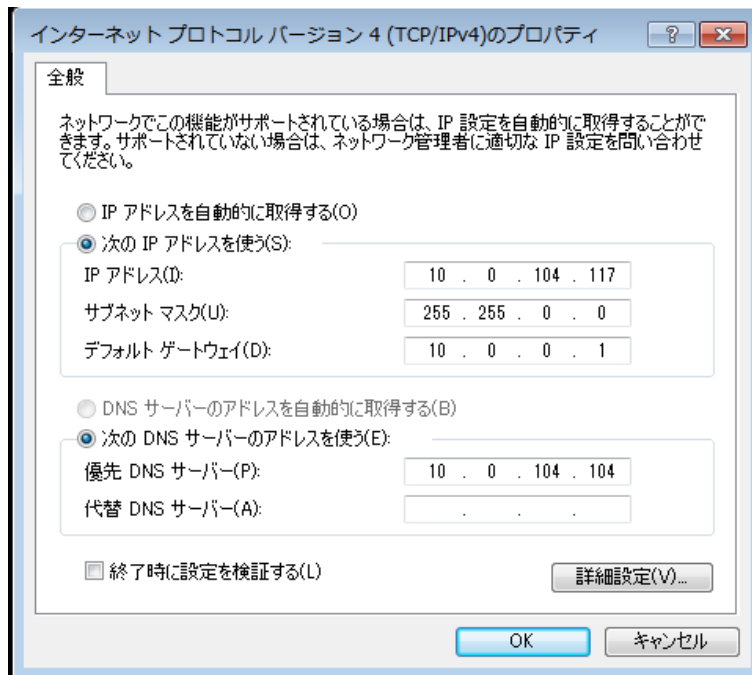
- RSATはインストールしただけでは利用不可
  - [コントロールパネル]-[プログラム]-[Windowsの機能の有効化または無効化]で[リモートサーバー管理ツール]を有効に





# 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に切り替えてみよう

# デモ環境

- Windows AD DC
  - Windows Server 2008 R2
    - hostname:takeuchi28.testdom.com
    - IPアドレス:10.0.104.28
    - フォレスト機能レベル:Windows Sever 2008 R2
- Samba4
  - CentOS 6.4 64bit ([Minimal]インストール)
    - hostname:takeuchi114.testdom.com
    - IPアドレス:10.0.104.114
      - Samba4パッケージのインストールまで完了

# 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

- 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



# OSSTech

「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

OpenAMはオープンソース・ソリューション・テクノロジー株式会社の日本での登録商標です。(登録 第5398965号)

 **OSSTech** オープンソース・ソリューション・テクノロジー株式会社 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