最新Samba 4.0.0 新機能のすべて

日本Sambaユーザ会

たかはしもとのぶ（髙橋基信）

monyo@samba.gr.jp

Samba 4.0系列とは

- Active Directory（以下AD）のドメインコントローラ（以下DC）機能（以下ADDS）を実装したSambaの最新版
  - 現在の最新版はSamba 4.0.3(2013/02/05)
  - ADDS機能とそれ以外でバイナリが二分されている
    - ADDS機能→sambaバイナリ
    - その他機能→レガシーバイナリ（smbd/nmbd/winbindd）
    - sambaバイナリとレガシーバイナリは共存不可
  - ファイルサーバなど、ADDS以外の機能については、レガシーバイナリの使用が推奨

※レガシーバイナリという用語はわたしの造語です

レガシーバイナリの特徴、変更点

- 前バージョン（3.6系列）の特徴を引き継ぐ
  - ADのメンバサーバ、ファイル/プリンタサーバ、SambaドメインのDCなどとして従来通り使用できる
  - 設定方法は従来と基本的に変わらず
    →Samba 3.X系列の知識で設定可能
- 主な変更点
  - security = share/serverが廃止
    - 元々Windows 9x由来の機能であり、サポートが困難に
  - SMB2.1（大半の機能）、SMB3.0（主要機能）サポート
  - CTDBによるクラスタ機能が正式サポート

sambaバイナリの特徴

- ADDSに特化
  - nmbd、smbd、winbinddを包含した単一プロセス
- DCとして必要なサービスの大半を単独で実装
  - 外部ライブラリへの依存性を極力排除
    - Kerberos（Heimdal Kerberosをソースに取り込み）
    - LDAP（独自実装）
      - **OpenLDAPの使用は考慮されていない**（alpha15以降）
        →OpenLDAPではADが必要とする機能をサポートできないため
  - 別プロダクトと連携して実現している機能
    - DNS（BIND）→内蔵DNSが標準だが、大規模環境ではBIND連携推奨、NTP（ntpd）
    - スクリプティング（Python）← Pythonがないとビルド不可

Samba 4.0によるADの構築

- コンパイル、インストール
  - Samba4-HOWTO通りに行えばほぼ間違いなし
    - Samba 3.X系列より依存ライブラリは減少している
- 初期設定
  - samba-tool domain provisionコマンドを実行して smb.confファイルを生成 & smb.confを修正
  - DNSとNTP関連を適宜追加で設定する
- sambaプロセスの起動
  - 「samba」という名称のプロセスを起動する
    - 従来のsmbd/nmbd/winbinddは起動不要

※詳細は、SAMBA4-HOWTO (http://wiki.samba.org/index.php/Samba4/HOWTO）やSoftware Design誌2013年2月号などを参照してください

samba-tool domain provisionコマンド

- 初期設定を行うpythonスクリプト
  - 最低限のsmb.confも併せて生成
  - ADDSの（最初の）サーバを構築する際は、必ず本スクリプトを実行する必要がある

オプション名	デフォルト	意味
--realm	ー	レルム名（FQDN名の大文字）
--domain	ー	NetBIOSドメイン名
--adminpass	（ランダム文字列）	Administratorのパスワード（3種類以上の文字種からなるパスワード必須）
--dns-backend	SAMBA_INTERNAL	DNS実装方式（次スライド参照）
--use-ntvfs	（なし）	ファイルサーバ実装方式（次スライド参照）
--use-rfc2307	（なし）	UNIX属性を有効化

DNSとファイルサーバの設定

- DNSとして以下の3種類の方式をサポート

方式	概要	特徴
Samba内蔵	・DNSサーバはSamba内蔵 ・ゾーン情報はADから取得	・設定が簡単 ・基本的な機能のみ実装
BIND9DLZ モジュール	・DNSサーバはBIND9 ・ゾーン情報はADから取得 ※BIND9のDLZ機能を使用	・複雑、大規模環境への適用が可能 ・DLZ機能に対応したBIND 9.7以降が必要
BIND9静的 ファイル	・DNSサーバはBIND9 ・ゾーン情報はBIND9のゾーンファイルから取得	・複雑、大規模環境への適用が可能 ・Sambaの設定変更に伴うゾーン情報の更新を手作業で行う必要がある

- ファイルサーバとして以下の方式をサポート

方式	概要	特徴
s3fs	・バックエンドで起動されたsmbdがファイルサーバ機能を実現	・枯れている ・UNIX側のACLとの相互接続性あり
ntvfs	・samba内蔵のファイルサーバ機構を使用	・現時点では安定性に難あり? ・UNIX側のACLとは連携しない

参考:コマンド実行例

- 対話的実行、非対話的実行いずれも可能

対話的実行

root@squeeze32-2:~# **/usr/local/samba/bin/samba-tool domain provision**
Realm [LOCALDOMAIN]: **SAMBA40AD3.SAMBA.LOCAL**
Domain [SAMBA40AD3]:
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) [192.168.135.32]: **192.168.135.2**
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
…
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: squeeze32-2
NetBIOS Domain: SAMBA40AD3
DNS Domain: samba40ad3.samba.local
DOMAIN SID: S-1-5-21-4212942094-2789858589-3300345304

非対話的実行

root@squeeze32-2:~#
/usr/local/samba/bin/samba-tool domain provision --realm=SAMBA40AD3.SAMBA.LOCAL --domain=SAMBA40AD3 --adminpass='P@ssw0rd' --use-rfc2307
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up secrets.ldb
Setting up the registry
…
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: squeeze32-2
NetBIOS Domain: SAMBA40AD3
DNS Domain: samba40ad3.samba.local
DOMAIN SID: S-1-5-21-2691997093-816562956-3944966943

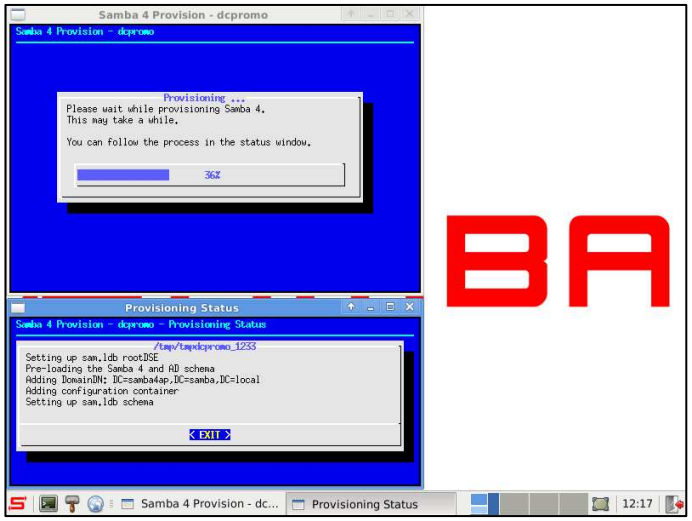
NTP（時刻同期）の設定

- ADDSでは時刻同期が必須
  - Kerberos認証のため、時刻のずれを5分以内に抑える必要がある
  - 同期方法はなんでもよい（NTP以外でも可）
- ntpd 4.2.6以降は、セキュアなNTPを実装済
  - configureで--enable-ntp-signdを有効にした上で、以下のような設定を行うことで、時刻同期を許可するクライアントを同一ADのクライアントに制限可能

```
ntpsignedsocket /usr/local/samba/var/lib/ntp_signd/
restrict default mssntp
```

参考：Samba4アプライアンス

- ドイツのSerNetから、Samba 4.0のADDS機能を設定済のアプライアンスが提供
  - Samba 4.0のドメイン機能を手軽に試したい人向け
    - http://ftp.sernet.de/pub/samba4AD/sernet-samba4-appliance/ からISOイメージを入手可能
    - 普通にインストールするだけで、Samba4ドメイン環境を簡便に構築可能



Samba 4.0によるADの設定

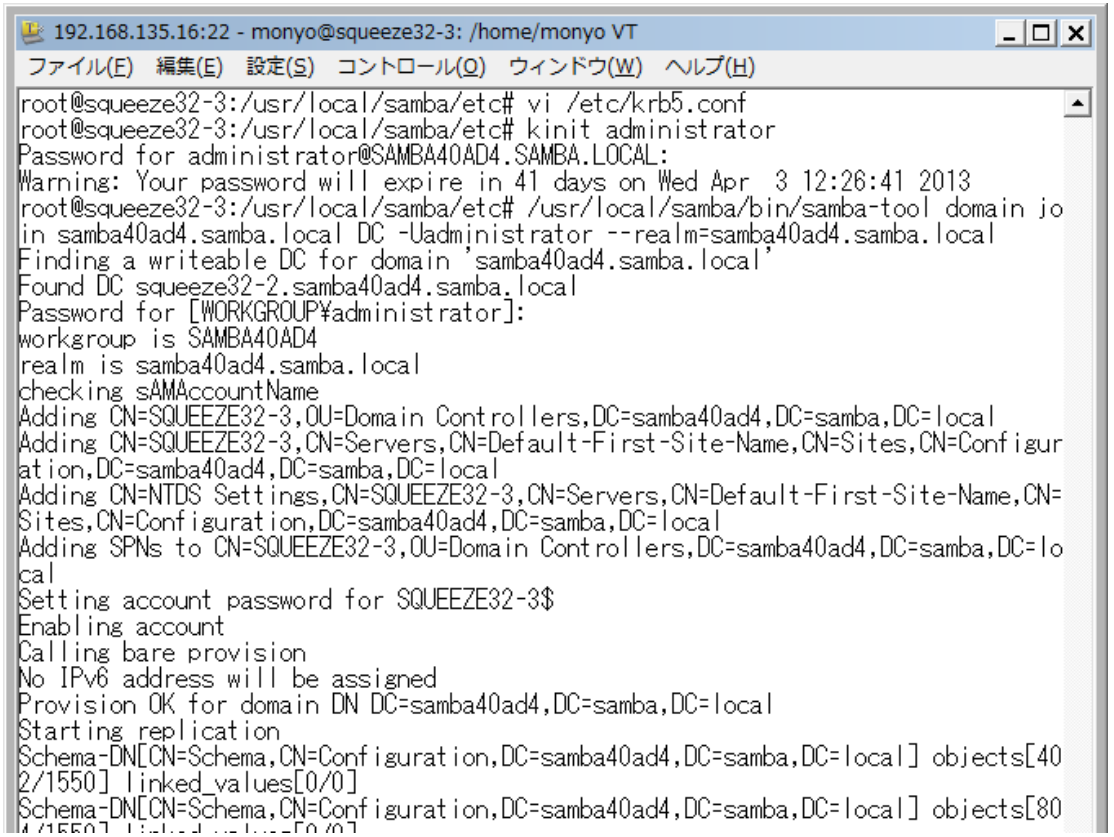
- smb.confの設定はあまり必要でない
  - 実はスクリプトが生成したままでも使えてしまう
- samba-toolによる動的な設定の増加
  - AD周りの設定は、ほぼコマンドorGUI
  - ファイルサーバのアクセス制御もGUIから行うのが基本
  - Windows的スキルがないと管理しきれない

```
# Global parameters
[global]
        workgroup = SAMBA40AD3
        realm = SAMBA40AD3.SAMBA.LOCAL
        netbios name = SQUEEZE32-2
        server role = active directory domain controller
        dns forwarder = 192.168.135.2
        idmap_ldb:use rfc2307 = yes

[netlogon]
        path = /usr/local/samba/var/locks/sysvol/samba40ad3.samba.local/scripts
        read only = No

[sysvol]
        path = /usr/local/samba/var/locks/sysvol
        read only = No
```

スクリプトの生成したsmb.conf例

参考：Samba 4.0のDCを既存ADに追加

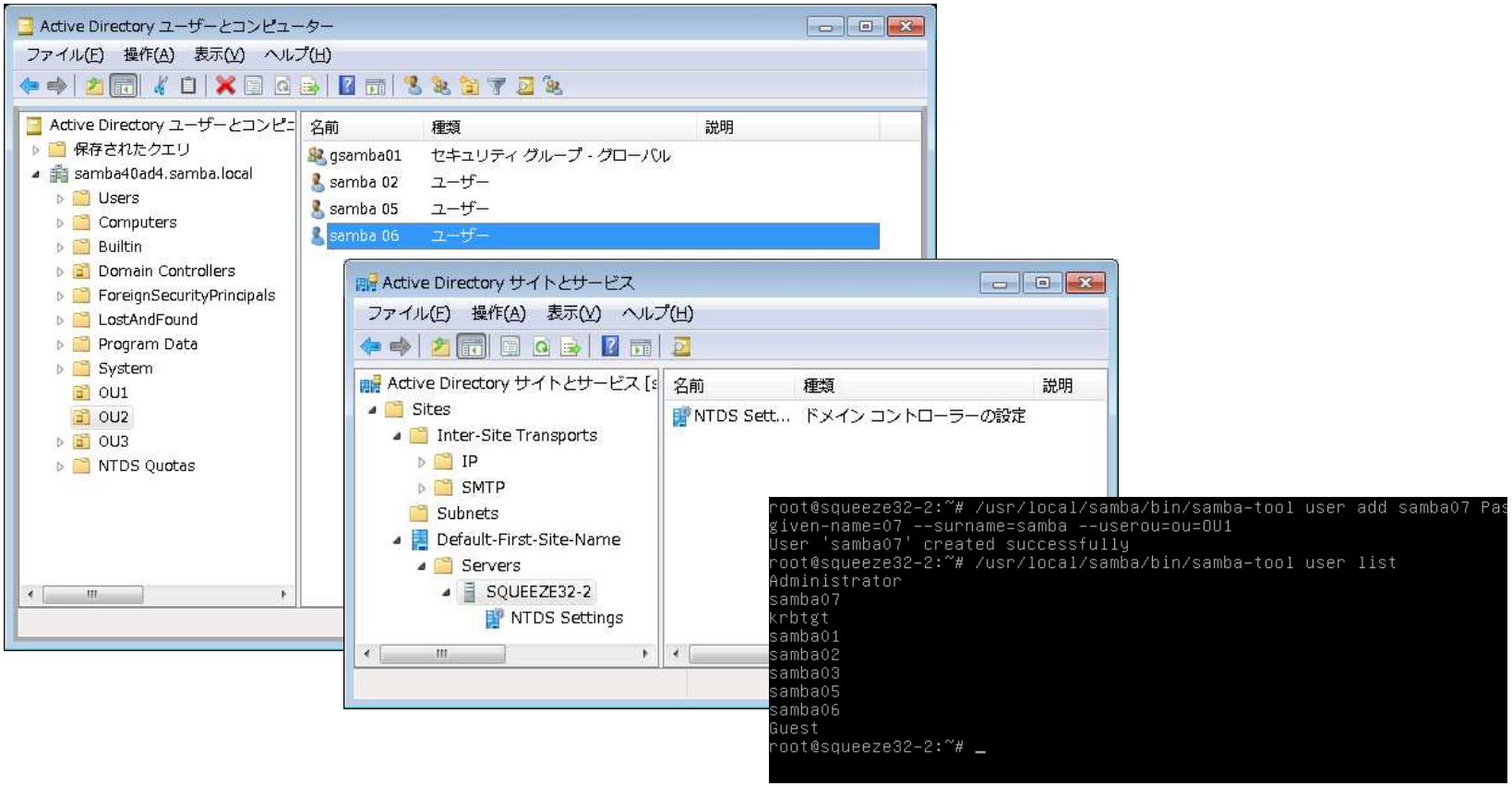
- 追加自体は特に問題なし
- SYSVOL共有は、rsyncなどで手動同期させる必要がある



https://wiki.samba.org/index.php/Samba4/HOWTO/Join_a_domain_as_a_DC

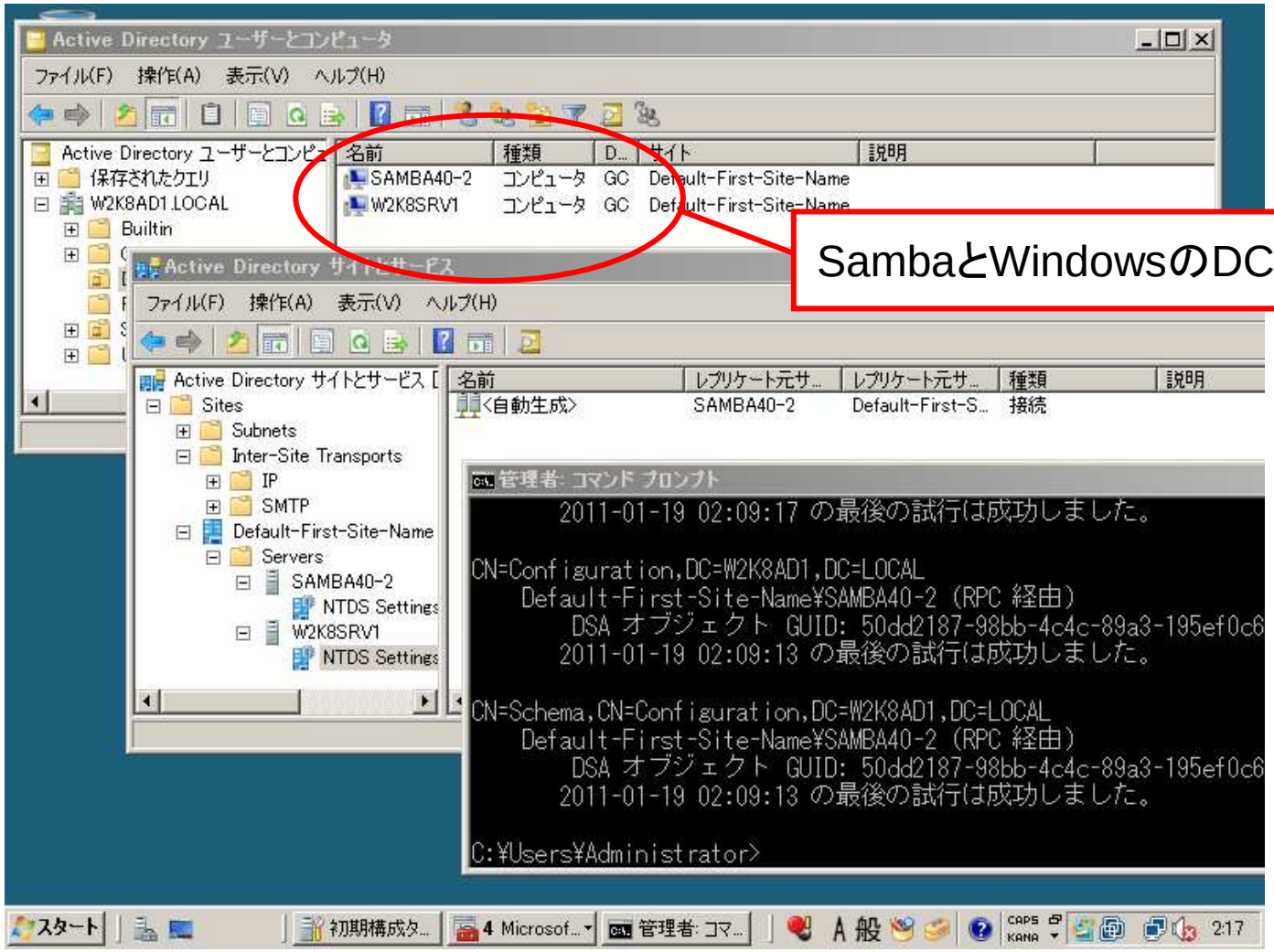
Samba 4.0によるADの操作

- 基本的には各種Windows管理ツールから操作
  - samba-toolによるコマンドライン操作も可能



参考：SambaとWindowsのDC混在

- SambaのDCとWindowsのDCの混在



Samba 4.0によるADの機能

- 大規模環境向け機能を中心に未サポート機能が散見されるが、基本的な機能はほぼサポート

項目	Samba 4.0系列	【参考】Win 2008 R2
フォレスト・ドメイン機能レベル	◎	◎
FSMO操作	◎	◎
サイト	◎	◎
信頼関係	◎	◎
マルチフォレスト・ドメイン	×	◎
Windows DCの参加	○（Win 2012は現在不可?）	◎
RODCの参加	△（いろいろトラブルがあるよう…）	◎
ディレクトリ複製（DRS）	○	◎
ファイル複製（FRS）	×（rsyncなどで別途対応必要）	◎
OUによる権限の委任	○（一部不具合があるっぽい）	◎
グループポリシ	○（ACL機能に一部不具合あり）	◎
ドメインベースDFS	△（ADDSに必要な範囲）	◎

既存のSambaドメインからの移行

- （もちろん）サポートされている
  - samba-tool domain classicupgrade というコマンドが用意されている
    - インプレースアップグレード前提
  - アップグレード元のSambaドメインのデータベースにゴミや不整合があると移行に失敗するので移行リハできちんと取り除いておくこと（SID重複など）

SambaによるAD上のUNIXユーザ管理

- メンバサーバ上 →以前と同じ
- DC上 → サポートレベルは（体感的に）低下
  - Winbind機構が必ず動作
    - UNIXユーザのUID/GIDは自動生成（3,000,000~）
    - シェルなどを個別設定できない
- UNIXユーザの属性を制御したい場合は…
  - SambaのユーザDB（LDBファイル）を直接書き換え →UID、GIDを変更可能
    - ldb_modifyなどのコマンドを使用
    - 直接書き換えを不要とするパッチあり。テスト中とのこと https://bugzilla.samba.org/show_bug.cgi?id=9520